

Infraon Infinity

User Guide

INFRAON INFINITY USER GUIDE

Information in this document is subject to change without prior notice. Companies, names, and data used in examples herein are fictitious and for illustration purposes only unless otherwise stated. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose without the express permission of Infraon Corp.

ABOUT THIS DOCUMENT

This document aims to outline the features of Infraon products and give detailed information on how to customize & use all the modules available within Infraon products. This document contains sensitive information. Access to this document or the content within should be provided only to authorized users of Infraon products software on a need-to-know basis.

Any unauthorized use or sharing of information in this document will be considered a breach of respective confidentiality/copyright and shall be treated accordingly.

Table of Contents

INFRAON INFINITY USER GUIDE	2
ABOUT THIS DOCUMENT	2
Getting Started	12
Welcome to Infraon!.....	12
Know Infraon!.....	13
Top Panel	14
Left Menu Panel.....	14
Notification Icon	15
User's first login	16
Workspace	17
Add the Ticket/ Request/ Change/ Problem/ Release.....	17
Dashboard.....	22
What you see on the screen.....	22
Widgets	23
Categories	23
Add Dashboard	27
Instructions to 'Add Dashboard'.....	27
Instructions to 'Edit the Dashboard'	28
Asset.....	29
How does it work?	29
Asset Types.....	32
Steps to Look for a Specific Asset	32
Asset Categories/Sub-Categories	33
Mandatory Asset Properties	33
Instructions to add the Asset Category.....	35
Asset Grid Page	37
Add Asset/Add Item	39
Instructions to 'Add Single Asset'.....	39
Instructions to 'Import from CSV'	42
Asset Information – SDH / PDH	43
Instructions to Schedule RDP	44
Details	45
Asset Lifecycle	46
Panel View.....	46
Inventory Tree	47
Software	47

Hardware Inventory	48
My Topology	49
Configuration Details.....	49
Events	50
Tickets	51
Services	51
Performance	52
Activity Log	53
Lambda Usage (Applicable to DWDM / OTN / ASON)	53
Port Utilization	53
CTP Utilization (Applicable to SDH)	53
E1 Trails (Applicable to SDH)	53
VCG Trails (Applicable to SDH).....	54
Cross Connections (Applicable to SDH).....	54
Flow Domain (Applicable to SDH)	55
Protection Group (Applicable to SDH).....	55
Channel Mapping (Applicable to PDH)	55
E1 Channel Utilization (Applicable to PDH).....	55
Consumable Asset (Beta)	56
What do you see on the screen	56
Add Consumable Asset.....	57
Asset Details.....	59
Software Assets	62
Software License.....	62
CMDB view	63
CI relationship in CMDB Downstream	63
CI relationship in CMDB Upstream	72
Contract Management	82
What do you see on the screen	82
View Contract Details.....	83
Add contract.....	84
Add Software Contract	84
Add Hardware, Lease, and Service Contracts	86
NCCM	87
Download Job	87
Calendar View.....	88
IMACD	88

What you see on the screen	90
About IMACD process:	90
Instructions to add a process.....	92
Installation	92
Move	93
Addition	94
Change	95
Destroy	96
Gate pass.....	97
Instructions to add a Gate Pass	98
Tickets	98
Ticket Management	98
State and Status	100
Tickets.....	101
How does it work?	102
What you see on the screen	102
Components	102
Communication	103
Working on a ticket.....	103
The Right Panel	103
Ticket Quick Actions.....	104
Ticket Grid Page Actions.....	104
Add ticket.....	106
Pre-requisites.....	106
Add a ticket	106
Additional Notes:.....	109
Self-Service for Requester	109
Request Management.....	109
State and Status	110
Request	111
How does it work?	111
What do you see on the screen?	111
Working on a Request	112
Request Views	112
Add a Request	115
Pre-requisites:	115
Steps to add a Request	115

Problem Management	117
Problem	117
How does it work?	117
Benefits of Problem Management	117
Problem Management Process.....	118
State and Status	120
Demo data for ITSM module Problem KB for new Org	121
Problem	121
How does it work?	121
What do you see on the screen?.....	121
Add Problem	121
Pre-requisites:	122
Steps to add a Problem	122
Working on a Problem.....	124
Problem Views	124
Analysis	126
5 Whys Method	126
Chronological Method.....	126
Kepner Tregoe Method	126
Solution/Workaround.....	127
Workaround.....	127
Solution	127
Change Management.....	129
Benefits of Change Management	129
Essential Roles in Change Management.....	129
Change Management Process.....	129
State and Status	130
Demo data for ITSM module change for new Org	131
Change	131
How does it work?	131
Types of Change	132
What do you see on the screen?.....	132
Add Change	132
Pre-requisites:	133
Steps to add a Change	133
Working on a Change	135
Views of the Change Request.....	135

Planning and Risk Analysis	137
Release	139
What you see on the screen	139
Instructions to add a New Release.....	140
Events.....	143
Event Management.....	143
Events	144
How does it work?	144
What you see on the screen	144
Log Management.....	145
Log Search	145
Log Stream	145
Report.....	147
How does it work?	147
What you see on the screen.....	147
Instructions to Add Report.....	148
Knowledge Base.....	154
Knowledge Base.....	154
Why Knowledge Base?	155
How to build an effective Knowledge Base?	155
SLA Management	156
SLA	156
Benefits of SLA:	156
Two Essential Components of an SLA.....	157
Metric	157
Profile	158
Service Level Target	159
Applied For	160
Geomap.....	160
What you see on the screen	160
Network Diagram.....	162
How does it work?	162
What you see on the screen	162
Instructions to Add Network Diagrams	163
Network Planning	163
Network Congestion – Traffic Congestion	163
What you see on the screen	164

Node Capacity Utilization.....	164
What you see on the screen.....	164
Topology	165
Topology View	165
Node:	165
Edge:.....	166
Topological Links.....	167
What you see on the screen.....	167
Steps to add a topology	168
Infraon Configuration	169
General Settings	170
API Registration	171
Audits	172
Business Hours	172
Tag Management.....	174
User Management	177
Department	178
Active users.....	179
Leaves	179
My Leaves	180
Password Policy.....	181
Requesters	183
Roles & Privileges	187
Teams.....	194
Users	196
Invite User	197
Service Management	198
How to build an effective service catalogue?	199
Service Catalogue.....	200
Notifications	205
Configure SMS	205
Configure SMTP.....	206
Messenger Audit.....	208
Trigger Configuration	208
Infraon Automation	211
Business Rule.....	211
Escalation.....	215

Email Integration.....	216
Customer Feedback Template	220
Mail Automator.....	221
Microsoft Outlook	223
Workflow	223
Bots	228
Deployment of Infraon Agent from Active Directory via Group Policy	228
Bots assistance	239
Data Collector	241
Inventory Agent	243
Organization	246
Address Book.....	246
License.....	247
IT Operations.....	248
Advance Resource Configuration	248
Blacklist and Whitelist	251
CLI Jobs/ Sessions.....	252
Circuit Discovery	255
Rules	256
Device Credentials	260
Diagnosis Tools	263
Discovery.....	266
Job Progress	283
LED Display	284
Maintenance	285
Network Configuration	286
Thresholds.....	373
Trap Configuration.....	377
Infraon Platform.....	378
Account Signup	378
CI Rule Configuration	378
Infraon URL	379
Login Settings	380
Module Prefix Configuration	380
Rebrand Infraon	382
Template Configuration	383
Vendor.....	383

SSP Configuration.....	384
Log Management.....	385
Access Control	386
How does it work?	386
Log Multi-Index	387
Log Search	391
Log Stream.....	393
Export Configs	395
Marketplace	396
Azure Active Directory	396
Pre-requisites.....	396
The Process	396
Infraon Dell	405
Description	405
How to Install	405
Google Workspace.....	407
Description	407
How to Install	407
Infraon JAMF	414
Description	414
How to Install	414
Infraon ServiceNow	418
Description	418
How to Install	418
Infraon Slack	422
Description	423
How to Install	423
FAQ	423
Infraon Teams	423
Description	423
How to Install	424
Infraon WhatsApp	439
Description	440
How To Install.....	440
Infraon Ring Central	456
Description	456
How to Install	456

Infraon LDAP	466
Description	466
How to Install	466
Infraon JIRA	471
Description	471
How to Install	471

Getting Started

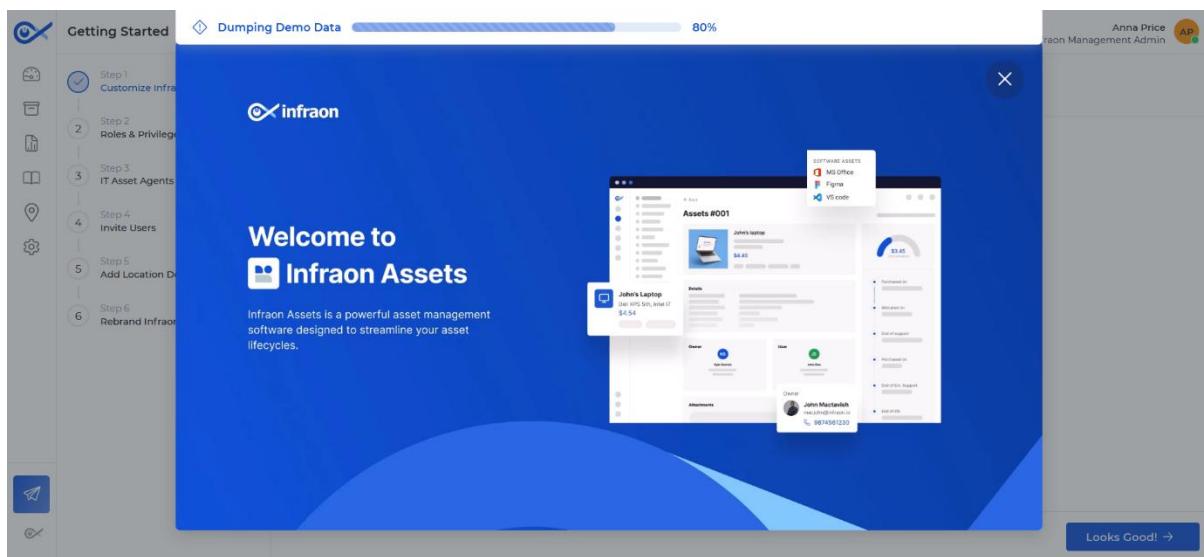
Welcome to Infraon!

Once the registration process is complete, proceed to log in. Use the default credentials to log in.

Alternatively, you can also use your Google mail address to log in. Once you log in, you will be redirected to the below page.

Additional information link in getting started based on product or ITSM / Asset

Simplified Onboarding! Access additional setup options via the 'Getting Started' page, enabling swift platform configuration for new accounts.



There are seven steps in the '**Getting Started**' part of Infraon.

- Infraon URL - Customize the Infraon Portal URL for your employees to access. Though it is recommended not to make changes, it is possible to change this URL later.
- Set up your Email - Add a Support Desk email address. Mails sent to this address are converted as Incidents. This email address also replies to the mail address for all customer communication. You can either set up a new email address on Infraon's mail domain or configure your existing mail server on Infraon.
- Roles & Privileges - Infraon uses dynamic role-based access control. There are multiple default roles with pre-defined privileges. There are five levels of privileges - view, add, edit, delete, and copy. As an administrator, you can create new roles, clone/edit privileges of existing roles, or delete

default roles to suit your organizational needs. Default role names can be edited too.

- **Invite Agents** - Adding users to Infraon is a piece of cake. Add email address(es) and select a role. Use a comma as a separator while adding multiple email IDs. You can invite multiple users across v roles from this page. Only pre-defined roles can be assigned to invitees.
- **Account Information** - Basic account information is extracted from the registration information. However, additional information can be added. It is recommended to add complete account information.
- **Branch Information** - Add the organization's H.O. and branch office location and address information here. If this information is added, aligning users, assets, and services across multiple locations becomes easier.
- **Brand Styling Information** - Who wouldn't love customization? Change Infraon's theme to suit your organization's theme. Customize the theme, add branding, change container and navigation bar colors, and select your preferred language. Preview it in real-time and save the look you like the most.

Now that you are all set with customizing Infraon proceed to [Know Infraon](#).

Know Infraon!

Once the initial customization is saved, you are all set to use Infraon. Your default landing page looks like the below:

The screenshot shows the Infraon dashboard with the following data:

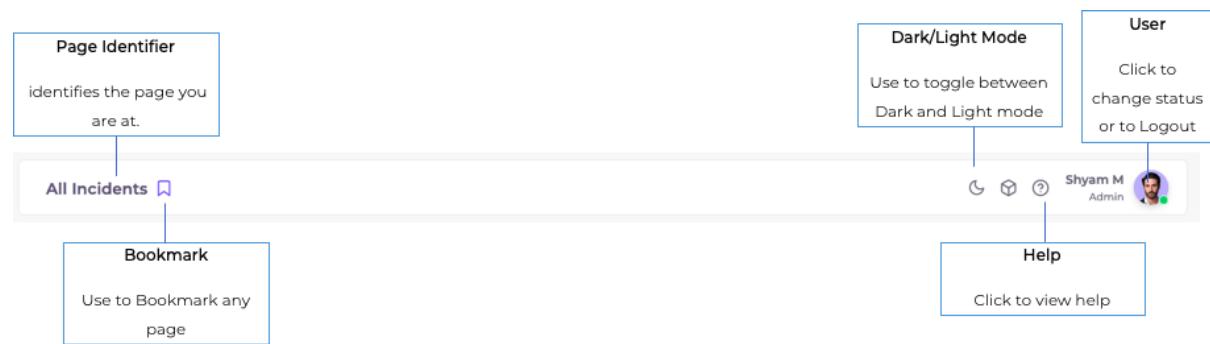
Assets By Value		New Purchases (Current Quarter)		Upcoming Expenses (Next Quarter)	
IT Assets	Fixed Assets	IT Assets	Fixed Assets	IT Assets	Fixed Assets
1	2	0	0	0	1
USD 800	INR 63000				INR 10000
IT Asset Summary	Fixed Asset Summary	Vendor Summary		Current Year Purchase	
1 Laptop	1 Laptop Accessories	3 Other		Laptops	Desktops
	1 Monitor Accessories			0	0
				Servers	Switches
				0	0

There are three default sections across all modules/pages of Infraon.

1. Top Panel
2. Left Menu Panel
3. Notification Icon

Let's see these in detail.

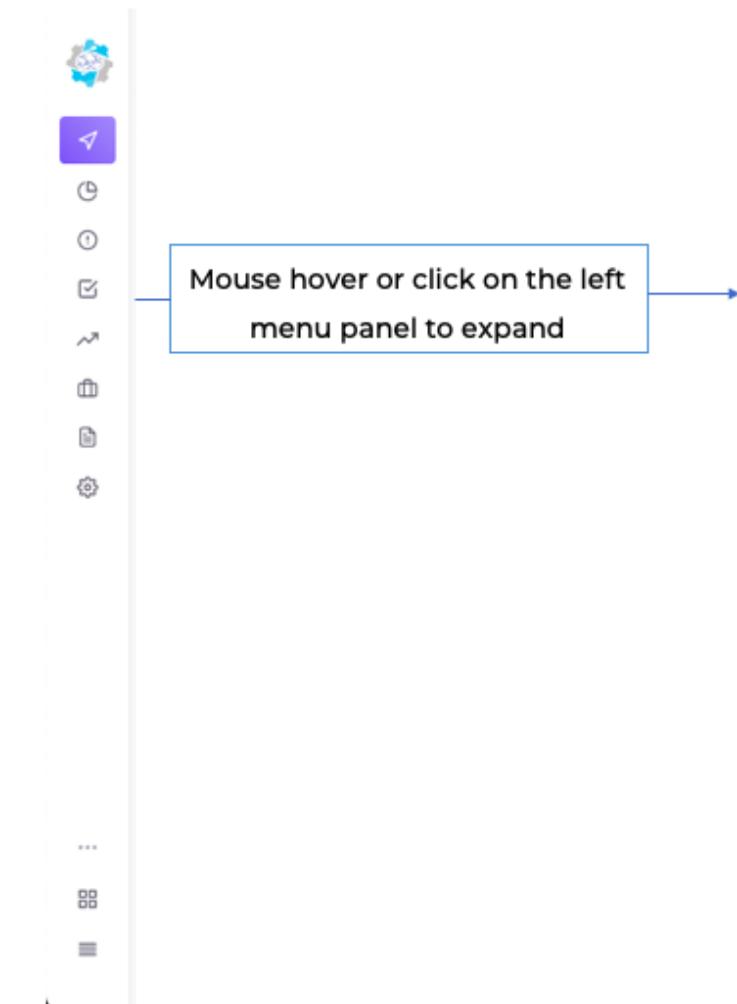
Top Panel



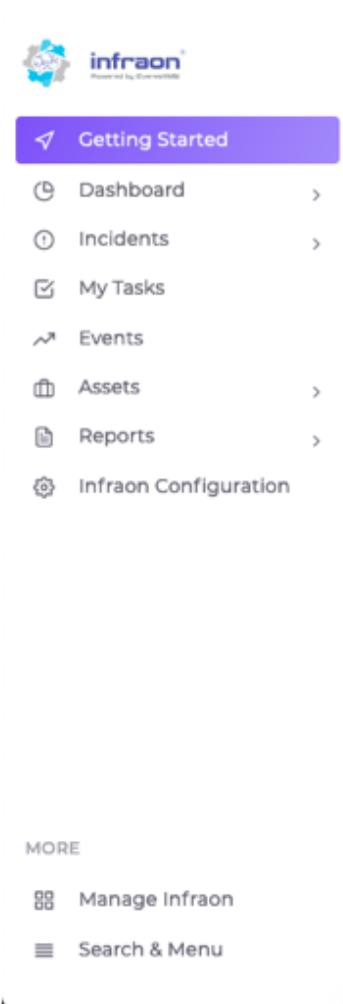
Left Menu Panel

The left menu panel can be expanded to view menu labels.

Minimized



Expanded



Notification Icon



The notification icon  is displayed across all modules of Infraon.

The number on the icon denotes the no. of new notifications for the user. The panel includes both task and information notifications. You can also approve/reject requests from the notification panel.

Click on the  [Manage Notifications](#) to make changes. Re-click the notification icon or use the close icon on the top right corner to close the notification panel.

User's first login

User(s) can self-register on Infraon when they receive an invitation from the administrator(s). Click on the link, add details, and Voila! You are all set.

Please note that your Administrator/Manager has predefined your role-based privileges.

Please contact your administrator or manager if you cannot view any Infraon modules/pages.

When you first log in, Infraon offers options to customize your theme.

Workspace

In the workspace, users can access multiple modules within a specific environment. This includes incidents, tasks, requests, problems, changes, and release modules. Specifically, IT Service Management (ITSM) modules, which are process-oriented, are integrated. These modules can also be communicated through a chat interface for seamless collaboration.

Add the Ticket/ Request/ Change/ Problem/ Release

- Click any one channel.
- Click Add Ticket/ Request/ Change/ Problem/ Release
- Search the requesters from the drop-down.
- Fill in all the mandatory details in the report.
- Choose the team from the drop-down menu, or the user can opt for self-assignment, also known as 'self-assignee',
- Select the request type/ problem type/ from the drop-down.
- Select the priority from the drop-down.
- Select the n number of followers from the drop-down.
- Select the Impact from the drop-down
- Select the urgency, severity, and Risk from the drop-down.
- Write the number of versions in the version bar.
- Select service category and tags from the drop-down menu.
- Click on the calendar icon and select the due date.
- Select the release manager from the drop-down.
- Select the priority and release type from the drop-down
- Write the notes in the given space.
- To add any documents, click on the attachments and select the file.
- Add the subject line and brief description for the ticket and click 'submit as new'

The added ticket/request/change/problem/release will appear in the channel.

Workspace Metadata update: If an issue is raised in the workspace within a Ticket ID, it will reflect on both pages simultaneously.

What happens after creating the Ticket/Request/ Change/ Problem/ Release?

When users click on the channel, the created ticket/ Request/ Change/ Problem/ Release will be displayed. Double-tapping on the ticket ID/ Request ID/ Change ID/ Problem ID/ Release ID redirects to a page containing comprehensive details. This page provides the user with the ticket's creation time and date.

There are a few tabs for the Tickets / Requests/ Changes/ Problems/ Releases such as,

Basic Details | Workspace

Name	Description
------	-------------

Status	The status of the ticket can be changed from new to responded etc.
Priority	Priority can be critical, high, medium, or low.
Urgency	Select the urgency from the drop-down such as high, medium or low
Impact	Select the impact from the drop-down
Impact service	Select the impact service from the drop-down
Service classification	Select the Service classification from the drop-down.
Attachment	If there are any documents to attach, click on attachment and attach the document.

For release, the following details are included,

Risk	Select the risk from the drop-down
Due date	Click on the due date column the calendar pops up, and select the date.
Version	Write the version

Communication

The communication tab will appear as shown below,

The written email will be visible under the 'Communication' tab. Here, the user can reply, forward, add notes, and perform other related actions.

Rephrase communication content via open AI: In the Incident page, within the Communication section, users can leverage text enhancement features, offering various styles to refine communication content using OpenAI.

Relation

The relation tab will appear as shown below,

- Click 'ticket +' button
- Search ticket from the search tab.
- Select relation type as 'associated'

Click 'Submit'. This selected ticket will appear in the relation page

Attachment

The attachment tab will appear as shown below,

To add the attachment,

- Click on the 'add' tab

- User can either drag and drop the document or click on the drag and drop to attach the document
- Select the category from the drop-down, such as the default category, ticket screenshot, team docs, etc.
- Describe the attachment.

Click 'Upload files'

Knowledge base

The knowledge base tab will appear as shown below,

The knowledge base is created only when the ticket is resolved or closed.

Interaction

The interaction tab will appear as shown below,

The raised issue will display the five most recent issues in the 'Interaction' tab.
The 'Recent Activities' tab will showcase a history of all actions performed.

Recent activities

Recent activities are the history of the activities logged.

For change/ Release

The change/ Release workspace includes the planning and tasks as shown below,

Planning

The Planning tab will appear as shown below,

- Click on the calendar icon and select the start and end dates.
- write the reason for the change.
- Add the rollout and rollback plan.
- Click 'save'

Task

To add a new task,

- Click on the '+' icon
- Write the title and description in the given space.
- Select the status, priority, and assignee from the drop-down
- Select the due date from the calendar.

For Problem

The problem workspace includes the analysis and submission as shown below,

Analysis and Submission

The analysis and submission tab will appear as shown below,

There are two tabs such as analysis and Solution:

Analysis | Solution

- Click on the '+' icon from right side corner of the page.
- There are two tabs: cause details and Technique details

Cause details | Technique details

Name	Description
Submitter	Select the submitter from the 'drop-down'
Analysis Technique	There are three types of analysis techniques, namely: <ul style="list-style-type: none">• Chronological analysis techniques• 5-Way analysis technique• Kepner- Tregeo Technique
Type	Select the type from the drop-down, such as general, troubleshooting, Analysis, or testing
Category	Select the category from the drop-down based on the type
Submission date	Click on the calendar icon and click on the date.

Click 'Next'

Cause details | Technique details

Based on the analysis technique selected, technique details to be filled,

There are three types of analysis techniques, namely:

- Chronological analysis techniques: Toggle the button to enable it to represent the actual root cause. Provide a detailed description of the problem's origin, then click 'save'
- 5-Way analysis technique: In the designated space, describe the problem. Choose 'yes' if it's a root cause, or select 'no' to proceed with the next technique.
- Kepner- Tregeo Technique: Answer the five questions to identify the problem. Click 'save'

Analysis | Solution

The technician gives the solution based on the analysis.

- Click 'resolve'.
- Fill in the mandatory details and click resolve.

To add the other workspace from the present workspace, refer below,

1. For the Ticket, add the request/ Problem/ change.
2. For Request, add the Ticket/ Change
3. For Change, add the ticket.

4. For release, add the Ticket/ Change

- Click on the three vertical dots in the right-hand corner of the taskbar.

Note: When the Ticket/ Problem/ change/ Request is resolved, the three vertical dots on the taskbar will display an option 'Infinity convert to KB.'

Stages of the tickets

When a ticket is created, it progresses through several stages, including:

Name	Description
Logged	When the ticket is raised, the status will show as logged.
Responded	The ticket status will show responded when the user gets the response.
Investigation	In this stage, the raised ticket will be investigated to resolve the problem
On Hold	This stage is optional. To get confirmation from higher authority, the ticket is kept on hold
Resolution	Resolution is provided to the user after approval only if the ticket is hold.
Closure	The ticket is closed after the resolution is provided.

Dashboard

Dashboards are visual representations of critical data. Infraon Dashboards are designed to display direct-to-the-point yet, thoroughly detailed views of various monitoring and performance metrics.

Infraon allows customization of the dashboard wherein the user can add metrics and reports to suit their requirement. Dashboards can also be exported as PDFs to help with reporting.

Note: Access to view and customize dashboards are part of Role privileges and must be enabled by the administrator. Access can be controlled on a User/User Group level.

It is essential to know and understand Widgets before customizing a Dashboard.

What you see on the screen

1. Asset Summary

Below are the details which can be viewed in this tab:

- Asset Name
- Asset ID
- Operational Status
- Status
- Type
- Make
- Active

2. Service Availability

Below are the details which can be viewed in this tab:

- Service Name
- Status
- A End Node
- A End IP
- A End Port
- Z End Port
- Z End IP
- Z End Port
- Type
- Trail Type
- Bandwidth (MBPS)

3. Event Summary

Below are the details which can be viewed in this tab:

- Issue
- Date
- Event ID
- Node

- Resource
- Acknowledged
- Event Type
- EMS Name
- Vendor

Hover over the mouse to the respective dashboard to see the below features:

Label	Action	Description/ Example
Pin	Click to Pin the widget.	Promote a dashboard to the top of your list for easy access.
Edit	Click to Edit.	Edit to make changes to the dashboard.
Clone	Click to clone.	Make a copy of the same dashboard.
Delete	Click to delete.	Click to delete the selected dashboard.

Widgets

Infraon widgets are pre-configured code snippets meant to extract essential information from the infrastructure or network and present it in an easy-to-understand graphical face/format. (Pie chart, Graph View, Panel View, Data Table, Bar Chart, Line Chart)

Though the widgets have a pre-configured purpose, they can be customized by selecting a specific time frame and colour scheme and adding additional filters.

Categories

There are multiple types of widgets on Infraon. These widgets are grouped into:

Assets - The asset widget offers a central view of all your assets, including a complete list summary, new additions, and their agent-assigned statuses for easy management.

The asset widgets are further classified into the following sub-categories to provide focused functionalities.

- Asset Summary
- New Purchases
- AMC Expiry
- Asset Count Panel
- License Usage
- True-up Cost
- Top Publishers
- Consumable Summary
- Location Wise Asset Summary
- Agent Status
- Asset Summary Drilldown Table
- Location Wise Asset Summary

Statistics - Widgets that are designed to display overall metrics and statistical information.

The statistics widgets are further classified into the following sub-categories to provide focused functionalities.

- Stat Summary
- Multistate Summary
- Resource Trend
- Resource Status
- Statistic Panel
- Node Status Panel
- Link Status Panel

Events - This event summary widget provides a visual breakdown of all system events, categorized by severity (critical, major, minor) for easier comprehension.

The events widgets are further classified into the following sub-categories to provide focused functionalities.

- Events Summary
- Event Count
- Event Trend
- Aging Summary

Views - This widget provides device status summaries and network topology visualizations in glanceable snippet formats.

The view widgets are further classified into the following sub-categories to provide focused functionalities.

- Device Status Summary
- Text Panel
- Network Diagram

ITSM - This widget acts as a central hub, bringing together snips from all your ITSM modules. Effortlessly access key information like CSAT scores, ticket summaries, request details, problem reports, SLA management data, and release summaries, all in one place.

The ITSM widgets are further classified into the following sub-categories to provide focused functionalities.

- CSAT Summary
- CAST Score
- CSAT Trend
- Ticket Summary
- Ticket Count
- Ticket Created Vs Resolved
- Request Summary
- Request Count

- Request Created Vs Resolved
- Problem Summary
- Problem Count
- Problem Created Vs Resolved
- Change Summary
- Change Count
- Change Created Vs Closed
- SLA Compliance By Templates
- Requester Summary
- Assignee Summary
- Response time Count
- Release Summary
- Release Count
- Release Created Vs Closed
- Ticket Count Summary

Contract Management - The widget displays a concise overview of contractual agreements, including key details such as contract type, vendors, manufacturer, status, and contract name. It enables users to easily track and manage contract information.

The contract management widgets are further classified into the following sub-categories to provide focused functionalities.

- Contract Summary
- Contract Count Panel

IMACD - This widget provides a comprehensible real-time report fragment summarizing IMACD activities.

The IMACD widgets are further classified into the following sub-categories to provide focused functionalities.

- IMACD Summary
- IMACD Count

NCCM – These widgets enhance visibility into network configuration management activities by providing insights into backup success and failure rates, enabling technicians to track reliability.

The NCCM widgets are further classified into the following sub-categories to provide focused functionalities.

- Backup Success
- Backup Failed
- Recent Downloads
- Baseline V/S Running
- Baseline V/S Startup
- Previous V/S Running
- Previous V/S Startup
- Startup V/S Running
- Vendor Summary

Details | Configuration

These widgets can be used to customize data representation, i.e., users can choose how they want to represent data – line chart, bar chart, pie chart, data panel, area chart, or data table. Other levels of customization include:

- [Timescale](#) - last hour, 3 hrs, 6 hrs, 12 hrs, etc.
- [Statistics](#) - to suit the requirement.
- [Palette](#) - Colour customization
- Filters like asset tag, incident, assignee, etc.
- Multiple dashboards in presentation mode.
- Auto Reload – Can select the amount of time required for the auto reload.

Details | Custom Filter

Filters are visible based on selected preferences.

Different types of filters are available on Infraon Infinity, which can be applied to a widget to filter data displayed in the Dashboard.

Here is the list of custom filters depending on the field

- Asset ID
- IP Address
- Device Type
- Asset Type
- IT Asset Status
- Fixed Asset Status
- Location Name
- Installed Location
- Organization Name
- Is Active
- Designation
- Floor
- Building
- SAP ID
- Location
- OLD Associated Assets
- Colour
- Service Catalogue
- Organization Name
- Department
- Team

*Additional filters may be added in future versions.

and respective conditions, which can be added to the dashboard.

Multiple dashboards in presentation mode

Introducing Dashboard Presentation Mode! Configure and set time intervals (6-300 seconds) for automated dashboard presentations. This mode is ideal for dynamic assets and other dashboard displays.

Add Dashboard

Dashboards are visual representations of critical data. Infraon Dashboards are designed to display direct-to-the-point yet, thoroughly detailed views of various monitoring and performance metrics.

Additionally, three categories in the release dashboard, release summary, release count, and release created v/s closed. The release process for the dashboard is streamlined, making it easy to configure and schedule with privacy controls. The feature makes valuable insights into release performance and tracks progress toward release goals. Overall, the release dashboard provides a comprehensive view of release management and enhances the efficiency of the release management process.

There are a few pre-configured dashboards on Infraon. In addition, Infraon allows customization of a dashboard wherein the user can add metrics and reports to suit their requirement. Dashboards can also be exported as PDFs to help with reporting.

Instructions to 'Add Dashboard'

- Go to Infraon Dashboard -> All Dashboard.
- Click the 'Add' icon -> 'Create' to add a new dashboard.
- You will need to add a new widget to create a new dashboard.

Dashboards are made of widgets. Add a widget to start configuring the dashboard.

There are two tabs on the '[Add New Widget](#).' Refer to the table for more information.

[Widget](#) Configuration

Various categories of widgets are listed in the table.

Label	Description
Event-Based	Widgets that can display events on the dashboard.
Stat Based	Widgets that can display overall metric and statistical information.
Link	Widgets can display information and the status of the selected links/interfaces in various purposed ways.
Site	Widgets can display information about the status and summary of the chosen site or device.
Views	Widgets can show standard views like resource trend, resource status, and status summary.

Service Manager	Applicable only when the dashboard is integrated with the service manager. These widgets display service-related information such as incidents, tickets, etc.
Prediction	Prediction widgets are used to predict test data based on a trained model.
Custom	Custom widgets are used to provide additional capabilities of resources. You can modify the published widgets or change the profile of custom widgets.

Select any widget categories, and click '[Next](#)' to see the '[Configuration](#)' tab.

Instructions to 'Edit the Dashboard'

Label	Action	Description/ Action
Add Widget	Click to add a new Widget to the dashboard.	
Assignee	Click to add a new assignee.	Select to assign to Users or to a Team.
Submit	Click on the button once the changes are made to satisfaction.	

Asset

The CMDB part of ITSM is incorporated as Assets within Infraon. Infraon Assets allows administrators/asset managers to view and manage all organizational assets, i.e., all IT and non-IT assets, in one place.

Any device with an IP is known as IT Asset or Node. It can be a Server, Router, Storage Device, Transport Device, Wireless controller, Access point, etc., As part of Asset, Infraon collects and maintains the complete inventory details for an asset.

Infraon collects basic yet important inventory information for each device, server, hypervisor, and application. The inventory information includes:

- IP Address
- Hostname
- Device Type
- Vendor
- Model
- Serial Number
- Operating System and Version
- MAC Address
- CPU Information
- Memory
- HDD Details
- Port Level information

Etc.,

- For Hypervisors,
 - CPU Socket
 - No of Processor
 - CPU Speed
 - Hyper Threading
 - Memory Size

Etc.,

How does it work?

Assets must be added to Infraon to enable management. There are multiple ways to add assets.

- Assets can be added directly from the asset module on Infraon. Within the asset module, there are options to manually add an asset or bulk assets using a .csv file.
- Agent-based discovery initiated from the Infraon configuration module.

Assets can be viewed in Grid and card views. Clicking on the corresponding action icons in the assets allows you to scan and search for assets, export them, and perform maintenance actions.

Label	Action	Description/ Example
Search	Search for the required asset.	
Filter	Filter can be added based on the field (Card name, card type, device IP, part number, and serial number) and condition from the drop-down box below.	
Actions		
Scan & Search Asset	Search by barcode: type the asset's code.	To scan and search for an asset, click on the 'Scan and search asset' option, then use your phone to scan the QR code, which will initiate the asset search process.
Export	Click to choose the category.	To export the data, click the 'Export' button, then choose the desired category, and finally download the CSV file containing the selected data.
Maintenance	Click to redirect to the Maintenance page.	When an asset is designated for maintenance, its status is changed to the "maintenance" stage. After scheduling the maintenance time, the asset is set to run automatically during that scheduled period. Once the maintenance is completed, the asset reverts back to its previous state, resuming normal operations or the state it was in prior to the maintenance activity.
Bulk Edit	<ul style="list-style-type: none"> • Go to the Infraon Asset Card page -> Actions -> Bulk Edit. • Select the Category. • Download the CSV file (excel sheet) and Enter the Asset details in the sheet. • Upload the same edited CSV file. • Click Next -> Import -> Proceed with Valid Records. 	To Edit Multiple Assets information or details at once.

Download Agent	Click to download the Infraon agent available on Windows, MAC, and Linux.	
Customize Asset ID	To customize the Asset ID configuration.	
CLI Session	Click to navigate back to the CLI session module.	CLI Jobs/sessions in NCCM create direct CLI sessions (SSH or TELNET) between the Device and the User through the NCCM application.
Download Job	Click to navigate back to the Download Job module.	NCCM's Download Jobs added through Discovery process or manual Device addition will start downloading Device configurations, Operational Data, Device Inventory Details, OS image details based on "Configuration Profile" assigned, Device Credentials, Connection & Download protocol selection and Schedule period.

Selecting multiple assets:

Multi-selection of assets is facilitated by clicking the checkboxes adjacent to each desired asset.

Users can now:

- Assign a new owner
- Assign a requester
- Assign a tag
- Print
- Change the Status of the assets.
- Edit the Location
- Enable/ Disable
- Add to NCCM
- Delete multiple assets at once.
- Add to Log Management
- Add Download Jobs/ Edit Download Jobs
- Diagnose
- Mask Alarms
- Unmask Alarms
- Maintenance
- Change category

Asset Types

There are multiple types of assets in an organization. The first step of asset management is the categorization of assets. Broader categorization enables better management. The default categorization of assets within Infraon is as follows:

Asset Type -> Asset Category -> Asset Sub-Category -> Asset

The process of managing an asset is based on the type of asset. Infraon asset has been split into four modules based on asset type.

IT Assets are physical assets or devices used in an organization's business activities that fall under the responsibility of IT staff. For example, computers, servers, routers, scanners, fax machines, printers, modems, hubs, and IoT (Internet of Things) devices.

Fixed Assets are any physical objects or vehicles you consider 'assets' to your organization. It can be easily converted into cash—for example, vehicles, machinery, equipment, etc.

Consumables are assets that organizations use. They must be replaced regularly because they wear out or are used up—for example, mouse devices, external keyboards, computer cables, printer toners, etc.

Software Assets are any functional software in an organization that requires service level agreement to ensure compliance with software licenses. For example, software assets may be internal or external, on-premises, or in the cloud.

Within these asset Types, assets are further classified into:

Categories – Categories are also referred to as 'parent' categories. A category is the first division of assets within the selected asset type. For example, within IT assets, there can be categories like laptops, desktops, etc.

Sub-Categories - Sub-categories are also referred to as child categories. The sub-category is the next level of asset division within the category. For example, if the categories are laptop or desktop, sub-categories within IT assets can be Dell, Lenovo, Apple, etc. Assets or asset items can be added here.

Refer to the 'Asset Grid Page' and '**Asset Categories**' sections for details and instructions.

Note: Assets can be added in the category and the sub-category level. The steps to view, add, edit, and manage assets are the same regardless of the asset type.

Steps to Look for a Specific Asset

- Expand the left menu panel.
- Click on Assets
- Select the respective asset type.
- Click on the respective asset category or asset to view more details.

Asset Categories/Sub-Categories

Defining the asset category and sub-category is the first step in adding the asset. Categories can also be called Parent categories. It is recommended to add an asset category before adding an asset. The process of adding a category and a sub-category is the same.

Hovering the mouse over the category:

Label	Action
(+)	To add a sub-category.
Edit	Click to make changes to the category.
Delete	Click to delete the category.

Before adding an asset category/sub-category

The 'Add Category' field tab is where you can define or configure asset properties. Asset properties may include basic details like make, model, size, dimensions, etc., and critical information like EOL, EOS, end of support, etc. Some properties are mandatory for all asset categories.

The properties within Infraon are categorized into sections. Some sections are optional, whereas some are mandatory. The optional sections are available for selection based on the type or category of assets.

How does it work?

The sections are listed below the title, '[Available Section](#)'. Once selected, they are added to the '[Selected Section](#)' part and are available for defining permissions and field-level customizations. Please note that the selection of fields makes them mandatory for the selected asset category. Field selection is also possible for mandatory sections too.

In addition, Infraon allows you to create custom fields and select unique identifiers.

Mandatory Asset Properties

Few asset properties are mandatory across all asset categories. The mandatory properties and the fields are as follows:

Label	Fields
Common Properties	Status, Criticality, Service Status, Operational Status, Business Function, Description, Installation Date, Usage Type, State Change, Reason, Retire Reason, Vendor, Uninstall Date
Procurement Properties	Warranty In Year & Month, Warranty Expiry Date, Expiry Date, Purchase Vendor, AMC Vendor, AMC Cost, AMC Expiry Date, Lease End Date, Disposal Date, Reason, End Of Life, End Of Sale, End Of Support, End Of Extended Support, Last Renewal Cost, Next Support Renewal Cost, Effective Date, Effective Cost, Estimated Cost, Book Value, Tax Credit,
Cost Properties	Invoice No., Part No., Cost, Purchase Date, Depreciation Type, Salvage Value, Currency
Location Properties	Location Hierarchy, Country, State, City, Pin Code, Landmark, Flat House No Building Company, Area Colony Street Sector Village, Zone, Region, Division, Location Code, Latitude, Longitude
Assignment	Department, Managed By Tag, Managed By, Used By
Software Properties	Publisher, Version, Software Type, Software Category, Platform, Size, Note

The below asset properties are optional and are available for selection.

Label	Examples
Hardware Properties	Serial Number, Hostname, Alias, Make, Model, UUID, Manufacturer, Domain, IP Address, Series, Tag No, QR Code, Barcode
OS Properties	OS Name, OS Version, OS Service Pack, OS Install Date, OS Installed By, Build Number, Product ID, Product Key, Virtual Memory
CPU Properties	CPU speed, Logical Processors, CPU Stepping, CPU Cores Count
BIOS Properties	Manufacturer, BIOS Version, Install Date
Disk Properties	Drive Name, Drive Type, Drive Capacity, Drive Filetype, Drive Serial Number

Monitor Properties	Monitor Type, Refresh Rate, Monitor Serial Number, Resolution
Keyboard Properties	Keyboard Type, Keyboard Serial Number
Mouse Properties	Mouse Serial Number, Number of Buttons

Additional customizations are enabled within the 'Selected Sections.' You can define role-based view and edit permissions. These can be defined at the property level as well as the field level. You can choose to enable or disable a specific field as well as make it mandatory using the relevant action icons.

[Unique Fields](#)

Unique fields are unique identifiers for assets. Use the unique field drop-down to select as per requirement.

[Create a Custom Field](#)

In addition to the default asset property fields, Infraon allows you to add custom fields.

Check the '[Add Custom Field](#)' section below for more information.

Add pound currency in the asset management from UI symbols verification

Expanded Currency Options! Now offering 163 currencies, with INR as the default. Detailed asset currency view, cost estimates, and currency display in asset life cycle and depreciation graphs.

[Instructions to add the Asset Category](#)

Select Assets -> Asset Type (IT Asset or Fixed Asset, etc.) from the left menu panel to view the asset grid page. The category panel is displayed on the left, and the assets are listed in a card view on the right.

- Click on the + icon in the category panel.
- 'Add asset category' window appears.
- Choose whether you are adding the category or the sub-category using the option button.

There are two tabs to add a category/sub-category.

[Basic Details | Fields](#)

Label	Action	Description/Example
Category Name	Add the asset category name.	Define the asset category name you want to categorize for asset management. For example, the IT asset

		defines the category as laptop, desktop, etc.
Associate Item Types	Use the dropdown menu to associate asset items to this category.	For example, items like routers and firewalls can be categorized under 'Network'.

Other Details | Fields

Label	Action	Description
Mark as CI	Select the toggle button to mark it as CI	CIs (Configuration Items) enable better tracking, management, and understanding of the asset's relationships and dependencies with other CIs.
Notify End Users on Asset Allocation (End Users can Accept/Deny assets)	Select the toggle button to enable the functionality	Enabling the toggle button will trigger a notification for the end user to accept/deny the allocation of the asset.
Send bulk allocation email / Send bulk deallocation email	Select the toggle button and correspondingly add the trigger notification timer.	Unified notification system for handling large-scale allocations/deallocations across various asset categories. The allocation/ deallocation email process begins when an asset is assigned to a user for the first time. A single email containing all allocated asset information from that specific period will be sent to the De-allocation or vice versa.
Notify End Users on Asset De-allocation	Select the toggle button to enable the functionality	Enabling the toggle button will trigger a notification for the end user to accept/deny the deallocation of the asset.
Notify Owner on Warranty and AMC expiry	Select the toggle button and correspondingly add the trigger notification timer.	Turn on the toggle and set the alert date. This will automatically notify asset owners when their warranties and AMCs are about to expire.
Notify owner on discovery of blacklisted Application	Select the toggle button to enable the functionality	The owner of the IT asset will be notified via email upon discovery of a blacklisted application.

Notify Owner on Hardware Changes	Select the toggle button to enable the functionality	Enable email alerts to keep IT asset owners informed of any hardware modifications.
----------------------------------	------------------------------------------------------	-------------------------------------------------------------------------------------

After this step, click 'Next' to define fields for the selected asset category.

To add a sub-category within the selected category, proceed as below:

Sub-Category	Click on the sub-category.	Select this option to define an asset sub-category. A sub-category can be defined for an existing category too.
Parent Category	Select the parent category name using the drop-down menu.	Define the parent category of your asset sub-category.

Click 'Next' to define 'Fields' for the sub-category.

[Basic Details](#) | [Fields](#)

The mandatory sections are added by default. There are multiple levels of customization available here.

[Level 1](#): From the list of mandatory fields, select fields to make them mandatory.

[Level 2](#): Scroll down to select additional sections to add them to the selected section.

[Level 3](#): Select fields from the additional sections to make them mandatory.

[Level 4](#): Define role-based privileges, enable/disable fields or make them mandatory.

[Level 5](#): Create a custom field to suit your specific needs.

[Level 6](#): Select fields from the list of unique identifiers to add them.

Once the customization is complete, click '[Submit](#)' to save. Refer to the '[Add Item](#)' section for details and instructions on adding an asset.

Asset Grid Page

There is no single home page for Assets. Assets are added based on the asset type, each with a grid page. Click on the respective asset type from the left panel to view the list of assets in the selected category. This page is referred to as the 'Asset Grid Page'.

Assets can be viewed as a card or a grid view. Asset details include the following information.

- Asset Name
- IP Address
- Asset Category
- Asset ID
- Asset Status
- Device Type
- Make

Asset Search/Scan

There are three ways to search for an asset.

- **Barcode Search** - Click on the 'Scan & Search Asset' icon and use the barcode scanner. The asset information is displayed accordingly.
- **QR Code:** Select any asset, QR code, and click on the print icon. Customize the displayed information with options like QR/bar code, tag name, warning label, Property of, and asset ID tag.
- **Asset Search** - Click on the 'Scan & Search Asset' icon and type the asset ID to search.
- **Filter** - Click on the 'Search Filter' field and type the name, asset ID, hostname, IP address, or category/sub-category to search.

Assets column selection

Customize columns based on the unique preferences. With a simple drag-and-drop action, arrange columns effortlessly, and streamline the experience for optimal efficiency and organization.

Asset Actions

Select one or more assets to view the below asset actions:

- Owner - Click to add/change asset owner.
- Requester - Click to update the requester and/or owner.

- Tag - Click to update the asset tag.
- Print - Click to print the asset label(s).
- More - Click to update asset status and location, enable, disable, or delete the asset.

The asset(s) must be in an 'enabled' state to edit.

Sorting drop-down feature for Asset card view page

Enhanced Software Management! Now, easily sort asset ID, name, operational status, and overall status in ascending or descending order while adding software.

Add Asset/Add Item

Assets are referred to as Items in Infraon. Before adding an asset, the category and subcategory must be defined.

Note: Refer to the '[Asset Categories](#)' section for more information.

Navigate to the respective Asset page (IT, fixed, consumables, etc.). If no categories/subcategories are pre-defined, these can be added when adding the asset (item).

There are three ways to add assets:

- 1. Single Asset** - You can add a single asset from the drop-down menu in the top right corner
- 2. Import from CSV** - If you have the asset CSV file, you can import it from the drop-down menu in the top right corner.
3. Add Assets through Discovery - This only applies to IT assets. Any asset with an IP can be discovered using agent-based discovery. Refer to the '[Discovery](#)' section for details.

Instructions to 'Add Single Asset'

- Go to Asset -> Asset Type.
- Click the '[Add](#)' button -> Single Asset

There are two tabs on the 'Add Asset' page. Refer to the table for information.

[Define Asset](#) | Asset Properties

Label	Action	Description/Example
Asset Name*	Add your asset name.	Asset names can be server, host, computer, device, etc.
Category	Add asset category.	Select an asset category that suits your requirement. Refer to the

		asset categories section for more details.
Asset ID	Customize the asset ID	Customize the asset ID for the assets as required by changing the prefix, number, type, and custom format of the asset ID from the Infraon Configuration. You can opt for alphanumeric, random or auto-increment and a custom format. This allows overwriting of existing assets IDs that update all previously assigned IDs to the new format.
Asset Workflow (Beta)	Edit and customize the stages and statuses of the IT Assets.	Flexible to edit and customize the stages and statuses of IT assets and change the flow based on the requirements. Easily modify the default workflow, add new statuses, and control transitions. Experience improved asset management and status tracking similar to ticket workflows.
Asset Allocation Mail	Approve or reject the mail by identifying the owner of the email.	Acceptance and rejection are identified through the email sent to the asset's owner. Allowance of resending the email by eliminating the previous restriction.
Calculation	Depreciation calculation	Calculate the depreciation based on the two methods provided for the assets. These methods gradually reduce the asset's value to provide more accurate and comprehensive reports. Enhances the accuracy and efficiency of asset management, providing a more comprehensive view of asset performance.
Maintenance	Maintenance Configuration	Configure the assets for maintenance, schedule maintenance periods and easily track progress and history.
Self-service portal	Asset details in self-service portal	With the new portal, you can easily view the complete details of the assets, which allows for a self-service portal and a more convenient and user-friendly experience.

Owner/Technician	Select the owner or technician using the drop-down menu.	
Requesters	Select the requester using the drop-down menu.	
User Tag	Select user tags from the drop-down.	Assets may be grouped using these using tags.
Location	Add the asset location.	The location where you are working or performing business activities.

* Upload images if you have product images.

Note: Next button will work only when you have filled all the information correctly, viz; correct asset name, category, owner/technician, requesters, user tags, and location.

Click '**Next**' to add '**Asset Properties.**'

Please refer to the previously mentioned asset properties; you can find them in the 'Add asset Categories' section.

Upon clicking on the added assets, icons appear at the top, including the owner, requester, tag, print, and additional options.

Two sections will be displayed on this page when clicking on the asset.

Asset name: In this section, the asset name, IP address, and status are displayed, and the status can be modified to Trial run, In Use, Maintenance, Parts repairs, Accident/failure, Audit, or Lost. To add the requester's location and allocation details, click "more options."

Sections: On the left side of the page, there are seven sections represented by tabs; clicking on these tabs will display specific data on the right side of the page. These sections include

- 1 **Details:** If an asset picture has been uploaded, it will be displayed. Essential details such as hostname, device type, asset status, Asset ID, barcode, IP address, QR code, make, and OS name are displayed in the details section.
 - **Performance section:** System uptime, CPU utilization, memory, and Disk is displayed.
 - **Attachment:** Attachments can be added by clicking the 'add' button and uploading a CSV file.
 - **Details:** Details of assets such as Alias, Asset Name, IP Version, and Model are displayed.
 - **Owner:** Owner details is displayed, such as name, e-mail, and phone number.

- 2 **Asset Lifecycle:** The asset life cycle refers to the stages that an asset goes through, from its acquisition to retirement, encompassing its

management, maintenance, and utilization throughout its entire existence.

- 3 **Hardware:** Any hardware components collectively enable the device to function and perform specific tasks.
- 4 **Events:** Infraon detects all changes or activities of CIs or configuration items, observes anomalies based on the configured thresholds, and records them as events. If triggers are configured for the same, notifications or incidents are raised accordingly.

Enable the events menu in the asset summary page to display Windows events and CI enables the option for asset

The event Page Module is now enabled on the Asset page. Access login/logout history and detailed event data. Analyze key information like domain name, login type, machine name, and system details including IP addresses. To enable, visit Event Page settings, choose 'Show History' for universal events, or select specific asset events from the asset page for targeted insights.

Define Asset | Asset Properties

Following are the sections within the 'Asset properties' tab:

- Sections
- Show Only Mandatory button.
- Back
- Submit

Label	Description/Example
Sections	Under sections, you can find various asset properties. If your assets have more than one property, you can select multiple properties and fill in the details in the left section.
Show Only Mandatory Button	When you toggle the show only mandatory button, you will get only the hardware properties, and you need to fill in only those details.
Back Button	If you feel you have entered the incorrect information, you can click the back button and fill in the correct information.
Submit	After filling in all the asset property details, click on the submit button to import the single asset.

Instructions to 'Import from CSV'

- Go to Asset -> Asset Type
- Click the '**Add**' button -> Import from CSV

In the '**Import from CSV**', there are two tabs.

Upload| Column Matching

Label	Action	Description/Example
-------	--------	---------------------

Category*	Select asset category using the drop-down menu.	Server, Fans, etc. Download the sample CSV file and add details accordingly.
Import Asset List from CSV*	You can either drag and drop the file or browse to upload the CSV file.	Ensure to add asset details to the default file before uploading.

Click 'Next' to continue with column matching.

Note: '**Next**' button is enabled only when you have uploaded a relevant CSV file.

Upload| Column Matching

Label	Action	Description/Example
Mandatory Fields*	Select the columns to match with the data entered in the CSV.	You may add mandatory fields using the toggle button to 'Show Only Mandatory.'

Once the column matching is completed, click 'Import' to import your asset CSV file for asset management.

Asset information is imported from the CSV to the respective category on Infraon. Asset information can be viewed, edited, or deleted using the respective action icon.

Asset Information – SDH / PDH

Upon adding an asset to the Infraon portal, users will be presented with a default view showcasing key details about the asset. This information serves as a quick reference point and can be customized later to fit specific needs.

Asset Properties | Details

Label	Description/ Example
Asset Name	Identify the asset with a user-friendly name.
Asset ID	A unique identifier is assigned to the asset within the system for easy tracking and reference.
IP Address	View the network address associated with the asset.
Status	Quickly understand the asset's current operational state (e.g., Active, Inactive, or Under Maintenance).
Manufacturer	Identify the company that produced the hardware asset.

OS Version	View the operating system version installed on the asset.
Actions	
Edit	Modify any of the asset's details to ensure accuracy and reflect any changes.
Delete	Remove the asset from the inventory if it's no longer needed.
Add Owner	Assign a specific user as the asset's owner, facilitating responsibility and ownership tracking.
Schedule RDP	This functionality is available depending on the specific configuration. It allows users to schedule a remote desktop connection to the asset (useful for managing Windows-based devices remotely).
CLI Session	Initiating a CLI session connects to a network device to execute commands for tasks like configuration, diagnostics, and software updates, enabling efficient device management.

Steps to Initiate CLI Connection

To initiate a CLI session/ Job, follow the below steps:

- Locate the desired asset within the IT asset list.
- Click on the "More Options" menu (usually represented by three dots) and select "CLI Session."
- A pop-up window will appear.
- On the new pop-up tab, enter the IP address, username, port, and access reason, and select the SSH or TELNET protocol.
- Once done, click "Submit" to initiate.

Instructions to Schedule RDP

- Locate the desired asset within the IT asset list.
- Click on the "More Options" menu (usually represented by three dots) and select "Schedule RDP."
- A pop-up window will appear. Choose the date, time, and desired duration (in minutes) for your RDP session.
- Click the "Schedule" button to save your configuration.
- Once scheduled, a "Session is Active" icon will appear on the IT asset within the list. Click on this icon to securely launch the remote desktop connection.

From the Asset grid page, filter the category SDH / PDH and in the filtered grid page, click on the Device Name or IP to view additional information. There are multiple sub views with all necessary information about the device. These are:

Details

Includes Inventory information like basic details, additional properties, Custom Fields and Health Summary.

The following section breaks down the details:

- Device Details
 - Hostname
 - Device Type
 - Tags (Click on 'Edit' to add or remove the tags)
 - Asset ID
 - Device Type
 - IP Address
 - Make
 - Active Version
 - Ci Name
 - Managed EMS IP
 - Managed EMS Name
 - Model
- Owner Details
 - Name
 - Mail ID
 - Mobile number
 - Edit – Click to make changes.
- User Details
 - Name
 - Mail ID
 - Edit – Click to make changes.
 - Deallocate – Click to allocate a new user.
 - Resend Email – Click to resend the e-mail.
- Attachment
 - Choose from the categories (Default, Procurement Documents, Service Documents, Retirement Documents).
 - Add – Click to add new attachments.
- Asset Configuration
 - Creation Time
 - Last Update Time
 - Login Profile
 - Login Profile ID

User Logins/Logouts

Audit the user login and logout entries within the asset management module. This allows IT administrators to identify which users have accessed specific IT

assets (laptops, desktops) and when. This information can help troubleshoot access issues, monitor asset usage, and maintain security compliance.

The inventory agent gathers data on login and logout activity for each asset at regular intervals (inventory updates) and presents this data within the user logins and logouts module.

What you see on the screen

The asset details page displays a user login and logout card. This module details the profile name, number of logins, and number of logouts associated with each user profile for the selected asset. Additionally, a date filter allows technicians to refine the displayed data for a specific timeframe.

Label	Description/ Example
No of Logins	Displays the total number of times a user profile has accessed this specific IT asset.
No of Logouts	Displays the number of times a user profile has ended a session on the IT asset.
Profile Name	This will typically be the user's network login name or alias.
Filter	The date filtering function allows technicians to narrow down the displayed data to a desired timeframe.

Asset Lifecycle

The following section breaks down the details:

- Asset History: Track the entire journey of an asset, from initial purchase through use, maintenance, and eventual disposal.
- Purchase Order Details: View crucial information from the purchase order, including the date, cost, supplier, and specifications.
- Annual Maintenance Contract (AMC): Monitor active AMCs associated with the asset, displaying coverage period, service provider, and key terms.
- Warranty Information: Access comprehensive warranty details like start/end dates, covered components, and claims history.

Panel View

Displays graphical view of a node with all inventory information including shelf, slot, card and port. Port information includes status of port, port utilization and other details.

The following section breaks down the details:

- Service State
- Serial Number
- Vendor
- Name
- Type
- Location
- Capacity
- Layer Rate
- SFP (Small Form Factor) Type
- Vendor
- SFP Status
- SFP Serial Number
- SFP Product Code
- Loopback Mode
- Transmitted Trace
- Received Trace
- PTP (Port of Tanjung Pelepas)
- SFP Installed Version
- IP Address
- MTU (Maximum Transmission Unit)
- PTP (Port of Tanjung Pelepas)
- PVID

Inventory Tree

Displays the list of inventories, part of the device like Rack / Shelf / Slot / Card / Port / SFP details. Click on a specific inventory to view its properties. The inventory includes Shelf, Slot, Card and Port. On click of each port it will show port information for example: Port Status, Optical values of Port etc.

The following section breaks down the property details:

- Name
- IP Address
- Host Name
- Type
- Card Name
- Component Type
- Serial Number
- Part Number
- Physical Status
- Service State

Software

Displays detailed information about the software, including the software name, version, and license details, such as whether the license is purchased or subscription-based and its expiration date. This helps identify the specific program installed and ensures compatibility with other systems. Additionally, it lists all applications installed on the IT asset. To improve searching, a search and

filter feature has been added, allowing filters based on fields like name, type, vendor, and version, with respective conditions.

The following section breaks down the details:

- Alias
- Build Number
- Device Type
- Last Boot-Up Time
- Organization
- OS Installed By
- System Directory
- Version
- Windows Directory
- Boot Device
- Description
- Hostname
- Manufacturer
- OS Installed Date
- OS Name
- Product Key
- System Drive
- Virtual Memory
- Application

Hardware Inventory

Displays complete hardware information of all hardware components. Details include Slot name, Card Name, card state etc. This information can be downloaded in a CSV, Excel or PDF using the action icons.

The following section breaks down the details:

- Search – Click to search the respective inventory.
- Export – Click to choose your export format: Download the inventory as a separate CSV file or an Excel-compatible XLS file.
- Shelf Number
- Slot Number
- Slot Name
- Card Name
- Port Name
- Port State
- Port Number
- SFP Installed
- SFP Type
- Expected Hardware
- Installed Hardware
- Serial Number
- State

My Topology

Displays topology connections for the selected NE. Devices are marked in red/green based on their availability. Mouse over on an asset to view details. Use action icons to navigate through, zoom in and zoom out topology connections.

The following section breaks down the details:

- Grid View – Click to view in a tabular format.
- Map View – Click to view in a map view format.
- Node – Click to see the below details:
 - Host Name
 - IP Address
 - Make
 - Model
 - Device Type
 - EMS Name
 - Firmware Version
 - Region
 - State
 - City
 - Location
- Edge – Click to see the below details:
 - Description
 - Source IP
 - Source Device
 - Source Port
 - Destination Ip
 - Destination Device
 - Destination Port
 - Layer Rate
 - Active Events (Click to redirect to the Active Events page)
 - Services (Click to redirect to the Services page)
- Export – Click to create a PDF of the current topology view.
- Zoom Keys - Icons can be used to navigate through the topology diagram.
- Arrow Keys - Icons can be used to navigate through the topology diagram.

Configuration Details

This option provides technicians with comprehensive access to vital information about network devices. This tab includes a detailed Download Job Summary, offering insights into recent configuration download activities and their outcomes.

The Configuration Details section displays the device's current and historical configurations, enabling comparison and change tracking.

The Inventory Details offer a complete overview of the device's hardware and software inventory. This centralized access to configuration, job summaries, and inventory details empowers technicians to manage and audit network devices efficiently, ensuring configurations are up-to-date and compliant with organizational standards.

The following information can be derived from the page:

Download Job Summary

- Device Credential
- Configuration Profile
- Connection Protocol
- Download Status
- Agent
- Status
- Download Start Time
- Download End Time
- Next Retry Action Time
- Inventory Download protocol
- Startup Configuration download protocol
- Running Configuration download protocol

Configuration Details

- Baseline Running
 - Version
 - Download Time
- Current Running
- Previous V/S Current Running
- Baseline V/S Current Running
- Current Startup
- Baseline Startup
- Previous V/S Current Startup
- Baseline V/S Current Startup

Inventory Details

Events

Events are colour coded based on severity. Use the calendar icon to filter active events for a specific period.

Exports - Choose your export format: Download the topology as a separate CSV file or an Excel-compatible XLS file.

Each event allows the below actions by hovering over the mouse (Quick action tool):

- Analyse
 - Click to view the 'Impact Services' event details. Click on the 'More Details' button to be redirected to the event page.

- Includes details to help analyse the event. User can view the asset details and the statistics of what the current event is performing.
- Acknowledge
 - Used to acknowledge the event. NOC users or technicians can acknowledge and add a comment to let other users know they are working on it.
- Diagnosis
 - Used to perform active diagnosis. Diagnosis can be performed using Ping, SNMP Walk, and Trace Route.
- Ticket
 - Used to create an incident for the event.
- Clear
 - Used to clear the vent. Cleared events can be viewed using the 'Show History' toggle button.
- Activity log
 - Used to view the vent history.

Tickets

Displays the list of open tickets created for this asset.

Click on the ticket name to get redirect to the ticket page.

The following section breaks down the details:

- Ticket ID
- Status
- Created On
- Last Updated On
- Current Assigned
- Impact Asset
- Requester
 - Name
 - Email
 - Phone Number
- Urgency
- Severity
- Impact
- Impact Service
- Service Classification
- Event Status
- Attachment
- Knowledge Base

Services

Lists out all the services, that are verified by UNMS, for the selected NE in a table format.

The following section breaks down the details:

- Search
 - Search for the required service.
- Filter
 - Filter can be added based on the field and condition from the drop-down box below.
- Service Name
- Status (Icon is colour coded for easy identification of service status)
- Type
- A End Node
- E End IP
- A End Port
- Z End Node
- Z End IP
- Z End Port
- Trail Type
- Capacity
- VCAT Size
- Bandwidth (MBPS)
- VLAN ID
- Provision State
- Actions
 - Information - Click the (i) button to access detailed information about this service.
 - Activate – Click to activate the service.
 - Deactivate – Click to deactivate the service.
 - PM Data - Enter the respective details in the following dialog boxes to view the performance report.
 - Path
 - Click to delete the service.

Performance

Used to view performance of the selected Port, Port Type, Statistic etc. based on the applied filter.

The following section breaks down the details:

Filters available for performance report are:

- Port
- Granularity
- PM Type
- Statistic
- Aggregate
- Duration

Add filters to suit requirement and click generate.

Export – These reports can be downloaded in an excel or PDF format using the respective action icon.

Activity Log

The Activity Log meticulously tracks asset changes, providing a comprehensive history of each asset. It records all modifications made by technicians, including changes to city, country, criticality, connection protocol, device credentials, and download job details.

Entries are organized by date and time, allowing for easy monitoring and auditing of asset history. This detailed log ensures that all key actions and updates are documented, facilitating better management and oversight of IT assets.

Export - Audits can be downloaded in CSV, Excel, or PDF formats using the respective action icon.

Lambda Usage (Applicable to DWDM / OTN / ASON)

It displays the number of channels used for that device in a table format, along with the channels available to use.

Port Utilization

This comprehensive grid breaks down port utilization for different card levels and port types. Analyze total ports available, ports currently in use, unused ports, and the percentage of utilized capacity for each category.

CTP Utilization (Applicable to SDH)

Displays the STM Ports with Shelf/Slot/Card/Port information along with capacity used information like VC4, VC3, VC12 usage for that port in a graphical format along with what are the KLM available to use.

E1 Trails (Applicable to SDH)

Detailed Trail Information:

- EMS Name:

Pinpoint the Element Management System responsible for each E1 trail, simplifying network management tasks.

- Trail Label:

Easily identify specific E1 trails using their assigned labels for quick reference and troubleshooting.

- Trail State:

Monitor the current operational status of each E1 trail (e.g., Active, Inactive, Faulted). This allows for proactive problem identification and resolution.

- Node and Port Information:
 - A-End Node and Service Port:

Track the origin of each E1 service and the port it enters the node.

- Z-End Node and Service Port:

Identify the destination of each E1 service and the port it exits the node.

- Path:

Visualize the complete physical path of each E1 trail through the network, aiding in fault isolation and optimization efforts.

Export - Click to choose your export format: Download the details as a separate CSV file or an Excel-compatible XLS file.

VCG Trails (Applicable to SDH)

This feature provides a detailed view of VCG (Virtual Circuit Group) and Ethernet services traversing through a specific node in your network, displayed in a table format.

The following section breaks down the details:

- VCG/Ethernet Service ID: Unique identifier for the service.
- Source: Originating point of the service, including node and port information.
- Destination: Ending point of the service, including node and port information.
- Type: Specifies the service type (e.g., VCG-64, VCG-4096, Ethernet Link).
- Status: Indicates the current state of the service (e.g., Active, Dropped, Passing Through).
- Reason (for Dropped Services): Provides details about why the service is dropping at the selected node (e.g., Administrative shutdown, Faulty link, Bandwidth shortage).
- VLAN (for Ethernet Services): Displays the associated VLAN ID for Ethernet services.

Cross Connections (Applicable to SDH)

The list details all cross connections established between various optical ports and client ports, including:

- Optical Port Type: Identify the type of optical port involved in each connection (e.g., STM-1, STM-4, Ethernet).
- Client Port Type: Understand the nature of the client port connected to the optical port (e.g., E1, ATM, IP).
- Additional Information: The following section breaks down the details:
 - User Label
 - Source Port
 - Source JKLM
 - Destination Port
 - Destination JKLM
 - Source Protected Port.

Export - Click to choose your export format: Download the details as a separate CSV file or an Excel-compatible XLS file.

Flow Domain (Applicable to SDH)

A comprehensive view of all configured Ethernet to VCG mappings at your fingertips. Identify how specific Ethernet ports are associated with corresponding VCGs, ensuring clear understanding of traffic routing within the node.

Export - Click to choose your export format: Download the details as a separate CSV file or an Excel-compatible XLS file.

Protection Group (Applicable to SDH)

Get a comprehensive overview of all protection groups established between optical ports within the node. Easily identify their names, types, and associated ports for quick reference and analysis.

Export - Click to choose your export format: Download the details as a separate CSV file or an Excel-compatible XLS file.

Channel Mapping (Applicable to PDH)

Displays the E1 Channel Mapping between E1 Ports and E1 to Client (Voice, Data, Voice_Data) Channels in tabular format. Each entry clearly depicts the source E1 port, the specific E1 channel involved, and the corresponding client circuit type it serves. This detailed view fosters accurate tracking and understanding of signal routing within your network.

E1 Channel Utilization (Applicable to PDH)

Displays the E1 Ports with Shelf/Slot/Card/Port information along with channel used information for that port in a graphical format along with what channel is mapped to 64Kbps of Voice, Data, Voice_Data Service.

Consumable Asset (Beta)

Consumable assets are resources gradually used or consumed over time, such as printer ink, paper, cleaning supplies, or markers. While essential to daily operations, these items require careful management to ensure continuous availability and cost control.

Infraon Infinity's **Consumable Assets** module offers a robust solution for tracking and managing these resources. This module allows users to monitor asset availability and associated costs, ensuring comprehensive oversight of all consumable assets.

What do you see on the screen

The Consumable Asset management interface shares a consistent layout with other asset management sections, including IT Assets, Fixed Assets, Software Inventory, and Software Licenses. Asset categories are displayed in the screen's left navigation panel.

To help you get started:

- Browse categories by using the intuitive left sidebar
- Click any category to view its associated assets
- Use filters and sorting options to find specific items quickly

Like the **IT Assets** and **Fixed Assets** modules, consumable assets can be organized into categories for easier management and tracking. This allows organizations to classify and manage resources based on type, usage, or department needs.

Note: Refer to the '[Asset Categories](#)' section for more information.

The following table provides detailed information about consumable asset management:

[Consumable Assets](#) | Basic Details |

Label	Action	Description/ Example
Search	Allows searching for specific consumable assets	Search by asset ID, asset name, owner, etc., to quickly find the required consumable asset
Filter	Apply filters based on specific fields and conditions	Fields: Asset Name, ID, Owner, Location, Requester, and Type. Conditions: "in," "not in," "equal to," "and" "not equal to" from the drop-down options.

Add Item	Click to add a new consumable asset to the inventory	Choose between adding an asset manually or importing a CSV file for bulk upload.
Asset Name	Click on the asset name to view more details in a pop-up window	Displays the asset name (e.g., Markers, Printer Ink). Clicking will open a pop-up showing Summary, Inventory Details, and Recent Activities.
Asset ID	View-only field: no actions can be taken	Displays the unique asset ID associated with the consumable asset (e.g., INFRAON0448).
Vendor	View-only field: no actions can be taken	Shows the vendor name associated with the consumable asset (e.g., Microsoft, Camlin).
Type	View-only field: no actions can be taken	Indicates the asset type, such as whether the asset is degradable or non-degradable (e.g., Degradable, Non-Degradable).
Total Quantity	Modify the asset's quantity	It displays the total stock available. Click on the plus or minus to adjust the quantity and add the respective details: Location, Quantity, Price, Total Price, Expiry By, and Vendor in the pop-up window.

Add Consumable Asset

There are two ways to add consumable assets:

1. **Single Asset** - You can add a single asset from the drop-down menu in the top right corner
2. **Import from CSV** - If you have the asset CSV file, you can import it from the drop-down menu in the top right corner.

Instructions to 'Add Single Asset'

- In the **Asset** module, go to the **Consumable Asset** submodule page.
- Click **Add Item** and choose **Single Asset**.

There are two tabs on the 'Add Asset' page. Refer to the table for information.

[Define Asset](#) | Add Asset info

Label	Action	Description/ Example
Product Image	Add an image or icon representing the asset	Use the drag-and-drop feature or upload files in

		PNG, JPG, or JPEG formats (Max size: 20 MB)
Asset Name	Enter a specific name for the asset	Assigning a unique name makes it easier to locate and identify the asset
Category	Select the appropriate category from the dropdown	Placing an asset in a specific category streamlines navigation and organization
Owner/Technician	Choose from the dropdown list	Designate an owner or technician responsible for the asset
End User/Requester	Choose from the dropdown list	Identify the end user or requester who will be utilizing the asset
Owner Tags	Select tags from the dropdown	Assign tags to the owner for simplified identification and filtering
Asset Tags	Select tags from the dropdown	Tag the asset for enhanced searchability and filtering
Location	Choose the asset's storage location from the dropdown	Specify where the asset will be stored to assist in inventory tracking and management

Note: Fields marked with asterisk (*) are mandatory.

Once all the parameters are added, click 'Next' to add consumable details.

[Consumable Details](#) | [Common Properties](#)

Label	Action	Description/ Example
Quantity	Enter a whole number or decimal value	Specify the available quantity of the asset in the inventory
Re-Order Quantity	Enter a whole number or decimal value	Define the minimum quantity level that will trigger a reorder to maintain stock availability
Buying Price	Enter a whole number or decimal value	Specify the purchase price per unit of the asset
Selling Price	Enter a whole number or decimal value	Set the selling price of the asset if it's available for resale
Low Stock Threshold	Enter a whole number or decimal value	The minimum quantity level set for inventory items triggers a reorder alert to prevent stockouts.

Threshold User Type	Select from the dropdown	Select whether the threshold is based on a Department or User level
Threshold To	Choose from the dropdown	Based on the selected user type, choose the specific user or department responsible for managing the threshold
Type	Select from the dropdown	Specify whether the asset is Degradable or Non-Degradable
Expiry Date	Click to open a calendar to select a date	Enter the expiration date of the consumable asset
Model	Input the model number	Provide the model number associated with the asset for better tracking and identification
Description	Input descriptive details	Include relevant details about the asset to enhance clarity and understanding
Currency	Select from the dropdown	Choose the currency in which the asset was purchased to maintain accurate cost records

Note: Clicking "**Show Mandatory Icon**" will display only the mandatory fields within the tab.

Once all the parameters are added, click 'Submit.' The Asset is added under the selected category within Infraon Infinity.

Instructions to 'Import from CSV'

Upload a CSV file containing the asset details to add multiple assets simultaneously. This process works similarly to importing a CSV file to add multiple IT or Fixed Assets. [Click here to learn more.](#)

Asset Details

The **Asset Details** page provides a comprehensive overview of each asset, displaying essential information on the top panel, such as:

- Product Image
- Asset Name
- Asset ID
- Asset Type
- Model
- Vendor

On the left panel of the page:

Cost Properties

Users can track the financial aspects of consumable assets, with each asset listing key cost-related information, such as:

- Total Inventory Cost
- Average Buying Price
- Selling Price

This feature allows organizations to effectively monitor costs and profitability, providing better control over financial resources.

Managed By

Under the " Managed By " section, administrators can assign specific users to oversee individual assets, ensuring clear accountability and efficient management.

Tags

This section displays a list of tags associated with each asset, enabling easier navigation and quick filtering for faster access to relevant asset information.

Action Icons

Refer to the following table for detailed information:

Action Icons | Basic Details

Label	Action	Description/ Example
Add Stock	Click to modify inventory details	Use this option to add more items to the inventory. In the pop-up window, provide details such as Location, Quantity, Price, Expiry Date, and Vendor , then click Add to confirm.
Distribute	Click to allocate inventory assets	Distribute the asset to specific users or departments. In the pop-up window, enter details such as Location, Quantity, and Distribution Type (User/Department) , then click Distribute to finalize.
Edit	Click to open a pop-up window for updates	It allows users to modify asset details, including the Name, Image,

		Owner, Requester , and other relevant fields.
Delete	Click to remove the asset from the inventory	Permanently deletes the consumable asset from the inventory. Confirm the action by selecting Yes, Delete It.

The **Asset Details** page is organized into three distinct sections located on the left panel of the page.

Summary

The module offers comprehensive tracking of inventory status across various periods—**weekly, monthly, and yearly**.

Users can monitor asset availability by **location**, gaining insights into the number of assets in **Instock**, newly **Added** items, and those that have been **consumed**. This functionality ensures optimal inventory management and aids in predicting future asset needs.

Inventory History

The **Inventory History** section provides a comprehensive overview of stock movements, allowing users to view **inventory levels by location, quantity, available quantity, action type, vendor, status, added date, and expiration date**. This makes it easy to track changes in stock over time, helping teams plan for restocking or asset replenishment based on consumption trends.

Recent Activities

The **Recent Activities** section captures the complete history of each asset, including:

- When the asset ID was created, modified, or updated.
- Any changes in asset status, location, or ownership.
- This audit trail ensures that users have full visibility into each asset's lifecycle, making it easier to trace any changes for reporting or troubleshooting purposes.

Action Icons

Label	Action/ Description
Search	Search for the required asset's history by adding its name or ID or filtering by the user who made changes to it.
Date Range	Apply a filter to view the asset history within a specified time frame. From the drop-down menu, select options

	such as Current Hour, Last 30 minutes, Last Hour, etc.
Export	Click to download the asset history details in CSV format. This format enables easier analysis of asset history for tracking and financial purposes.
Timeline View	View the asset history in a timeline format. This provides a visual representation of changes made over time, allowing users to assess the sequence of events and modifications quickly.
Grid View	Switch to a grid view for a more structured and tabular representation of the asset history. This view is ideal for comparing and analyzing multiple data points at once.

Software Assets

When devices are discovered using Infraon (inventory agent), software installed in those devices is listed under the asset module as Software.

Download, view, and manage software entries, also blacklist/whitelist and uninstall software.

The discovered software is categorized based on the manufacturer. You have the option to blacklist or whitelist a specific software.

Check the Blacklist and Whitelist and Software License Management module for details.

Software License

What is Software license management?

A Software license is a document that refers to the software's developers and users. It defines how software can be used and paid for.

What do you see on screen?

Publishers: The publishers can be Adobe, Autodesk, Windows, and more.

Search: Search the License by adding filters.

License name: The license name will appear in card view.

Total: Total License for particular software appears here.

Allocated: Allocated license for the particular software appears here.

Free: Free License appears here.

License Type: License type can be selected from the drop-down.

Software image: Upload the image of the software.

Click on the license and the software license view page opens. There are five sections such as:

1 Software details:

- 1 License software image along with the version
- 1 Pie chart of the License usage such as Total license, available license, allocated license, and under-licensed.
- 1 The compliance status, License based on, and license type appear in this tab.

2 **License Life Cycle:** The start date as effective from and the end date of the license appears in this page.

3 **Insights:** Overall view of the license with the license details as it is allocated and the effective start date.

4 **License usage:** License usage is shown in a graph from the start to the end.

5 **Allocated assets:** The asset's Hostname, IP Address, Device Type, Vendor, and actions are in the allocated assets sections.

Bulk Upload Of Software License

Import licenses in bulk via CSV files, with a generous limit of 5000 records. Download the sample to update license information and make the necessary changes easily.

Software license alert notification

Set up alert notifications for license expiry on the Software License Page. Enable the notify toggle, and specify the notification period along with the recipient's email address. The Alert notification is applicable only for license types with an end date.

CMDB view

Easily establish connections between assets and their respective locations or departments. Simply navigate to the asset, click 'relationship', and choose 'upstream' or 'downstream'. Explore an intuitive dropdown menu with location and department options, which makes asset management more precise and streamlined.

Update CI relation and asset when user, requester, department, asset, or location is modified and CI relation created based on the rule

Introducing CI Rule Configuration in CMDB! Customize rules for departments, locations, requesters, software, and users. Automatic addition of required rules. Enable/disable CI visibility based on relationships and configurations for a tailored experience.

CI relationship in CMDB Downstream

Name	Parent	Child	Description
Author of	Author of the selected CI	Selected CI is written by this CI	The attribute pertains to the authorship of a selected CI
Backed up by	Back up of the selected CI	Is backed up by the Selected CI	This feature refers to the backup status of a chosen CI
Cluster of	Belongs to the cluster of the selected CI	Belongs to the cluster of the selected CI	This signifies the membership of a chosen CI within a specific cluster.
Connected by	Selected CI is connected by this CI	Connected by the selected user	Indication that the chosen CI is connected by another CI or user, highlighting a relationship where the selected CI is linked or associated with the connecting CI or user. Example: Internet Connection, a smartphone is connected by a cellular network, providing access to the internet.
Connected to	Selected CI is connected to this CI	Connected to the selected CI	Showcases a connection or relationship between the two components. For example: IoT, the connected to field for the bulb would display the hub's name.
Consists of	Selected CI consists of this CI	Consists of selected CI	This indicates that the chosen Configuration Item is composed of or includes another CI as its component or part, highlighting a relationship where the selected CI is made up of the specified component CI. Example: Data model, a database schema consists of tables, relationships, and attributes that define the data structure.
Consumed by	Selected CI is consumed by this CI	Consumed by the selected CI	This attribute indicates that the chosen Configuration Item is consumed or utilized by another CI or process, highlighting a relationship where the selected CI is a resource, input, or service used by the consuming CI. Example: Service Dependency, a micro service is consumed by another micro service in a micro services architecture.
Attached by	Selected CI contains this CI	Is attached by the selected CI	This attribute indicates that the chosen Configuration Items attached, linked, or associated with another CI, highlighting a relationship where the selected CI is connected or added as a component or part to the attaching CI. Collaborative Document contains an attached comment thread for discussions.

Contains	Selected CI contains this CI	Contains the selected CI	Indication that the chosen Configuration Item includes, encompasses, or holds another CI as a part, component, or element, highlighting a relationship where the selected CI acts as a container for the contained CI. Example: Database Table contains multiple tables that store structured data.
Cools	Selected CI cools this CI	Cools the selected CI	The attribute indicates that the chosen Configuration Item functions to cool, dissipate heat, or regulate temperature for another CI, highlighting a relationship where the selected CI plays a role in maintaining the temperature of the cooled CI.
Defines Resources for	Selected CI defines resources for this CI	Define Resources for the selected CI	The chosen Configuration Item establishes, specifies, or sets resources, capabilities, or allocations for another CI, highlighting a relationship where the selected CI provides resource definitions or guidelines to the CI it defines resources for. Example: Cloud Resource Configuration defines resources like virtual machines and storage for a cloud deployment.
Depends on	Selected CI depends on this CI	Depends the selected user	This attribute indicates that the chosen Configuration Item relies on or has a dependency on another CI or user, highlighting a relationship where the selected CI requires the support, functionality, or input of the depending CI or user to operate effectively. Example: Network Connectivity, a printer depends on network connectivity to receive print jobs from users.
Distributed by	Selected CI is distributed	Is distributed by the selected CI	The chosen Configuration Item is distributed or made available to others by another CI, entity, or user, highlighting a relationship where the distributing CI facilitates the dissemination or availability of the selected CI. Example: Newsletter Dissemination. An email newsletter is distributed by a company to its subscribers.

DR provided by	Selected CI's DR (Disaster Recovery) is provided by this CI	DR provided by the selected CI	The chosen Configuration Item serves as the source or provider of Disaster Recovery capabilities for another CI, highlighting a relationship where the providing CI ensures the availability of recovery mechanisms in the event of a disaster affecting the selected CI. Example: Data archival system ensures disaster recovery by storing historical data for compliance and recovery purposes.
Editor	Editor of the selected CI	Edited by the selected user	Indication that the chosen Configuration Item is associated with an entity or user who is responsible for making edits, modifications, or updates to the content, settings, or configuration of the selected CI. This relationship highlights the role of the editor in managing changes to the selected CI. Document Editor: An editor is responsible for editing and revising a document (selected CI) to improve its content.
Enables	Enables the selected CI	Is enabled by the selected CI	This attribute indicates that the chosen Configuration Item empowers or allows the functionality, operation, or capabilities of another selected CI. This relationship highlights the role of the enabling CI in providing necessary support or resources for the enabled CI. Example: An API enables developers to interact with software components programmatically.
Exchanges	Selected CI exchanges information with the selected CI	Exchanges information with the selected CI	Indication that the chosen Configuration Item is involved in a two-way exchange of information, data, or communication with another selected CI. This relationship highlights the active communication and interaction between the two CIs. Data Synchronization: Two databases exchange data updates to ensure consistency between them.
Exchanges data with	Selected CI exchanges data with this CI	Exchanges data with the selected CI	The attribute indicates that the chosen CI shares or transfers data with another CI, highlighting a relationship where both CIs interact to exchange specific data or information. Example: API Communication A web application can exchange data with a third-party API to retrieve external information or perform specific actions.

Feeds	Selected CI feeds this CI	Is fed by the selected CI	The chosen Configuration Item provides data, information, resources, or inputs to another CI, highlighting a relationship where the selected CI serves as a source or supplier of essential elements to the fed CI. Example: Sensor Data in a smart home feed data on temperature, humidity, and occupancy to a central control system.
From template	Selected CI has this CI	From template for selected CI	The indicates that the chosen Configuration Item is derived, created, or instantiated from a specific template CI, highlighting a relationship where the selected CI is based on or follows the structure, configuration, or guidelines provided by the template CI. Example: Software codebase is developed following a coding template for coding standards and best practices.
Has Registered	Selected CI has been registered to this CI	Has registered on the selected user	The chosen Configuration Item has been registered or recorded on another CI, highlighting a relationship where the selected CI is associated with or documented on the registering CI. Example: Software License has been registered with a licensing server, enabling the authorized use of the software.
Hosted on	Selected CI has been hosted on to this CI	Hosted on the selected CI	This attribute indicates that the chosen Configuration Item is hosted, deployed, or run on another CI, typically a server or computing environment. This relationship highlights that the selected CI relies on the hosting CI for execution and resources. Example: Cloud Service Hosting is hosted on a cloud provider's infrastructure for scalability and availability.
Impacted By	Selected CI is impacted by this CI	Impacted by the selected CI	The chosen Configuration Item is affected, influenced, or impacted by another CI, event, or factor, highlighting a relationship where the selected CI's functioning, state, or performance is influenced by the impacting CI or event. Example: Network Outage, a server is impacted by a network outage causing loss of connectivity.

Implement End Point To	Selected CI is implemented the endpoint from this CI	Implement the endpoint from the selected CI	Indication that the chosen Configuration Item has implemented an endpoint from another CI, implying that the selected CI has established a connection, interface, or access point to the endpoint CI. Example: IoT Device Interaction, a smart home controller implements endpoints from various IoT devices to control and monitor them.
In Rack	Selected CI has been in rack to this CI	In Rack contains the selected CI	The chosen Configuration Item is physically located within or housed in a specific rack or rack unit. This relationship highlights the physical placement of the selected CI within the specified rack. Example: Storage system are installed in storage racks for data storage and retrieval.
Includes	Selected CI has been included on to this CI	Includes the selected CI	The chosen Configuration Item encompasses or contains another CI as a component, feature, or part, highlighting a relationship where the including CI has the selected CI as an integral element. Example: Software Module, an application platform includes individual software modules that provide specific functionalities.
Instantiates	Selected CI has been instantiated on this CI	Instantiates the selected CI	This attribute indicates that the chosen Configuration Item has been created, initialized, or instantiated on another CI, typically a computing environment or platform. This relationship highlights the process of setting up and initiating the selected CI within the context of the instantiating CI. Example: Software execution, an application is instantiated on a user's device or computer to run and perform tasks.
IP Connection	Selected CI has IP Connection to this CI	IP connection of the selected CI	This attribute indicates that the chosen Configuration Item is linked or connected to another CI through an Internet Protocol connection, facilitating data transmission and communication between the two CIs. Example: Remote Access, a remote desktop application, uses IP connections to allow remote access to a host computer.

Located In	Selected CI located in this CI	Located In for the selected CI	The chosen Configuration Item is physically situated within or positioned inside another CI, typically a larger or encompassing physical entity. This relationship highlights the spatial location of the selected CI. Example: Storage room, files are located in a storage room for safekeeping.
Located in Zone	Selected CI located in zone to this CI	Located In zone for the selected CI	This attribute indicates that the chosen Configuration Item is positioned within a specific zone or area, usually with defined boundaries or characteristics. This relationship highlights the spatial location of the selected CI within the context of the zone CI. Example: Medical zone, the Medical devices are located in a medical zone within a hospital.
Manages	Selected CI has been managed on to this CI	Manages the selected CI	The chosen Configuration Item is under the management, control, or supervision of another CI or entity. This relationship highlights the overseeing and administrative role of the managing CI over the selected CI. Example: Asset Management, an IT asset management system manages computers and devices by tracking their usage and status.
Master of	Selected CI has master of the selected CI	Master of the selected CI	This attribute indicates that the chosen Configuration Item serves as a master or primary entity in relation to another CI. This relationship highlights that the selected CI is governed, controlled, or derived from the master CI. Example: Master Configuration, a master configuration file, defines standard settings for software applications.
Owns	Selected CI has been owned on to this CI	Owns the selected CI	The chosen Configuration Item is owned, possessed, or controlled by another CI or entity. This relationship highlights the ownership and responsibility that the owning CI has over the selected CI. Example: Resource Ownership, a team owns a shared server and manages its access and usage.

Powers	Selected CI has been Powered on to this CI	Powers the selected CI	Indication that the chosen Configuration Item is a source of power that enables the operation or functionality of another CI. This relationship highlights the role of the powering CI in supplying the necessary energy for the selected CI. Example: Power adapter, powers a printer by converting electrical current.
Provided By	Selected CI depends on this CI	Provides by the selected user	This Configuration Item relies on or is supported by another CI or entity for specific resources, services, or functionalities. This relationship highlights the provider's role in offering what the dependent CI needs. Example: Network connection, an application depends on a network router to establish internet connectivity.
Provides storage for	Selected CI's storage is provided by this CI	Provides storage for the selected CI	This attribute serves as a source or provider of storage resources for another CI. This relationship highlights the role of the providing CI in supplying the storage capacity required by the dependent CI. Example: Storage Array provides high-performance storage for databases in an enterprise environment.
Provisioned From	Selected CI depends on this CI	Provisioned from the selected CI	The chosen Configuration Item is provisioned, set up, or derived from another CI or entity. This relationship highlights the source from which the selected CI is created or obtained. Example: Server blueprint, a physical server is provisioned from a server blueprint that defines hardware and software settings.
Receives data from	Selected CI depends in this CI	Receives data from the selected CI	This attribute indicates that the chosen Configuration Item receives data, information, or communication from another source or CI, highlighting a relationship where the selected CI depends on the specified CI to provide data or input. Example: IoT Data exchange is a central data hub receives data from multiple IoT devices for storage and analysis.

Registered on	Selected CI has been registered on this CI	Registered on the selected CI	Indicates that the chosen CI is registered or associated with a specific user, highlighting a relationship where the selected CI is linked to the specified user for identification or ownership purposes. Example: Software Licenses is registered on user's account, indicating that the user has ownership rights to use the software.
Routes Traffic	Selected routes traffic depends on this CI	Routes Traffic for the selected CI	This attribute plays a role in directing or routing network traffic for another CI. This relationship highlights the routing capabilities of the routing CI and its influence on the path of traffic for the selected CI. Example: Router, routes network traffic between subnets and directs data packets for servers.
Runs	Initiated running for selected CI	Runs the selected CI	Configuration Item initiates or is responsible for the execution and operation of another CI. This relationship highlights the role of the running CI in starting and managing the functionality of the selected CI. Example: Web Server, a web server runs websites and serves web content to users.
Sends Data To	Selected CI sends data to selected CI	Sends data to selected CI	The attribute indicates that the chosen Configuration Item is capable of transmitting or forwarding data to another selected CI. This relationship highlights the ability of the sending CI to deliver information or data to the receiving CI. Example: Network device, a computer sends data to a printer for printing.
Submits	Selected CI has been submitted to this CI	Submits the Selected CI	This attribute indicates that the chosen Configuration Item is presented or provided to another CI or entity for a specific purpose, often involving approval, review, or processing. This relationship highlights the action of submitting the selected CI to the receiving CI. Example: Document Submission, an employee submits an expense report to the finance department for reimbursement.
Subscribes to	Selected CI depends on this CI	Subscribes to by selected user	The attribute indicates that the chosen Configuration Item is linked to or relies on another CI or entity for receiving updates, notifications, or information. This relationship highlights the act of subscribing to the source CI for relevant updates. Example: Software Updates, a

			system administrator subscribes to software updates for security patches.
Supports	Selected CI has been supporting to this CI	Supports the selected CI	The chosen Configuration Item provides assistance, help, or resources to another CI or entity. This relationship highlights the role of the supporting CI in aiding and assisting the supported CI. Example: Technical Support, a help desk provides technical support to resolve issues with software applications.
Use End Point To	Selected CI uses end point to this CI	Use End Point to the selected CI	The chosen Configuration Item leverages or interacts with another CI or entity as an endpoint to achieve a specific purpose. This relationship highlights the utilization of the endpoint CI to fulfill a particular function for the using CI. Example: Messaging Platform, a chatbot uses a messaging platform's endpoint to interact with users.
Used by	Selected CI is used by the this CI	Used by the selected user	This attribute indicates that the chosen Configuration Item is actively utilized, operated, or relied upon by another CI or entity. This relationship highlights the role of the using CI in utilizing the functionalities or resources of the selected CI. Example: Application Usage, a software application is used by end-users to perform tasks.
Virtualized by	Selected CI is virtualized by this CI	Virtualized by the selected CI	The chosen Configuration Item has been transformed into a virtualized instance by another CI or entity. This relationship highlights the role of the virtualizing CI in creating and managing virtual instances of the selected CI. Example: Desktop virtualization, virtualizes desktop environments for remote access.

CI relationship in CMDB Upstream

Name	Parent	Child	Description
Written By	Selected CI is written by this CI	Author of the selected CI	The attribute pertains to the authorship of a selected CI
Backed up by	Is backed up by the Selected CI	Back up of the selected CI	This feature refers to the backup status of a chosen CI

Cluster	Belongs to the cluster of the selected CI	Belongs to the cluster of the selected CI	This signifies the membership of a chosen CI within a specific cluster.
Connects	Connects to the selected CI	Selected CI is connected by this CI	Indication of the selected CI is linked to or communicates with the specified CI. For Example: if a router (selected CI) is connected to a switch (connecting CI), the "Connects" attribute for the router would show the switch's name, indicating the network link.
Connected to	Connected to the selected CI	Selected CI is connected to this CI	Showcases a connection or relationship between the two components. For example: IoT, the connected to field for the bulb would display the hub's name.
Are part of	Is a part of the selected CI	Selected CI is part of this CI	Signifies that the chosen CI is a component or element within another CI, illustrating a hierarchical relationship.
Consumes	Consumes the selected CI	Selected CI is consumed by this CI	The chosen CI utilizes or relies on another CI for its operation or functionality, representing a dependency where the selected CI consumes the specified CI.
Attached to	Is attached to the selected CI	Selected CI contains this CI	Denotes that the selected CI is connected to or contained within the specified CI. For example: In email clients, files attached to an email are indicated through the "Attached to" field. The files are linked to the email they are attached to.
Contained By	Is contained by the selected CI	Selected CI contains this CI	Signifies that the chosen CI is encompassed or hosted within another CI, indicating that the selected CI is a part of or nested within the specified CI. For example: In web development, widgets or elements contained by a web page are represented by the Contained By field. The elements are part of the web page's content.
Cooled By	Is cooled by the selected CI	Selected CI cools this CI	This attribute signifies that the chosen CI is responsible for cooling another CI, indicating a relationship where the selected CI is the source of cooling for the specified CI. Example:
Gets Resources from	Gets resources from the selected CI	Selected CI defines resources for this CI	The chosen CI receives resources from another CI, signifying a dependency where the selected CI relies on the specified CI to provide necessary resources. Network devices like routers get resources such as bandwidth and routing information from core switches.

			The Gets resources from field for the router would list the core switch's name.
Used by	Is used by the selected user	Selected CI depends on this CI	The attribute signifies that the chosen CI is utilized by a specific user, indicating a relationship where the selected CI plays a role in providing functionality or value to the user. For example: Software applications, this is used by a certain user, the attribute for the application would display the user's name. This indicates that the user relies on the application for their tasks.
Distributes	Is used to distribute the selected CI	Selected CI is distributed	Indication that the chosen CI serves the purpose of distributing another CI, highlighting a relationship, selected CI is responsible for disseminating or sharing the specified CI. Example: Data sharing point, where a file service distributes files and documents to authorized users. The distributes field for the service would indicate its role in distributing files.
Provides DR for	Provides DR (Disaster Recovery) for the selected CI	Selected CI's DR (Disaster Recovery) is provided by this CI	The attributes signifies that the chosen CI is responsible for offering disaster recovery services for another CI, indicating a relationship where the selected CI is a source of recovery in case of a disaster affecting specified CI. Example: High availability cluster, provides disaster recovery by ensuring seamless failover in case of components failures
Is Edited by	Is edited by the selected user	Editor of the selected CI	This attribute indicates that the chosen CI is modified or edited by a specific user, highlighting the relationship where the selected CI is subject to changes made by the specified user. Example: Configuration Files: A configuration file is edited by an administrator to adjust settings or parameters for a software application or system.
Is enabled by	Is enabled by the selected CI	Enables the selected CI	This signifies that the chosen CI is made functional or operational by another CI, highlighting a relationship where the selected CI relies on the specified CI to enable its functionality. Example: Network Services, like remote desktop access is enabled by a service

			daemon that runs in the background to facilitate the service.
Exchanges	Exchanges information with the selected CI	Selected CI exchanges information with the selected CI	Indication that the chosen CI shares or transfers information with another CI, showcasing a relationship where both CIs interact to exchange data or communication. Example: IoT Devices, in a smart home can exchange data with a central hub to provide real-time status updates and receive commands.
Exchanges data with	Exchanges data with the selected CI	Selected CI exchanges data with this CI	The attribute indicates that the chosen CI shares or transfers data with another CI, highlighting a relationship where both CIs interact to exchange specific data or information. Example: API Communication A web application can exchange data with a third-party API to retrieve external information or perform specific actions.
Fed By	Is fed by the selected CI	Selected CI feeds this CI	The chosen CI receives inputs or resources from another CI, emphasizing a relationship where the selected CI is supplied with essential inputs or support by the specified CI. Example: Workflow automation, an automated process can be fed by data inputs that trigger different stages of the workflow.
Template for	Is a template for selected CI	Selected CI has this CI	This attribute indicates that the chosen CI serves as a template for another CI, highlighting a relationship where the selected CI provides a blueprint or predefined structure that the specified CI follows. Example: Email Template, provides a standardized format for creating consistent emails. The "Template for" field for the template would indicate its role in email communication.
Is Attached To	Is attached to the selected CI	Selected CI has this CI	This attribute signifies that the chosen CI is physically or logically connected to another CI, highlighting a relationship where the selected CI is part of or connected to the specified CI. Example: Documents in Email, an attachment is attached to an email indicating that the attachment is sent along with the email.
Is Registered On	Is registered on the selected user	Selected CI has been registered to this CI	Indicates that the chosen CI is registered or associated with a specific user, highlighting a relationship where

			the selected CI is linked to the specified user for identification or ownership purposes. Example: Software Licenses is registered on user's account, indicating that the user has ownership rights to use the software.
Hosts	Hosts the selected CI	Selected CI has been hosted on to this CI	The attribute indicates that the chosen CI provides hosting or support for another CI, highlighting a relationship where the selected CI is being hosted or managed by the specified CI. The attribute indicates that the chosen CI provides hosting or support for another CI, highlighting a relationship where the selected CI is being hosted or managed by the specified CI. Example: Cloud Infrastructure a virtual machine instance hosts a software application in a cloud environment, providing the necessary resources for the application to run.
Impacts	Impacts the selected CI	Selected CI is impacted by this CI	The attribute indicates that the chosen CI has an effect or influence on another CI, highlighting a relationship where the selected CI directly or indirectly affects the specified CI. Example: Software Updates can impact the stability and functionality of an application, potentially introducing new features or causing compatibility issues.
Implement End Point From	Implement the endpoint from the selected CI	Selected CI is implemented the endpoint from this CI	The chosen CI is used to create or establish an endpoint based on another CI, highlighting a relationship where the selected CI is implemented to provide a specific endpoint using the features or capabilities of the specified CI. Example: Network Endpoint is implemented by configuring a network device, allowing data to be sent or received through the endpoint.
Rack contains	Rack contains the selected CI	Selected CI contains this CI	This indicates that the chosen CI is physically located within a rack, emphasizing a relationship where the selected CI is housed or positioned inside the specified rack. Example: Server Rack Configuration is contained within a server rack, highlighting that the server is physically installed and mounted in the rack.
Member of	Is a member of the selected CI	Selected CI contains this CI	The chosen CI is a part of or belongs to a larger entity or group represented by

			the selected CI. This relationship highlights that the selected CI contains or encompasses the specified CI as a constituent element. Example: Software modules, can be a member of a larger platform, indicating that the application is part of the platform offering various functionalities.
Instantiated by	Is instantiated by the selected CI	Selected CI initiates this CI	The indication that the chosen CI is initiated, created or brought into existence by another CI, highlighting a relationship where the selected CI is the result of an instantiation process initiated by the specified CI. Example: Virtual machine can be instantiated by a hypervisor, indicating that the hypervisor creates and manages the VM.
IP Connection	IP connection of the selected CI	Selected CI has IP Connection to this CI	This CI has an IP connection to another CI, highlighting a relationship where the selected CI is connected to the specified CI through an IP-based network connection. Example: Web services can have an IP connection to a load balancer distributing incoming traffic among multiple instances of the service.
Contains Room	Contains room for selected user	Selected CI has room	Provides a room intended for a specific user, highlighting a relationship where the selected CI encompasses a physical space designated as a room for the specifies user.
Zone contains	Zone contains for selected CI	Selected zone contains the selected CI	A specific zone or area, highlighting a relationship where the selected zone encompasses or contains the specified CI.
Managed by	Is managed by the selected user	Selected CI depends on this CI	The management or oversight of a specific user, highlighting a relationship where the selected CI relies on the specified user for administration, control or maintenance. Example: Network device management is managed by a network engineer, indicating that the engineer is responsible for its configuration and operation.
Stack Member of	Stack member of the selected CI	Selected Stack member of the selected CI	The chosen CI is a member or component of a larger stack or assembly represented by the selected CI. This relationship highlights that the selected CI is part of the specified stack

			or grouping. Example: Automation frameworks can be stack member within an automation framework, highlighting that the module is part of the framework's functionality.
Owned by	Is owned by the selected CI	Selected CI is owned by this CI	This attribute indicates that the chosen CI is owned or possessed by a specific entity, user, or group represented by the selected CI. This relationship highlights that the selected CI is under the ownership or responsibility of the specified owner. Example: Digital Assets ownership is owned by the organization.
Powered by	Is powered by the selected CI	Selected CI is powered by this CI	The chosen configuration is powered or energized by another CI, highlighting a relationship where the selected CI relies on the specified CI for the necessary power source or energy supply. Example: Data center servers are powered by uninterruptible power supplies to ensure continuous operation during power outages.
Provides	Provides the Selected CI	Selected CI has been provided on to this CI	The attribute indicates that the chosen CI offers a specific service, capability or resource to another CI, highlighting a relationship where the selected CI serves as a source of provision for the specified CI. Example: API Provider, provides access to certain functionalities for a software application, allowing the application to interact with those functionalities.
Stored on	Is stored on for the selected CI	Selected CI has been stored on to this CI	Logically stored on another CI, highlighting a relationship where the selected CI is located, hosted or saved on the specified CI. Example: Data storage is stored on a hard drive indicating that the file's data is physically stored on the drive.
Provisioned	Provisioned to the selected user	Selected CI depends on this CI	Allocated or prepared for a specific user, system or entity, highlighting a relationship where the selected CI relies on the provisioning CI for its availability and operation. Example: Resources in cloud, Cloud resources like storage volumes are provisioned by a cloud service provider, allowing users to allocate and manage resources.
Sends data to	Sends data to the selected user	Selected CI sends data to the CI	The chosen CI sends data, information or communication to another CI, highlighting a relationship where the selected CI sends data to the target CI.

			selected CI transmits data to the specified CI. Example: Machine-to-Machine Communication in a production line send production data to a control system, facilitating process monitoring.
Has registered	Has Registered for the selected CI	Selected CI has been registered on this CI	The chosen Configuration Item has been registered or recorded on another CI, highlighting a relationship where the selected CI is associated with or documented on the registering CI. Example: Software License has been registered with a licensing server, enabling the authorized use of the software.
Receives Traffic	Receives traffic for the selected CI	Selected CI received traffic on this CI	This attribute receives incoming data, communication, or activity, usually in the form of network traffic or interactions, from another source or CI. This relationship highlights that the selected CI is a target for incoming traffic. Example: Email Server receives incoming emails from other email servers or clients for distribution to recipients.
Runs On	Runs on by the selected user	Selected CI depends on this CI	The chosen Configuration Item is executed or operated on another CI, highlighting a relationship where the selected CI relies on the specified CI for its functioning or operation. Example: Automation script runs on an automation platform, executing the scripted tasks and workflows.
Receives Data From	Receives from the selected user	Selected CI depends in this CI	This attribute indicates that the chosen Configuration Item receives data, information, or communication from another source or CI, highlighting a relationship where the selected CI depends on the specified CI to provide data or input. Example: IoT Data exchange is a central data hub receives data from multiple IoT devices for storage and analysis.
Submitted by	Is submitted by the selected user	Selected CI depends on this CI	This attribute indicates that the chosen Configuration Item has been submitted or provided by a specific user or entity, highlighting a relationship where the selected CI relies on the submitting CI for its creation, input, or initiation. Example: Change Requests is submitted by a stakeholder initiating a

			formal request for changes to a system or process.
Subscribed by	Is subscribed by the selected user	Selected CI depends on this CI	This attribute indicates that the chosen Configuration Item is subscribed to or followed by a specific user, entity, or system, highlighting a relationship where the selected CI depends on the subscribing CI for updates, notifications, or interactions. Example: Email Subscriptions, an email newsletter is subscribed to by a user, receiving regular updates and content.
Supported by	Is supported by the selected user	Selected CI depends on this CI	The chosen Configuration Item is supported, maintained, or provided assistance by a specific user, team, or entity, highlighting a relationship where the selected CI relies on the supporting CI for its maintenance, troubleshooting, or operational assistance. Example: Helpdesk Services, an IT helpdesk is supported by IT support agents, providing technical assistance to users.
Use End Point From	Use End Point from the selected CI ,	Selected CI depends on this CI	Indication that the chosen Configuration Item utilizes or accesses an endpoint provided by another CI, highlighting a relationship where the selected CI relies on the specified CI's endpoint for its functionality or data exchange. Example: Data Source, a dashboard application uses a data endpoint from a database server to fetch and display real-time data.
Uses	Uses the selected CI	Selected CI has been Used on to this CI	The chosen Configuration Item is utilized, employed, or incorporated by another CI for its functionality, operation, or capabilities. This relationship highlights that the selected CI is a component or resource used by the using CI. Example: Network device, a network switch uses network cables to establish connections.
Virtualizes	Virtualizes the selected CI	Selected CI has been virtualized on to this CI	Indication that the chosen Configuration Item is subjected to virtualization, transforming it into a virtual representation that operates within a virtual environment. This relationship highlights that the selected CI has been virtualized on the specified virtualization platform. Example: Cloud Computing, a cloud provider's infrastructure) virtualizes resources like

		compute, storage, and networking (selected CI) for cloud services.
--	--	-----------------------------------------------------------------------

Contract Management

Contract Management is a dedicated module in Infraon Infinity designed to handle and track all essential contractual agreements. It ensures streamlined organization and visibility into each contract's lifecycle. This module allows users to efficiently store and monitor important details such as start and end dates, renewal terms, obligations, compliance requirements, and associated costs.

With the Contract Management module, organizations can manage various contract types, including:

- **Software Contracts:** Manage licenses and service terms for software.
- **Hardware Contracts:** Oversee terms for physical assets, including warranties and maintenance.
- **Lease Contracts:** Handle lease agreements for equipment and infrastructure.
- **Service Contracts:** Track contracts for outsourced or third-party services.

What do you see on the screen

The Contract Management page provides an organized view of all the contracts stored in the inventory and their associated details. Users can access a pre-configured list of contract categories on the left panel, including **Software**, **Hardware**, **Lease**, and **Service**.

These categories are dynamically displayed based on the types of contracts added to the system.

Note: Users cannot create new contract categories. Only the predefined categories—software, Hardware, Lease, and Service—are available for selection.

The following table outlines the available action icons and their functionality:

Basic Details | Contract Management |

Label	Action	Description
Search	Search for specific contracts by name, type, etc.	Use this feature to locate contracts in the inventory quickly based on specific details.
Filter	Apply filters based on fields and conditions.	The fields include Contract Name, Type, ID, Vendor, Status, Managed By, Approver, Description, Start Date, and End Date.
Grid View	Display the contract data in a grid format.	Provides a structured, row-column view of all contracts for easy comparison.
Card View	Display the contract data in a card-based layout.	Allows users to view contracts as individual cards for a concise summary of key details.

New Contract	Add a new contract to the inventory.	Create new contracts in any predefined categories: Software, Hardware, Lease, or Service.
Edit	Modify details of an existing contract.	Enables users to make changes to already added contracts.
Delete	Remove a contract from the inventory.	Permanently delete the selected contract and its associated details.

The main page also displays essential fields for each contract, ensuring users have quick access to critical information at a glance. These fields include:

- Contract Name
- Contract ID
- Type
- Vendor
- Manufacturer
- Status
- Renewal Status
- Expiry Date

View Contract Details

Clicking on a specific contract opens a detailed pop-up window for privileged users. This window provides a comprehensive view of the contract's key information and associated details. Refer to the table below for more information:

Contract Details | Contract Management |

Label	Action	Description
Top Panel	View-only field, no actions can be performed here.	Displays fundamental contract details such as the contract ID, name, and associated information.
Summary	View-only field, no actions can be performed here.	Showcases detailed contract information, including basic details, software license properties, terms of the contract, and itemized cost details.
License Info	View-only field, no actions can be performed here.	Provides a summary of the license information linked to the contract, ensuring clear visibility of license-specific attributes.
Attachment	Privileged users can upload attachments	It enables privileged users to add files by dragging and dropping or browsing to upload (accepted formats: png, jpeg, jpg, txt, doc, docx, CSV, xls, xlsx, pdf; max size: 20 MB). Attachments are categorized under Default Category, Contract Agreement, Insurance and Bonding, Legal Notices, Payment Terms, and Terms and Conditions.

Activity Log	Can be viewed in grid or card view; includes search functionality	Displays the complete history of all activities performed on the contract since its creation, with advanced search capabilities for ease of navigation.
Recent Activities	View-only field, no actions can be performed here.	Highlights only the most recent actions taken on the contract, providing a quick overview of recent updates.

Add contract

Infraon Infinity platform supports four contract types: **Software**, **Hardware**, **Lease**, and **Service**. Follow the steps below to add a new contract seamlessly:

- Navigate to the '**Add Contract**' button located at the top-right corner of the page.
- Choose the appropriate category for the new contract from the predefined options.

Add Software Contract

Two tabs must be completed when adding a Software Contract: **Contract Properties** and **Item Details**. Below is a detailed breakdown of each section:

Add Software Contract | Contract Properties

Label	Action	Description
Basic Details		
Contract Name*	Add a name for the contract.	Example: Microsoft Office
Vendor*	You can select the associated vendor from the list in the inventory or click Add Vendor to add a new one.	Example: Microsoft Corporation
Manufacturer*	Select the manufacturer from the dropdown list.	Example: Microsoft
Status	Set the status of the contract based on the available options.	Options: Draft, Waiting for Approval, Review. Example: Draft
Managed By	Select the user responsible for managing the contract from the dropdown.	Example: John Doe (IT Asset Manager)
Approver	Select the team responsible for approving the contract.	Example: IT Procurement Team
Visibility Type	Select the visibility type for the contract.	Options: Department, Team, User. Example: Team
Visibility To	Add the specific team, user, or department based on the selected visibility type.	Example: IT Operations Team
Description	Add a description for the contract.	Example: This contract covers enterprise-level Microsoft

		Office licenses for all corporate employees.
Software License Properties		
License Type	Select the type of license from the dropdown list.	Options: Perpetual, Subscription, Free License, Trial License, Volume. Example: Subscription
License Key	Enter the associated license key.	Example: XXXXX-XXXXX-XXXXX-XXXXX
License Based On	Select the licensing model from the dropdown list.	Example: Number of users, device count, or site-based.
Terms of Contract		
Start Date	Select the start date from the calendar.	Example: 01-01-2024
End Date	Select the end date from the calendar.	Example: 31-12-2024
Auto Renew	Toggle ON to enable auto-renewal.	Example: The contract will renew for an additional year upon expiration.
Notify Expiry	Toggle ON to enable notifications for contract expiration.	Example: Notify the IT Procurement Team 30 days before expiry.
Terms and Conditions	Add any terms, conditions, or special notes.	Example: The subscription will be terminated if payment is not received within 30 days of renewal.

Once all details are entered, click '**Next**' to proceed to the next section.

Add Software Contract | Item Details

Label	Actions	Description
Software*	Select the software from the dropdown list or click to add new software.	Example: Microsoft Office Suite, Adobe Photoshop
Billing Cycle*	Select the billing frequency from the dropdown list.	Options: Monthly, Quarterly, Yearly. Example: Yearly
Plan Name*	Add a name for the plan.	Example: Enterprise Subscription Plan
Pricing Model*	Select the pricing model from the dropdown list.	Options: Per Unit, Fixed, One Time. Example: Per Unit
Cost*	Enter the cost for the plan.	Example: \$10,000 annually
Count*	Enter the number of licenses or units included in the plan.	Example: 50 licenses
Comments	Add any relevant comments about the plan.	Example: This plan includes access to all Office apps and 1TB of OneDrive storage per user.

Note: Fields marked with Asterisk (*) are mandatory.

Once all the details have been added, click “**Submit**” to add the software contract to the inventory.

Add Hardware, Lease, and Service Contracts

- Navigate to the ‘Add Contract’ button located at the top-right corner of the page.
- Choose one of the following categories: Hardware, Lease, or Service.
- Fill in the required details as outlined below.

Add Contract | Contract Properties

Label	Action	Description
Basic details		
Contract Name*	Click to add a name to the contract.	Examples are Dell Hardware Warranty for Hardware, Office Space Lease Agreement for Lease, or Annual Maintenance Service Contract.
Vendor*	Select the vendor from the dropdown or click Add Vendor to add a new one.	Examples are Dell Technologies, Real Estate LLC, and ABC Maintenance Services.
Manufacturer*	Select the manufacturer from the dropdown list.	Example: Dell, HP (for Hardware). Leave blank if not applicable for Lease or Service contracts.
Status	Set the status of the contract from the dropdown.	Options: Draft, Waiting for Approval, Review. Example: Draft.
Currency	Select the currency in which the contract is priced.	Example: USD, EUR, INR.
Cost*	Enter the cost associated with the contract.	Example: \$25,000 annually.
Managed By	Select the user responsible for managing the contract.	Example: Jane Doe (Facilities Manager) for Lease or John Smith (IT Manager) for Hardware or Service.
Approver	Select the team responsible for approving the contract.	Example: IT Procurement Team, Facilities Team.
Visibility Type	Select the visibility type for the contract.	Options: Department, Team, User. Example: Department.
Visibility To	Based on the selected visibility type, add the specific team, user, or department.	Example: Finance Department.

Description	Add a description of the contract.	Example: This contract covers hardware replacement for Dell laptops under warranty.
Terms of Contract		
Start Date	Select the start date from the calendar.	Example: 01-01-2024.
End Date	Select the end date from the calendar.	Example: 31-12-2025.
Auto Renew	Toggle ON to enable auto-renewal.	Example: Renew for another term if no cancellation is made before expiry.
Notify Expiry	Toggle ON to enable expiry notifications.	Example: Notify the Facilities Team 15 days before expiry.
Terms & Conditions	Add any terms and conditions or special notes.	Example: The vendor will provide on-site support for faulty hardware during the contract period.

Add Contract | Asset Properties

In this tab, map the relevant asset with the contract. For example, Dell Latitude Laptops can be linked to a hardware contract to ensure accurate asset mapping and management.

Label	Action/ Description
Link Asset	Click Link Asset to select an existing asset from the inventory. Use the search and filter options to find the asset.
Search and Filter	Use the search bar or filters to find the required asset.
Add Asset	Click Add Asset to add a new asset. This page allows you to add both IT Assets and Fixed Assets.

Note: Fields marked with Asterisk (*) are mandatory.

Once all the details have been added, click “**Submit**” to add the contract to the inventory.

NCCM

This enables Network administrators to efficiently manage remote IT networks and IP-enabled security devices from a centralized location.

[Click here](#) to access the detailed network configuration and change management content and manage your network configurations effectively.

Download Job

[Click here](#) to access the detailed Download Job content and manage your network jobs effectively.co

Calendar View

The calendar view summarizes daily activity, including processed successful, failed, completed, and total configurations.

This is a privilege-based feature: The user will be able to access, view, add, edit, delete, execute, and export only if the administrator has given them privileges. This will be defined under roles and privileges.

The calendar view, as the name states, gives a detailed report of the selected parameters. By default, it displays information for the current month. However, arrow keys can be used to navigate to the previous months(s)/year(s).

- Calendar Views display details based on daily NCCM activity.
- Complete Count: Displays the Completed device count enabled for the day's download.
- Total: Displays the total node count added to the NCCM tool (to date).
- Download Success: Displays the count of successful configuration download devices for the day.
- Download Fail: Displays the count of failed configuration download devices for the day.
- New Node: Displays the count of new devices for the day.
- Vulnerable Count: Displays the count of the day's vulnerable devices.
- Left Arrow navigates to the previous month's data.
- Right Arrow navigates to the next month's data.

Note:

- Clicking complete count redirects you to the status of the download job enabled for the day.
- Clicking the Success/Fail count will redirect you to the download result page.
- Clicking vulnerable count redirects to the vulnerable list page.
- Clicking a new node redirects to the newly added device list page.

IMACD

IMACD stands for Install, Move, Add, Change, and Dispose, which provides a structured way to manage organizational changes smoothly. It combines various aspects like system installation, coherent movement, planned inclusions, adaptation, and organized disposal, forming a strong guide for transformation.

It's a well-organized path for handling any shift, from setting up new systems to retiring outdated resources. Following this approach ensures smoother transitions, minimizes disruptions, and streamlines changes within the ever-evolving business landscape.

From setting up new systems to responsibly recycling old ones, the IMACD process breaks down into five distinct stages, each tackling a core element of IT management and resource handling:

Installation

The Installation phase focuses on the deployment and configuration of new IT assets within the target infrastructure. This encompasses provisioning compute nodes, client devices, applications, and network fabric. Meticulous installation guarantees the functional integrity and optimal performance of these components.

It serves as the foundational layer for a highly available and resilient IT ecosystem, where adherence to best practices ensures optimal system operation and efficient resource utilization.

Move

The IMACD Move phase addresses the physical and logical relocation of IT resources. This encompasses the migration of hardware assets to a new site (e.g., office relocation or reconfiguration) and the data and software transfer between servers or cloud environments.

Add

The "Add" phase of IMACD focuses on the planned integrations of new IT components into the existing infrastructure. This involves the strategic onboarding and configuration of various elements, including:

- Software applications: Deployment and integration of new software tools with existing systems, ensuring compatibility and data interoperability.
- Hardware upgrades: Incorporation of enhanced hardware components to augment performance, functionality, or capacity, adhering to technical specifications and compatibility standards.
- Network expansions: Extension of the network infrastructure to accommodate additional devices, locations, or increased bandwidth requirements, following network design principles and security best practices.

Change

The configuration management workflow within IT operations hinges on controlled deployments to modify or update hardware or software configurations. This Change Management phase addresses evolving business needs and issues through controlled modifications. Examples include:

- Network infrastructure modifications: Adjusting routing protocols, firewall rules, or VLAN configurations.
- Software updates: Deploying new versions of operating systems, applications, or firmware.
- Security enhancements: Implementing additional access controls, encryption protocols, or intrusion detection systems.

Decommissioning

The Disposal stage of the IMACD encompasses the planned and secure retirement or removal of hardware and software assets at the end of their useful life. This stage is crucial for asset optimization by effectively reallocating resources and minimizing security vulnerabilities inherent to outdated systems. Additionally, it ensures compliant data disposal and prioritizes the secure handling of sensitive information.

What you see on the screen

Label	Action/ Description
Search	Search for the required IMACD process.
Filter	Filter can be added based on the field (Name, Status, State, Creation Time, Assignee, IMACD ID, Priority, and Process Type) and select the condition from the drop-down box below.
Grid View	Click to view in a tabular format.
Panel View	Click to view the details in the form of a Summary Card.
New Process	Click to add an IMACD process
IMACD	Displays the IMACD ID associated.
Process name	Indicates the process name associated with the IMACD process.
Assignee	Displays the name of the assignee assigned to the respective process.
Process Type	Denotes the type of process instance associated with a particular IMACD.
Status	Displays the current status of the process.
Priority	Indicates the priority of the process; the priority can be low, medium, high, or critical.
Asset Count	Displays the asset count involved in the process.
Actions	
Delete	Click to delete the process.

About IMACD process:

Clicking the IMACD process will display the following information:

[IMACD Details](#) | Fields

Label	Description/ Example
IMACD Details	
Basic Details	
Description	Displays a brief description of the IMACD process.
Status	Indicates the current state of the process. (Ex. New or Waiting for Approval)
Process Type	Shows the type of IMACD process. (Move, Add, etc.)
Priority	Low, Medium, High, and Critical.
Workflow	Indicates the name for the Visual flowchart of processes.
Shipment Details	
Shipping Address	The designated address at which the package is to be retrieved. (Example Branch Office)
Destination Address	The physical address where the physical package should be delivered. (Example Head Office)
Asset Details	
Asset Type	Defined the type of asset whether to be IT or fixed asset.
Asset Category	Category is the first division of assets within the selected asset type. For example, within IT assets, there can be categories like laptops, desktops, etc.
Asset Details	Displays the name of the asset selected.
Comment	Any comment associated with the asset.
Left Panel	
Assignee	Displays the name of the assignee assigned to the respective process.
Gate Pass	Shows the selected gate pass processed by the admin.
Communication	
All	Displays all the communication that happened in between the process.
Email	Displays the email communication.
SMS	Displays the SMS communication.
Comment	Displays the comment made during the process or shipment of the asset.
Mail	Click to add or send a mail during the process.

Add Notes	Click to add notes for better communication.
Attachments	
Default Page	Displays all the attachments (documents) aligned to the process.
Add	
Recent Activities	
Default Page	Provides a real-time overview of all activities, both in progress and completed, within the corresponding IMACD stage.
Search	Click to search for the required communication within the process.

Instructions to add a process

Installation

- In the Infraon platform, navigate to the IMACD module.
- Click on the Add process -> Install, located at the top right corner of the page.
- Enter the respective call-out boxes.

Install IMACD | Fields

Label	Action	Description/Example
Name	Add a necessary name to the process.	Define the process by adding a suitable name. For example, "Adding asset."
Description	Provide a brief description of the add process.	
Priority	Add the required level of priority aligned to the process.	Priority can be chosen from Low, Medium, High, and Critical.
Assignee	Select from the drop-down box.	Name of the user to whom the task is assigned.
Location	Select the location from the drop-down box. Note: If the desired location isn't listed in the dropdown, click "Add" to create a new entry.	Displays the location of the asset.
Add Asset		

Add	Click to add the asset that needs the installation process.	
Asset Type		Defined the type of asset whether to be IT or fixed asset.
Asset Category		Category is the first division of assets within the selected asset type. For example, within IT assets, there can be categories like laptops, desktops, etc.
Asset Details		Displays the asset name of the asset selected.
Comment	Click to add a comment about the asset.	Example: Handle with care.
Save	Click to save the process.	The following details will get saved once clicked.

- Once all the details are filled correctly, click **Save**.
- The following IMACD process will be created successfully.

Move

- In the Infraon platform, navigate to the IMACD module.
- Click on the Add process -> Move, located at the top right corner of the page.
- Enter the respective call-out boxes.

Move IMACD | Fields

Label	Action	Description/Example
Process Name	Add a necessary name to the process.	Define the process by adding a suitable name. For example, "Moving IT team's systems."
Description	Provide a brief description of the movement process.	
Priority	Add the required level of priority aligned to the process.	Priority can be chosen from Low, Medium, High, and Critical.
Assignee	Select from the drop-down box.	Name of the user to whom the task is assigned.
Address Details		

Shipping Address	Select the required address from the drop-down below or click Add to enter a specific address manually.	The designated address at which the package is to be retrieved.
Destination Address	Select the required address from the drop-down below or click Add to enter a specific address manually.	The physical address where the physical package should be delivered.
Add Asset		
Add	Click to add the asset that needs the installation process.	
Asset Type		Defined the type of asset whether to be IT or fixed asset.
Asset Category		Category is the first division of assets within the selected asset type. For example, within IT assets, there can be categories like laptops, desktops, etc.
Asset Details		Displays the asset name of the asset selected.
Comment	Click to add a comment about the asset.	Example: Handle with care.
Save	Click to save the process.	The following details will get saved once clicked.

- Once all the details are filled correctly, click **Save**.
- The following IMACD process will be created successfully.

Addition

- In the Infraon platform, navigate to the IMACD module.
- Click on the Add process -> Add, located at the top right corner of the page.
- Enter the respective call-out boxes.

Install IMACD | Fields

Label	Action	Description/Example
Name	Add a necessary name to the process.	Define the process by adding a suitable name. For example, "Adding asset."

Description	Provide a brief description of the add process.	
Number of Assets	Specify the number of assets to be added (numeric value).	Example: 4,5, etc.
Priority	Add the required level of priority aligned to the process.	Priority can be chosen from Low, Medium, High, and Critical.
Assignee	Select from the drop-down box.	Name of the user to whom the task is assigned.
Location	Select the location from the drop-down box. Note: If the desired location isn't listed in the dropdown, click "Add" to create a new entry.	Displays the location of the asset.
Save	Click to save the process.	The following details will get saved once clicked.

- Once all the details are filled correctly, click **Save**.
- The following IMACD process will be created successfully.

Change

- In the Infraon platform, navigate to the IMACD module.
- Click on the Add process -> Change, located at the top right corner of the page.
- Enter the respective call-out boxes.

Change IMACD| Fields

Label	Action	Description/Example
Process Name	Add a necessary name to the process.	Define the process by adding a suitable name. For example, "Moving IT team's systems."
Description	Provide a brief description of the movement process.	
Priority	Add the required level of priority aligned to the process.	Priority can be chosen from Low, Medium, High, and Critical.
Assignee	Select from the drop-down box.	Name of the user to whom the task is assigned.

Location	Select the location from the drop-down box. Note: If the desired location isn't listed in the dropdown, click "Add" to create a new entry.	Displays the location of the asset.
Add Asset		
Add	Click to add the asset that needs the installation process.	
Asset Type		Defined the type of asset whether to be IT or fixed asset.
Asset Category		Category is the first division of assets within the selected asset type. For example, within IT assets, there can be categories like laptops, desktops, etc.
Asset Details		Displays the asset name of the asset selected.
Comment	Click to add a comment about the asset.	Example: Handle with care.
Save	Click to save the process.	The following details will get saved once clicked.

- Once all the details are filled correctly, click **Save**.
- The following IMACD process will be created successfully.

Destroy

- In the Infraon platform, navigate to the IMACD module.
- Click on the Add process -> Destroy, located at the top right corner of the page.
- Enter the respective call-out boxes.

Change IMACD| Fields

Label	Action	Description/Example
Process Name	Add a necessary name to the process.	Define the process by adding a suitable name. For example, "Moving IT team's systems."
Description	Provide a brief description of the movement process.	

Priority	Add the required level of priority aligned to the process.	Priority can be chosen from Low, Medium, High, and Critical.
Assignee	Select from the drop-down box.	Name of the user to whom the task is assigned.
Location	Select the location from the drop-down box. Note: If the desired location isn't listed in the dropdown, click "Add" to create a new entry.	Displays the location of the asset.
Add Asset		
Add	Click to add the asset that needs the installation process.	
Asset Type		Defined the type of asset whether to be IT or fixed asset.
Asset Category		Category is the first division of assets within the selected asset type. For example, within IT assets, there can be categories like laptops, desktops, etc.
Asset Details		Displays the asset name of the asset selected.
Comment	Click to add a comment about the asset.	Example: Handle with care.
Save	Click to save the process.	The following details will get saved once clicked.

- Once all the details are filled correctly, click **Save**.
- The following IMACD process will be created successfully.

Gate pass

It is used to move important IT equipment or valuable assets across different locations within the organization. A gate pass becomes the essential tool for streamlined and secure movement. Essentially, it acts as an authorization document granting permission for specific assets to leave and enter designated areas. This ensures transparent and accountable transfer, whether the asset is shipped between offices or handing over fixed assets within a department.

For added convenience and security, gate passes usually come equipped with either a barcode or a QR code. This allows for quick and easy scanning at checkpoints, further enhancing control and record-keeping.

It typically includes information like:

- Date and time of issuance: To track authorized movement within a specific timeframe.
- Description of goods: Details about the items being moved, like quantity, type, and serial numbers.
- Recipient and origin: Identifying who receives the goods and where the asset came from.
- Admin's signature: Authorizing the movement by designated personnel.

Instructions to add a Gate Pass

Follow the below steps to construct the gate pass of the respective asset for the IMACD process:

- Clicking on the IMACD process ID.
- Navigate to the 'Add Template' located in the right panel of the page in the Gate Pass section.
- Enter the below details:

Gate Pass| Fields

Label	Description/ Example
Template Name	Enter a custom name for this gate pass template.
Transporter Name	Enter the transporter name for the assigned shipment.
Transporter	Add the transporter details.
Bundle ID	Add the unique identifier assigned to the respective asset.
Shipment ID	Add the Shipment ID associated with the assigned process.
Due On	Set the date this gate pass will no longer be valid.
Issue Date	Add the date when the gate pass will be issued.
Phone Number	Enter the phone numbers of the respective assignee.

- Select the type of scanning required, either barcode or QR code.
- Once all the details are entered correctly, click on the Save option.

Note: Click on the [Add Custom Field](#) to personalize your pass with additional information beyond the standard categories. This can help ensure smoother gate procedures and improve record-keeping.

Tickets

Ticket Management

Infraon's ticket Management module enables users/organizations to achieve their goals through the following steps:

- **Ticket Detection and Recording** - This is the first step of ticket management which involves an end-user who identifies an interruption and decides to record it by submitting a ticket. Tickets can be submitted by
 - logging it directly on the portal
 - sending an email to the service desk mail address
 - calling the service desk helpline number
 - using Infraon mobile app (future release)
- **Classification & Categorization** - Though tickets can be identified and recorded by anyone (agents/technicians/end users), it is the responsibility of the service desk agent to classify and categorize them appropriately. tickets are usually given a category and sub-category.
- **Initial support** - Once identified, based on the simplicity of the issue reported, the service desk technicians can offer initial support to the requester.
- **Investigation & Diagnosis** - Next, the service/help desk agent moves on to troubleshoot the issue reported by investigating it further and coming up with a diagnosis. It is not about finding the root cause and fixing it with tickets. Tickets are about resuming services ASAP, which means finding workarounds, temporary fixes, etc.
- **Escalation & Notification** - When a ticket requires additional or advanced support, support/help desk agents escalate them to the next level of support (L2/L3) or field engineers while keeping the requester and technicians informed of the proceedings.
- **Resolution & Recovery** - Resolution being a workaround/temporary fix/software patch is applied and confirmed that the service is recovered/restored.
- **Ticket closure** - Though the service desk technician adds a resolution and marks recovery, a ticket is considered closed only when the requester agrees on the resolution given.
- **Auto Closure for tickets:** The system configuration will automatically close the ticket after the specified days. Requests can be applied similarly, making managing and completing large requests easy.

Apart from these, Infraon also covers ticket ownership, monitoring, tracking, and communication - throughout the life cycle of each ticket.

Tickets are managed through tickets. Tickets can be raised by service desk agents or end-users referred to as requesters. Tickets follow multiple state(s) and status(es) through the life cycle of a ticket.

Ticket Logging: State **Open**, Status **New**

Ticket Categorization: Status [Assign](#) - Categorize Service Category, Service, Impact, Urgency, Priority, Source

Ticket Diagnosis: State [In progress](#), Status [Analysis](#)

Escalation Functional: State [In progress](#), Status [Escalated](#)

Escalation Hierarchical: Runs in the back end (Automatically)

Resolution: State [Resolved](#), Status Waiting for closure (Provide Resolution)

Closure: State [Closed](#), Status [Completed](#) (Update closure Category, Closure Note)

State and Status

The status of a ticket is based on the state of the ticket.

State	Status	Status Scenario
Open	New	When a ticket is newly reported.
In Progress	Analysis	When the ticket is in progress, and the technician is performing an analysis of the ticket detail.
In Progress	Escalated	When the ticket is in progress and is being escalated due to missing or incomplete information.
On-Hold	Pending	The status can only be 'Pending' when the ticket is kept on hold.
Resolved	Accepted	When the ticket is resolved, and the Customer accepts the solution. Once the customer marks it as accepted, the ticket will be automatically redirected to Formal closure of the ticket with the State marked as Closed.
Resolved	Rejected	When the customer does not accept the solution, it is marked as Rejected, automatically resulting in Reopen of the ticket.
Resolved	Resolved by Event	When the ticket is automatically closed by an external event.
Resolved	Resolved by Origin ticket	When the ticket is closed by primary/parent ticket
Resolved	Waiting for Closure	Information is to be updated when the ticket is resolved and is waiting for closure.

Customized Status(es) can be configured from the 'Workflow' module to suit the requirement.

Easily convert resolved tickets to Knowledge Base articles. KB icon appears post-resolution, ensuring efficient knowledge management.

Reporting manager's approval: Configure the approval settings and enable the approval toggle button, the system will automatically send an approval email to the reporting manager, including an approval link. It allows for a streamlined approval process and helps ensure that requests are approved or rejected, it is easy to configure and can be done in just a few clicks.

Auto Approval submission: Enable the toggle button and the approval link is sent to accept or reject the ticket from the email. This feature streamlines the approval process and saves time for both the requester and the approval team.

SLA Status Indication in Tickets and SLA widgets: Visualize the SLA profile with the metric name on the panel view page, configure the SLA profile, map one or multiple metrics, and check the status of an SLA profile. The system manifests whether the SLA is achieved, breached, or canceled. Easily monitor and manage SLAs to ensure timely resolution of issues. Includes a response time count that shows the number of SLAs and corresponding profiles and metrics and indicates the number of SLAs that have been achieved or breached. This compliance-based feature provides a quick and easy way to monitor the service level agreements. With this information, you can proactively resolve any issues impacting SLAs and improve service delivery.

Workspace Incident Action: Allowing users to track the assigned tickets conveniently. Discover Incident actions, a dynamic set of features accessible via mouse hover, providing quick access to recent activity, interactions, attachments, and more for streamlined ticket handling.

Complete and Resolve button for simplifying ticket resolution in a single click. Moreover, the flexibility of Incident Card Inline Edit, enables hassle-free updates to assignees and ticket details.

Auto closure: The system configuration will automatically close the ticket after the specified days. Requests can be applied similarly, simplifying the managing and completion of large requests.

Request summary based on ticket count: Quick overview of the ticket status, open, on hold or closed. Identify the frequent issues raised multiple times, delete them using the widgets, and address them quickly. The summary is sorted based on ticket count, making it easier to identify high-volume requesters. Reduces the overall resolution time for tickets.

Re-Open: The ticket can be requested to be re-opened by the user/requester unsatisfied with the resolution. This can be done only when the Status of the ticket is marked as 'Waiting for Closure.' If the ticket is marked as 'Closed,' a new ticket must be raised.

Demo data for ITSM module Ticket for new Org

Knowledge Base Modules! Explore added knowledge articles to understand the functionality and purpose of KB modules.

This new ticket can be linked to the parent ticket.

Tickets

A Ticket can be defined as an unplanned interruption to an IT service, reduction in the quality of an IT service, or failure of an asset/Item that has not yet impacted service. Ticket Management is the process responsible for managing the life cycle of tickets. The goal of ticket Management is to restore standard service as quickly as possible with minimal to no disruption to the business. This ensures that the highest achievable levels of availability and service are maintained.

How does it work?

Tickets can be created by end-users/requesters through the [web portal](#) or [mobile app access](#), via [email](#), or by a technician on call. When tickets are created from email, the message's subject line becomes the summary of the ticket, the message body becomes the description, and the source field is set to Email.

The quick action panel helps technicians resolve tickets in no time. This reduces ticket resolution time by 80%.

What you see on the screen

The tickets page lists all tickets with details like summary card, impact service, status, subject, team, requester name, and actions, sorted by time. Refer to the 'Working on a Ticket' section for detailed information.

Working on a ticket

The service desk is the core of Ticket Management. Though there are multiple ways to record a ticket, the Ticket's working or resolution is in the hands of Technicians.

Before working on the Ticket, it is necessary to understand the life cycle of Tickets and the key components within Infraon's Ticket module.

Components

- [Ticket Summary Card](#) - The ticket summary card briefly summarizes the ticket. This summary contains all the important information needed to work on the ticket. Details include:
- [Ticket ID](#) – Auto-generated when a ticket is created. Click on the ticket ID to view the communication history, reply to and forward emails, add notes, analyze, add symptoms and root causes, and view and add work logs. You can resolve a ticket from this screen too.
- [Ticket Source](#) – This shows how the ticket was submitted.
- [Priority](#) – The priority of the ticket (derived from the asset)
- [Asset ID](#) - Asset for which the ticket is raised. Click on the asset ID to view detailed asset information.
- [Comment](#) – The requester or technician's comment on the ticket
- [Analyze](#) – Used to view details of the ticket
- [Requester Icon](#) – Displays the name of the requester (initial)

- **Subject** – Subject of the ticket (derived from the ticket subject line)

Communication

The Communication tab acts as your central hub for all ticket interactions. Clicking on it opens a dedicated window displaying the complete communication history, including emails, SMS messages, and any comments added throughout the ticket lifecycle.

This streamlines resolution by allowing technicians to quickly access all relevant information, keeping everyone informed—assignee, team, and requester.

The tab also empowers technicians to send emails and SMS messages directly to the end-user without leaving the window.

For added convenience, Infraon Infinity features a dynamic section with a requester dropdown, eliminating the need for manual entry. Furthermore, both technicians and end-users can attach files and add signatures for enhanced clarity and authenticity.

Text enhancement - Effortlessly refine your communication in tickets. Receive real-time prompts for improved text, with options for tone and style adjustments. Elevate your message with professional, conversational, emphatic, or simple tones. Explore the proofread, rephrase, and content expansion tools, all in one seamless interface!

The summary card details can be configured to suit requirements. Use click on the configure icon to customize the summary card.

Working on a ticket

The service desk is the core of Ticket Management. Though there are multiple ways to record a ticket, the Ticket's working or resolution is in the hands of Technicians.

Before working on the Ticket, it is necessary to understand the life cycle of Tickets and the key components within Infraon's Ticket module.

The Right Panel

- **Impact Service:** To select the service that has been impacted
- **Status:** Displays the current status of the Ticket. Technicians can change the status from here too
- **Subject:** Subject of the Ticket

- **Team:** The team assigned to work on the Ticket
- **Requester Name:** Name of the requester
- **Actions:** Quick action icon to work on the Ticket

Note: The quick action bar appears as a floater on each Ticket line.

The Ticket summary card and the quick action floater help to cut the technician's resolution time by 80%.

Ticket Quick Actions

- **Resolve:** Click to resolve the Ticket. The resolution date and time are recorded automatically. The technician is required to change the status and add a resolution to **resolve** the Ticket.
- **Ticket aging for helpdesk/ ITSM close and resolve conditions:** Grid View includes Aging Metric. Track ticket resolution time accurately. Click 'Resolve' or 'Close' to stop the aging clock. Get detailed aging reports based on resolved status.
- **Assign To:** Click to assign the Ticket. Tickets can be assigned to a user individually or a user from a specific team, expertise, or level.
- **Quick Edit:** To perform quick edit actions like status, priority, urgency, severity, impact, impact service, and the Ticket assignee. *Use the 'Detailed Edit' button to edit the Ticket details.*
- **Edit:** To edit the Ticket in detail.
- **Delete:** To delete the Ticket. This action cannot be reverted.
- **Additional Actions:** Use the additional action button to view the ticket history and to convert the Ticket to a Knowledge Base. Use the 'Edit Options' icons to customize the additional action options. You can select up to four actions.

Ticket Grid Page Actions

Apart from these, the Ticket page has:

- **Expand icon** to view Ticket filters.
- **Search bar** to help search for a specific Ticket using the Ticket number, assignee, etc.

- [Calendar](#) to filter the Tickets by a specific day, date, or date range.
- [Convert Ticket to Request](#) - If the technician feels that the ticket is more of a Request, then the ticket can be converted into a Request.
- [Convert Ticket to KB](#) - Option to convert the ticket into a Knowledge Base (KB). This action is possible only if the status of the ticket is "Resolved" or "Closed".
- [Add Change](#) - A ticket resolution may be implemented through a change. A Change Request can be added to this ticket. This action is possible only if the status of the ticket is 'Open', 'In Progress', or 'On Hold'.
- [View Change](#) - If a change request has been created for a ticket, then this option is visible. This can be clicked to view the related change request.
- [Tag](#) - Select A ticket to view the tag option. Tagging is a way to group Tickets.
- [Merge](#) - Select more than two Tickets to view the merge option.
- [Pause the icon](#) to pause the auto-reload.
- [Configure the icon](#) to configure the summary card and column selection

Icons to toggle between list and smart grid view.

Ticket panel view actions

Enhance ticket management with the ability to modify ticket details, track SLA status, and streamline communication effortlessly. Experience efficient incident, request, and problem handling with the integrated panel view.

The revamp of the panel view for tickets. The improved interface offers enhanced data visibility, with aging metrics conveniently displayed. This helps in faster navigation and reduced system load for a seamless user experience.

Add ticket

Tickets can be created by end-users/requesters through the [web portal](#) or [mobile app access](#), via [email](#), or by a technician on a call with the customer. When tickets are created from email, the message's subject line becomes the summary of the ticket, the message body becomes the description, and the source field is set to Email.

Tickets may also be created by network monitoring systems configured to send problem reports to the system through one of the standard APIs. In the Event Management module, you can configure the event types that result in a ticket and the event resolutions that result in the ticket's closure. Refer to the events section for more details.

Pre-requisites

To add a ticket, the below must be pre-configured

- Requester - the user requesting the service (the user impacted by the ticket)
- Priority - priority of the ticket
- Impact Service - Service impacted by the ticket
- Service Classification, if required.
- Assignee - usually the technician assigned to the ticket. Use the 'Take it' option to self-assign.
- Followers - users who are notified of the changes in the ticket. Use the 'Follow' button to follow directly.
- Tags - ticket groupings used for classification
- Process visibility - Enhancement of process visibility for service details that enable or disable the process based on the services. Not required process visibility in a service, like a ticket, request, change, problem or release process, can be disabled. The process visibility feature provides control and flexibility to manage the services leading to a better outcome.

Add a ticket

- Go to the ticket page
- Click on the 'New ticket' button.

If requesters are added already, use the search option to add the requester's name. Use the 'Add a New Requester' button if no requesters have been added.

Follow the 'Requester' module for details. You can select or add a requester from the next page too.

To add A ticket, follow the steps from the below table:

Label	Action	Description/Example
Requester*	Add a new requester or search for an existing requesting requester.	Requesters are usually users requesting the service.
Ticket URL	Easily tracks the progress of requests.	Receive a ticket URL in the acknowledgment email request and visit the self-service portal to view the ticket status and any updates.
Reported by	Use the icon to expand this section. Add the reporter's name and email address, if applicable.	Reporters are users reporting the service on behalf of the requester.
Priority	Select the priority of the ticket using the dropdown menu.	Priority can be medium, high, or critical, based on the ticket's impact.
Impact Service	Select the impacted service.	If the requester's name is not selected, the impact service field will be blank. Services can be made available to selected users, to suit the organizational needs.
Service Classification	Select the classification within the impacted service	This is used when a specific service has multiple classifications. For example, if the impacted service is email, the classifications can be connectivity, email configuration, and so on. Leave this field blank if no classifications are defined.
Assignee	Select a technician to assign the ticket.	Use the 'Take it' option to self-assign it.
Email Notification	Track the Email	Email notifies the assignee about the ticket creation, our feature allows you to track whether the assignee has read the email. The pop-up notification will be

		automatically closed when the assignee reads the email.
Followers	Select a user to add them as followers.	Users who must be notified of the ticket or any changes to the ticket can be added as followers. Use the 'Follow' option to self-follow the ticket.
Tags	Select a tag to tag the ticket.	Ticket tags must be predefined in the 'General Settings -> Tag Management module.
Subject	Add a subject line for the ticket.	The subject line can be a short summary of the ticket. For example, Unable to sync email, Keyboard not working, etc.
Communication/Internal Note	Use the dropdown to select if the content is a part of the communication or an internal note for the technician.	If communication is selected, add the email address in the given textbox.
Message	Add the ticket description or the note to your team member in detail.	
Add Attachment	Use the action icon to add an attachment to the ticket.	Attachments can include emails, screenshots, etc.
Add signature	Customize the signature	Customize signature to tickets, requests, concerns, transitions, and releases. Customize the new signature by copying and pasting any desired images or text or simply typing on a given space. Option to create multiple signatures and choose the one that meets the requirements.
IMAP and SMTP	Choose the IMAP from the drop-down	Simplified email communication with IMAP integration. Create a ticket, choose the IMAP option in the communication dropdown, and provide a subject. Once the ticket is created, easily reply to emails directly from the

		IMAP mailbox associated with the ticket, ensuring seamless and convenient communication.
--	--	------------------------------------------------------------------------------------------

Additional Notes:

When the requester's name is added, Infraon displays the list of interactions the requester has had in the past. Click on the ticket ID to view ticket details.

When A ticket title is added, Infraon displays related Knowledge Base articles. If a related resolution is available, the technician can add the same as the [ticket Resolution](#) and close the ticket directly.

Once all details are added, the user can choose to either save it as

- Submit as New - the ticket is saved as a new ticket (new occurring)
- Submit as Pending - the ticket is saved as pending
- Submit as Resolved - the ticket is saved in 'resolved' status.

Self-Service for Requester

Once a requester has been given access, they will be able to access the requester's portal, raise tickets, change requests, follow up, and communicate about other tickets/requests. Read more about it at the [requester Portal Help](#).

Request Management

A Service Request is a formal request raised by a user for information, support, access to IT, or something new to be provided. In Infraon, service requests are called "Request." Request Management is the process responsible for managing the life cycle of requests. Request Management aims to support the agreed quality of service by handling all pre-defined, user-initiated requests in an effective and user-friendly manner.

Infraon's Request Management module enables users/organizations to achieve their goals through the following steps:

- [Request Recording](#) - This is the first step of request management. A user identifies the need for a service and raises a formal request for it through the request management portal. Requests can be raised through the following channels:
 - logging a request through the portal
 - sending an email to the service desk mail address

- calling the service desk helpline number
- **Classification & Organization**- Though requests can be identified and recorded by anyone (agents/technicians/end users), it is the responsibility of the service desk agent to classify and organize them appropriately. Requests have a type and classification.
- **Initial support**- Once identified, based on the simplicity of the service requested, the service desk technicians can offer initial support to the requester.
- **Escalation** - If an agent feels that the request is more of a ticket and impacts a service, he can convert the request into a ticket and assign it to the appropriate team.
- **Resolution** - Resolution is providing the information requested by the requester, new hardware provided to the requester, and so on.
- **Closure**- The service desk technician adds a note and marks the request as Resolved. A request is considered closed only when the requester agrees on the resolution given.

Request Transfer state

Apart from these, Infraon also covers request ownership, monitoring, tracking, and communication - throughout the life cycle of each request. Requests are managed through the "Request" module. Requests can be raised by service desk agents or end-users referred to as requesters. Requests follow multiple state(s) and status(es) through their life cycle.

Request Logging: State [Open](#), Status [New](#)

Request Categorization: Status [Assign](#)- Categorize Request Type, Service Classification, Priority, Followers, Tags

Request Diagnosis: State [In progress](#), Status [Analysis](#)

Escalation Functional: State [In progress](#), Status [Escalated](#)

Resolution: State [Resolved](#), Status [Waiting for closure](#) (Provide Resolution)

Closure: State [Closed](#), Status [Completed](#)(Update closure Category, Closure Note)

State and Status

The status of a request is based on the state of the request.

State	Status	Status Scenario
Open	New	When a request is newly logged.

In Progress	Analysis	When the request is in progress, and the technician is performing an analysis of the request.
In Progress	Escalated	When the request is in progress and is being escalated due to missing or incomplete information.
On-Hold	Pending for User Input	The status can only be "Pending" when the request is kept on hold while waiting for user input.
Resolved	Accepted	When the request is resolved, and the customer accepts the solution. Once the customer marks it as accepted, the request will be automatically redirected to Formal closure with the State marked as Closed.
Resolved	Resolved by Event	When the request is automatically closed by an external event.
Resolved	Waiting for Closure	Information is to be updated when the request is resolved and is waiting for closure.

Customized Status(es) can be configured from the "Workflow" module to suit the requirement.

Easily convert resolved Request to Knowledge Base articles. KB icon appears post-resolution, ensuring efficient knowledge management.

Request

A Request is a formal request raised by a user for information, support, access to IT, or something new to be provided. The module that handles the Requests in Infraon is called Request Management. Request Management aims to support the agreed quality of service by handling all pre-defined, user-initiated service requests in an effective and user-friendly manner.

How does it work?

Requests can be created by end-users/requesters through the web portal, [mobile app](#), [email](#), by a technician on call, [WhatsApp](#), or [chatbot](#). When requests are created from email, the message's subject line becomes the summary of the service request, the message body becomes the description, and the request source is set to "email".

When requests are created from email, the message's subject line becomes the summary of the request, the message body becomes the description, and the source field is set to email.

What do you see on the screen?

The "Request" page lists all requests with two views: Panel View and Grid View. The page lists all requests with details like summary card, request, status, subject, team, requester name, and actions, sorted by time.

Working on a Request

The service desk is the core of Request Management. Though there are multiple ways to record a request, the resolution of the Request is in the hands of Technicians.

Before working on the Request, it is necessary to understand the life cycle of Requests and the key components within Infraon's Request module.

Request Views

There are two ways to view request details in the right panel. They are:

Panel View - In the Panel view, you see request details in the form of a Request Summary Card. The request summary card gives a brief summary of the request. This summary contains all the important information needed to work on the request. Details include:

- **Request ID**: Auto-generated when a request is created.
- **Requester**: Name of the requester
- **Team**: The team assigned to work on the request
- **Status**: Displays the current status of the request. Technicians can change the status from here too.
- **Priority**: Displays the priority of the request. Technicians can change the priority of the request.
- **Service**: The area in which service is requested
- **Resolve**: The technicians have the option to resolve the request from this panel.
- **Actions**: Quick action icons to work on the request

The revamp of the panel view for tickets. The improved interface offers enhanced data visibility, with aging metrics conveniently displayed. This helps in faster navigation and reduced system load for a seamless user experience.

Grid View - In Grid view, you see request details in tabular form. Clicking on the Request ID shows the details of the request.

- **Request ID**: Auto-generated when a request is created. Click on the request ID to view the communication history, reply to and forward emails, add notes, analyze, and view and add work logs. You can resolve a request from this screen too.
- **Request Source**: This shows how the request was submitted.
- **Priority**: The priority of the request
- **Analyze**: Used to view details of the request
- **Requester**: Displays the name of the requester (initial)
- **Subject**: Subject of the request (derived from the request subject line)
- **Team**: The team to which the request is assigned

- **Assignee:** The person to whom the request is assigned
- **Actions:** Quick action icons to work on the request

Note:

- The quick action bar appears as a floater on each request line and is common in both Panel and Grid views. The quick-action floater aims to cut the resolution time by 80%.
- The summary card details can be configured to suit requirements. Click on the "Configure" icon to customize the details you want to see on the screen.
- Configure icon is available only in Grid View.

Additional Icons

Name	Description
Comment	A user/technician can see the comments on the request and also can add new comments.
History	Shows the history of the current request from the time it was created.
Interaction	Shows the history of the requests created by the requester.
Attachment	Shows all the attachments of the current request.
Request Source	Shows the source of the request, like email, web, etc.
Convert Request to Ticket	Option to convert the request into a ticket. This action is possible only if the status of the request is "Open" or "In Progress".
Convert Request to KB	Option to convert the request into a Knowledge Base (KB). This action is possible only if the status of the request is "Resolved" or "Closed".
Add Change	A request resolution may be implemented through a change. A Change Request can be added to this Request. This action is possible only if the status of the ticket is 'Open', 'In Progress', or 'On Hold'.
View Change	If a change request has been created for a Request, then this option is visible. This can be clicked to view the related change request.

Quick Actions

Name	Description
Quick Edit	To perform quick edit actions like status, priority, urgency, severity, impact service, and the Request assignee. <i>Use the "Detailed Edit" button to edit the Request details.</i>
Edit	To edit the Request in detail.
Delete	To delete the Request. This action is irreversible.
Copy	To copy the details of a request and create a new request.

Request aging for helpdesk/ITSM close and resolve conditions	Grid view includes aging metric. Track Request resolution time accurately. Click 'Resolve' or 'Close' to stop the aging clock. Get detailed aging reports based on resolved status.
---------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Page Actions

The Request page also has the following actions.

Label/ Icon	Description
Expand Icon	To View the Request filters
Search Bar	To help search for a specific Request using the Request number, assignee, etc.
Calendar	To filter the Requests by a specific day, date, or date range
Tag*	Select a request to view the tag option. Tagging is a way to group requests
Merge*	Select more than two requests to view the merge option.
Pause	To pause the auto-reload
Configure	To configure the summary card and column selection

*Select at least one request to enable these options.

To understand the difference between these four types of requests, refer to the table below.

Type of Request	Definition	Example
Service Request	A Service Request is a formal request from a user for information, access to IT, or something new to be provided.	A user needs a new laptop
Tickets	A ticket can be defined as an unplanned interruption to an IT service, reduction in the quality of an IT service, or failure of an asset/Item that has not yet impacted service.	User unable to connect to Outlook
Problem	A problem is an underlying root cause of one or more tickets. Recurring incidents with common issues lead to a problem.	Multiple users unable to connect to Outlook
Change	A change is "the addition, modification, or removal of any authorized, planned, or supported service or service component that could affect IT services.	Release an OS patch to fix the problem of Outlook Connectivity

Add a Request

Requests can be created by end-users/requesters through the [webportal](#), [mobile app](#), [email](#), by a technician on call, [WhatsApp](#), or [chatbot](#). When requests are created from email, the message's subject line becomes the summary of the service request, the message body becomes the description, and the request source is set to "Email".

Pre-requisites:

To add a request, the following must be pre-configured

Requester - the user requesting the service

- Priority - priority of the request
- Service Classification, if required.
- Assignee - usually the technician assigned to the request. Use the "Take it" option to self-assign.
- Followers - users to be notified of the changes in the request. Use the "Follow" button to follow directly.
- Tags - groupings used for the classification of requests

Steps to add a Request

- Go to the "[Request](#)" page
- Click on the "[New Request](#)" button.

If requesters have been added already, use the search option to select the requester's name. Otherwise, use the "Add a New Requester" button if no requesters have been added or to add a new requester. Follow the "Requester" module for details. You can select or add a requester from the next page too.

To add a request, follow the steps from the below table:

Label	Action	Description/Example
Requester*	Add a new requester or search for an existing requester.	Requesters are usually users requesting the service.
Reported by	Use the icon to expand this section. Add the reporter's name and email address, if applicable.	Reporters are users requesting the service on behalf of the requester.
Assignee	Select a technician to assign the request.	Use the "Take it" option to self-assign it.
Request Type	Select the type of request.	This is used when a specific service has

		multiple classifications. Leave this field blank if no classifications are defined.
Service Classification	Select the classification within the "Request For" category	This is used when a request category has multiple sub-categories.
Priority	Select the priority of the request using the drop-down menu.	Based on the request, the priority can be low, medium, high, or critical.
Followers	Select a user to add them as followers.	Users who must be notified of the request or any changes to the request can be added as followers. Use the 'Follow' option to self-follow the request.
Tags	Select a tag to tag the request.	Request tags must be predefined in the 'General Settings -> Tag Management module.
Subject	Add a subject line for the request.	The subject line can be a summary of the request. For example, a Request for a new laptop.
Request For	Use the drop-down to select one of the request categories	
Internal Note	Add description of the service request or a detailed note to your team member.	
Add attachments	Use the action icon to add an attachment to the service request.	Attachments can include emails, screenshots, etc.

Additional Notes:

- When the requester's name is added, Infraon displays the list of interactions the requester has had in the past. Click on the Request ID to view the request details.
- When a request title is added, Infraon displays related Knowledge Base articles. If a related resolution is available, the technician can add the same as the [request resolution](#) and close the request directly.

Once all details are added, the user must click "[Submit as New](#)" - to submit the request.

Problem Management

A problem is an underlying root cause of one or more tickets. Recurring incidents with common issues lead to a problem. *A problem can be linked to tickets(reported for the same underlying issue), a request, or a change(part of a future release). Problem Management is the process responsible for managing the lifecycle of the problem from its creation till its closure. Problem Management aims to provide solutions or workarounds to problems so that there is minimum impact on the organization. Problem Management also seeks to prevent a problem from reoccurring.

Problem

A problem is an underlying root cause of one or more tickets. Recurring tickets with common issues lead to a problem. In other words, for anything that requires a root cause analysis, there is a need to log a problem. The outcome of a problem can be a solution, a change, or a service request.

How does it work?

Only a technician or users with the required permissions can log a Problem. While adding a problem in the Problem module, a technician records the source of the problem. The source can be one of the following:

- Web portal
- Mobile app
- Email
- By a technician on call

Streamlined problem-to-ticket association. Create a problem, log a ticket from the problem view page, add internal notes and submit to establish the relationship. Click on the ticket ID and the ticket opens in a new page for seamless navigation and management.

Benefits of Problem Management

Efficient Problem Management can have several benefits for an organization. It can also add substantial value to a business. Some of the benefits of Problem Management are:

- Increase in Service Availability
- Increase in Productivity
- Customer Satisfaction
- Decrease in the number of tickets

- Cost Saving

Problem Management Process

Infraon's Problem Management module enables organizations to achieve their goals through the following steps:

- Problem Detection - This is the first step of Problem Management. A problem can be detected in two ways.
 - Suppose different requesters raise multiple tickets for the same issue. Then it means there is an underlying issue that needs to be further analyzed. Then a problem is recorded.
 - If a completely new issue arises with an unknown underlying cause, then a problem is recorded.
- **Problem Recording** - Only a technician or users with the required permissions can log a Problem in the module.
- **Classification & Prioritization** - It is essential to capture all the details of the problem, such as problem type and description. A problem has a category and sub-category. Capturing and classifying the details makes it easier to assign & monitor the problem.
- **Investigation & Diagnosis** - Problem Management is about finding an issue's root cause. A detailed Root Cause Analysis(RCA) is performed based on the urgency and severity of the problem. Multiple analyses can be added until the root cause is identified. The various methods used for analysis are:
 - 5-Whys
 - Chronological
 - Kepner Tregoe
- **Create a Known Error Record** - In ITIL, a Known Error is "a problem with a documented root cause and a workaround." It is essential to record this information into a Known Error Database (KEDB) so that if this issue or problem arises in the future, the service desk technician can quickly look into the KEDB and provide a quick resolution or associated workaround. This leads to less downtime.
- **Create a workaround, if necessary** - A workaround is a temporary solution to a problem so that it can reduce the impact on a business. A workaround for a problem can be created and documented in the KEDB.
- **Escalation & Notification** - A technician escalates the problem to L2/L3 level technicians or engineers when a problem requires more significant expertise. The technicians are kept well-informed of these proceedings through notification emails.

- **Resolution** - A resolution is a permanent fix for a problem such that it can no longer cause another ticket.
- **Review & Closure** - A review is performed to check the effectiveness of the resolution. Once the technicians are satisfied with the resolution, the problem can be closed.

Problem Management and relation with other processes

Process	Relation with Problem Management
<u>Ticket Management</u>	<p>Different requesters raising multiple tickets for the same issue denotes an underlying issue that needs to be further analyzed.</p> <p>A new issue is raised with an unknown underlying cause</p> <p>In the above cases, a problem is logged. These tickets can be linked to the problem. The tickets are put on hold until a workaround/solution is provided.</p>
<u>*Request Management</u>	<p>A service request raised by a user to install new software in the laptop may have disrupted/corrupted other software.</p> <p>Implementing a resolution to a problem may require a user to raise a service request to install a software patch.</p> <p>In the above cases, the service requests can be linked to the problem.</p>
<u>*Change Management</u>	<p>Sometimes, a change may disrupt service. This leads to logging a ticket and, subsequently, a problem in analyzing the cause.</p> <p>Problem Management may initiate resolution through a change request. The approval/implementation of the change is beyond the scope of Problem Management. This needs to be done in Change Management.</p> <p>In this case, a change request is linked to the problem.</p>

*Knowledge Management	<p>Important information regarding workarounds, resolutions and Known Errors (KE) is often the output of Problem Management.</p> <p>Similarly, information and documents available in Knowledge Base(KB) can serve as a beginning point to diagnose and investigate a problem. In these cases, Knowledge Management comes into the picture. KBs can be attached to the problem, or a resolution or Known Error information can be turned into a Knowledge Base article.</p>
------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

*These linking options will be part of the future release.

Infraon also covers problem ownership, monitoring, tracking, and communication - throughout the life cycle of each problem.

Problems are managed through the "Problem" module. Problems can be raised by technicians or users with the required permissions referred to as requesters. Problems follow multiple state(s) and status(es) through their life cycle.

State and Status

State	Status	Status Scenario
Open	New	When a new problem is logged in the system. The status of the associated tickets is put "On-Hold."
Open	Waiting for Assignee	When a problem is newly created, it is next waiting to be assigned to a technician.
In Progress	Investigation	When the Root-Cause Analysis of the problem is in progress.
In Progress	Diagnosis	When the problem analysis is in progress and misses the "Due By" date. Then it is escalated to the next technician.
On-Hold	Waiting for Customer	The status can only be 'Pending' when the problem is kept on hold either for Customer input.
On-Hold	Pending Changes	If any changes are pending to be implemented.
Resolved	Resolution Applied	When a resolution(permanent fix) is applied to the problem. The users are notified.
Resolved	Solved	When the users are satisfied with the resolution provided by the technicians.

Customized Status(es) can be configured from the 'Workflow' module to suit the requirement.

Easily convert resolved Problem to Knowledge Base articles. KB icon appears post-resolution, ensuring efficient knowledge management.

Demo data for ITSM module Problem KB for new Org

Knowledge Base Modules! Explore added knowledge articles to understand the functionality and purpose of KB modules.

Problem

A problem is an underlying root cause of one or more tickets. Recurring tickets with common issues lead to a problem. In other words, for anything that requires a root cause analysis, there is a need to log a problem. The outcome of a problem can be a solution, a change, or a service request.

Problem Management is the process responsible for managing the lifecycle of the problem from its creation till its closure. Problem Management aims to provide solutions or workarounds to problems so that there is minimum impact on the organization. Problem Management also seeks to prevent a problem from reoccurring.

How does it work?

Only a technician or users with the required permissions can log a Problem. While adding a problem in the Problem module, a technician records the source of the problem. The source can be one of the following:

- Web portal
- Mobile app
- Email
- By a technician on call
- WhatsApp
- Chatbot

What do you see on the screen?

The "Problem" page lists all problems with two views: Panel View and Grid View. The page lists all problems with details like summary card, problem description, status, subject, team, requester name, and actions, sorted by time.

Add Problem

Only a technician or users with the required permissions can log a Problem. While adding a problem in the Problem module, a technician records the source of the problem. The source can be one of the following:

- Web portal
- Mobile app
- Email
- By a technician on call
- WhatsApp
- Chatbot

Pre-requisites:

To add a problem, the following must be pre-configured

- Requester - the user logging the problem
- Priority - priority of the problem
- Problem Classification, if required.
- Assignee - usually the technician assigned to the problem. Use the "Take it" option to self-assign.
- Followers - users to be notified of the changes in the problem status. Use the "Follow" button to follow directly.
- Tags - groupings used for the classification of problems.

Steps to add a Problem

- Go to the "Problem" page
- Click on the "New Problem" button.

If requesters are already added, select the requester's name in the search option. If no requesters have been added or to add a new requester, use the "Add a New Requester" button. Follow the "Requester" module for details. You can select or add a requester from the next page too.

To add a problem, follow the steps from the below table:

Label	Action	Description/Example
Requester*	Add a new requester or search for an existing requester.	Requesters are usually technicians or users with the required permissions who can add a problem.
Reported by	Use the icon to expand this section. Add the reporter's name and email address, if applicable.	Reporters are users raising the problem on behalf of the requester.
Assignee	Select a technician to assign the problem.	Use the "Take it" option to self-assign it.

Impact Service	Select the impacted service if already known.	This can be left blank. As the root cause analysis progresses, a technician can later select the impacted service.
Problem Classification	Select the classification within the impacted service.	This is used when a specific service has multiple classifications. For example, if the impacted service is Network, the classifications can be connectivity, router issue, and so on. Leave this field blank if no classifications are defined.
*Priority	Select the priority of the problem using the drop-down menu.	Based on the problem, the priority can be low, medium, high, or critical.
Followers	Select a user to add them as followers.	Users who must be notified of the problem or any changes to the problem can be added as followers. Use the 'Follow' option to self-follow the problem.
Tags	Select a tag to tag the problem.	Problem tags must be predefined in the 'General Settings -> Tag Management module.
Subject	Add a subject line for the problem.	The subject line can be a summary of the problem. For example: Unable to connect to the network.
Known Error	When this is selected, the problem details get saved in the Known Error Database(KEDB).	The details get stored in the Known Error Database(KEDB) which can be published in Knowledge Base articles. The articles will have visibility control.
Problem Source	It specifies the method through which the tickets were raised.	A technician records the source of the problem based on the associated tickets.
*Due By	It is the due date by which a technician aims to resolve the problem.	A technician does a detailed root cause analysis and tries to resolve the problem by this date. If he is not able

		to resolve the problem, he will at least try to provide a workaround by this date.
Symptom of Fault	Describe the symptoms of the issues in detail.	
Add attachments	Use the action icon to add an attachment to the problem.	Attachments can include emails, screenshots, etc.
Internal Note	This is a note shared by technicians internally.	

*Priority is derived from the asset. It can also be changed later using the "Quick Edit/Edit" options.

*Due by - Only a manager has the privilege to extend the due date.

Additional Notes:

- When the requester's name is added, Infraon displays the list of past interactions the requester has had. Click on the Problem ID to view the details.
- When a problem title is added, Infraon displays related Knowledge Base articles from Known Error Database(KEDB). If a related resolution/workaround is available, the technician can add the same as the [problem resolution](#) and close the problem directly.

Once all details are added, the user must click "[Submit as New](#)" - to submit the problem.

Working on a Problem

Problem Management requires a high level of expertise. There are multiple ways to record a problem, but the resolution of the problem is in the hands of L2/L3 level technicians.

Before working on the problem, it is necessary to understand the life cycle of problems and the key components within Infraon's Problem module.

Problem Views

There are two ways to view problem details in the right-side panel. They are:

Panel View - In the Panel view, you see problem details in the form of a Summary Card. The summary card gives a summary of the problem. This summary contains all the important information needed to work on the problem. Details include:

- **Problem ID:** Auto-generated when a problem is created.
- **Requester:** Name of the requester
- **Team:** The team assigned to work on the problem.
- **Status:** Displays the current status of the problem. Technicians can change the status from here as well.
- **Priority:** Displays the priority of the problem. Technicians can change the priority of the problem.
- **Service:** The area in which the problem is reported.
- **Resolve:** The technicians have the option to resolve the problem from this panel.
- **Actions:** Quick action icons to work on the problem.

The revamp of the panel view for tickets. The improved interface offers enhanced data visibility, with aging metrics conveniently displayed. This helps in faster navigation and reduced system load for a seamless user experience.

Grid View - In Grid view, you see problem details in tabular form. Clicking on the Problem ID shows the details of the Problem.

Problem ID: Auto-generated when a problem is created. Click on the Problem ID to view the communication history, reply to and forward emails, add notes, analyze, view, and add work logs. You can resolve a problem from this screen too.

- **Problem Source:** This shows how the problem was submitted.
- **Priority:** The priority of the problem
- **Requester:** Displays the name of the requester (initial)
- **Subject:** Subject of the problem (derived from the problem subject line)
- **Team:** The team to which the problem is assigned
- **Assignee:** The person to whom the problem is assigned
- **Actions:** Quick action icons to work on the problem

Note:

- The quick action bar appears as a floater on each problem line and is common in both Panel and Grid views.

- The summary card details can be configured to suit requirements. Click on the "Configure" icon to customize the details you want to see on the screen.
- Configure icon is available only in Grid View.

Analysis

Problem Management is about finding the root cause of an issue. A detailed Root Cause Analysis(RCA) is performed based on the urgency and severity of the problem. When we click on the Problem ID, it opens the details of the problem. In the right-side panel, there is an option to add the analysis of the problem. Multiple analyses can be added until the root cause is identified. These analysis details are saved as a Draft and can be viewed/edited at any time. The various methods used for analysis are:

5 Whys Method

The 5 whys method was originally developed by Sakichi Toyoda, the founder of Toyota Industries. The 5 whys is an iterative analysis technique that aims to expose the underlying cause by asking the question, "Why" five times. The number '5' comes from the observation that usually five iterations of the question 'why' reveals the underlying root cause.

How to implement the 5 whys method:

- Ask why the problem took place. Write the answer to this question.
- Keep asking 'why' to the successive answers and note down the answers.
- Repeat the step above until you reach the root cause of the problem.

This may take five or less than five 'whys'. If you feel satisfied with the analysis, click on 'Save Changes' to save the analysis.

Chronological Method

As the name suggests, Chronological analysis is a time-based approach. It helps take a look at the events in the order of occurrence from first to last. All the events from the time a problem occurred are recorded in a chronological manner and analyzed.

Kepner Tregoe Method

Kepner Tregoe method is a problem-analysis method developed by Charles Kepner and Benjamin Tregoe. It is a step-by-step approach to systematically gathering information and evaluating it. It gathers the following information in a structured way.

- What is the problem? Begin by defining the problem.
- Where does the problem occur? Note down the LOCATION of the problem.
- When did the problem occur? Note down the TIME of the problem occurrence.
- How frequently has the problem occurred?
- What is the size of the problem? How many parts are affected?

Solution/Workaround

Workaround

Sometimes it is possible to temporarily fix the problem so the user may continue with the business as usual. This can be documented in the Solution/Workaround section. Once a workaround is provided, the associated tickets can be closed. The problem's status will remain open until a permanent solution is found.

Solution

A Solution is a permanent fix to the problem. This can be documented in the Solution/Workaround section, and an entry is made into the Known Error Database(KEDB), and the problem is marked as Closed.

Additional Icons

Name	Description
Comment	A user/technician can see the comments on the problem and also can add new comments.
History	Shows the history of the current problem from the time it was created.
Interaction	Shows the history of the problem created by the requester.
Attachment	Shows all the attachments of the current problem.
Problem Source	Shows the source of the problem, like email, web, phone, etc.
Convert Problem to KB	Option to convert the problem into a Knowledge Base (KB). This action is possible only if the status of the problem is "Resolved" or "Closed".
Add Change	Problem Management may initiate resolution through a change request. A Change Request can be added for this problem. This action is possible only if the status of the problem is "Open", "In Progress", or "On Hold".

View Change	If a change request has been created for a problem, then this option is visible. This can be clicked to view the related change request.
--------------------	------------------------------------------------------------------------------------------------------------------------------------------

Quick Actions

Name	Description
Quick Edit	To perform quick edit actions like status, priority, urgency, severity, impact service, and the assignee. <i>Use the "Detailed Edit" button to edit the Problem details.</i>
Edit	To edit the Problem in detail.
Delete	To delete the Problem. This action is irreversible.
Copy	To copy the details of a problem and create a new problem.
Problem aging for helpdesk/ITSM close and resolve conditions	Grid view includes aging metric. Track problem resolution time accurately. Click 'Resolve' or 'close' to stop the aging clock. Get detailed aging reports based on resolved status.

Page Actions

The Problem page also has the following actions.

Label/ Icon	Description
Expand Icon	To View the problem filters.
Search Bar	To help search for a specific problem using the problem ID, assignee, etc.
Calendar	To filter the problem by a specific day, date, or date range.
*Tag	Select a problem to view the tag option. Tagging is a way to group problems.
*Assignment	Select one or more problems to assign to a group.
*Delete	Select one or more problems to delete.
Pause	To pause the auto-reload.
Configure	To configure the summary card and column selection

*Select at least one problem to enable these options.

Change Management

ITIL defines Change as "the addition, modification, or removal of any authorized, planned, or supported service or service component that could affect services." In other words, a Change is adding, removing, or modifying anything that could directly or indirectly affect the organization's services and operations. The changes could include documentation, processes, applications, or IT infrastructure. In Infraon, the module that handles all the change requests is called "Change."

Change Management is a set of processes defined to manage the lifecycle of a change request. Change Management aims to minimize the risks and disruptions to IT services and business operations while implementing the changes.

Benefits of Change Management

- Reduced system downtime and outage
- Faster change implementation
- Decreased negative impact on business and IT services
- Visibility into future IT changes

Essential Roles in Change Management

Change Manager - A Change Manager is responsible for reviewing the submitted change requests, scheduling Change Advisory Board(CAB) meetings, updating the change records, reviewing the rollback and rollout plans, coordinating the implementation of changes, and reviewing the implemented changes. Usually, a high-level manager or a Domain Expert is assigned as a Change Manager to a change request.

Change Advisory Board(CAB) - A Change Advisory Board (CAB) may consist of Business, IT Operations, Development, Customer, Domain Experts, and Solution Architects, depending upon the type of the change. A CAB is carefully selected to ensure all facets of an organization are represented while discussing the impacts, benefits, and implementation of a change. CAB requires financial data, the technical advantage of the change request, the number of resources required, criticality, and so on, to make an informed decision on the change request. Depending upon the severity of the change, the Change Manager may decide whom to include in the discussions. A CAB chooses whether to approve or reject a change.

Change Management Process

Infraon's Change Management module enables users/organizations to implement changes through the following steps seamlessly:

- **Change Detection** - This is the first step of Change Management. For example, A customer may request a change in the services or ask for

additional services. This is logged as a change request. A change request may also arise from a ticket, request, or problem.

- **Change Recording** - A technician or user with the required permissions can log a change in the module.
- **Planning** - In this stage, planning of the change request happens. A comprehensive plan is essential for the successful implementation of a change. A detailed plan showcases the risks, impacts, rollout plan, rollback plan, and associated downtime(if any) to all the stakeholders. Planning is important in getting approvals from the Change Advisory Board (CAB).
- **Analysis** - A detailed analysis is performed to understand a change's risks and impacts on the organization or service(s).
- **Change Approvals** - Next, the change plan needs to be reviewed, and a decision is taken by the Change Advisory Board (CAB). The change plan may be approved/rejected.
- **Change Implementation** - Once approved, the change manager ensures the change is implemented as detailed in the plan and at the right time. A Change Manager also ensures there is coordination between different teams involved in the change implementation.
- **Review** - Once a change is implemented, a Post Implementation Review is conducted to confirm if the change implementation was successful. A review is also performed to determine if the change achieved its objectives. If the change implementation is unsuccessful, the rollback plan is activated promptly.
- **Closure** - This is the last step in the Change management process. After conducting Post Implementation Review, the change can be closed with closing comments on whether the change was successful, executed on time, and so on.

Apart from these, Infraon also covers change ownership, monitoring, tracking, and communication - throughout the life cycle of each change request.

Changes are managed through the "Change" module. Changes can be raised by users with appropriate permissions. Changes follow multiple state(s) and status(es) through their life cycle.

State and Status

State	Status	Status Scenario
Open	New	When a new change is logged in the system.
In Progress	Planning	When the planning of the change request is in progress.

In Progress	Analysis	When the possible risk analysis is in progress.
In Progress	Implementation	When the proposed change plans are being implemented.
In Progress	Deployment	When the change is being deployed in production.
In Progress	Verification	When the deployed change is being verified.
On Hold	Pending	If any changes are pending to be implemented.
Close	Closed	After Post Implementation Review, the change can be closed with closing comments.
Close	Cancel	If the change implementation is canceled.

Customized Status(es) can be configured from the 'Workflow' module to suit the requirement.

Easily convert resolved Change to Knowledge Base articles. KB icon appears post-resolution, ensuring efficient knowledge management.

Demo data for ITSM module change for new Org

Knowledge Base Modules! Explore added knowledge articles to understand the functionality and purpose of KB modules.

Change

ITIL defines Change as "the addition, modification, or removal of any authorized, planned, or supported service or service component that could affect IT services." In other words, a Change is adding, removing, or modifying anything that could directly or indirectly affect the organization's services and operations. The changes could include changes to documentation, processes, applications, or IT infrastructure.

Change Management is a set of processes defined to manage the lifecycle of a change request from start to closure. Change Management aims to minimize the risks and disruptions to IT services and business operations while the changes are being implemented.

How does it work?

Domain experts, management, architects, and/or solution architects are involved in planning and implementing a change request.

Types of Change

Type	Description	Example
Standard Change	Standard Changes are the ones that frequently occur in an organization. These changes are low-risk and have a pre-defined set of documented and approved processes to be followed. This pre-defined and approved process is called a template.	Reset the Password of an email account.
Minor Change	A minor change is a small change that is low-impact and low-risk. These changes only occur occasionally in an organization. A minor change needs approval from the Change Advisory Board(CAB). It is essential to document all the important information for future reference. A minor change could be converted to a standard change in the future.	Changes to the company website.
Major Change	A major change is a high-risk and high-impact change. A major change could impact an organization's services if it is not planned properly. It requires an in-depth proposal on risk analysis, financial implications, and cost-benefit analysis. It requires approval from the Change Advisory Board(CAB) as well as from the management.	Changes to Network Infrastructure
*Emergency Change	Emergency changes are unexpected disruptions that must be assessed and implemented as soon as possible to restore the normal functioning of an organization.	Dealing with a server outage

*Emergency Change is not part of this release. It will be implemented in a future release.

What do you see on the screen?

The "Change" page lists all change requests with two views: Panel View and Grid View. The page lists all changes with details like summary card, change description, status, subject, team, requester name, and actions, sorted by time.

Add Change

Requesters can add a Change request through the "Change" module. A requester is a user requesting the change. A change could also arise from a ticket, a request, or a problem.

Pre-requisites:

To add a change, the following must be pre-configured

- Requester - the user requesting the change
- Priority - priority of the change
- Change Manager - A Change Manager is usually a domain expert overseeing the change request.
- Change Implementer - A Change Implementer is the user responsible for implementing the change.
- Followers - users to be notified of the "change" status updates. Use the "Follow" button to follow directly.
- Tags - groupings used for the classification of changes.

Steps to add a Change

- Go to the "Change" page.
- Click on the "New Change" button.

If requesters have been added already, use the search option to select the requester's name. If no requesters have been added or to add a new requester, use the "Add a New Requester" button. Follow the "Requester" module for details. You can select or add a requester from the next page too.

To add a change, follow the steps from the below table:

Label	Action	Description/Example
Requester*	Add a new requester or search for an existing requester.	Requesters are usually technicians or users with the required permissions who can add a change.
Reported by	Use the icon to expand this section. Add the reporter's name and email address, if applicable.	Reporters are users raising the change on behalf of the requester.
Change Manager	Select a Change Manager from the list.	A change manager overlooks the change analysis and implementation.
Change Implementer	Select the change implementer from the list.	A change implementer can be a user or a team responsible for implementing the change.
Impact Service	Select the Impact Service from the list.	This can be left blank. As the risk analysis progresses, the technicians can later select the impacted service.

Service Classification	Select the classification within the impacted service.	This is used when a specific service has multiple classifications. For example, if the impacted service is Network, the classifications can be connectivity, router issue, and so on. Leave this field blank if no classifications are defined.
Followers	Select a user to add them as followers.	Users who must be notified of the change request or any changes to the status of the change request can be added as followers. Use the 'Follow' option to self-follow the change request.
Tags	Select a tag to tag the change.	These tags must be predefined in the 'General Settings -> Tag Management module.
Subject	Add a subject line for the change.	The subject line can be a summary of the change. For example: Unable to connect to the network.
Description	Provide a brief description of the change.	
Due By	It is the due date by which a team aims to implement the change.	
Priority	Select the priority of the change from the list.	
Risk	Select the risk level from the list.	
Change Type	Select the type of Change from the list.	<p>The changes can be of four types:</p> <ul style="list-style-type: none"> ◦ Standard Change ◦ Major Change ◦ Minor Change ◦ *Emergency Change
Reason for Change	Specify the reason for requesting the change.	
Add attachments	Use the action icon to add an attachment to the change.	Attachments can include emails, screenshots, etc.
Rollout	Specify the plan to rollout the change.	Leave this field blank if the rollout plan is not yet decided.

Rollback	Specify the plan to rollback the changes.	Leave this field blank if the rollback plan is not yet decided.
-----------------	-------------------------------------------	-----------------------------------------------------------------

*Emergency Change is not part of this release. It will be implemented in a future release.

Note:

- When the requester's name is added, Infraon displays the list of interactions the requester has had in the past. Click on the Change ID to view the details.

Once all details are added, the user must click "Submit as New" - to submit the change.

Custom Change template creation.

- Go to "Add change"
- Click on the select template.

The default templates and the ability to create custom templates for planning and specific changes. Ensure seamless data integration and automating tasks for increased efficiency.

E-mail alerts on asset hardware changes

Automated Hardware Change Notifications! Enable in feature plan, select an asset, and edit sub-category. Configure templates for custom mail notifications, including logo, keys, and menu order adjustments.

Working on a Change

Change Management involves people from different dimensions of a business. They work together in analyzing, planning, and implementing the change request.

Views of the Change Request

There are two ways to view change details in the right-side panel. They are:

Panel View - In the Panel view, you see change details in the form of a Summary Card. The summary card gives a brief summary of the change. This summary contains all the important information needed to work on the change. Details include:

- **Change ID:** Auto-generated when a change is created.
- **Requester:** Name of the requester
- **Change Manager:** Name of the manager overlooking the change request.

- **Status:** Displays the current status of the change. Users can change the status from here as well.
- **Priority:** Displays the priority of the change. Technicians can change the priority of the change.
- **Service:** Service category in which change is requested.
- **Actions:** Quick action icons to work on the change.

The revamp of the panel view for tickets. The improved interface offers enhanced data visibility, with aging metrics conveniently displayed. This helps in faster navigation and reduced system load for a seamless user experience.

Grid View- In the Grid view, you see change details in tabular form. Clicking on the Change ID shows the details of the Change.

- **Change ID:** Auto-generated when a change is created. Click on the Change ID to view the communication history, reply to and forward emails, add notes, analyze, view and add work logs.
- **Subject:** Subject of the change (derived from the change subject line).
- **Reason for Change:** Reason detailing why the change was requested.
- **Change Type:** Type of change: Standard, Major, Minor, and emergency.
- **Status:** Displays the current status of the change. Users can change the status from here as well.
- **Impact Service:** Service Category which the change could impact.
- **Priority:** The priority of the change.
- **Risk:** Risk level of the change.
- **Requester:** Displays the name of the requester (initial)
- **Change Manager:** Name of the manager overseeing the change request.
- **Change Implementer:** Name of the user responsible for change implementation.
- **Actions:** Quick action icons to work on the change.

Note:

- The quick action bar appears as a floater on each change line and is common in both Panel and Grid views.

- The summary card details can be configured to suit requirements. Click on the "Configure" icon to customize the details you want to see on the screen.
- Configure icon is available only in Grid View.

Planning and Risk Analysis

Implementing a change requires intensive planning, risk analysis, defining tasks, and approvals. To help users achieve this, the "Change" module has the following tabs:

1. **Planning** - A comprehensive plan is essential for the successful implementation of a change. In the planning tab, a user can enter the following details:
 - **Rollout Plan** - A rollout plan is a detailed step-by-step description of how the change will be implemented in the production environment. The rollout plan is created in such a way that there is minimal impact on the organization. A rollout plan describes whether the change will be implemented in a phased manner or as a whole.
 - **Rollback Plan** - A rollback plan is a verified step-by-step fallback or back-out plan in case the change implementation doesn't go as expected. It is essential to have a rollback plan when implementing a major change.
 - **Impact** - A user can enter the anticipated impact of the change on various dimensions of the organization. It can be categorized into the following:
 - Business
 - Location
 - Department
 - Group
 - User
 - **Planned Start Date** - The intended date to begin implementing the change.
 - **Planned End Date** - The intended date to end implementing the change.
2. **Tasks** - In this tab, a user can enter the details of the tasks involved in the change.
 - **Title** - Title of the task.
 - **Description** - A brief description of the task.
 - **Status** - Status of the task. The different statuses of the task are:
 - To-Do (Open)
 - On Going (In Progress)
 - Blocked (On Hold)
 - Done (Close)
 - Cancelled (Close)
 - **Priority** - Priority of the task.
 - **Assignee** - Name of the user to whom the task is assigned.
 - **Due By** - The expected date by which the task is due to be completed.

3. **Risks** - In this tab, a user can enter the details of the risks involved in the change.

- **Name** - Name of the task.
- Risk Type - Type of the risk. It can be of the following types:
 - Business
 - Financial
 - Technical
 - Others
- **Mitigation Plan** - A risk mitigation plan outlines a strategy to prepare for or lessen the effects of risks.
- Description - A brief description of the risk.

Additional Icons

Name	Description
Comment	A user/technician can see the comments on the change and also can add new comments.
History	Shows the history of the current change request from the time it was created.
Interaction	Shows the history of the change request created by the requester.
Attachment	Shows all the attachments of the current change request.
Change Source	Shows the source of the change, like email, web, phone, etc.

Quick Actions

Name	Description
Quick Edit	To perform quick edit actions like change manager, status, priority, urgency, severity, impact service, and the assignee. Use the "Detailed Edit" button to edit the Change details.
Edit	To edit the Change in detail.
Delete	To delete the Change. This action is irreversible.
Task	Shows the tasks involved in the change.
*Risk	Shows the risks involved in the change.
*Add Ticket	If any issues occur while implementing the change, a ticket can be raised.
Change aging for helpdesk/ ITSM close and resolve conditions	Grid View includes Aging Metric. Track Change resolution time accurately. Click 'Resolve' or 'Close' to stop the aging clock. Get detailed aging reports based on resolved status.

*These quick action tools are available only for Major and Minor Changes.

Page Actions

The Change page also has the following actions.

Label/ Icon	Description
Expand Icon	To View the change filters.

Search Bar	To help search for a specific change request using the Change ID, assignee, etc.
Calendar	To filter the change requests by a specific day, date, or date range.
Workspace task App	Enjoy a seamless and streamlined experience with the powerful capabilities of the Task Common Module for enhanced task management within the application.
*Tag	Select a change request to view the tag option. Tagging is a way to group change requests.
*Assignment	Select one or more change requests to assign to a team.
*Delete	Select one or more change requests to delete them.
Pause	To pause the auto-reload.
Configure	To configure the summary card and column selection.

*Select at least one change request to enable these options

Release

What you see on the screen

The release page view can be toggled between Grid View and Card View using the button next to the '**New Release**' button.

Details displayed are as follows:

- Release Manager
- Team
- Status
- Priority
- Risk
- Release Type
- Due Date

Label	Action	Description/ Example
View	Click on the view icon, to view the categories.	All, My Approval, Pending Releases etc.
Search	Search for the required release.	
Filter	Filter can be added based on the field and condition from the drop-down box below.	Field – Actual Closure Date, Agreed Closure Date, Assignee, Callback, Closed Type, Closed by, Creation Time, Creator, Due Date, Impact, Last Updated Time, Priority, etc. Condition – in, not in, equal to, not equal to, contains, not contains.

Auto Reload	Click to Stop (Default is Auto)	It reloads the topology view at every interval of 60 seconds.
New Release	Click to add a new release.	Follow the below to add a new release.

Each Release allows the below actions by hovering over the mouse (Quick action tools):

Label	Action/ Description
Comment/ Communication	Access existing comments or share your own insights via Mail, Notes, or the workflow with a simple click.
History	Click here to view the complete timeline and details of the releases.
Interaction	This button unlocks the release interaction log, providing a data-driven perspective on user engagement, feedback trends, and support activity.
Attachment	Click here to access the docs/ screenshot etc. attached to the release.
Quick Edit	Click for quick configuration changes.
Edit	Click here for advanced/ detailed release editing.
Delete	Access this button to delete the selected release.
Relation	Clicking this button enables users to add a Ticket, Problem, Change or a request to the release.
Complete	Click to change the status to Complete and simultaneously closing the release.

Instructions to add a New Release

- Go to Infraon OSS portal -> Release.
- Navigate and click on the 'New Release' button at the top right corner of the page.
- Enter the below details in the respective callout boxes:

Label	Action	Description/ Example
-------	--------	----------------------

Requester Details		
Assignee	Select the Name of the Assignee from the drop-down box.	Click on the "Take it" button to self assign.
Impact	Select the required call-out from the drop-down box.	Business, Location, Department, Group.
Urgency	Select the type of Urgency needed for the release.	Low, Medium or High.
Severity	Select the level of severity of the release.	Minor, Major or Critical.
Risk	Select the level of risk associated with the release.	Low, Medium, High or Critical.
Version	Enter the Version details for the release.	
Service Category	Select the service category from the drop-down filter box.	IT Services <ul style="list-style-type: none"> • Email Support <ul style="list-style-type: none"> ◦ Email Client Installation ◦ Mailbox Quota Request ◦ Email Delete ◦ New E-Mail Account • Hardware Support <ul style="list-style-type: none"> ◦ Printer Service ◦ PC • Software Support <ul style="list-style-type: none"> ◦ Antivirus Service
Tag	Select a Tag to assign in the release.	Click on the "New Tag" to create a new Tag for the instance.
Title	Enter a descriptive title for your release	
Description	Give a brief description about your release.	
Release Details		
Due Date	Select the required due date for your release.	
Release Manager	Click to assign a release manager.	
Priority	Select the priority from the drop-down box.	Low, Medium, High or Critical.

Release Type	Select the type of release from the drop-down box.	
Notes	Click to add a specific notes for your release.	

Once all details are filled, click Submit to add it.

Events

Event Management

Any change observed and detected within your organization is referred to as an event.

The primary objective of the event management module within ITIL is to detect all changes or activities within the infrastructure, observe for anomalies and raise the alarm, if necessary. Events are Infraon's way of active and passive monitoring of

- CI items like laptops, desktops, etc.,
- Software licensing and performance
- Application performance
- Server performance

Monitoring the status and availability of items are part of active monitoring, while detection and correlation of operational alerts based on the configured thresholds and triggers are passive monitoring.

Infraon's Event Management module enables users/organizations to achieve their goals through the below steps:

- There are constant changes in the infrastructure. Ideally, a user's login, upgrade of software/hardware, or regular maintenance are all events. However, these are not events that need to be notified or taken action upon. When there is a change in the server's performance or availability, it needs to be reported immediately. Infraon extracts the necessary data from the happenings of the infrastructure and detects 'events that need attention on occurrence.'
- These anomalies or changes are run through the default thresholds and categorized as basic, informational, major, or performance. Thresholds can be sorted as minor, major, or critical. Refer to the Thresholds section for details.
- Anomalies and changes are categorized and reported as events.
- Technicians or NOC users can use these events to perform necessary actions.

Note: If triggers are configured for events, a notification is triggered either at the event's occurrence or after correlating.

Refer to the [Events](#) section for more details.

Events

Infraon detects all changes or activities of CIs or configuration items, observes anomalies based on the configured thresholds, and records them as events. If triggers are configured for the same, notifications or incidents are raised accordingly.

How does it work?

Infraon is configured with built-in thresholds for all the monitoring nodes and their components. Infraon monitors the assets constantly. It detects threshold breaches and records them as events. If any thresholds, devices, or metrics are linked in a trigger, Infraon either triggers a notification or converts the event to an Incident.

What you see on the screen

The events page lists all events - Issue, Date, Node, Resource, and Event ID, sorted by time. Events have default filters like:

- [Critical, Major, and Minor](#) - based on the threshold
- [Acknowledged and Ticketed](#) - based on the action
- [Priority](#) - based on the asset property
- [Root](#) - based on the correlation
- [NCCM](#) – This shows events focused exclusively on the NCCM module, including download jobs and configuration changes. By applying this filter, technicians can focus on network configuration and change management activities, making monitoring and addressing NCCM-related issues easier.

Each event allows the below actions (Quick action tool):

Events can be filtered by dates or downloaded using the respective icons.

Label	Action	Description/ Example
Analyse	Click to view the 'Impact Services' event details. Click on the 'More Details' button to be redirected to the event page.	Includes details to help analyse the event. User can view the asset details and the statistics of what the current event is performing.
Acknowledge		Used to acknowledge the event. NOC users or

		technicians can acknowledge and add a comment to let other users know they are working on it.
Diagnosis		Used to perform active diagnosis. Diagnosis can be performed using Ping, SNMP Walk, and Trace Route.
Ticket		Used to create an incident for the event.
Clear		Used to clear the event. Cleared events can be viewed using the 'Show History' toggle button.
Activity Log		Used to view the event history.

Log Management

Log Management is a crucial component that analyzes logs from various IT systems in real-time, providing insights for security monitoring, compliance, auditing, IT operations, anomaly detection, application troubleshooting, and business analytics.

It processes data from diverse sources across the IT infrastructure, offering visibility into system status and processes.

[Click here](#) to access the detailed Log Management content and learn how to manage your logs effectively.

Log Search

Log Search is a tool that enables rapid querying and analysis of large volumes of structured and unstructured log data. It uses an index-based storage architecture in an Elastic database, allowing efficient searching across specific log categories. This approach significantly reduces search times, delivering results within seconds, even for extensive log collections.

[Click here](#) to access the detailed information about this module.

Log Stream

Log Stream is a centralized tool in Infraon Infinity that provides unified access to all logs in the Elasticsearch database. It enables users to search, filter, and tail logs in real time without logging into individual servers. Features include live streaming, auto-complete filtering, a navigation log graph, quick message categorization, streamlining log analysis, and pattern identification.

[Click here](#) to access the detailed information about this module.

Report

Data without perspective can be useless. To make the possible use of the data, Infraon provides attractive and easily customizable reports that ensure data monitoring most appropriate for everyone within the organization.

Infraon reports provide a summarized and detailed analysis of the performance and fault-related data collected. Reports include:

- Trending, pattern, and summary analysis to analyze the past behaviour
- Perform trend analysis and pattern analysis with historical data to help predict future behaviour.

Infraon's default reports are highly configurable and flexible. Long-term data can be easily managed by collecting, summarizing, and pruning historical data. The combination of real-time and historical reporting aids in identifying trends, predicting system behaviour, and making well-informed management decisions to drive future expansions.

Infraon's timescale and data fields in the report to filter the asset details at a granular level using the columns, timescale orders, and order by. Improvising asset report functionality, providing enhanced data analysis and filtering capabilities.

Infraon supports exporting of reports and pre-configured auto-reports in PDF/Excel/CSV formats. Advanced real-time and historical reporting capabilities can be customized according to user preferences to help them view essential data.

How does it work?

There are multiple pre-configured reports available on Infraon. These can be customized in addition to adding new custom reports.

What you see on the screen

The reports page lists all default reports and offers options to add new reports, view, edit, and delete existing reports.

Data Privacy

Mask/ Unmask Requester Info

Admins can enable to hide requester's info in reports to comply with data privacy.

Mask	Unmask
------	--------

Name	Enabling this toggle button will obfuscate the requester's name in reports to comply with data privacy.	Employ the designated toggle switch to restore the display of the requester's name within the report interface for authorization purposes.
Contact	Enabling this toggle button will obfuscate the requester's contact in reports to comply with data privacy.	Employ the designated toggle switch to restore the display of the requester's contact within the report interface for authorization purposes.
Email	Enabling this toggle button will obfuscate the requester's email ID in reports to comply with data privacy.	Employ the designated toggle switch to restore the display of the requester's email within the report interface for authorization purposes.

Instructions to Add Report

Click on the [Add Report](#) in the top right corner. There are three tabs on the 'Add Report' page. Refer to the table for more information.

[Category](#) | Configuration | Filter

'Report' has various categories. You can click the specific category that you want to get the report.

Label	Action	Description/Example
Availability Reports	Select the availability report box to send the report.	Availability report helps technicians to analyze situations in which problems have occurred. It can be plotted against time in each interval and viewed as a data table, line chart, area chart, bar chart, etc. Example; Login hours, shift hours, availability percentage, etc.
Node Summary Report	Click the Performance Reports on the left panel and select the Node summary report.	The node summary report provides statistical information about the node at the selected time interval. For example, total words coded to a node, number of sources coded at a node, number of users coded at a node, etc.
Event Report	Click the Event Reports on the left panel and select the Event Report.	The event report provides statistical information about the specific event for the selected time interval.

Event Summary Report	Click the Event Reports on the left panel and select the Event Summary Report.	The event summary report gives comprehensive statistical data for all the events for the selected time interval.
Incident Report	Click the Helpdesk Reports on the left panel and select the Incident Report.	Incident Report provides statistical information about the specific incident for the selected time interval.
Incident Summary Report	Click the Helpdesk Reports on the left panel and select the Incident Summary Report.	Incident Summary Report gives comprehensive statistical data for all the incidents for the selected time interval.
Depreciation Report	Click the Helpdesk Reports on the left panel and select the Depreciation Report	Generate the Depreciation Report for Assets and select the relevant report from the provided list. Submit the report request and select the financial year start date to generate the report according to the specific needs. The generated report provides accurate and up-to-date information about asset depreciation.
Location Report	Click on the organization on the left panel and select the address book. Click on the 'Export' icon.	Manage and track the location of the assets by exporting the address book details from the organization's address book. With the ability to import and export location details, quickly generate comprehensive location reports for the assets.
Detailed Asset Report	Click on the Helpdesk Reports on the left panel and select the Asset Reports. Click on the Detailed Asset Report	Comprehensive asset hardware, software, and activity log all in one report with detailed asset report by selected tags and duration and generate information that contains the asset name, IP address, inventory details and more.
Asset ticket report	Click on the reports on the left panel and select	Effortlessly access and segregate asset-related and

	the ITSM reports. Click on the Asset ticket report	ticket-related data in separate reports. Select specific product categories for enhanced insights, and enjoy functionalities like scheduling, saving, and previewing reports with ease.
Installed vs purchased report advance	Click on the reports on the left panel and select software reports.	Access the 'Software Installed vs Purchase' report in the software report section. Track software names, purchase details, installation status, and compliance metrics.
Software Detail Report	Click on the reports on the left panel and select software reports.	Access detailed reports for respective software in Software Detail Reports. Identify software status as 'Discovered' if found through the agent, or 'Managed' if manually added.
Software by publisher reports	Click on the reports on the left panel and select software reports.	Enable all columns in Software by Publish Reports. Gain detailed insights into respective assets, including application name, vendor, help link, and more. Filter by asset tag and custom criteria for comprehensive software tracking.
ITSM Ticket Summary Report	Click on the reports on the left panel and select the ITSM reports. Click on the Ticket summary report.	Enables key metrics and statistics related to tickets, such as incidents, service requests, changes, or problems, managed by an IT service desk or support team. This report serves as a snapshot of ticket-related data within a specified timeframe, allowing stakeholders to quickly understand the performance, workload, and trends within the IT service desk.

IMACD Summary Report	Click on the reports on the left panel and select the IMACD. Click on the IMACD report.	Provides a consolidated overview of the key metrics and statistics related to installation, movement, addition, changes, and destroy processes handled by the IT service management team. Helps monitor service delivery, identify areas for improvement, make data-driven decisions, and enhance customer satisfaction.
Forecast Prediction Report	Click on the reports on the left panel and select the ITSM. Click on the IMACD report.	This report leverages AI/ ML to forecast resource utilization trends of a single statistic. The predicted data is then segmented into three categories based on utilization levels, allowing for proactive resource allocation and optimization.
Forecast Summary Report		This report leverages AI/ ML to forecast and predict resource utilization for a single statistic and summarizes them based on configured thresholds. This information can be used for proactive maintenance planning and capacity assessments.
Server Capacity Planning Report		This report leverages monitoring data to assess server resource utilization (CPU, memory, disk). It categorizes resources as underutilized, optimally utilized, or overutilized, enabling informed resource allocation decisions.
Device Capacity Planning Report		This report leverages monitoring data to assess device resource utilization

		(CPU, memory, disk). It categorizes devices as underutilized, optimally utilized, or overutilized, enabling proactive capacity planning.
Link Capacity Planning Report		Analyses interface utilization based on polling data and categorizes them as under, optimal, or over-utilized, aiding proactive capacity planning.
Prediction Trend Report		This report displays a comparative graph of past data and predicted resources for proactive planning.
Ticket Escalation Notification Report	Click on the reports on the left panel and select the ITSM reports. Click on the Ticket Escalation Reports.	Generate comprehensive statistical data on ticket notifications escalated within a chosen timeframe, analyzing trends across various columns such as user, requester, impacted services, and more. Customize the report to highlight specific areas of interest, enabling a detailed examination of trends and patterns within the selected period for more insightful analysis.
Configuration Download Result Report	Click on the reports on the left panel and select the NCCM reports.	Generate a detailed summary of configuration download activities for network devices. This report includes the status of each download (success or failure), device details, and any encountered errors.
Jobs Account Audit Report	Click on the reports on the left panel and select the NCCM reports.	Summarizes audit information related to user actions during download job executions. It captures details such as device IP address, account information, connection protocol, job type, and any failure messages.

After selecting the specific Report, click [Next](#) to add Configuration.

Category | [Configuration](#) | Filter

Configuration boxes vary based on the selected Report. You will see three-four sections in the configuration tab. Refer to the table for more information.

Label	Description
Statistics	You can modify your report by adding statistical details like CPU utilization, Availability, etc.
Columns	You can choose assets from the column. This column is optional; you can proceed to the next tab without filling it.
Show Top	You can select the top 5 or 10 to see only the full 5 or 10 reports.
Resolution	You can select resolution duration as min, hour, day, or month. Note: The resolution option is only available in Availability Report.

After selecting the appropriate boxes on the Configuration tab, click '[Next](#)' to add details on Filter.

Category | Configuration | [Filter](#)

Filter options vary based on the selected Report. You will see three sections in the Filter tab.

You can apply a filter to see only the details you selected.

Label	Description
Duration	Select the particular duration that you want to see on the report. By default, it is selected as the last hour.
Asset Tag	Select any asset tag for your report.
Incident Tags	Select the incident tags that you wanted to see on your report. Note: This option is only available in Incident Report and Incident Summary Report.
Assignee	Select the assignee name to whom you want to send the report. Note: This option is only available in Incident Report and Incident Summary Report.

After applying Filter, click [View Report](#) to see your report on the Report dashboard.

Knowledge Base

Infraon's Knowledge Base

Infraon's Knowledge Base module enables users to author their articles, curate articles/guides from internal or external sources, and use, share and manage knowledge across organization and end-users.

Infraon's KB is categorized into:

- **Article** - The article must contain a complete set of Information with details on all aspects of the selected topic. Articles are usually intended to solve a common problem - [How to configure an Email account on Outlook](#) or [How to reset Infraon password etc.](#), news sourced internally ([Updates on KB module of Infraon](#)) or externally, [What to expect with the latest update of MS Office](#)), etc.
- **FAQ** - Frequently asked and answered questions.
- **Information** - A piece of information that can be published to keep others informed about the topic. It can be a problem, instructions for a single step in a process, etc.
- **Known Error** - When a problem has been reported and classified as 'Known Error' and contains instructions for a temporary fix or workaround.
- **Solution** - When a reported problem has a permanent solution. Known errors must be deprecated when a solution is found.

The main page displays all recent articles with an option to sort highest rated or bookmarked articles. Information in the knowledge base is grouped into 'Categories' defined in the 'Service Catalog.'

Below are the actions available on each KB:

- **Bookmark** - Bookmark an article used frequently. Bookmarked posts are displayed on the right panel for easy access.
- **Helpful** - Mark if the KB was helpful.
- **Rating** - If the article was helpful, add ratings and reviews for the article. If not beneficial, add feedback to help improve.
- **Comment** - Add a comment on the KB.
- **Like** - Like an article.
- **Edit** or **Delete** - Privileged users can edit or delete the KB.
- **Version History** - View Version history and changes.
- **Attachments** - View documents/files attached to the KB

The default status of a KB would be Draft, which is changed to "Published" when the KB is published.

Knowledge Base

Knowledge Base (KB) is a repository of information about products, services, related topics, etc., intended for self-service. KB makes it easy for users to search for solutions instead of contacting the help desk/experts for repeated/common problems. It is recommended to include articles/guides about

all products and services within the organization to enable contactless, round-the-clock self-service.

Infraon's Knowledge Base module enables users to author their articles, curate articles/guides from internal or external sources, and use, share and manage knowledge across organizations and end-users.

Why Knowledge Base?

Studies conducted by Forrester and Ciboodle state that:

- **70%** of customers prefer to use a company's website to get answers to their questions rather than use phone or email.
- An efficient Knowledge Base can enable customers to manage **85%** of their relationship with an enterprise without interacting with a human, allowing the organizations to save.
- Organizations saw a **50%** increase in Customer Satisfaction ratings through social Customer Support (Public Knowledge Base).

An adequate Knowledge Base empowers the end user to quickly find answers and information needed when they need them without having to go through the hassle of waiting to get hold of an agent on call/waiting for their incident to get assigned to a Techie.

Having said that, to get all the advantages of a Knowledge Base, it is essential to present such complicated and detailed information in a user-friendly format, which Infraon's Knowledge Base offers. Infraon's KB is designed to add quick problem-solving tips, troubleshooting guides, answers to frequently asked questions, sharing best practices through Articles, known errors so on in a user-friendly manner.

How to build an effective Knowledge Base?

A study by Coleman Parkes for Amdocs states that **91%** of customers would be glad to use the available online database only if it is tailored to their needs. As easy as it may seem to build a knowledge base, it is a constant 'Work in Progress.' Follow the below steps to build an effective KB.

Gather	Optimize	Monitor	Re-Organize
<p>Collect only necessary, helpful, and relevant information. Include both internal and external services offered by the organization. Use Infraon's Incident to KB option or create a KB (article/FAQ etc.) directly.</p>	<p>Keep your content easy to understand and searchable. Ensure that your knowledge base is seamless to navigate through. Add relevant tags to each KB article/documentation and keep the instructions simple and user-friendly.</p>	<p>Monitor and observe entered keywords, understand the usage of your end customer, and use them to enhance User Experience.</p>	<p>Tune your data and clean up your database regularly. Help customers find the information they are looking for effortlessly. Delete/archive old articles and keep your KB clutter-free.</p>

SLA Management

SLA

An SLA stands for Service Level Agreement. ITIL4 defines SLA as "A documented agreement between a service provider and a customer that defines both the services required and the expected level of service." SLA is a detailed document that defines the standards of services the customer expects from the service provider. SLAs differ across services, vendors, and industries. It is an integral part of a vendor contract because it lists the services agreed upon between the parties and the quality, availability, remedies, and penalties.

In Infraon, the "[SLA](#)" module is an SLA-capturing tool. It is not yet implemented as a full-fledged SLA Management tool. It allows the definition of SLA metrics and service details.

Benefits of SLA:

- [Sets clear guidelines and expectations](#) - An SLA sets clear guidelines regarding expectations and commitments.
- [Improved customer service](#) - Because of the existence of SLA between two parties, the service provider monitors and measures if the terms of the service are being met. Thus the team works efficiently to achieve the deadlines. There will be a decrease in ticket response time and hence improves customer service.

- **Peace of Mind** - An SLA gives peace of mind to the customer since they have a contract they can refer to in case their demands are unmet.
- **Strengthens Customer Relationships** - Above mentioned benefits enable a strong relationship between the service provider and the customer.

Two Essential Components of an SLA

The two essential components of an SLA are Metrics and Penalties.

Metrics - Metrics are the criteria for measuring services. It is an agreed-upon measurable target between the customer and the service provider. Metrics make it easier to spot SLA breaches.

***Penalty** - Penalty is a disciplinary measure to be followed in case the SLA is breached. The penalty could be imposed regarding monetary refunds, service credits, etc. These terms are captured in an SLA.

Metric

The metric tab is used to create specific conditions so that the SLA calculations start, pause, resume, and stop at the right times. To add a Metric, go to the [SLA module](#) -> [Metric](#) -> [Add Metric](#) -> [Ticket](#).

Add the following details:

Label	Action	Description/Example
Name	Name of the Metric.	Give a name for the Metric.
Criticality	Select the criticality of the Metric.	Suppose there are many parameters, the system will know which metric to follow with the help of 'Criticality'.
Description	Description of the Metric.	
Start Condition	Start Condition enables a user to specify the condition under which the SLA will be attached to the ticket and begin metering. Start conditions can be configured to capture the SLA starting from when the ticket was first created or when the ticket was assigned from one team to another.	Suppose a ticket was assigned to team A, and the team realizes it is not in their domain and assigns it to team B. In such cases, *OLA guidelines help manage the SLA timelines.
Close Condition	Close Condition enables a user to specify the condition under which the SLA completes.	
Pause Condition	Pause Condition enables a user to specify the conditions under which the SLA metering will be paused.	

Resume Condition	Resume Condition enables a user to specify the conditions under which the SLA will resume the metering. The Resume Condition option will be enabled only if the Pause Condition is specified.	
Cancel Condition	Cancel Condition enables a user to specify the conditions under which the SLA will be canceled.	

*OLA - An OLA stands for Operational Layer Agreement. An OLA is an internal agreement in which a service provider defines the guidelines for internal teams to meet SLAs.

Once the SLA conditions are specified, click on the '[Submit](#)' button to create the Metric.

Profile

An SLA Profile defines the objectives regarding the quality of service and performance. For example, a Gold profile customer may get a quicker response and resolution than a Silver profile customer. An SLA profile consists of SLA Type, Service Level Targets, and the conditions under which these targets are applicable.

To add an SLA Profile, go to the [SLA module](#) -> [Profile](#) -> [Add SLA Profile](#) -> [Ticket](#). There are three tabs under which the details of a profile are captured.

Profile Details

In Profile Details, one can specify basic details of the profile like name, type, description, start and end dates, and so on. The description of the fields is given below:

Label	Action	Description/Example
Name	Name of the SLA profile.	Give a name for the SLA profile. For Example, Gold, VIP, and Platinum.
SLA Type	Select the type of the SLA.	<p>Service - define the quality of service offered.</p> <p>Performance - define the availability of the services.</p>
Status	Select the status of the profile.	The status of the profile can be Active or In-Active.

Compliance Target	Set the compliance percentage.	A compliance target is the percent of the performance of the SLA to check if the terms were met over a period of time.
Start Date	Start Date of the SLA	
End Date	End Date of the SLA	
Description	Describe the SLA profile.	

Service Level Target

In this tab, the commitments made by the service provider in terms of availability, response, or resolution times are captured.

- **Business Hours Profile** - Business hours can be defined as the daily working hours of teams/departments within the organization. Select the business hours profile from the drop-down. The business hours can be configured in [Infraon Configuration](#) -> [General Settings](#) -> [Business Hours](#) -> [Add Profile](#).
To know more about Business Hours, click [here](#).
- **Target Profile** - In this section, metrics for response and resolution times can be defined. Go to [Target Profile](#) -> [Add New Profile](#).

Label	Action	Description/Example
Target Profile	Specify a name for the target profile.	
*Select Metric	Select the type of the Metric.	<p>Examples of metrics:</p> <ul style="list-style-type: none"> • Response - Define the time duration within which the customer can expect a response/acknowledgment based on the 'Priority' of the ticket. • Resolution - Define the time duration within which the customer can expect a resolution for the ticket based on its 'Priority.'
Business Hours	Define the number of minutes, hours, or days required to respond/resolve a ticket based on its priority.	Suppose a ticket with a priority of 'Critical' is newly created, and the response metric is set at 10 mins. The service desk has to respond/acknowledge within 10 mins to the customer.

*Non-Business Hours	Define the number of minutes, hours, or days required to respond/resolve a ticket based on its priority during non-business hours.	
----------------------------	------------------------------------------------------------------------------------------------------------------------------------	--

*Non-Business Hours are optional.

*Metrics are derived from the Metrics tab of the SLA module. Custom metrics can be defined for conditions like Start, Pause, Resume, etc.

Applied For

In the '[Applied For](#)' tab, a user can specify the conditions under which the SLA metrics are applicable.

After entering all the details, click '[Submit](#)' to create the SLA Profile.

An SLA Profile can be edited or deleted after it is created. [Deleting an SLA Profile is an irreversible action.](#)

Default SLA

Customize default metrics like response and resolution times, and tailor them to your specific operations. Improved flexibility with predefined business hours and effortlessly applied services to meet the unique requirements.

Geomap

Geomap allows for visualization of the location of all the assets by associating a geographic area with GPS coordinates. Geomap enables you to visualize the location of the assets and also provides information about the working condition of these assets.

Geomap makes managing assets, identifying opportunities, and providing quick service easy. If the technician's location matches the asset location, it becomes straightforward to assign the technician and, in turn, results in a quick resolution. Prompt service, in turn, enhances the customer experience.

What you see on the screen

Label	Action/ Description
Save	Click to save the current map view in the network diagram.
Rescan	Click to rescan the map view.
	Click to see the map in full-screen for a wider view.

The following information is shown when the mouse pointer hovers over a geomap location:

Name	Description
State	Name of the state(territory). Example: Karnataka, Tamil Nadu
District	Name of District. Example: Jalalsar, etc.
Total Sites	Total number of sites in the state with the assets.
Total Devices	Total number of locations in the state with the assets.
Maintenance	Number of assets that are in the maintenance condition.
Up Devices	Number of assets that are up and in running condition.
Down Devices	Number of assets that are not reachable.
Disabled Devices	Number of assets that are in "Disabled" status.
Unknown	Number of assets whose status is not known.

The geomap pins show different colors based on the status of the nodes. The meaning of these colors are:

Color	Description
Green	All the nodes are up and running.
Orange	One or more nodes are in "Disabled" status.
Gray	If all the nodes are in "Disabled" status.
Red	If all the nodes are down.

The maps can be viewed in the following types:

View

- OSM
- Google Roadmap
- Google Terrain
- Google Altered Roadmap
- Google Satellite
- Google Terrain Only
- Google Hybrid
- Bing Road
- Bing Aerial
- Bing Aerial with Labels
- Bing Road Dark
- Offline Map

Sort By

- City
- District
- State
- Country

Network Diagram

A network diagram is a pictorial representation of a network. It shows the various components that make up a network and how these components interact with each other. A network diagram typically consists of routers, devices, hubs, firewalls, etc.

The Network Diagram module of Infraon is a diagram creator tool like MS Visio, with drag-and-drop icons that can be used to depict the complete network and assets. It provides multiple options to map devices and components to the specific icon.

The user will be able to access, add, edit, clone, and delete the Network Diagrams only if those privileges have been given by the administrator. The privileges will be defined under Roles and Privileges.

How does it work?

Users can add, edit, and delete network diagrams. Infraon supports exporting network diagrams in PDF and JPG formats.

What you see on the screen

The network diagram page has options to add new network diagrams and view, edit, and delete existing ones.

Label	Action	Description/ Example
Search	Search for the required Network.	
Filter	Filter can be added based on the field and condition from the drop-down box below.	Field (Creator, Description, Name) and Condition (in, not in, equal to, not equal to)
Add Network Diagram	Click to add a new network Diagram	Follow the below steps to add a new network diagram.
Name		Name for the chosen network diagram.
Description		Description of the Network diagram.
Creator		Name of the user, who have the created this network diagram.
Action		
Edit		Click to edit the network diagram.
Clone		To clone the network diagram.
Delete		To delete the network diagram.

Instructions to Add Network Diagrams

Click on '[Add Network Diagram](#)' in the top right corner. This action allows the creation of a Network Diagram and the arranging of the devices, interfaces, and servers in the required network diagram.

- A developing window appears with default tools and shapes required to create a diagram.
 - The center of the page is the worksheet used to create the Network Diagram.
 - The Left panel consists of objects and shapes required to configure the node.
 - A Tool Bar with options to Zoom in, Zoom Out, Fill, edit, etc., is available on the top panel.
 - Click on the plus symbol to insert a link or an image.
 - Use the Right panel to manage extended properties of the shapes added in the Network Diagram.
- Click on a shape to add it to the Network Diagram.
 - Right-click and select '[Edit Data](#)' to customize the device label and add properties. Click '[Apply](#)' to save.
 - Right-click on a particular device to view the Node and Event Options (based on the '[Edit Data](#)' settings).
- Click [File](#) -> [Save](#) to save the Network Diagram. The '[Save](#)' window appears. Provide the required details and click the '[Save](#)' button.
- The saved Network Diagram is displayed on the dashboard.
- The color of the devices will be displayed based on the status of the device.
 - **Red** - if the status of the device is '[Down](#)'
 - **Green** - if the status of the device is '[Up](#)'
 - Gray - if the status of the device is '[Unknown](#)'

The network diagrams can be viewed, edited, cloned, or deleted from the dashboard. Click on the name of the network diagram to view it.

Click '[Export View](#)' to export the diagram in '[PDF](#)' or '[JPG](#)' format.

Network Planning

Network Congestion – Traffic Congestion

The network congestion tool diagnoses areas experiencing high traffic volume beyond capacity. The network planning tool allows strategic placement of new services by leveraging underutilized pathways.

What you see on the screen

Label	Action	Description/ Example
Search	Search for the required Network.	
Filter	Filter can be added based on the field and condition from the drop-down box below.	Field (City, Device Type, EMS Name, Host Name, IP Address, Make, Region, Ring Name, State) and Condition (in, not in, equal to, not equal to)
Locate Node	Select from the drop-down box.	The selected number of neighbors will be displayed.
Profile	Select from the drop-down box.	Select a profile for the required network.
Topology Type	Select from the drop-down box.	Select a topology which can be viewed (Single Topology, Higher Topology and Traffic).
Usage	Select from the drop-down box.	Weekly, Monthly and Quarterly.
Utilization	Select from the drop-down box.	Select the preferred utilization required (<10%, 10%-25%, etc...)
Arrows Key		Icons can be used to navigate through the topology diagram.
Zoom Key		Icons can be used to navigate through the topology diagram.

Node Capacity Utilization

Node Capacity Utilization is a valuable tool for network administrators, empowering them to optimize network performance, ensure service quality, and plan for future growth. See how various types of ports (e.g., Ethernet, VCG, STM, E1) are being utilized within each node. This helps prioritize critical traffic and strategize resource allocation.

What you see on the screen

Label	Action	Description/ Example
Search	Search for the required Network.	

Filter	Filter can be added based on the field and condition from the drop-down box below.	Field (Name, IP Address) and Condition (in, not in, equal to, not equal to)
Export	Choose your export format: Download the topology as a separate CSV file or an Excel-compatible XLS file.	
Name		Name of the Node.
IP Address		Indicates the IP Address (192.168.52.11, 192.168.52.77, etc.)
E1		E1, also known as Primary Rate Digital Service (PRDS), is a digital telecommunications standard widely used in Europe and parts of Asia.
STM		Synchronous Transport Module.
Ethernet		Indicates the Ethernet port number.
VCG		VCG stands for Virtual Container Group. It is a concept used in Synchronous Digital Hierarchy (SDH) networks, which is built upon the STM standard. It allows flexible allocation of bandwidth based on traffic requirements within the network.

Topology

Topology View

Topology refers to how various nodes, devices, and connections on your network are physically or logically arranged in relation to each other. Topology View displays the complete topology of all the connected devices in the network. The connections are configured to change colours automatically based on the faults or thresholds.

Node:

Clicking on the node shows the inventory details about the selected node.

Node Devices:

- SDH MUX

- Routers
- SDH EMS Firewall
- PDH MUX

On the right click of the node, it shows the Device View, Active Events, and Services.

Below are the details which can be viewed:

- Host Name
- IP Address
- Make
- Model
- Device Type
- EMS Name
- Firmware Version
- Region
- State
- City
- Location

Properties

The colours on the Node indicate the status of the device, which depends on the severity of the operation.

Blue -> **Grey** -> **Green** -> **Yellow** -> **Orange** -> **Red** -> **Dark Red**

(**Green** for Up, **Red** for Down, and **Grey** for Disabled devices).

Edge:

Clicking on the edge shows the connection details and the current performance parameters between the connected nodes, depending on the type.

Below are the details which can be viewed:

- Description
- Source IP
- Source Device
- Source Port
- Destination Ip
- Destination Device
- Destination Port
- Layer Rate
- Active Events (Click to redirect to the **Active Events** page)
- Services (Click to redirect to the **Services** page)

What you see on the screen

Label	Action	Description/ Example
-------	--------	----------------------

Filter	Filter can be added based on the City and Condition from the drop-down box below.	
Locate Node	Locate a Node from the drop-down. Select the No. of hops, using the drop-down menu. The selected number of neighbors will be displayed.	
Profile	Locate a Profile from the selected drop-down box.	
Vendors	Locate a Vendor from the selected drop-down box.	
Stop Auto Reload	Click to Stop (Default is Auto).	It reloads the topology view at every interval of 60 seconds.
Export	Creates a PDF of the current topology view.	
Edit	To save a new topology profile or a new topology view. Drag nodes to adjust the view.	
Arrows Key	Icons can be used to navigate through the topology diagram.	
Zoom Key	Icons can be used to navigate through the topology diagram.	

Note: The thickness of the interface indicates the offered Bandwidth.

Topological Links

What you see on the screen

Label	Action	Description/ Example
Filter	Filter can be added based on the Field and Condition from the drop-down box below.	
Add	For new topologies, you can choose the guided 'Add topology' option or	To add a new Topology.

	manually import data from a CSV file.	
Export	Choose your export format: Download the topology as a separate CSV file or an Excel-compatible XLS file.	To Export the configuration
Edit		To Edit the changes to a Topology.
Trace Test	Click to enter the details in the respective call-out boxes. (Link Name, Description, Source Node, Source Port, Destination Node, Destination Port, Layer Rate, Direction, Ring Name)	It uses trace data to improve assertion capabilities and validate relationships between two nodes.

Steps to add a topology

Method 1: Manually

- Go to the Infraon OSS page; on the left panel, click on the Topology -> Topological Link.
- Navigate to Add -> Add Topology, enter the details, and click on Submit.

Label	Action/ Description
Link Name	Add a name for the Link.
Description	Provide a brief description of the topology.
Source Node	Select from the respective drop-down box.
Source Port	Select from the respective drop-down box.
Destination Node	Select from the respective drop-down box.
Destination Port	Select from the respective drop-down box.
Layer Rate	Select the OSI (Open System Interconnection) layer.
Direction	Bi-directional/ Unidirectional
Ring Name	Select a Ring for the Topology.

Method 2: CSV File

- Go to the Infraon OSS page; on the left panel, click on the Topology -> Topological Link.
- Navigate to Add -> CSV File
- Download the CSV file and enter the details required.
- Upload the same CSV file and click **Next**.
- Confirm the selected column matching and click **Import**.
- Validate the CSV file and click **Proceed with valid records**.

To Export the configuration, click on the 'Export' icon at the page's top right corner.

Infraon Configuration

The Infraon Configuration module consists of all types of configurations required for the efficient functioning of modules. While there are multiple levels of configurations, few of these configurations are mandatory.

[General Settings](#)- Configure business hours, create tags for grouping assets, users, etc. and go through the complete audit log.

[User Management](#) - Invite requesters and users, assign roles, group them as teams or departments, and view their leave information.

[Service Management](#) - Configure technical and service catalogues to offer services and products seamlessly through the self-service portal.

[Notifications](#) - Configure and track notifications sent through Infraon.

[Infraon Automation](#)- Configure workflows within Infraon to define a flow of process modules like Incident, Request, Etc.

[Bots](#) - Install agents to enable discovery and monitoring.

[Organization](#) - View and add organization and branch locations.

[IT Operations](#) - Add device credentials to initiate the discovery of devices.

[Vendor configuration](#)- Customize the multiple tasks in the vendor configuration module, access various details about the vendors, display them in the address book, easily edit or delete them and utilize them on the software license page for efficient management.

[Infraon Platform](#) - Check and edit account configuration settings.

Additional Configurations

There are a few additional configurations that are needed to enable the monitoring of devices. Follow the instructions in the below links to enable protocols as required.

[Enabling SNMP in Cisco Routers/Switches](#)

Pro feature in Infraon configuration

Upgrade Option for Credential-less Organizations! Users can access the management portal for service selection. Selected services are enabled post-payment, with 193 options.

Enable SNMP Configurations in Cisco Routers and Switches

Enabling SNMP is vital to initiate monitoring of the routers and switches. Follow the below steps to enable SNMP in Cisco routers and switches.

- Connect to the router/switch via telnet.
 - prompt#**telnet testrouter**
- Now, enter the password to enter the enable mode.
 - Router>**enable**
 - Password:
 - Router#
- The next step is to configure your device:
 - Router#**configure terminal**.
Enter one configuration command per line and finish each line with CNTL/Z.
Router(config)#
- Add the Read-Only community string using the following command.
 - Router(config)#**snmp-server community public RO** ('Public' is the Read-Only community string here)
- For a Read-Write community, use the below command.
 - Router(config)#**snmp-server community private RW** ('Private' is the Read-Write community string here).
- You can now exit the configuration mode and save the settings
 - Router(config)#**exit**
Router#**write memory**
Building configuration...
[OK]
Router#

General Settings

The general settings module is a part of Infraon Configuration and is accessible by administrators and other users authorized by administrators.
This module of Infraon consists of three additional modules. They are:

- [Audits](#) - Infraon monitors and records all actions of every user. Only the administrator can access these audits.
- [Business Hours](#) - Configure business hours to control SLAs and efficient work allocation better.
- [Tag Management](#) - Tagging is a way of grouping assets, users, etc. Tags can be applied to multiple categories across Infraon.

Let's see each of these in detail.

API Registration

APIs or Application Programming Interfaces are added to enable data exchange between Infraon and computers/programs/applications. API integrations are possible with other third-party applications and web services supporting HTTP protocol.

Infraon supports REST API. REST stands for *Representational State Transfer* that adheres to REST architectural constraints. REST serves as a bridge between the client and the server, allowing communication over HTTP. It enables servers to cache responses, resulting in improved application performance.

The REST-API serves as a single point of entry into the system. Before granting access to the application's resources, it encapsulates the business logic and processes all client requests, including authorization, authentication, data sanitization, and other necessary tasks. Infraon supports the below content types:

- application/json
- application/x-www-form-urlencoded
- txt/plain

APIs use authorization to secure client requests accessing data. While integrating third-party APIs, these credentials are provided by the respective API provider. Based on the API, you can select one of the below Auth Types:

- API Key - Uses a key-value pair in the API's request headers or query parameters.
- Basic Auth - Uses a verified username and password with the request.
- Custom Auth - Uses token-based authorization that requires CSRF URL, token, key, username, and password with the request.
- No Auth - Uses when there is no authorization to request data.

API Supported Operations

- Requests
- Sites
- Technicians
- Assets
- Worklog

Instructions to 'Add API'

- Go to Infraon Configuration -> General Settings -> API Registration
- Click the 'Add API' button

Label	Action	Description/Example
Name*	Give a name to the API.	ITSM API, For NMS, etc.
Content-Type*	Select API content type using the drop-down menu.	
Authentication Type*	Select authorization type from the given option.	Additional fields appear based on the selection. Refer to the below section for auth-type-based fields.
Base URL*	Add base URL	
Description	Add a brief description of the API	
Header Parameter	Use the 'Add Parameter' button.	Add Key, Value, and enable the Query Parameter, if required.

Auth-Type Fields

- API Key - Auth Key, Auth Value, and Add Key to (Header/Query)
- Basic Auth - Username and Password
- Custom Auth - Token details, Key, Request Type (GET, POST), Username, and Password
- No Auth - No credentials required.

Once all the parameters are added, click 'Submit' to add the API. APIs can be edited or deleted using the respective icons.

Audits

Infraon records all automated and manual activities that occur within. All these are saved within the tool as Audits.

Audit records information of the user, the action performed, the IP address, and the time stamp when the action was performed.

No actions can be performed from this page.

Business Hours

The daily working hours of teams/departments within an organization are referred to as business hours. This, in turn, aids in the assignment of work based on users working hours, as well as the setting and meeting of SLAs.

Add a Business Hour Profile

When creating a profile, you could choose between specific working days/hours and 24/7 availability.

Use the Exclude hours option to add a break in the business hours. This can be the weekend, an official lunch hour/break time, or a change in the Technician's shift. SLAs are adjusted as needed.

To view the complete list of holidays applicable to your region, add '[Holiday](#)' or click on import holidays. '[Exclude hours and Holidays](#)' are excluded while calculating SLAs for the ticket.

Instructions to 'Add a Business Hour Profile'

- Go to Infraon Configuration -> General Settings -> Business Hours.
- Click the '[Add Profile](#)' button

Label	Action	Description/Example
Profile Name*	Give a name to the Business Hour Profile.	Support Team, Main Branch, Tech Support
Description	Add a brief description of the profile.	Tech support team from the Head Office.
Timezone	Select Timezone applicable for the profile.	Select 'Timezone' based on the team's work location. Multiple business profiles can be created to align to SLAs of multiple teams supporting multiple locations.
Work Hours	Use the option to select if the team works 24*7 or selected working days/hours. 24*7 - Select exclude hours for your team. Select Working Days/Hours - Select weekdays, start and end times. The selected days and hours are taken as official working hours for the organization/team.	For the 'Select Working Days/ Hours' option, there is an option to add multiple Business Hour profiles. This can define business hours on weekends (Saturday/Sunday) or other holidays.
Exclude Hours	Add a reason and select weekdays, start, and end times to add exclude hours.	This can be the weekend, an official lunch hour/break time, or a change in the technician's shift. Use the 'Add Exclude Hours'option to add multiple instances.

		'Exclude Hours' are excluded while calculating SLAs.
Yearly Holiday List	Add Date and Holiday Name to add a specific day as a holiday.	To view the complete list of holidays applicable to your region, add 'Holiday' or click on import holidays. 'Holidays' are excluded while calculating SLAs for the ticket.

Once all the parameters are added, click '[Submit](#)' to save the profile. Business Hour Profiles can be linked to SLA, Reports, and Discovery. Please refer to the respective module for more details.

Repeat the process to add multiple profiles. Business Profiles can be edited or deleted using the respective icons.

Tag Management

Tags are simplified identification keywords used to group items or users within Infraon. Tags can be applied to users, assets, Incidents or requests, articles, etc.

Tag Types

Tagging enables quick grouping of items/users. At this point in time, tags are be added for:

- [Assets](#) - Tag assets by brand, vendor, location or technician, etc.
- [Users](#) - Tag users by the team, skills, location, service catered, etc.
- [Expertise](#) - Tag teams (team creation) with expertise like Hardware, Python, Django, or product expertise like washing machines, TV, etc.
- [Services](#) - Tag services by team, location, category, classification, etc.
- [Incident](#) - Tag incidents by the team, technician, site, catalogue, criticality, device, etc.
- [Requests](#) - Tag incidents by the team, technician, site, catalogue, criticality, device, etc.

How to use a tag effectively?

In a business where the end-users call from multiple locations for support on laptops and desktops, asset tags such as Laptop, Desktop, NY, AU, and IND can be used to assign these incidents to technicians tagged as Laptop, Desktop, NY, AU, and IND.

Instructions to 'Add a Tag'

- Go to Infraon Configuration -> General Setting -> Tag Management
- Click the "Add Tag button"

Label	Action	Description/Example
Tag Name*	Give a name to the tag	Laptops, Desktops, IT, HR, India, NY, etc.
Type*	Select tag type using the drop-down menu.	Refer 'Tag Types' section above for detailed information

Once both the parameters are added, click '**Submit**' to save the tag.

Repeat the process to add multiple tags. Tags can be edited or deleted using the respective icons.

Note: Assigned tags cannot be deleted.

Instructions to 'Assign a Tag'

Asset Tag

Here are the 7 methods you can assign the asset tag.

Method 1: Single Asset

- Go to Infraon Asset Card page -> Select the asset-> (:) More -> Edit
- Enter the required details, add the tag in Asset Tag, and click **Next**.
- Check the details in Asset Properties and click **Submit**.

Method 2: Bulk- Card/ Grid View

- Go to the Infraon Asset Card page -> Select multiple Assets.
- Click on **Tag** at the center of the top panel. Click on "**Yes, Edit it.**"
- Name your Tag and click **Submit**.

Method 3: Bulk Edit

- Go to the Infraon Asset Card page -> Actions -> Bulk Edit.
- Select the Category.
- Download the CSV file (excel sheet) and Enter the Tag name in the sheet.
- Upload the same edited CSV file.
- Click **Next** -> **Import** -> **Proceed with Valid Records**.

Method 4: Tags can be assigned directly while adding an asset.

- Go to the Infraon Asset Card page -> Add Item -> Single Asset
- Add the required details to add the asset.
- Select the Tag in the **Asset Tag** section.
- Click **Next** -> **Asset Properties** -> **Submit**.

Method 5: Manually from CSV file (excel sheet)

- Go to the Infraon Asset Card page -> Add Items -> Import from CSV
- Select the required Category and download the CSV file.
- Enter the Tag name in the sheet, use semicolon (;) to add multiple tags at a time Eg: SHQ;BHQ
- Upload the same edited CSV file.
- Click **Next** -> **Import** -> **Proceed with Valid Records**.

Method 6: Asset details page

- Go to the Infraon Asset Card page -> Select the Asset Name and redirect to the **Details** page.
- Locate the Tags button in the centre of the page, near the left panel.
- Click to proceed to Add the required tags.

Method 7: Import from CSV

- Go to Infraon configuration page -> IT Operations -> Discovery -> Automatic Discovery.
- Click the "Import from CSV" button at the bottom centre of the page.
- Download the CSV file (excel sheet) and Enter the Tag name in the sheet.
- Upload the same edited CSV file.
- Click **Next** -> **Import** -> **Proceed with Valid Records**.

Resource Tag

Method 1: Bulk

- Go to the Infraon Asset Card page -> Select the Asset Name and redirect to the **Resource** page.
- Check the boxes next to the resources you need to tag.
- Click on the Add Tag option, add the required tag, and click **Submit**.

Method 2:

- Go to Infraon configuration page -> IT Operations -> Advance Resource Configuration.
- Click **Configure**.
- Navigate to the top right corner and click Actions -> Tag.
- Add the required Tag.

Method 3: Advance configuration (CSV file)

- Go to Infraon configuration page -> IT Operations -> Advance Resource Configuration.
- Click **Configure**.
- Click the "Export" button in the top right corner.
- Clicking the button downloads the CSV file immediately (a pop-up may appear).

- Enter the Tag name in the sheet.
- Now navigate to the Infraon configuration page -> IT Operations -> Advance Resource Configuration.
- On the top right corner, click **Bulk Resource Update**.
- Upload the same edited CSV file.
- Click **Next** -> **Import** -> **Proceed with Valid Records**.

Owner/ User Tag

Method 1: Single

- Go to Infraon Asset Card page -> Select the asset-> (:) More -> Edit
- Enter the required details, add the tag in Owner Tag, and click **Next**.
- Check the details in Asset Properties and click **Submit**.

Method 2: Bulk Edit

- Go to the Infraon Asset Card page -> Actions -> Bulk Edit.
- Select the Category.
- Download the CSV file (excel sheet) and Enter the Tag name in the sheet.
- Upload the same edited CSV file.
- Click **Next** -> **Import** -> **Proceed with Valid Records**.

Method 3: Bulk- Card / Grid View

- Go to the Infraon Asset Card page -> Select multiple Assets.
- Click on **Tag** at the center of the top panel. Click on "**Yes, Edit it.**"
- Name your Tag and click **Submit**.

Method 4: Import from CSV

- Go to Infraon configuration page -> IT Operations -> Discovery -> Automatic Discovery.
- Click the "Import from CSV" button at the bottom center of the page.
- Download the CSV file (excel sheet) and Enter the Tag name in the sheet.
- Upload the same edited CSV file.
- Click **Next** -> **Import** -> **Proceed with Valid Records**.

User Management

User Management is a part of Infraon Configuration and is accessible by administrators and authorized users. User management is where you manage users and define their role and access level across modules of Infraon.

The User Management module of Infraon consists of six additional modules.

They are:

[Users](#) - Invite new users or edit/delete existing users.

[Roles & Privileges](#) - Create new roles or edit/delete existing roles and define privileges for roles.

[Requesters](#) - Create special accounts for end-users to raise Incident or Change requests.

[Teams](#) - Create teams of users with similar skills for ease in assigning tasks to enable collaboration and mutual support.

[Department](#) - Create departments, assign team members and align them with managers.

[Password Policy](#) - Create a password policy to enhance security and meet compliance standards.

[My Leave](#) - View and apply leave of absence from work.

[Leaves](#) - View Holiday List and leave categories as per organizational policy.

Department

Departments are created within Infraon to group users in a logical way to suit the organization's requirements. Assigning departments to help align teams to workflows, thereby assigning tickets, tasks, and prioritization of work.

In short, Departments are added for efficient assignment of work and management of teams.

Users can be part of multiple departments at the same time.

Add Department

Click on the '**Add Department**' button in the top right corner. Provide a department name, select a department head and a prime user and save.

***Department Head** - Can be managers or business owners who are decision-makers or otherwise known as high-level approvers.

***Prime User** - can be team leads or a senior member of the team who is in charge of the allocation of work. They are the primary responsibility owners and have basic approval privileges too.

Instructions to 'Add a Department'

- Go to Infraon Configuration -> User Management -> Department
- Click on the 'Add Department' button.

Label	Action	Description/Example
-------	--------	---------------------

Department Name*	Give a name to your Department password policy.	Incident Management, Finance, HR, etc.
Department Head	Select a user using the dropdown menu to make them the department's head.	Department Heads can be managers or business owners who are decision-makers. They are otherwise known as high-level approvers.
Prime User	Select user(s) using the dropdown menu to make them the department's head.	Prime User(s) can be team leads or a senior member of the team who is in charge of allocating work. They are the primary responsibility owners and have basic approval privileges too.
Description	Add a brief description of the department.	Handles tickets, Manages payroll and taxation, For new hire onboarding, etc.

Once all the parameters are added, click '[Submit](#)' to save the department. Repeat the process to add multiple departments. Departments can be edited or deleted using the respective icons.

Active users

Active users are individuals who are currently logged in and actively engaging with activities. They represent the real-time presence of people who are currently using the system, indicating their availability for interaction or collaboration.

From this page:

- You can see a list of users who are currently online.

Note: No actions can be performed from this page.

Leaves

Displays multiple categories of leaves available within the organization—filter information based on Leave Types or User.

The Calendar on the right displays leaves taken by the team for the selected period (Month/Week/Day).

What you see on the screen

Administrators or privileged users can configure leaves, i.e., configure/allot limit or no. of leave days applicable for each category. Leaves taken by users are

displayed in a calendar view with options to view week/day/list. Filters can be applied to both leave types and users.

Instructions to 'Configure Leaves'

- Go to Infraon Configuration -> User Management -> Leave
- Click on the 'Configure' button.

Label	Action	Description/Example
Leave Type - Number of Days	Add a number in the Number of days column of the respective leave type.	This data must be based on the leave policy of your organization.

Once all the details are added, click 'Update/Configure' to save. Once configured, users can see the leaves and apply for the necessary type, as required.

My Leaves

Displays leave details of the logged-in user. Users can view multiple categories of leaves available within the organization, apply for leave and check available leave balance as on date.

What you see on screen

Leave categories with information on the number of leaves available vs. the number of leaves taken.

Use the '**Apply Leave(s)**' button to apply for leave(s). Select date or date range, leave type, and specify a reason. Click 'Apply.'

Leave Type must be pre-defined by the administrator.

Instructions to 'Apply Leave'

- Go to Infraon Configuration -> User Management -> Leaves
- Click on the Apply Leave(s) button.

Label	Action	Description/Example
Leave Date*	Choose a date or range of dates you want to apply for leave.	Leave days are auto-calculated based on the selection.
Leave Type	Select leave type using the dropdown menu.	Leave type must be pre-configured by the administrator.
Reason*	Add a reason for leave.	The reason is a mandatory field.

Click '[Submit](#).' Leave requests are submitted to the reporting manager for approval. Users can edit leave requests as long as they are not approved.

Password Policy

Passwords are mandatory to verify user identity (authentication) and protect information. It is crucial to have more robust password policies across Organization.

Infraon can be configured with multiple Password Policies to suit the organization's internal and external compliance. Different password policies can be configured for various roles.

What you see on the screen

The Password Policy page can be used to create new policies and edit and delete existing policies.

Instructions to 'Add a Password Policy'

- Go to Infraon Configuration -> User Management -> Password Policy
- Click the 'Add' button.

There are two tabs on the 'Add Password Policy' page.

Policy Details tab contains options to customize passwords, including Password Length, Upper/Lower Case, Numbers, Symbols, Frequency to Change Password, etc. The applicability tab lets the user choose the privacy level of the policy.

Policy Details | Applicability

Label	Action	Description/Example
Policy Name*	Give a name to the password policy.	Vendor Team, Requesters Only.
Description*	Add a brief description of the policy.	Assign to the external vendor team; This is for requesters only.
Change Password Every N Day(s)	Enter the number of days until the password needs to be changed.	Users are reminded to change their passwords every (n) day by Infraon.
Last-Used Password Count	Enter the count of last used passwords that are considered for non-repetition.	If the number '4' is entered, Infraon will not enable users to use the previous four passwords when changing or resetting their passwords.
Minimum Password Length	Enter the minimum number of characters for the password length.	If the minimum password length is set to '8', Infraon will only accept passwords at least eight characters long.

Maximum Password Length	Enter the Maximum number of characters for the password length.	If the maximum password length is set to '20', Infraon will only accept passwords less than twenty characters long.
Minimum Upper Case Characters	Enter the minimum amount of uppercase or capital letter characters required in the password.	If the minimum upper case character length is set to '2', Infraon will only accept passwords with two uppercase characters (neither one nor more than two).
Minimum Lower Case Characters	Enter the minimum amount of lowercase or minor letter characters required in the password.	If the minimum lower case character length is set to '2', Infraon will only accept passwords with two lowercase characters.
Minimum Numerals	Enter the minimum amount of numerals or numeric characters required in the password.	If the minimum numerals are set to '2', Infraon will only accept passwords with two digits (neither one nor more than two).
Minimum Special Characters	Enter the minimum amount of special characters required in the password.	If the minimum unique character is set to '2', Infraon will only accept passwords with two special characters (neither one nor more than two). Special characters include
Continuous N Upper Case Characters	Enter the count of continuous upper case characters allowed in the password sequence.	If the continuous upper case character is set to 1, Infraon will not allow more than one upper case character in the password sequence. For example, Eims would be accepted, whereas EIMS would not.
Continuous N Lower Case Characters	Enter the count of continuous upper case characters allowed in the password sequence.	If the continuous lower case character is set to 3, Infraon will not allow more than three lower case characters in the password sequence. For example, Eims would be accepted, whereas eims would not.

Continuous N Numerals	Enter the count of continuous numerals or number characters allowed in the password sequence.	If the continuous numeric character is set to 3, Infraon will not allow more than three numeric characters in the password sequence. For example, Eims123 would be accepted, whereas Eims1234 would not.
Continuous N Special Characters	Enter the count of special characters allowed in the password sequence.	If the continuous unique character is set to 2, Infraon will not allow more than two special characters in the password sequence. For example, Eims@123! would be accepted, whereas Eim\$@1234 would not.

Fields marked with * are mandatory.

Click 'Next' to configure password policy applicability.

[Policy Details](#) | [Applicability](#)

Label	Action	Description/Example
Roles	Select a role to apply the password policy.	Vendor Team, Requesters. Roles must be pre-defined to be available for selection.

Fields marked with * are mandatory.

Once all the parameters are added, click '[Submit](#)' to save the password policy. Password policies can be linked to newer roles.

Administrators and privileged users can edit and delete policies using the respective icons.

Note: Password policies must be de-linked from roles to be deleted.

The default password policy cannot be deleted.

Requesters

Requesters can be internal or external users. Infraon enables Technicians (Tech Support User/NOC Operator) to raise an incident/request on behalf of the requester.

Requesters can be enabled with access to the Infraon Requester Portal, allowing them to raise incidents, service requests, and change requests. Requesters can also access the Knowledge Base.

What you see on the screen

The requesters' page view can be toggled between List View and Card View using the button next to the '**Invite Requester(s)**' button.

Details displayed are as follows:

- Username
- Mobile
- Requester Type
- Department
- Status
- Action

Edit and delete action icons are available for each list item or card (on mouse hover). Requester status must be 'Active' to log in to Infraon.

Invite Requester(s)

There are two ways to add Requesters onto Infraon - Invite and Add. Click on the 'Invite user(s)' button on the top right corner.

Enter mail address(es) and select role using the dropdown menu. Multiple requesters can be invited in a single instance.

The invite link expires in 36 hours (can be changed in settings). New invites must be sent to re-invite requesters.

Instructions to 'Invite a Requester'

Click on the 'Invite Requester' button.

Label	Action	Description
Enter Requester's Email ID	Add the email address(es) of the requester(s) you wish to invite onto Infraon. Separate multiple addresses using a semicolon (;) or a comma (,)	John.doe@company.com; Jane.doe@company.com; This email address will be used for future communications with the requester.

Click on the '**Invite.**' Administrators and other privileged users can see the status of pending invites and resend them using the pending notifications icon.

Instructions to 'Add a Requester'

- Go to Infraon configuration on the left panel and navigate to User Management -> Requester.
- Now click on the "Add a Requester" located at the top panel beside the 'Pending Invitation' option.

To add a Requester, there are two options; let's see each one in detail.

Manually

Add the below details in the respective call-out boxes.

Requester Details| Fields

Label	Action	Description/ Example
Change	Click to add or change the requester's profile photo.	
Full Name	Add the first and the last name of the requester.	
Email	Add the mail address of the requester.	
Phone Number	Add the specific mobile number of the requester.	
Landline Number	Add the landline number of the requester.	
Contact Extension	Enter the shorter telephone number that can be assigned either to an individual, to a team, or to a department.	
Type	Select the type of requester.	A requester can be Internal or External. Note: If 'External' provide the organization name.
Enable Login		Configure the requester's login credentials for self-service portal access.
Is Active		This option applies if the requester is currently active and their account is in use.
User ID	Add a user ID for the requester.	

Password	Add the required password to log in.	
Time zone	Add the specific time zone the requester is available in.	
Language	Select the appropriate language.	
Enable Reporting		<p>Add the requester's reporting manager (optional) with a click of the toggle icon.</p> <p>Note: Add the reporting manager in the consecutive call-out box.</p>

Click **Submit** to create the requester. To add work details and address, click **Next**.

Work Details| Fields

Label	Action	Description/ Example
Designation	Click to add the designation of the requester.	
Department	Select the department from the drop-down box.	Technical Department, IT System, etc.
Employee Type	Select the type of employee from the drop-down.	Internal or External.
Joining Date	Add the joining date of the employee.	
Notify Email ID(s)	To notify the respective user, add the email ID.	
Notify Phone No(s)	To notify the respective user, add the mobile number.	
Tags	Select to add a tag from the drop-down box.	DevOps, Front Desk Manager, etc.
Service Hubs	Select the appropriate service of the requester from the drop-down box.	Head Office, Branch Office, etc.
Employee ID	Enter the employee ID of the requester.	

Address Details| Fields

Based on the requester's work location (Base location or Work Location), populate the address field. Choose the appropriate location from the dropdown menu. Utilize the addresses already stored in Infraon's address book.

Import from CSV

This method is used to add multiple requesters at once. Follow the below steps:

- Download the CSV file (excel sheet) and enter the requester details in the sheet.
- Upload the same edited CSV file.
- Click **Next -> Import -> Proceed with Valid Records.**

Bulk Requester Delete from UI

Bulk Delete Requesters! Remove requesters with mapped assets, ensuring ticket closure. The Owners with active tickets or associated users cannot be deleted; replace the owner in the pop-up.

Roles & Privileges

Access control within Infraon is managed through role-based privileges. A Role defines a user's role within Infraon, and Privileges define the user's level of access across multiple modules of Infraon. Infraon comes with seven default roles with pre-defined privileges.

What you see on the screen

On Infraon, there are multiple default Roles, displayed as a list with icons to edit, clone, and delete. The 'New Role' button is at the top right corner of the page.

Details displayed are as follows:

- Role Name
- User Count
- Role Description
- Icons to edit/clone/delete

Roles

While Infraon comes with seven default roles, you can edit an existing role's privileges and add a new one to suit your needs.

Role	Description
Requester	Are end-users who have access only to the requester portal from where they can raise incidents, service

	& change requests and go through the complete Knowledge Base?
Tech Support Operator	Are users part of the technical support team that provides technical support to end-users/requesters? A Technical Support Operator can access Service Catalog, Workflow, Assets, user Dashboards, and Reports. A Tech Support Operator also has privileges to add and edit Incidents.
Tech Support Manager	Are users with privileges of a Requester + Tech support operator + admin privileges to manage the assigned team? By default, a Tech Support Manager has privileges to add Fixed Assets, add/edit/delete Tech Support Operators, add/edit/delete Incidents, Dashboards, and Reports.
NOC Operator	Are users assigned to monitor the organization's network and have all the privileges of Tech Support operators? By default, a NOC Operator has complete privileges over Alarms, Events, and Notifications.
IT Support Operator	Are users assigned to monitor and provide IT infrastructure-related support? By default, an IT Support operator has privileges to add /edit Discovery Profiles, add/edit assets through Discovery/CSV (on approval), and complete privileges over Alarms, Monitoring Dashboards*, Monitoring Reports*, and Notifications.
Administrator	Are users with complete access across all modules of Infraon Note: The 'Administrator' role cannot be cloned/edited/deleted.

*Monitoring Dashboards and reports are those dashboards/reports assigned to the user to enable monitoring.

Instructions to 'Add a new Role.'

- Go to Infraon Configuration -> User Management -> Role and Privileges
- Click on the 'New Role' button in the top right corner.

Privileges for default roles are saved as templates and can be selected and customized to suit needs. Privileges are customized at the 'General,' 'Ticket,' 'NCCM,' 'Privacy Settings,' and 'Reports' levels.

Label	Action	Description/Example
Role Name*	Add a name for the new role.	Manager, Support Team, L1 Support, etc.,
Select Template	Select a template to import privileges.	Selecting existing role templates helps import privileges from an existing role to the new role.
Description	Add a brief description of the role.	Assign to L1 support members of the team.

Privileges	Select privileges to enable access to the new role.	Privileges are split into modules: General, Ticket, NCCM, Privacy Settings, and Reports. Permissions can be explicitly selected - view, add, edit, delete, copy, and configure.
-------------------	-----------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Privileges are as follows:

The Privileges module within Infraon Infinity empowers administrators with granular control over user permissions. This ensures users have the necessary access to perform their tasks effectively while safeguarding sensitive data within the platform.

Here, admins can define specific actions/modules that users can perform within each module using checkboxes. These levels include:

Label	Action	Description/Example
View	If selected, the 'View' privilege allows the user only to view the selected module/page.	For example, if the user is given the 'View' privilege to the 'Business Catalogue' module, the user will be able to view the services listed.
Add	If selected, 'Add' allows the user to view and perform add operations within the selected module/page.	For example, if the user is given the 'Add' privilege to the 'Business Catalogue' module, the user will be able to view the services listed and add new services. The user will, however, not have edit or delete privileges.
Edit	If selected, 'Edit' allows the user to view and perform edit operations within the selected module/page.	For example, if the user is given the 'Edit' privilege to the 'Business Catalogue' module, the user will be able to view the services listed and edit existing services. The user will, however, not have add or delete privileges.
Delete	If selected, 'Delete' allows the user to view and perform add operations within the selected module/page.	For example, if the user is given the 'Delete' privilege to the 'Business Catalogue' module, the user will be able to view the services listed and delete existing services. The user will, however, not have to add or edit privileges.
Copy	If selected, 'Copy' allows the user to view and perform add operations within the selected module/page.	For example, if the user is given the 'Copy' privilege to the 'Business Catalogue' module, the user will be able to view the services listed

		and add new services. The user will, however, not have edit or delete privileges.
Configure	If selected, 'Configure' allows the user to view and perform add operations within the selected module/page.	For example, if the user is given the 'Add' privilege to the 'Business Catalogue' module, the user will be able to view the services listed and add new services. The user will, however, not have edit or delete privileges.
Upload	If selected, 'Upload' allows the user to view and perform add operations within the selected module/page	
Download	If selected, 'Download' allows users to download and perform export operations within the selected module/page.	The Download privilege allows users to export logs from the Log Management module in PDF, CSV, or XLS formats, enabling offline analysis, sharing, and integration with other tools.

Here's a breakdown of the functionalities offered by the Privileges module and its sub-modules:

General:

Grant access to various Infraon Infinity modules:

- Agent
- API Registration
- Audit
- Business Hour
- Bot Configuration
- Business Rule
- Business Catalogue
- Change
- CI Relation rule
- Asset
- Contract Management
- Correlation Rule
- CSAT
- Client Registration
- Dashboards
- Department
- Device Credentials
- Diagnosis Tools
- Discovery
- Events

- Geomap
- Holiday
- IMACD
- Mail Automator
- Jobs
- Knowledge Base
- Leaves
- Maintenance
- Messenger
- My Profile
- Network Configuration
- Network Diagram
- Organization
- Address Book
- Password Policy
- Problem
- Release
- Request
- Requester
- Service Catalogue
- Shift
- SLA
- SMS Gateway
- Software License
- SSP Configuration
- Tag
- Task
- Team Escalation
- Teams
- Template
- Thresholds
- Topology
- Trigger
- Technician
- Role
- Vendor
- Workflow
- Workspace

Log Management:

Manage user access to functionalities related to Log Management and configurations. This sub-module offers permissions for:

- **Log Multi-Index:** Create and manage the multi-indexes that help retrieve data from Elasticsearch.
- **Log Export Configs:** Export Configs define how logs are exported, including format, size, and downloaded exported log files.
- **Log Search:** Enables rapid searching and analysis of vast amounts of structured and unstructured log data, delivering results in seconds.

- **Log Rule:** A critical component in monitoring systems that defines how log data is processed and analyzed in real-time to detect and respond to security threats quickly.

Ticket:

Define permission levels (Add, View, Edit, Delete, etc.) for different user roles regarding ticket management tasks. This allows for granular control over how users interact with tickets within the system.

NCCM (Network Change & Configuration Management):

Manage user access to functionalities related to network changes and configurations. This sub-module offers permissions for:

- **Baseline Scheduler:** Control access to scheduling tasks for network baseline configuration.
- **Configuration Download Job:** Manage permissions for initiating downloads of network configuration data.
- **Configuration Parameters:** Define user access to view or modify network configuration parameters.
- **Configuration Profiles:** A configuration profile is a template or predefined set of configuration settings that network administrators can create and customize configuration profiles with information like device details and connection protocols for SSH and Telnet.
- **Configuration Search:** Configuration Search specifically focuses on download jobs, allowing users to view or export the "startup" or "running" configurations within these jobs to identify any configuration.
- **Configuration template:** Configuration templates hold the commands for uploading jobs and making changes to network devices, including provisioning, OS upgrades, creating or deactivating services, and any other change.
- **OS Image:** OS images are used primarily for managing and deploying configuration changes across network devices such as routers, switches, and firewalls.

Privacy Settings:

Administrators can control the visibility of requester information for technicians working on service requests. This helps strike a balance between transparency and data privacy within your Infraon Infinity platform.

Unmask Requester's Contact: This section provides a toggle button. Enabling this option grants technicians visibility to the requester's contact information, potentially including phone numbers. This can be beneficial for situations where direct contact with the requester might be necessary to resolve an issue.

Unmask Requester's Email: Another toggle button allows administrators to control the visibility of the requester's email address for technicians. Granting access to email addresses can facilitate direct communication between technicians and requesters, potentially expediting issue resolution.

Unmask Requester's Name: The final toggle button controls the visibility of the requester's name for technicians. Enabling this option ensures technicians can easily identify the person requesting assistance.

Report:

Define permission levels (Add, View, Edit, Delete, etc.) for different user roles regarding reports. This ensures users can access reports relevant to their needs while restricting access to sensitive data as necessary.

Once all the parameters are added, click '[Submit](#)' to save and add the role. Administrators and privileged users can edit and delete roles using the respective icons.

Note: 'Administrator' role cannot be cloned/edited/deleted.

Shift Configuration

Manage user shifts effortlessly: configure shifts, set business hours, and assign team members seamlessly. Keep track of employee availability and shortages and quickly reassign tickets during scheduled shifts. Elevate the team management experience today!

Basic Shift management (Alpha)

[Basic Shift configuration with conflict detection](#)

To efficiently manage various schedules and create and supervise shifts for hourly technicians or agents. In shift configuration, select the team and define business hours, which can also be designated from the Teams module.

Specify the shift name, code, team size, and start and end dates. The corresponding days of the week will be displayed based on the chosen business hours. Adjust shift timings as needed and click 'Submit' once all necessary actions are added.

[Auto Assignment Engine update based on shift](#)

Auto Assignment in shift management refers to the automated process of assigning or allocating shifts to team members or technicians based on predefined criteria or rules.

Teams

A bunch of users is grouped as a team on Infraon. Teams can be categorized based on a reporting manager, technical skills, support level (L1, L2), role, etc.

Users are assigned to multiple teams, and teams are assigned to specific modules, i.e., a team to manage Incidents or Service Requests or an asset team, etc.

[What you see on the screen](#)

From this page, you can add new teams and edit and delete existing teams.

Instructions to 'Add Team'

Click on the '[Add Team](#)' button in the top right corner.

There are two tabs in the 'Add Team' form. At this point, three types of teams can be created on Infraon.

Approval	Operation and Technical	Service Desk
The approval team consists of users who are in charge of approving requests.	The operation and Technical team comprises users performing operational or technical tasks within Infraon.	The Service Desk comprises users who are a part of the Helpdesk/service or support team. This team is generally the first level in in-charge of tickets.

Fields marked with * are mandatory.

There are three options for selecting staff for the team.

User Tags	Users	Expertise
Select users based on the user tags (groupings).	Select users directly for the team.	Select users based on their expertise.

Infraon can be customized with sequential approvals, enabling multi-level authorization to allow a hierarchical approach.

The configuration tab is enabled when adding an Approval or an Operation and Technical Team.

Approval Team - Used to configure.

Operation and Technical Team - Used to configure auto-assignment of tickets.

What is Auto Assignment?

An alert is raised when a ticket lands in the service desk queue. Either a technician self-assigns it, or a team leader takes the responsibility of assigning it to the team. When there is manual intervention, tickets may be picked based on ease of resolution, making it unfair for other technicians. It is also possible that new tickets are in the queue for too long while waiting to be assigned, impacting the SLAs. Auto assignment of tickets removes manual intervention, ensuring fairness and timely assignment. Infraon offers three methods to define auto-assignment.

Round Robin

Round Robin is the simplest way of assignment where tickets are assigned equally to active technicians in a circular order—recommended for businesses where tickets are raised to follow up on orders, requests, etc. Using this to auto-assign tickets helps save time on the manual assignment of tickets.

Use-case - An e-commerce business where tickets are raised to know order status, delays in delivery or refund status, etc. Since these are information-based tickets and no troubleshooting is required, the time spent on each ticket is minimal. Using the Round Robin method ensures that tickets are assigned equally and orderly.

Load Balancer

The load Balanced method assigns tickets based on the technician's load and is recommended for businesses offering a wide range of services, where the resolution time is different for each. Using the Load Balanced method ensures that the technicians have a balanced workload while they are already working on a ticket. When a new ticket is raised, the technician with the most negligible load is auto-assigned to the technician. Tickets are assigned based on the ticket queue's SLA, priority, and criticality. Thresholds must be defined to select this method.

Use-case - A technical support center for a product that offers 24/7 support where tickets are raised throughout the day. Some of these tickets may be inquiries, while others might have a long resolution. A round-robin method may not make sense here. The load balancer method checks the current load of the technician before assigning new tickets. This way, technicians are not burdened with work.

Skill Based

Skill Based method is used when there are multiple categories/levels of support offered by the organization—recommended for organizations providing support on a global level or across a wide range of products/services. Skill-based assignment ensures that the right technician assigns the tickets by matching their skill and level.

Use-case - A business that offers support or services on multiple products, regions, and time zones offering multi-lingual support. Here, tickets must be assigned based on the skill of the technician. The technician must be skilled in the language selected by the customer, know about the product chosen, etc. A skill-based allocation is best platformd for this.

Users

Users are members of the organization who has been invited to access Infraon. Users are added by administrators with pre-defined privileges across all modules of Infraon.

What you see on the screen

Users' page views can be toggled between List View and Card View using the button next to the '**'Invite user(s)'** button.

Details displayed are as follows:

- Username
-

- Mobile
- Role
- Status

Edit and delete action icons are available for each list item or card (on mouse hover).

User status must be 'Active' to log in to Infraon.

Invite User

Click on the 'Invite user(s)' button in the top right corner. Enter mail address(es) and select role using the dropdown menu. Multiple users and multiple roles can be invited in a single instance.

The invite link expires in 36 hours (can be changed in settings). New invites must be sent to re-invite users.

If invites with multiple roles have been sent to the same user, the user will be assigned the role associated with the link used to register first.

Instructions to 'Invite a User'

- Go to Infraon Configuration -> User Management -> Users.
- Click on the 'Invite User(s)' button.

Label	Action	Description/Example
Enter Email address(es)*	Add email address(es) of users you wish to invite onto Infraon. Separate multiple addresses using a semicolon (;) or a comma (,)	John.doe@company.com; Jane.doe@company.com
Select Role	Select a role using the dropdown menu.	Roles must be predefined before inviting people on to Infraon.
Add Invite	Use the 'Add Invite' button to add more rows of invites.	This option can invite multiple users while assigning different roles on Infraon.

Click 'Invite' to mail the invites. Administrators and other privileged users can see the status of pending invites and resend them using the pending notifications icon.

Group by asset data based on End User / Requesters and owner technician

Group Users and Requesters by Asset Data! Easily categorize users and requesters based on mapped asset tags for streamlined management.

Though it is possible to edit or delete users, adding users is through 'Invite' only.

Service Management

- Service Management, well known as ITSM, is an essential part of the lives of service-oriented businesses and organizations. ITSM, traditionally used to deliver technology solutions effectively, has now evolved into service management, which provides business values. Service management can help organizations simplify processes within other teams like HR, Administration, Finance, Legal, etc., who rely on technology.
- Service Management is an essential module of Infraon that helps organizations follow ITIL or other compliance-related practices while delivering consistent care and attention. A service-driven organization aims to support strategic business objectives with the support of ITIL.
- While ITIL V3 had defined 26 processes across the service lifecycle, in ITIL 4, these 26 processes have been replaced by 34 "practices." The noticeable change in ITIL 4 is its definition of service as a means to co-create value by facilitating customer desired outcomes without undergoing related costs or risks. To achieve this, ITIL Service Value System (SVS) has been introduced in ITIL 4 to replace the service lifecycle from ITIL v3. In addition to this, ITIL 4 has also introduced four dimensions replacing the 4 Ps of ITILv3:
 - Organizations and People
 - Information and Technology,
 - Partners and Suppliers
 - Value Streams and Processes
- Organizations looking to implement ITIL must know that ITIL defines two types of catalogues for IT Services. Why do we need two separate catalogues?

What is a catalogue, and why do we need separate catalogues?

A catalogue is a compilation of items available for selection by end-users to simplify their day-to-day requests. Articles from the catalogue can include:

- The organization's IT services include email creation, login credentials, laptop servicing, etc.
- Non-IT services like HR (Onboarding, letters, relieving), finance (Pay-slips, tax forms), admin (Access card, cupboard keys), etc.
- Asset requests for active assets like keyboard, monitor, laptop, etc.
- Asset requests for fixed assets like chairs, boards, pedestals, etc.,
- Consumables like batteries, printer cartridges, stationeries, forms, etc.

Service management has two sides - The service offering & the service requesting. Services are offered with the help of a service catalogue and requested using the business catalogue. By having two separate catalogues, organizations can target a smooth workflow in terms of assignment, approvals, and SLAs and enhance user experience simultaneously.

	Service Catalogue	Business Catalogue
The audience	Meant for the IT or other respective teams to define categories, subcategories, and services to be listed in Business Catalogue.	Meant for end users. Lists out offered products and services as a catalogue, making it readily available for selection by users.
Service Perspectives	Contains infrastructure components used to fulfill all listed services like backup, storage, Assets, HR forms, maintenance tools, etc.	Contains user-facing services like Email fixes, IT servicing requests, services for provisioning, products like Mouse, Laptop, etc.
Information	Lists out Items and components in detail in addition to teams/individuals available to support these services.	Lists out products/services with descriptions, making it easy for users to select.
Value	Facilitates delivery of services in the business catalog in compliance with SLAs.	Facilitates timely access to services enabling user experience.

To simplify, the service catalogue is the backend of services offered through the business catalogue.

Configuration of service catalogue enables consolidation of services offered and improved productivity levels, thereby enhancing service experience. Service Catalog is often integrated with a **Configuration Management DataBase (CMDB)**, a database of assets or CIs (Configurable Items) owned by the business. Infraon's CMDB is referred to as Assets.

How to build an effective service catalogue?

An effective service catalogue must fulfill user requirements, ease technicians' load, and stick to SLAs. The service catalogue must be defined to facilitate self-service.

Step 1: Understand user needs

Step 2: Define service offerings

Step 3: Keep the details crisp, clear, and user-friendly

Step 4: Align offerings with the right audience
Step 5: Setup the right service team
Step 6: Define owners, approvers, and permissions
Step 7: Refine offerings periodically
Add on: Keep an incident template handy.

Demo data for ITSM module services for new Org

Knowledge Base Modules! Explore added knowledge articles to understand the functionality and purpose of KB modules.

Service Catalogue

The service catalogue is the service offering part of service management. It is the backend of the services provided through the business catalog, i.e., the module where the administrator or catalogue manager defines and manages products or services. These configured items can be viewed, wish-listed, and requested by requesters (internal and external end-users).

A service catalogue is created to maintain a list of components offered as services to the end-user. Components can be used as support to enable services and not as a service directly.

Only authorized staff and users can access the catalogue and perform activities like view, add, modify, authorize and delete records based on the role.

The administrator or catalogue manager uses a service Catalog to define & manage services, add service categories, etc. Other users can authorize and view catalogue information.

Infraon's Service catalogue offers options to create and publish products or services in detail with descriptions to facilitate structured content for the self-service framework.

What can you do here?

Service Catalogue need not necessarily list out only the IT components. There are other teams within the organization that provide services to employees. For example - HR, Finance, etc. Any request from an end-user can be classified as a service. This includes a request for an email ID, request for information on HR policy, clarification on Salary Slips, etc.

Service Catalogue comprises

- Service
- Category of service
- Classification and child classification for each category

To define the audience, service owners, cost, and SLAs.

Before adding a Service

To add a service, the below must be defined.

- **Catalogue** - A branch or department offering the service within the organization. For example, the catalogue can be IT Services, Asset Requests, HR Services, Admin Services, etc.
- **Category** - Multiple categories within each catalog. For example, the IT Services catalogue can be split into categories like Desktop Servicing, Laptop Servicing, Components Servicing, etc.
- **Classification** - Classification for the specific service. Within the 'Desktop Servicing' category, for example, classifications can be made based on Desktop Brand or servicing needs such as Memory upgrade, Keyboard replacement, software requirement, and so on.
- **Service** - The actual Service that is being offered. For example, servicing laptops/desktops, installation of MS office, mouse, offering HR services like HR letters, leave balances, request for a payslip, form 16 from the finance team, etc.
- Once all the above parameters are defined, click on the '[Add Service](#)' button in the top right corner. There are four tabs in the 'Add Service' form.
 - **Basic Information** - Add basic service information like name, code, description, etc. Align the service to an existing catalogue or choose to add a new Catalogue, Category, or Classification.
 - **Advanced Information** - Add advanced information like cost, tag, overview, features, etc. Information added here enhances the user experience within the self-service portal.
 - **Ownership** - Assign service/business owners, reviewers, approvers, and service team. Define the audience by keeping the service open to all or limiting it to selected requesters/requester tags.
 - **Service Template** - Create a service template to ease the request of service.

Click '[Save](#).' It is recommended to keep the service in the 'New' state and 'Draft' status for as long as it is required to define, review and refine it to describe all service/product aspects to suit requirements.

Note: Service must be in 'Published' status to be available on the self-service portal (operational).

Instructions to 'Add a Service'

Click on the '[Add Service](#)' button in the top right corner. There are four tabs on the 'Add Service' page. Refer to the table for information.

[Basic Information](#) | [Advanced Information](#) | [Ownership](#) | [Test](#)

Label	Action	Description/Example
Product Image*	Add an image of the product or an icon to denote service.	You can add an image using the drag & drop option or upload files in PNG, JPG, or JPEG formats.
Service Name*	Add a name for the service.	For example, Laptop Setup, MS Office installation, Mouse, etc.
Service Code	Add a service code.	The service code is used as an identifier. This can be defined based on organizational norms. For example, MS_Install, AntiV-Install, HR_Serv_001, E-Fin-01, etc.
Catalogue*	Select a catalogue to group the service.	Based on the type of service, select catalogue - IT, HR, Finance, etc. Use the 'New Catalogue' option to create a new catalogue.
Service Classification	Add service classification.	Based on the type of service, add service classification. Within the 'Desktop Servicing' category, classifications can be made based on Desktop Brand or servicing needs such as Memory upgrade, Keyboard replacement, software requirement, etc.
Service Description	Add a brief description of the service.	It is recommended to include a detailed description of the service to enhance the end-user's self-service experience.
Status	Select the status of the service	While adding a service, status can be selected as 'Definition - Open' till the service is ready to be published. The status must be moved to 'Published - Operational' to make it active.
Criticality	Select criticality of the status	Based on how critical the service is to the business, select the criticality level - 1 being business-critical and four low.

Once all the parameters are added, click 'Next' to add advanced information.

[Basic Information](#) | [Advanced Information](#) | [Ownership](#) | [Test](#)

Label	Action	Description/Example
Currency	Select currency (for cost) of the service/product.	Choose the currency (INR or USD) for the service/product cost.
Cost	Add the price of the service or product. Services must have an established cost, even if it is not charged to the requester.	If the cost entered is 100 and the currency is selected as USD, the cost of the service/product is taken as USD 100.
Purchase Required	Select if the selected service involves a purchase of a product	Select if the request involves purchasing a product (from the business side), i.e., if the request is for a keyboard and the technician must buy the same to fulfill the request.
Shipping Required	Select if the service involves the shipping of a product.	Select if the request involves the shipping of a product, i.e., Select if the request is for a keyboard and the technician is required to ship it to the requester.
Tag	Add tags for better classification.	Refer to the 'Tags' module for details.
Overview	Add an overview of the service/product.	The overview can include size, product measurements, version, or service descriptions.
Key Feature	Add key features of the product or service.	Key features can include the unique qualities of your product/service.
ServiceAvailability	Add details about the availability of service, if any.	Availability can be quality, time, or rating based on the service's performance, maintenance, security, and reliability. For products, availability can be the delivery time, performance capabilities, etc.
Additional Fields	Add details in the following fields: Product/Service Information, Value Proposition, Service	Additional details help requesters get a thorough understanding of the service/product listed.

	Commitment, Training, Target Audience, Turnaround Time, and Business Processes Supported.	
--	-------------------------------------------------------------------------------------------	--

Once all the parameters are added, click 'Next' to define ownership. The ownership tab is used to determine service ownership and visibility.

Basic Information | Advanced Information | [Ownership](#) | Test

Label	Action	Description/Example
Service Visibility Section		
Service Owner	Select an owner for the service or product.	The service owner is usually the person in charge of the service design.
Business Owners	Select an owner for the business offering the specified service or product.	Business owners are usually the decision-makers behind the service.
IT Owners	Select an IT owner for the specified service or product.	IT Owners are users from the IT team in charge of fulfilling the product or service deliverables selected.
User Tags	Select user tags, as applicable.	User tags are used as filters to control service availability. If HR services
Subscription List(s)		
Subscribed All Requesters	Select this option to make the service available to all requesters.	To enable service for all requesters.
Requester Tag(s)	Select requester tag(s) to limit service availability	For example, HR services can be restricted to internal users by selecting the relevant tag. Or Region-based tags can be used to filter region-based services.
Requester(s)	Select tag(s) to limit service availability to selected requesters	This helps restrict service for selected users.

Once all the parameters are added, click 'Next' to define the incident template. Templates are used to ensure information consistency. It enables requesters to include all relevant information and create incidents quickly.

Basic Information | Advanced Information | Ownership | [Service Template](#)

Label	Action	Description/Example
-------	--------	---------------------

Incident Summary Owner	Add a summary of the incident.	The incident summary acts as the mail subject when an incident is raised.
Incident Description	Add a brief description of the incident.	Include information that is mandatory to work on the incident.

Once all the parameters are added, click 'Submit.' The service is added under the selected category within Infraon. Service view can be switched between cards and grid to suit requirements. To see all catalogues within a category, click on the category name on the left. Catalogues, categories, and services can be edited and deleted using the respective icons.

Note: All the dependent categories and services are deleted if a catalog is deleted. Similarly, all dependent services are also deleted when a category is deleted.

Notifications

Infraon is enabled with an intelligent notification system. Infraon Notifications are displayed as a floater across all pages. The respective notification icon is displayed with the notifications count when a notification is triggered.

The notifications module is a part of Infraon Configuration and is further split into:

[Messenger Audit](#) - View the log of communications sent from and received within Infraon

[Configure SMS](#) - Configure SMS gateway to enable SMS notifications from Infraon.

[Configure SMTP](#) - Configure your email server details to send and receive emails from Infraon.

[Trigger Configuration](#) - Configure a trigger to trigger an alarm or an event.

Let's see each of these in detail.

Configure SMS

Configuring SMS is mandatory to send out SMS notifications from Infraon. Before configuring, ensure that you have the below details from your service provider:

- SMS Gateway URL
- Status Code
- Key
- Value

Instructions to 'Configure SMS'

Go to Infraon Configuration -> Notifications -> Configure SMS Gateway

Label	Action	Description/Example
Title*	Give a name to the SMS gateway.	SMS, SMS Notification, etc.
URL*	Add the SMS gateway URL given by your service provider.	Enable 'Get Request' or 'HTTPS' based on the service provider.
Status Code	Add status code	
Request Parameters	Use the 'Add' button to add request parameters like key and value.	

Once all the parameters are added, click 'Submit' to save the configuration.

Steps to 'Configure SMS'

- Go to Infraon Configuration -> Notifications-> Config SMS.
- Give a name to the SMS gateway.
- Add the SMS gateway URL given by your service provider. Enable 'Get Request' or 'HTTPS' based on the service provider.
- Enter the Status Code in the Status Code text box.
- Use the 'Add' button to add request parameters like key and value.
- Click 'Submit' to save.

Note: Please use gateway_sms_recipients as the value for the mobile number key and gateway_sms_message as the message/content key value.

Configure SMTP

Configuring SMTP server information is mandatory to send out email notifications from Infraon. SMTP server configuration is a part of 'Getting Started' with Infraon. Mails sent to this address are converted as Incidents. This email address also acts as a reply to the mail address for all customer communication. Before configuring, ensure that you have the below details from your service provider:

- Host Name
- Host Username
- Password
- Port

There are two options within the SMTP server configuration. You can configure your existing email address onto Infraon or set up a new one using Infraon's email server.

Instructions to 'Configure SMTP'

Go to Infraon Configuration -> Notifications -> Configure SMTP

Here on the page, either login using the Microsoft OAuth login or manually entering API credentials.

Microsoft OAuth

Click to log in using the Microsoft account.

Enter the Microsoft credentials and grant the appropriate permissions to easily configure the SMTP configuration.

Other

There are two tabs in the SMTP configuration.

[Configuration](#) | [Test](#)

Label	Action	Description/Example
SMTP Hostname*	Add the SMTP Hostname.	The service provider usually gives this.
SMTP Host Username*	Add the SMTP Host Username.	The service provider usually gives this.
SMTP Host Password*	Provide the SMTP password.	The service provider usually gives this.
Sender Email*	Add Sender's email address.	Mails sent through Infraon are delivered with the specified email address as the sender.
SMTP Host Port*	Add SMTP host's port details.	Use the toggle option to enable SSL or TSL encryption.
Authentication Type	Select the authentication type from the drop-down	Basic Authentication and OAuth2 Microsoft. Configure SMTP with Office 365 is now seamless, requiring Client Secret, Tenant ID, Client ID, and Authority.

[Configuration](#) | [Test](#)

Label	Action	Description/Example
Test	Test the entered credentials.	Click 'Test' to send a test mail to authenticate the configured email credentials.

Once the test is successful, click 'Submit' to save the configuration.

Messenger Audit

Messenger Audit acts as the Notification Log. Displays the complete list of notifications triggered and received within Infraon.

Use the options on the left panel to filter out notifications based on the notification type.

- Email
- Slack
- WhatsApp
- SMS
- Trash

You can view, reply to or forward messages using the respective icons on the message.

Trigger Configuration

Triggers are rules or configurations that trigger an alert or an event within Infraon. Infraon allows adding of conditions to raise alerts or events when the specified rule is met.

There are two types of trigger configurations within Infraon. They are:

- **Alerts** - Alerts are based on configured thresholds (refer to Threshold module for details)
- **Correlation** - Infraon correlates events based on multiple conditions to trigger an action.

To configure a Trigger

There are three steps to adding a trigger:

- [Trigger](#) - Define a name and select if it is an alert or correlation.
- [Condition](#) - Define filters and conditions.
- [Action](#) - Select action between notifying through email/SMS or creating an incident

Triggers can be created for alarms, severity, asset IDs, names, etc. Ensure the trigger status is enabled to trigger the alerts/actions.

Instructions to 'Configure a Trigger'

- Go to Infraon Configuration -> Notifications -> Trigger Configuration
- Click 'Add Trigger.'

There are three tabs on the 'Add Trigger' page.

[Trigger](#) | [Conditions](#) | [Action](#)

Label	Action	Description/Example
Name*	Add a name for the trigger.	For example, Severity trigger, Asset-based, etc.
Trigger Type*	Select trigger type - Alert or correlation.	Alert triggers are based on a threshold, whereas correlations are based on multiple events correlated by Infraon.

Click 'Next.'

[Trigger](#) | [Conditions](#) | [Action](#)

Label	Action	Description/Example
Business Hour Profile*	Select the business hour profile applicable for the trigger.	Triggers can be configured to be generated during business hours (by selecting a business hour profile). The business hour profile must be pre-defined for this.
Filters	Select filters and conditions for the trigger. The 'Add Condition' option can add multiple filters or conditions. Use 'And/Or' to suit requirements.	If you select 'Alarm Message', for 'CPU Utilization' and 'Severity' 'In' 'Critical', Infraon triggers the selected action when both these conditions are met.
Criteria		

Note: When adding filters under the Conditions tab, if an alarm message is selected, corresponding log management value fields can be incorporated. This allows users to refine the filtering criteria by associating relevant log data with alarm messages, enhancing the precision and effectiveness of log analysis.

Click 'Next'.

[Trigger](#) | [Condition](#) | [Action](#)

Label	Action	Description/Example
Notify*	Notify action can be used to send Email/SMS notifications or create an incident.	Add information as requested.

Email	If selected, an email notification is sent to the configured email address.	Add the recipient's email address (use a comma or semicolon as a separator to add multiple addresses and a subject line).
SMS	If selected, an SMS notification is sent to the selected user.	Add the SMS content (Text), and select the user to be notified.
Create a ticket	On selecting this, Infraon creates a ticket, as configured (filters and conditions)	

[Macros](#) | [Details](#)

Simplify email composition for technicians by automatically inserting relevant details such as asset IP address, hostname, device type, and NCCM-specific events like job failures and configuration changes.

This automation saves time, reduces manual errors, and ensures accurate and comprehensive notifications. Using these macros, technicians can quickly generate clear, detailed emails, improving communication and efficiently managing network configurations and changes.

The following Macros can be availed:

- **Asset**

- IP Address
- Hostname
- Alias
- Device Type
- OS Name
- Asset ID
- Branch Name
- Branch Code

- **Basic Info**

- Severity
- Event Message
- Timestamp
- Alarm ID
- State
- City
- District
- Country
- Parameter Value

- **NCCM**

- Job Failure Reason
- Startup Changes
- Running Changes

- **Resource**

- Resource Type
- Resource Name
- Resource Tag
- Bandwidth configured
- Link ID
- Link Name
- Link Mode
- ISP Name
- Link Bundle Name
- Link Bundle Capacity

Click '[Submit](#)' to save the configuration. The respective action icon allows you to edit and delete triggers.

Infraon Automation

Infraon Automation is a part of Infraon Configuration and contains configurations that can be used to automate features, processes, and activities within Infraon.

This module of Infraon consists of the following:

[Mail Automator](#) - Configure IMAP mail accounts on infraon and refer guides to forward your existing emails to Infraon to convert emails into tickets.

[Workflow](#) - Visualize and create a flow of process involving a sequence of specific activities of the selected module.

[Business Rule](#) – Defines the business rule for the Infraon system for auto assignment of tickets.

[Escalation](#) - Defines the escalations process and automatic assignment mechanism are employed in support ticket resolution.

[Customer feedback templates](#) - Customize templates to collect feedback from customers to improve service quality and customer experience.

Let's see each of these in detail.

[Business Rule](#)

What is a business rule?

A business rule for an Infraon product refers to a specific guideline or constraint that governs the behavior, processes, or operations within the context of that product's infrastructure. These rules are typically defined and enforced to ensure consistency, compliance, and efficient functioning of the Infraon product.

Types in business rule

There are two types of business rules:

- **Load Balancer:** The ticket allocation system ensures a balanced distribution between users. Automatically routing any additional tickets beyond the initial allocation to the following user until the same number of tickets per user is reached. This ensures an equitable workload distribution.

For Example: User one has seven tickets, and user two has five tickets, the upcoming tickets will be automatically added to user two, as user one already has seven tickets greater than user two.

- **Round Robin:** Despite any existing ticket imbalances, prospective tickets raised are sequentially assigned to the first user, disregarding the need for a balanced distribution among users.

For Example, User One has five tickets, and User Two has three tickets; prospective tickets are automatically assigned to the user one even though user two has less number of tickets.

Instructions to add business rules

- Go to Infraon Configuration > Infraon Automation > Business rule
- Click the 'Add' Button

To the 'Add Business Rule' page. Refer to the table for information.

Label	Action	Description/ Example
Rule name	Add your rule name	Rule Name is an identifier assigned to a specific rule to distinguish it from other rules in the system.
Type	Select the rule type from the dropdown.	Predefined logic determines how tasks or actions are assigned or allocated based on specified criteria and conditions.
Description	Add the rule description	Write the description of the rule in fewer words.
Is Enable	Enable the toggle button or disable	Allows users to activate or deactivate the rule's

		functionality with a single click.
Select operand	Select the Operand type from the dropdown.	The specific service or component that will be affected or influenced by the execution of the rule's defined actions or tasks.
Select Operator	Select the Operator type from the dropdown.	Select in or in not depend on the requirement of the rule.
Select value	Select the Value from the dropdown.	Select the value depends on your rule created, for example, Email delete.
Assign to	Select the group from the dropdown.	Select the group based on the requirements of the rule.
Group	Select a group from the dropdown 'assign to'	A group refers to a collection or category of entities, such as users or resources.
Expertise	Select the Expertise type from the dropdown.	Expertise refers to individuals' or groups' specific knowledge, skills, or qualifications.
Level	Select the Expertise type from the dropdown.	Choose L1, there are multiple users in this level and the rule is assigned depending on the requirement.

Click the '**Submit**' button.

The auto-assignment process in L2 support, where technicians (U4, U5, U6) are categorized based on their levels. When opting for L1 auto-assignment, the system follows a sequential assignment of technicians (U1, U2, U3, and so on) for customer ticket resolution.

The SAAS team's auto-assignment mechanism to handle hardware issues. When a problem arises in the service, the team provides hardware support. In the event of hardware issues reported by developers, an expert L1 person is assigned based on load balancing or round robin, ensuring efficient resolution of customer tickets.

Manual Service Mapping

This functionality empowers administrators to define automatic ticket assignment rules based on impacted services and requester tags, enhancing the workflow and improving service delivery.

How does it work

Business rules automate ticket assignments based on predefined criteria. They are configured to:

Assign tickets based on impacted service:

Tickets associated with a specific impacted service (e.g., hardware diagnostics) can be automatically assigned to a designated team or technician based on expertise level.

Assign tickets based on the requester tag:

Tickets created by users belonging to a particular requester tag (e.g., front desk) can be routed to a predefined team or technician.

Creating Business Rules with Manual Service Mapping

This section guides admins through creating business rules with manual service mapping.

Define the Business Rule

- Assign a clear and descriptive name for the rule (e.g., "Hardware Diagnostics - Assign to IT Team Level 1").
- Select the type of rule (e.g., "Impact Service").
- Provide a brief explanation of the rule's purpose (e.g., "This rule automatically assigns tickets related to hardware diagnostics to IT Team Level 1 technicians").

Configure Impact Service Mapping

- Select the specific service impacted by the ticket (e.g., "Hardware Diagnostics").
- Choose the logical operator for the rule (e.g., "equals").
- **Assign To:**
 - **Group/Team:** Specify the team responsible for addressing tickets related to the impacted service (e.g., "IT Team").
 - **Expertise:** Define the specific expertise required for handling tickets (e.g., "Hardware").
 - **Level:** Select the appropriate technician level within the assigned team (e.g., "Level 1").

Example:

Considering a scenario where an IT team handles hardware diagnostics. Creating a business rule with the following configuration ensures tickets related to hardware diagnostics are automatically assigned to IT Team Level 1 technicians:

- Business Rule Name: Hardware Diagnostics - Assign to IT Team Level 1
- Type: Impact Service

- Description: This rule assigns tickets related to hardware diagnostics to IT Team Level 1 technicians.
- Impact Service: Hardware Diagnostics
- Operator: Equals
- Assign To:
 - Group/Team: IT Team
 - Expertise: Hardware (Optional)
 - Level: Level 1

Business Rules for Requester Tags

Business rules can also be based on requester tags. Here's how to create a rule for a specific requester tag:

- Assign Tickets from the Front Desk to the Procurement Team Level 1
- Add the respective Requester Tag as Front Desk Manager.
- Then Assign To:
 - Group/Team: Procurement Team
 - Level: Level 1 Technician

Example:

This rule ensures any ticket created by someone belonging to the "Front Desk Manager" tag is automatically assigned to the Level 1 Technician within the Procurement Team.

Escalation

What is escalation?

The escalation process and automatic assignment mechanism are employed in support ticket resolution. When a ticket is raised, it is initially assigned to an L1 user, if L1 cannot resolve the ticket, it is escalated to the appropriate escalation team. The escalation occurs from L1 to L2 and L3 in descending order.

Automatic escalation is triggered in L1, with the system selecting a user for escalation. The escalated team provides a response time for ticket resolution, such as 50 minutes for L1 and 30 minutes for L2, allowing multiple scheduled attempts to resolve the ticket within the given time frame.

Instructions to add the escalation

- Go to Infraon Configuration > Infraon Automation > Escalation
- Click the 'Add' Button

To the 'Escalation' page. Refer to the table for information.

Label	Action	Description/Example
Escalation Name	Add your Escalation name	The process of automatically routing or notifying higher-

		level authorities or individuals when certain conditions or thresholds are met, ensuring timely attention to critical issues or tasks.
Priority	Select the priority from the dropdown	Prioritize the ticket, critical, high, or medium also you can select all
Team Name	Select the team from the dropdown	Team Name refers to the designated identifier given to a specific team or group responsible for handling escalated issues or tasks within the system.
When	Select from the dropdown	The ticket not resolved option is available and the user should select the option while creating the escalation.

Click the '**Submit**' button.

Note: An automated escalation and assignment process in a multi-level support system consists of three levels. When creating an escalation, the priority is selected, and the system automatically assigns the first available assignee.

For Example: Here are three options: After 25 minutes (L2), changing the assignee, notifying without assigning or notifying, and changing the assignee to L2. After 30 minutes, the assignee is changed to L3; after 60 minutes, it is changed to L4. If a ticket is raised with an L1 user, after 25 minutes, the system triggers an email to automatically assign an L2 user from the pool of available options.

Email Integration

Integrate your external emails with Infraon to keep track of and manage your email correspondence with customers from Infraon. This is achieved by setting up email forwarding from your current email client (or server).

To begin with, we have added instructions for the most popular email clients:

- [Google Mail](#)
- [G Platform](#)
- [Microsoft Outlook](#)

Contact our support team if your email service provider is not listed above. We will help you set it up

Google Mail Forwarding

Google Mail forwarding can be used in the below scenarios:

- Forward all mails
- Forward specific emails from your inbox
- Forwarding emails from the "spam" folder

Forward All Mails

- Open Gmail and click the gear icon in your inbox. Choose "See all settings."
- Navigate to the "Forwarding and POP/IMAP" tab.
- Click "Add a forwarding address."
- Enter your Infraon address (found in Infraon Settings-> Inboxes), click "Next," and "Proceed."
- Check Infraon for the verification message. (Use the 'Click here to refresh' option from the 'Setup your Helpdesk Email (Step 2 of Getting Started module) page to get your verification code).
- Add the verification code and click "Verify."
- Select "Forward a copy of incoming mail to Org@infraon.com."
- Select the action for forwarded messages—keep them in your Gmail Inbox, mark them as "read," archive, or delete them to suit your requirements.
- Click 'Save Changes.'

Visit <https://support.google.com/mail/answer/10957?hl=en> for more details.

Forward Specific Mails

You can choose to forward selective messages using the filter option. You can choose to filter emails from a specific person, a keyword from the subject line, and so on.

To add a filter:

- Open Gmail and click the gear icon in your inbox. Choose "See all settings."
- Navigate to the "Filters and Blocked Addresses" tab. Google suggests some filters based on your usage.
- Click "Create a new filter."
- Choose from the available options to create a filter. There are eight main criteria to select from:
 - From-select the sender(s)
 - To select the recipient(s)
 - Subject-Add a keyword to look for in the subject line.
 - Has the words-Add keyword to look for in the mail content.

- Doesn't have-Add a keyword to look for the absence of the word in the mail content.
- Size-select from greater than or less than and add a specific size.
- Has attachment-check to select emails with an attachment.
- Don't include chats-check to ignore the chat history emails.
- Add filters to suit your requirements and click on "Create filter." Alternatively, you can select to import filters.
- Google prompts you to select the action for the selected filter.
- Select "Forward it" and click 'Add a forwarding address.' Add your Infraon email address.
- Click 'Proceed' to confirm. A confirmation pop-up appears.
- All your emails meeting the selected filter criteria will be auto-forwarded to Infraon.

Forward Spam Mails

Gmail may sort your customer's email as "spam." To avoid missing out on emails, you can configure it to forward such emails to Infraon.

Before proceeding, disable other filters if applied.

- Open Gmail and click the gear icon in your inbox. Choose "See all settings."
- Navigate to the "Filters and Blocked Addresses" tab. Google suggests some filters based on your usage.
- Click "Create a new filter."
- In the 'Has the words' section, add ' delivered to:youremailaddress.'
- Add filters to suit your requirements and click on "Create filter."
- Google prompts you to select the action for the selected filter.
- Select "Forward it" and click 'Add a forwarding address.' Add your Infraon email address.

- Click 'Proceed' to confirm. A confirmation pop-up appears.

Mails from the spam folder meeting the selected filter criteria will be auto-forwarded to Infraon.

If you use Groups in G Platform, include the Infraon forwarding address as one of the email addresses in your group.

Google Platform

Follow the below steps to forward emails from Google Groups.

Forward from an Existing Group

- If you use Groups in G Platform, include the Infraon forwarding address as one of the email addresses in your group.
- Open the G platform administrator console. Choose Groups.
- All your Google Groups will be visible. Choose the group you wish to add your Infraon address to.
- Navigate to the "members" section. Click on the 'Add Members' button.
- Add your Infraon email address and select 'Add to Group'.
- The Infraon email address is now added to the group.

Steps to create a New Group

Follow the below steps to create a new group:

- Go to the Google Groups list and click "Create group."
- Fill in group details like name and group email. Choose a group owner.
- It is important to enable External "Publish posts" to receive emails from outside your organization. Click on "Create Group."
- Click "Done."

Follow the steps from the previous section to add the Infraon email address to this newly created group.

Customer Feedback Template

Customer feedback templates in Infraon allow admins to take post-ticket surveys from the requesters. To gather customer insights and drive improvements in product features. These surveys capture customer feedback to guide product development and optimize the customer experience.

How does it work?

Infraon streamlines gathering customer feedback by offering pre-built templates. Admins can either choose a default template based on the impacted services or customize one to their needs. Once a template is created, it can be easily integrated into the workflow for that specific service. This means whenever a technician resolves a ticket linked to that service, the requester automatically receives an email prompting them to rate and comment on their experience. This seamless process ensures valuable feedback is collected consistently, helping improve service quality.

What you see on the screen

Label	Action	Description / Example
Search	Search for the required Template.	
Filter	Filter can be added based on the field and condition from the drop-down box below.	Field – Name, Description, Services, Link Expires in. Condition – contains, not contains.
New Feedback	Click to add a new Template.	
Available Templates		View the templates added to the configuration page.

Instructions to add Customer Feedback Template

- Go to Infraon Configuration > Infraon Automation > Customer Feedback Templates.
- Click the 'Add Feedback' button located at the top right corner of the page.

To the 'New Feedback' page. Refer to the table for more information.

Label	Action	Description / Example
Basic Details		

Feedback Name	Click to add a name to the template.	
Description	Click to add a brief description of the template.	
Services	Selected the impacted services from the drop-down box below.	For services not included in the dropdown, navigate to Service Management > Service Catalogue > Add Services to create a new one.
Link Expires In (Days)	Define the validity period for the requester's access link.	Choose a validity period (1-99 days) from the dropdown menu.
Default Star Rating	Define a default star rating that will be presented as the initial selection for the requester during the rating process.	Select from the drop-down below.

- In the create form page, drag and drop to select the relevant user experience aspects you want the user to rate for the service.
- Click on the configure option to make changes to a specific catalogue.
- Once done, click "**Save**" to add the template.

Mail Automator

Infraon automatically converts emails into tickets and sends them to end-users using IMAP configuration. It saves tremendous time by manually sending tickets from the mail.

How does it work?

IMAP (Internet Message Access Protocol) is a standard email retrieval (incoming) protocol. It saves email messages on a mail server and allows recipients to see and edit them as if they were locally saved on their device(s).

You can configure your email servers on Infraon using the IMAP Configuration module, which allows us to read emails and turn them into incidents.

What you see on the screen

Administrators or privileged users can configure (add), edit, and delete IMAP configurations. Refer to the '[Email Integrations](#)' section for instructions to forward from your existing email accounts.

Instructions to 'Configure IMAP'

- Go to Infraon Configuration -> Infraon Automation -> Mail Automator
- Click on the 'New Config' button.

Here in the page, either login using the Microsoft OAuth login or manually entering API credentials.

Microsoft OAuth

Click to login the using the Microsoft account.

Simply enter the Microsoft credentials and grant the appropriate permissions to easily configure the IMAP configuration.

Other

There are two tabs on the IMAP configuration page.

Email Config | Domain

Label	Action	Description/Example
Mail Server*	Add the incoming email server details.	imap.gmail.com
Email*	Add your email address.	john@gmail.com, rozi@thp.com, etc
Password*	Add your password	Add your email password credentials.
Incoming IMAP	Add server port and select encryption type, either SSL or TLS.	The port value is auto-generated. You may change it if required.
Outgoing SMTP	Add SMTP server, server port, and select encryption type, either SSL or TLS.	The port value is auto-generated. You may change it if required.

Fields marked with * are mandatory.

Note - Click the 'Test' button to see if your IMAP configuration is valid.

Click Next to add details on the Domains tab.

Email Config | Domains

Multiple IMAP configurations can be added for various service catalogues within the organization. Select the impact service to customize.

Label	Action
Impact Service	Select the 'Impact service using the drop-down to map the IMAP configuration to the specific catalogue. Use the 'Allow Duplicates' toggle to enable duplication. Enabling duplication allows multiple configurations to be selected for the same service catalogue.
Blocked Email	Enter the email address that you want to block.

Approve all Domains	Click on the toggle button beside the approve all domains. On toggle, you can see include or exclude domains. Select domains that you want to either exclude or include.
----------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------

After adding details on domains, click Submit to configure your email address. Now, the new email address is configured.

Configurations can be edited or deleted using the respective action icon.

Microsoft Outlook

Follow the below steps to forward emails from MS Outlook.

Forward from Outlook

From the MS Outlook application, click on Settings>View all Outlook settings.

- Select Mail > Forwarding.
- Select 'Enable Forwarding.'
- Enter your Infraon Helpdesk email address (from the 'Getting Started' part of Infraon).
- Check the 'Keep a copy of forwarded messages' if required.
- Click 'Save.'

Note: Outlook requires administrator permission to set up forwarding outside the organization if a company manages your email address.

Workflow

Workflows act as a visual flowchart of processes within Infraon. A workflow is created to automate and visualize a multi-step process as a sequence of activities, including assigning tickets, triggering an email or SMS notification, requesting approvals, etc. With Infraon, workflows can be created using simple drag-and-drop elements that can be added as a flowchart to indicate the flow of activities in a sequence.

How to Build a Workflow?

At this point, you can configure workflow for Incidents. Workflows can be triggered using single or multiple conditions within the service catalogue.

Components of Workflow

To build a workflow, the below components must be defined:

To build a workflow, the below components must be defined:

- **Trigger** - Triggers are the initial action(s) that trigger the workflow. There can be one or more triggers configured. At this point, only service catalogue-based triggers can be added.
- **Conditions** - One or more conditions can be added to be validated while executing. To add a condition, define
 - **Operand** - Operand is the parameter that needs to be validated. In this case, Service Catalogue.
 - **Value** - Value of the Operand or the parameter's value to validate.
 - **Relation** - (and/or) Relation between the conditions (applicable only if multiple conditions are selected)
- **Build Form** - Consists of drag-and-drop HTML elements. You can use it to add custom fields to the incident form based on your organizational, compliance, or process requirements. Additionally, section layouts can be changed, configured, or deleted to suit the need. You can preview sections to understand the placement of sections within the incident form.

This consists of your workflow's drag-and-drop elements like state, action, and condition. This helps create a customized workflow based on your organizational, compliance, or process requirements.

Using the 'Save' option saves the workflow. The workflow changes and conditions are added when they are published.

Note: Workflows must always start with an 'Open' state and end with 'Closed.' All other states are optional.

Advanced Options

Advanced configurations in workflow include:

Field Constraints - Used to define role-based privileges on the incident components. Fields can be hidden or made mandatory for selected statuses and roles. Worklog can be made mandatory for roles and statuses. For example, for the role of an IT Support Operator, while the incident status is 'Working (*In Progress*)', all closure-related fields (*Closure Note, Closed By, Close Type, Agreed Closure Date, and Actual Closure Date*) can be hidden, and fields like Diagnosis and Note can be made mandatory. Multiple constraints can be added to define limitations for all roles.

Permissions - Used to enable or disable role-based permissions for Incident actions. Actions like commenting on the wall, KB searches, adding attachments, adding tasks, defining relations, and escalating can be customized. For example, an API user can be restricted from adding attachments or tasks.

Workflows can be edited or deleted using the respective action icons.

What you see on the screen

You can see the following details on the screen:

- Title
- Description
- Created On
- State
- Services
- Action

Instructions to 'Add Workflow'

- Go to Infraon Configuration -> Workflow
- Click the Add New Workflow -> Incident

Label	Action
Name*	Add a name for the workflow.
Description	Add a brief description of the workflow.
Operand	Select the service catalogue from the drop-down menu.
Value	Select a value from the drop-down menu. These values are derived from the 'Service Catalogue' and must be pre-defined.

Note - Without selecting operand, value selection will be in disable mode.

After adding respective details, click Create. There are two tabs here.

[Build Form](#) | Configure Workflow

Before adding the build form, you need to know its components:

Build Form has five sections: Add Content Here, General Section, Assignment Section, Resolution Section, and Closure Section. Please note that the contents of the build form can be used in any of the four sections of the incident workflow.

- 'Add Content Here' consists of drag-and-drop HTML elements that can be inserted into any of the four sections mentioned above.
- After inserting any HTML elements, the 'Properties' column appears with two tabs: 'General' and 'Editor.' Details added in the 'General' tab are updated in the 'Editor' tab in HTML. Additionally, there are three toggle buttons;
 - Mandatory - Enable to mark the field mandatory
 - Show on add page - displays the field on the 'Add Incident' page.
 - Show on the customer portal - displays the field on the customer portal.

Click the '[Save](#)' button to save the Properties.

Note: The build form is made to add customized fields within the existing incident form, within the general, assignment, resolution, and closure sections. These are optional elements. You may skip them and directly go to the Configure Windows tab.

Custom field in Report for Request and Change

Offering greater flexibility in managing custom fields and service selections. The selected custom fields effortlessly propagate into the request report, providing comprehensive insights into the service-specific details. The power of personalized workflows, tailored to unique requirements, simplifies the request management process.

You can perform the following actions in the 'Build Form':

- [Preview](#): Preview any section after adding HTML elements.
- [Change layout](#): You can change the layout of added HTML elements.
- [Configure](#): Configure the added HTML elements.
- [Delete](#): Delete the HTML elements that you do not need.

After selecting the required HTML elements, Click 'Configure Windows' to add details.

Task Workflow

Upon creating a ticket/change/problem/request, the default status is 'Open,' situated at the top of the status hierarchy. Additional statuses can be arranged below 'Open' through drag-and-drop functionality. The final status will typically be either 'Closed' or 'Resolved.'

[Build Form](#) | [Configure Windows](#)

Configure Windows has three sections: State, Actions, and If Conditions. These drag-and-drop HTML elements are placed in the 'Configure Windows' area to complete the workflow.

[State](#) | [Actions](#) | [If Conditions](#)

Label	Action	Description
Open	By default, the state is open and new.	This is the initiation of workflow.

In Progress	Drag the in-progress button below the open state.	The In-progress state is added to show that the workflow is in a progressive state. You may add the In-Progress button and define the state and status.
Approval	Drag the Approval button below the 'in-progress' state, 'on-hold' or 'open' state.	Approval shows that the workflow status is in an approval state for acceptance or rejection by the approval team. You may configure the Approval button and define the state and status.
On Hold	Drag the on-hold button below the open or the In-progress state.	On Hold shows that workflow is on hold due to some conditions. You may configure the On Hold button and define the state and status.
Resolved	Drag the resolved button directly after the 'open' or below the 'in-progress' or 'on-hold' state.	Resolved shows that workflow status is being resolved. You may configure the Resolved button and define the state and status.
Close	Drag the Close button after the Resolved state.	Close shows that the workflow status is being closed. You may configure the Close button and define the state and status.

PIR (Post Implementation Review)- This functionality, Post-implementation review for valuable insights and feedback about the change implementation. Infraon determines the review team that comments on the process and delivers feedback on the implementation process, including problems faced and the resolution given. This enhances ITSM workflows, facilitating continuous improvement.

State | [Actions](#) | If Conditions

Actions are performed after the state is defined.

Label	Action	Description
Transfer State	Drag Transfer state if you want to change a specific state and status.	It generally comes after the 'If Conditions' button is applied to change or set the original state.
Set Value	Drag the Set value button under any state to set the predefined value.	Set Value has five operands: Priority, Status, Impact, Urgency, and Severity. And, It has three values: High, Medium, and Low. Set any operand to the desired value.
Send Email	Drag Send Email button under any state.	To, Subject, and Description boxes must be added to proceed further. Select one value from the dropdown menu to add the 'To' box, and write on the subject and description box. Click 'Save' to save it.
Send SMS	Drag Send SMS under any state.	Add 'To' and Description boxes to proceed further. Select one value from

		the dropdown menu to add the 'To' box, and write on the description box. Click 'Save' to save it.
--	--	---------------------------------------------------------------------------------------------------

Enhanced change management with the introduction of the "Ask for Change" functionality. This replaces the rejection option and allows for requesting changes during the review process. The transition state is activated upon request for changes, facilitating a seamless transition to the open state for effective change management.

State | Actions | If Conditions

Label	Action	Description
If Conditions	Drag the 'If Conditions' button under any state to implement conditions.	You can later configure conditions by putting correct values. 'If Conditions' has four sections: Operand, Operator, value, and Relation. Based on Operand and Operator selection, Value selection shows varying options. You can add more 'Relation' 'ADD' or 'OR' from the dropdown menu.

Note: Since conditions are optional, you can publish the incident workflow without adding them.

Email Notification for approval process:

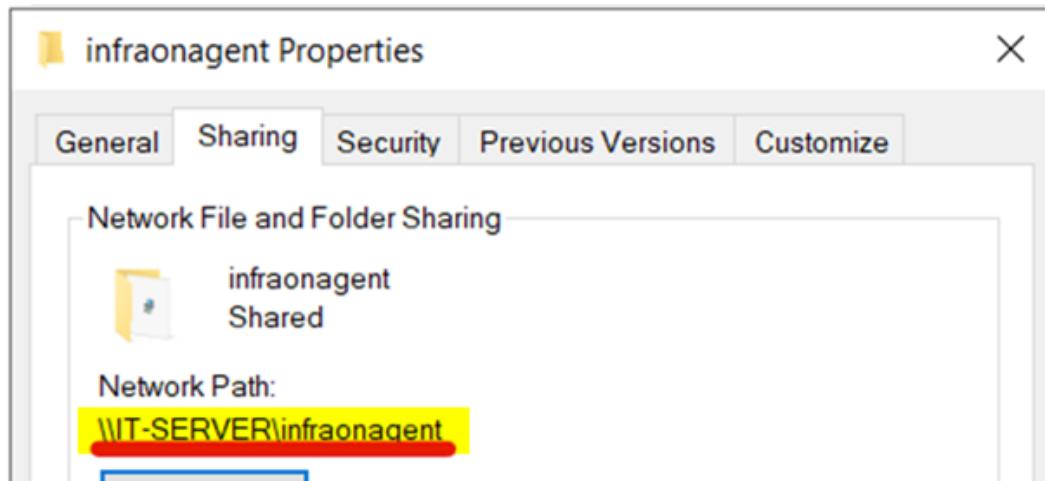
Enhanced approval functionality in workflows, such as the ticket workflow. Easily add an approval state with options for approval and rejection. Configure email settings when the approval is accepted, triggering automatic email notifications. This functionality applies to all workflows, ensuring efficient communication and streamlined approval processes.

Bots

Deployment of Infraon Agent from Active Directory via Group Policy

Pre-requisites

1. Download Infraon Agent & copy it in the Network Path as highlighted below.



Note: Please enable authenticated sharing.

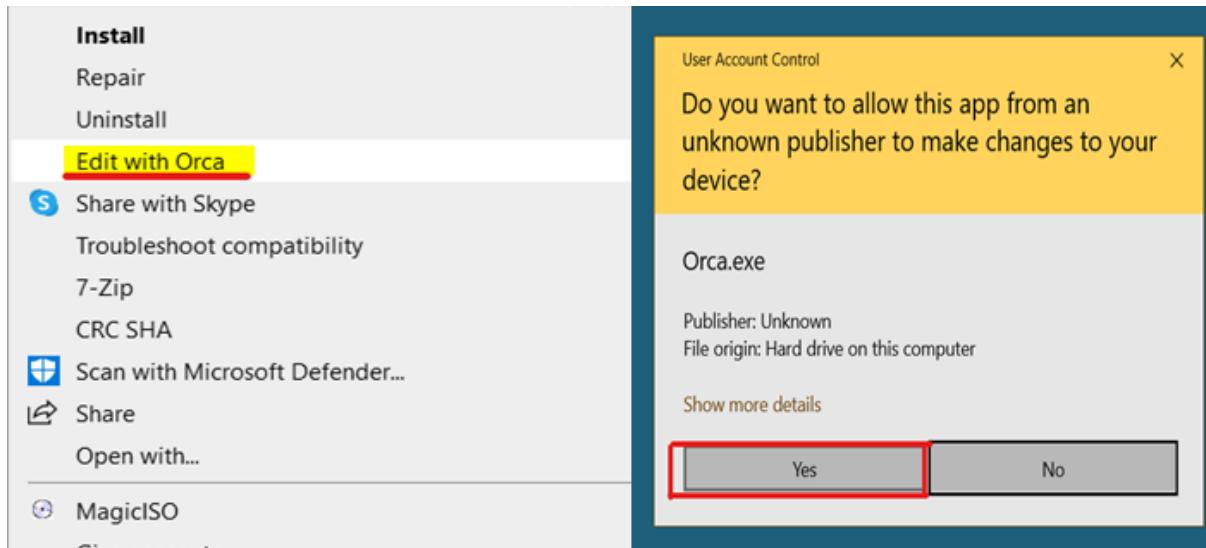
2. Download the [ORCA database table editor](#) and install it on the same server where Infraon Agent is copied. Use the network path used to pass the parameter for the MSI agent.
3. Navigate to the 'Download Inventory Agent' page of Infraon and copy the 'Agent Token' given here. This unique key is generated specifically for your organization, also called an Org Key or Organization Key.

Now, you are all set to deploy the Infraon agent.

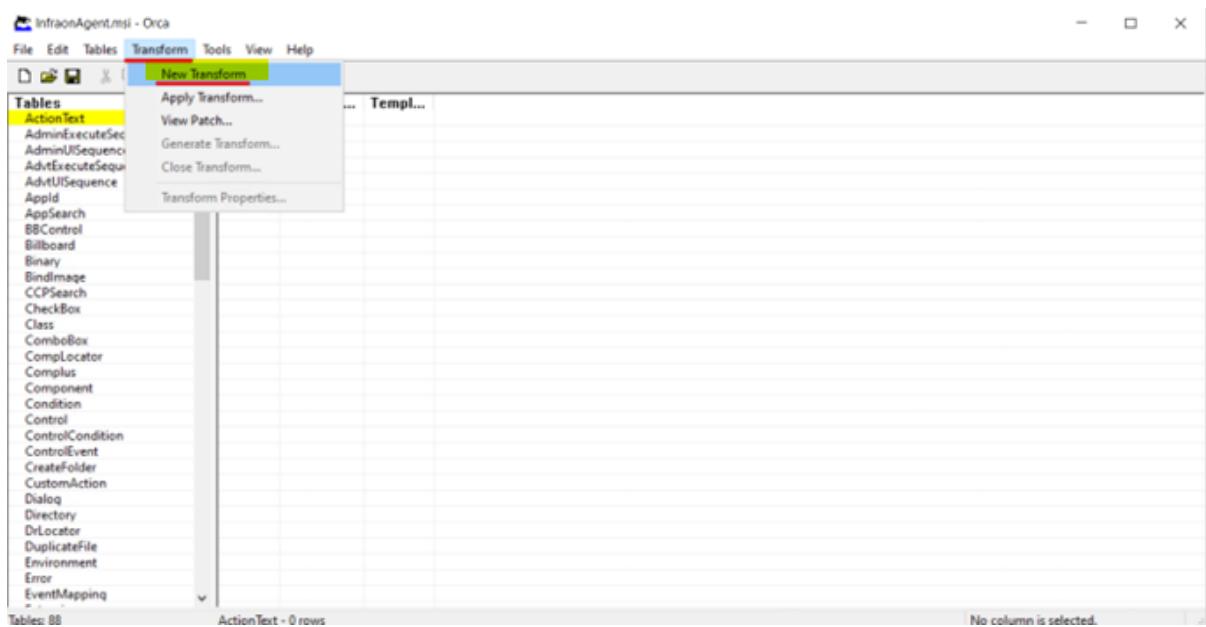
Deployment

Follow the below steps to enter the ORG_KEY in the MSI agent.

Step 1: Right Click on the **Agent**. Select **Edit with Orca** and click **Yes** to run the ORCA application.



Step 2: Open Orca. From the menu, select **Transform** -> **New Transform**.



Step 3: Find the keyword "ORG_KEY" using **Ctrl+F**.

InfraonAgent.msi - Orca

File Edit Tables Transform Tools View Help

Tables: 88 CustomAction - 19 rows No column is selected.

Tables	Action	T...	Source	Target
ActionText	_90813356_70A7_4268_8F98_2E6DFB72E7C7.uninstall	3073	InstallUtil	ManagedInstall
AdminExecuteSequence	_90813356_70A7_4268_8F98_2E6DFB72E7C7.uninstall SetProperty	51	_90813356_70A7_4268_8F98_2E6DFB72E7...	/installtype=notransaction /action=uninst...
AdminUISequence	_17D4F80C_EC6C_461A_BC48_8283B9857A7C.install	3073	InstallUtil	ManagedInstall
AdvtExecuteSequence	_17D4F80C_EC6C_461A_BC48_8283B9857A7C.install SetProperty	51	_17D4F80C_EC6C_461A_BC48_8283B9857...	/installtype=notransaction /action=instal...
AdvtUISequence	DIRCA_TARGETDIR	307	TARGETDIR	[ProgramFiles64Folder][Manufacturer]\P...
Appld	DIRCA_CheckFX	1	MSVBOPCADLL	CheckFX
AppSearch	DIRCA_CheckNETCore	1	MSVBOPCADLL	CheckNETCore
BBCcontrol	VSDCA_VsdLaunchConditions	1	MSVBOPCADLL	VsdLaunchConditions
Billboard	ERRCA_CANCELNEVERVERSION	19		[VSDVERSIONMSG]
Binary	ERRCA_UIANDADVERTISED	19		[VSDUIANDADVERTISED]
BindImage	CustomTextB_SetProperty_EDIT3	307	CPASSWORD_GUI	
CCPSearch	CustomTextB_SetProperty_EDIT2	307	PASSWORD_GUI	
CheckBox	CustomTextB_SetProperty_EDIT1	307	SUSERNAME_GUI	
Class	CustomTextB_SetProperty_EDIT4	307	EDITB4	
ComboBox	CustomTextA_SetProperty_EDIT3	307	HTTPS_PROXY_GUI	
Complocator	CustomTextA_SetProperty_EDIT2	307	HTTP_PROXY_GUI	
Complus	CustomTextA_SetProperty_EDIT1	307	ORG KEY GUI	
Component	CustomTextA_SetProperty_EDIT4	307	EDITA4	
Condition	VSDCA_FolderForm_AllUsers	51	FolderForm_AllUsers	ALL

Find
Find what: ORG KEY
Match whole word only
Match case
Direction: Up (radio button selected) Down
Cancel

Step 4: Paste the Organization Key in the target space provided. (Refer to the pre-requisite section for details).

Note: Add the org key directly. No prefix is required.

InfraonAgent.msi - Orca

File Edit Tables Transform Tools View Help

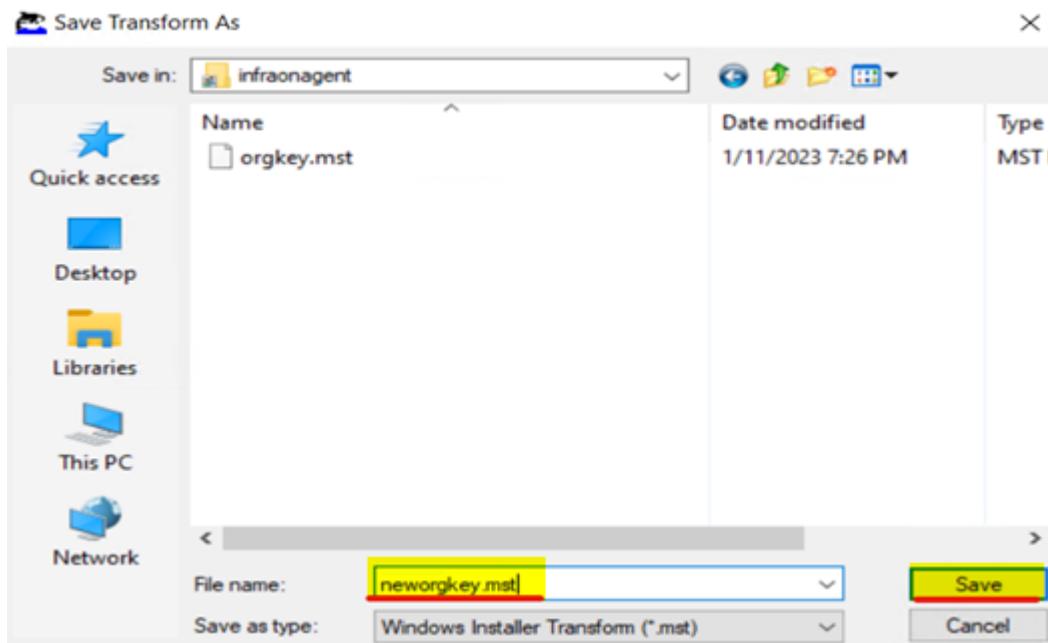
Tables: 88 CustomAction - 19 rows No column is selected.

Tables	Action	T...	Source	Target
ActionText	_90813356_70A7_4268_8F98_2E6DFB72E7C7.uninstall	3073	InstallUtil	ManagedInstall
AdminExecuteSequence	_90813356_70A7_4268_8F98_2E6DFB72E7C7.uninstall SetProperty	51	_90813356_70A7_4268_8F98_2E6DFB72E7...	/installtype=notransaction /action=uninst...
AdminUISequence	_17D4F80C_EC6C_461A_BC48_8283B9857A7C.install	3073	InstallUtil	ManagedInstall
AdvtExecuteSequence	_17D4F80C_EC6C_461A_BC48_8283B9857A7C.install SetProperty	51	_17D4F80C_EC6C_461A_BC48_8283B9857...	/installtype=notransaction /action=instal...
AdvtUISequence	DIRCA_TARGETDIR	307	TARGETDIR	[ProgramFiles64Folder][Manufacturer]\P...
Appld	DIRCA_CheckFX	1	MSVBOPCADLL	CheckFX
AppSearch	DIRCA_CheckNETCore	1	MSVBOPCADLL	CheckNETCore
BBCcontrol	VSDCA_VsdLaunchConditions	1	MSVBOPCADLL	VsdLaunchConditions
Billboard	ERRCA_CANCELNEVERVERSION	19		[VSDVERSIONMSG]
Binary	ERRCA_UIANDADVERTISED	19		[VSDUIANDADVERTISED]
BindImage	CustomTextB_SetProperty_EDIT3	307	CPASSWORD_GUI	
CCPSearch	CustomTextB_SetProperty_EDIT2	307	PASSWORD_GUI	
CheckBox	CustomTextB_SetProperty_EDIT1	307	SUSERNAME_GUI	
Class	CustomTextB_SetProperty_EDIT4	307	EDITB4	
ComboBox	CustomTextA_SetProperty_EDIT3	307	HTTPS_PROXY_GUI	
Complocator	CustomTextA_SetProperty_EDIT2	307	HTTP_PROXY_GUI	
Complus	CustomTextA_SetProperty_EDIT1	307	ORG KEY GUI	mbd7vkYEitjcur3DakqNc
Component	CustomTextA_SetProperty_EDIT4	307	EDITA4	
Condition	VSDCA_FolderForm_AllUsers	51	FolderForm_AllUsers	ALL

Step 5: From the menu, select **Transform -> Generate Transform** and save the file in the same network path where Infraon Agent is copied. Use a different name this time.

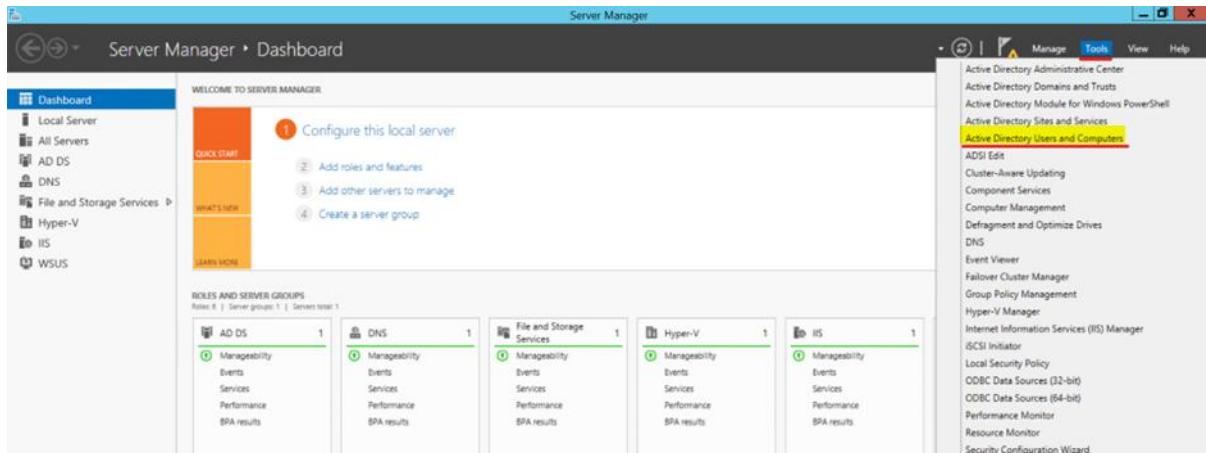
InfraonAgent.msi (transformed by Untitled) - Orca

	T...	Source	Target
68_8F98_2E6DFB72E7C7.uninstall	3073	InstallUtil	ManagedInstall /installtype=notransaction /action=unins...
68_8F98_2E6DFB72E7C7.uninstall SetProperty	51	_9D813356_70A7_4268_8F98_2E6DFB72E7...	ManagedInstall
51A_BC48_8283B9857A7C.install	3073	InstallUtil	/installtype=notransaction /action=instal...
51A_BC48_8283B9857A7C.install SetProperty	51	_17D4F80C_EC6C_461A_BC48_8283B9857...	[ProgramFiles64Folder][Manufacturer]\P...
	307	TARGETDIR	CheckFX
	1	MSVBDPCADLL	CheckNETCore
	1	MSVBDPCADLL	VsdlaunchConditions
	19	MSVBDPCADLL	[VSDVERSIONMSG]
	19	CPASSWORD_GUI	[VSDUIANDADVERTISED]
ERRCA_CHECKINGCORE	307	PASSWORD_GUI	
VSDCA_VsdlaunchConditions	307	SUSERNAME_GUI	
ERRCA_CANCELNEVERVERSION	307	EDITB4	
ERRCA_UIANDADVERTISED	307	HTTP_PROXY_GUI	
CustomTextB_SetProperty_EDIT3	307	HTTP_PROXY_GUI	
CustomTextB_SetProperty_EDIT2	307		
CustomTextB_SetProperty_EDIT1	307		
CustomTextB_SetProperty_EDIT4	307		
CustomTextA_SetProperty_EDIT3	307		
CustomTextA_SetProperty_EDIT2	307		
CustomTextA_SetProperty_EDIT1	307		
CustomTextA_SetProperty_EDIT4	307		
CustomTextA_SetProperty_EDIT4	307	ORG_KEY_GUI	mbd7vkYEitjcur3DakqNc
CustomTextA_SetProperty_EDIT4	307	FNIT4	



Note: The file type must be Windows Installer Transform (.mst)

Step 6: Connect to your AD Server. Open [Server Manager](#) -> [Tools](#) -> [Active Directory Users and Computers](#)

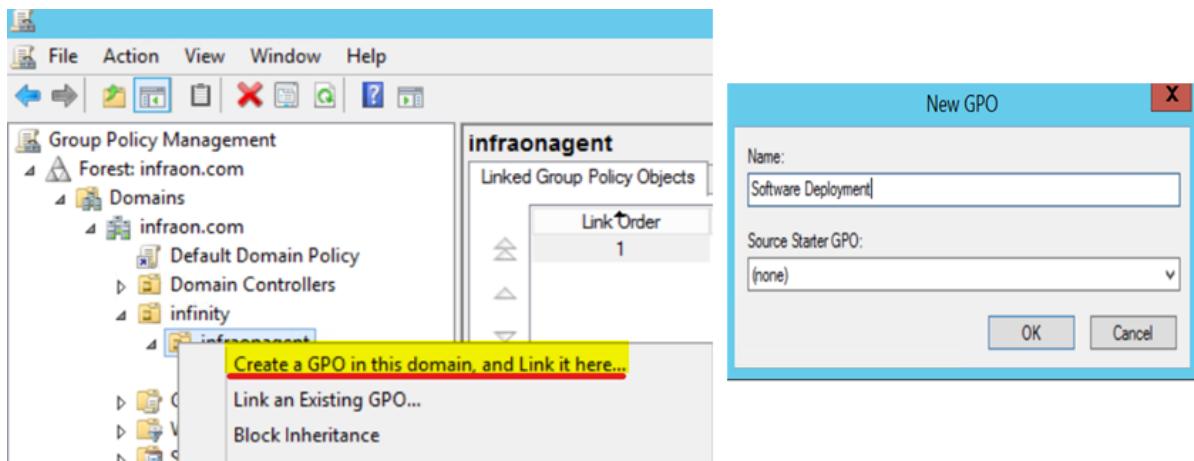


Step 7: Before deploying the agent, it is important to determine whether you are installing it at the computer or user configuration levels within the Group Policy Management editor. This can be determined based on your requirements.

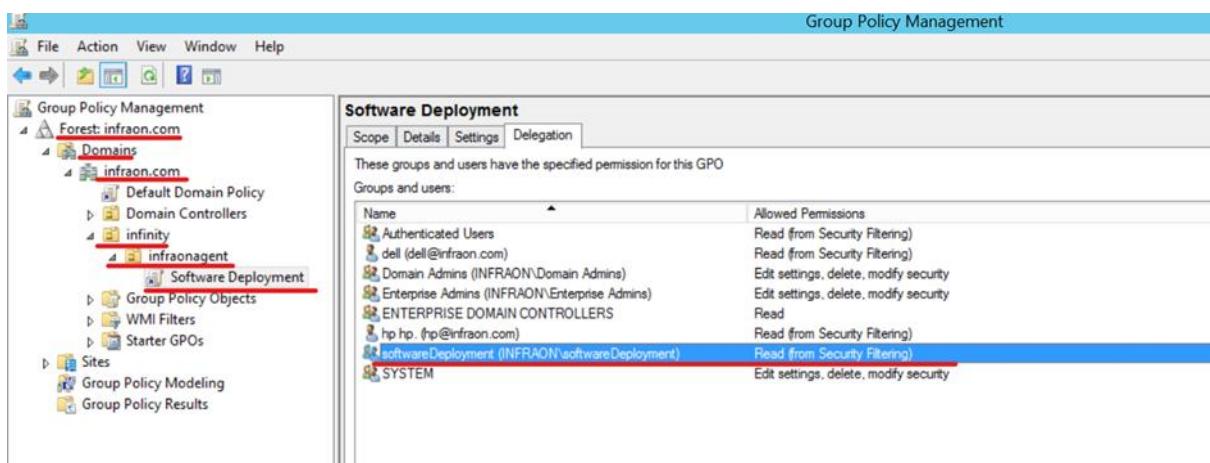
For example, we have taken 'infinity' as an OU (Operation Unit). Under this OU, we have two users added to the Software-Deployment Group. The GPO binds this group.

Name	Type	Description
dell	User	
hp hp.	User	

Step 8: Navigate to **Group Policy Management**. Right-click on the selected **OU** and select 'Create a New GPO in this domain, and Link it here...', add a name for the **GPO** and click OK. In this case, we have named it 'Software Deployment'.

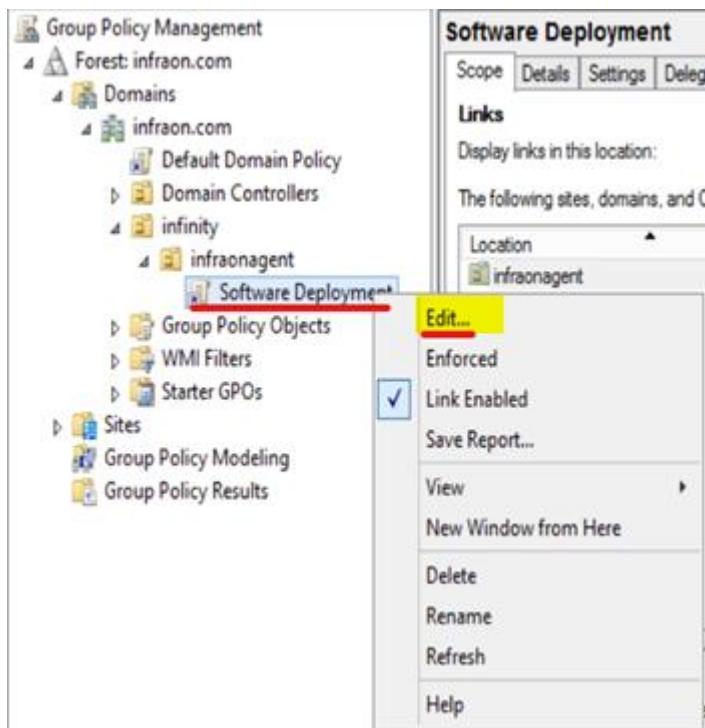


Step 9: In the Group Policy Management window, go to the "Delegation Tab," and verify whether the users or computers selected in the previous step have been added.

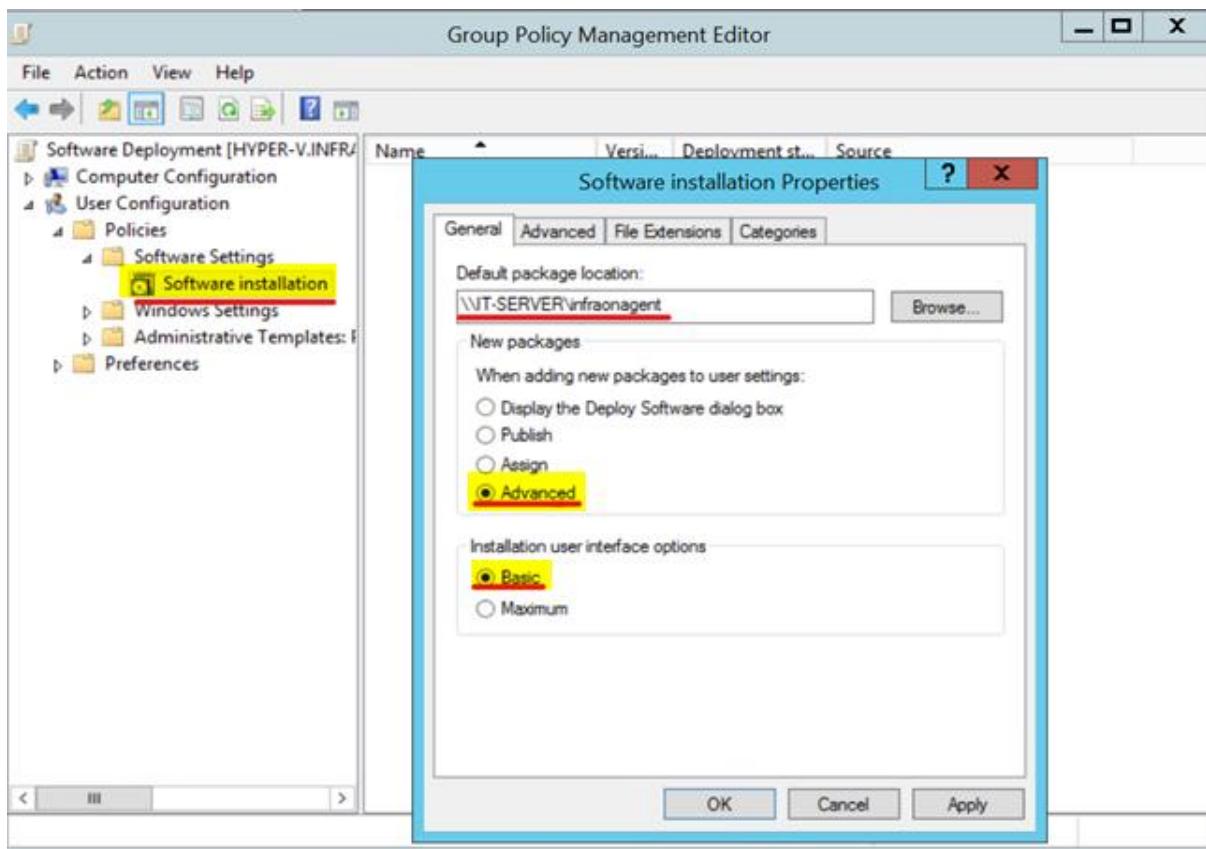


Note: Use the 'Add' button in the Security Filtering within the 'Scope' tab. Additionally, right-click on the GPO and ensure that it is 'Enforced.'

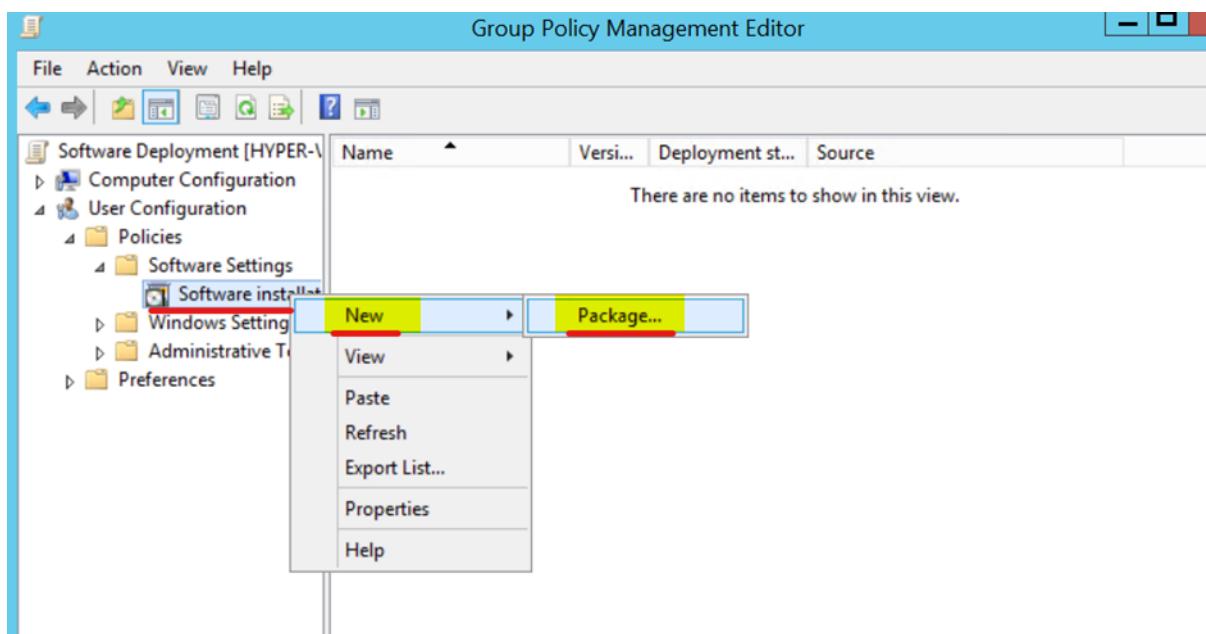
Step 10: Right-click on the New GPO, click **Edit**. The new GPO property window will open as shown below:



Step 11: Right-click on the New GPO. Select -> Properties -> Browse and select the Infraon Agent Network Path,. Ensure that "Advanced" is selected for 'New Packages' & "Basic" is selected for the 'Installation user interface option.' Click 'Ok'.

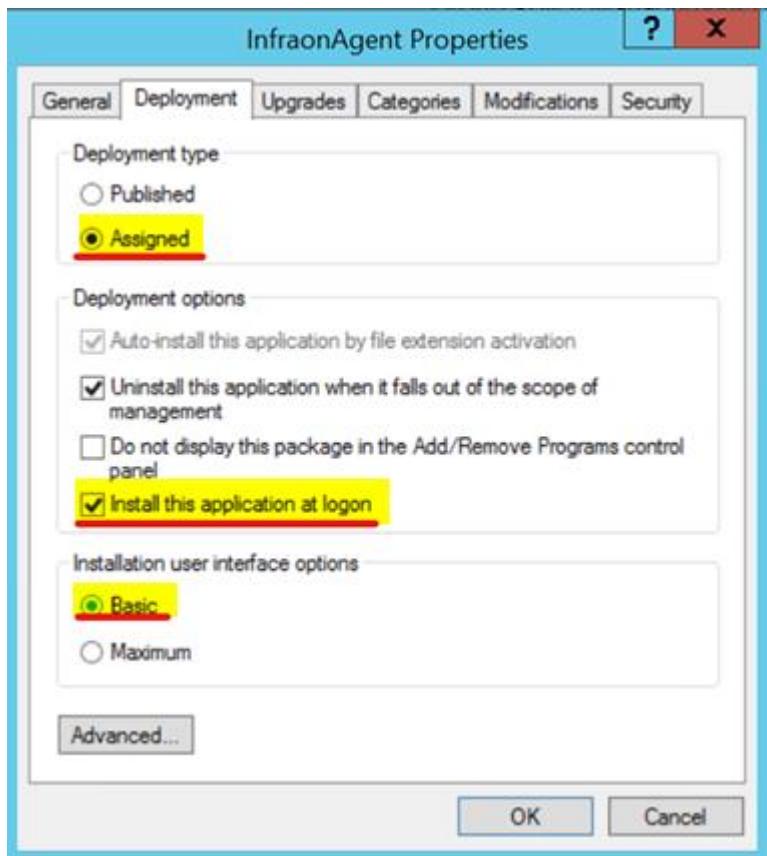


Step 12: Right-click on the new GPO link. Select [New -> Package...](#) and map the Infraon Agent in the Network Path.

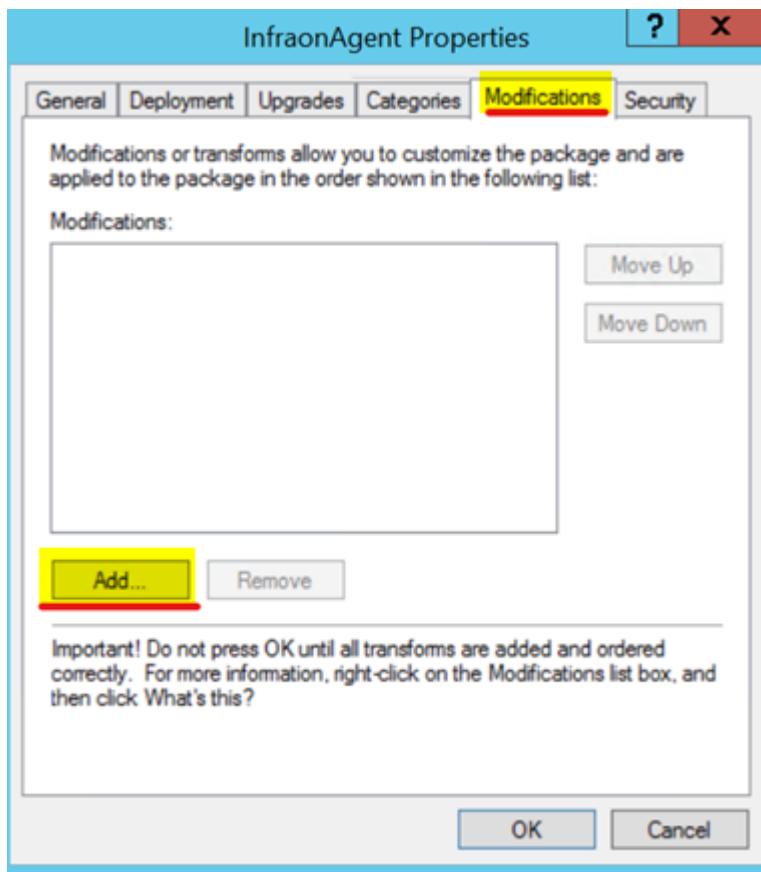


Step 13: A new Properties window will appear once the file is updated.

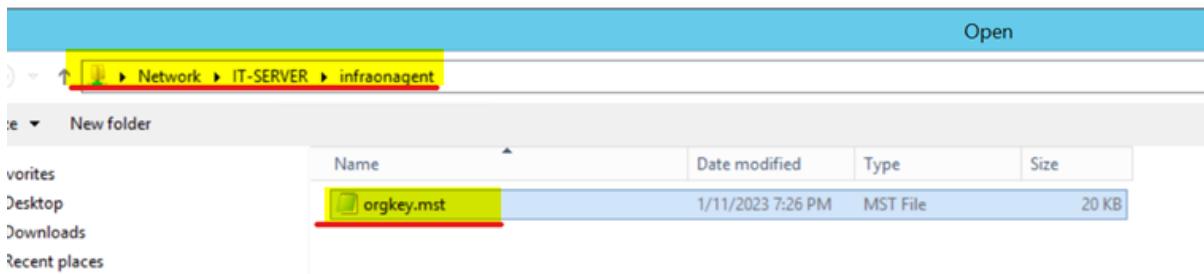
a) Navigate to the "Deployment" tab, and select the highlighted options.



b) Next, navigate to the "Modification Tab" and click Add.



c) Add the .mst file saved in the network path as shown below, and click OK.



With this, the installation of the Infraon agent in the server is complete.

Step 14: The IT administrators must instruct the users to run the [Group Policy Update command](#) & restart the device.

- Open command prompt
- Type 'gpupdate /force' and enter

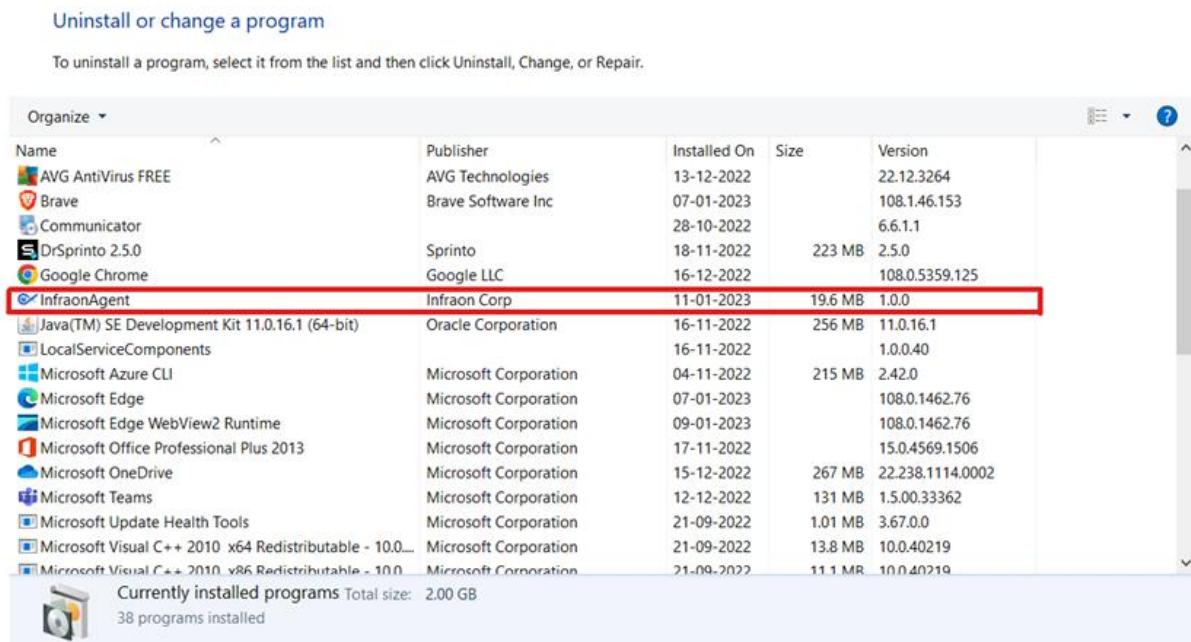
```
C:\ C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.19044.2364]
(c) Microsoft Corporation. All rights reserved.

C:\Users\          >gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
User Policy update has completed successfully.
```

Once the process is complete, restart the device.

Step 15: Log in to the device. Open [Programs and Features](#), and verify if "Infraon Agent" is installed.



You have successfully installed the Infraon agent on your device.

Bots assistance

Bots can be used for real-time problem-solving AI assistance. Admins can leverage pre-built AI bots for common queries based on various departments, which mainly include Finance, HR, IT, Legal, and Operations, or can create custom bots tailored to particular needs across various departments.

Default bots with their functionalities are stated below:

[Bots](#) | [Fields](#)

Label	Description
Finance	Offers instant access to comprehensive information topics on company policies and procedures, including financial management, expense reimbursements, accounts payable/receivable, credit & collection, cash handling & management, purchasing & procurement, financial reporting & compliance, tax Assistance, and even payroll.
HR Assistant	The HR Assistance Bot provides instant access to all your company's HR policies and procedures, including the Employee Handbook, EEO policy, anti-harassment and anti-discrimination policies, code of conduct, workplace safety, attendance, leave, performance management, compensation, privacy, social media, termination, training, remote work, travel, expenses, and even dress code topics.
IT Assistance	The IT Assistance Bot provides instant access to information and support for essential policies and procedures, including security, data protection, network access, backup & recovery, equipment acquisition, BYOD, and remote work. Boost your productivity by getting quick answers and streamlining IT processes.
Legal Assistance	The Legal Assistance Bot provides instant access to all your company's legal documents and policies, including incorporation agreements, shareholder agreements, ethics code, contract management, intellectual property, litigation, regulatory compliance, confidentiality agreements, recordkeeping, and employment law. Get quick answers and avoid legal confusion.
OPs Assistance	The Operations Assistance Bot provides instant info on all your company's operational policies and procedures, including inventory management, quality control, data privacy, supply chain & vendor management, and facilities management. Get quick answers and streamline your day-to-day operations.

Note: Admins can also customize default bots of the specific departments to align with their specific terminology and compliance requirements.

[Instructions to add Bot Assistance](#)

- Navigate to Infraon configuration -> Bots -> Bots Assistance.
- At the top right corner of the page, click on "Create New Bot"
- Add the necessary details.

Bots Configuration | Fields

Label	Description/ Example
Bot Name	Add a suitable to the respective created bot.
Description	Add a brief description of the bot.
Topics	Expand the bot's understanding by adding diverse and relevant topics to its content library. This will enable it to provide more accurate and informative responses.

Note: To ensure compatibility, please limit the uploads to plain text, PDF, or Microsoft Word files.

- Click on Validate to continue.
- Ensure the compliance of at least five bot responses by conducting a thorough review.
- Click to create the respective bot successfully.

Instructions to Initiate a Bot Assistance

- Navigate to any one of the default bot assistance and select on "Click to Initiate" option.
- Now attach the related content for the respective predefined topics. (This will enable Bot to provide more accurate and informative responses.)
- Click on Validate to continue.
- Ensure the compliance of at least five bot responses by conducting a thorough review.
- Click to initiate the respective bot successfully.

Data Collector

The Linux data collector agents are pre-configured with Infraon's token and are directly added to our system. On successful registration, this data collector can monitor other devices in the network. The data collector can do Agentless Inventory.

Download the Linux Data Collector by clicking the '[Download Agent](#)' icon. Use the 'Agent API Token' generated mainly for your organization for manual configuration. Copy this token and use it during agent installation and configuration. Once the agent is registered using this token, the agent is automatically added to Infraon. Once the installation is complete, the agent will monitor the devices on the network.

What you see on the screen

Basic Details | Information

Label	Action/ Description
Search	Search for the required Discovery.
Filter	Filter can be added based on the field and condition from the drop-down box below. (Field – Name, IP Address, Agent ID, CPU, Memory, Load, Version. Condition – in, not in, equal to, not equal to, contains, not contains.)
Name	Indicates the name of the Data collector
Last Heartbeat	Users can view the timestamp of the agent's most recent communication with the central server, indicating its current activity status.
CPU	Monitor the device's central processing unit (CPU) utilization.
Memory	Track the memory usage of the device.
Nodes	Indicates the number of node devices linked.
Load	View the overall system load on the device.
Time	Displays the current time.
Time zone	Displays the time zone linked to the device (For example: GMT +0530 IST)
KAFKA Status	Displays the KAFKA status.
Version	Displays the version number of the data collector.
Actions	
Edit	Click to make changes to the data collector.
Details	Click to view detailed information about the data collector.

Upon clicking the information action icon on the data collector, the following information is available:

- Name
- Logo
- IP address
- Last Heartbeat
- About
 - Agent ID
 - Agent Version

- Agent Build
 - Agent Time zone
 - Installation Directory
 - Agent Uptime
- Utilization
 - CPU
 - Disk
 - Memory
- Linked tags for current load and protocol-wise load can also be visible, for example:
 - Nodes
 - Resources
 - Statistics
 - Application
 - Download Jobs
 - ExternalEvent
 - HTTP
- System Info
- Processor Information
- Server Information
- Memory Information
- Disk Information
- Network Interface Information
- Process Information

NOTE: Technicians can refresh data collector information by clicking the **Resync** button, guaranteeing accurate system monitoring and management.

Inventory Agent

As a part of the 'Getting Started', you will be asked to install the inventory agent. All you have to do is to click 'Start' on the Quick Tutorial displayed for the selected agent. You can also install the agent from the 'Infraon Configuration' module.

What you see on the screen

This page provides a comprehensive view of the agents currently installed on various devices within the IT infrastructure. It serves as a central hub for monitoring agent health and managing their configurations.

[Agent List](#) | [Details](#)

Label	Description/ Example
Name	Quickly identify the specific device associated with each agent.
Last Heartbeat	Users can view the timestamp of the agent's most recent communication with the central server, indicating its current activity status.

CPU	Monitor the device's central processing unit (CPU) utilization.
Memory	Track the memory usage of the device.
Load	View the overall system load on the device.
Version	Identify the current version of the agent software installed on the device.
Actions	
Edit	Modify the configuration settings for a specific agent.
Details	Access a detailed view of the agent's information and performance metrics.
Delete	Remove an agent from a device if necessary.
Install RDP Agent	This functionality allows users to deploy a Remote Desktop Protocol (RDP) agent on compatible devices, potentially enabling remote access capabilities.

Instructions to install the Inventory Agent

Inventory agent can be installed on the following devices:

- Windows Agent - The inventory agent supports all Windows desktops/laptops, not Windows Servers. The agent can be installed on each device individually or in bulk through the Active Directory.
- Mac OS Agent - It supports all Mac versions. The agent supports devices with both Intel-based chips and M-series chips.
- Ubuntu(Linux) - Supports all Ubuntu desktops/laptops and servers.

The steps in installing an inventory agent are as follows:

- Windows Device
 - Go to Infraon Configuration -> Bots -> Agents.
 - Click the 'Download Agent' icon.
 - Download the Windows Agent.
 - The agent is downloaded to your device as an MSI file.
 - Copy the Agent API token displayed on this page. Use it at the time of agent installation.
 -

Double-click on the downloaded MSI file to initiate installation.

- Paste the Agent API token in the 'Organization Key' field and follow the prompts to finish the installation of the agent on your device.
- Add the HTTP or HTTPS proxy server details, if a proxy server is used to access the internet.
- Provide the administrator's username and password to install the Infraon agent with admin privileges. If not provided, the Infraon agent will be installed on the local account with default privileges.
- Once the agent is installed, ensure that the URL <https://instance01.wss.infraon.app/> is added to the whitelist.

[Mac OS](#)

- Go to Infraon Configuration -> Bots -> Agents.
- Click the 'Download Agent' icon.
- Download the Mac Agent.
- The agent is downloaded as a package onto your device. The package includes the PKG file and the API token.
- Double-click on the downloaded file to initiate installation. Provide your device credentials to confirm.
- Once the agent is installed, ensure that the URL <https://instance01.wss.infraon.app/> is added to the whitelist.

[Ubuntu](#)

- Go to Infraon Configuration -> Bots -> Agents.
- Click the 'Download Agent' icon.
- Download the Ubuntu Agent.
-

Your agent is downloaded as a DEB file. Open Command center. Type 'sudo dpkg -i InfraonAgent.deb' to initiate installation. Copy the 'Agent Token' from Infraon. Paste this code when the command center prompts for 'Organization Key'.

- Type 'y'(yes) to install missing dependencies.
- Your agent is installed successfully. You may use command 'journalctl -u infraonagent.service' to view installation logs. Ensure that the URL 'https://instance01.wss.infraon.app/' is added to the whitelist.

Organization

This is where you can record your organization's branch offices, vendors' location information and view license details..

The default address or the Head Office address is added based on the address given at the time of registration. Additionally, multiple branch offices can be added. Location information is used to align users, assets, and services.

Address Book

This is where you can record your organization's branch offices and vendors' location information.

The default address or the Head Office address is added based on the address given at the time of registration. Additionally, multiple branch offices can be added. Location information is used to align users, assets, and services.

Instructions to 'Add Address'

- Go to Infraon Configuration -> Organization-> Address Book
- Click on the '[New Address](#)' and select if you are adding a branch office address or a vendor's address

Label	Action	Description/Example
Location Name	Give a name to the branch office or support hub location.	Mumbai Office, Bangalore Branch Support 1, NY Support Hub, etc.
Country	Add the country	India, USA, etc.
State	Add the state	KA, MH, CA, etc.
City	Add the city	Bangalore, Los Angeles, etc.

Pin Code	Add the zip code or pin code of the address.	560078, 90001, etc.,
Landmark	Add a landmark for the address.	Near Laundromat, behind the Hyper-mart, etc.
Flat, House No. Building, Company	Add a detailed address line that includes the flat/house number, building name, or company name, as applicable,	4243 Hill Haven Drive, No.8, Garden Road, etc.
Area, Colony, Street, Sector, Village	Add an address line that includes the area, colony, street, sector, or village as applicable	Bellflower, Westminister Abbey, JP Nagar, etc.
Additional Information	Add any additional information for the address, if available.	First floor, third house on the left, etc.

Note: It is vital to add a detailed and accurate address. This address may be used for product and service delivery.

Once all the parameters are added, click '[Submit](#)' to save the location. Location details can be edited or deleted using the respective icons.

[**Edit Address Book from CSV file \(Bulk Mode\)**](#)

- Go to Infraon Configuration -> Organization -> Address Book and click on the **Bulk Edit**.
- Download the CSV file and enter the details required.
- Upload the same CSV file and click **Next**.
- Confirm the selected column matching and click **Import**.
- Validate the CSV file and click **Proceed with valid records**.

[**Edit Address Book from the Export option**](#)

- Go to Infraon Configuration -> Organization -> Address Book and click on the **Export (↓)**.
- Enter the details in the CSV file.
- Navigate to New Address -> Import from CSV.
- Upload the same CSV file and click **Next**.
- Confirm the selected column matching and click **Import**.
- Validate the CSV file and click **Proceed with valid records**.

[**License**](#)

View License details and upload based on permission.

What you see on the screen

- License Name

- Version
- Support Expiry Date
- Users
- Assets
- License Module

If you have a new license key, you can browse and add a new license key.

IT Operations

The IT Operations module is a part of Infraon Configuration and is accessible by administrators and other users authorized by administrators.

This module of Infraon consists of four additional modules. They are:

[Discovery](#) - As the user specifies, Discover network resources based on configurable parameters such as IP address, protocols, etc.. Options to discover include [Automatic](#), [Network](#), [Windows Servers](#), and [Linux Servers](#).

[Device Credentials](#) - Configure protocols and credentials for the device(s) to be discovered through Infraon.

[Job Progress](#) - To view the list of discovery jobs that are in progress.

[Thresholds](#) - View the list of default thresholds and add new thresholds, if necessary.

[Advanced Resource Configuration](#) - Will provide options to update configurations of the resources available in the system.

[Blacklist and Whitelist](#) – Define Blacklist and Whitelist information of software/applications installed.

[Correlation Rules](#) - Identify root causes of system issues by correlating server errors, network events, etc.

[Diagnosis Tools](#) – Used to identify, analyse, and troubleshoot problems or issues in various systems, devices, or networks.

[Circuit Discovery](#) – Discover the deployed trails and circuits from the network.

[LED Display](#) – Configure thresholds for parameters, monitored through Infraon.

Let's see each of these in detail.

Advance Resource Configuration

"Advanced resource configuration" refers to the process of customizing and fine-tuning various settings and parameters of a resource beyond the basic or default options, allowing for more specialized and optimized utilization in a particular context.

Steps to upload Bulk resource tag / Untag:

- Click the 'Bulk resource Tag / Untag' button from the top right panel.
- Two steps to be followed. Refer below table for reference.

Upload | Validation

Label	Action	Description/ Example
Import Bulk Resource tag/ Untag list from a CSV	Drag and drop the file or browse it to upload the CSV file.	Ensure to add resource configuration details to the default file before uploading.

Click 'Next' to proceed with Validation.

Upload | validation

The validation tab allows users to validate uploaded CSV files and provides a summary of valid and invalid records. Additionally, users can download a validation report for further analysis.

Click 'Close' after checking the validation.

Add the filter resource

- Go to IT Operations -> Advanced Resource Configuration.
- Click the 'Add' button, on the top right of the page. Refer to the below table for more information on adding the filter resource.

Label	Description/ Example
Name	Add your filter name.
Category	Select the category from the drop-down.
Condition	As per the selected category select the condition from the drop-down.

Bulk Resource Tag/ Untag categories are mentioned below:

Label	Conditions	Value
Resource Name	Contains, Equal to. Mention the value in the given space.	
Resource Description	Contains, Equal to. Mention the value in the given space.	

Resource Alias	Contains, Equal to. Mention the value in the given space.	
Resource Type	Contains, Equal to, and IN. Mention the value in the given space.	If 'IN' is selected, chose the value from the drop-down such as device, disk, Ethernet, Gigabit Ethernet, Hypervisor Host Machine, Hypervisor Snapshot, Hypervisor storage, Hypervisor virtual machine, Hypervisor virtual machine disk, INode, Interface, Link aggregate, LogicalDisk, Loop back, Memory, Networkinterface, PPP, Processor, Prop Virtaul, system, tunnel and others.
Device IP Address	Contains, Equal to. Mention the value in the given space.	
Device Hostname	Contains, Equal to. Mention the value in the given space.	
Polling Status	IN. Mention the value in the given space.	Choose the value from the drop-down either active or Inactive.
Resource tag	IN. Mention the value in the given space.	Choose the value from the drop-down such as Device, Node, NOC
Poll profile	Contains, Equal to, and IN. Mention the value in the given space.	If 'IN' is selected, choose one or more values from the drop-down such as CiscoDevice.cfg, device.cfg, esxihost.cfg, esxihoststorage.cfg, esxisnapshot.cfg, esxivmdisk.cfg, esxivmstat.cfg, ifmib.cfg, juniperexdevice.cfg, mib2if.cfg, ssgDevice.cfg, ssgDisk.cfg, sshinode.cfg, sshInterface.cfg, sshMemory.cfg, StatusIf.cfg, wmi_PerfFormattedData_PerFOS_Memory.cfg, wmi_PerfFormattedData_PerFOS_Processor.cfg, wmi_PerfFormattedData_PerFOS_System.cfg, wmi_PerfRawData_PerfDisk_LogicalDisk.cfg, wmi_PerfRawData_Tcpip_NetworkInterface.cfg
Asset Tags	IN. Mention the value in the given space.	If 'IN' is selected, choose one or more values from the drop-down

	such as IT- Asset, IT-asset, Samsung, TAG1, Windows, Core, noc, and more.
--	---------------------------------------------------------------------------

Click 'Cancel' to cancel the filter resource created. To save click 'Save and Proceed' button.

Configure the Advanced Resource Configuration

- Go to Infraon Configuration -> IT Operations -> Advanced Resource Configuration.
- Click the 'Configure' icon under the action tab.

Click the 'Action' button on the top right of the page and select the actions from the drop-down such as:

1. **Tag:** Select Tag from the drop-down and click the 'Submit' button.
2. **Enable Polling:** Click 'Enable polling' when the pop-up appears.
3. **Disable polling:** Click 'Disable polling' when the pop-up appears.
4. **Change poll period:** Mention the poll period in the given space and click the 'submit' button.

To Export the configuration, click on the 'Export' icon at the page's top right corner.

Blacklist and Whitelist

In the realm of software and application security, two key concepts arise: blacklisting and whitelisting. These methods, though seemingly opposite, both play crucial roles in safeguarding your system from unwanted programs and vulnerabilities.

What is blacklisting?

Blacklisting operates on a principle of exclusion. A blacklist is a curated list of programs deemed undesirable, malicious, or unauthorized. Software identified on the blacklist is then blocked from installation or execution on a system. Here are some common reasons why software might be blacklisted:

- Known malware or viruses: These programs are designed to harm your system, steal data, or disrupt operations.
- Unwanted applications: Some software might be considered disruptive or inappropriate for certain environments.
- Pirated software: Using illegal copies of software can be harmful and is often blacklisted.
- Vulnerable applications: Programs with known security flaws pose a risk and might be blacklisted until patched.

What is whitelisting?

Whitelisting, on the other hand, takes the opposite approach. Instead of listing what's bad, it defines what's good. A whitelist is a curated list of programs explicitly permitted to be installed or run on a system. Any software not on the whitelist is automatically restricted.

Whitelisting offers several advantages:

- Enhanced security: Only authorized and vetted software can run, significantly reducing the risk of malware and unauthorized access.
- Simplified management: Administrators have complete control over what software is allowed, making it easier to maintain a secure environment.
- Improved compliance: Whitelisting can help organizations comply with specific security regulations or internal policies.

Steps to add the configuration

- Go to Infraon Portal -> Infraon Configuration -> IT Operations -> Blacklist and Whitelist.
- On the top right corner of the page navigate to the 'Add' button to add a new configuration.
- Enter the below details in the respective dialog boxes.

Label	Action	Description
Type	Select the appropriate from the drop-down box below.	Example – Software, etc.
Profile		Enter a profile name to the configuration.
Description		Enter a brief description about the configuration.
Blacklist	Select the appropriate from the drop-down box below.	
Whitelist	Select the appropriate from the drop-down box below.	

CLI Jobs/ Sessions

CLI Jobs/sessions in NCCM create direct CLI sessions (SSH or TELNET) between the Device and the User through the NCCM application. Using a CLI Job, the user can write direct commands on devices similar to the Putty application.

The user will request a CLI connection by inputting the Device IP Address, Device account username (in case of SSH), and the reason for the connection. Based on the user's role (administrator privileged, CLI whitelisted, or normal user), the CLI job will either open a direct connection to the device or put the CLI request into the **Request Queue** for Change Approval process.

The CLI Job will audit all device user commands, including device response. NCCM does not provide command restrictions in case of Policy violations. The NCCM Policy engine remediates policy violation commands periodically.

This is a privilege-based feature:

The user can access, view, add, edit, delete, execute, and export only if the administrator has given them privileges. These will be defined under roles and privileges.

The user will be white-listed for CLI operations (no need for Approval) only if the "CLI Job Pre-Approved" permission is enabled in the Account Roles and Privileges.

From the "**Jobs**" menu, click '**CLI Jobs/Sessions**'

- All CLI Jobs, including history connection and live session, are listed with their active status.

What you see on the screen

Clicking the session details icon will display live audits.

Note: CLI Jobs requested by Non-Whitelisted users will be submitted for approval and executed only when approved. However, Whitelisted users' CLI Jobs will be executed without approval.

Using this audit, the administrator can identify the changes, the user responsible for them, and the time of the change.

CLI Jobs not approved within the expiry time will get to the Expired State, and the expiration duration can be configured using System Parameters.

Action Icons – CLI Jobs/Sessions

Label	Action/ Description
Search	Search for the required CLI job.
Filter	A filter can be added based on the field (Job Name, Client IP, Device IP Address, Device Account, and Reason), and the condition can be selected from the drop-down box below.
Terminate Session	Terminating CLI abruptly ends an unresponsive session, stopping all active processes. Re-establishing the connection may be required.
Close CLI	Close CLI gently ends a CLI session, ensuring all tasks are finished before closing, preventing data loss.
Assets	Click to navigate to the Assets page

Export as ELXS	Click to download the “CLI Jobs” in an ELXS file
Go to Assets	Click to navigate back to the asset page.
Actions	
Session Details	Click to view the session details
View Session Terminal	Click to view the session terminal

CLI Jobs/Sessions Search

- Select the time from the calendar options.
- Input the Requester Name in the textbox.
- Input Client IP Address in textbox.
- Input Device IP Address in textbox.
- Select Device Group using the dropdown menu.
- Input Device Account in the textbox
- Select ‘Protocol Type’ using the dropdown menu.
- Select Status using the dropdown menu.
- Select ‘Approval Type’ using the dropdown menu.
- Input ‘Approver Name’ in the textbox.
- Input the Reason in the textbox.
- Input the command in the textbox.
- Click “Search” to perform the search.

Terminate Session

A checkbox appears on the job row when a CLI job is in progress. The user can select the CLI job and terminate the session immediately.

- Select Job and click “**Terminate CLI Session**” to terminate the session.

CLI Job/Session Export

Navigate to the top panel at the right corner of the page; click the “CLI Jobs” option to download an ELXS file.

Circuit Discovery

Discover the deployed trails and circuits from the Network. It enhances the overall functionality, performance, and connectivity of the network.

What you see on the screen

Label	Action	Description/ Example
Search	Search for the required Discovery.	
Filter	Filter can be added based on the field and condition from the drop-down box below.	Field – Circuit Type, Profile Name, Technology. Condition – in, not in, equal to, not equal to, contains, not contains.
Add	Click to add a new Circuit Discovery.	Follow the below steps to add a new Circuit Discovery.
Profile Name		Indicates the Name of the Profile assigned.
Technology		Indicates the type of technology (SDH, PDH, VSAT, IP/MPLS).
Circuit Type		Indicates the circuit type (E1, Ethernet, Data, etc.).
Schedule Type		Run Immediately or Schedule for an hour, week, etc.
Current Status		Displays the current status of the Profile.
Last Action		Indicates the date and time of the last discovery.
Next Action		Indicates the date and time of the next discovery.
Actions		
Audit	Click on the Audit button to view the Circuit Discovery Result. Top of Form	Iteration, Iteration ID, Next Iteration, Start Time, End Time, Duration, and selected discovery options.
Edit	Click on the Edit button.	Make changes to your Circuit Discovery.
Delete	Click on the Delete button.	Click this button to delete the selected Circuit Discovery permanently. (Use a trash can icon)

Rescan	Click on the Rescan button.	This option can be used to rescan the Circuit Discovery tab.
---------------	-----------------------------	--------------------------------------------------------------

Steps to add a new Circuit Discovery

- Go to Infraon OSS portal -> Infraon Configuration -> IT Operations -> Circuit Discovery.
- Navigate and click on the 'Add' button at the top right corner of the page.
- Enter the respective dialog boxes.

Label	Action	Description/ Example
Profile Name	Add a Profile Name to your Circuit Discovery.	Test, Run, etc.
Technology	Select from the drop-box below.	SDH or PDH.
Circuit Type	Select from the drop-box below.	E1, Ethernet, STM, Voice or Data.
Discovery Schedule		
Run Immediately	Click to select Run Immediately.	Selecting this, Circuit Discovery will create it immediately.
Schedule Immediately	Click the schedule mode at once, every, daily, weekly, or monthly at a specific chosen time.	Selecting this Circuit Discovery will create it immediately, but the scan will happen at a scheduled time.

Once entering all the credentials, click 'Submit' to save the Circuit Discovery.

Rules

Log Rule

A robust Infraon Infinity solution must monitor certain events in real-time to facilitate swift responses to security threats. Log rules are essential components that define how log data is processed, examined, and acted upon within logging and monitoring systems.

Note: Ensure you have the appropriate permissions before creating or modifying alerts.

Infraon's alerting system allows you to set up rules that continuously scan log data for specific conditions. When these conditions are met, the system triggers predefined alerts.

In essence, rules are predetermined scenarios that, when matched, initiate an alarm, event, or configured action. Each rule consists of three key elements:

- A specific query to be executed
- Parameters that determine what constitutes a rule match
- A set of alerts to be triggered when a match occurs

Rule Types:

Infraon Infinity allows you to set up rules that can trigger alarms or send notifications to users through email or SMS. These rules are based on specific criteria you define, such as error rate thresholds or particular log patterns. The system offers two main types of rules:

Custom Query

Custom query rules use tailored search parameters to identify alert-worthy conditions in your log data. To set up a custom query rule:

- Formulate a query that filters the log data you want to monitor
- Design the query to capture the exact conditions that should trigger an alert
- Specify how often the system should run this query to check for matching log entries (e.g., every 5 minutes)

Threshold Rule

Activates when defined thresholds are reached. Select the metric or data point for monitoring. For instance, you could track the number of error logs or the average response time. Establish the alert triggers, such as limits for high error frequencies or unexpected data surges.

- Trigger Condition: For example, if the error tally reaches over 100 in 5 minutes.
- Alert Frequency: The regularity of condition assessment (e.g., every 5 minutes).

Instructions to add a New Log rule

- Go to Infraon configuration -> IT Operations -> Rules and click on the 'New Rule' button at the top right corner and Add Log rule option to continue.
- Refer to the table below to add the details respectively.

Add Log Rule | Details

Label	Action/ Description	Example
Log Rule		
Name	Add a name to the Log rule	
Description	Add a brief description of the Log rule	

Status	Activate the rule by switching the toggle button on. The rule will only function when its status is on.	
Rule Type	Select the respective rule type from the below call-out boxes.	Custom query and Threshold Count.
Criteria		
Index Pattern/ Data View	Select the type of data to be entered.	
Value	Input the relevant value in the Multi-Index field to specify which index the rule should be applied to.	Windows*, or windows-2024.09.12, windows-2024.09.13
Custom Filters	Add custom filters to define specific conditions for your logs or metrics.	For example, you might want to filter logs where the <code>status_code</code> is 500 and the <code>response_time</code> exceeds 2s.
Check Every	This will run periodically and detect alerts within the specific time frame.	2 seconds/minutes
Look Back	Add time to the look-back period to prevent missed alerts.	3 seconds/minutes
Group By	Add the field by which you want to group. This could be any field from your logs or metrics.	For example, you might group by <code>service_name</code> to get separate alerts for each service.
Count	Add the respective count from the drop-down box below.	Hostname, IP Address, Message, Agent Name, Host ID.
Threshold	Set a limit for how many times a certain event can happen. This limit is based on the group of users you're looking at.	2,3,4.... Etc.
Action		
Severity	Choose the appropriate urgency level for the event this rule will generate from the drop-down box below.	Critical, Major, and Minor are the highest and Minor the lowest.
Alarm/ Event Message	Enter a personalized notification text that will appear in the event when the rule is triggered.	

Once the details have been added, click “Save” to confirm the rule configurations.

Correlation Rule

Topology Correlation

Topology-based correlation uses topology data to correlate defined related events. It is a solution that uses topology-based techniques to provide automated root cause analysis, service impact analysis, and customer impact analysis. It helps network operators identify the root causes of issues and quickly determine the services and customers affected by network events.

Event Based Correlation Rule

Event correlation refers to the processes involved in sensing and analyzing relationships between events. By correlating the parent and child events occurring in the network, event correlation automatically reduces the noise and allows IT to focus on those issues that really matter to the business service and IT objectives.

Instructions to add a new correlation rule

- Go to Infraon configuration -> IT Operations -> Rules and click on the ‘New Rule’ button at the top right corner and select Correlation Rule.
- Add the respective Correlation Rule Details, select the criteria and add the action details.

What you see on the screen

Label	Action	Description/Example
Name	Add a name for the credential	Applicable for all protocols. A name is usually used as an identifier.
Description	Add a brief description of the profile	Applicable for all protocols
Status	Select the status of the configuration.	The status of the configuration can be Active or In-Active.
Parent Event	Select from the drop-down box.	The type of complication has occurred in the event.
Child Event	Select from the drop-down box.	The type of complication has occurred in the event.

Match Criteria	Select from the drop-down box.	Match whether it's for one or more than one event.
Correlation Window	Select the time in minute(s)	The required for the correlation window.
Group by	Node	
Filter	Filter a range of data based on the criteria you define.	
Severity	Select severity using the dropdown.	Available options are critical, major, and minor.
Alarm/ Event Message	Add a message for the configuration.	This message will be included in the trap configuration alarm/notification.
Clear Message	Add a message for the configuration.	This message will be included in the configuration alarm/notification.

Once you've filled in all the information, click the "Submit" button to save your credentials.

Device Credentials

The device Credentials module of Infraon is used by the administrator/authorized user to configure and store Device/Account information such as login credentials (user name, password, and other protocol-relevant parameters) of a specific connection protocol. Device Credentials are used in 'Discovery' and are mandatory for discovering devices for monitoring and management.

Appropriate device communication protocol must be selected while configuring device credentials to build successful connectivity.

Each device shall be associated with a device credential at the time of discovery. Subsequent monitoring is done using these stored credentials. Should there be any change in the login credentials (password), the administrator must update the same to ensure seamless monitoring.

Devices and Protocols

At this point, Infraon supports SNMP, WMI, SSH, and HTTP protocols below. Refer to the below table for details.

Protocols	Description	Supported Devices	Protocol Parameters
SNMP	SNMP v1 and v2c versions use community-based security models and user read& Write Community for access. SNMP v3 version uses an enhanced user-based security model and uses authentication and encryption. If v3 is selected, related parameters need to be configured. Refer 'SNMP v3 Parameters' section for details.	Most Network devices, Servers, and other SNMP-supported devices.	SNMP v1 and v2c: Read & Write Community, Port, Timeout, and Retries. SNMP v3: Username, Security Level, Authentication Type, SNM V3 Password, Privacy Type & Privacy Password.
SSH	SSH or Secure Shell protocol establishes an encrypted connection between network devices.	CLI Option for network devices, Linux, Unix-based servers, and Xen servers.	Login Name, Login Prompt, Password Port, SH Key File, Connection Command, Timeout, and Retries.
WMI	WMI commonly uses CIM conceptual model to represent various components of windows devices.	Windows Servers	Domain Name/user Name, Password, Authentication Level, Impersonation level, Timeout, and Retries.
HTTP	HTTP acts as the foundation of data exchange on the web.	vCenter, VMware API, CUCM cluster	Username and Password

Click 'Test and Save' to test the credentials for authenticity before saving and proceeding to discovery.

What you see on the screen

The device credentials page can be used to add, edit and delete device credentials for the SNMP, SSH, WMI, and HTTP.

The device credential view can be toggled between the card view and the list view using the respective icon.

Instructions to 'Add Device Credential'

- Go to Infraon Configuration -> IT Operations-> Device Credentials.
- Click on 'Add' and select 'Protocol' as desired.

There are two tabs on the 'Add Credential' page. Refer to the table for information.

[Configuration](#) | Test

Few fields vary based on the protocol selected. Refer to the 'Description' column for details.

Label	Action	Description/Example
Profile Name*	Add a name for the credential.	Applicable for all protocols. A name is usually used as an identifier.
Description	Add a brief description of the profile.	Applicable for all protocols.
Port	The default value is auto-populated. This, however, can be changed.	Applicable for SNMP and SSH.
Timeout (Seconds)	The default value is auto-populated. This, however, can be changed.	Applicable for all protocols. The number of seconds post which Infraon stops attempting to reach the device.
Retries	The default value is auto-populated. This, however, can be changed.	Applicable for all protocols. The number of instances Infraon tries to reach the device.
For SNMP	Select the SNMP version, as applicable. Based on the selection, additional fields appear.	Applicable for SNMP only V1 - Read Community*, Write Community v2c - Read Community*, Write Community, Scan Requests v3 - User Name, Context Name, Security Level, Authentication Protocol, Authentication Password*, Privacy Protocol, Privacy Password*, Scan Requests
For SSH	Select between Credential, and Public Key, as applicable. Based on the selection, additional fields appear.	Applicable for SSH only Credential - Login Name*, Password, Login Prompt, Enable Password, Enable Prompt Public Key - Hash Key* v3 - User Name, Context Name, Security Level, Authentication Protocol, Authentication Password*, Privacy Protocol, Privacy Password*, Scan Requests.

For WMI	Select between WMIC, and WinRM, as applicable. Based on the selection, additional fields appear.	Applicable for WMI only Login Name* and Password* are standard fields for WMIC and WinRM. WMIC - Authentication WinRM - WinRM Authentication Level, Protocol, WinRM Port, WinRM Certificate Validation, WinRM Certificate File, WinRM Public Key.
For HTTP	Select between HTTP, and HTTPS, as applicable. Based on the selection, additional fields appear.	Applicable for HTTP/HTTPS only HTTP - Username*, Password* HTTPS - Username*, Password*,

Once all the parameters are defined, click 'Submit' to save the credentials or click 'Test & Save' to test the credentials before saving.

Configuration | [Test](#)

Label	Action	Description/Example
IP Address*	Add an IP address to test the credential.	Applicable for all protocols.
Agent*	Select agent to test.	Applicable for all protocols

Click '[Test](#)'.

Saved credentials can be edited or deleted by using the respective action icons.

Note: Credentials must be correct to ensure seamless discovery.

Diagnosis Tools

Used to identify, analyze, and troubleshoot problems or issues in various systems, devices, or networks.

Ping

A method of determining latency or the amount of time it takes for data to travel between two devices or across a network.

Infraon uses the Ping option, which is a diagnostic tool that checks if your device is reachable. Infraon sends a data packet to the device and, in return, receives a data packet if the connection is complete.

How to perform PING Diagnosis

Click 'Ping' and enter the following details:

Label	Description/ Example
IP Address	A unique number identifying your device.
Data Collector	Select from the drop-down box.
Count	Select the count preferred.
Packet Size	Select the required one in either of 16/32/64...
Timeout	The number of seconds post which Infraon stops attempting to reach the device.

Click 'Test'. The test results will be displayed in real-time.

SNMP Walk/MIB Walk

Utilized for overseeing and controlling network devices interconnected via an IP network.

Infraon uses SNMP, which is an application that queries the network for a tree of information about a selected device.

How to perform SNMP Diagnosis

Click 'SNMP Walk' and enter the following details:

Label	Description/ Example
IP Address	A unique number identifying your device.
Data Collector	Select from the drop-down box.
OIDS	Object Identifiers
Port	The default value is auto-populated. This, however, can be changed.
Version	Select the required version.
Read Community	Enter the confidential credential.
Write Community	Enter the confidential credential.
Get Bulk	Selecting this would configure for all the items.
Get	Selecting this would configure for one single item.
Retries	Selecting this would automatically repeat an action until it succeeds.

Click 'Test'. The test results will be displayed in real-time.

SSH Check

A communication protocol for computer networks that facilitates data exchange and interaction between two computers.

How to perform SSH Diagnosis

Click 'SSH Check' and enter the following details:

Label	Description/ Example
IP Address	A unique number identifying your device.
Data Collector	Select from the drop-down box.
Port	The default value is auto-populated. This, however, can be changed.
Login Name	Enter your selected login name.
Password	Enter the password.
Login Prompt	Enter the login Prompt.
Enable Password	Enter the Enable Password.
Enable Prompt	Enter the Enable Prompt.
Timeout	The number of seconds post which Infraon stops attempting to reach the device.
Retries	Selecting this would automatically repeat an action until it succeeds.
Hash Key	Input the required Hash Key for authentication.

Click 'Test'. The test results will be displayed in real-time.

WMI Check

Microsoft's specifications for centralized management of devices and applications in Windows networks.

How to perform WMI Diagnosis

Click 'WMI Check' and enter the following details:

Label	Description/ Example
IP Address	A unique number identifying your device.
Data Collector	Select from the drop-down box.
Login Name	Enter your selected login name.
Password	Enter the password.

Timeout	The number of seconds post which Infraon stops attempting to reach the device.
WinRM	Windows Remote Management
WMIC	Windows Management Instrumentation
Authentication Type	Select from the given drop-down box.
Transport Method	Select from the given drop-down box.
WinRM Port	Enter the WinRM Port details.
Authentication Level	Select from the given drop-down box.
Impersonation Level	Select from the given drop-down box.

Click 'Test'. The test results will be displayed in real-time.

Discovery

Infraon uses multiple protocols to monitor and manage multi-vendor/multi-technology networks, such as IT Infrastructure, Core IP Backbone, Fiber, Transport, Transmission, and SCADA, and data center networks, such as Servers (both physical and virtual platforms), hosted applications, and databases. Infraon supports IPv4 and IPv6-based environments and is proven to scale in monitoring capabilities.

Infraon provides multiple ways to discover networks using:

- EMS/NMS Registration and Discovery
- Automatic Network Discovery (based on CIDR, IP Range, Hostname)
- Single Node Discovery (Protocol Specific)
- CSV Based Discovery (For bulk provisioning with additional manual input data for enrichment)
- Hypervisor Discovery
- Application-Specific Discovery
- Database Discovery
- Scheduled Discovery (for Network Change Detection)

Infraon's discovery process

- Scans network as per the given input (IP range, selected protocol, and discovery options set)
- Identifies inventory details (refer to below list) in node level
 - Hostname
 - IP Address

- Make/Model/Series/OS details
 - Device Type
 - Gateway
 - Location
 - Contact Details
 - Individual Component Details
- Collects inventory-specific details at the node and component levels.
- Creates monitoring profile for the node and component per the defined KPI.
- Initiates monitoring process for nodes and components.

Discovery Types

Multiple forms of discovery allow for the addition of a wide range of devices. As a result, Organizations will have comprehensive coverage of devices:

- [Automatic Discovery](#) - Discovers all network resources based on various protocols.
- [Network Discovery](#) - Discovers network devices using SNMP.
- [Windows Servers](#) - Discovers Windows servers using WMI Protocol.
- [Linux Servers](#) - Automatically discover SSH-supported devices.

Automatic Discovery

The automatic Discovery option can discover Network, Windows, and SSH-supported devices.

Initiate Automatic Discovery

There are three tabs on the 'Automatic Discovery' page.

[Discovery Details](#) | [Filters](#) | [Schedule](#)

Label	Action	Description/Example
Profile Name*	Add a name for the Discovery Profile. Discovery Profiles are created to save preferences and identify profiles to track and initiate discovery periodically.	The name of the profile helps identify the profile.
Discovery Options	There are two options for discovery. Choose the option that suits your requirement.	1. Discover inventory with availability and performance monitoring. 2. Discover only Inventory Information.

		3. Discover inventory with availability and performance monitoring.
Provide Profile Details	Add a brief description of the discovery profile.	For example, For WMI devices, Desktops only, etc.
IP Address*	Type IP, IP range, or Subnet IP to be discovered.	192.168.11, etc
Import from CSV	Import device list from a CSV to start monitoring.	
Configuration Download	Click the toggle button to make changes	Click here to access the detailed Configuration job content and manage your network jobs effectively.
Device Credentials	Select the relevant device credential using the drop-down menu.	Device Credentials must be pre-configured for selection.
Add to NCCM	Select the toggle button to make changes	Discovered network devices are automatically added to NCCM for management, backup, change, compliance, and monitoring.
Agent Details*	Click the Pick Agents Here button to add the agent details.	Infraon agent collects data from devices configured for discovery. It can support SSH, SNMP, WMI, etc.

* Fields are mandatory.

Note: Import from CSV file is optional. Without importing CSV, you can click the 'Next' button.

[Discovery Details](#) | [Configuration Download](#) | [Details](#)

Profile Details:

- Select Configuration profile (only if the Range of Input Devices can have the same profile to manage) or keep it as 'Select Configuration Profile.' NCCM will automatically find the right Profile for each device during discovery.

Protocols:

- Select the Connection protocol (for all the Range of Input Devices that can have the same Connection protocol), or NCCM will automatically set the default connection Protocol from System Parameters.
- Select the Configuration Download protocol (for all the Range of Input Devices that can have the same Configuration Download protocol), or NCCM will automatically set the default Download Protocol from System Parameters.

- Select the Other configuration Download protocol (for all the Range of Input Devices that can have the same Other configuration Download protocol), or NCCM will automatically set the default Other configuration Download Protocol from System Parameters.
- Select the Inventory Download protocol (for all the Range of Input Devices that can have the same protocol), or NCCM will automatically set the default Inventory Download Protocol from System Parameters.
- Select OS Image Download Protocol (for all the Range of Input Devices that can have the same OS Download protocol), or NCCM will automatically set the default OS Download Protocol from System Parameters

Schedule Download:

For a [Discovery Schedule](#), refer to the table.

Label	Action
Schedule Mode	Click the discovery schedule mode at once, every, daily, weekly, or monthly.
At	Click the calendar icon to add the date and time to the next column.

Click '[Next](#)' to add details on '[Filters](#).'

[Discovery Details](#) | [Filters](#) | Schedule

'Filters' has two sections: Device Filters and Server Component Filters.

[Device Filters](#) | Server Component Filters

Label	Action
Device Filters	Click the first condition box to include or exclude devices.
Include Devices/ Exclude Devices	Click the second condition box to add an IP address, Device Type, or Device Name.
	If you have chosen Device Name in the second condition box, Click Equals or Contains in the third condition box.
	Add a number or device name to enter the fourth condition box.

Include Devices/Exclude Devices -> IP Address/Device Type/Device Name -> Equals/Contains -> Number or Device name

[Device Filters](#) | [Server Component Filters](#)

Label	Action
Process	Enable or disable the 'Process' button.
Service	Enable or disable the 'Service' button.
SQL	Enable or disable the 'SQL Core Monitoring' button.
DotNet	Enable or disable the 'Dot-Net core monitoring' button.
Exchange	Enable or disable the 'Exchange Core Monitoring' button.
Share Point	Enable or disable the 'Share Point Core Monitoring' button.
Active Directory	Enable or disable the 'Active Directory Monitoring' button.
IIS Monitoring	Enable or disable the 'IIS Monitoring' button.

Note: 'Filters' tab is optional. You can click the 'Next' button without adding details on Filters.

After adding Device Filters, click 'Next' to add 'Schedule.'

Discovery Details | Filters | [Schedule](#)

Before clicking on the Schedule tab:

There are two options for scheduling discovery: either 'Discover Now' or a 'Discovery schedule' time. If you enable the button on 'Discovery Now,' the discovery will be initiated from the current time.

For '[Discovery Schedule](#),' refer to the table for more information.

Label	Action
Schedule Mode	Click the discovery schedule mode at once, every, daily, weekly, or monthly.
At	Click the calendar icon to add the date and time to the next column.

After adding details to the 'Discovery Schedule,' click 'Submit' to initiate the 'Automatic Discovery.'

Note: 'Discovery Schedule' section is optional. By default, it will enable the 'Discover Now' button.

On Successful discovery, Download Jobs (per device) will be created automatically with inputs given on the Discovery Page and from System Default, and the Configurations and operational Data will be downloaded immediately.

[Network Discovery](#)

Network discovery can discover all the network devices like hubs, modems, printers, switches, routers, bridges, and access points, with the help of SNMP protocols.

Initiate Network Discovery

There are three tabs on the 'Network Discovery' page.

[Discovery Details](#) | [Filters](#) | [Schedule](#)

Label	Action	Description/Example
Profile Name*	Add a name for the Discovery Profile. Discovery Profiles are created to save preferences and identify profiles to track and initiate discovery periodically.	The name of the profile helps identify the profile.
Discovery Options	There are two options for discovery. Choose the option that suits your requirements.	1. Discover inventory with availability and performance monitoring. 2. Discover only Inventory Information. 3. Discover inventory with availability and performance monitoring.
Provide Profile Details	Add a brief description of the discovery profile.	For example, For network devices, Routers & Switches only, etc.
IP Address*	Type IP, IP range, or Subnet IP to be discovered.	You can choose to import from a CSV file too.
Import from CSV	Import device list from a CSV.	This is an alternate option to adding the IP, IP range, or subnet.
Configuration Download	Click the toggle button to make changes	Click here to access the detailed Configuration job content and manage your network jobs effectively.
Device Credentials	Select the relevant device credential using the dropdown menu.	Device Credentials must be pre-configured for selection.
Add to NCCM	Select the toggle button to make changes	Discovered network devices are automatically added to NCCM for management, backup, change, compliance, and monitoring.
Agent Details*	Click the 'Pick Agents Here' button to add the agent details.	Infraon agent collects data from devices configured for discovery. It can support SSH, SNMP, WMI, etc.

* Fields are mandatory.

Note: 'Import from CSV' and 'Device Credentials' are optional. You can click the 'Next' button without adding any details to them.

Discovery Details | [Configuration Download](#) | Details

Profile Details:

- Select Configuration profile (only if the Range of Input Devices can have the same profile to manage) or keep it as 'Select Configuration Profile.' NCCM will automatically find the right Profile for each device during discovery.

Protocols:

- Select the Connection protocol (for all the Range of Input Devices that can have the same Connection protocol), or NCCM will automatically set the default connection Protocol from System Parameters.
- Select the Configuration Download protocol (for all the Range of Input Devices that can have the same Configuration Download protocol), or NCCM will automatically set the default Download Protocol from System Parameters.
- Select the Other configuration Download protocol (for all the Range of Input Devices that can have the same Other configuration Download protocol), or NCCM will automatically set the default Other configuration Download Protocol from System Parameters.
- Select the Inventory Download protocol (for all the Range of Input Devices that can have the same protocol), or NCCM will automatically set the default Inventory Download Protocol from System Parameters.
- Select OS Image Download Protocol (for all the Range of Input Devices that can have the same OS Download protocol), or NCCM will automatically set the default OS Download Protocol from System Parameters.

Schedule Download:

For a [Discovery Schedule](#), refer to the table.

Label	Action
Schedule Mode	Click the discovery schedule mode at once, every, daily, weekly, or monthly.
At	Click the calendar icon to add the date and time to the next column.

Click 'Next' to add details on '[Filters](#).'

[Discovery Details](#) | [Filters](#) | [Schedule](#)

Filters have two sections: Device Filters and Network Component Filters.

[Device Filters](#) | [Network Component Filters](#)

Label	Action
Device Filters	Click the first condition box to add either include or exclude devices.
Include Devices/ Exclude Devices	You may include or exclude IP Address, Device Type, or Device Name.

Choose the condition to suit your requirement. You may add additional conditions using the + icon. Move to add network component filters.

[Device Filters](#) | [Network Component Filters](#)

Label	Action
Interface	Enable or disable the 'Interface' button.
Interface Type	Add Interface Type from the drop-down menu.
Interface Name	Add the Interface Name from the drop-down menu.
Sub Interface	Enable or disable the 'Sub Interface' button.
Sub Interface Monitoring	Add Sub Interface Monitoring details from the drop-down menu.
STP	Enable or disable the 'STP Monitoring' button.
BGP	Enable or disable the 'BGP Monitoring' button.
OSPF	Enable or disable the 'OSPF Monitoring' button.
EIGRP	Enable or disable the 'EIGRP Monitoring' button.
QoS	Enable or disable the 'QoS Monitoring' button.
Jitter	Enable or disable the 'Jitter Monitoring' button.
VRF	Enable or disable the 'VRF Monitoring' button.
VLAN	Enable or disable the 'VLAN Monitoring' button.
IPSec	Enable or disable the 'IPSec Monitoring' button.
Wireless Controller	Enable or disable the 'Wireless Controller Monitoring' button.
VPC & VDC	Enable or disable the 'VPC & VDC Monitoring' button.

Host	Enable or disable the 'Host Monitoring' button.
-------------	-------------------------------------------------

Note: 'Filters' tab is optional. You can click the 'Next' button without adding details on Filters.

Once done, click 'Next' to add details 'Schedule'.

Discovery Details | Filters | [Schedule](#)

There are two options for Schedule. You can schedule 'Discovery Now' or set a 'Discovery schedule' time.

If you enable the button on 'Discovery Now,' the discovery will occur from the current time.

For '[Discovery Schedule](#),' refer to the table for more information.

Label	Action
Schedule Mode	Click the discovery schedule mode at once, every, daily, weekly or monthly button.
At	Click the calendar icon to add the date and time to the next column.

After adding details to 'Discovery Schedule,' click 'Submit' to initiate the 'Network Discovery.'

Note: 'Discovery Schedule' section is optional. By default, it will enable the 'Discover Now' button.

Windows Servers

Windows servers can discover windows servers using WMI protocols. It supports Windows Server - 2019/2016/2012/2008/2003.

Initiate Windows Servers

There are three tabs on the 'Windows Servers' page.

Discovery Details | Filters | Schedule

Label	Action	Description/Example
Profile Name*	Add a name for the Discovery Profile. Discovery Profiles are created to save preferences and identify	The name of the profile helps identify the profile.

	profiles to track and initiate discovery periodically.	
Discovery Options	There are two options for discovery. Choose the option that suits your requirement.	1. Discover inventory with availability and performance monitoring. 2. Discover only Inventory Information. 3. Discover inventory with availability and performance monitoring.
Provide Discovery Profile Details	Add the discovery profile details.	Give a brief detail of your discovery and the devices that will be discovered.
IP Address*	Type IP, IP range, or Subnet IP to be discovered.	You can choose to import from a CSV file too.
Import from CSV	Import device list from a CSV.	This is an alternate option to adding the IP, IP range, or subnet.
Device Credentials	Select the relevant device credential using the dropdown menu.	Device Credentials must be pre-configured for selection.
Agent Details*	Click the Pick Agents Here button to add the agent details.	Infraon agent collects data from devices configured for discovery. It can support SSH, SNMP, WMI, etc.

Note: Import from CSV file is optional. Without importing CSV, you can click the 'Next' button.

Click '[Next](#)' to add details on '[Filters](#).'

[Discovery Details](#) | [Filters](#) | [Schedule](#)

'Filters' has two sections: Device Filters and Server Component Filters.

[Device Filters](#) | Server Component Filters

Label	Action
Device Filters	Click the first condition box to add either include devices or exclude devices.
Include Devices/ Exclude Devices	Click the second condition box to add IP address, Device Type, or Device Name.
	Suppose you have chosen Device Name in the second condition box, Click Equals or Contains in the third condition box.
	Add a number or device name to enter the fourth condition box.

Include Devices/Exclude Devices -> IP Address/Device Type/Device Name ->
Equals/Contains -> Number or Device name

Device Filters | [Server Component Filters](#)

Label	Action
Process	Enable or disable the 'Process' button.
Service	Enable or disable the 'Service' button.
SQL	Enable or disable the 'SQL Core Monitoring' button.
DotNet	Enable or disable the 'DotNet core monitoring' button.
Exchange	Enable or disable the 'Exchange Core Monitoring' button.
Share Point	Enable or disable the 'Share Point Core Monitoring' button.
Active Directory	Enable or disable the 'Active Directory Monitoring' button.
IIS	Enable or disable the 'IIS Monitoring' button.

Note: 'Filters' tab is optional. You can click the 'Next' button without adding details on Filters.

After adding details on Device Filters, click 'Next' to add details on 'Schedule.'

Discovery Details | Filters | [Schedule](#)

There are two options for Schedule. You can schedule 'Discovery Now' or set a 'Discovery schedule' time.

If you enable the button on 'Discovery Now,' the discovery will occur from the current time.

For '[Discovery Schedule](#),' refer to the table for more information.

Label	Action
Schedule Mode	Click the discovery schedule mode at once, every, daily, weekly, or monthly button.
At	Click the calendar icon to add the date and time to the next column.

After adding details to the 'Discovery Schedule,' click 'Submit' to initiate the 'Windows Servers.'

Note: 'Discovery Schedule' section is optional. By default, it will enable the 'Discover Now' button.

Linux Servers

Linux Servers module is used to discover Linux servers that support SSH protocols.

Initiate Linux Server Discovery

There are three tabs on the 'Linux Servers' page.

[Discovery Details](#) | [Filters](#) | [Schedule](#)

Label	Action	Description/Example
Profile Name*	Add a name for the Discovery Profile. Discovery Profiles are created to save preferences and identify profiles to track and initiate discovery periodically.	The name of the profile helps identify the profile.
Discovery Options	There are two options for discovery. Choose the option that suits your requirement.	1. Discover inventory with availability and performance monitoring. 2. Discover only Inventory Information. 3. Discover inventory with availability and performance monitoring.
Provide Profile Details	Add a brief description of the discovery profile.	For example, For Linux servers only, H.O Servers, etc.
IP Address*	Type IP, IP range, or Subnet IP to be discovered.	You can choose to import from a CSV file too.
Import from CSV	Import device list from a CSV.	This is an alternate option to adding the IP, IP range, or subnet.
Device Credentials	Select the relevant device credential using the dropdown menu.	Device Credentials must be pre-configured for selection.
Agent Details*	Click the Pick Agents Here button to add the agent details.	Infraon agent collects data from devices, configured for discovery. It can support SSH, SNMP, WMI, etc.

Note: Import from CSV file is optional. If not using the CSV, click the 'Next' button.

Click '[Next](#)' to add details on '[Filters](#)'.

[Discovery Details](#) | [Filters](#) | [Schedule](#)

'Filters' has two sections: Device Filters, and Server Component Filters.

[Device Filters](#) | Server Component Filters

Label	Action
Device Filters	Click the first condition box to add either include or exclude devices.
Include Devices/ Exclude Devices	You may include or exclude IP Address, Device Type, or Device Name.

Choose the condition to suit your requirement. You may add additional conditions using the + icon.

[Device Filters](#) | [Server Component Filters](#)

Label	Action
Process	Enable or disable the 'Process' button.
Process Name	After enabling the 'Process' button, the 'Process name' will appear. Add 'Process Name' from the drop-down menu.
Server Flavour	Add 'Server Flavour' from the drop-down menu.

Note: 'Filters' tab is optional. You can click the 'Next' button without adding details on Filters.

After adding details on Device Filters, click 'Next' to add details on 'Schedule.'

[Discovery Details](#) | [Filters](#) | [Schedule](#)

There are two options for Schedule. You can schedule 'Discovery Now' or set a 'Discovery schedule' time.

If you enable the button on 'Discovery Now', the discovery will occur from the current time.

For 'Discovery Schedule,' refer to the table for more information.

Label	Action
Schedule Mode	Click the discovery schedule mode at once, every, daily, weekly or monthly button.
At	Click the calendar icon to add the date and time to the next column.

After adding details to the 'Discovery Schedule,' click 'Submit' to initiate the discovery.

Note: 'Discovery Schedule' section is optional. By default, it will enable the 'Discover Now' button.

[Hypervisor Monitoring](#)

Streamline device credential management and seamless VMware integration. Create device credentials, select HTTP with name and password, then discover and connect to VMware. Easily view assets through IT assets virtualization.

Hypervisor Host

Discover detailed information about individual physical hosts, VM inventory, and resource allocation. View VM names, IP addresses, device details, and cluster status. The intuitive Timeline feature gives valuable insights into CPU, memory, storage, and VM states. Uncover data store capacity, VM allocation, and host connectivity. Explore device and storage resources for optimized host management.

Hypervisor cluster

Seamlessly manage host clusters with comprehensive CPU, memory, and storage information: track VM and host details within the cluster. Monitor storage allocation, create VM templates, and adjust resources as needed. Explore host, VM, datastore, and resource insights for seamless cluster administrator.

VMware

VMware is a virtualization and cloud computing software provider for Hypervisor products.

Initiate VMware Discovery

There are three tabs on the 'VMware' page.

Discovery Details | Filters | Schedule

Label	Action	Description/Example
Profile Name*	Add a name for the Discovery Profile. Discovery Profiles are created to save preferences and identify profiles to track and initiate discovery periodically.	The name of the profile helps identify the profile.
Discovery Options	There are three options for discovery. Choose the option that suits your requirements.	<ol style="list-style-type: none">1. Discover only Inventory Information2. Discover inventory with availability monitoring.3. Discover inventory with availability and performance monitoring
Provide Profile Details	Add a brief description of the discovery profile.	Give a brief detail of your discovery and the devices that will be discovered.
IP Address*	Type IP, IP range, or Subnet IP to be discovered.	You can choose to import from a CSV file too.

Import from CSV	Import the device list from a CSV.	This is an alternate option to adding the IP, IP range, or subnet.
Device Credentials	Select the relevant device credential using the dropdown menu.	Device Credentials must be pre-configured for selection.
Agent Details*	Click the Pick Agents Here button to add the agent details.	Infraon agent collects data from devices, configured for discovery. It can support SSH, SNMP, WMI, etc.

Note: Import from CSV file is optional. If not using the CSV, click the 'Next' button.

Click 'Next' to add details on 'Filters.'

Discovery Details | **Filters** | Schedule

Device Filters

Label	Action
Device Filters	Click the first condition box to add either include or exclude devices.
Include Devices/	You may include or exclude IP Address, Device Type, Device Name, or value.
Exclude Devices	

Choose the condition to suit your requirement. You may add additional conditions using the + icon.

Note: 'Filters' tab is optional. You can click the 'Next' button without adding details on Filters.

After adding details on Device Filters, click 'Next' to add details on 'Schedule.'

Discovery Details | Filters | **Schedule**

There are two options for Schedule. You can schedule 'Discovery Now' or set a 'Discovery schedule' time.

If you enable the button on 'Discovery Now', the discovery will occur from the current time.

Label	Action
Schedule Mode	Click the discovery schedule mode at once, every, daily, weekly or monthly button.
At	Click the calendar icon to add the date and time to the next column.

For 'Discovery Schedule,' refer to the table for more information.

After adding details to the 'Discovery Schedule,' click 'Submit' to initiate the discovery.

Note: 'Discovery Schedule' section is optional. By default, it will enable the 'Discover Now' button.

URL/ Web Services

URL/Web Service monitoring empowers us to be proactive, informed, and in control of discovery. Keep a watchful eye on any web server, including your own and others.

Steps to Add the Discovery

- Go to Infraon OSS portal -> Infraon Configuration -> IT Operations -> Discovery.
- Navigate to URL/ Web Services.
- Enter the details in the respective dialog boxes and click on Submit.

What you see on the screen

Label	Action/ Description or Example
Application	Select the required Profile name for the service.
Description	Add a description for your service.
URL	Enter the URL required for the service.
Data Collector Details	Pick a respective data collector.

Wireless Controller

A Wireless controller monitors and manages wireless access points in the organization. Wireless controllers connect to routers and allow devices from the organization to connect to the router via access points.

Initiate Wireless controller Discovery

There are three tabs on the 'Wireless Controller' page.

Discovery Details | Filters | Schedule

Label	Action	Description/Example
Profile Name*	Add a name for the Discovery Profile. Discovery Profiles are created to save preferences	The name of the profile helps identify the profile.

	and identify profiles to track and initiate discovery periodically.	
Discovery Options	There are three options for discovery. Choose the option that suits your requirement.	1. Discover only Inventory Information 2. Discover inventory with availability monitoring. 3. Discover inventory with availability and performance monitoring
Provide Profile Details	Add a brief description of the discovery profile.	Give a brief detail of your discovery and the devices that will be discovered.
IP Address*	Type IP, IP range, or Subnet IP to be discovered.	You can choose to import from a CSV file too.
Import from CSV	Import the device list from a CSV.	This is an alternate option to adding the IP, IP range, or subnet.
Device Credentials	Select the relevant device credential using the dropdown menu.	Device Credentials must be pre-configured for selection.
Agent Details*	Click the Pick Agents Here button to add the agent details.	Infraon agent collects data from devices, configured for discovery. It can support SSH, SNMP, WMI, etc.

Note: Import from CSV file is optional. If not using the CSV, click the 'Next' button.

Click 'Next' to add details on 'Filters.'

Discovery Details | **Filters** | Schedule

Filters have two sections: Device Filters and Network Component Filters.

Device Filters | Network Component Filters

Label	Action
Device Filters	Click the first condition box to add either include or exclude devices.
Include Devices/	You may include or exclude IP Address, Device Type, Device Name or value.
Exclude Devices	

Choose the condition to suit your requirement. You may add additional conditions using the + icon. Move to add network component filters.

Device Filters | **Network Component Filters**

Label	Action
Access Points	Enable or disable the 'Access Point Monitoring' button.
Host	Enable or disable the 'Host Monitoring' button.

Note: 'Filters' tab is optional. You can click the 'Next' button without adding details on Filters.

Once done, click 'Next' to add details 'Schedule'.

Discovery Details | Filters | **Schedule**

There are two options for Schedule. You can schedule 'Discovery Now' or set a 'Discovery schedule' time.

If you enable the 'Discovery Now' button, the discovery will occur from the current time.

Label	Action
Schedule Mode	Click the discovery schedule mode at once, every, daily, weekly or monthly button.
At	Click the calendar icon to add the date and time to the next column.

For 'Discovery Schedule,' refer to the table for more information.

After adding details to the 'Discovery Schedule,' click 'Submit' to initiate the discovery.

Note: 'Discovery Schedule' section is optional. By default, it will enable the 'Discover Now' button.

Job Progress

The job Progress page displays the list of discovery jobs that are in progress (active discoveries).

What you see on the screen

The Job Progress page displays the list of discoveries and their results. The details include the following:

◦

Profile Name

- Type
- Schedule Type
- Current Status
- Last Action
- Next Action
- Action

Use the action icons to view:

- Information - details of the discovery
- Audit - logs
- Delete - delete the discovery job

LED Display

Configure thresholds for parameters monitored through Infraon.

What you see on the screen

Label	Action	Description/ Example
Search	Search for the required Display.	
Filter	Filter can be added based on the field and condition from the drop-down box below.	Field – Location, Type. Condition – in, not in, equal to, not equal to, contains, not contains.
Add LED Display	Click to add a new LED Display.	Follow the below steps to add a new Circuit Discovery.
IP Address		Indicates a unique number identifying your device.
Location		Headquarters location, region of operation.
Tags		Indicates the tags assigned.
Port		Indicates the port number assigned.
Message		Indicates a message.

Actions		
Edit	Click to make changes to the category.	
Delete	Click to delete the category.	

Steps to add a new LED Display

- Go to Infraon OSS portal -> Infraon Configuration -> IT Operations -> LED Display.
- Navigate and click on the 'Add LED Display' button at the top right corner of the page.
- Enter the below details in the respective dialog boxes:
 - IP Address
 - Location
 - Tag
 - Port
 - Message
- Once the details are entered, click on the Submit button to add the LED Display.

Maintenance

Maintenance refers to the ongoing process of inspecting, repairing, and optimizing equipment, or software to ensure their reliability, performance, and longevity, thus minimizing downtime and preventing potential issues.

Maintenance involves the deliberate shutdown of a device for a specific purpose or action, often driven by a scheduled event or a particular requirement. During the maintenance process, alarms are suspended, and polling operations are halted on the device undergoing maintenance. This measure is undertaken to prevent the occurrence of extraneous alerts and to ensure that any unnecessary activities are averted, enhancing the overall efficiency of the maintenance operation.

Refer to the following table for more information:

Label	Description/ Example
Reason	Mention the reason for the maintenance
No. Of Assets	Mention the number of assets for maintenance
Status	Status is changed as per the maintenance.
Maintenance Window	The date will be displayed i.e. To – From date.

Click on the 'action'; tab and click the 'edit' or 'delete' icon.

In Edit, there are two tabs, mentioned below:

Asset Details | Schedule

- Write the reason for the maintenance.
- Select 'Mask Alarm' or 'Stop polling' and click 'Next'

Mask Alarm: A mask alarm in terms pertains to a condition where no alarm signals are intended to activate. This implies that the system operates under circumstances ensuring the absence of any alarm triggers.

Stop Polling: Stop polling refers to an elective intermediary action positioned between "mask alarm" and itself. When the verification is selected, polling operations are suspended; however, if the checkbox remains unmarked, polling continues, though an alarm won't be generated even if it aligns with the threshold.

Asset Details | Schedule

- Click on the 'Calendar' icon to select the start time and select the time.
- Click on the 'Calendar' icon to select the end Time and select the time.
- Click 'Submit'

Maintenance can be deleted by clicking the 'delete' icon from the action tab.

Note: A corresponding maintenance icon becomes visible on the device interface when a device enters a maintenance state. Selecting the maintenance icon results in the cessation of polling operations; if the checkbox is activated, polling is suspended, and data remains empty.

Network Configuration

This enables Network administrators to efficiently manage remote IT networks and IP-enabled security devices from a centralized location.

Key benefits:

- Discover and audit all changes on Network devices
- Backup and Restore Device configurations
- Authorized Configuration changes
- Distribute Operating system and patch updates
- Detect network changes and alert via E-mail, SMS, Syslog, and Helpdesk tickets
- Perform differential Audits between configuration versions
- Establish and enforce Compliances through compliance and Baseline Policies
- Provide role-based access control
- Detect and report vulnerable devices with remediation strategies
- Report all Aspects of Network Device Configurations, Changes, and Compliances

- Automatic Remediation for Device Policy compliance to a Specific or Default Configuration.

The NCCM module of Infraon consists of ten additional modules:

Configuration Download

- **Calendar View** – Calendar View provides a daily activity summary, including successful, failed, completed, and total configurations processed.
- **Configuration Parameters** - These parameters encompass various aspects of the device's operation, including network settings, security policies, access controls, and performance configurations.
- **Configuration Profile** - A configuration profile is a template or predefined set of configuration settings that network administrators can create and customize with information like device details and connection protocols for SSH and Telnet.
- **Configuration Search** - Configuration Search specifically focuses on download jobs, allowing users to view or export the Startup or Running configurations within these jobs to identify any configuration.
- **Download Jobs** - Download jobs are tasks that retrieve configurations from network devices for backup, analysis, auditing, or comparison.
- **OS Image** - OS images are used primarily for managing and deploying configuration changes across network devices such as routers, switches, and firewalls.
- **OS Image Download Schedular** - This feature is used to compare the configuration data by downloaded version or file.

Configuration Upload

- **Configuration Template** - Configuration templates hold the commands needed for upload jobs and making changes to network devices, including provisioning, OS upgrades, creating or deactivating services, and any other change.

Utilities

- **Configuration Comparison** - This feature is used to compare the configuration data by downloaded version or file.

- **Configuration File Compare** - Compares the Configuration File provided by the user.
- **Generate MD5** - Generate MD5 Key.

CLI Access Profile

- **Authentication Profile** - This profile manages user authentication for accessing network devices via CLI. It verifies user identity before granting access, ensuring only authorized users can initiate CLI sessions. The Authentication Profile allows users to use SSO (Single Sign-On) to access network devices as per the configurations.
- **Authorization Profile** – This profile defines user access levels and permissions for network devices, ensuring only authorized users can execute commands or modify configurations.

It integrates the AAA (Authentication, Authorization, and Accounting) security framework, aligning with NCCM's Block, Notify, and Terminate actions to enforce security policies by restricting unauthorized actions, alerting admins, or terminating sessions when necessary.

Baseline Scheduler

The Baseline Configuration module in Infraon Network Configuration and Change Management (NCCM) allows users to establish and manage stable configurations for critical network devices. When a configuration version is identified as stable, flexible, and reliable—such as the 2nd version—it can be labelled as a baseline.

This baseline serves as a reference point, making it easy to revert to a known, stable state if any subsequent changes, like in a 3rd version, prove unnecessary or problematic. Users can quickly identify and restore preferred configurations using the Baseline Configuration module, ensuring their network infrastructure's consistent stability and reliability.

This feature is used to simultaneously change the baseline configuration for a single or multiple device.

Note:

- We can choose the previous version or the previous download for the baseline setting.
- If the Configuration is selected as “Last Successful download” and the date is not chosen, the previous version or previous successful download will be taken as the baseline setting.
- If “Date” is chosen, the previous version or previous successful download will be taken as the baseline settings based on the date selected.

Example:

For Previous Version:

Total versions of the device: 48 versions

Date: 10-02-2019 (On 10th Feb, the last version was 40)

Previous Version: 10

The baseline set version should be "30"

For Previous Download:

Total versions of the device: 48 versions

Date: 10-02-2019 (On 10th Feb, total download was 5)

Previous Download: 4

The baseline set should be the first download that happened on Feb 10th

What you see on the screen

Multiple action icons are displayed on the page.

Label	Action
Search	Search for the required Baseline Scheduler.
Filter	A filter can be added based on the field (Name, Device IP Address, Exclude IP Address, Vendor, OS Type, Schedule Mode), and the condition can be selected from the drop-down box below.
Add	Click to add a Baseline Scheduler.
Action Icons	
Edit	Click to make changes to the Baseline Scheduler
Delete	Click to Delete the Baseline Scheduler

The Baseline Scheduler page provides comprehensive details about scheduled baseline generation processes. Key information displayed includes:

- Name
- Description
- Schedule Details
- Vendor
- OS Type
- Device IP Address
- Exclude IP Address
- Next Action Type
- Modified By
- Last Modified Time
- Created By

- Creation Time

Add Baseline Scheduler

To configure baseline scheduling, navigate through the Infraon application and access the Infraon configuration settings. Within this section, locate the '**IT Operations**' module, which encompasses network management functionalities. Finally, proceed to the '**Network Configuration**' sub-module to find the specific Baseline Scheduler configuration options.

To configure a new baseline schedule, navigate to the appropriate section within the NCCM application and locate the "**Add**" button. Click this button to initiate the baseline creation process.

On the subsequent **Add Baseline Configuration** pop-up, provide the following details:

[Add Baseline Configuration](#) | Details

Label	Action	Description/ Example
Basic Details		
Name	Assign a distinct and informative name to identify the schedule easily.	
Description	Add brief or a concise explanation of the baseline's purpose or scope.	
Schedule Details		
Other Details		
Schedule Mode	Select the desired frequency for baseline generation from the available options.	Once, Every, Daily, Weekly, or Monthly.
At	Select the desired start time for the baseline generation process. This step ensures that the system executes the baseline collection at the designated moment.	Select the calendar icon to specify the desired date.
Scheduled on		Displays the selected start date and time for the baseline generation process.
Vendor	Choose the appropriate vendor for the target devices from the provided drop-down menu.	Oracle, Nivetti.

OS Type	Choose the appropriate OS Type from the provided drop-down menu for the target devices.	
Device IP Address	Input the IP addresses of devices to be included in the baseline.	
Exclude IP Address	Add the Exclude IP addresses if necessary.	
Configuration Type	Determine the specific type of configuration data to be captured.	For example: Running, Startup, etc.
Baseline Preferences	Select whether to use the " Last successful download " or specify a " Date " as the baseline reference point.	

Once all required information has been entered, click the "**Save**" button to finalize the baseline configuration. The system will initiate the baseline generation process according to the specified parameters.

Note:

- The baseline setting is based on the schedule configured in the Baseline scheduler.
- Baseline setting will be initiated based on the Job's start & end date.

Edit Baseline Scheduler

Select the baseline scheduler profile and click the "**Edit**" icon to redirect to the Edit Baseline Scheduler window.

Make changes as necessary and click on "**Save**" the changes.

Delete Baseline Scheduler

Select the baseline scheduler Profile(s) and click the "**Delete**" icon to redirect to the delete confirmation window.

Click **Yes** to delete the baseline scheduler Profile or click **No** to cancel the delete operation.

Configuration Comparison

Compare configuration is used to compare device configuration types (startup or running) to assess the configuration differences between two devices.

What you see on the screen

Comparing Device Configurations

- From the **Vendor** section, select two device vendors. The IP addresses of the selected model are displayed in the **IP Addresses** section.
- From the **IP Addresses** section, select the IP address of the corresponding devices.
- From the **Configuration Type** section, select the configuration types to compare.

Optional: To compare with the latest successful download configuration, in **Upload your Configuration**, click **Choose File** and select the .txt file

- In the **Configuration snapshot**, select the versions to compare.
- Click **Compare**. The **Configuration Comparison** page appears.
- Optional: To toggle between **Showing only differences** or **Showing the full configurations** view.

Configuration File Compare

The configuration file compare module enables users to analyze device configurations by highlighting the differences between current and previous versions. This feature facilitates the swift identification of intentional and accidental changes, aiding in troubleshooting and ensuring policy adherence.

What you see on the screen

Select any two configurations and Click full screen to compare Configurations:

- Click the compare icon from the comparison window to toggle between displaying difference between configurations and all configurations.
- Export the result into PDF.
- Click on the cross icon to close the result window.

Note: The configuration file supports only the following formats: txt, cfg, and conf. The maximum file size is 2 MB, and the aspect ratio must be 4:1.

Configuration Parameters

Configuration parameters are essentially variables with specific functions within a tool. They act as adjustable settings, allowing users to tailor the tool's behavior according to their needs. The complete set of these variables is collectively known as the "configuration parameters."

Compiled languages typically use static variables for configuration, meaning they have a lifespan that covers the entire program execution. This is like pre-determining the settings before starting a journey. In contrast, interpreted languages allocate configuration variables dynamically during declaration, as their values might not be known in advance. Imagine adjusting navigation points mid-journey based on new information.

This is a Privilege-based feature: The user will be able to access, view, add, edit, delete, and execute only if privileges have been given by the administrator. This will be defined under roles and privileges.

What you see on the screen

Details| Fields

Label	Description/ Example
Search	Search for the required configuration parameter.
Filter	Filter can be added based on the field (Parameter, description, and value) and select the condition from the drop-down box below.
Parameter	Displays the parameter associated with the configuration.
Value	Indicates the value described in the configuration.
Description	A brief description of the respective configuration.
Actions	
Edit	Click to make changes to the configuration.
Delete	Click to delete the configuration.

Steps to Add a Configuration Parameter

- Navigate to Infraon Configuration -> IT operation -> Network Configuration and select the Configuration parameter option.
- Click on 'ADD', located at the top right corner of the page.
- Input the below details:

Add | Fields

Label	Action/ Description
Parameter	Click to add a required parameter name for the configuration.
Value	Add the respective value.
Description	Add a suitable brief description of the configuration.

Note: Enabling "Password Field" triggers secure storage and masked display of the value field (When the Checkbox is ticked, the password will be kept hidden).

- Click [Submit](#) to configure the Parameter or click [Cancel](#) to abort the operation.

Configuration Profile

Network admins create and manage comprehensive configuration profiles, including device details and connection protocols (SSH/Telnet), for efficient device setup and control.

This is a Privilege based feature: The user will be able to access, view, add, edit, delete, execute & export, only if privileges have been given by the administrator.

What you see on the screen

Label	Action/ Description
Search	Click to search the required configuration profile.
Filter	Filter can be added based on the field (Profile Name, Vendor, OS Type and Series) and select the condition from the drop-down box below.
Grid View	Click to view in a tabular format.
Card View	Click to view a concise and organized presentation of content.
Export	Download the configuration profiles as a separate CSV file.
Add	
Add Configuration	Click to add the configuration profile manually.
Import Configuration	Click to add the configuration profile in bulk through a CSV file.
Details	
Profile Name	Displays the name of the configuration profile.
Vendor	Displays the name of the vendor assigned to the configuration profile.
OS Type	Indicates the name of the operating system type.
Series	Denotes the series of the specific device/ server.
Description	Shows a brief description about the configuration profile.
Actions	
Edit	Click to make changes to the profile.
Delete	Click to delete the configuration.

Download	Click to download/ Export the particular configuration in a CSV file (excel sheet).
Copy	Click to clone the configuration profile.

Steps to Add a Configuration Profile

- Navigate to Infraon Configuration -> IT operation -> Network Configuration and select the Configuration profile option.
- Click on 'Add' located at the top right corner of the page.

There are two methods to add the configuration profile:

Method 1: Add Configuration (Manually)

- Enter the below details in the respective call-out boxes.

Create Configuration Profile | Fields

Label	Description/ Example
Profile Name	Add a name to the required configuration.
Vendor	Enter the name of the specific vendor for which the profile is being created.
OS Type	Add the operating system which supports the configuration.
Series	Enter the unique identifier series number.
Description	Add a brief description of the configuration profile.

- Click **Submit** to configure the Parameter or click **Cancel** to abort the operation.
- Add the configuration profile data as follows:

Configuration Profile Data | Fields

Connection | Fields

Action	Example

Input the Connect Template in textbox (SSH and Telnet Connection commands)	<pre>{% if Job.connection_protocol == "SSH" %} <command shell="remote" prompt="[[Pp]password,[Pp]ass,assword:,assword]">ssh -o StrictHostKeyChecking=no -o UserKnownHostsFile=/dev/null {{Profile.ssh_loginname}}@{{Device.IPAddress}} -p {{Profile.ssh_port}}</command> <command prompt="#,>">{{Profile.ssh_password}}</command> <command prompt="#,>">{{Profile.ssh_password}}</command> {% endif %}</pre>
Input the below Local Connect Template command in the given textbox.	<pre>{% if Job.connection_protocol == "SSH" %} <command shell="remote" prompt="[[Pp]password,[Pp]ass,assword:,assword]">ssh -o StrictHostKeyChecking=no -o UserKnownHostsFile=/dev/null {{Profile.ssh_loginname}}@{{Device.IPAddress}} -p {{Profile.ssh_port}}</command> <command prompt="#,>">{{Profile.ssh_password}}</command> <command prompt="#,>">{{Profile.ssh_password}}</command> {% endif %}</pre>

Config Download | Fields

Action	Example
Input the for 'Running Template' in the textbox.	<pre>{% if Job.protocol == "Terminal" %} <command prompt="[>,#]">set cli mode -page OFF</command> <command prompt=" Done" action="output-to-store" timeout="300">show ns runningConfig</command> <command prompt="" action="exit">exit</command> {% endif %}</pre>

Input the Download Configuration commands for Startup Template in textbox	<pre>{% if Job.protocol == "Terminal" %} <command prompt="#">term len 0</command> <command prompt="#" action="output-to-store" timeout="300">show startup-config</command> <command prompt="" action="exit">exit</command></pre>
----------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Config Upload | Fields

Action	Example
Input the Upload Configuration commands for 'Running Template' in textbox.	<pre><tftp> <command prompt="\]\?>copy tftp: nvram:running-config</command> <command prompt="\]\?>{{Global.managementIP}}</command> > <command prompt="\]\?>{{Job.uploadfilename}}</command> <command prompt="#" timeout="300">running- config</command> <command prompt="" action="exit">exit</command> </tftp></pre>
Input the Upload Configuration commands for Startup in textbox.	<pre><tftp> <command prompt="\]\?>copy tftp: nvram:startup-config</command> <command prompt="\]\?>{{Global.managementIP}}</command> > <command prompt="\]\?>{{Job.uploadfilename}}</command> <command prompt="#" timeout="300">startup- config</command> <command prompt="" action="exit">exit</command> </tftp></pre>

OS Download | Fields

Action	Example
--------	---------

Input the OS Image Download Configuration commands in textbox.	<pre>{% if Job.image_protocol == "TFTP" %} <command prompt="\]\?>copy {{Device.image_file_name}} tftp:</command> <command prompt="\]\?>{{Global.managementIP}}</command> <command prompt="#" action="output-to-store" timeout="600">CRLF</command> <command prompt="" action="exit">exit</command></pre>
-----------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

OS Upload | Fields

Action	Example
Input the OS Upload commands in the textbox.	Note: OS Upload Profile will be taken directly from the Template.

Operational Data | Fields

Action	Example
Input the Operational download configuration commands in 'Upload Template' textbox	<pre>% if Job.inventory_protocol == "Terminal" <command prompt="#">terminal len 0</command> <command prompt="#" action="output-to-store" type="Version" timeout="10">show version</command> <command prompt="#" action="output-to-store" type="Users" timeout="10">show users</command> <command prompt="#" action="output-to-store" type="Interface Brief" timeout="10">show IP interface brief</command> <command prompt="#" action="output-to-store" type="Hardware Module" timeout="10">show module</command> <command prompt="#" action="output-to-store" type="Show ARP" timeout="10">show arp</command></pre>

```

<command prompt="#" action="output-to-store" type="Hardware Inventory"
    timeout="10">show inventory</command>
<command prompt="#" action="output-to-store" type="Interface Details XML" timeout="10">show IP interface brief | format</command>
<command prompt="" action="exit">exit</command>
{%
    %} endif %
}

```

Others | Fields

Action	Example
Input the Other configuration commands in the textbox.	
Add ZTP configuration details to enable ZTP. <ul style="list-style-type: none"> ● Select a ZTP template using the dropdown menu. ● Select the mandatory CSV column using the dropdown menu. ● Add runtime values. You can either add the values directly or add them from a file. ● Once the values are added, an additional option to add a MAC address and review is displayed 	

Syslog | Fields

Action	Example
Input the Syslog Patterns in textbox.	<code>^.*(%SYS-5-CONFIG_I)((?!\\s+NCCMID\\s?).)*\$</code>

Comment | Fields

Action	Example
Input Ignore Configuration Lines /Comments:	Building configuration Current configuration

<p>Comment pattern ignores the configuration lines from the downloaded configuration</p>	Last configuration change at show startup-config show start show run Using \d* out of \d* bytes NVRAM config last updated ntp clock-period ! No configuration change
<p>Input the Difference ignores Patterns in the textbox.</p> <ul style="list-style-type: none"> o Difference ignore Pattern ignores the configuration lines from both comparing versions during configuration difference operation 	
<p>Input the Authentication error Patterns in textbox.</p>	
<p>Authentication error Patterns raise the authentication error on matching authentication failure command response.</p>	
<p>Default Authentication Error Patterns:</p> <p>Authentication failed Access denied Access failure Access failed Login failed Login failure Login denied Invalid password Invalid user Invalid credential Logged fail</p>	
<p>Input the Authorization error Patterns in the textbox.</p> <ul style="list-style-type: none"> o Authorization error Pattern raises the command error, on matching command failure response. o Default Authorization Error Patterns: <p>Invalid command received in Valid input detected Syntax error, expecting Unknown command Ambiguous command Incomplete command</p>	

Wrong parameter
Unrecognized command
%error opening

Method 2: Import Configuration (CSV File)

- Download the CSV file (excel sheet) and enter the respective fields in the sheet.
- Upload the same edited CSV file.
- Click **Next** -> **Import** -> **Proceed with Valid Records.**

Miscellaneous

Edit Configuration Profile

To edit a profile, select any of the existing profile and click "**Edit.**" Make changes as necessary and save the changes.

Delete Configuration Profile

To delete Profile, select the profile(s) and click the delete icon.

Click "**Yes**" to delete the Configuration Profile or click "**No**" to cancel the operation.

Note: Profile cannot be deleted if it is associated with a download job.

Copy Configuration Profile

To Copy a profile, select any existing profile and click the copy icon . Follow the same procedure as Add Profile to copy the profile.

Profile Import

Click the download icon to redirect to the upload window, to import the template file (.xls supported).

Profile Export

Click upload icon to export NCCM's configured Profiles to the XLS file.

Configuration Profile Search

Click filter icon to open the search options.

- Input Profile Name in the textbox.
- Input the Vendor in the textbox.
- Input OS Type in the textbox.
- Input Description in the textbox.

Click "**Save**" to search based, on the applied filter.

Configuration Search

Configuration search is used to compare device configuration types (startup or running) to assess the configuration differences between two devices.

What you see on the screen

Searching Configurations for Specific Commands

From the "**Actions**" menu, click "Configuration Search." The **Configuration Search** page appears.

- Select the search criteria, such as **Vendor, OS Type, IP Address Range, Device Group, Configuration Type, and Commands** (mandatory parameter).
- Click Search. The Command Search Results page appears.
- To export the search result to Microsoft Excel, click.
- Save the file in the required folder.

Configuration Template

Configuration changes like "Provisioning", "OS Upgrade", "Service Creation", "Service Deactivation" and "any change" on Networking Devices can be done using Configuration Templates.

Template Execution

- Template is a Collection of commands (one or more) with zero or more variables to be executed on devices for specific operations (like ACL Modification, Route ADD, Interface NAC configuration, Interface IP Change, Interface Enable Disable, SNMP/LLDP/CDP enable or Disabling, OS Upgrade). By substituting different values (to variables) for different Devices, user can reuse the same template for similar operations on multiple devices. Device Credentials, Device Interface Name/IP Address, and command inputs will become a variable portion in the command template.
- Templates are vendor and OS-type specific, which means separate templates are required to be built for the same operation on two different vendor devices or for two different OS Types of the same vendor. This is

due to a difference in the command syntax and command formats for the same operation on two vendor devices.

- Apart from the command portion, Templates also contain information about the Vendor, OS Type, Series, and Model where the template can run, along with the ACL configuration that defines who can manage the Templates.
- Once the Configuration Template is built, the user can execute the Templates on devices using the Upload Job functionality.
- Configuration Template (Network Diagnosis type) can be used in Network Diagnosis functionality for Checking the Device's operational data and for doing simple configurations like Crypto cache clearing, daily diagnosis check, etc., (Which does not affect and is not a part of the Device Configuration).
- Configuration Template command portion should be written in XML format.

The Configuration Template inherits Jinja2 Template standards, and the user gets all the benefits of Jinja2 Template, such as Data Types (Integer, Boolean, List), Control Statements (If—elif—else, for loop, while Loop), and Operator conditions (=, !=, >, =, =, etc.).

Note: *The same Template framework and fundamental is followed in*

- Configuration Profile - Used by Configuration Download Job to download Configurations, Inventories, and Operation Data.
- OS Image Download and Upgrade
- Configuration Triggers
- Policy Rule – Command Execution Scope
- Policy Remedy Execution
- CLI (Command Line Interface) Job

Users will be given Direct CLI (SSH or Telnet) access to the Devices from the NCCM Application (like a Gateway process) for changing configurations.

What you see on the screen

This is a privilege-based feature: The user will be able to access, view, add, edit, delete, execute, and export only if the administrator has given them privileges. This will be defined under roles and privileges.

The Configuration Template Grid page lists all templates created by the user and also the templates assigned to the same user by an admin or template management full-privileged user.

The **Access Control List** feature in this module lets admin-privileged users decide who can view, edit, or delete any specific templates in NCCM.

Configuration Template Grid shows

- Template ID - To know the creation sequence (recently created or old).
- Name of Template - The name will be unique and will be used in other features while using the Template.
- Vendor – The Vendor Device where this template can RUN (Vendor Specific).
- OS Type – The Vendor Device OS Type where this Template can only RUN (OS specific).
 - In case the Template can RUN on all OS Types of the same Vendor, Input the OS Type as '**ALL TYPE.**'

For example, **CISCO IOS, IOS XE, NXOS, IOSXR, and ASA** may use **different** command syntaxes for the same operation.

- Type of Template—NCCM supports 9 Types of Templates, each of which will be explained in detail in the following sections.
- Active Status—Enabled/Disabled—During execution, this flag does not impact Jobs that are set as Disabled (template disabled) but already assigned to an Upload Job. On the other hand, Disabled Templates will not be allowed to be used in New Upload Job Creation.
- Execution ready or Production Status—It should be in the Ready State to use in the Upload Job for configuration change.
- Approval Required Flag - The value will always be Yes (Approval is always required).
- Actions – There are two action icons displayed here – Execute & Quick Execute.

Note: When the Template is used in the Upload Job by a whitelisted user or Approver, the Approval Process is bypassed, and the job is executed directly.

- Created User – The user who created the Template.
- Description – Template description which defines the operation purpose.

How to write Command Portion in Template

NCCM supports two ways of writing commands in Template

1) Plain command format (Writing Device Command as it is)

- a. In plain command format, the user writes the device commands as defined by the vendor. This format will be used only inside the Command Execution & Network Diagnosis template type but not in Download Job Profiles, OS Upgrade Job, Configuration Trigger, Policy Rules, and Remedy.
- b. Though it is simple to write the template in this format, it is not recommended since it does not allow for additional information to be added to the command, such as command timeout, response prompt, and error check condition on response.
- c. The timeout for each command using plain command format is always 30 seconds, and each command takes the full 30 seconds even if the execution has been completed before.

2) XML Command Format

- a. In XML command format, each command is enclosed in an XML node, and additional input to the command, like command timeout, prompt, expected pattern, previous match, and action, will be added in XML node properties.
- b. The XML command format is the recommended format for all NCCM features, including Download, Upload, Upgrade, and Diagnosis.

Sample command portion for changing Device hostname in plain text format and XML format:

Plain Format	XML Format
conf t	
hostname	<command prompt="#" timeout="10">conf t</command>
newname	<command prompt="#" timeout="10">hostname newname</command>
exit	<command prompt="#" timeout="10" action="exit">exit</command>

In the above example, the plain format takes the device command as it is the same way the command is executed using Putty or xtrem application, but in XML Format, each device command will be placed inside the XML node "Data" section, and other information in the XML node property section.

XML Command Syntax

```
<command property1="value" property2="value"> Device Command  
</command>
```

Command Properties	Actual Command
---------------------------	-----------------------

XML Command Sample

```
<command prompt="#" timeout="10">hostname newname</command>
```

The **device command** for every device will be inside the Data portion of XML Node, and the additional properties or information will be inside XML's **property** portion. The property value must always be inside the Double quotes character.

NCCM supports the following properties:

- 1) timeout - value (in seconds). Every command execution is considered as complete either till the prompt pattern value is matched or till the timeout second count is reached.

- 2) prompt - is generally the last character of **command response** that informs the command execution completion of a Device. When the response from Device is not matching the prompt, command execution is considered as COMMAND ERROR.

prompt="#"

- a. The prompt can be a single character or a word or a line.

prompt=" #"

prompt="Router27#"

prompt="([Are you confirm the reboot action]?)"

- b. The prompt value is always a regex pattern and it can be escaped using \ to make exact match. Below example. (Dot) regex character is escaped with \ to consider it literally as '.' (Dot) and not as regex pattern.

```
prompt="\."
```

Follow the URL <https://regex101.com/> to verify or check the regex pattern before saving the template.

- c. The prompt also supports multiple patterns (multiple single characters or multiple words) to match the command execution completion

```
prompt="#,>,\$]"
```

```
prompt="[Username, login, User]"
```

- d. When the given prompt is not matched within the specified timeout seconds, NCCM will declare it as Command error and stop or continue the execution based on Task IP/Command continuation input from Upload Job task input.

3) "action" property is used to

- a. Inform NCCM that exit command is executed and to not wait for prompt.

```
action="exit"
```

- b. Inform NCCM to store the result of command for storing the configuration output of device and also to copy the command output for Trigger parsing.

```
action="output-to-store"
```

4) "shell" property is used to Inform NCCM to open a remote session (TELNET or SSH) from a Device for further command executions.

```
shell="remote"
```

```
<command shell="remote" prompt="Password"> ssh -o StrictHostKeyChecking=no -o UserKnownHostsFile=/dev/null {{Profile.ssh_loginname}}@{{Device.IpAddress}} - p {{Profile.ssh_port}}</command>
```

5) "error_pattern" property is used to check the command response; if the pattern values match the command response, command execution is considered as COMMAND ERROR. Similar to prompt property, error_pattern can take multiple values. **NOTE:** - Prompt property is used to check for command completion however error_pattern property is for checking whether the Response is as per the expectation.

```
error_pattern="[Unknown command, Invalid Command]"
```

Example: when “copy tftp” command is not supported by a device, response will be %Error opening tftp and the error_pattern to catch the error will be

```
error_pattern="[%Error opening tftp]"
```

The below properties also follow the same principle as error_pattern .

6) “expected_pattern” property is used to check the command response; if the pattern value does not match the command response, command execution is considered as COMMAND ERROR.

```
expected_pattern="[bgp is enabled]"
```

7) “expected_any_response” property is used to check the command response; if the device does not respond to any data, command execution is considered as COMMAND ERROR. The value of property is not required and hence input can be empty double quotes

```
expected_any_response=""
```

8) “expected_empty_response” property is used to check the command response; if the device responds with any data, command execution is considered as COMMAND ERROR. The value of property is not required and hence, input can be empty double quotes

```
expected_empty_response=""
```

9) “expected_count_response” property is used to check the command response; if the device response line is not equal to count value data, command execution is considered as COMMAND ERROR. The value of property is the response line count. The count can be any number

```
expected_count_response="5"
```

NCCM expects a 5 line response.

10)“expected_count_response” property is used to check the command response; if the device response line is not equal to the count value data, command execution is considered as COMMAND ERROR. The value of property is response line count. The count can be any number.

```
expected_count_response!="5"
```

NCCM expects the response to be anything other than 5 lines.

11)“expected_count_response” property is used to check the command response; if the device response line is less than 6, command execution is

considered as COMMAND ERROR. The value of property is count of line. The count can be any number.

expected_count_response=">5"

NCCM expects the response to be greater than 5 lines.

12)"expected_count_response" property is used to check the command response; if the device response line is greater than 4, command execution is considered as COMMAND ERROR. The value of property is count of line. The count can be any number.

expected_count_response="=5"

NCCM expects the response to be more than 4 lines.

14)"expected_count_response" property is used to check the command response; if the device response line is greater than 5, command execution is considered as COMMAND ERROR. The value of property is count of line. The count can be any number.

expected_count_response("<=5"

NCCM expects the response to be less than 6 lines

15)"**type**" property is used to store the command response under property value. NCCM stores the command output in Operation Data store.

For example:

If the output of the command, show IP interface brief is required to store in NCCM as **Interface Brief**, XML command should be written as

```
<command prompt="#" timeout="5" type="Interface Brief"> sh  
ow IP  
interface brief</command>
```

Sample command to shut down an interface in plain text and XML format.

Plain Format	XML Format
conf t int Gi 0/0 shutdown exit	<pre><command prompt="#" timeout="10">conf t</command> <command prompt="#" timeout="10"> int Gi 0/0 </command> <command prompt="#" timeout="10">shutdown</command> <command prompt="#" timeout="10" action="exit">exit</command></pre>

Sample command to enable syslog in plain text format and XML format.

Plain Format	XML Format
<pre>conf t logging source- interface Loopback100 end write mem ory</pre>	<pre><command prompt="#" timeout="10">conf t</command> <command prompt="#" timeout="10"> logging sourcei nterface Loopback100 </command> <command prompt="#" timeout="10">end</command> <command prompt="#" timeout="10" action="exit">writ e memory</command></pre>

Below are some sample commands to replace the Device configuration file from NCCM server.

```
<command prompt="\?\>copy tftp: running-config</command>
<command prompt="\?\>{{Global.managementIP}}</command>
<command prompt="\?\>{{Job.uploadfilename}}</command>
<command prompt="[\],#" timeout="300">running-config</command>
<command previous_match="\]" prompt="#" timeout="300">yes</com
mand>
<command action="exit" prompt="">exit</command>
```

Note: Plain text command cannot be written since the timeout of some commands are more than 30 seconds.

NCCM also supports writing of Comments inside the command portion, for better understanding of commands. To define a line as a comment, add # character at the beginning of a line.

Example for writing Comments inside commands:

```
# Make Terminal Len 0terminal length 0

<command prompt="#" timeout="60">terminal length 0</command>

# Copy the Image to Flash

<command prompt="]\?\>copy tftp flash:</command>

# Remove boot system

<command prompt="#" timeout="60">no boot system</command>
```

Note: At the time of execution, NCCM ignores all lines starting with # (comment lines)

NCCM Variable Substitution

NCCM follows **Jinja2 Template** engine for converting **command templates** into actual commands. Jinja2 Template engine provides features like

- Variable substitution
 - For substituting specific values for specific Devices
- Variable declaration
- Data structures like Integer, Boolean, List, and Dictionary
- Loop Statements like
 - For o While
 - Do while
- Conditional Statements like
 - If
 - If else
 - If elif else
- Conditional operators like

o =

o !=

o in

o not in

o > and >=

o < and <=

Variable Substitution:

Variables are **command inputs** given by a user dynamically during the execution time.

For example, if the user wants to change the hostname in Cisco devices, the command syntax will be

#hostname <New Hostname>

hostname is the **command** and <New hostname> is the **variable** or **input portion** to **hostname** command

Through variable substitution, single template is enough to change hostname of all devices same Vendor and OS Type configured in template; else each device requires a separate template.

To substitute a variable, follow the below steps, based on the condition applicable:

1) Use “Double Curly Brackets” before and after the **variable {{ }}**, only if variable is not inside Jinja2 statements

```
<command prompt="#" timeout="5">hostname {{Runtime.hostname}}</command>
```

Runtime is a substitution object.

NCCM Substitution Objects in Template:

NCCM supports 10 types of **substitution objects** for Variable substitution within configuration template

1) Runtime object

Runtime object will be used in Configuration Upload and Network Diagnosis activities. Runtime object variables will be converted into user input form to get values while configuring upload task or Network Diagnosis creation.

Ex {{Runtime.hostname}}

2) Global object

All Global parameters configured in NCCM are available through Global object for Variable substitution.

Ex {{Global.managementIP}}

3) Type object

Defines the field, based on the variable type specified such as Text Area, Text field, DropDown, Multi DropDown.

Ex : Type.Speed=DropDown

4) Default object

The default value for Type Object I defined here.

Ex: Default.Speed=10,100,1000

5) Remark object

Displays the Text on mouse hover on the Variable Name.

Ex: Remark.Speed=enter speed of interface

6) Optional object

If variable is declared 'Optional', the input for the field is not mandatory.

Ex: Optional.VariableName

7) Check object

Ensures that the Input format matches the defined format.

Ex: In Textfield, it should allow only 1 to 255 ^([1-9]| [1-9][0-9]| [1-2][0-5][0-5])\$

8) LOCAL_SHELL object

LOCAL_SHELL object gets values from LOCAL_ACCOUNT profile, configured in Device credential for Variable substitution.

Ex {{LOCAL_SHELL.username}}

9) Device object

Device object gets values from **Device database** of corresponding Device where command execution takes place.

Ex {{Device.IPAddress}}

10) Interface object

Interface object gets values from **Device Interface database** of the corresponding Device where command execution takes place.

Ex {{Interface.name}}

Ex {{Interface.description}}

11) Job object

Job object gets values from Job Database (Upload or Download Job) of corresponding Device where command execution takes place.

Ex {{Job.name}}

12) Profile object

Profile object gets values from Profile Database (Configuration Profile) of corresponding Device where command execution takes place.

Ex {{Profile.download_profile.user_name}}

13) Trigger object:

Trigger object gets values from Configuration Trigger Database of corresponding Trigger name used in Configuration Template.

Ex {{Trigger.triggername}}

Note: A template can have more than one Trigger variable.

14) Profile object:

Profile object gets values from Device Credential Database of corresponding Device (Device Credential) where command execution will take place.

Ex {{Profile.ssh_loginname}}

15) Time object:

Time object gets values from NCCM server based on current time which is for substituting time values in a template during execution

Ex {{Time.now}} – Time in unix epoch format

{{Time.YYYYMMDD}} – Time in YYYY MM DD format

{{Time.uniquestring}} – Unique string

2) Directly writing variable, if variable is inside Jinja2 expression statement **{% %o %}**

{% if Runtime.hostname. == "router27" %}

Conditioning in Template:

NCCM supports condition based Templating using “if”, “if else” and “if elif else” conditional statements

A. “If” Condition:

```
{% if Runtime.interface_name == "GigabitEthernet0/0" %}  
    IP address 192.168.1.1 255.0.0.0  
    no shutdown  
{% endif %}
```

B. “If else” Condition:

```
{% if Runtime.interface_name == "GigabitEthernet0/0" %}  
    IP address 192.168.1.1 255.0.0.0  
    no shutdown  
{% else %}  
    IP address 192.168.2.1 255.0.0.0  
    no shutdown  
{% endif %}
```

C. “If elif else” Condition:

```

{%
if Runtime.interface_name == "GigabitEthernet0/0" %}
    IP address 192.168.1.1 255.0.0.0
    no shutdown
{%
elif Runtime.interface_name == "GigabitEthernet0/1"   %}
    IP address 192.168.1.1 255.0.0.0
    no shutdown
{%
else %}
    IP address 192.168.2.1 255.0.0.0
    no shutdown
{%
endif %}

```

Looping in Template:

NCCM supports loop based Templating using “for” loop statements

“For Loop” Condition:

```

{%
for interface_name in Runtime.interface_names %}
    {%
if {{interface_name}} == "GigabitEthernet0/0" %}
        IP address 192.168.1.1 255.0.0.0
        no shutdown
    {%
endif %}
{%
endfor %}

```

Guidelines for Configuration Template:

#Substitution, Conditioning, Looping in Template should be in Jinja2 standard.
Refer <http://jinja.pocoo.org/docs/2.10/> for more tutorials.

Points to Remember

Always enclose the commands within **{% %}** for “if” and “for”, “while” conditional statements

Always enclose the variables inside **{{ }}** for substitution

Sample Template Configuration

Example 1: Create an Empty List and add values into List and DO a simple 'For Loop'

```
# Declaring a string variable to store value from Runtime or user. Default ("")  
function will make variable empty string till USER input
```

```
{% set myinput = Runtime.interface_list | default("") %}
```

```
# Converting User Input to a list using Split function
```

```
{% set mylist = myinput .split(",") %}
```

```
#Doing for Loop or Looping of Each Item
```

```
{% for each_interface in mylist %}  
    <command prompt="#">int {{each_interface}}</command>  
    <command prompt="#">shutdown</command>  
# for requires endfor to close the section  
{% endfor %}
```

Example 2: Conditions (if case elif Case and else case)

```
{% for each_interface in mylist %}  
    {% if each_interface == "Gi0/1" %}  
        <command prompt="#">int {{each_interface}}</command>  
        <command prompt="#">shutdown</command>  
    {% elif each_interface == "Gi0/2" %}  
        <command prompt="#">int {{each_interface}}</command>  
        <command prompt="#">no shutdown</command>  
    {% else %}  
        <command prompt="#">I dont know</command>  
    {% endif %}  
{% endfor %}
```

Example 3: Taking List Input from a Trigger

#down_interface_list_cisco_ios is a Trigger in Configuration Trigger

```

{%
set mylist1 = Trigger.down_interface_list_cisco_ios | default([]) %}
{%
for each_interface in mylist1 %}
    <command prompt="#">int {{each_interface}}</command>
    <command prompt="#">shutdown</command>
{%
endfor %}

```

Example 4: Disable the Interface named 'Ether'

String Manipulation **startswith, endswith, find, lower, upper, strip**

```

{%
set myinput = Runtime.InterfaceNames | default ("") %}

{%
set mylist = myinput.split(",") %}

{%
for each_item in mylist %}
    {%
if each_item.lower().startswith("ether") %}
        <command prompt="#">int {{each_item}}</command>
        <command prompt="#">shutdown</command>
    {%
endif %}
{%
endfor %}

```

Example 5: Taking First Element from the Trigger

```

{%
set mylist = Trigger.down_interface_list_cisco_ios | default ([])%}\

{%
if mylist %}
    <command timeout ="10" prompt ="#" >config t</command>
    <command timeout ="10" prompt ="#" >interface {{mylist[0]}}</command>
    <command timeout="10" prompt  ="#" >IP address 172.17.230.2
255.255.255.252</command>
    <command timeout ="10" prompt  ="#" >no shut</command>
{%
endif %}

```

Action Icons

Multiple action icons are displayed on the top right corner of the page.

Label	Actions
Filter	Click to use filter options to search
Add	Click to add 'Configure Template'
Edit	Click to edit a Template

Delete	Click to delete a Template
Production Ready	Click to mark the template ready for Production
Enable	Click to enable template
Disable	Click to disable Template
Execute	Click to execute the template immediately
Import	Click to import Template
Export	Click to export Template

Configuration Template Filter

NCCM allows filtering the Configuration Templates based on the following columns.

- Template Name
- Vendor
- OS Type
- Model
- Template type
- Active Status
- Template Group
- Production Status
- Approval State

Click "Search" to perform the filter based search on filter columns selection.

Note: NCCM supports full match and pattern match for user input fields.

Add Template

Click on the (+) icon located at the top right corner to add a Configuration Template.

NCCM supports nine different types of Templates and each type is used for specific requirement. They are

- o Command Execution
- o Configuration Merge
- o Configuration Replace
- o Configuration Rollback
- o OS Image Upgrade

- o Network Task Automation
- o NETCONF Merge
- o NETCONF Replace
- o Network Diagnosis
- o HTTP REST-API Configuration
- o Golden Template

Command Execution

Command Execution is used to execute a series of command (one by one) on devices, which is similar the user executing commands through putty application for configuration changes. This template type should be used for changing small set of configurations which does not roll back to previous ones.

Click "**Command Execution**" and click "OK" to proceed further.

- Input the Template Name
 - o Template Name should be unique.
- Select the Template Group using the dropdown menu.
- Select Vendor using the dropdown menu.
 - o This is mandatory since Template commands are specific to vendor device.
- Select the OS Type
 - o This is mandatory since Template commands are specific to vendor device OS types. In case of commands being executable on all devices of vendor then input as ALL TYPE.
- Input the Model details.
- Input the Series details.
- Approval Required Checkbox is mandatory and user cannot uncheck it. (This is a compliance requirement).
- Input the Template Description.

Click "**Template Configuration**" panel.

- Select the Configuration Type or Store using the dropdown menu.
 - Supported Types are Startup, Running and Candidate.
 - This value does not impact the operation but acts as a label for type of configuration that is required to be changed.
- Click or to load configuration
 - User can load configurations from existing downloaded version or load the configuration commands from a text file.
 - After loading the configuration commands, user has to make device specific changes and create variables, to be filled by NCCM during device execution.

Click "**Access Control**" panel

- Select the visibility
 - **Note:** If the visibility is "Private", User and User group dropdown will be enabled and selected user and administrator will only be able to manage this template.
- Select the User(s).
- Select the User group(s).
- Click "**Save**" to save the template with given input.
- Click "**Cancel**" to abort the Template creation.

Example for Command Execution:

```
<command prompt="#">conf t</command>
<command prompt="#">hostname {{Runtime.xxxx}} </command>
```

Configuration Merge

Configuration Merge is used to upload or merge a command block into Device. This type should be used for creating or merging a configuration block into device.

Click "**Configuration Merge**" and click "**OK**" to proceed further.

- Input the “Configurations to Merge” by directly typing or ‘Loading from Snapshot’ or from a file.
- Input the “CLI Commands to Merge”. The CLI Commands will merge the new Configurations into Device Configuration.

Example Commands to Merge:

```
<command prompt="[\]\?">copy tftp: running-config</command>
<command prompt="[\]\?">{{Global.managementIP}}</command>
<command prompt="[\]\?">{{Job.uploadfilename}}</command>
<command previous_match="confirm\]" prompt="#" timeout="300">yes</command>
<command action="exit" prompt="">exit</command>
```

Note: NCCM will auto fill the “Configurations to merge commands” into Job object uploadfilename variable. The rest of the inputs are similar to “Add Command Execution.”

Configuration Replace

Configuration Replace is used to replace a full configuration into device. This should be used for replacing default or configuration discrepancies with backed up configuration version.

Click “**Configuration Replace**” and click “**OK**” to proceed further.

- Input the “Configurations to Replace” by directly typing or Loading from Snapshot or from a file.
- Input the “CLI Commands to Replace”. The CLI Commands will replace the new full Configurations into Device Configuration.

Example Commands to Replace:

```
<command prompt="[\],#" timeout="300">configure replace
tftp://{{Global.managementIP}}/{{Job.uploadfilename}}</command>

<command previous match="confirm\]" prompt="#" timeout="300">y</command>

<command action="exit" prompt="">exit</command>
```

Note: NCCM will auto fill the “Configurations to Replace commands” into Job object uploadfilename variable.

The rest of the inputs are similar to “Add Command Execution”.

Configuration Roll back

Configuration Rollback template will Roll the device configuration back to its previous configuration version.

Click "**Configuration Rollback**" and click "**OK**" to proceed further

- Input the "Configurations to Replace" by loading either from Snapshot or from a file.
- Input the "CLI Commands to Rollback". The CLI Commands will roll the Device Configuration back to the uploading Configuration version.

Example Commands to Rollback:

```
<command prompt="[\],#" timeout="300">configure replace  
tftp://{{Global.managementIP}}/{{Job.uploadfilename}}</command>  
  
<command previous_match="confirm\]" prompt="#"  
timeout="300">y</command>  
  
<command action="exit" prompt="">exit</command>
```

Note: NCCM will auto fill the "Configurations to Rollback commands" into Job object upload filename variable.

- User can also Input the following TAGS in "CLI Commands to Rollback" rather filling the actual Configuration.

BASELINE-STARTUP-CONFIGURATION

NCCM will roll back the Baseline Startup configuration of the corresponding device.

PREVIOUS-STARTUP-CONFIGURATION

NCCM will roll back the previous startup configuration of the corresponding device.

BASELINE-RUNNING-CONFIGURATION

NCCM will roll back the baseline running configuration of the corresponding device.

PREVIOUS-RUNNING-CONFIGURATION

NCCM will roll back the previous running configuration for the corresponding device.

Note: **Tags** will be used while Replacing Configurations on multiple devices, at the same time. The rest of the inputs are similar to "Add Command Execution".

Note: Before creating a "Roll Back upload job" or "Auto creation of Rollback Job" from Upload Job Task Result, Configuration Replace templates should be created in NCCM for each vendor & OS Type and Template should follow naming standards.

Name of the Replace Template should be

- "**Configuration Rollback To Base - <Vendor><OS type>**"
- "**Configuration Rollback To Previous - <Vendor><OS type>**"

Example for CISCO IOS

Configuration Rollback to Base - Cisco-IOS

Configuration Rollback to Previous - Cisco-IOS

Example for CISCO NXOS

Configuration Rollback to Base – Cisco - NXOS

Configuration Rollback to Previous – Cisco - NXOS

Example for CISCO any OS type

Configuration Rollback to Base – Cisco - ANY Type

Configuration Rollback to Previous – Cisco - ANY Type

OS image Upgrade

OS Image upgrade is used to upgrade the OS Image or OS Patch update into device.

Click "**OS Image Upgrade**" and click "**OK**" to proceed further.

- Input the CLI commands for OS Upgrade specific to Device OS.

Example for Cisco IOS Upgrade:

```
# Make Terminal Len 0  
<command prompt="#" timeout="60">term len 0</command>
```

```
#Copy the Image to Flash  
<command prompt="]\?" timeout="60">copy tftp flash0:</command>
```

```

#Input the TFTP Server IP
<command prompt="]\?>" timeout="60">{{Global.managementIP}}</command>

#Input the Source OS Image
<command prompt="]\?>" timeout="60">{{Runtime.osimagename}}</command>

#Destination OS Image as Enter
<command prompt="#, confirm" timeout="600" error_pattern="Error">CRLF</command>

#Overwrite the OLD OS
<command prompt="#, confirm" timeout="600" previous_match="confirm" error_pattern="Error">y</command>

#For Erase Confirmation due to size
<command prompt="#, confirm" timeout="600" previous_match="confirm" error_pattern="Error">{{Runtime.erase_flash_when_low_memory}}</command>

#For Erase Double Confirmation due to size
<command prompt="#" timeout="600" previous_match="confirm" error_pattern="Error">{{Runtime.erase_flash_when_low_memory}}</command>

#File Copied or not check
<command prompt="#" timeout="60" error_pattern="Error" >dir flash0:{{Runtime.osimagename}}</command>

#Do boot sequence
<command prompt="#" timeout="60">conf t</command>

#no boot system
<command prompt="#" timeout="60">no boot system</command>

#Boot from new OS Image
<command prompt="#" timeout="60">boot system flash0:{{Runtime.osimagename}}</command>

```

```

#Change Register to config-register 0x2102
<command prompt="#" timeout="60">config-
register 0x2102</command>

#Exit out of Conf t
<command prompt="#" timeout="60">exit</command>

#Copy Running to Start
<command prompt="#,[#\]\?]" timeout="60">copy run start</command
>

#Confirmation
<command prompt="#" timeout="60" previous_match="config">CRLF</c
ommand>

#Reload
<command prompt="]" timeout="60">reload</command>

#Send No for Saving System Configuration
<command prompt="]" timeout="120" previous_match="yes">no</com
mand>

#Reload Confirmation
<command prompt="[" action="exit" timeout="30"
previous_match="confirm">y</command>

```

Note:

1. NCCM also supports md5 checksum, and Activation Key for Cisco IOS Upgrade in command template variable substitution and check constraint check.
2. In case of other vendors and Cisco other OS Types, OS Upgrade template should be built as per vendor command standard.
3. Before creating an “OS Image Roll Back Upload Job” automatically from OS Upload Job Task Result, OS Upgrade templates should be created in NCCM for each vendor & OS Type and Templates should follow naming standards. Name of the Template should be

“OS Image Upgrade - <Vendor> <OS type>”

Example for CISCO IOS

OS Image Upgrade - Cisco-IOS

Example for CISCO NXOS

OS Image Upgrade - Cisco-NXOS

The rest of the inputs are similar to "Add Command Execution".

Network Task Automation

Network Task Automation is similar to Command Execution Template which executes a series of commands, one by one.

This template should be used for Network Automation tasks like Health Check, Trace Route, Backing up important data's, finding device service configurations like "SNMP Status, BGP Status, SSH Status, TFTP reachability" regularly.

Click "**Network Task Automation**" and click "**OK**" to proceed further.

The rest of the inputs are similar to "Add Command Execution".

Example:

If we have to check important application servers availability from core router on a daily basis, write the below command in the template.

```
<command prompt="#> ping 192.168.50.235</command>
```

NETCONF Merge

NETCONF merge is used to merge the given configurations into existing device configuration (Applicable only for NETCONF protocol supporting devices).

Click "**NETCONF Merge**" and click "**OK**" button to proceed further.

- Input the Netconf Merge Commands in NetCONF XML protocol format. The rest of the inputs are similar to "Add Command Execution."

NETCONF Replace

Replace full configuration into existing device configuration (Applicable only for NETCONF protocol supporting devices).

Click "**NETCONF REPLACE**" and click "**OK**" to proceed further.

- Input the Netconf Replace Commands in NetCONF XML protocol format.

The rest of the inputs are similar to "Add Command Execution".

Network Diagnosis

This is similar to Command Execution Template which executes a series of commands, one by one. This template should only be used for Network Diagnosis tasks like Health Check, Trace Route, finding device service configurations like "SNMP Status, BGP Status, SSH Status" on an adhoc basis.

Click "**Network Diagnosis**" and click "**OK**" to proceed further.

- Input the Commands for Diagnosis.

The rest of the inputs are similar to "Add Command Execution".

Note: *Network Diagnosis Template will be used in "Network Diagnosis feature" by service engineers.*

HTTP REST-API Configuration

This option is used to perform Network and service configurations through HTTP (REST) API. It takes HTTP(S) URL, Headers, Form or RAW JSON content to execute a configuration change.

Click "**HTTP REST-API Configuration**" and click "**OK**" to proceed further.

- Input the Template Name
 - Template Name must be unique.
- Select the Template Group using the dropdown menu.
- Select Vendor using the dropdown menu.
 - This is mandatory since Template commands are specific to vendor device.
- Select the OS Type
 - This is mandatory since Template commands are specific to vendor device OS types. In case of commands being executable on all devices of vendor then input as ALL TYPE.
- Input the Model details.
- Input the Series details.
- Approval Required Checkbox is mandatory and user cannot uncheck it. (This is a compliance requirement).

- Input the Template Description.

Click "**Template Configuration**" panel.

- Select the Configuration Type or Store using the dropdown menu.
 - Supported Types are Startup, Running and Candidate.
 - This value does not impact the operation but acts as a label for type of configuration that is required to be changed.
 - Select Method (POST, GET, PUT, DELETE, PATCH) and provide URL.
 - Input Parameters and Headers in the respective text boxes.
 - Select Body type and RAW type using the dropdown menu.
 - Input Body (commands), Success code, Pattern, and configuration Trigger in the respective text boxes.

Click "**Access Control**" panel.

- Select the visibility
 - **Note:** If the visibility is "Private", User and User group dropdown will be enabled and selected user and administrator will only be able to manage this template.
- Select the User(s).
- Select the User group(s).
- Click to save the template with given input.

Golden Template

This feature will be used to identify the missing and additional configurations across the devices, based on a standard template defined by the organization.

Note: This is just a placeholder to save the Golden Template commands and not to be used to execute.

Click "**Golden Template**" and click "**OK**" to proceed further.

- Input the Template Name
 - Template Name must be unique.
- Select the Template Group using the dropdown menu.
- Select Vendor using the dropdown menu.

- o This is mandatory since Template commands are specific to vendor device.
- Select the OS Type
 - o This is mandatory since Template commands are specific to vendor device OS types. In case of commands being executable on all devices of vendor then input as ALL TYPE.
- Input the Model details.
- Input the Series details.
- Approval Required Checkbox is mandatory and user cannot uncheck it. (**This is a compliance requirement**).
- Input the Template Description.

Click "**Template Configuration**" panel

- Select the Configuration Type or Store using the dropdown menu.
 - o Supported Types are Startup, Running and Candidate or all..
 - o This value does not impact the operation but acts as a label for type of configuration that is required to be changed.
- Click or to load configuration
 - o User can load configurations from existing downloaded version or load the configuration commands from a text file.
 - o After loading the configuration commands, user has to make device specific changes and create variables, to be filled by NCCM during device execution.

Click "**Access Control**" panel

- Select the visibility
 - o Note: If the visibility is "Private", User and User group dropdown will be enabled and selected user and administrator will only be able to manage this template.
- Select the User(s).
- Select the User group(s).

- Click "**Save**" to save the template with given input.

Device Authorization Profile

This feature will be used to define set of commands that can be executed/denied execution by a specific user/user group on Infraon NCCM. Administrators can also restrict/permit command execution authorization based on device models.

Click "**Device Authorization Profile**" and click "**OK**" to proceed further.

- Input the Template Name
 - o Template Name must be unique.
- Select the Template Group using the dropdown menu.
- Select Vendor using the dropdown menu.
 - o This is mandatory since Template commands are specific to vendor device.
- Select the OS Type
 - o This is mandatory since Template commands are specific to vendor device OS types. In case of commands being executable on all devices of vendor then input as ALL TYPE.
- Input the Model details.
- Input the Series details.
- Approval Required Checkbox is mandatory and user cannot uncheck it.

(This is a compliance requirement).

- Input the Template Description.

Click "**Template Configurations**" panel.

Infraon NCCM accepts command input in regex pattern only. Command inputs are split into five sections. They are:

- **Terminate Commands** - Command (sets) that are denied for execution by the User/User Group. When a user tries these set(s) of commands, Infraon NCCM terminates the CLI Session immediately.

- **Block Commands** - Command (sets) that are denied for execution by the User/User Group. When a user tries these set(s) of commands, Infraon NCCM blocks these commands from being executed. The CLI session is not terminated here.

- **Notify Commands** - When a user tries these set(s) of commands, Infraon NCCM executes the same and triggers a notification about the action. If this option is selected, Notifier (Notification Alert) must be selected using the dropdown menu.

- **Permit Commands** – Command (sets) that are permitted for execution by the User/User Group. Commands that are not added in the ‘Permit’ section will be blocked at the time of execution.

- **System Commands** – used to ignore inputs like password and other User credential input. For example: When a user tries to execute a Command, that requires authentication by the system, the user is prompted by the system to provide additional information. In this case, system prompt must be added in the ‘Ignore’ section. If not, system runs the command through the Permit command list and may end up blocking the command/command set.

There are two ways to input commands:

1. Adding commands in the respective text boxes.
2. Importing saved commands from a file. To import commands, click on the respective button:

Load Terminate Commands from File, Load Block Commands from File, Load Notify Commands from File, Load Permit Commands from File, Load System Commands from File

Click "Access Control" panel

- Select the visibility
 - Note: If the visibility is “Private”, User and User group dropdown will be enabled and selected user and administrator will only be able to manage this template.
- Select the User(s).

- Select the User group(s).
- Click "**Save**" to save the template with given input.

Miscellaneous

Edit Template

Select an existing template and click on "**Edit**" to edit. Edit operation follows the same steps as 'Add Template'. Other than Template Type all other fields on template can be modified.

Delete Template

Select the Template(s) and to the delete the Template, click on the delete icon.

Click "**YES**" to delete the Template or "**NO**" to cancel the delete operation.

Enable Template

Select Template(s) and click to enable the template i.e. to move the template state to active. Only Active Templates will be used in Upload job and Network Diagnosis.

Disable Template

Select Template(s) and click to disable the template. Disabled templates will not be used in Upload job and Network Diagnosis.

Production Ready

Select Template(s) and click to change the templates' Production status to active. Only Active production Templates will be used in Upload job and Network Diagnosis. Templates manually created by user will be saved in Production Ready and Enabled State. In case of Import Templates, Production Ready status will be in 'Disabled' state.

Note: Templates imported into NCCM using excel must be changed manually to 'Production Ready' state.

Execute/Add Upload Job

Click to execute the template, which will redirect to 'Add an Upload Job'.

Template Import

Click to upload/Import the template file (Only .xls file format is supported).

Template Export

Click to export NCCM's configured Templates to the XLS file. Click to Download/Export the templates into excel file.

Download Jobs

Download Job refers to a task that involves retrieving configuration files from network devices such as routers, switches, firewalls, and others and storing them centrally within the system.

The download typically captures the devices' current running configuration and start-up configuration. This job helps IT teams maintain up-to-date backups for disaster recovery, ensure compliance with internal policies, and track any configuration changes over time.

The management admin (user with appropriate privileges) initiates the download process, where network devices can be selected and the configuration type (running or start-up configuration) specified. The tool helps ensure that all configurations are securely backed up, enabling efficient configuration management across multiple devices and vendors.

Infraon's Download Jobs added through the Discovery process or manual Device addition will start downloading:

- Device configurations (Startup & Running - when both are supported by the vendor)
- Operational Data (which can be customized by the administrator)
- Device Inventory Details
- OS image details based on 'Configuration Profile' assigned
- Device Credentials
- Connection & Download protocol selection
- Schedule (daily, weekly, monthly, and Every 'N' days) period

Infraon's Download Job downloads the configurations from devices that support at least one of the management protocols:

- SSHv1
- SSHv2
- TELNET

NETCONF protocol will also be supported in addition to the above protocols to maintain the configuration in XML Format.

Each device will have its own Download job to schedule the download frequency at different intervals.

What you see on the screen

The **Download Job** page displays the list of active and scheduled download jobs in the network configuration inventory. The following table outlines the available action icons and their descriptions.

Download Jobs Details | Basic Details

Label	Action	Description/ Example
Search	Search for the required download job.	Search by device credentials, asset ID, name, etc., to quickly locate a specific download job.
Filter	Apply a filter based on field conditions.	Filters can be applied to various fields, including IP address, device credentials, vendor, status, and configuration type. Conditions include equals, contains, etc.
Date Range	Filter download jobs by a specified time frame.	Select time ranges such as the current hour, last 30 minutes, last hour, etc., to narrow down job history.
Go to Assets	Navigate to the asset module homepage.	Redirects to the IT Assets module to manually add or manage devices and download jobs.
Download Results	View the results of download jobs.	Opens a pop-up displaying the status and outcome of configuration downloads, including device name, IP address, status (success/failure), and error logs.
Column Selection	Customize the columns shown on the page.	It allows users to modify which columns appear in the table by dragging and dropping them from 'Available' to 'Selected'. Columns can also be rearranged or frozen.
Export	Export download job data to a CSV file.	Download a CSV file containing details of all download jobs for offline use.
Bulk CSV Update	Edit multiple download jobs at once via CSV.	Follow the steps outlined below to complete the import successfully: <ul style="list-style-type: none">• Download the sample CSV template to ensure proper data structure.

		<ul style="list-style-type: none"> Enter the required information into the CSV file accurately. Upload the completed CSV file and click "Next." Review the system's column mapping, adjust if necessary, and click "Import."
Import from CSV	Add download jobs in bulk via CSV.	<p>Upload a CSV file with the respective fields, then review and import the jobs after verifying the data.</p> <p>Import from CSV File</p> <ul style="list-style-type: none"> Download the CSV file (excel sheet) and enter the respective fields in the sheet. Upload the same edited CSV file. Click Next -> Import -> Proceed with Valid Records.
Column Details		
Summary Card	Click any field to view detailed information.	<p>This displays a summary of the download job, including the name, IP address, configuration profile, and associated device credentials.</p> <p>Example: Error in making a connection to the device. Verify the connection commands in the Configuration Profile are valid and check the Download Job Audit for finding the invalid command</p>
Device Credential	View-only field, no actions.	Displays the device credentials associated with the download job.
Status	View-only field, no actions.	Indicates the operational status of the download job.
Running Configuration	Click to view the running configuration.	<p>The pop-up window displays the current running configuration, including the download date and time. Search and export options (.txt) are available.</p> <p>(Where Device Connection and Download Commands are maintained)</p>

		Example: Download Time: Dec 23, 2024, 12:10 PM (V33).
Startup Configuration	Click to view the start-up configuration.	The pop-up window displays the current start-up configuration, including the download date and time. Search and export options (.txt) are available. (Where Device Connection and Download Commands are maintained)
		Example: Download Time: Dec 23, 2024, 12:10 PM (V25).
Agent	View-only field, no actions.	Displays the agent name, IP address, and vendor details associated with the download job.
Next Action Time	View-only field, no actions.	Displays the scheduled time for the next action associated with the download job.
Last Action Time	View-only field, no actions.	Displays the timestamp of the last action performed on the download job.

Action Icons | Download Jobs

Label	Action	Description/ Example
Edit	Modify an existing download job.	Update job details like configuration, connection, download, retry, and other details.
Delete	Click to remove a download job from the list.	Deletes the selected download job from the system.
Download Now	Initiate an immediate configuration download.	Select a job and click the download icon to download the device configurations immediately.
View Result	View the results of the executed download job.	Displays detailed results of the configuration download, including status and timestamps.
View Audit	Review the audit trail for the executed job.	Displays a log of actions taken during the download process, including user actions and system changes.
Change Agent	Change the agent used for the download process.	It allows users to select a different agent from the list to monitor or fetch the device configuration during the download.

Configuration Details	<p>View the configuration details of the download job.</p>	<p>Displays detailed configuration data, including:</p> <ul style="list-style-type: none"> • Download Job Summary <ul style="list-style-type: none"> ◦ Device Credential ◦ Configuration Profile ◦ Connection Protocol ◦ Download Status ◦ Agent ◦ Status ◦ Download start time ◦ Download end time ◦ Next download time ◦ Inventory download protocol ◦ Startup configuration download protocol ◦ Running Configuration download protocol • Configuration details <ul style="list-style-type: none"> ◦ Baseline Running ◦ Current Running ◦ Current Startup ◦ Baseline Startup ◦ Previous v/s Current running ◦ Previous v/s Current Start-Up ◦ Baseline v/s Current running ◦ Baseline v/s Current Start-Up
Resync Agent	<p>Resynchronize the agent associated with the job.</p>	<p>Synchronizes the download job with the assigned agent to prepare it for the configuration download.</p>

View Result | Action Icons

It summarizes configuration retrieval jobs from network devices like routers, switches, and firewalls. It displays key details such as the job status (success or failure), device information (IP addresses and versions), and timestamps for initiating and completing the download.

The following table outlines the available action icons and their descriptions:

Label	Action	Description/ Example
--------------	---------------	-----------------------------

Search	Search for the required download job result.	Search by IP Address to locate a specific download job quickly.
Filter	Apply a filter based on field conditions.	Filters can be applied to various fields, including IP address, Configuration Type, Download Triggered From, and Download Status. Conditions include equals, contains, etc.
Date Range	Filter download job results by a specified time frame.	Select time ranges such as the current hour, last 30 minutes, last hour, etc., to narrow down job history.
Export	Export download job result data to a CSV file.	Download a CSV file containing details of all download jobs for offline use.
Column Details		
Version	Click to re-direct to the comparison data	Displays the version name or number for the respective result.
Configuration	Click to open the configuration type linked	In the pop-up window, display the type. Search and export options (.txt) are available. Example: Configuration Type: start-up (Configuration: Dec 21, 2024, 08:12 PM (-NA-))
IP Address	View-only field: no actions can be taken	Displays the IP address of the device from which the configuration was downloaded.
Configuration Type	View-only field: no actions can be taken	Indicates whether the configuration is a running or start-up configuration.
Status	View-only field: no actions can be taken	Displays the current status of the download job, such as success, failure, or pending.
Download Triggered From	View-only field: no actions can be taken	Indicates the origin of the download trigger, whether it was manual, scheduled, or automatic.
Agent	View-only field: no actions can be taken	It displays the name of the agent who facilitated the download process, along with its IP address and vendor details.
Actions		
Baseline	View-only field: no actions can be taken	Allows users to flag the selected jobs as standard or reference configuration.

View Audit | Action Icons

Displays a detailed log of activities related to a specific download job. It includes timestamps for when the job was initiated, modified, or completed. The audit log

also captures configuration details such as the type of configuration downloaded (running or start-up), error logs, and any issues encountered during the process.

The following table outlines the available action icons and their descriptions:

Label	Action	Description
Search	Search for the required download job.	Search by Message, date, etc., to quickly locate a specific download job.
Filter	Apply a filter based on field conditions.	Filters can be applied to various fields, including Message and Message Type. Conditions include equals, contains, etc.
Auto Refresh	Click to turn on the toggle to get the page automatically refreshed.	Enables real-time updates of the download audit log without needing a manual refresh.
Timestamp	View only field; no actions can be taken.	Displays the exact date and time when the download job activity occurred. Example: Dec 21, 2024 08:11:37 PM
Message Type	View only field; no actions can be taken.	Displays the type of message (e.g., success, error, warning) related to the job. Example: Audit, Running.
Message	View only field; no actions can be taken.	Shows detailed messages describing any issues that occurred during the download job. Example: Connection failed with Primary IP address: 10.0.5.58, Primary Device credential: Infraon Server evere\$T using SSH connection protocol.

Bulk Actions

Bulk action icons enable users to manage multiple download jobs at once efficiently. Users can perform bulk actions through the pop-up menu by selecting jobs with checkboxes.

Refer to the table below for detailed actions and their functionalities:

Bulk Actions | Action Icons

Label	Actions	Description
Delete	Click to delete selected download jobs	Removes the selected download jobs from the system.

Edit	Click to edit selected download jobs	Allows users to modify the details of the selected download jobs, such as configurations and settings.
Enable	Click to enable selected jobs	Activates the selected download jobs, allowing them to run based on their scheduled configurations.
Disable	Click to disable selected jobs	Temporarily deactivates the selected download jobs, preventing them from running until re-enabled.
Change Agent	Click to change the agent for selected jobs	Allows users to assign a different agent to manage the selected download jobs.
Download Now	Click to initiate an immediate download for selected jobs	Forces the selected download jobs to start instantly, overriding the scheduled time.
Resync Agent	Click to resync the agent for selected jobs	Re-establishes the connection between the selected download jobs and the agent, ensuring smooth operations.

Add Download Jobs

There are three ways to add download jobs: manually, by entering the required details individually through the interface, or via CSV bulk upload, which allows users to add multiple jobs at once using a preformatted CSV file, and by selecting the “**Configuration Download**” toggle in the Automatic discovery page.

Manual

To add download jobs for a specific IT asset, follow these steps:

- Click on “**Go to Assets,**” located on the top panel of the page. (This will redirect you to the IT Assets page.)
- Select the checkbox under the desired IT asset, then go to the top panel and choose “**More**” -> “**Add Download Jobs**”.
- Refer to the table below to enter the required details.

Add Download Jobs | Manually

Label	Action	Description
		Device IP Address
IP Address	Enter the unique identifier for the device.	The IP address helps in identifying the network device for which the job is being added. Example: 192.168.0.1.

Configuration Profile		
Profile*	Select from the drop-down to identify the configuration profile to add.	The profile name helps group and manage configurations for specific devices. Example: Cisco IOS SGS.
Vendor*	Provide the vendor's name associated with the configuration profile.	This is the manufacturer of the device. Example: Cisco, Juniper, Nivetti, etc.
Schedule Details *		
Schedule Details	Choose a schedule mode from the options: once , every , daily , weekly , or monthly , and set a specific time .	Schedule details determine when the download job will be executed automatically. Example: Scheduled on 23 December 2024, 12:0
Device Credentials*	Select the primary device credential profile from the drop-down list.	Device credentials include a username and password for accessing the device securely. Example: Cisco Infraon Server.
Secondary Device Credentials	Select an optional secondary device credential profile from the drop-down list.	Secondary credentials act as a backup in case primary credentials fail. Example: SNMP Default
Select Agent*	Pick the relevant agent from the drop-down list.	The agent is a service or application responsible for executing the download job. Example: INFRAON_APP.
Connection Details		
Ping Timeout (msec)	Enter the timeframe in milliseconds.	If the "Filter by Ping" option is enabled, the specified ping timeout (in msec) will be applied. Example: 500.
Filter by Ping	Toggle to enable or disable the functionality.	When enabled, this option ensures that only devices that respond to a PING request are considered for configuration downloads.
Configuration Download Shell	Select either Remote or Local. Note: Shell property is used to Inform NCCM to open a	Choose the method to download the configuration file. Remote means downloading the configuration from a remote server, while

	remote session (TELNET or SSH) from a Device for further command executions.	Local means downloading the configuration from a local source.
Inventory Download Shell	Select either Remote or Local. Note: Shell property is used to Inform NCCM to open a remote session (TELNET or SSH) from a Device for further command executions.	Choose the method for downloading the inventory information. Remote fetches inventory data from a remote server, whereas Local uses data stored locally for the download.
Other Configuration Download Shell	Select either Remote or Local. Note: Shell property is used to Inform NCCM to open a remote session (TELNET or SSH) from a Device for further command executions.	Select the method for downloading additional configuration files (other than the main configuration). Remote or Local options determine whether the download is from a remote or local source.
Connection Protocol	Choose the protocol for Connection Download from the dropdown menu.	The communication protocol is used to connect to devices. Options include SSH , TELNET , or a combination of both.
Download Protocol		
Running Configuration Download Protocol	Select the protocol for Running Configuration Download using the dropdown menu.	Protocols available for downloading running configurations: TFTP , FTP , Terminal , SCP , and SFTP .
Start-Up Configuration Download Protocol	Select the protocol for Startup Configuration Download using the dropdown menu.	Protocols available for downloading start-up configurations: TFTP , FTP , Terminal , SCP , and SFTP .
OS Image Download Protocol	Select the protocol for OS Image Download using the dropdown menu.	Protocols for downloading OS images include TFTP , FTP , Terminal , SCP , and SFTP .
Inventory Download Protocol	Select the protocol for Inventory Download using the dropdown menu.	Options for downloading inventory details: TFTP , FTP , Terminal , SCP , SFTP .
Other Configuration Download Protocol	Select the protocol for Other Configuration Download using the dropdown menu.	Additional configuration protocols are supported: TFTP , FTP , Terminal , SCP , and SFTP .
Retry Times		
Retry Times	Choose the number of retries for a failed download from the dropdown menu.	Specifies how many times the system will attempt to re-download after a failure.

		Options: 0 to 5.
Retry Interval in Hrs	Specify the retry interval in hours using the dropdown menu.	Sets the time interval (in hours) between retries. Options range from 0 to 10 .
Other Details		
VTY Properties	Enter the VTY properties for the device.	Defines terminal properties for the Virtual Teletype (VTY) interface. Example: {"TERM":"xterm"}.
Minimum Configuration Lines Count	Define the minimum number of configuration lines to process.	Specifies the lower limit for configuration line processing. Example: 10.

Note:

- Fields marked with an asterisk (*) are mandatory and must be filled out.
- Connection, Download, Retry, and Other Details** are pre-filled by default. To modify these fields, use the "Edit" action icon.

Once the details have been filled, click "**Submit.**"

CSV Upload

To add download jobs for bulk, follow these steps:

- Navigate to the Download Jobs and select the "**Import from CSV**" option located on the top right corner.
- Download the CSV file (Excel sheet) and enter the respective fields on the sheet.
- Upload the same edited CSV file.
- Click Next -> Import -> Proceed with Valid Records.

Generate MD5

This module creates a unique identifier, called an MD5 hash, for each file. Similar to a fingerprint, the MD5 produces a 128-bit hash key that allows administrators to confirm a file's integrity and authenticity. By comparing the generated hash with a known or expected value, they can identify any modifications or corruption that might have happened during file transfers or storage. This function is crucial for maintaining the reliability and security of files within the network management system.

Jobs Account Audit

The Job(s) Account audit is basically User account-based audit information. From the "Audits" menu, click "Job(s) Account Audit."

This page captures and displays audit information on actions performed on the target device through Download Jobs, Upload Jobs, Trigger & Network Diagnosis.

Job(s) account audit displays the below information:

- Device IP Address
- Device Account
- Connection Protocol
- Password
- Enable Password
- Connect Time
- Connect Status
- Task Owner
- Job Type
- Job Name
- User IP Address
- Process
- Connect for (reason given by the user)
- Failure Message

OS Image

This is a privilege-based feature: The user will be able to access, view, add, edit, delete, execute, and export only if the administrator has given them privileges. This will be defined under roles and privileges.

Quick Action Icons

The quick action icons below can be placed at the top right corner of the Rule Group home page.

Label	Actions
Filter	Click to use filter options to search
Add	Click to add 'OS Image'
Edit	Click to edit OS Image
Delete	Click to delete OS Image
OS versions	Click to navigate to OS Versions page

Add Image

Click (+) redirects to the Add OS Image window.

- Select Vendor using the dropdown menu.
- Input the Series in the textbox.
- Input Model in the textbox.
- Select OS type using the dropdown menu
- Select OS Version using the dropdown menu.
- Mention the Image Type in the given textbox
- Select OS Image using the 'Choose File' option
- Check to replace the old image.
- Provide MD5 Hash Key in the given textbox (This is a mandatory field)
- Input Description in the given textbox.

Click "**Save**" to configure the Upload job or click "**Cancel**" to abort the job.

Note: To generate a new **MD5key**, navigate to and select the '**Generate MD5'** option.

Edit OS Image

Select the OS Image and click "**Edit**" to edit the OS image. Make the necessary changes and click "**OK**" to save the changes.

Delete OS Image

Select the OS Image and click the delete icon to redirect to the delete confirmation window.

Click "**Yes**" to delete the OS image or click "**No**" to abort the delete operation.

OS Image Search

Click Filter to open the search options.

- Input the Vendor in the textbox.
- Input the OS type in the textbox.
- Input the Series in the textbox.

- Input the Updated details in the textbox.
- Input the Image Name in the textbox

Click "**Search**" to perform the search, based on the applied filter

OS Versions

Whenever a new OS image is uploaded to the device, all the previous versions will be maintained here. Click to redirect to the OS version page.

Note:

- o New OS images will be added whenever an OS image is downloaded from the device.
- o OS Images can be downloaded by clicking the OS Image column (OS Images Grid page).

OS Image Download Status

This feature keeps users in the loop regarding operating system downloads for your network devices. It offers real-time updates on the download's progress, whether it's ongoing, finished, stuck in a queue, or encountered errors. Details like **Vendor, OS Image, Download Status, Next Action Time, Actions (Audits and OS Download Now)** can be accessed.

Monitoring this status is crucial for ensuring successful OS deployments and allows administrators to troubleshoot download issues, guaranteeing devices receive the necessary updates.

OS Image Download Scheduler

This module empowers administrators to orchestrate operating system updates for network devices. This feature lets you plan and automate downloads at specific times, often during off-peak hours, to minimize network congestion. You can ensure a controlled rollout, prioritize critical devices, and efficiently manage large deployments by scheduling updates. Ultimately, the scheduler streamlines network maintenance, boosting overall reliability and reducing the risk of disruptions.

What you see on the screen

Details | Basic

Label	Action
Search	Search for the Download Schedule using the name, IP Address, etc.

Filter	Filter can be added based on the field (Name, Status, IP Address Mode, Agent Mode) and condition from the drop-down box below.
Actions	
Edit	Click to make any required changes to the schedule.
Delete	Click to delete the schedule

Configuration Details | [OS Download Image Scheduler](#)

- Name
- Description
- Status
- IP Address Mode
- IP Address
- Agent Mode
- Agent
- Created By
- Modified By
- Creation Time
- Last Update Time
- Schedule Description

How to Add Schedule

- Navigate to the **Infraon Configuration -> IT Operations -> Network Configuration** and select **OS Image** module.
- To schedule a download of an OS Image, click on the "**Add Schedule**" option at the top right corner of the page.
- Add the required name and description for the schedule.
- Select the required IP Address and Agent details in the respective call-out boxes.
- Choose how often you want to download the OS image: Select a schedule mode from "**Once,**" "**Every,**" "**Daily,**" "**Weekly,**" or "**Monthly,**" and then specify the date and time for the download.
- Once done, click on "**Submit**" to proceed.

Upload Jobs

Upload jobs involve changing or updating configuration files or firmware from the Infraon NCCM server to network devices. They're commonly used for deploying new devices, updating existing ones, and upgrading device firmware. For instance, users can simultaneously upload entire configuration files or specific snippets to individual or multiple devices.

While backup involves taking a copy of the device configuration and retaining it in the NCCM, upload refers to the opposite. "Upload" transfers the configuration from the NCCM to the device. Entire configuration files or select lines/snippets within a file can be uploaded using the Network Configuration Manager.

This is a privilege-based feature: The user can access, view, add, edit, delete, execute, and export only if the administrator has given them privileges. This will be defined under roles and privileges.

Upload jobs are controlled ways of changing the Device Configuration and Device OS Image within a defined period.

What you see on the screen

The **Upload Job** page displays the list of active and scheduled jobs in the network configuration inventory. The following table outlines the available action icons and their descriptions.

Upload Jobs Details | Basic Details

Label	Action	Description/ Example
Search	Search for the required Upload job.	Upload Job name.
Filter	A filter can be added based on the field, and the conditions can be selected from the drop-down box below.	Field: Agent Name, Job Name, Job Status, Status. Conditions: in, not in, equal to, not equal to.
Download Jobs	Click to navigate to the Download Jobs module	Redirects users to the Download Jobs module, where they can view, manage, or track jobs related to downloading configurations or firmware.
Configuration Templates	Click to navigate to the Configuration Template module	Opens the Configuration Template module, allowing users to create, edit, or manage predefined templates for configuration uploads.
Job Task	Click to navigate to the Upload Job Task to view more details.	Filter by: Upload Task IP Results, Completed, In-Progress
Export	Click to export the uploaded job file.	Upload Job data can be exported in an XLS file.
Add	Click to add an Upload job in the NCCM tool.	Users can create a new upload job by specifying the configuration, device details, and schedule parameters.
Column Details		
Job Name	No actions can be taken.	Displays a unique Name to identify the Job.
Status	Click to change the upload job from an active to an Inactive state or vice-versa.	Active, In-Active.
Agent	Displays the agent name associated with the upload job.	Indicates the name, logo, IP address, and indicator to check the status.

Kafka Status	View-only field, no actions can be taken	Displays the real-time status of Kafka messages associated with the upload job, such as Success, Failed, or NA.
Job Status	No actions can be taken. This displays the status.	<p>Job Status:</p> <ul style="list-style-type: none"> • Waiting For Schedule • Send to Queue in Progress • Added in Send Queue • Agent Received • Agent Execution In Progress • Completed • Requesting OS Image • OS Image Copied to Node Server • OS Image Agent Download In Progress • Waiting For Execution • Waiting For Rerun • Job Closed
Frequency	No actions can be taken. This displays the frequency of the job.	<p>Frequency</p> <ul style="list-style-type: none"> • Execute Now • Execute at • At Every • Weekly • Daily • Monthly
Visibility	View-only field: no actions can be taken	This shows whether the upload job is designated as Private (restricted access) or Public (accessible to authorized users).
Last Action Time	No actions can be taken.	This displays the last action time of the job.
Next Action Time	No actions can be taken.	This displays the next action time of the job.

Action Icons | Upload Jobs

Label	Action	Description/ Example
Edit	Click to make changes to the upload job.	Job Details, Task Details, and Other details can be made.
Delete	Click to make changes to the upload job.	This action will allow users to delete the executed upload job.
View Result	Click to view the executed upload job result.	Refer to the below sections for in-depth details
View Audit	Click to view the executed upload job audit.	Refer to the below sections for in-depth details

Close Job	Click to close the job	Terminates the upload job, marking it as completed or manually stopped by the user.
Reset to Next Schedule	Click to initiate the action	Resets the upload job for execution at the next scheduled time per the defined upload schedule.

View Result | Action Icons

After clicking the 'View Result' option, a pop-up window will appear displaying details such as Timestamp, Job Name, Task Name, Vendor, Template Name, Task Owner, Device Account, Created By, Task Status, Task End Time, Next Retry Action, Retry Count, and Retry Status.

Please refer to the table below for additional details:

Label	Action	Description/ Example
Search	Search for the required Upload job results based on timestamp, Job name, etc.	Job Name and Task name.
Filter	A filter can be added based on the field, and the conditions can be selected from the drop-down box below.	Field: Task Name, Vendor, Template Name, Task Owner, Device Account, Task Status, and respective conditions can be made.
Sort By	Sort the result window based on respected criteria from the drop-down box.	Current hour, Last 60 minutes, Last hour, 3 Hours, etc.
Stop Auto Reload	Click to stop the reloading of the page	Disable the automatic page refresh, which occurs by default after every selected time interval.
Export	Click to export the uploaded job result file.	Upload Job Result data can be exported in an XLS file.
View IP Details	Click to view the IP details tab.	Refer to the section below for more details.
Re-Run all Devices	Click to perform the necessary action.	This will Re-execute the selected Task. Task Re-run will be executed for all the devices.
Re-Run Failed Devices	Click to perform the necessary action.	This will Re-Run the tasks only for failed devices.

View IP Details | View Result

After clicking the 'View IP Details' option, a pop-up window will appear displaying details such as Timestamp, IP Address, Vendor, Model, Serial Number, Task Owner, Device Account, Execution Identifier, Task Status, Task Started, Task Ended, and Error Message.

Label	Action	Description/ Example
Search	Search for the required IP details based on timestamp, Job name, etc.	Examples: IP Address
Filter	A filter can be added based on the field, and the conditions can be selected from the drop-down box below.	Field: Vendor, Execution Identifier, IP Address, Task Owner, Device Account, Task Status, and respective conditions can be made.
Sort By	Sort the result window based on respected criteria from the drop-down box.	Current hour, Last 60 minutes, Last hour, 3 Hours, etc.
Stop Auto Reload	Click to stop the reloading of the page	Disable the automatic page refresh, which occurs by default after every selected time interval.
Export	Click to export the uploaded job result file.	Upload Job Result data can be exported in an XLSX file.

Please refer to the below sections for additional details about the Task IP Audits:

Job Execution Trail | View IP Details

View Trails lets you track the history of actions for a job, showing details like changes made, who made them, and when. It's useful for auditing and reviewing the steps taken during job execution.

Upon clicking the corresponding icon, the following details will be available: Upload Job, Configuration Template, IP Address, Vendor, Created By, Executed By, and Result.

The Result tab will display all command information related to the job execution.

Job Execution Result | View IP Details

View results show the outcome of a job after it's completed. It provides details such as the job status (success or failure) and any relevant execution information or errors.

Upon clicking the corresponding icon, the following details will be available: Upload Job, Configuration Template, IP Address, Vendor, Created By, Executed By, and Result.

View Audit | Action Icons

After clicking the 'View Audit' option, a pop-up window displaying details such as Timestamp, Task Name, IP Address, and the respective message will appear.

Please refer to the table below for additional details:

Label	Action	Description/ Example
Search	Search for the required audits based on timestamp, Job name, etc.	Task Name, IP Address, and Message.
Filter	A filter can be added based on the field, and the conditions can be selected from the drop-down box below.	Field: Task Name, Device IP Address, Audit Message, and respective conditions can be made.
Auto Refresh	Click to enable the auto-refresh feature.	This automatically refreshes the Upload Job audits page, providing real-time data updates.
Export	Click to export the uploaded job result file.	Upload Job Result data can be exported in an XLSX file.

Bulk Actions

Bulk action icons enable users to manage multiple upload jobs at once efficiently. Users can perform bulk actions through the pop-up menu by selecting jobs with checkboxes.

Refer to the table below for detailed actions and their functionalities:

Bulk Actions | Action Icons

Label	Action	Description
Enable	Click on the checkbox to enable the multi-selection panel.	This action will initiate the upload job and activate the execution process. Disabled jobs will be activated and executed based on the scheduled time.
Disable	Click on the checkbox to enable the multi-selection panel.	This action will terminate the upload job, deactivate the process, and prevent further execution. Once the upload is disabled, the job will go to a disabled state, which means it won't RUN until enabled.

Add Upload Job

Click the plus icon on the Upload Job page to create a new Upload Job. The 'Add Upload' page includes three additional tabs:

Job Details | Add Upload Jobs

Label	Action	Description / Example
Job Name	Enter the appropriate name for the job.	This name will be used to identify the upload job within the system. Example: "Network Backup Job."
Job Description	Provide a brief description of the upload job.	This description helps users understand the purpose and details of the job. Example: "Backup configuration for all routers."
Type	Select the type of upload job from the drop-down list.	Options include Regular Job and OS Upgrade Job.
Job Execution Window (Mins/Hrs)	Choose the time frame for executing the upload job.	Select the time window in minutes or hours to specify when the job should run. Example: "Execution window: 24 hours."
Notify to	Select users to be notified about the upload job.	Choose the relevant users who should receive notifications about the job's completion or completion from the drop-down list.
Agent	Choose the respective agent from the drop-down list.	The agent refers to the entity responsible for executing the upload job.
Job Status	Toggle the button to enable or disable the job status.	Enable the job status to allow the job to run. If disabled, the job will not execute.
Download Configuration before and after Upload	Turn on this functionality if needed.	This action is used to take a backup of the configuration before the upload job begins, and once the upload is complete, another backup is taken to ensure the updated configuration is saved.

Once the details have been added, click on Next to continue.

Task Details | Add Upload Jobs

Each Job has one or more tasks to be executed in a specific order, as defined. Task is the smallest unit where command execution on Devices is defined. Every task will have its Configuration Template, and the Devices will RUN with Runtime object input.

Each Task supports multiple command executions with multiple parameter substitutions simultaneously for individual location devices. Every task gets Device Credentials from the User when it is created.

Each task requires the following inputs from the User

- Task Name.
- Task Description.
- Vendor
- Configuration Template (Based on the Vendor).
 - View template - used to view the selected template.
 - Task Command(s) - used to view and edit task-related commands.
 - Select Template - used to select the template from the Template(s) collection.

Note: View and Edit template functionalities can be availed only when editing the job.

Note: Configuration template options are enabled based on the applied license. The buttons (View Template & Select Template) will not be visible if the configuration template license is inactive.

- Device group and IP Address and IP Address from CSV - Using the dropdown or IP Address(s) in textbox or IP address from the CSV by using Load IP Address from CSV
 - Configuration profile (Mandatory for null vendor)
 - Configuration protocol (Mandatory for null vendor)
 - Connection Port (Mandatory for null vendor)
 - Device Username
 - Device Password
 - Confirm Password
 - Enable Password
 - Confirm Enable Password
 - Select if Shell must be installed remotely or locally.
 - Update Device credentials using the dropdown menu. (This option is for performing password rotation)
 - Task Enabled/Disabled
 - Task retry count
 - Task retry interval window (mins/hrs)
 - Continue next IP Address on Error
 - Continue the next Command on Error
 - Run after (Previous Task(s) Name)
 - Run only (Previous Task(s) Status)
 - Wait After Previous Task(s) Completion in seconds

Click Add to Add the Task to the Upload Job Execution Queue.

- To Edit the Added Task, select the Task and click Edit
- Select the Task and click Delete to remove the Task from the upload job.
- Clicking ^ on will move the task up.
- Clicking ^ on will move the task down.

Other Details | Add Upload Jobs

Schedule Details | Add Upload Jobs

Click the Schedule Details Tab. Update the information below

- Select the execution schedule option.
 - Once
 - Every
 - Daily
 - Weekly
 - Monthly
- Select the Hours and Minutes from the Execute

Access Control | Add Upload Jobs

Click the Access Control tab.

- Choose the visibility using the Radio button
If visibility is "Private," User and User group dropdown will be enabled.
 - Select User(s) using dropdown.
 - Select Team(s) using dropdown.

If the Upload job is private, only selected users and User groups can view the job.

Note: Fields marked with * are mandatory to add.

Review Job

Click Review to Review the Upload job.

- The review process displays all Tasks, their definitions, and completed details, including commands to execute before saving the job.
- Review results could be exported into PDF.

Click Save to configure the Upload job. Click Cancel to abort the job.

Note:

- If the Upload job has been added by a White-listed user, it will be executed based on the execution time.
- If a Non-White-Listed user has added an Upload job, it will be executed only after the approval process.

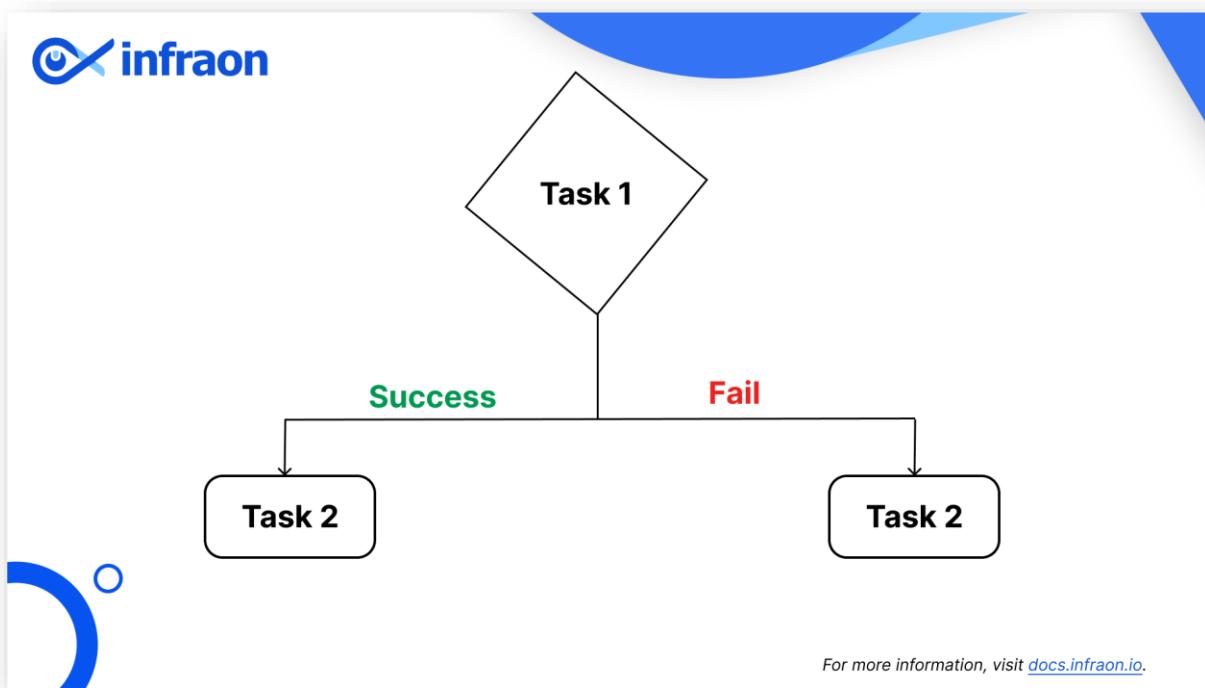
- The task waiting Period will suspend the execution of the next Task until the end of the period, at which point the Task execution resumes.
- If the device(s) vendor is not identified (due to SNMP not being reachable), then the upload Job must be selected with Profile, Protocol, and Port to override download Job null entries.
- If any particular task has failed, the task will execute again based on the Retry count and interval before the dependent task execution.
- If the first task fails, the second task will be executed after completing the whole retry interval of the previous task.
- If a task has multiple IP(s) configured and at the time of execution, if any IP(s) fail, the next retry will happen only for the failed IPs.

Configuring Task Chain or Task Dependency

The upload job supports Task dependencies by associating 'Previous Task's Name' from the previous task name list and the previous execution result status as a condition for the current task to execute.

Three tasks have been configured:

- Task1 - Enabling the BGP
- Task2 - BGP Additional-Paths Select
- Task3 - Start the Interface
 - Task1 is the Parent or Previous Task for the Task2 and Task3.



Upon successful execution of Task 1, Task 2 will be executed (not Task 3).

- If Task1 fails, Task3 will be executed (Task2 will not be executed).

Task 1 Details:

Task 1 has been configured with the below parameters,

Label	Value
Execution Window	2 Hours
Run After	Start
Run if Previous Task	Success
Retry Count	1
Retry Interval	2 Hours

- Task 1 should be executed within 2 hours of initiating it.
- If Task 1 fails during execution, it will retry the same task one more time in 2-hour intervals.
- If the input for the “Run After” field is given as ‘Start’, there is no dependency on the previous task.

Task 2 Details:

Task 2 has been configured with the below parameters.

Label	Value
Execution Window	15 minutes
Run After	Task1
Run if Previous Task	Success
Retry Count	3
Retry Interval	15 Minutes

- Task 2 should be executed within 15 minutes of starting the execution.
- Run After is “Task1” and Run if Previous Task is “Success,” which means “Task2” is dependent on “Task1” and will only be executed if “Task1” has been successfully executed.
- If Task 2 fails during execution, it will retry the same task three times within 15-minute intervals.

Task 3 Details:

Task 3 has been configured with the below parameters.

Label	Value
Execution Window	2 Hours
Run After	Task1
Run if the Previous Task	Fail
Retry Count	2
Retry Interval	30 Minutes

- Task 3 should be executed within 2 hours of starting the execution.

- Run After is “Task1” and Run if Previous Task is “Fail,” which means “Task3” is dependent on “Task1”; if “Task1” fails, only then will “Task3” get executed.
- If Task 3 fails during execution, it will retry the same task three times within 30-minute intervals.

Note: Users will only receive notifications upon the completion of the upload job.

Edit Upload Job

To edit an upload job, select an existing job, click on Edit, and Follow the same procedure as ‘Add job’ to edit.

Note:

- Job re-run cannot be in the In-progress state.
- Once the job execution has been completed, we can Re-run the same job.
- Re-run options are only available if the job is enabled or completed.

Job Re-RUN

This will trigger the job to re-execute the same job. However, users cannot re-run a job if any associated tasks are currently in progress or if the job is disabled.

terminating sessions when necessary.

Service Template

One or more configuration templates can be configured to create a service template, which is used to fulfill services within NCCM.

This is a privilege-based feature: The user can access, view, add, edit, delete, execute, and export only if the administrator has given them privileges. This will be defined under roles and privileges.

Services are specific to organizations based on the types of services offered. Since service templates are usually a combination of multiple tasks needed to fulfill a service, NCCM does not have default service templates.

Administrators create Service Templates that operators can use.

In **network devices**, a **Service** refers to a specific function or capability that the device provides, such as monitoring, logging, authentication, or automated configuration changes.

In NCCM's Service Template, a **service** defines a structured approach to executing predefined tasks on multiple network devices. It standardizes configurations, updates, and other operations to ensure consistency and efficiency.

Examples:

- **Backup Configuration Service** – Periodically saves the current configuration of a device.
- **Firmware Upgrade Service** – Automates the upgrade of the OS or firmware on multiple devices.
- **Compliance Check Service** – Ensures that configurations align with security and operational policies.

What do you see on the screen

The **Service Template** page displays a list of predefined templates available in the NCCM network.

Basic Details | Service Template

Label	Action	Description/Example
Search	Search for the required template.	Service Template name.
Filter	A filter can be added based on the field, and the conditions can be selected from the drop-down box below.	Field: Description and Service Name. Conditions: in, not in, equal to, not equal to.
Export as JSON	Click to export the selected template(s) in JSON format.	Useful for backup, sharing, or importing templates into another system.
Add	Choose from three options: Import JSON , Import Text , or Manually .	Allows users to create a new service template using different input methods. Import JSON and Text help in importing the content from the older setup
Service Name	View-only field. No actions can be taken.	Displays the name of the service template.
Description	View-only field. No actions can be taken.	Provides details about the purpose of the service template.
Status	Click to toggle between ON/OFF .	Indicates whether the template is Public (accessible to all) or Private (restricted access).
Associated Configured Templates	View-only field. No actions can be taken.	Displays linked configuration templates, e.g., Enable SNMP on Linux devices .

Visibility	View-only field. No actions can be taken.	Indicates whether the template is Public or Private .
Created By	View-only field. No actions can be taken.	Shows the username of the individual who created the template.
Modified By	View-only field. No actions can be taken.	Displays the username of the last person who modified the template.
Action Icons		
Edit	Select an existing template and click Edit .	Allows modifications to all fields except Template Type .
Clone	Click Clone to duplicate an existing template.	Opens a copy of the selected template for minor modifications. After making changes, click Save to create a new template.
Delete	Select one or multiple templates and click Delete .	Permanently removes the selected template(s) from the system.
Add Upload Job	Click to use the template as an Upload Job .	Initiates service execution by redirecting users to the Add Service Job page. See the Add Service Job section for details.

Note:

Users can perform bulk actions by selecting the checkbox next to each service template. Once selected, they can:

- **Enable:** Activates the selected template(s), making them available for use. Only active templates can be assigned as an Upload Job.
- **Disable:** This option deactivates the selected template(s), preventing them from being used in an Upload Job.
- **Delete:** Removes the selected template(s) from the system permanently.

Add Service Template

To create a new service template in the inventory, click the **Add** button located at the top right corner of the page.

There are three ways to add a service template:

- Upload a pre-configured JSON file.
- Paste the template content in text format.
- Manually configure the template details.

Refer to the table below for detailed input fields:

Service Details | Add Service Template

Label	Action	Description/Example
Service Name*	Enter a unique name for the service template.	Example: Network Backup
Description*	Provide a brief description of the template.	Example: Backup configuration for Cisco routers.
Status	Toggle ON/OFF to activate or deactivate the template.	ON: Active, OFF: Inactive
Visibility	Select the visibility setting.	Private: Restricted access Public: Available for all users

Once all details are entered, click **Submit** to save the template or **Next** to proceed with additional configurations.

Note: Fields marked with * are mandatory.

Template Details | Add Service Template

Label	Action	Description/Example
Task Name*	Enter a unique name for the task.	Example: Device Config Backup
Template Selection		
Vendor*	Choose a vendor from the dropdown list.	Example: Cisco, Juniper
Configuration Template*	Select a configuration template from the list.	Example: Router Backup Script
Task Execution Details		
Shell*	Choose the execution method.	Shell or Remote
Task Retry Count*	Set the number of retry attempts (0-10).	Example: 3
Task Retry Interval Window (Min/Hrs)*	Set the interval between retries.	Example: 1 minute, 5 minutes
Task Status	Toggle ON/OFF to activate or deactivate.	ON: Active, OFF: Inactive
Continue to Next IP on Error	Toggle ON/OFF to continue execution on failure.	ON: Enabled, OFF: Disabled
Continue to Next Command on Error	Toggle ON/OFF to continue execution on failure.	ON: Enabled, OFF: Disabled
Task Dependency Details		
Run After (Previous Task(s))*	Select a preceding task.	Example: Start
Run Only if (Previous Task(s) Status)*	Choose a dependency condition.	Failed, Success, Any
Wait After Previous Task(s) Completion	Set a delay before execution.	Example: 2 minutes, 5 minutes

Once all configurations are completed, click **Submit** to save the Service Template.

Note: Fields marked with * are mandatory.

Service Job

A Service Job is an execution instance of a Service Template. It allows users to select devices, define tasks, and schedule service execution. Service Jobs can be created in two ways:

1. **From the Service Template page** – use the "Add to Upload Job" option.
2. **From the Upload Job page** – select an existing Service Template.

Add Service Job

The service Job (Add Job) page is used to select devices, define tasks (select devices for specific tasks), and set a schedule for service execution.

When adding a service job from the Upload Job page, the service template must be selected before the device is selected.

Job Details | Add Service Details

Label	Action	Description/ Example
Job Name*	Enter a unique name for the Service Job.	The name should be descriptive enough to identify the job's purpose. Example: "Firmware Upgrade – Core Switches"
Description*	Provide a summary of what the Service Job does.	Clearly explain the job's purpose and impact. Example: "This job upgrades firmware on all core switches to version 2.0 for security compliance."
Service Template*	Select the relevant Service Template from the drop-down list.	The selected template defines the execution steps. Example: "Compliance Check – Routers"
Job Type*	Choose the job type from the drop-down list.	Options: Regular Job, Configuration Rollback Job, OS Rollback Job, OS Upgrade Job, OS Upgrade for Vulnerability.
Notifier	Select recipients who should be notified about the job.	Notifications ensure that relevant stakeholders are informed. Example: "Network Admins, Security Engineers"
Agent*	Choose the appropriate agent responsible for executing the job.	The agent acts as the execution engine for the job. Example: "Infraon_NCCM_Agent_1"
Job Status	Toggle the switch ON/OFF to enable	Note: The job must be enabled for execution. Example: "ON (Enabled)"

	or disable job execution.	
Download Configuration Before & After Upload	Toggle the switch ON/OFF based on requirement.	If enabled, it captures device configurations before and after the job runs for auditing purposes. Example: "ON (Configuration snapshots taken before and after execution)"
Device Selection		
IP Address	Select an IP address from the drop-down list.	Choose the device(s) to which the service will be applied. Example: "192.168.1.10"
Asset Tags	Select tags to filter and categorize devices.	Asset tags help identify and group devices. Example: Switches, Firewalls, Routers
Load IP Address from CSV	Click Download Sample CSV , fill in IP addresses, and upload using Import from CSV .	Use this option to add multiple devices at once. Example: "Upload a CSV with 100+ device IPs."
Device Account		
Username	Enter the username required for device authentication.	The username should have sufficient privileges to execute the service. Example: "admin"
Password	Enter the device access password.	The password is required for login. Example: " (Hidden for security reasons) "
Enable Password	Enter the enable password for privileged mode access.	This is needed to execute privileged commands on the device. Example: "cisco_enable_123"

Once done, click on **Next** to Add Task details.

Task Details | Add Service Job

Task details are updated as per the selected service template.

Device details can be changed for individual tasks to suit the requirement. Multiple devices can be selected.

- Select Configuration Profile using the dropdown menu.
- Select Connection Protocol using the dropdown menu.
- Select Connection Protocol using the dropdown menu.
- Select device credentials accordingly.

Click **Next** to continue.

Schedule Details | Add Service Job

Label	Action	Description/ Example
Execute Now	Click to select the Run Immediately option.	The service job will be created and executed instantly upon submission.
Schedule Now	Click to choose a scheduling mode: once, every, Daily, Weekly, or Monthly, and then specify the execution time.	The service job will be created immediately, but execution will occur per the selected schedule.
Visibility	Select either Private or Public .	Private: The job is accessible only to the creator. Public: The job is visible to other authorized users.

Once done, click **Submit** to add the service job, or click **Request** to proceed with additional approvals.

Authentication Profile

The Authentication Profile module manages user authentication for accessing network devices via CLI (Command Line Interface) sessions. It ensures that only authorized users can establish CLI sessions with network devices by verifying their identity before granting access.

This is a **privilege-based feature**: Users can only view, add, edit, delete, execute, or export authentication profiles if they have the necessary permissions assigned by the administrator.

What do you see on the screen

Basic Details | Authentication Profile

Label	Action	Description/Example
Search	Enter keywords to search for a specific profile.	Example: "Admin Profile"
Filter	Apply filters based on predefined fields and conditions.	Fields: Profile Name, Status, User Tag, Asset Tag, Device IP Address, Device Credential. Conditions: In, Not In, Equal To, Not Equal To.
CLI Jobs	Click to navigate to the CLI Jobs module.	CLI Jobs establish direct CLI sessions (SSH or Telnet) between a device and a user via the NCCM application, allowing users to execute commands similar to PuTTY .
Add	Click to create a new Authentication Profile .	Example: Add a profile for network administrators with specific device access.
Profile Name	View-only field.	A unique identifier for the authentication profile is used to

		distinguish different access configurations. Example: "Admin-Access"
IP Address	View-only field.	The IP address of the network device associated with this profile. Example: "192.168.1.1"
Asset Tag	View-only field.	A unique tag is assigned to a device for tracking and identification within the inventory. Example: "Router-001"
User Name(s)	View-only field.	The list of users associated with the profile authorized to access the device. Example: "admin, user1"
Device Credential	View-only field.	The authentication method used for accessing the device, such as SSH keys, passwords, or certificates. Example: "SSH Key - Admin"
Protocol	View-only field.	The communication protocol used for CLI access. Supported options include SSH and Telnet. Example: "SSH" or "Telnet"
Description	View-only field.	A brief note explaining the purpose or function of the profile. Example: "Admin profile for core routers."
Status	View-only field.	Indicates whether the profile is active or inactive. Example: "Active" or "Inactive"
Visibility	View-only field.	Defines whether the profile is Public (accessible to all authorized users) or Private (restricted access). Example: "Public" or "Private"
Action Icons		
Edit	Select a profile, make necessary modifications, and save changes.	Editing follows the same procedure as the Add operation.
Clone	Duplicate an existing profile with minor modifications.	Select a profile and click Clone . The Add Authentication Profile page appears with pre-filled details—modify as needed and save.

Delete	Remove a selected authentication profile.	Example: Delete an obsolete profile no longer in use.
Detail View	Open a pop-up with detailed profile information.	Displays User Name(s), Email, Profile Name, IP Address, and Status.
Bulk Actions		
Enable	Select multiple profiles and enable them in bulk.	Enabled profiles will be marked as Active .
Disable	Select multiple profiles and disable them in bulk.	Disabled profiles will be marked as Inactive .
Delete	Remove multiple authentication profiles at once.	Example: Bulk-delete outdated or unnecessary profiles.

Add Authentication Profile

To add a new authentication profile, click on the **Add** option located at the top right corner of the page. Fill in the required details as outlined in the table below:

Add Details | Authentication Profile

Label	Action	Description/Example
Profile Name*	Enter a unique name for the authentication profile.	Example: "Admin-Access"
Description*	Provide a brief description of the authentication profile.	Example: "Admin profile for critical network devices."
Status	Toggle between ON (Active) or OFF (Inactive) to enable or disable the profile.	Default: "ON"
IP Address	Enter the device management IP address. Accepts a single IP or a list of IPs separated by commas, semicolons, or spaces.	Example: "192.168.1.1; 192.168.1.2, 192.168.1.3"
	Alternatively, import IP addresses from a CSV file. Click the Download icon to get a sample CSV template.	Example CSV: "Device Name, IP Address"
Asset Tag	Select from the drop-down.	Choose the appropriate asset tags for device grouping. Example: "Router-001, Switch-002"
User	Select a user from the drop-down list.	Example: "admin, user1"

User Tag	Select a predefined user group from the drop-down list.	Example: "Network Admins, IT Support"
Protocol	Select the access protocol from the drop-down.	Options: "SSH, TELNET"
Device Credential	Select the appropriate credential method for authentication.	Example: "SSH Key - Admin, Password Auth"
Visibility	Choose profile visibility.	Public (accessible to authorized users) or Private (restricted access).

Note:

- You can add devices using either **IP Address** or **Asset Tag**.
- You can select **individual users** or assign a **User Tag** to group users under a common profile.

Once all details are entered, click **Submit** to save and add the authentication profile to the inventory.

Authorization Profile

The Authorization Profile module defines user access levels and permissions for interacting with network devices. It ensures that only authorized users can execute specific commands or modify configurations.

What do you see on the screen

Basic Details | Authorization Profile

Label	Action	Description/Example
Search	Enter at least three characters to search for an existing profile.	Example: "Admin" will return "Admin_Profile1, Admin_Profile2"
Filter	Apply filters based on predefined fields and conditions.	Fields: "Profile Name, Default Action, Status, Asset Tag" Conditions: "In, Not In, Equal To, Not Equal To"
CLI Jobs	Click to navigate to the CLI Jobs module.	The CLI Jobs module manages direct CLI sessions (SSH/Telnet) between a device and a user through the NCCM application.
Default Authorization Profile	View the system-defined default authorization profile.	This profile applies default access policies when no specific profile is assigned.

Add	Click to create a new authorization profile.	Opens the Add Authorization Profile page.
Profile Name	No actions; view-only.	Displays the unique profile name. Example: "Network_Admins_Profile"
Status	No actions; view-only.	Displays whether the profile is Active (ON) or Inactive (OFF) .
IP Address	No actions; view-only.	Displays the associated device management IP addresses. Example: "192.168.1.10"
Asset Tag	No actions; view-only.	Displays the assigned asset tags for this profile. Example: "Switches, Firewalls"
User Name(s)	No actions; view-only.	Displays users assigned to this profile. Example: "John Doe, Jane Smith"
User Tag	No actions; view-only.	Displays user groups assigned to this profile. Example: "Network Engineers"
Default Action	No actions; view-only.	Displays the default permission for users:
Deny Commands	Click to view commands added.	Lists commands that users in this profile cannot execute. Example: "shutdown, reload"
Permit Commands	Click to view commands added.	Lists commands that users in this profile are allowed to execute. Example: "show running-config, ping"
System Commands	Click to view commands added.	Displays system-defined commands available to the profile. Example: "exit, logout"
Description	No actions; view-only.	Provides a brief description of the authorization profile. Example: "Admin access to core routers"
Visibility	No actions; view-only.	Indicates if the profile is Public (shared) or Private (restricted).
Action Icons		
Edit	Select a profile and click Edit to modify it.	Users can update profile settings such as commands, visibility, user tags, etc.
Clone	Duplicate an existing profile with minimal modifications.	Clicking Clone will open a new profile with pre-filled details from the selected profile.
Delete	Remove an existing profile.	Select a profile and click Delete to permanently remove it.
Detail View	View detailed information about the profile in a pop-up window.	Displays users, profile names, IP addresses, and status in an expanded view.
Bulk Actions		

Enable	Select multiple profiles and enable them in bulk.	Enabled profiles will be marked as Active .
Disable	Select multiple profiles and disable them in bulk.	Disabled profiles will be marked as Inactive .
Delete	Remove multiple authentication profiles at once.	Example: Bulk-delete outdated or unnecessary profiles.

Add Authorization Profile

To add a new authorization profile, click on the **Add** option located at the top right corner of the page. Fill in the required details as outlined in the table below:

Profile Details | Add Authorization Profile

Label	Action	Description / Example
Profile Name*	Enter a unique name for the authorization profile.	Example: Admin_Access, Read_Only_Profile
Profile Description*	Provide a brief description of the authorization profile.	Example: "Allows full configuration access for admin users."
Status	Toggle the switch to enable or disable the profile.	ON (Active) / OFF (Inactive)
Select from Authentication Profile	Choose an existing authentication profile from the drop-down list.	Example: TACACS_Auth, RADIUS_Auth
IP Address	Enter a single device management IP or a list of device management IPs separated by a comma, semicolon, or space.	Example: 192.168.1.1; 192.168.1.2
	Click the CSV Import icon to upload multiple IP addresses.	Download the sample CSV template before uploading.
Asset Tag	Select relevant asset tags from the drop-down list.	Example: Switches, Firewalls, Routers
User	Select a user from the drop-down list.	Example: John Doe, Alice Smith
User Tag	Select a user group or predefined tag from the drop-down list.	Example: Network Engineers, Operators
Visibility	Choose between Public or Private access.	Public : Accessible to all authorized users. Private : Restricted to specific users.

Note:

- You can add devices using either **IP Address** or **Asset Tag**.
- You can select **individual users** or assign a **User Tag** to group users under a common profile.

Once all details are entered, click **Next** to save and add SSH and TELNET details.

SSH and TELNET Details | Add Authorization Profile Details

In this tab, users must select templates and configure command settings.

Label	Action	Description/ Example
Record CLI Session	Click to turn ON/OFF the toggle button.	If enabled, the system tracks all activities performed in the terminal and keeps a record. These logs can be accessed from the CLI Job/ Sessions page.
Block Up/ Down keys	Click to turn ON/OFF the toggle button.	Prevents users from navigating through previous commands.
Block Horizontal TAB key	Click to turn ON/OFF the toggle button.	Restricts the use of the TAB key in the CLI session.
Default Action	Select from Block, Terminate, and Notify .	Defines the action for unrecognized commands. If a command isn't explicitly defined under Terminate, Block, Notify, Permit, or System , the selected default action will apply.

Infraon NCCM allows defining five types of command input rules:

Five types of command input options can be defined in an Authorization Profile. They are:

- **Terminate Commands** - Command (sets) denied for execution by the User/User Group. When a user tries these set(s) of commands, Infraon NCCM terminates the CLI Session immediately.

```
Warning: Permanently added '10.0.4.88' (ED25519) to the list of known hosts.
Warning: Permanently added '10.0.4.88' (ECDSA) to the list of known hosts.
root@10.0.4.88's password:
Last login: Thu Apr  3 17:16:11 2025 from 10.0.4.130
[root@test ~]# ls *****Terminating-session-due-to-UnAuthorized-command-[ls]-identified*****
```

- **Block Commands** - Command (sets) denied for execution by the User/User Group. When a user tries these set(s) of commands, Infraon NCCM blocks them from being executed. The CLI session is not terminated here.

```

Warning: Permanently added '10.0.4.88' (ED25519) to the list of known hosts.
Warning: Permanently added '10.0.4.88' (ECDSA) to the list of known hosts.
root@10.0.4.88's password:
Last login: Thu Apr  3 17:16:26 2025 from 10.0.4.88
[root@test ~]# *****UnAuthorized-command-identified*****
-bash: *****UnAuthorized-command-identified*****: command not found
[root@test ~]# █

```

- Notify Commands** - When a user tries these set(s) of commands, Infraon NCCM executes them and triggers a notification about the action. If this option is selected, Notifier (Notification Alert) must be selected using the dropdown menu.

Immediate:

```

Warning: Permanently added '10.0.4.88' (ED25519) to the list of known hosts.
Warning: Permanently added '10.0.4.88' (ECDSA) to the list of known hosts.
root@10.0.4.88's password:
Last login: Thu Apr  3 17:23:49 2025 from 10.0.4.88
[root@test ~]# ll
total 9143384
-rw----- 1 root root      1027 Apr  4  2012 anaconda-ks.cfg
-rw-r--r-- 1 root root 252691012 Dec  5 15:23 asr920-universalk9_npe.03.13.00.5.154-3.5-ext.bin
-rw-r--r-- 1 root root 6442459944 Jan 28 14:21 emptyfile.bin
-rw-r--r-- 1 root root 1073741824 Jan 28 14:30 emptyfile.img
-rw-r--r-- 1 root root 1073741824 Jan 28 14:30 emptyfile.zip
-rw-r--r-- 1 root root 35288273 Jun 12 2024 infraonagent_airtel.zip
drwxr-xr-x 20 root root    4896 May 31 2024 Infraon-Branch_DevBeta
-rw-r--r-- 1 root root 484890497 May 31 2024 Infraon-Branch_DevBeta.zip
drwxr-xr-x  3 root root     23 Jul 15 2024 media
-rw-r--r-- 1 root root      0 Nov 29 10:36 nccm_connection_cache.db
-rw-r--r-- 1 root root      0 Jan 27 16:38 ssh_22
-rw-r--r-- 1 root root    942 Mar 21 12:32 test.py
[root@test ~]# █

```

Command Authorization Notify for : 10.0.4.88 by dhivagar

Dear User,

Sensitive Command [ll] is executed by [dhivagar] on device [10.0.4.88] on Thu Apr 03 2025 17:19:03 GMT+0530 (India Standard Time)
Please find more details about the device

IP Address	10.0.4.88
Hostname	new-trigger
Vendor	VMware Inc.
Series	x86_64
Model	VMware Virtual Platform
Operating System	Oracle Linux Server
OS Version	8.3
Location	Head Office
City	Pochampalli
Region	south
State	Tamil Nadu

This E-mail and any attachments are private, intended solely for the use of the addressee. If you are not the intended recipient, they have been sent to you in error; any use of information in them is

Close:

```

Warning: Permanently added '10.0.4.88' (ED25519) to the list of known hosts.
Warning: Permanently added '10.0.4.88' (ECDSA) to the list of known hosts.
root@10.0.4.88's password:
Last login: Thu Apr  3 17:23:49 2025 from 10.0.4.88
[root@test ~]# ll
total 9143384
-rw-----. 1 root root 1027 Apr  4 2012 anaconda-ks.cfg
-rw-r--r--. 1 root root 252691012 Dec  5 15:23 asr920-universalk9_npe.03.13.00.S.154-3.S-ext.bin
-rw-r--r--. 1 root root 6442458944 Jan 28 14:21 emptyfile.bin
-rw-r--r--. 1 root root 1073741824 Jan 28 14:30 emptyfile.img
-rw-r--r--. 1 root root 1073741824 Jan 28 14:30 emptyfile.zip
drwxr-xn-x. 20 root root 4096 May 31 2024 Infraon-Branch_DevBeta
-rw-r--r--. 1 root root 35288273 Jun 12 2024 infraonagent_airtel.zip
drwxr-xr-x. 20 root root 4096 May 31 2024 Infraon-Branch_DevBeta.zip
drwxr-xr-x. 3 root root 23 Jul 15 2024 media
-rw-r--r--. 1 root root 0 Nov 29 10:36 nccm_connection_cache.db
-rw-r--r--. 1 root root 0 Jan 27 16:38 ssh_22
-rw-r--r--. 1 root root 942 Mar 21 12:32 test.py
[root@test ~]# ll
total 9143384
-rw-----. 1 root root 1027 Apr  4 2012 anaconda-ks.cfg
-rw-r--r--. 1 root root 252691012 Dec  5 15:23 asr920-universalk9_npe.03.13.00.S.154-3.S-ext.bin
-rw-r--r--. 1 root root 6442458944 Jan 28 14:21 emptyfile.bin
-rw-r--r--. 1 root root 1073741824 Jan 28 14:30 emptyfile.img
-rw-r--r--. 1 root root 1073741824 Jan 28 14:30 emptyfile.zip
-rw-r--r--. 1 root root 35288273 Jun 12 2024 infraonagent_airtel.zip
drwxr-xn-x. 20 root root 4096 May 31 2024 Infraon-Branch_DevBeta
-rw-r--r--. 1 root root 484890497 May 31 2024 Infraon-Branch_DevBeta.zip
drwxr-xr-x. 3 root root 23 Jul 15 2024 media
-rw-r--r--. 1 root root 0 Nov 29 10:36 nccm_connection_cache.db
-rw-r--r--. 1 root root 0 Jan 27 16:38 ssh_22
-rw-r--r--. 1 root root 942 Mar 21 12:32 test.py
[root@test ~]#

```

Command Authorization Notify for : 10.0.4.88 by dhivagar

Dear User,

Please find the below sensitive command(s) executed by **dhivagar** on the device **10.0.4.88**

Time	Command
Thu Apr 03 2025 17:23:52 GMT+0530 (India Standard Time)	
Thu Apr 03 2025 17:23:55 GMT+0530 (India Standard Time)	

Please find more details about the device

IP Address	10.0.4.88
Hostname	new-trigger
Vendor	VMware Inc.
Series	x86_64
Model	VMware Virtual Platform
Operating System	Oracle Linux Server
OS Version	8.3
Location	Head Office
City	Pochampalli
Region	south
State	Tamil Nadu

This E-mail and any attachments are private, intended solely for the use of the address. If you are not the intended recipient, they have been sent to you in error; any use of information in them is strictly prohibited.

- Permit Commands** – Command (sets) permitted for execution by the User/User Group. Commands not added in the ‘Permit’ section will be blocked during execution.
- System Commands** – Used to ignore inputs like password and other User credential input. For example, when a user tries to execute a command that requires authentication by the system, the system prompts the user to provide additional information. In this case, a system prompt must be added in the ‘Ignore’ section. If not, the system runs the command through the Permit command list and may end up blocking the command/command set.

Label	Action	Description/ Example
Notification Alert	Select from the drop-down list.	Choose users who will receive notifications.
Notification Type	Select from Immediate or Session Close.	Immediate: Real-time command execution alerts. Session Close: Alerts are triggered when the session is terminated.

Once all details are entered, click **Submit** to save and add the authorization profile to the inventory.

Thresholds

Infraon allows users to define health indexes for monitoring the network's performance. Thresholds play an essential role in tracking the fault and performance of devices and detecting faults and performance-based alerts. These faults and performance are indicated using severity levels as follows:

- **Critical**: Indicated in Red
- **Major**: Indicated in Orange
- **Minor**: Indicated in Yellow
- **Informational**: Indicated in Green

Furthermore, there are two state-based indicators which are:

- **Unknown/Dependent**: Indicated in Blue – when the parent/primary device is down, the dependent/Child device's status is unknown.
- **Under Maintenance**: Indicated in Grey – When a device/node is placed under maintenance for a planned outage.

Thresholds can be defined for any monitoring KPIs (Key Performance Indicators). Infraon is configured with built-in thresholds (global) for all the monitoring nodes and their components. Based on these thresholds, users can quickly spot resources that require attention even before thresholds are breached.

Default threshold configuration covers important indicators like:

- CPU Utilization
- Memory Utilization
- Disk Utilization
- Latency
- Packet Loss
- Network Bandwidth Utilization
- BGP Status
- Error Rate
- Discard Rate

- Process CPU Usage
- Process Memory Usage

Infraon offers multiple threshold configurations where the administrator can configure threshold settings for a specific resource or as a group. Infraon allows the user to define the following:

- Set Point
- Reset Point
- Set Message
- Reset Message
- Set Alarm Hold Time
- Reset Alarm Hold Time
- Severity

Alarm Condition Logic

For the positive polarity parameters:

If the Current Value is > Set Point, the node/device gets into an alarm state and continues to be in an alarm state until the value <= Reset Point.

For the negative polarity parameters:

If the Current Value is < Set Point, the node/device gets into an alarm state and continues to be in an alarm state until the value >= Reset Point.

In addition to the standard/global thresholds across the network, the Adaptive/Dynamic threshold or baseline helps determine the performance issue of every component within the network based on its performance benchmarks and expectations. It helps eliminate unwanted alerts, thus resulting in focused business operations. Infraon UNMS supports an ML-based algorithm for auto-baselining thresholds for various performance metrics.

Thresholds are mainly for Performance metrics such as Traffic Utilization, Latency, Jitter, CPU Utilization, Memory Utilization, Temperature, etc., Users can define multiple thresholds with different severity levels for a single monitoring parameter. For e.g.,

- CPU Utilization Thresholds can be defined as follows:
- If CPU Utilization > 50%, severity is 'Minor'
- If CPU Utilization > 75%, severity is 'Major'
- If CPU Utilization > 90%, severity is 'Critical'

What you see on the screen

This page displays the list of predefined thresholds on Infraon. We recommend you not make any changes to the default values. However, these values can be edited or deleted using the action icon on each line item. Information display includes:

Label	Description/Example
Category	Denotes categories of the Threshold like Performance, Availability, etc.
Threshold Name	Name of the Threshold parameter like Access Point, Interface, etc.
Statistics	Denotes the statistic applicable for the Threshold, i.e., Device Availability, Overflow Rate, Packet Loss, etc.
Severity	Indicates severity in case of threshold breach (Critical, Major, Minor, Informational).
Alarm Message	Displays the message to be included in the alarm/notification raised.
Set Point	Denotes the configured Threshold point or Set Point.
Status	Displays the status of the selected Threshold. Thresholds can be enabled/disabled using the edit option.
Action	Displays action icons to edit or delete the selected Threshold.

Note: Disabling Thresholds results in non-monitoring of devices for the particular Thresholds. Alarms are not raised for the same.

The Device Credential View can be toggled between card view and list view using the respective icon.

Instructions to 'Add a Threshold'

- Go to Infraon Configuration -> IT Operations-> Threshold
- Click on 'Add' and select 'Protocol' as desired.

There are two tabs on the '[Add Threshold](#)' page. Refer to the table for information.

[Category](#) | Applicable Devices

Few fields vary based on the protocol selected. Refer to the 'Description' column for details.

Label	Action	Description/Example
Threshold Name*	Add a name for the threshold.	Name is usually used as an identifier. E.g., Access Point Availability, CPU Utilization, etc.,

Status	Use the toggle to mark the threshold active/inactive.	Infraon monitors only active thresholds.
Category*	Select the threshold category using the dropdown menu.	Available options are performance, basic, major, and informational.
Statistic*	Select statistics using the dropdown menu.	Multiple options are available.
Severity*	Select severity using the dropdown.	Available options are critical, major, and minor.
Type	Select if the Threshold type is Rising or Falling.	
SetPoint	A setpoint is a baseline for the threshold. Setpoint includes Threshold*, Hold Time, and Breach Count.	Threshold* - Add value for the threshold. Hold Time (Optional) - Add hold time in seconds. An alarm or notification will be raised if and only the threshold value crosses the mentioned hold time. Breach Count (Optional) - Add breach count for the threshold. An alarm or notification will be raised if and only the threshold value crosses the hold time, the mentioned number of times.
Alarm Message	Add a message for the threshold.	This message will be included in the threshold breach alarm/notification.
Reset point	Add a reset point for the threshold. Reset point includes Threshold* and Hold Time.	Threshold* - Add value for the reset point threshold. Hold Time (Optional) -Add hold time in minutes. Denotes the no. of minutes the node has to be equal to or below the Reset point to be reported as within the Threshold Limit.
Clear Message	Add a message for the reset point.	This message will be included in the threshold reset alarm/notification.
Threshold configuration	Customize the asset-level details	Customize the asset-level details in the threshold configuration module and input details like asset ID, IP address, Hostname, and more. This permits configuring thresholds applicable for all selected devices and triggering an

		alert when a threshold breaches.
--	--	----------------------------------

Once all the parameters are defined, click 'Save' to save the credentials or click 'Next' to apply thresholds to a specific device or a set of devices.

Category | [Applicable Devices](#)

Label	Action	Description/Example
Applicable For*	Select if the threshold must be applied for selected nodes or all devices.	Add filter conditions if the 'Selected Nodes' option is selected. The filter includes a condition (informational, minor, major, critical) and a value.

Click 'Submit.' Saved thresholds can be edited or deleted using the respective icons.

Trap Configuration

Used to configure Traps to trigger the Event(s). It's a crucial feature that allows you to fine-tune how automated alerts, called Traps, are generated and sent in response to specific system Events.

These are primarily used to capture or handle events or signals that occur within a system.

Instruction to add a Trap Configuration

Go to Infraon Configuration -> IT Operations -> Trap Configuration and click on the 'New Profile' button.

What you see on the screen

Label	Action	Description/Example
Profile name	Add a name for the credential	Applicable for all protocols. A name is usually used as an identifier.
Description	Add a brief description of the profile	Applicable for all protocols
Trap OID	Add a Trap OID (Object Identifier)	The trap message contains the time, an identifier, and a value.

Status	Select the status of the configuration.	The status of the configuration can be Active or In-Active.
Type	Select the type using the drop-down menu.	
Severity	Select severity using the dropdown.	Available options are critical, major, and minor.
Bind Resource Type		
Resource Varbind		
Alarm Message	Add a message for the configuration.	This message will be included in the trap configuration alarm/notification.
Clear Message	Add a message for the trap configuration.	This message will be included in the trap configuration alarm/notification.

Enter the details and then click "Submit" to proceed.

Infraon Platform

The Infraon Portal acts as the central hub for configuring and managing various aspects of your Infraon ITSM environment. It provides a user-friendly interface to access and manage sub-modules that cater to different administrative tasks.

Account Signup

This module is designed for initial user registration within the Infraon Infinity platform. Administrators can verify their accounts by providing essential details like their email address, name, company name, and mobile number. This information is stored securely within the Infinity data, allowing registered administrators to access and utilize the various functionalities.

CI Rule Configuration

The CI Rule Configuration empowers administrators to automate the way Configuration Items (CIs) are discovered, categorized, and managed in your environment. Here, admins can select and configure specific rules based on different criteria to streamline CI management.

Department Rule:

This rule automates department assignments for your Configuration Items (CIs). With this rule enabled, whenever a department is linked to an asset within the system (mapping can be enabled or disabled), a CI relation is automatically

created. This eliminates the need for manual assignment, ensuring accurate and up-to-date departmental ownership of CIs throughout your IT infrastructure.

Location Rule:

The Location Rule automated location assignment for your Configuration Items (CIs). Similar to the Department rule, admins can enable or disable location mapping on assets. When enabled, this rule automatically creates a CI relation whenever a physical location is linked to an asset. This eliminates manual effort, guarantees CIs are accurately assigned to their corresponding locations within your IT infrastructure and improves organization and location-based reporting.

Requester Rule:

The Requester Rule automates by enabling or disabling requester mapping on assets. Admins can configure this rule to automatically create CI relations whenever a service request or incident is linked to a specific user. This eliminates manual assignment and ensures CIs are associated with the appropriate requester, providing valuable insights into departmental or user-based IT asset usage.

Software Rule:

The Software Rule simplifies CI management by automating the creation of CI relations for discovered software. Admins can turn software mapping on or off on assets within the system. With this rule active, a CI relation is automatically created whenever software is automatically identified or manually linked to an asset. This eliminates manual effort and ensures accurate tracking of software assets associated with specific hardware, improving overall visibility into your IT infrastructure.

User Rule:

The User Rule automates CI relations based on designated technicians or managing users within your ITSM system. By enabling or disabling "manage by/technician" mapping on assets, you can configure this rule to automatically create CI relations. Whenever a specific user is assigned as the technician or manager for an asset, this rule triggers the creation of a CI relation. This eliminates manual assignment, ensuring CIs are linked to the appropriate technicians, which can be crucial for service accountability and troubleshooting workflows.

Infraon URL

Here, administrators can customize the web address (URL) that employees use to access the Infraon Infinity portal. This functionality provides greater flexibility and branding opportunities.

For instance, instead of using a generic URL provided by Infraon, administrators can create a custom URL that reflects your organization's name.

Admins can choose a user-friendly and memorable option, such as "**EverestIMS**" for your full company name or "**EIMS**" for a shorter version.

This customization enhances brand recognition and potentially improves user experience by making the helpdesk URL more easily recognizable to employees.

Login Settings

The Login Settings module provides administrators with granular control over how users authenticate when logging into the Infraon Infinity platform. It goes beyond the default username and password method by offering a variety of authentication options to suit the organization's security preferences.

The following section breaks down the details:

Username & Password (Default):

This is the standard login method for Infraon ITSM, allowing users to access the platform with a registered email address and password combination. It provides a familiar login experience for most users.

Mobile Number & SMS:

This method strengthens login security by incorporating two-factor authentication. Users enter their registered mobile number during login, and a unique SMS verification code (OTP) is sent to their phone. Access is granted only after entering the correct OTP, adding an extra layer of protection against unauthorized login attempts.

Microsoft SSO:

This option leverages the power of Single Sign-On (SSO) for a more convenient and potentially more secure login experience. Users can log in to the Infraon Infinity portal directly using their existing Microsoft credentials, eliminating the need to manage separate passwords for the platform. Relying on Microsoft's robust authentication infrastructure improves user experience and potentially enhances security.

Google SSO:

This login method prioritizes both convenience and security. Users can access the Infraon portal with their existing Google credentials, eliminating the need for separate login details.

Module Prefix Configuration

Customize your language and time zone settings on Infraon.

The module offers a centralized location for administrators to manage various user experiences and formatting settings for different modules within the Infraon Infinity platform.

Here's a breakdown of the key functionalities:

Language and Time Zone:

Admins can define the default language and time zone for the entire platform, ensuring a consistent user experience.

Timeout:

Set the duration of user inactivity before automatic session lockout to enhance security and prevent unauthorized access to open sessions.

Module Formatting:

This powerful feature allows for customization of how specific data is formatted within various Infraon modules. For example, admins can define prefixes for modules like Tickets, Assets, Requests, etc. These prefixes will be displayed instead of the actual names within the portal, potentially improving organization and clarity for users.

Additionally, formatting options for these modules can be configured, providing granular control over how information is presented.

The following section breaks down the details:

For instance, admins can configure these formatting preferences

- Ticket
 - Prefix
 - Resolve ticket will close automatically in (1,2,3,...) days
 - Select a filter for aging time calculation (Resolved, Closed)
- Asset
 - Prefix
- Request
 - Prefix
 - Resolve ticket will close automatically in (1,2,3,...) days
 - Select a filter for aging time calculation (Resolved, Closed)
- Change
 - Prefix
- Problems
 - Select a filter for aging time calculation (Resolved, Closed)
- Releases

- Prefix
- Risks
 - Prefix
- Tasks
 - Prefix
- Knowledge Base
 - Prefix

Once the changes are made to satisfactory, click "**Save**" to proceed.

Rebrand Infraon

The Rebrand Infraon module within the Infraon Portal allows administrators to customize the platform's appearance to align with the organization's branding. This fosters a more cohesive user experience and strengthens brand recognition.

Here's how it works:

Logo Upload:

Upload your organization's logo to be displayed prominently within the Infraon Infinity platform. To ensure optimal display, the recommended size (170x96 px) and supported file formats (jpeg, png) are provided.

Color Theme Selection:

Admins can choose from pre-defined color themes (Fixed or Spaced Out) and light, dark, or semi-dark variations to match your organization's branding preferences.

Granular Color Control:

For even greater customization, administrators can define specific colors for elements like the logo container, navbar, and user interface text. This allows for a highly tailored look and feel.

Language Selection:

Admins can select the preferred language (English or Hindi) for the entire platform interface, ensuring user comfort and efficient interaction with the ITSM system.

Once the changes are made to satisfactory, click "**Save**" to proceed.

Template Configuration

The Template Configuration module allows administrators to manage and customize various pre-defined templates used throughout the Infraon Infinity platform. This ensures the templates align perfectly with your organization's specific needs and workflows.

Here's a breakdown of the functionality:

Admins can access and edit pre-existing templates for tasks like **Asset Allocation, Deallocation, and Hardware changes**. These templates likely contain predefined content and formatting that streamline these processes.

To modify a template, simply click the "**Edit**" option under the "**Action**" menu. This allows for tailoring existing templates to better fit your organization's requirements.

Note: In addition to editing existing templates, administrators can create entirely new configurations from scratch. This provides maximum flexibility and allows for the creation of custom templates specific to your organization's unique workflows or processes.

Vendor

The Vendor module within Infraon Infinity acts as a centralized hub for managing information about software vendors associated with the organization's IT environment.

What you see on the screen

The main screen displays a comprehensive list of vendors, providing a clear overview of the vendor landscape.

Details | Basic information

Label	Action
Search	Click to search, enabling efficient navigation through the vendor list.
Filter	Filter can be added based on the field (Vendor Name, Status, Location, Web URL, Contact Person, Email ID, and Phone Number) and select the respective condition from the drop-down box below.
Vendor Name	To quickly identify the vendor.
Status	Indicates the vendor's current standing (active, inactive, etc.).
Location	View the vendor's physical location.
Web URL	Access the vendor's website with a single click.

Contact Person	Identify the designated point of contact at the vendor company.
Email ID & Phone Number	Facilitate easy communication with the vendor.
Actions	
Edit	To make changes to the vendor information.
Delete	Click to delete a specific vendor information from the inventory.

Instructions to Add Vendor

- To manage vendor information within the Infraon Infinity portal, navigate to the **Infraon Configuration** section. From there, select "**Infraon Portal**" and then choose the "**Vendor**" module.
- Select the **Add Vendor** option located at the top right corner of the page, and add the below details respectively:
 - Vendor Name
 - Status (Draft, New, and Publish)
 - Vendor Location
 - Web URL
 - Contact Person
 - Email
 - Phone Number
 - Description
- Once the changes are made to satisfactory, click "**Save**" to proceed.

SSP Configuration

The SSP (Self Service Portal) Configuration module, exclusive to Infraon Management Admins, empowers admins to customize the self-service portal (SSP) experience for their end-users.

What you see on the screen

Utilize the toggle buttons for each module to determine which options appear as menu items on the top panel of the SSP portal.

This allows admins to curate the functionalities available to end-users based on your organization's specific needs.

From this central location, admins can control the visibility (by enabling the toggle buttons) of various modules within the SSP (located at the top panel).

The following section breaks down the details:

Home:

Provide a familiar starting point for end-users.

Dashboard:

Customizable dashboards offer quick access to asset summaries and relevant information in a graphical representation (limited to a maximum of 5 reports).

Report:

Empower users with the ability to view pre-defined reports for self-service data analysis (limited to a maximum of 10 reports).

Ticket:

Enable end-users to submit and track their service requests directly through the SSP.

Request:

Allow users to submit and view older requests and requests, such as access requests or catalog items.

Assets:

Provide a view of relevant IT assets associated with the end-user.

Knowledge Base:

Offer a repository of self-help articles and resources for troubleshooting and problem-solving.

Workspace:

Depending on your configuration, admins can manage the visibility of a Workspace module within the SSP.

Log Management

Logging is an integral part of IT infrastructure management and process. Logs are generated from Routers, Switches, firewalls, IDS/IPS, Servers, Databases, and Web Servers across the IT infrastructure. They can be a generic live status of the end system or a detailed log of the running processes.

Log Management, a part of Infraon Infinity, helps in real-time analysis that can be used for security, compliance, audit, and IT operations.

Log Management enables reacting to anomalies based on log events and patterns, which play a crucial role in application troubleshooting, business analytics, marketing insights, resource management, and regulatory compliance.

Access Control

This guide is intended only for Infraon Infinity operators/users with access based on selected roles and privileges assigned by the administrator.

Access depends on the type of license purchased by the portal operator.

Note: *The administrator drafted this document after accessing all the operator/user portal modules.*

Administrators are responsible for adding or editing user roles and privileges to manage logs. Similar to other modules, specific roles will be configured for the Log Management module. The log management system will update These roles and permissions to ensure appropriate access control.

Users can log in with the assigned credentials and perform tasks within the Log Management module based on their privileges and permissions. Access to various features within the module will depend on the Roles and Privileges the administrator enables. (Click here to view the guide on how to add or edit users with specific roles and permissions.)

How does it work?

Log management collects, stores, analyses, and monitors log data generated by systems, applications, and services within an IT infrastructure. This module will be taking logs of assets uploaded to our system.

This module enables users to access network device logs via the Syslog server. For Windows-specific logs, utilize the Winlog beat server. To collect Linux logs, employ the file beat server.

Logs will be saved in the elastic database, and log stash can be used as a pipeline to dump data into it.

Log Management will fetch data from the elastic database and show it in the Infraon interface based on configuration.

Monitoring, documenting, and analyzing system events are crucial components of security intelligence (SI). Regarding compliance, regulations such as PCI have specific mandates relating to audit logs.

Log management software automates many of the processes involved. For example, an event log manager (ELM) tracks organizational IT infrastructure changes. These changes are reflected in audit trails that must be produced for a compliance audit.

Log Management is then configured in the below sub-modules:

[Log Multi-Index](#): Create and manage the multi-indexes that help retrieve data from Elasticsearch.

[Log Search](#): Provide options to quickly search and filter the logs and get information about the field's structure.

[Log Stream](#): Provide a way to visualize and analyze log data in real-time.

[Export Configs](#): Export Configs define how logs are exported, including format, size, and download of the generated log files.

Let's see each one in detail:

Log Multi-Index

The Log Multi-Index feature allows users to configure and manage log indices in a structured way. It creates a unified view of similar indices, enabling efficient storage and retrieval of log data within the system.

Log indices are collections of patterns that link the log management server with the data stored in Elasticsearch. Users can define how the system interprets and displays log data by configuring index patterns. This module allows users to add, edit, or delete indices as needed.

Each index name follows a structured format based on the timestamp, which helps organize logs efficiently.

Example: windows-yyyy.mm.dd

To retrieve logs for the last three days, users can select the relevant index patterns to create a comprehensive multi-index.

Example: windows-2024.09.03, windows-2024.09.04, and windows-2024.09.05

Users can use wildcard patterns to retrieve logs for multiple days or all related indices.

Example: windows* groups all Windows-related indices.

The multi-index generated will include default fields such as:

- host.ip
- host.id
- host.name.

Additionally, users can customize the columns displayed on the log search page for each index to ensure relevant data is easily accessible.

What do you see on the screen?

Refer to the table below for the information shown on the Multi-Index page:

Multi-Index Details | Fields

Label	Action/ Description
Search	Search for the required Index.
Name	Displays the name of the Index created
Spaces	Identify the space associated with the index
Actions	Click to delete an Index from the database
Check Box	Select multiple indices by checking the boxes to perform bulk actions, such as simultaneously deleting them.

Note: Click the up arrow next to the Name field to sort multi-indices in descending order.

Instructions to create Multi-Index

Infraon Infinity requires a Multi-Index to access the Elasticsearch data you want to explore. A data view can point to one or more indices and data streams. For example, a data view can point to your log data from yesterday, or all indices that contain your data.

To add a Log Multi-Index in the log management tool, follow the steps outlined below:

- Navigate to the Log Multi-Index sub-module within the Log Management module under Infraon Configuration.
- Click "Create a multi-index" in the top right corner of the page.
- Provide a name for the Multi-Index.
- Enter an index pattern in the designated field.
 - Infraon Infinity will suggest matching index names, data streams, and aliases.
 - You can view all available sources or limit your view to those targeted by multi-indexes.
- Use wildcards (*) to match multiple sources (e.g., windows* matches windows-2024.09.03, windows-2024.09.04).
- To match multiple specific sources, enter their names separated by commas without spaces (e.g., windows-2024.09.03,windows-2024.09.04).
- Open the Timestamp field dropdown and select the default field to filter your data by time.
- Click "Save Multi-Index" to complete the process.

Log Multi-Index View

Users can access detailed information about the Multi-Index by selecting it. This leads to a dedicated view page that provides comprehensive details and management options for the selected Multi-Index.

Multi-Index View Details | Fields

Label	Actions/ Description	Example
Index Pattern	Displays the index pattern associated with the group.	Linux*
Time Field	Shows the field used for time-based filtering of log data.	@timestamp
Set as Default	Click to make this field at default.	
Delete	Allows users to remove the current Multi-Index. Exercise caution when using this option.	
Edit	Opens the editing interface to modify the Multi-Index settings.	
Search	Provides a search functionality to find specific fields within the Multi-Index.	@version.keyword, agent.ephemeral_id
Field Type	A filter that allows users to select and view fields based on their data type.	Available options include date, text, keyword, _id, _index, _source, boolean, and long.
Schema Type	A filter that allows users to select and view fields based on their data type.	Available options include Index and Runtime.
Refresh	Updates the view to reflect any recent multi-Index changes or associated data.	This refreshes a local multi-index field list.
Add Field	This option will allow users to include additional fields to the Multi-Index for more comprehensive log analysis.	
About Field		
Name	Indicated the name for the field created.	Device Type, _id, _index.
Type	Displays the type associated with the field	Keyword, date, text.
Actions		
Edit	Click to make changes to the field.	
Delete	This will delete the field in the Multi-Index view.	

Instructions to Add a Custom Field

Users can add custom fields to the Multi-Index for more comprehensive log analysis. To create a new field:

- Navigate to the Log Multi-Index View page.
- Locate the "Add Filed" button in the upper right section of the page, adjacent to the refresh option.
- Click this button will open the field creation interface.

In the subsequent dialog, enter the required information for the new field. Refer to the table below for details on each input field:

Create Filed Details | Fields

Label	Action/ Description
Name	Enter a name for the new field
Type	Select the field type from the drop-down menu. Options include: Keyword, Long, Double, Date, IP, Boolean, Geo Point, and Composite
Set Custom Label	(Optional) Create a label to display instead of the field name in Log Search, Maps, Lens, Visualize, and TSVB. This is useful for shortening long field names. Note that queries and filters will still use the original field name
Set Custom Description	(Optional) Add a description for the field. This will be displayed next to the field on the Log Search, Lens, and Data View Management pages
Set Value	(Optional) Set a specific value for the field instead of retrieving it from the field with the same name in _source
Set Format	(Optional) Choose your preferred format for displaying the field's value. Be aware that changing the format can affect the value and may prevent highlighting in Discover

Note: While filling out the form, users can see a preview section adjacent to the input fields. This preview updates in real-time, allowing users to see how their custom field will appear and make adjustments accordingly.

After entering all the required information, click the 'Save' button to finalize and apply your custom field configuration.

Log Search

The Log Search module is a powerful tool designed to help users efficiently navigate and analyze large volumes of structured and unstructured log data. The Log Search feature addresses this challenge by enabling quick and effective searching across extensive log collections, providing results within seconds.

At its core, the Log Search queries and analyzes log data stored in the Elastic database. The module's architecture is built on index-based storage, where logs are structured, grouped, and stored based on index values. This approach allows efficient searching across specific log categories, significantly reducing search times and improving overall performance.

What do you see on the screen?

The log search page presents the data distribution of documents over time. A table lists the fields for each document matching the current multi-index. To narrow down the results, you can apply filters and customize the table to show only the fields you wish to explore.

Log Search Details | Fields

Label	Action/ Description
Top Panel	
Multi-index	Select the type of Multi-index that needs to be present on the Log search page.
Query Menu	The query menu lets you save queries, including text, filters, and time ranges, for reuse across any query bar. For example, after building a query in Log Search with custom inputs, filters, and a time range, you can save it by embedding it in dashboards, creating visualizations, or sharing results via link or CSV. Saved queries also store Log Search settings like selected columns, sort order, and multi-index, making them ideal for adding search results to a dashboard.
Add Filter	Click to add a new filter based on Fields (@timestamp, @version, etc.), operator, and value.
Search	Click to search for particular multi-Index data using your KQL syntax.
Time Range	Easily adjust the time range of your time-based data by using the Calendar icon to select quick, preset, or custom time ranges, with options to refresh data automatically.

	(Refer to the section below for more details)
Refresh	This refreshes a local multi-index field list.
Download	Users can generate a report for the Multi-Index created by clicking on the download section. Once the exported logs are generated in the Logs Export Configs module, they can be downloaded. The report, including the generated logs, will be available in PDF, CSV, and XLS formats.

Adjusting the Time Range

If your index contains time-based events and a time field is configured for the selected multi-index, you can display data within a specific time range. The time range is set to 15 minutes by default, but you can modify it to suit your needs.

- Click the **Calendar** icon located on the top panel.
- Choose from the following options:
 - **Quick select:** Set a time range based on a specific number of seconds, minutes, hours, or other units in the past or future.
 - **Commonly used:** Select a preset time range, such as the last 15 minutes, Today, or Week-to-date.
 - **Recently used date ranges:** Reapply a previously selected time range.
 - **Refresh every:** Set an automatic refresh interval for the data.
- To customize the start and end times, click the bar next to the time filter. In the popup, choose between **Absolute**, **Relative**, or **Now** and configure the options as needed.

Modify the Document Table

You can adjust the appearance and content of the document table by resizing columns and rows, sorting fields, and applying filters to refine your document view.

Reorder and Resize Columns

- To move a single column, click its header and select "Move left" or "Move right" from the dropdown menu.
- To rearrange multiple columns, click "Columns," then drag and drop column names in the pop-up to reorder them.
- To resize a column, drag the right edge of the column header until it reaches the desired width.

Adjust Row Height Click the row height icon (displayed as a table icon) to set the row height to either one or more lines or automatically adjust it to fit the content.

Sort Fields Data can be sorted by one or more fields in ascending or descending order. By default, sorting is based on the time field, from newest to oldest.

- To sort a single field, click its column header and select the sort order.
- To sort by multiple fields, click "Field sorted," choose the fields from the dropdown, and add them.
- To reorder fields in the sort, drag them to the desired position.

Edit a Field You can modify how Infraon Infinity displays a field:

- Click the column header for the field and select "Edit multi-index field."
- In the "Edit field" form, change the field name and format as needed.

Filter Documents You can filter documents to focus on the specific data you're interested in:

- Select the documents you wish to compare.
- Click the "Documents selected" option and select "Show selected documents only."

Set Rows per Page To adjust how many rows are displayed per page, use the "Rows per page" menu. The default setting is 100 rows per page.

Inspect a Document You can explore an individual document to view its fields, apply filters, and review documents that occurred before or after it:

- Click the expand icon (a double arrow) next to a document in the list.
- You can view the document in two formats:
 - **Table View:** Displays fields and values in a row-by-row format.
 - **JSON View:** Shows how the document is returned from Elasticsearch.
- In Table View, hover over the Actions column to:
 - Filter results to include or exclude specific fields or values.
 - Toggle a field on or off in the document table.
 - Pin a field to keep it at the top.
- To navigate to the next or previous document, use the < and > arrows at the top of the view.
- Click "Single document" to create a bookmarkable and shareable view of a document. The link will remain valid if the document is available in Elasticsearch.
- To view documents before or after the current event, click "Surrounding documents." The same columns and filters from the Log search view will apply, with pinned filters remaining active and others copied in a disabled state.

Log Stream

The Log Stream in Infraon Infinity allows you to search, filter, and tail all logs ingested into the Elasticsearch database without logging into different servers,

changing directories, or tailing individual files. All your logs are conveniently accessible within the Log Stream.

Features include live log streaming, filtering with auto-complete, and a log graph for efficient navigation. You can also quickly categorize log messages to identify patterns in your log events.

What do you see on the screen?

The top panel features the same search, filter, time range, refresh, and download options in the Log search. [Click here](#) for a closer look.

Log Stream Details | Home page

Label	Action/ Description
Customize	Click to modify the view of the stream page. You can choose options for line wrapping and adjust the text size from large to medium.
Highlights	This option will emphasize specific fields on the page, making searching for and viewing them easier.
Stream Live	Initiate a live stream of incoming logs and document fields by clicking here. To terminate the stream, click again.

Log Stream settings

The Settings page within the Log Stream section allows users to customize and manage their log streams effectively. This page provides functionality to configure the multi-index names, manage log sources, and customize log columns. Below is a detailed description of the available options and their functionalities.

Multi-Index Name

- Users can specify or modify the name of the Multi-Index directly from this page. This feature is essential for organizing and categorizing log data across multiple indices for better accessibility and management.

Add New Multi-Index: Enter a new name for it and save it to create a new index.

Edit Existing Multi-Index: You can modify the name of an existing Multi-Index by selecting it and updating the name field.

Log Source Configuration

- This section allows users to add or remove log sources linked to the current log stream. Configuring log sources ensures the right data is collected and managed effectively.

Add Log Source: Provide details such as source type, connection information, and any required authentication to specify new log sources.

Edit Log Source: Update the configuration of existing log sources if source details or connection parameters change.

Remove Log Source: Delete a log source that is no longer needed or is causing issues.

Log Columns Customization

- Users can adjust the columns displayed in log entries to fit their needs better. This includes adding new fields for more detailed log information or removing obsolete ones.

Add New Field: Introduce new columns to the log entries by defining field names and specifying their types. This feature helps capture additional data points that may be relevant for analysis.

Delete Existing Field: Remove any necessary or relevant fields that are no longer necessary to streamline log data presentation.

Note: Only users with the appropriate privileges can change the Log Stream Settings page.

Export Configs

Exporting logs or data from Log management can be useful for offline analysis, reporting, or sharing with others. Infraon Infinity provides a few data export methods, including PDF, Excel, and CSV. Any data exported in the log search and log stream pages will be listed on the log export page. The user can just download the logs by clicking the download button.

What do you see on the screen?

Export Configs Details | Home page

Label	Action/ Description
Search	Search for the required exported Multi-Index file.
Filter	Filters with respective conditions can be added based on the Fields (Name, type, file type, and status).
Creation Time	This will display the date and time when the report was generated.

Name	Indicates the name of the exported log report.
Description	Displays a brief description (if added) of the log report.
Type	Shows the type of the file selected while generating the Log report.
File Type	Indicates the file of the exported configs. (Ex: PDF, XLS, or CSV)
File Size	Displays the size of files that have been generated.
Status	Indicates the report's status, such as whether it is available for download or still in progress (e.g., Done or in progress).
Action	Click to download the generated Log using the respective file type.

Marketplace

Azure Active Directory

You can sync Azure Active Directory with Infraon to enable user/requester account synchronization. Follow the below steps to configure Azure Active Directory.

Pre-requisites

- An active Azure account

The Process

Follow the below steps on your Azure portal.

Step 1: Register your app

1. Log in to your Azure account and click 'App Registrations.'



2. Select 'New registration.'



The screenshot shows the Microsoft Azure portal interface. At the top, there's a blue header bar with the 'Microsoft Azure' logo and a search bar. Below the header, the 'App registrations' section is visible. A navigation bar at the top of this section includes 'New registration' (which is highlighted with a grey background), 'Endpoints', 'Troubleshooting', 'Refresh', 'Download', 'Preview features', and a 'Got feedback?' link. There are also icons for settings, help, and other portal functions.

3. Add a display name for your application, select the account type, and click 'Register.'

Home > App registrations >

Register an application

* Name

The user-facing display name for this application (this can be changed later).

 ✓

Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (Single tenant)
- Accounts in any organizational directory (Multitenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Select a platform ▼ e.g. <https://example.com/auth>

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

By proceeding, you agree to the Microsoft Platform Policies [↗](#)

[Register](#)

4. The application is created, and the details are displayed per the reference screenshot. Copy the Application and Tenant ID.

Home > App registrations > Infraon Client

Overview

Display name : Infraon Client
 Application (client) ID : Your Application ID is displayed here
 Object ID :
 Directory (tenant) ID : Your Tenant ID is displayed here
 Supported account types : My organization only

Client credentials : Add a certificate or secret
 Redirect URIs : Add a Redirect URI
 Application ID URI : Add an Application ID URI
 Managed application in I... : Infraon Client

Get Started Documentation

Build your application with the Microsoft identity platform

The Microsoft identity platform is an authentication service, open-source libraries, and application management tools. You can create modern, standards-based authentication solutions, access and protect APIs, and add sign-in for your users and customers. [Learn more](#)

Step 2: Enable API Permissions

1. Navigate to 'API Permissions' and click 'Add a permission.'

Home > App registrations > Infraon Client

API permissions

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission

API / Permissions name	Type	Description	Admin consent requ...	Status

2. A slider appears. Click on the 'APIs my organization uses' tab.

Request API permissions

Select an API

Microsoft APIs APIs my organization uses My APIs

Apps in your directory that expose APIs are shown below

Start typing an API name or Application ID

Name	Application (client) ID
------	-------------------------

3. Select 'Microsoft Graph' from the list of APIs displayed.

Request API permissions

X

Select an API

Microsoft APIs APIs my organization uses My APIs

Apps in your directory that expose APIs are shown below

Start typing an API name or Application ID

Name	Application (client) ID
Policy Administration Service	0469d4cd-df37-4d93-8a61-f8c75b809164
Windows Azure Active Directory	00000002-0000-0000-c000-000000000000
Billing RP	80dbdb39-4f33-4799-8b6f-711b5e3e61b6
Azure Storage	e406a681-f3d4-42a8-90b6-c2b029497af1
Azure Key Vault	cfa8b339-82a2-471a-a3c9-0fc0be7a4093
Microsoft Azure App Service	abfa0a7c-a6b6-4736-8310-5855508787cd
Windows Store for Business	45a330b1-b1ec-4cc1-9161-9f03992aa49f
Networking-MNC	6d057c82-a784-47ae-8d12-ca7b38cf06b4
M365 License Manager	aeb86249-8ea3-49e2-900b-54cc8e308f85
func-SAAS-TEST-3alw	cf471a45-fe81-4aee-9ccc-291857c4917b
Windows Azure Service Management API	797f4846-ba00-4fd7-ba43-dac1f8f63013
Application Insights API	f5c26e74-f226-4ae8-85f0-b4af0080ac9e
Azure Resource Graph	509e4652-da8d-478d-a730-e9d4a1996ca4
Partner Customer Delegated Administration	2832473f-ec63-45fb-976f-5d45a7d4bb91
Azure DevOps	499b84ac-1321-427f-aa17-267ca6975798
Microsoft Graph	00000003-0000-0000-c000-000000000000
Device Registration Service	01cb2876-7ebd-4aa4-9cc9-d28bd4d359a9
Compute Recommendation Service	b9a92e36-2cf8-4f4e-bcb3-9d99e00e14ab

4. Scroll down and look for 'User' related APIs. Expand and select 'User.Read.All' to enable.

Request API permissions

The screenshot shows the 'Request API permissions' interface. At the top, there's a header 'Request API permissions' with a close button 'X'. Below it is a tree view of API categories:

- IdentityUserFlow
- SynchronizationData-User
- TeamsAppInstallation
- TeamsTab
- User-LifeCycleInfo
- UserAuthenticationMethod
- UserNotification
- UserShiftPreferences

Under 'User', there are seven items:

Permission	Description	Status
<input type="checkbox"/> User.EnableDisableAccount.All ⓘ	Enable and disable user accounts	Yes
<input type="checkbox"/> User.Export.All ⓘ	Export user's data	Yes
<input type="checkbox"/> User.Invite.All ⓘ	Invite guest users to the organization	Yes
<input type="checkbox"/> User.ManageIdentities.All ⓘ	Manage all users' identities	Yes
<input checked="" type="checkbox"/> User.Read.All ⓘ	Read all users' full profiles	Yes
<input type="checkbox"/> User.ReadWrite.All ⓘ	Read and write all users' full profiles	Yes

At the bottom, there are two buttons: 'Add permissions' (highlighted in blue) and 'Discard'.

5. Once the permissions are added, details are displayed per the reference.

The screenshot shows the 'API permissions' section of the Azure portal for the 'Infraon Client' application. The 'Grant admin consent for Company' checkbox is checked. A success message in a toast notification says 'Updating permissions' and 'Successfully saved permissions for Infraon Client.'

6. Click on 'Grand Admin Consent' and confirm your selection.

The screenshot shows the 'Grant admin consent confirmation' dialog. It asks if you want to grant consent for all accounts in Company Name. Two buttons are shown: 'Yes' (highlighted) and 'No'.

Step 3: Create a client secret

1. Navigate to 'Certificates and secrets' -> Client Secrets.

Infraon Client | Certificates & secrets

Search

«

 Got feedback?

 Overview

 Quickstart

 Integration assistant

Manage

 Branding & properties

 Authentication

 Certificates & secrets

 Token configuration

 API permissions

 Expose an API

 App roles

 Owners

 Roles and administrators

 Manifest

Support + Troubleshooting

 Troubleshooting

 New support request

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens. You can use a certificate or a client secret (and a certificate) to prove the identity of your application. We recommend using a certificate (instead of a client secret) as a more secure scheme. For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a more secure scheme.

 Application registration certificates, secrets and federated credentials can be found in the tabs below.

[Certificates \(0\)](#)

[Client secrets \(0\)](#)

[Federated credentials \(0\)](#)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as a client ID.

[+ New client secret](#)

Description	Expires	Value ⓘ
-------------	---------	---------

No client secrets have been created for this application.

1. Go to the Azure portal and select the app registration.
2. Add a new client secret. Provide a description and an expiration date. The client secret is valid only for the selected period. A new client must be created on the expiry of this. Click 'Add' once done.

Add a client secret

X

Description	Infinity
Expires	<p>Recommended: 180 days (6 months)</p> <p>Recommended: 180 days (6 months)</p> <p>90 days (3 months)</p> <p>365 days (12 months)</p> <p>545 days (18 months)</p> <p>730 days (24 months)</p> <p>Custom</p>

3. The client secret is generated. Copy the value to the clipboard. Please note that this value will be hidden on page refresh.

Home > App registrations > Infraon Client

Infraon Client | Certificates & secrets

Search Got feedback?

Overview Quickstart Integration assistant

Certificates enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Got a second to give us some feedback? →

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates (0) Client secrets (1) Federated credentials (0)

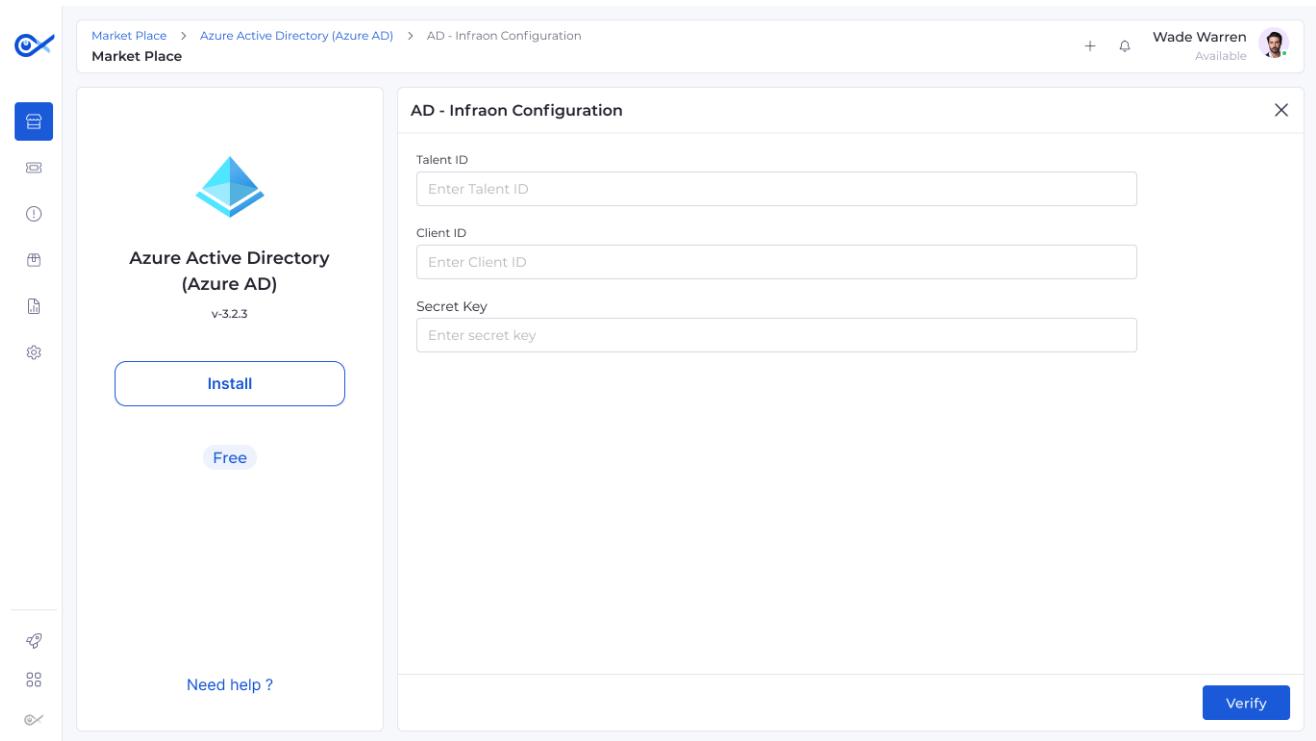
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

New client secret

Description	Expires	Value	Copy to clipboard	ID
Infinity	10/17/2023	FpO8Q~IbdSP4NtisCdxW-cvAYg86SbFg...	6982412b-2676-4824-bd87-c89a16788886	⋮

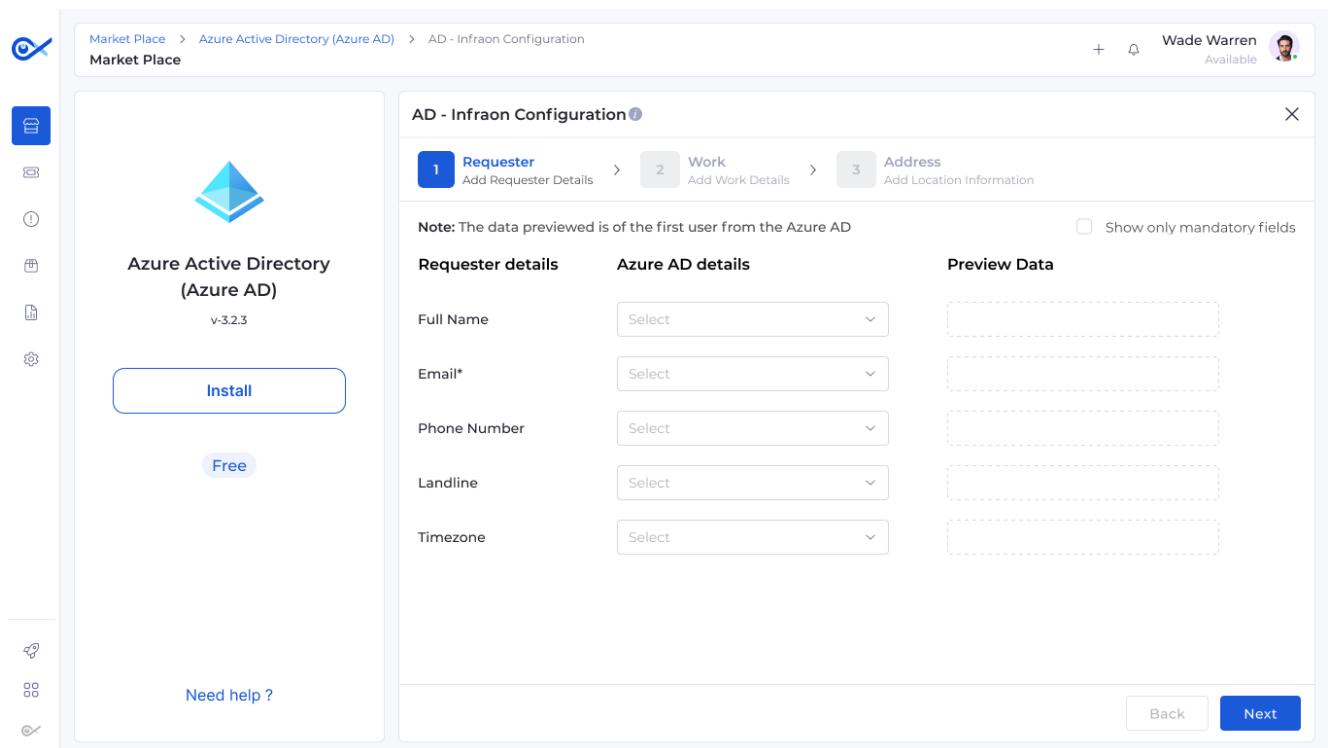
Step 4: Register your app on Infraon.

1. Navigate to Infraon -> Market Place -> Azure Active Directory (Azure AD). Click 'Install'. Add the 'Talent ID', Client ID, and Secret Key. Click 'Verify.'



2. Per the reference screenshot, you will be redirected to the field mapping screen on successful verification. Select column names to the respective field name in the below tabs on Infraon.

- Requester
- Work
- Address



3. Click 'Submit' when you are done. It might take a few minutes for Infraon to complete the synchronization. Once complete, all your Azure users are added as requesters on Infraon.

Infraon Dell

Description

Infraon Dell integration makes it a comprehensive and centralized platform for gathering, analyzing, and managing information about your Dell infrastructure.

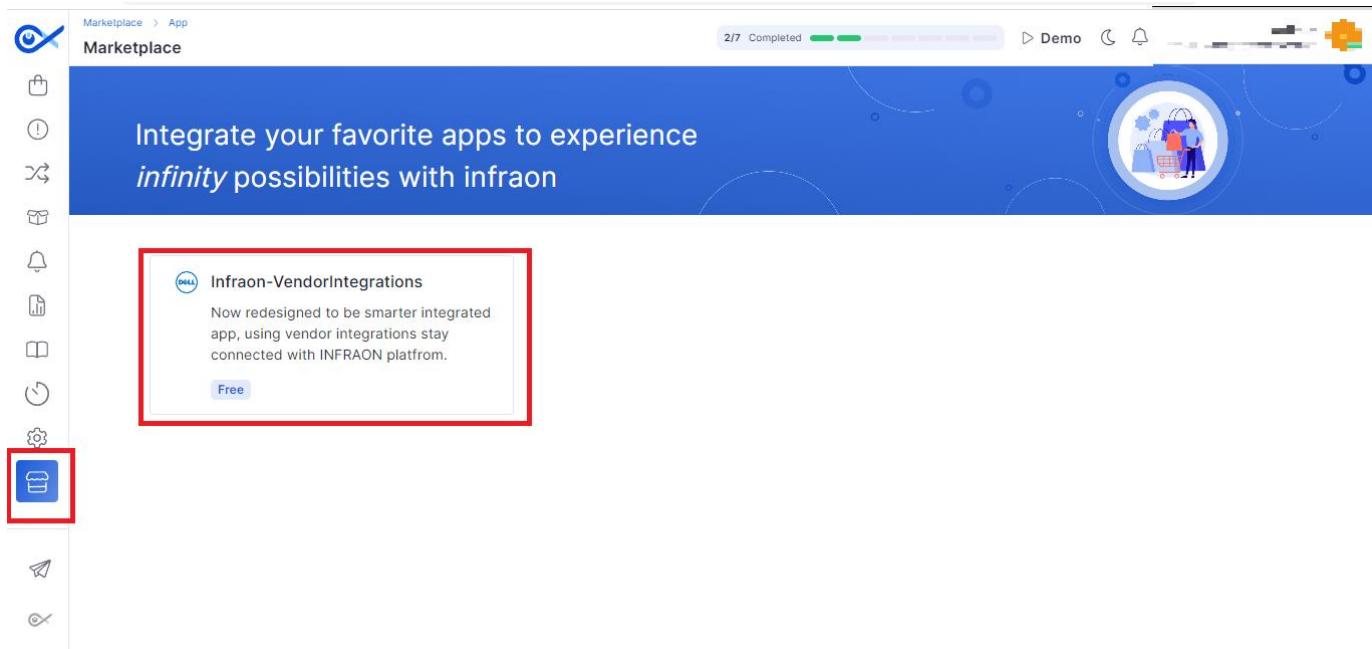
You can now check the details of the following:

- Hardware Inventory
- Health
- Software
- Configuration Management
- Warranty
- Manufacturing date

How to Install

STEP 1: Log in to your Infraon account. On the left panel, click on the Marketplace tab.

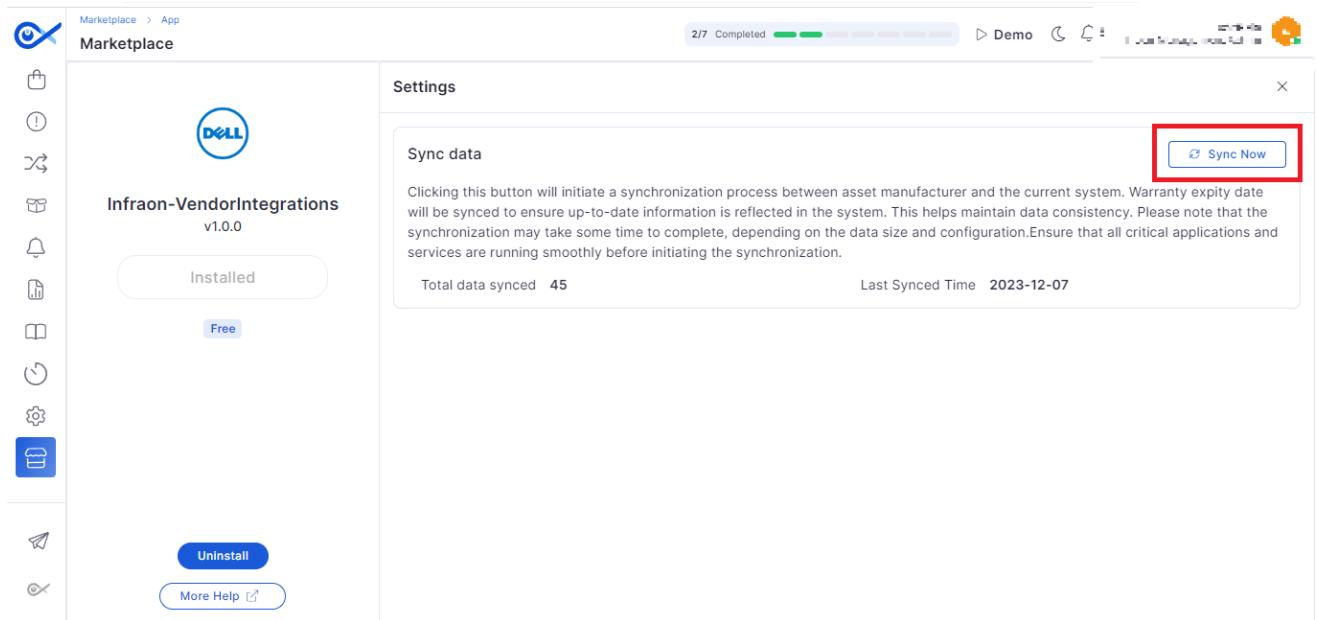
Select the “**Dell**” integration.



STEP 2: After clicking the tab, go ahead and install.

A screenshot of the Infraon Marketplace interface, showing the same "Infraon-VendorIntegrations" app page after installation. The "Install" button is now highlighted with a red rectangle. The app card now shows the status "Installed". To the right, there is a "Settings" panel with a "Sync data" button, which is also highlighted with a red rectangle. Below the sync button is a note about the synchronization process. At the bottom of the page, there are "Uninstall" and "More Help" buttons.

STEP 3: Click "Sync Now" to sync your data.



The process is now complete.

Google Workspace

Description

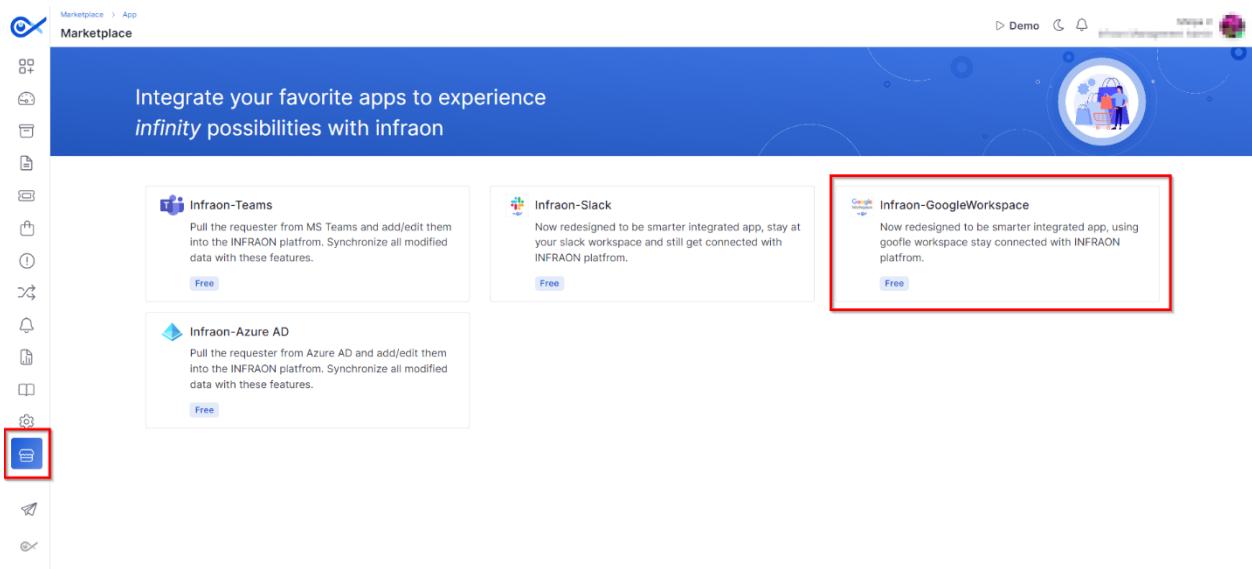
Infraon is now integrated with Google Workspace. This lets end users see requester info directly in Infraon. Just sync your data and enjoy seamless interactions. Now users can:

- View Infraon requester details and connect them to Infinity, all within Google Workspace.
- Streamline Infraon workflows and communication with effortless integration into Google Workspace.
- Leave the platform switching behind! Infraon comes to Google Workspace for smooth collaboration.

How to Install

STEP 1: Log in to your **Infraon** portal, click the Marketplace icon on the left,

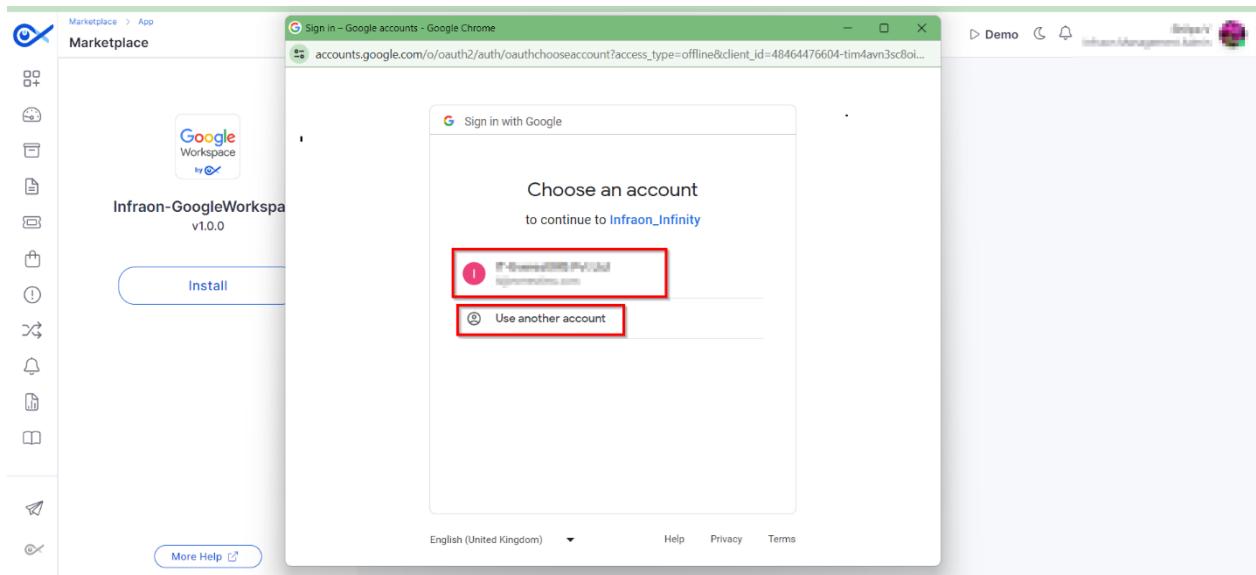
and then select "**Google Workspace Integration.**"



STEP 2: Navigate to the "**INSTALL**" button to continue.

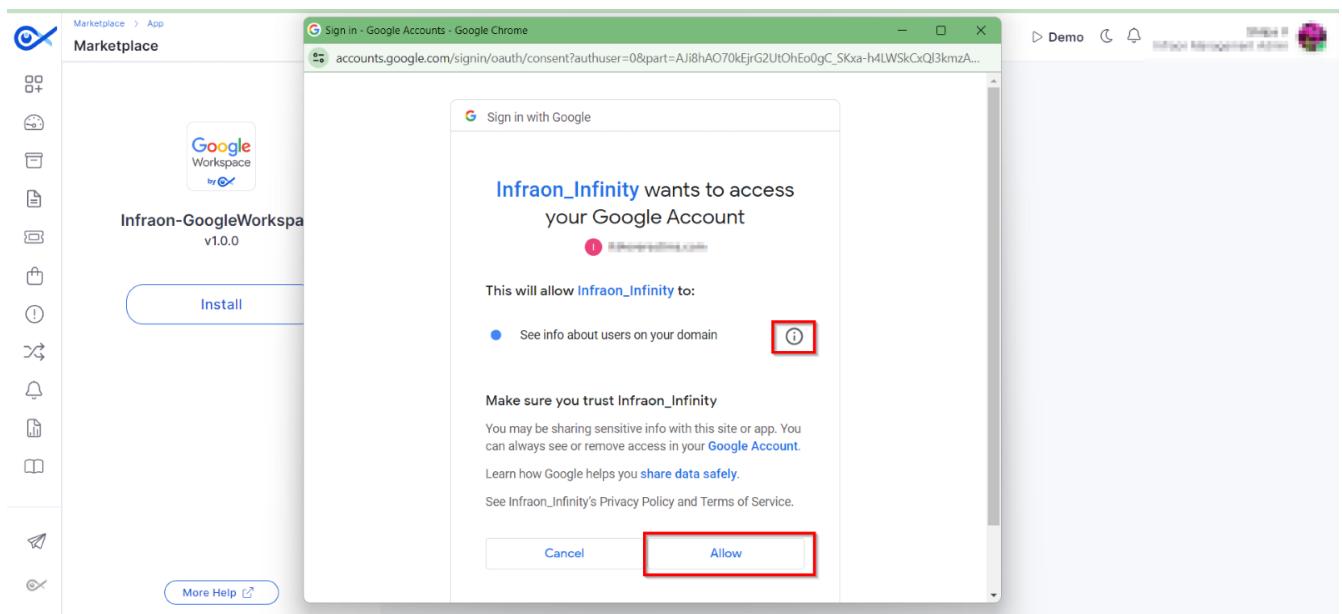
A screenshot of the Infraon-GoogleWorkspace app details page. The page includes a header with the Infraon logo and a "Marketplace" link. The main content area shows the app icon (Google Workspace), name ("Infraon-GoogleWorkspace v1.0.0"), and a large "Install" button which is highlighted with a red box. To the right of the install button is a "Description" tab and a "How to install" section. The "How to install" section contains a detailed description of the integration and a bulleted list of benefits. Below this is an "Additional Information" section with developer and published by details. At the bottom of the page is a "More Help" button.

STEP 3: After clicking "**Install**," a pop-up will appear asking you to choose your Google account. Select the one you want to use for this integration or click "**Use another Account**" if it's not listed.

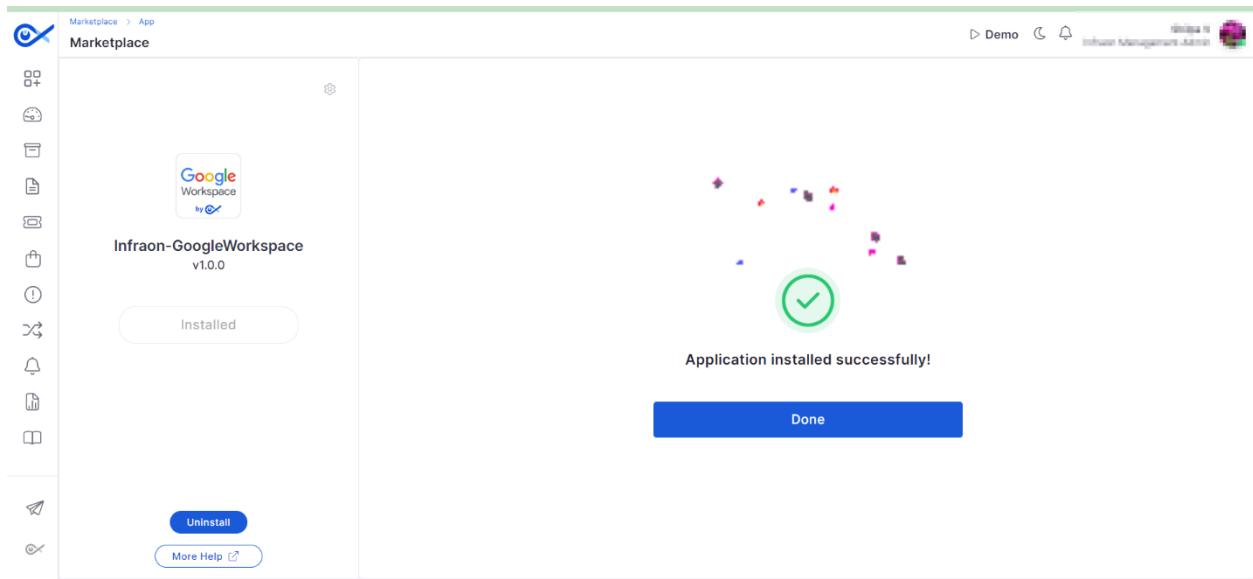


STEP 4: Click "**Allow**" after selecting your Google account to authorize Infraon and complete the integration.

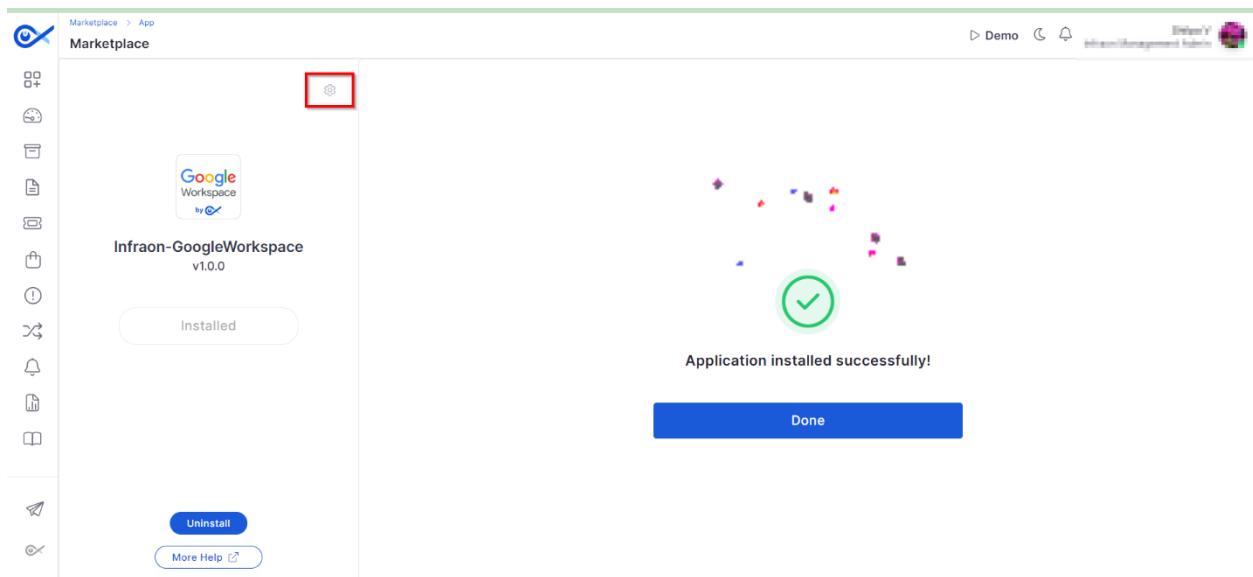
Note: Click on the **(i)** button for more info.



The below page appears once the installation is complete.

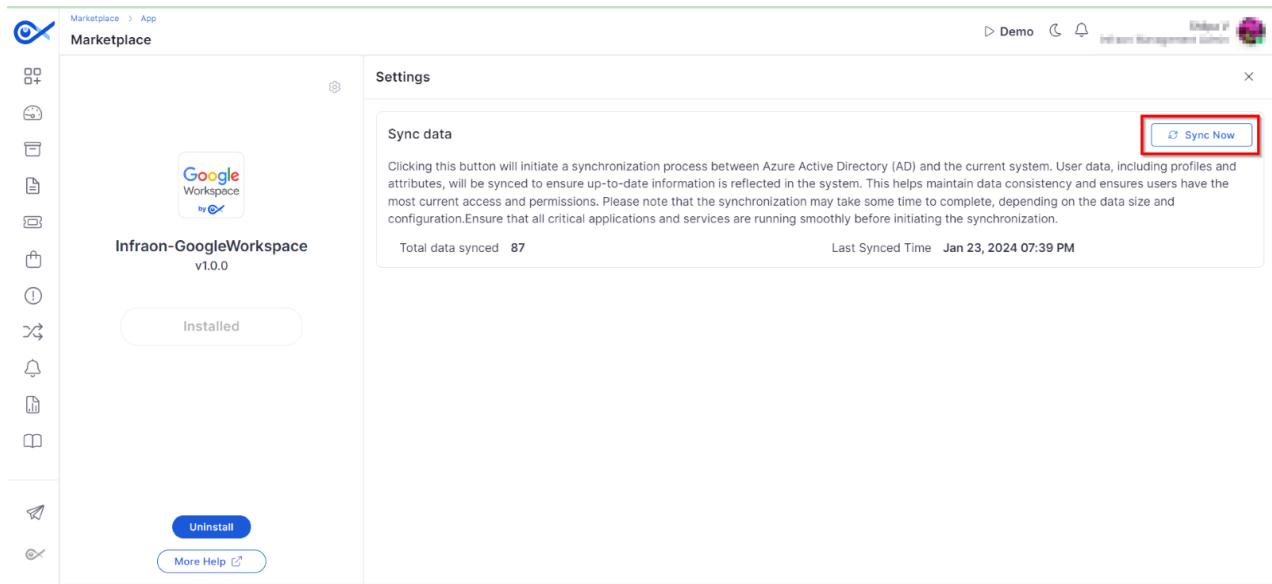


STEP 5: To complete the integration, navigate and click on the "**Settings**" icon.



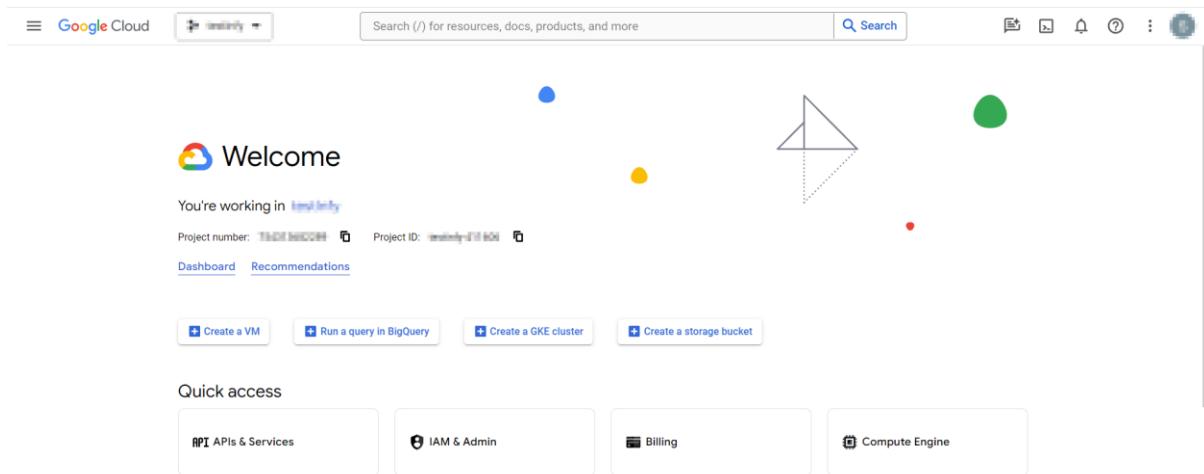
STEP 6: Clicking "**Sync Now**" in the top right corner completes the data synchronization process between Google Workspace and Infraon.

Note: Depending on the amount and complexity of your data, it could take some time to complete.



STEP 5: Requesting to add minimum OAuth scopes to add to the project.

- Sign in to the [Google Cloud Console](#). Select the project ID required for the services.



- On the left panel, navigate to APIs & Services -> OAuth consent screen, configuration page.

The screenshot shows the Google Cloud Platform API & Services dashboard. On the left sidebar, under the 'API' section, 'OAuth consent screen' is highlighted with a red box. A dropdown menu is open over this item, also containing 'OAuth consent screen', which is also highlighted with a red box.

- Click on the Edit App registration to continue.

The screenshot shows the 'OAuth consent screen' configuration page. On the left sidebar, 'OAuth consent screen' is selected and highlighted with a red box. In the main area, there is a large blue button labeled 'EDIT APP' which is also highlighted with a red box.

- Scroll the page to the bottom and click "Save and Continue" to move to the next page.

The screenshot shows the 'Edit app registration' page. At the bottom of the page, there is a red rectangular box highlighting the 'SAVE AND CONTINUE' button.

- Now, in the "Scopes," click on the "Add or Remove Scopes" and follow the below steps carefully.

- A new pop-up will display to update the selected scopes. Here either choose from the list of given scopes or manually add any one OAuth scope from the list below.

Authorization scopes

- <https://www.googleapis.com/auth/admin.directory.user>
- <https://www.googleapis.com/auth/admin.directory.user.readonly>
- <https://www.googleapis.com/auth/cloud-platform>

For more information, see the [Authorization guide](#).

Now click Add to Table -> Update.

API	Scope	User-facing description
<input type="checkbox"/> Admin SDK API	.../auth/admin.chrome.printers	See, add, edit, and permanently delete the printers that your organization can use with Chrome
<input type="checkbox"/> Admin SDK API	.../auth/admin.chrome.printers.readonly	See the printers that your organization can use with Chrome
<input type="checkbox"/> Admin SDK API	.../auth/admin.directory.device.chromebrowsers	See and manage Chrome browsers under your organization
<input type="checkbox"/> Admin SDK API	.../auth/admin.directory.device.chromebrowsers.readonly	See Chrome browsers under your organization
<input type="checkbox"/> Admin SDK API	.../auth/admin.directory.device.chromeos	View and manage your Chrome OS devices' metadata
<input type="checkbox"/> Admin SDK API	.../auth/admin.directory.device.chromeos.readonly	View your Chrome OS devices' metadata
<input type="checkbox"/> Admin SDK API	.../auth/admin.contact.delegation	View and manage contact delegation settings for users in your Organization

Rows per page: 10 ▾ 1 – 10 of 68 < >

Manually add scopes
 If the scopes you would like to add do not appear in the table above, you can enter them here. Each scope should be on a new line or separated by commas. Please provide the full scope string (beginning with "https://"). When you are finished, click "Add to table".

ADD TO TABLE **UPDATE**

- Once the selected Click Submit for verification.

The screenshot shows the Google Cloud Platform interface for managing APIs & Services. On the left sidebar, 'OAuth consent screen' is selected under 'APIs & Services'. The main area displays three entries under 'Account':

API	Scope	User-facing description
BigQuery API	~ /auth/devstorage/full_control	Manage your data and permissions in Cloud Storage and see the email address for your Google Account
BigQuery API	~ /auth/devstorage/read_only	View your data in Google Cloud Storage
BigQuery API	~ /auth/devstorage/read_write	Manage your data in Cloud Storage and see the email address of your Google Account

Below this, a section titled 'Your restricted scopes' is shown with the note: 'Restricted scopes are scopes that request access to highly sensitive user data.' A table header row is visible but contains no data.

At the bottom right of the main area, there are 'SAVE AND CONTINUE' and 'CANCEL' buttons, with 'SAVE AND CONTINUE' being highlighted by a red box.

The above process is now completed.

Infraon JAMF

Description

The Infraon-JAMF application solution provides detailed inventory and tracking of Apple devices. Integration with JAMF allows you to import device data from JAMF automatically, eliminating manual entry and ensuring accuracy.

You can now:

Access detailed information and explore comprehensive hardware, software, inventory management, and asset lifecycle data.

How to Install

STEP 1: Log in to your Infraon account. On the left panel, click on the "Marketplace" tab. Select "**JAMF Integration.**"

Marketplace > App Marketplace

Integrate your favorite apps to experience infinity possibilities with infraon

Infraon-Slack
Now redesigned to be smarter integrated app, stay at your slack workspace and still get connected with INFRAON platform.

Infraon-Azure AD
Pull the requester from Azure AD and add/edit them into the INFRAON platform. Synchronize all modified data with these features.

Infraon-Teams
Pull the requester from MS Teams and add/edit them into the INFRAON platform. Synchronize all modified data with these features.

Infraon-ServiceNow
Sync your existing asset to servicenow

Infraon-VendorIntegrations
Now redesigned to be smarter integrated app, using vendor integrations stay connected with INFRAON platform.

Infraon-Whatsapp
Now redesigned to be smarter integrated app, using whatsapp stay connected with INFRAON platform.

Infraon-Jamf
Pull the devices from Jamf and add/edit them into the INFRAON platform. Synchronize all modified data with these features.

STEP 2: Click "INSTALL" to continue.

Marketplace > App Marketplace

Screenshots

Description How To Install

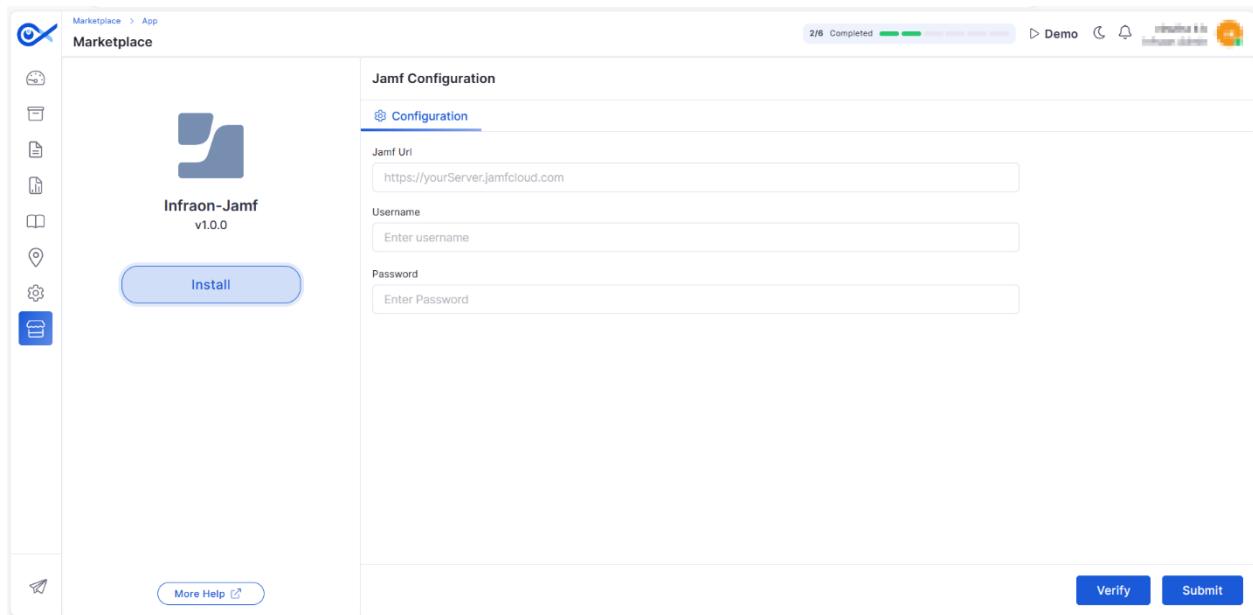
The Infraon Jamf Pro Marketplace Application Jamf Pro is a standardized and efficient method that enables seamless user synchronization between Jamf Pro and Infraon. With Jamf Pro synchronizations, organizations can automate creating and modifying users. The process utilizes a RESTful API-based approach, simplifying implementation, configuration, and maintenance of identity synchronization between Jamf Pro and Infraon. Real-time synchronization ensures that changes to Jamf Pro user attributes, such as name, email, or role, can be done with the click of a button.

Additional Information

Developed By	:	Infraon Corp.
Published By	:	Infraon Corp.
Platform	:	Jamf Pro

More Help ⓘ

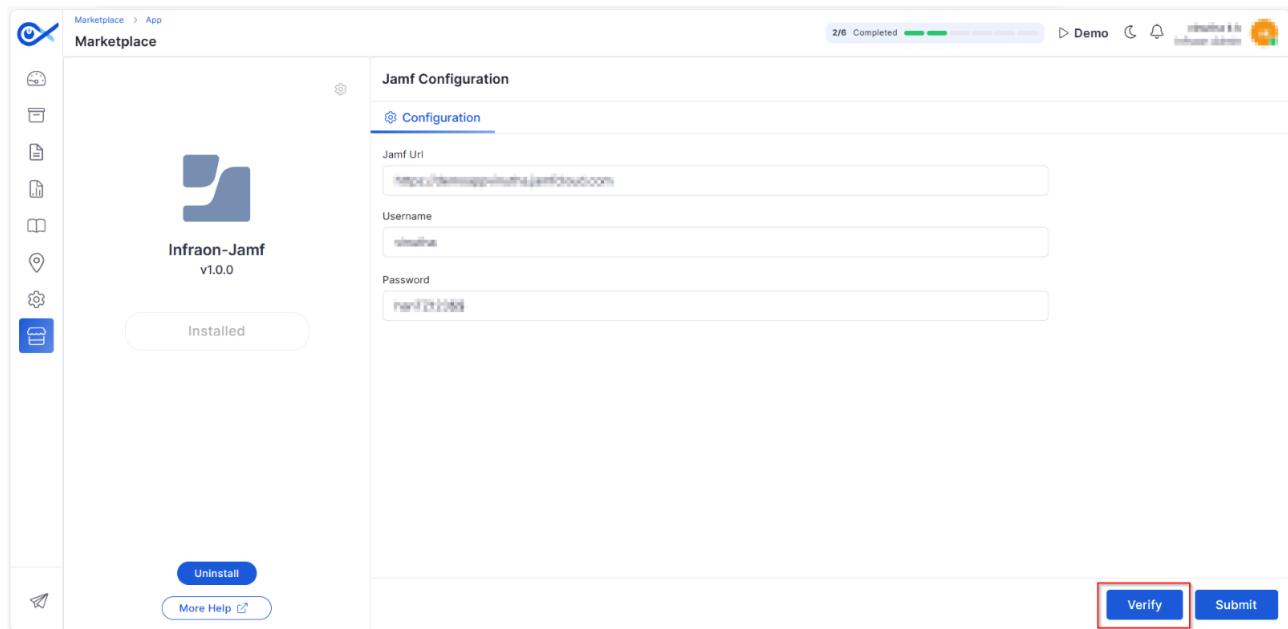
STEP 3: Enter the credentials in the required dialog boxes.



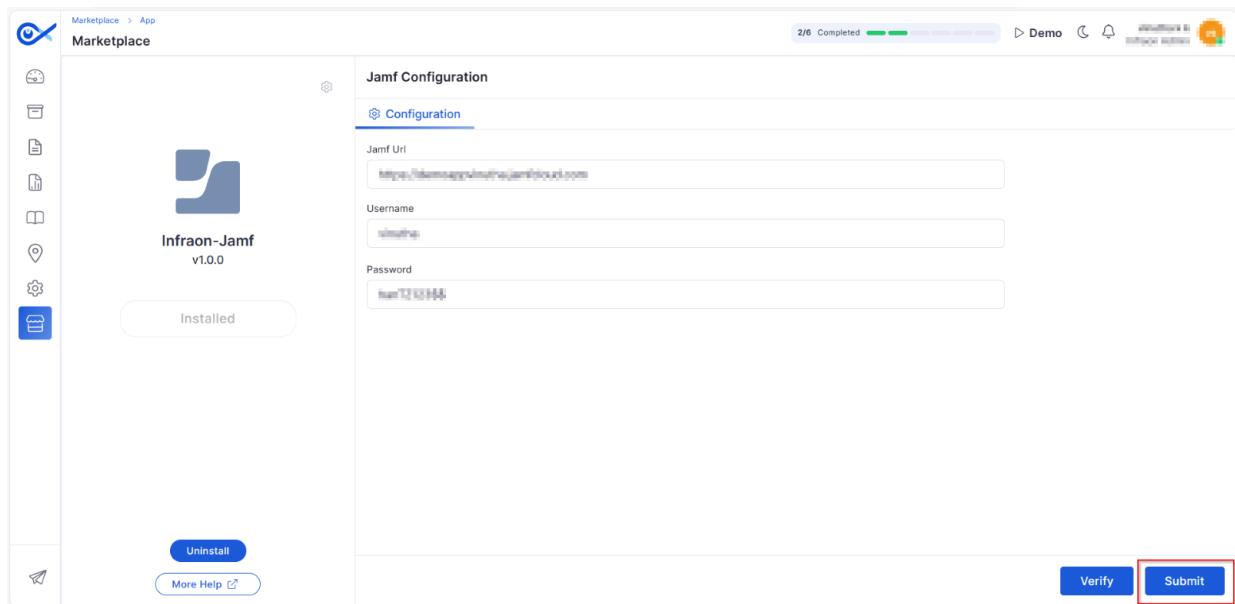
STEP 4: To enter the credentials, go to [JAMF setup assistance](#) and log in with your username and password. You can create a new account if you are a new user.

A screenshot of a help article titled 'Completing the Jamf Pro Setup Assistant'. The left sidebar shows a 'CONTENTS' menu with links like 'Getting Started with Jamf Pro', 'Completing the Jamf Pro Setup Assistant' (which is highlighted), 'Creating a Push Certificate', 'Connecting to Apple', 'Viewing the Jamf Pro Summary', and 'Additional Resources'. The main content area has a video player at the top. Below it, a section titled 'Requirements' is enclosed in a red box. It contains the text: 'You must have the following to complete the Setup Assistant:' followed by a bulleted list: '• Jamf Pro instance name' (with a note to contact Jamf Support), '• Jamf Pro activation code from Jamf Account' (with a note to access it via https://account.jamf.com). To the right, there's a 'RELATED CONTENT' sidebar with links to 'Single Sign-On (Jamf Pro)', 'SMTP Server Integration (Jamf Pro)', and 'User Accounts and Groups (Jamf Pro)'.

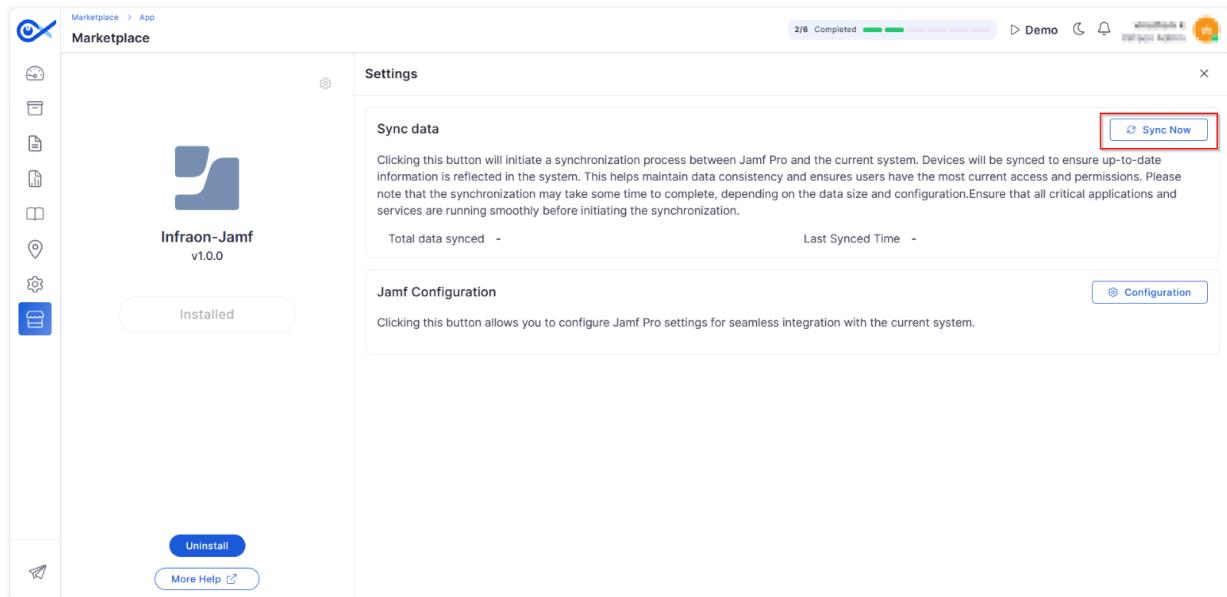
STEP 5: Copy the credentials and paste them on the configuration tab. And click "**VERIFY**" to continue.



STEP 6: Once verification is done, click "**SUBMIT**" to continue.



STEP 7: Navigate to "**SYNC NOW**" to complete the setup.



The process is now completed.

Infraon ServiceNow

Description

The Infraon–ServiceNow integration automates workflows and seamlessly optimizes resource allocation. This leads to significant cost savings and improved productivity, allowing your IT team to focus on high-priority tasks and deliver faster resolutions.

You can now:

- Create a new ticket
- View the status of the ticket

How to Install

Install the App

STEP 1: Log in to your Infraon account. On the left panel, click on the Marketplace tab. Select the “**ServiceNow**” integration.

Marketplace > App

Marketplace

Integrate your favorite apps to experience *infinity* possibilities with infraon

Infraon-Slack

Now redesigned to be smarter integrated app, stay at your slack workspace and still get connected with INFRAON platform.

Free

Infraon-Azure AD

Pull the requester from Azure AD and add/edit them into the INFRAON platform. Synchronize all modified data with these features.

Free

Infraon-Teams

Pull the requester from MS Teams and add/edit them into the INFRAON platform. Synchronize all modified data with these features.

Free

Infraon-Jamf

Pull the devices from Jamf and add/edit them into the INFRAON platform. Synchronize all modified data with these features.

Free

Infraon-ServiceNow

Sync your existing asset to servicenow

Free

Infraon-VendorIntegrations

Now redesigned to be smarter integrated app, using vendor integrations stay connected with INFRAON platform.

Free

STEP 2: After clicking the tab, go ahead and install.

Marketplace > App

Marketplace

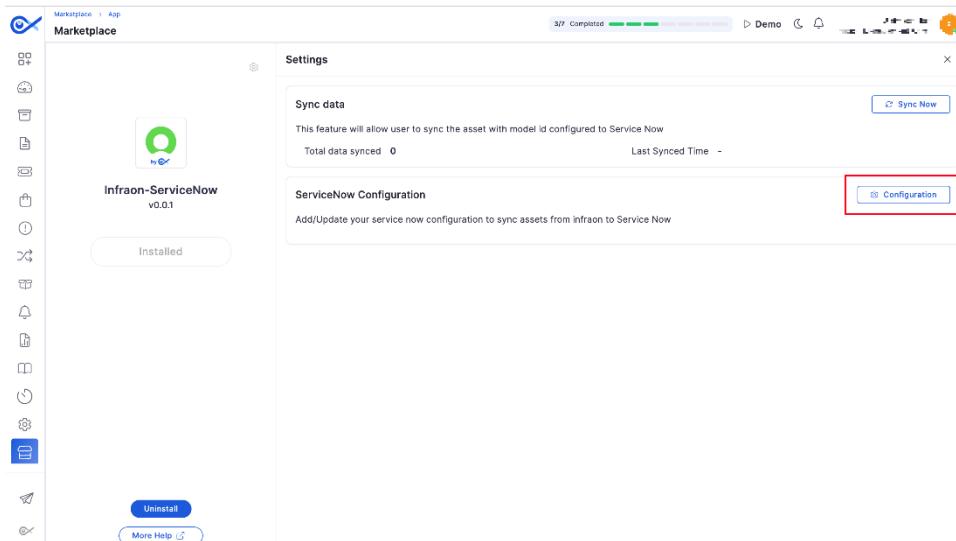
Screenshots

Infraon-ServiceNow v0.0.1

Install

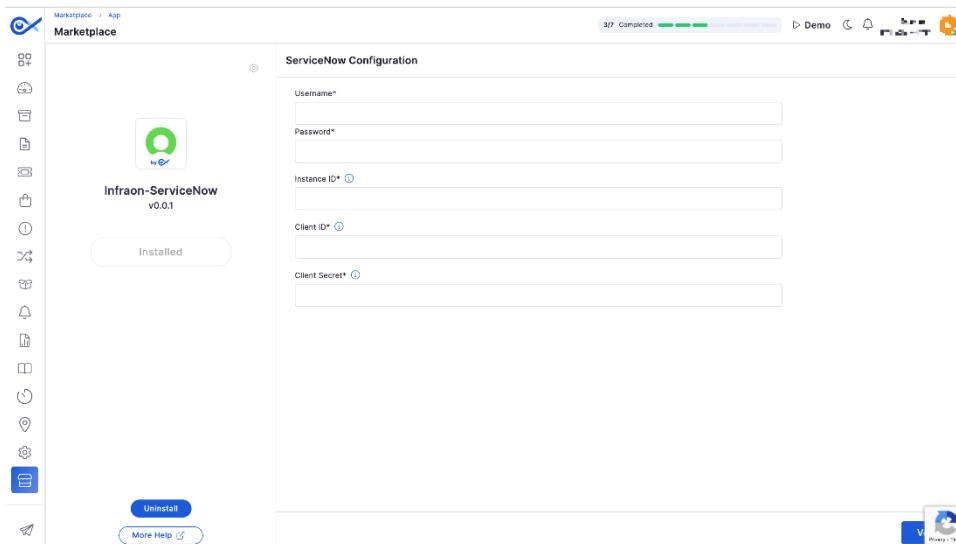
More Help

Step 3: Once the installation is done, click on the configuration tab.



STEP 4: Enter the credentials below from your ServiceNow admin account.

(**Note:** Click on the  button to find more.)
The below snip will be visible.



Entering the credentials

STEP 5: Log in to your ServiceNow admin account by [clicking here](#) to enter the credentials.

STEP 6: Once logged in to the ServiceNow Admin portal, on the top left corner, click on the “All” tab and search for “**System OAuth > Application Registry**.”

STEP 7: You can copy credentials from the page.

If you don't have your application registered, you can add a new one by clicking "New" at the extreme top right corner.

Name	Active	Type	Client ID	Comments
ADFS	true	External OAuth Provider	[redacted]	
Auth0	true	External OAuth Provider	[redacted]	
AzureAD	true	External OAuth Provider	[redacted]	
Google	true	External OAuth Provider	[redacted]	
Infron Client	true	OAuth Client	W4Z7M4P7D0D0D0D0D0D0D0D0D0D0D0D0	
Integrator	true	OAuth Client	409541A6-C91F-11E8-B40A-000C29B87D4	
Mobile API	true	OAuth Client	3000d340c100d00d0d0d0d0d0d0d0d0	Used by the mobile app to allow account creation
Office365	true	External OAuth Provider	[redacted]	
ServiceNow Agent	true	OAuth Client	409541A6-C91F-11E8-B40A-000C29B87D4	
ServiceNow Client Mobile App	false	OAuth Client	2e57bd0d6d0d0d0d0d0d0d0d0d0d0d0	
ServiceNow Request	true	OAuth Client	5d1d9ed3d0d0d0d0d0d0d0d0d0d0d0	
ServiceNow Virtual Agent Example App	true	OAuth Client	5d1d9ed3d0d0d0d0d0d0d0d0d0d0d0	
Update Microsoft User Graph	true	OAuth Provider	[redacted]	
Webkit Token Token Auth	true	External OAuth Provider	[redacted]	
Webkit ITML to PDF	true	OAuth Client	98e659d6d0d0d0d0d0d0d0d0d0d0d0	Used by the ServiceNow ITML to PDF API

STEP 8: Now enter the required dialog boxes, as per the conditions below. Once done, click "**Update**" on the extreme right bottom corner.

OAuth client application details.

- * Name: Infron Client
- * Client ID: (auto-generated)
- Client Secret: (auto-generated)
- Redirect URL: (empty)
- Logo URL: (empty)
- Public Client: (unchecked)
- Comments: (empty)

Application: Global
Accessible from: All application scopes
Active:

* Refresh Token Lifespan: (empty)
* Access Token Lifespan: (empty)
Login URL: (empty)

Auth Scopes

Auth Scope
(empty)

Buttons: Update (highlighted with a red box), Delete

Copy the credentials and enter them on *STEP 4*.

Step 9: Click the “Sync Now” tab once the configuration is done.

Marketplace

Infraon-ServiceNow v0.0.1

Installed

Settings

Sync data

This feature will allow user to sync the asset with model id configured to Service Now

Total data synced: 0 Last Synced Time: (dropdown)

Sync Now (highlighted with a red box)

ServiceNow Configuration

Add/Update your service now configuration to sync assets from infraon to Service Now

Configuration

Buttons: Uninstall, More Help

The process is now completed!

Infraon Slack

Description

The Infraon Slack Marketplace application enhances collaboration and communication, enabling users to collaborate and communicate within their teams effortlessly. With features like ticket management, support task sharing, and prompt issue resolution, productivity, and efficiency are significantly improved.

Overall, the Infraon Slack app empowers teams to collaborate effortlessly, communicate seamlessly, manage tickets efficiently, and leverage the strengths of both Slack and Infraon platforms to optimize productivity and effectiveness in their work processes.

- Infraon's Slack integration allows seamless ticket management within the Slack system.
- Users can directly use the integration without a learning curve and work with the existing product without difficulties.
- Create and update tickets, including ticket notes, within Slack workspace.

How to Install

- Log in to the Infraon portal and navigate to **Marketplace > Slack**. Click 'Install,' and wait for installation.
- You will now be redirected to Slack. Sign into your Slack account and continue.
- Enter the OTP if prompted. On successful authentication, you will be redirected to Infraon Marketplace.

FAQ

1. How can I create a ticket from Slack to Infraon?
 - Ticket emoji helps to create a ticket on a message
 - by adding emoji to the message body
 - by replying to emoji as a reaction to a message
 - Slash command to invoke the ticket model
 - "/ infraon ticket" [ENTER]
 - You can utilize the Shortcut "Create Ticket."
 - at the Global level by running /creating a ticket
 - at the Message level by clicking the message [:] action button
2. How can I update a ticket and add a note?
 - Access the ticket thread, input the necessary updates and notes, and save the changes.
 - View the updated ticket and their respective threads within the Infraon application.

Infraon Teams

Description

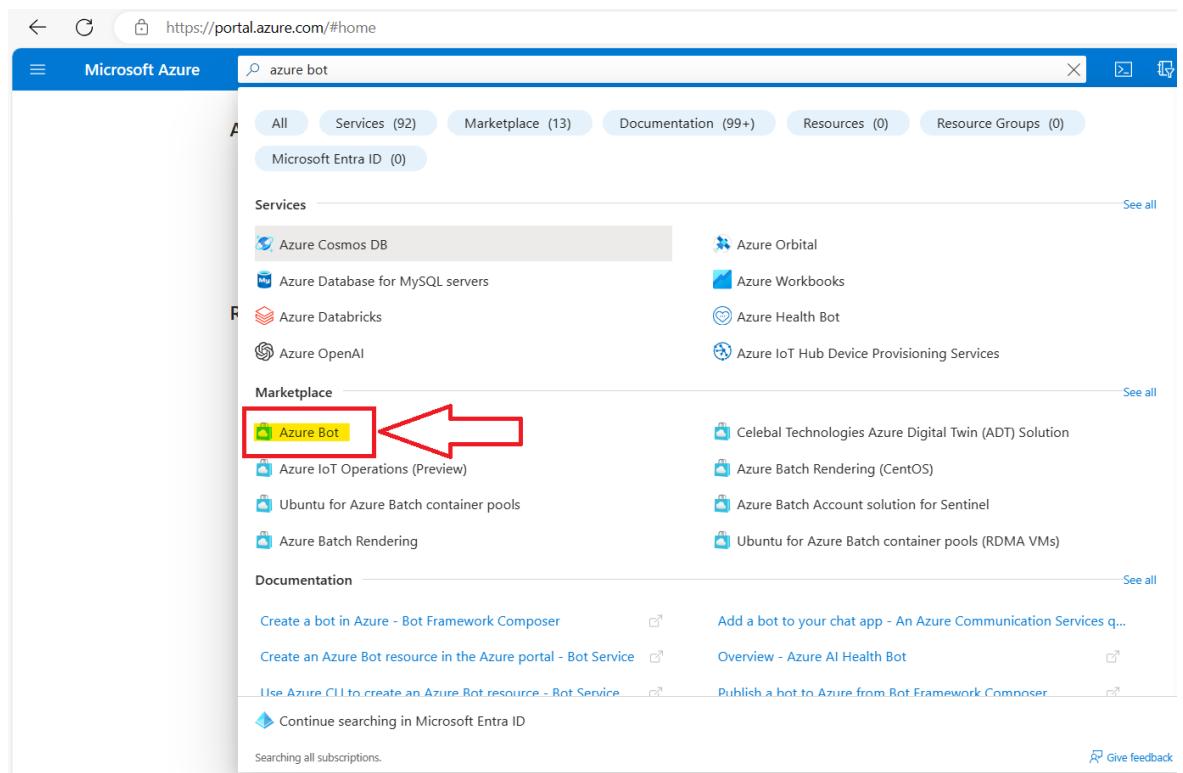
The Infraon-Teams application enables the integration of critical IT alerts within your existing MS Teams channels, triggering immediate collaboration and swift resolution. You can now:

- Create tickets
- Create requests
- View ticket detail
- Real-time updates on status changes
- Real-time updates on Comments

How to Install

Create Azure Bot

STEP 1: Go to the Azure portal, and in the right panel, select "**CREATE A RESOURCE.**" In the search box, enter Azure Bot, press Enter, and choose.



STEP 2: After selecting the Azure Bot, the below snip is visible. Enter “**Bot Handle**,” “**Subscription**,” and “**Resource Group**” details in the respective dialog box.

[Note: *one's are mandatory to fill.]

The screenshot shows the 'Create an Azure Bot' page in the Microsoft Azure portal. The 'Basics' tab is selected. The 'Project details' section includes fields for 'Bot handle' (filled with a placeholder), 'Subscription' (selected from a dropdown), and 'Resource group' (selected from a dropdown). Below these, 'Data residency' is set to 'Global'. The 'Pricing' section shows 'Pricing tier' as 'Free' (selected) with a 'Change plan' link. Under 'Microsoft App ID', it says 'A Microsoft App ID is required to create an Azure Bot resource.' Below this, 'Type of App' is set to 'Multi Tenant'. A note states that an App ID can be automatically created or manually created. The 'Creation type' section has 'Create new Microsoft App ID' selected. The URL for the screenshot is <https://i.imgur.com/3XWzQZG.png>.

STEP 3: Click **Review & Create** to continue.

<https://portal.azure.com/#create/Microsoft.AzureBot>

Create an Azure Bot

Basics Tags Review + create

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Bot handle *

Subscription *

Resource group * Create new

Data residency * Global Regional

Pricing

Select a pricing tier for your Azure Bot resource. You can change your selection later in the Azure portal's resource management. Learn more about available options, or request a pricing quote, by visiting the [Azure Bot Services pricing](#).

Pricing tier **Free** [Change plan](#)

Microsoft App ID

A Microsoft App ID is required to create an Azure Bot resource. If your bot app doesn't need to access resources outside of its home tenant and if your bot app will be hosted on an Azure resource that supports Managed Identities, then choose option User-Assigned Managed Identity so that Azure takes care of managing the App credentials for you. Otherwise, depending on whether your bot will be accessing resources only in its home tenant or not, choose either Single tenant or Multi-tenant option respectively.

Type of App

An App ID can be automatically created below or you can manually create your own, then return to input your new App ID and secret in the open fields. [Manually create App ID](#)

Creation type Create new Microsoft App ID Use existing app registration

[Previous](#) [Next](#) **Review + create**

Azure bot is created successfully.

Add the Microsoft Team Channel

STEP 4: Go to **Bot Services > Click on the new bot created**, navigate to the vertical left panel, and click "**Channels >Available Channels.**" add Teams.

[Search resources, services, and docs \(G+\)](#)

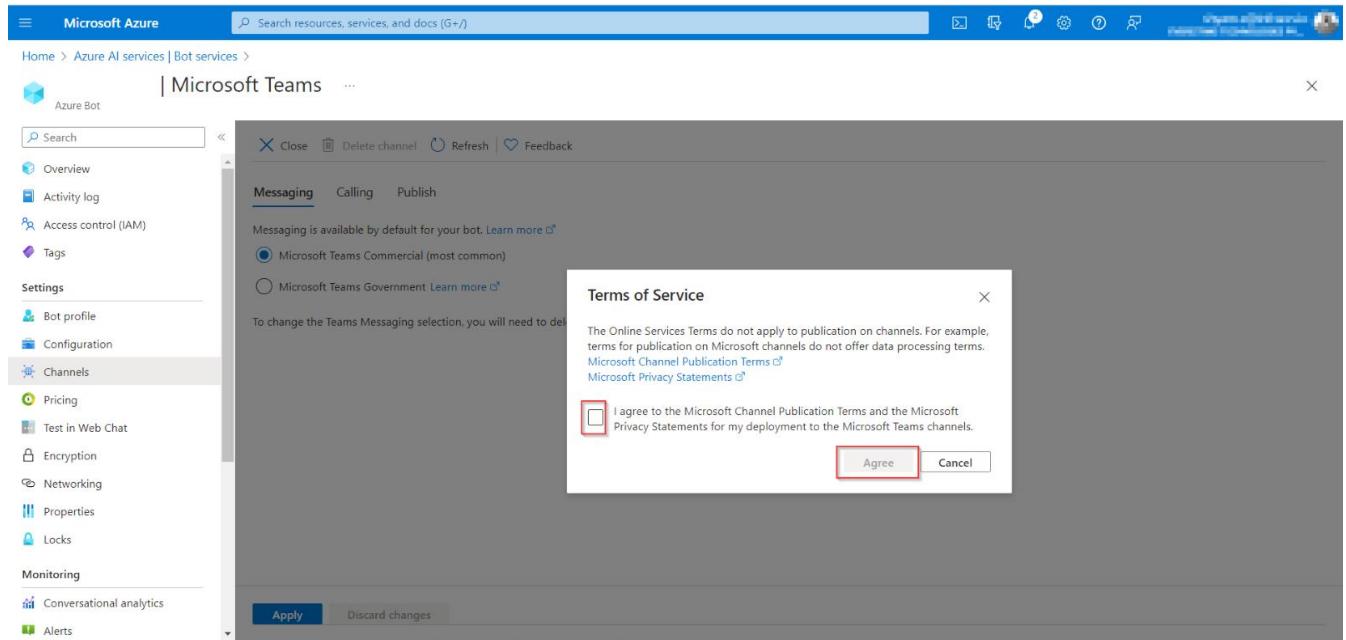
Home > Azure AI services | Bot services

Channels

Available Channels

Channel	Details
Alexa	Alexa Channel
Communication Services - Chat	Communication Services - Chat Channel
Direct Line Speech	Direct Line Speech Channel
Email	O365 Email Channel
Facebook	Support for Text Messaging via Facebook
GroupMe	GroupMe Channel
LINE	Support for LINE Channel
Microsoft 365	Enable message extensions in Outlook, and Microsoft 365 apps
Microsoft Teams	Microsoft Teams Channel

STEP 5: Agree to the “**Terms of Service**” and click “**Agree**” to continue.



STEP 6: Select the Teams Messaging Option as per your Teams license. Click on “**Apply**” to enable the channel.

Create a New Client Secret ID (I)

STEP 7: Go to the search bar and search for **Microsoft Entra ID**. On the left panel, click on the "**APP REGISTRATION**".

The screenshot shows the Microsoft Azure portal with the following details:

- Left Sidebar (Manage Section):**
 - Overview
 - Preview features
 - Diagnose and solve problems
 - Users**
 - Groups
 - External Identities
 - Roles and administrators
 - Administrative units
 - Delegated admin partners
 - Enterprise applications
 - Devices
 - App registrations** (highlighted with a red box)
 - Identity Governance
 - Application proxy
 - Custom security attributes
 - Licenses
 - Cross-tenant synchronization
- Top Bar:** Microsoft Azure, Search resources, services, and docs (G+/)
- Page Title:** EverestIMS Technologies Pvt Ltd | Overview
- Header Actions:** Add, Manage tenants, What's new
- Overview Tab:** Overview (selected), Monitoring, Properties, Recom
- Search Bar:** Search your tenant
- Basic Information:**

Name	EverestIMS Technologies
Tenant ID	b7e0d1b1-1111-4444-8888-000000000000
Primary domain	everestims.com
License	Microsoft 365 Business Premium
- Alerts:**

Microsoft Entra Connect v1 Retirement

All version 1.x builds of Microsoft Entra Connect (formerly AAD Connect) will soon stop working between October 2023 – March 2024. You must move to Cloud Sync or Microsoft Entra Connect.

[Learn more](#)

STEP 8: Click on the “**OWNED APPLICATIONS**” and click on the [Infraon](#) to view the credentials.

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes 'Microsoft Azure' and a search bar. Below the navigation bar, the breadcrumb path 'Home > EverestIMS Technologies Pvt Ltd' is visible. The main title is 'EverestIMS Technologies Pvt Ltd | App registrations'. On the left, a sidebar titled 'Manage' lists various options like 'Users', 'Groups', 'External Identities', etc., with 'App registrations' being the active tab. The main content area displays a table of applications. The first application listed is 'Infraon' with a green icon, followed by 'Infraon_botid'. A red box highlights the 'Owned applications' tab in the table header. A red arrow points to this highlighted tab from below.

After clicking, this page can be visible.

This screenshot shows the detailed configuration page for the 'Infraon' application. The left sidebar includes 'Overview', 'Quickstart', 'Integration assistant', 'Manage', 'Branding & properties', 'Authentication', 'Certificates & secrets' (which is currently selected), 'Token configuration', 'API permissions', 'Expose an API', 'App roles', 'Owners', 'Roles and administrators', and 'Manifest'. The main content area displays the application's details under the 'Essentials' tab. It shows the display name 'Infraon', application ID, object ID, and directory (tenant) ID. Under 'Certificates & secrets', there is a note about the deprecation of ADAL and AAD. The 'Get Started' and 'Documentation' buttons are at the bottom of the sidebar.

STEP 9: On the left panel, click “**CERTIFICATES & SECRETS**”
Create a new secret -> Click certificate and secrets -> New Client Secret and copy the credentials.

[**Note:** Copy the value and keep it safe as the key gets hidden on refresh]

Certificates (0) Client secrets (2) Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value	Secret ID
secret	5/2/2024	Wo*****	[REDACTED]
No description	11/4/2025	bV*****	[REDACTED]

Create a New App Registration

STEP 10: Navigate to **Home > Microsoft Entra ID > New Registration**. In the search box panel, enter “**bot2-test2**”. You can select the required option.

The user-facing display name for this application (this can be changed later).

bot2-test2

Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (EverestIMS Technologies Pvt Ltd only - Single tenant)
- Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)
- Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- Personal Microsoft accounts only

Help me choose...

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but it's required for most authentication scenarios.

Select a platform (e.g. https://example.com/auth)

By proceeding, you agree to the Microsoft Platform Policies

Register

STEP 11: Once completing the registration, search for your new app registration ID in the “**OWNED APPLICATIONS**”

All applications Owned applications Deleted applications

bot2-test2

2 applications found

Application (client) ID	Created on	Certificates & secrets
[REDACTED]	12/4/2023	Current
[REDACTED]	12/4/2023	Current

STEP 12: Once the registrations are done, you can save the below keys in the overview section on the left panel.

The screenshot shows the 'Overview' tab of the Azure App registrations interface. It displays the application's details: Display name (bot2-test2), Application (client) ID, Object ID, Directory (tenant) ID, Client credentials (0.certificate_2.secret), Redirect URI (Add a Redirect URI), Application ID URI (Add an Application ID URI), and Managed application in ... (Create Service Principal). A note at the bottom states that starting June 30th, 2020, no new features will be added to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph, and that support for these services will end on November 9th, 2020.

Create a New Client Secret ID (II)

STEP 13: Once the previous step is completed, you can go back to “**CERTIFICATE & SECRETS**” -> Click on the “**NEW CLIENT SECRET**”

The screenshot shows the 'Certificates & secrets' tab of the Azure Certificates & secrets interface. It lists two client secrets: 'New client secret' (Description: test, Expires: 6/1/2024, Value: 1024***** and Secret ID: VMT*****). A note at the top indicates that certificates enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme).

STEP 14: Click “**ADD**” to proceed.

[**Note:** This value will be hidden on page refresh.]

The screenshot shows the Microsoft Azure portal interface for managing app registrations. In the left sidebar, under 'Manage', 'Certificates & secrets' is selected. On the right, the 'Client secrets' tab is active. A modal window titled 'Add a client secret' is open, showing a table with one row. The first column is 'Description', containing 'test'. The second column is 'Expires', showing '6/1/2024'. The third column is 'Value', containing 'XXXXXXXXXXXX'. Below the table are 'Description' and 'Expires' input fields, and a 'Value' input field with placeholder 'No description'. At the bottom of the modal are 'Add' and 'Cancel' buttons, with 'Add' highlighted by a red box.

Enable App Registration the permission to be a contributor for the bot.

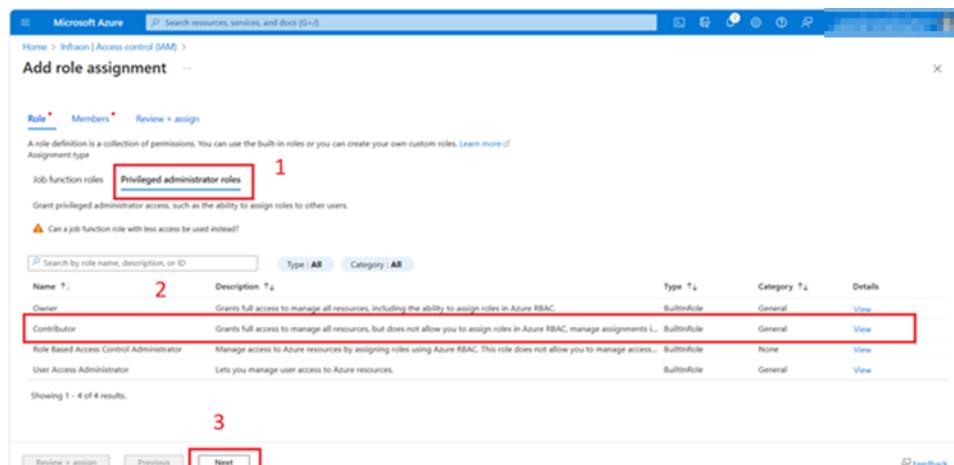
STEP 15: Navigate to **Bot Services > Your Bot**. On the left panel, click **Access Control (IAM)**.

The screenshot shows the Microsoft Azure portal interface for managing access control (IAM). In the left sidebar, 'Access control (IAM)' is selected. The main area has several sections: 'Check access' (with tabs for Role assignments, Roles, Deny assignments, and Classic administrators), 'My access' (with a 'View my access' button), 'Check access' (with a 'Check access' button), 'Grant access to this resource' (with a 'Add role assignment' button), 'View access to this resource' (with a 'View' button), and 'View deny assignments' (with a 'View' button). A red box highlights the 'Access control (IAM)' option in the sidebar.

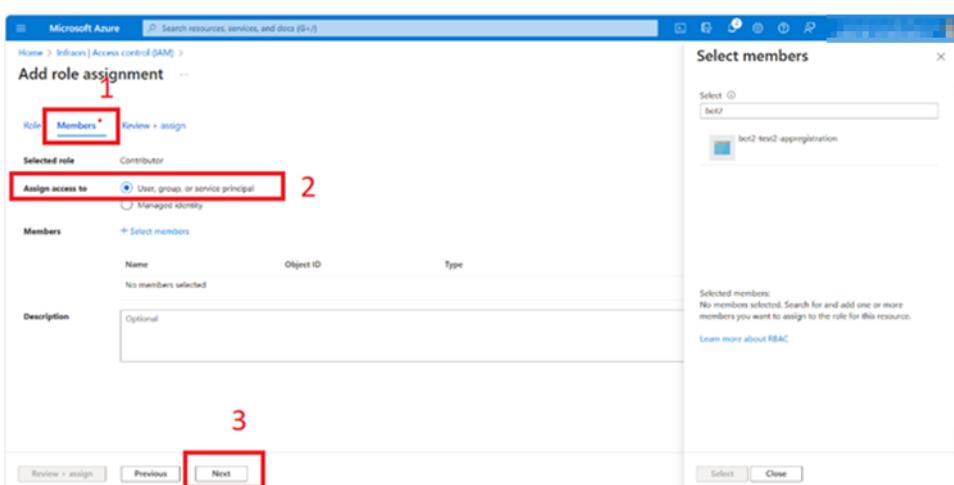
STEP 16: Click "Role Assignment"

This screenshot is identical to the previous one, showing the Microsoft Azure Access control (IAM) interface for the Infraon bot. The 'Access control (IAM)' option in the sidebar is highlighted with a red box. The main area shows the same sections: 'Check access', 'My access', 'Check access', 'Grant access to this resource' (with a 'Add role assignment' button highlighted by a red box), 'View access to this resource', and 'View deny assignments'.

STEP 17: Click **Privileged administrator roles**, click **Contributor role**, and Click > **NEXT**.



STEP 18: Now redirect to **Members** > **Select members to add mail ID**. Click **Next** to continue.



STEP 19: Once you've reviewed everything, click **Review + Assign** to complete the process.

Follow the above steps to create multiple channels to suit your requirements.

Adding Infraon Integration with Microsoft Teams

STEP 1: Log in to your [Infraon](#) account. On the left panel, click on the **Marketplace** tab. Select **Microsoft Teams integration**.

Marketplace > App Marketplace

Integrate your favorite apps to experience *infinity* possibilities with infraon



→ Demo ⏪ ⏩ 🔍

Infraon-Teams

Pull the requester from MS Teams and add/edit them into the INFRAON platform. Synchronize all modified data with these features.

Free

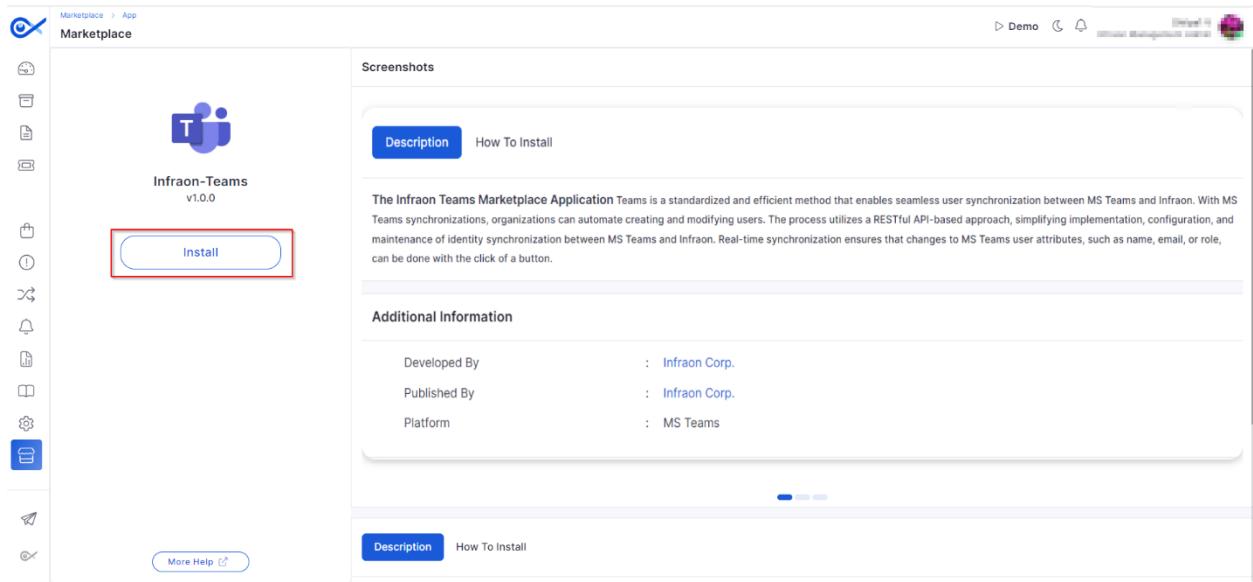
Infraon-Slack

Now redesigned to be smarter integrated app, stay at your slack workspace and still get connected with INFRAON platform.

Free

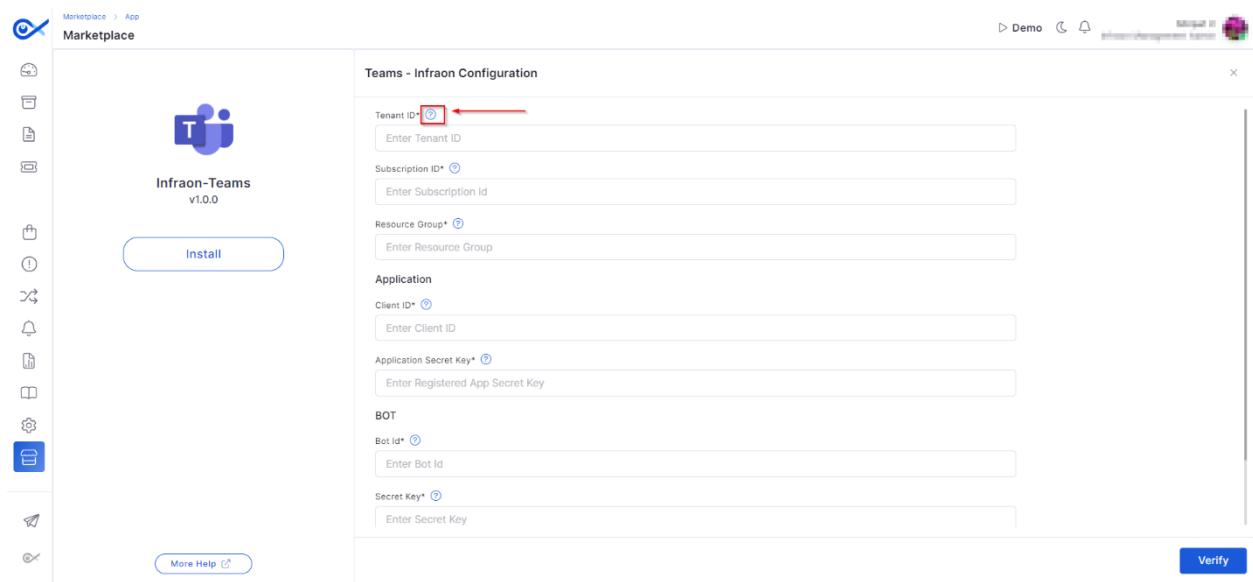
Marketplace

STEP 2: Click "**INSTALL**" to continue.

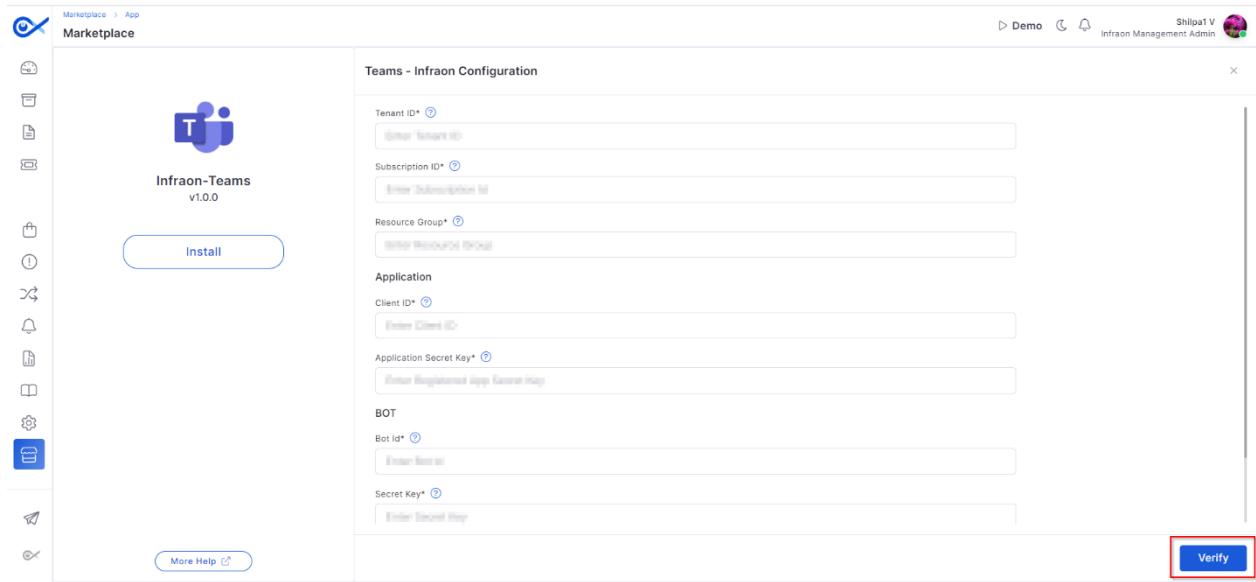


STEP 3: Enter the credentials in the following dialog boxes.

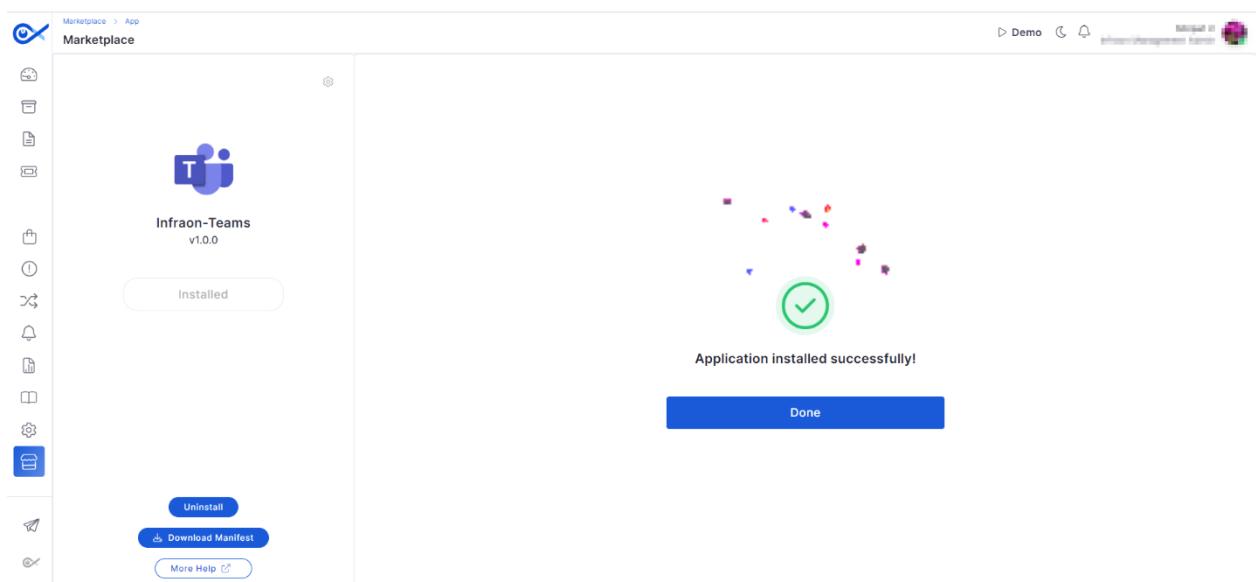
(**Note:** Click the button to learn more.)



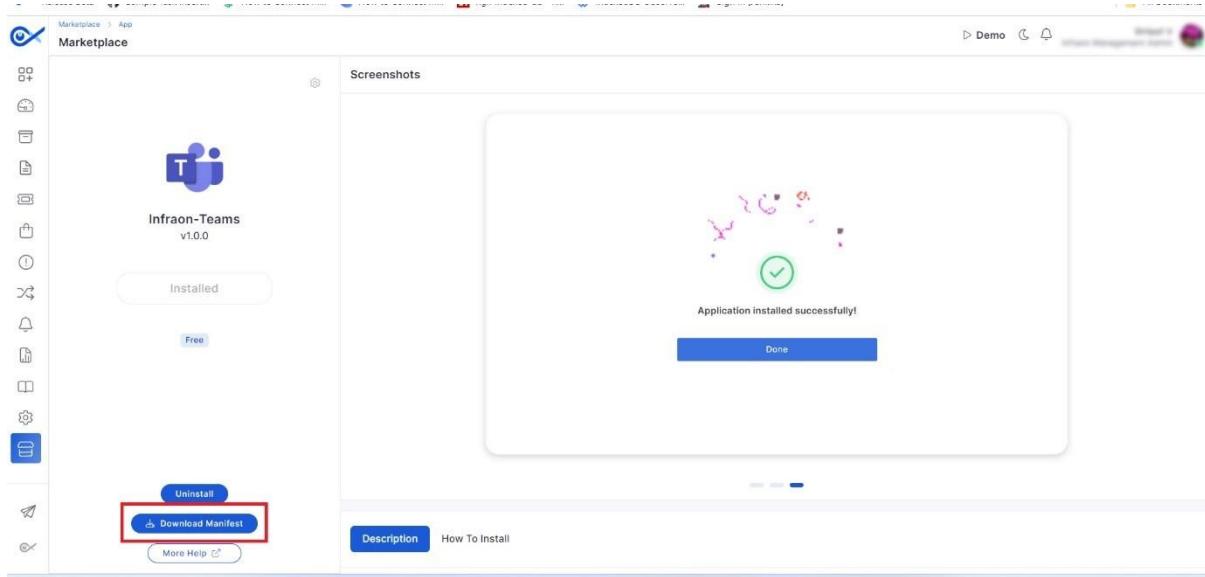
STEP 4: Once you have entered the credentials, click "**VERIFY**" to continue.



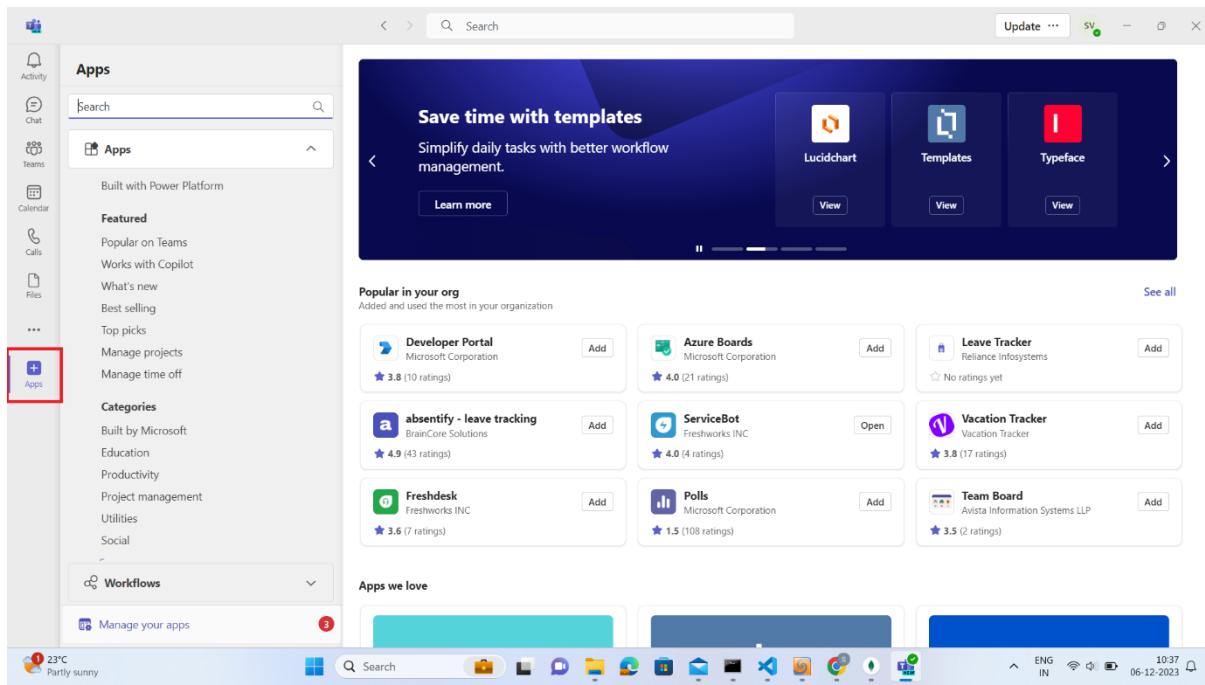
Once the installation is done, the below snip will be visible.



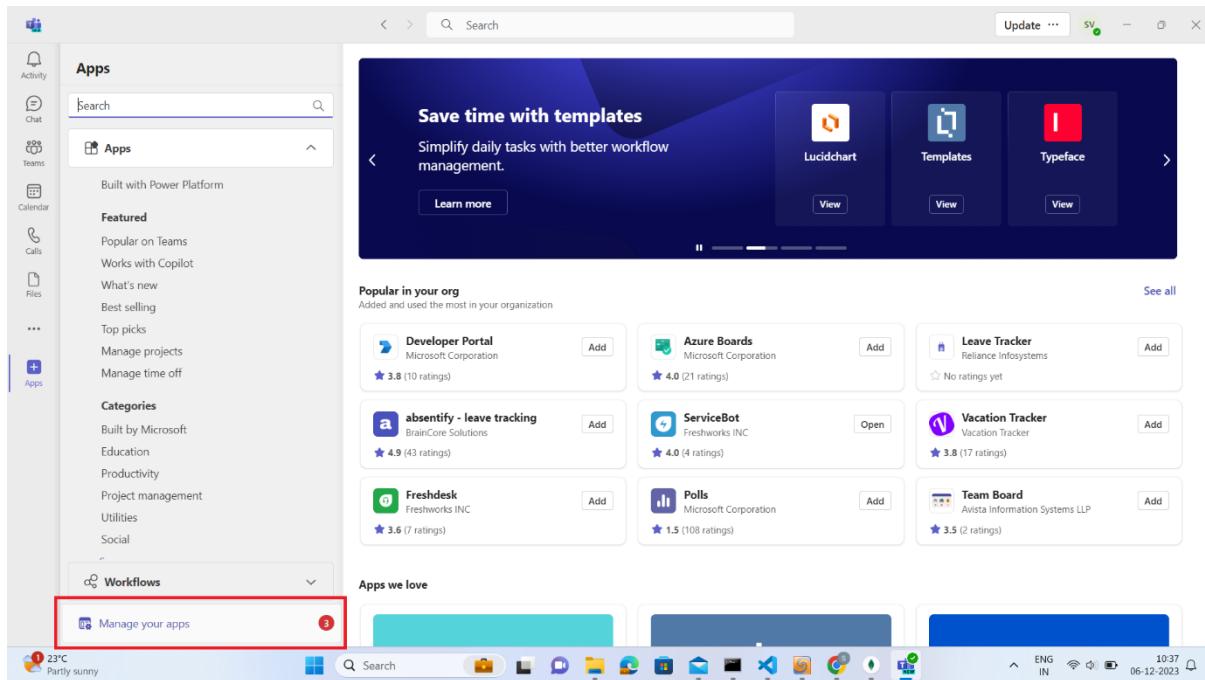
STEP 5: Now, download the “**MANIFEST**” file to add Infraon integration to your Microsoft Teams.



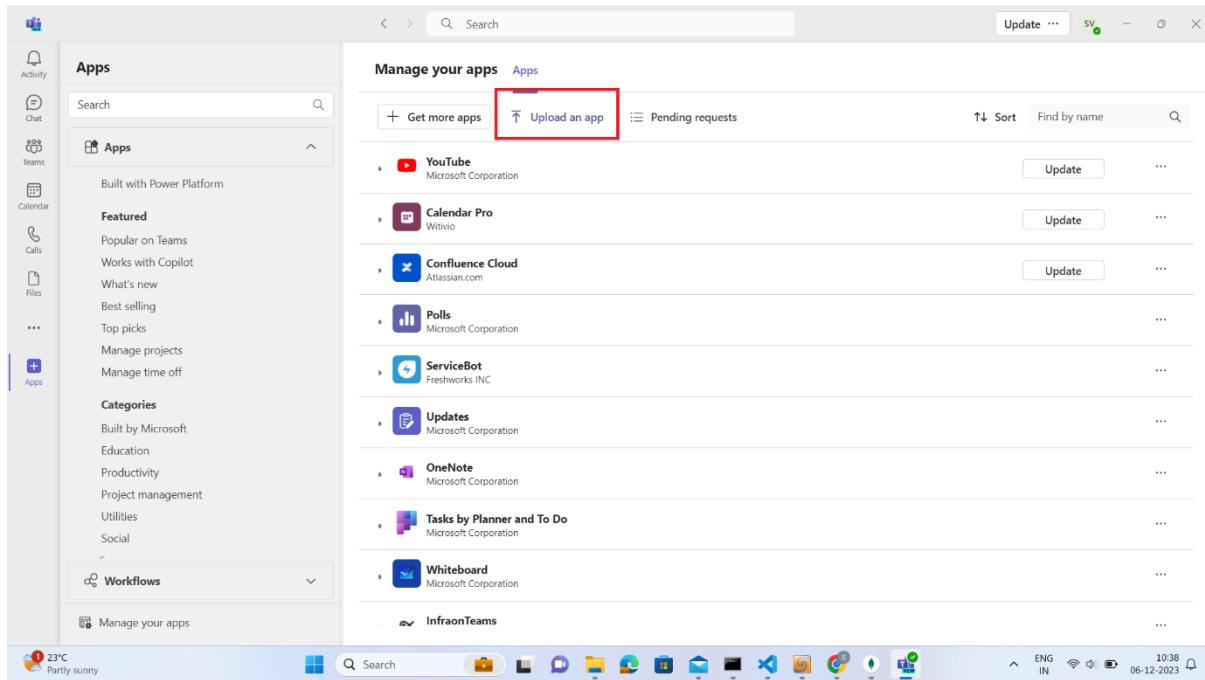
STEP 6: Go to Microsoft Teams. From the left panel, click “**APPS**.”



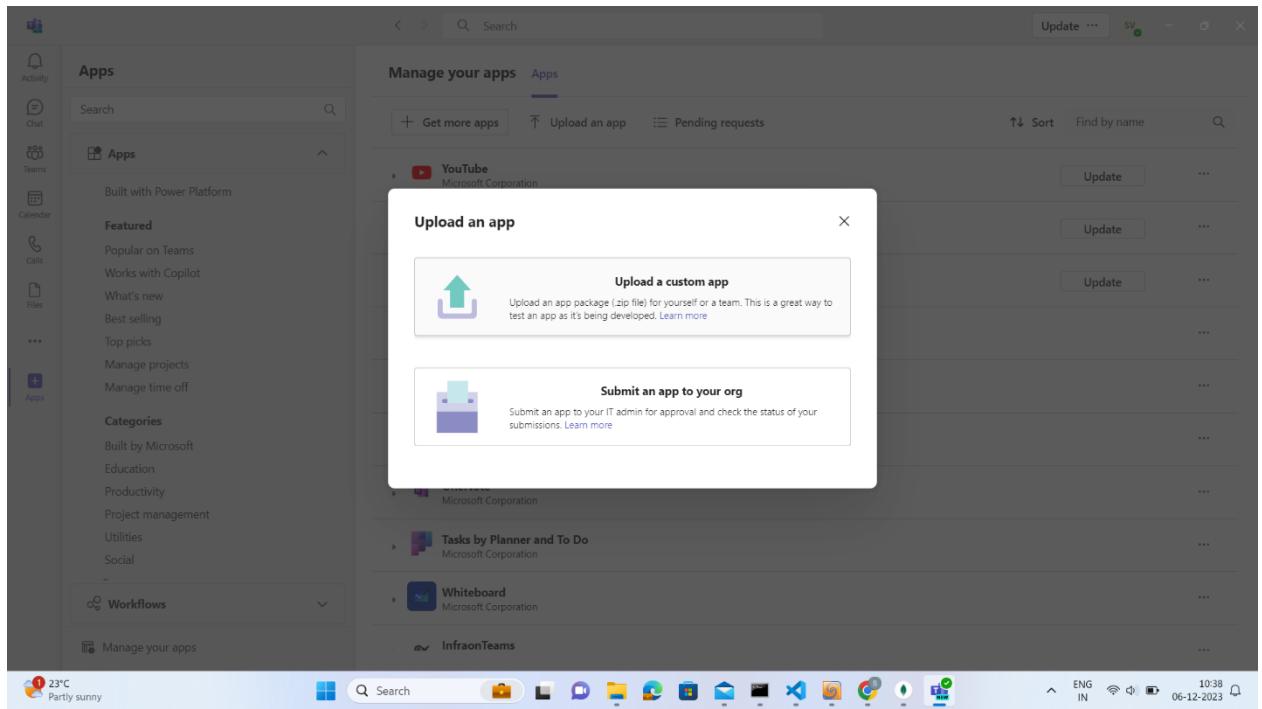
STEP 7: Click “**MANAGE YOUR APPS**” in the bottom left corner.



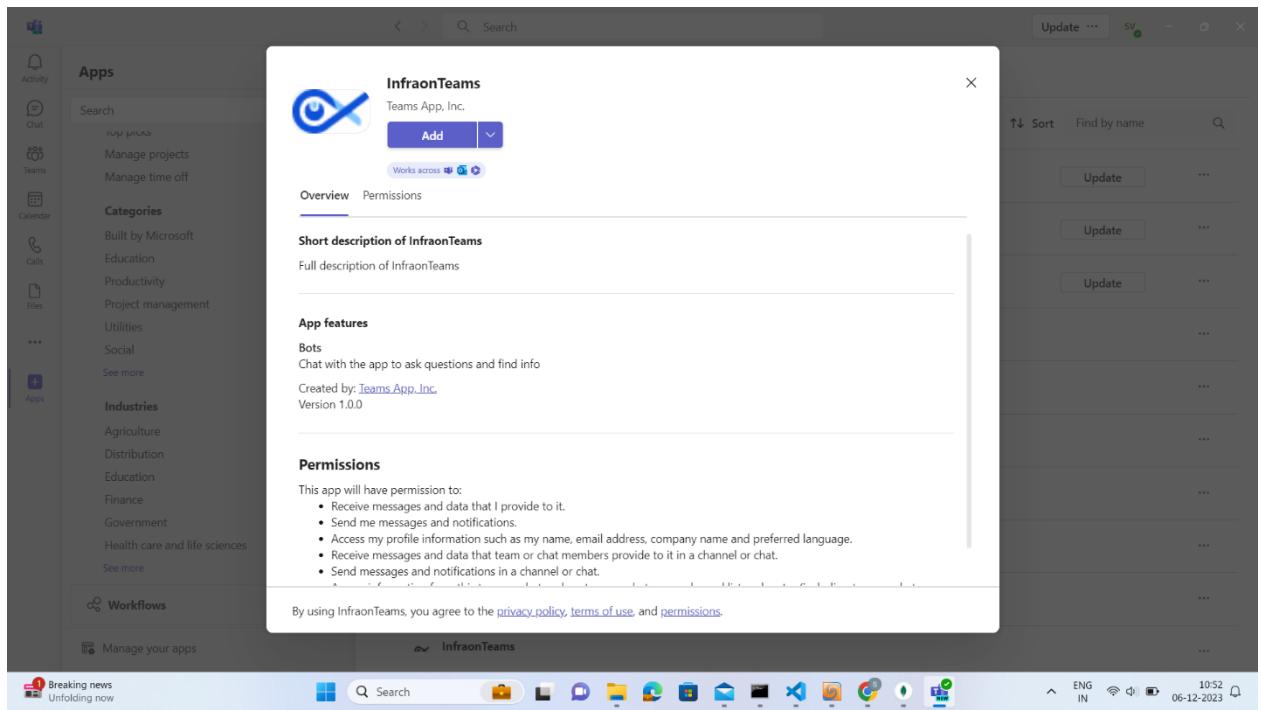
STEP 8: Click on “UPLOAD AN APP”



STEP 9: Click “UPLOAD CUSTOM APP” and upload the downloaded manifest file.



STEP 10: Once you select the required manifest file, click “**ADD**” to proceed.



The process is now completed.

Infraon WhatsApp

Description

The Infraon-WhatsApp application eliminates complexity by offering a unified IT support platform. Users can simply report their issues via WhatsApp chat, eliminating the need to navigate different systems or make time-consuming phone calls.

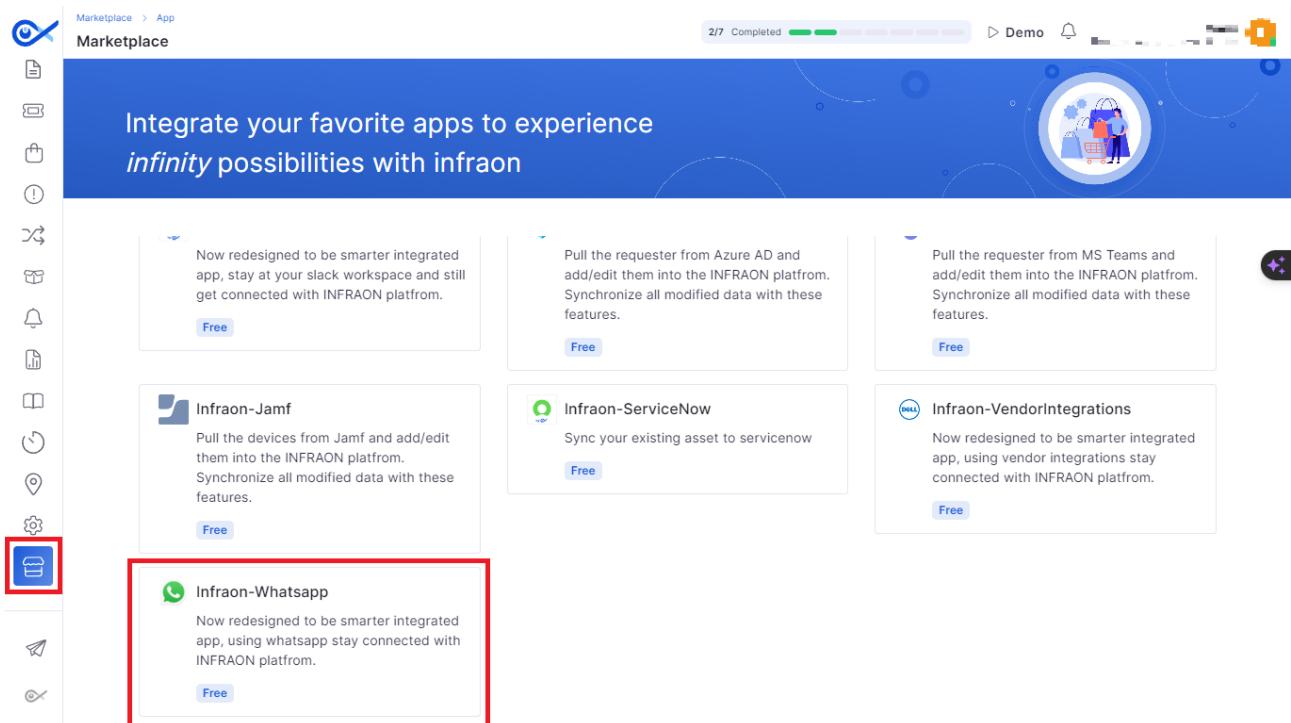
You can now:

- Create tickets
- Create requests
- View ticket detail
- Real-time updates on status changes

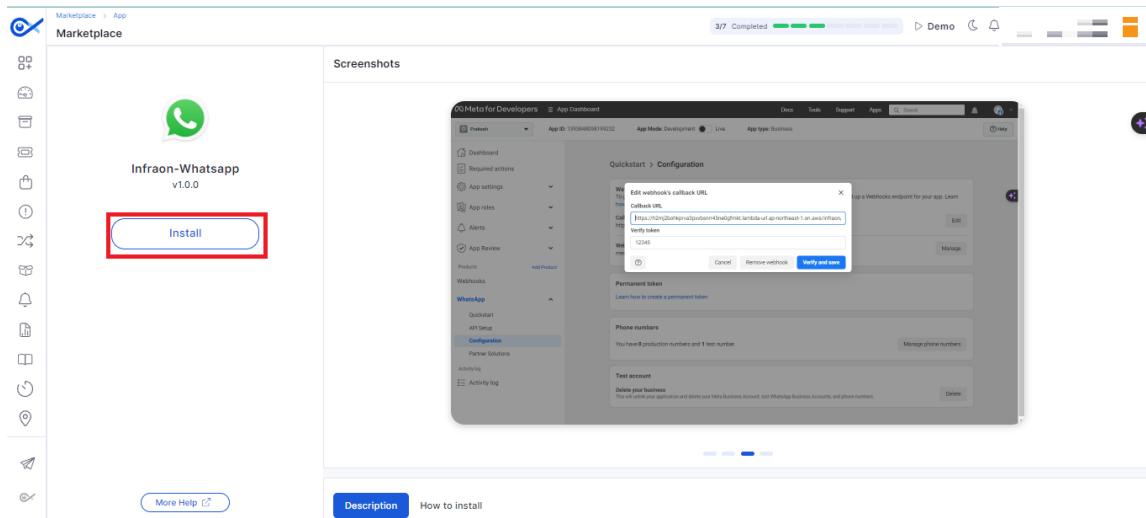
How To Install

Installing the app

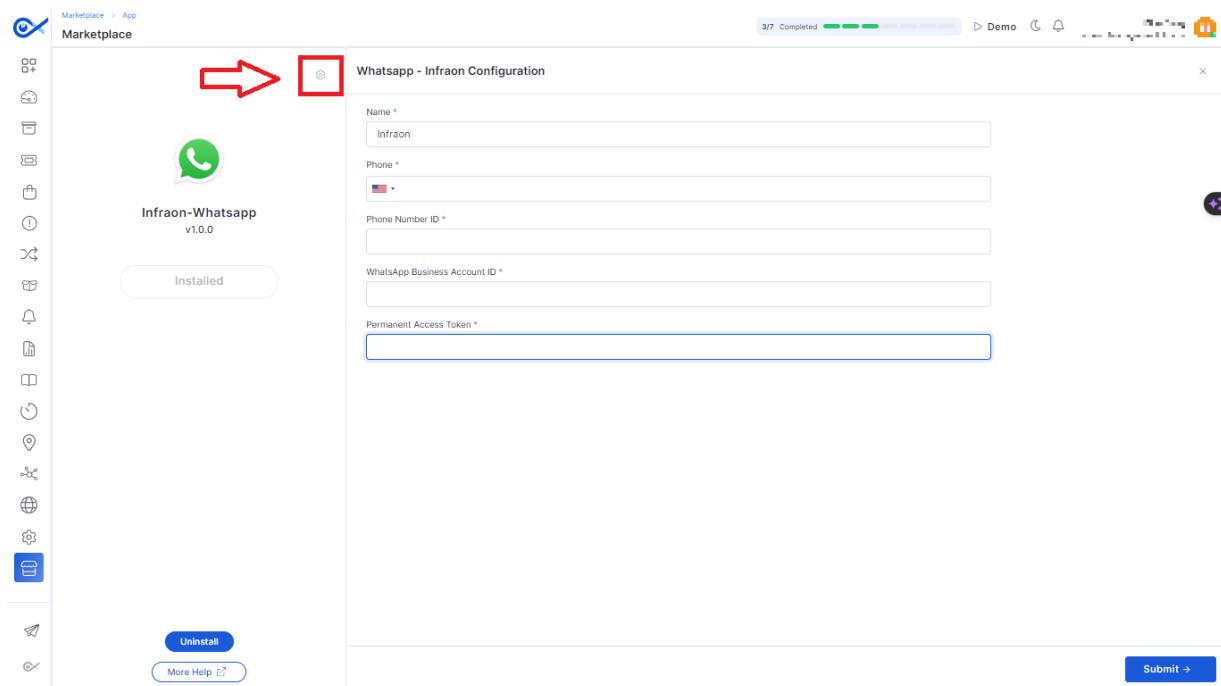
STEP 1: Log in to your Infraon account. On the left panel, click on the **Marketplace** tab. Select the "**Infraon-WhatsApp**" integration.



STEP 2: After clicking the tab, click Install.



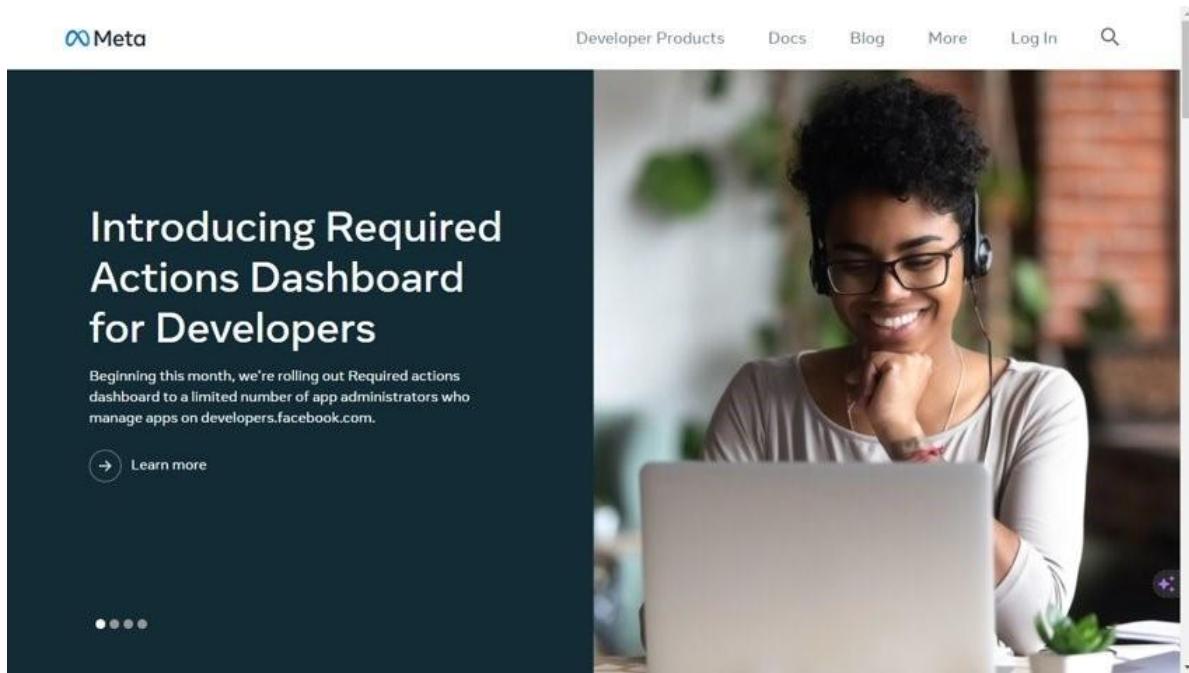
Step 3: Once the installation is done, click on the WhatsApp-Infraon configuration tab.



Enter the credentials as prompted - Enter the Name, **Phone Number**, Phone Number ID, **WhatsApp Business Account ID**, and **Permanent Access Token**. Follow the below steps to get the required information.

Create an App

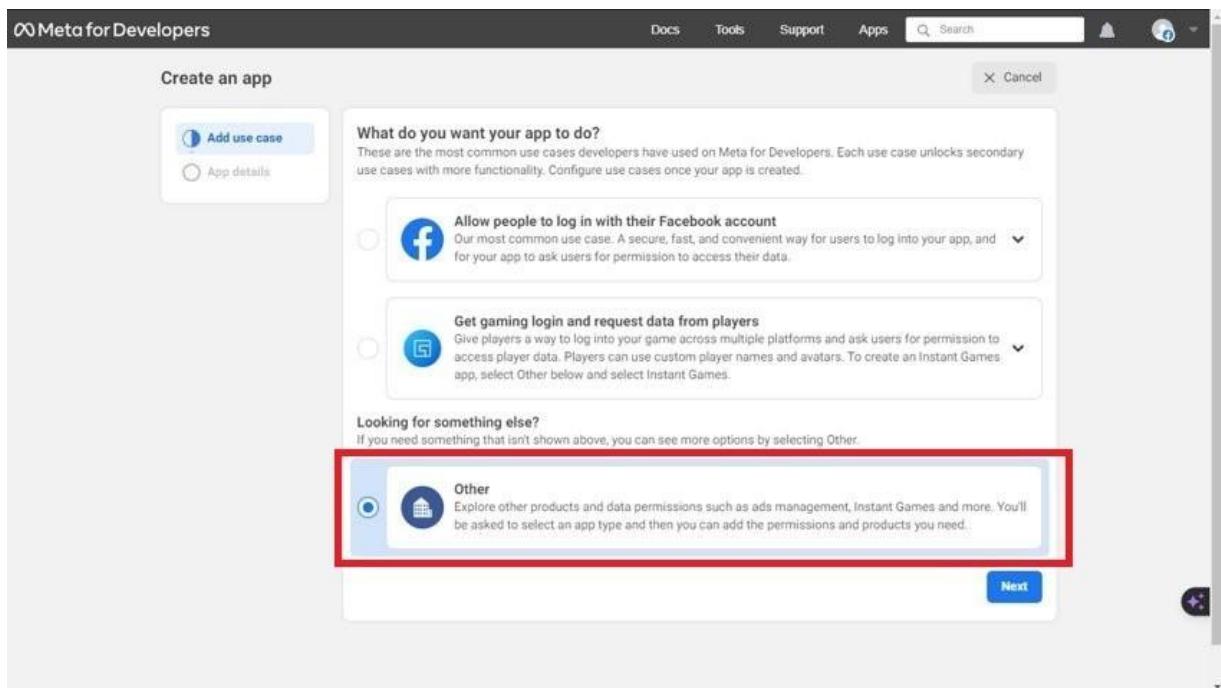
STEP 3.1: Log onto [Meta Business Platform](#) using a Facebook or Instagram account.



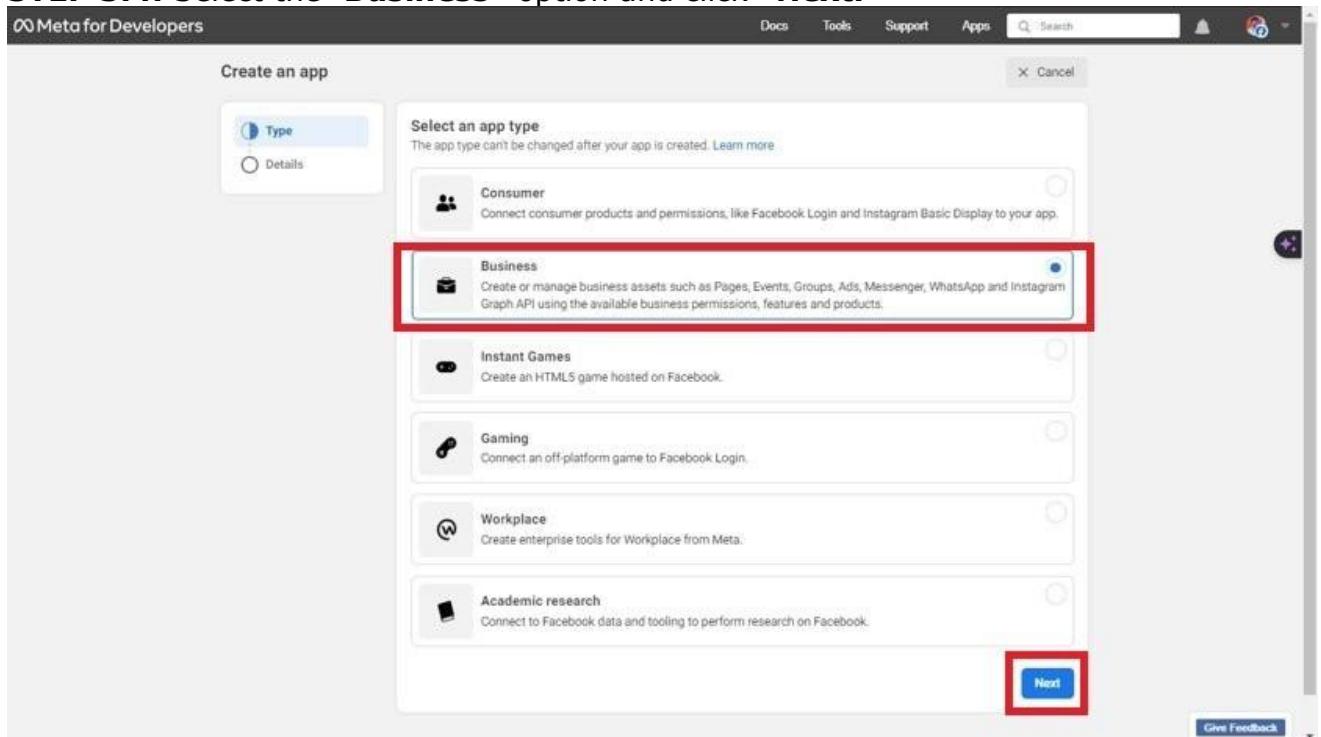
STEP 3.2: Once logged in, on the top panel, click “**Apps**,” and then click on the “**Create App**” tab.

This screenshot shows the 'Apps' section of the Meta for Developers website. At the top, there's a navigation bar with 'Docs', 'Tools', 'Support', and 'Apps' (which is highlighted with a red box and a circled '1'). Below that is a search bar with a 'Search' button and a 'Create App' button (also highlighted with a red box and a circled '2'). The main area shows a list of apps, with one named 'Infraon' selected. On the left, there's a filter sidebar with options like 'All Apps (2)', 'Archived (1)', and 'Required actions'. At the bottom, there's a footer with the Meta logo, social media links ('Follow Us'), and various links for 'Products', 'Programs', 'News', 'Support', and 'Terms and Policies'.

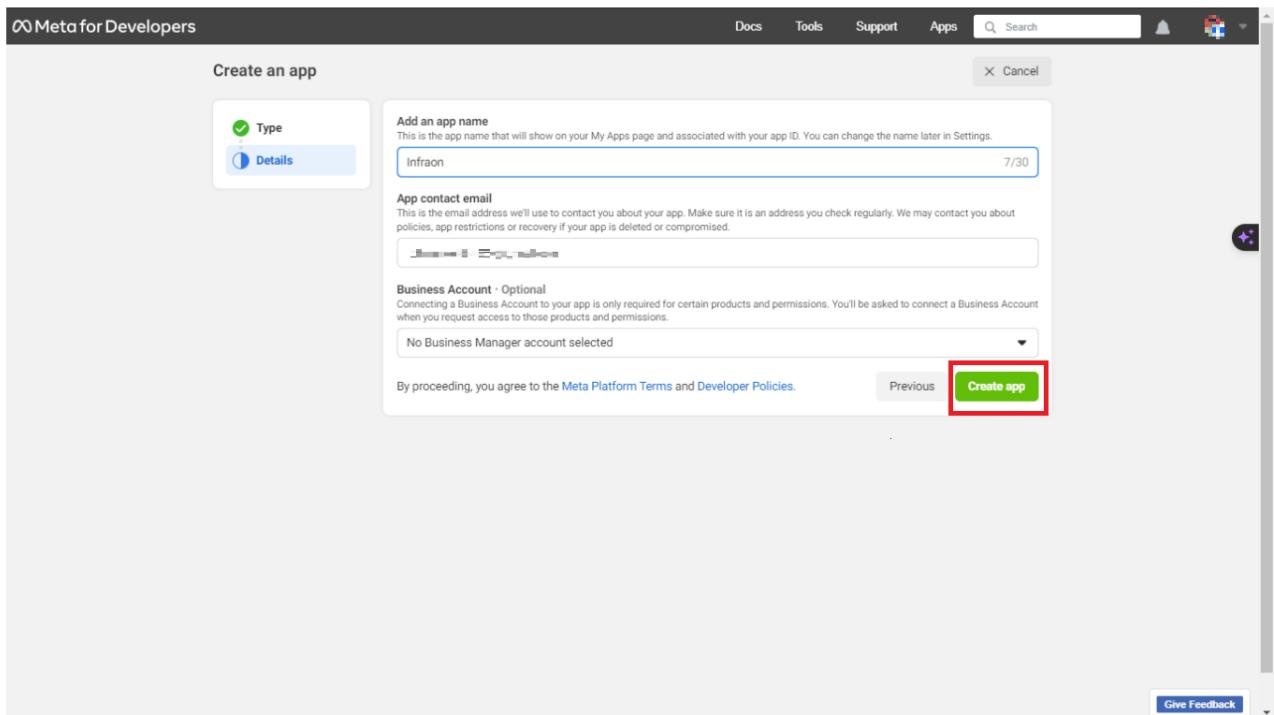
STEP 3.3: Select “**Other**” and continue by clicking “**Next.**”



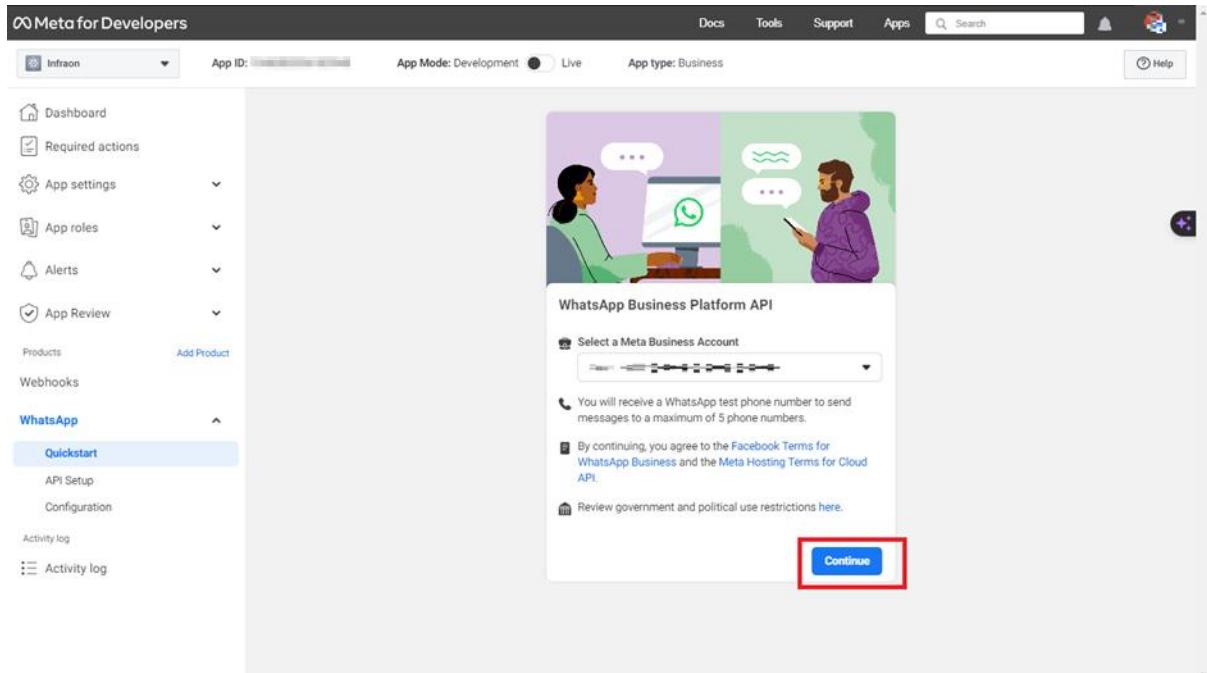
STEP 3.4: Select the “Business” option and click “Next.”



STEP 3.5: Now enter the required credentials (Name and email address) in the dialog box, and click “Create App.”

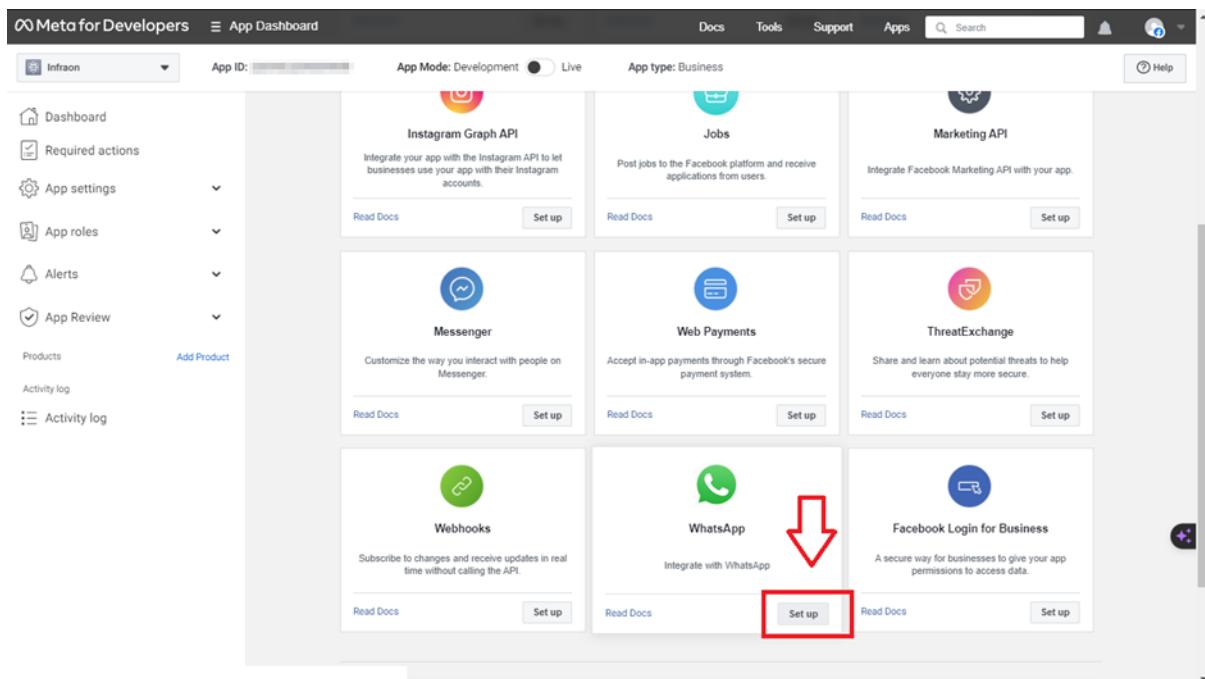


Once done, the below notification pops up. Click "**Continue**" to proceed.



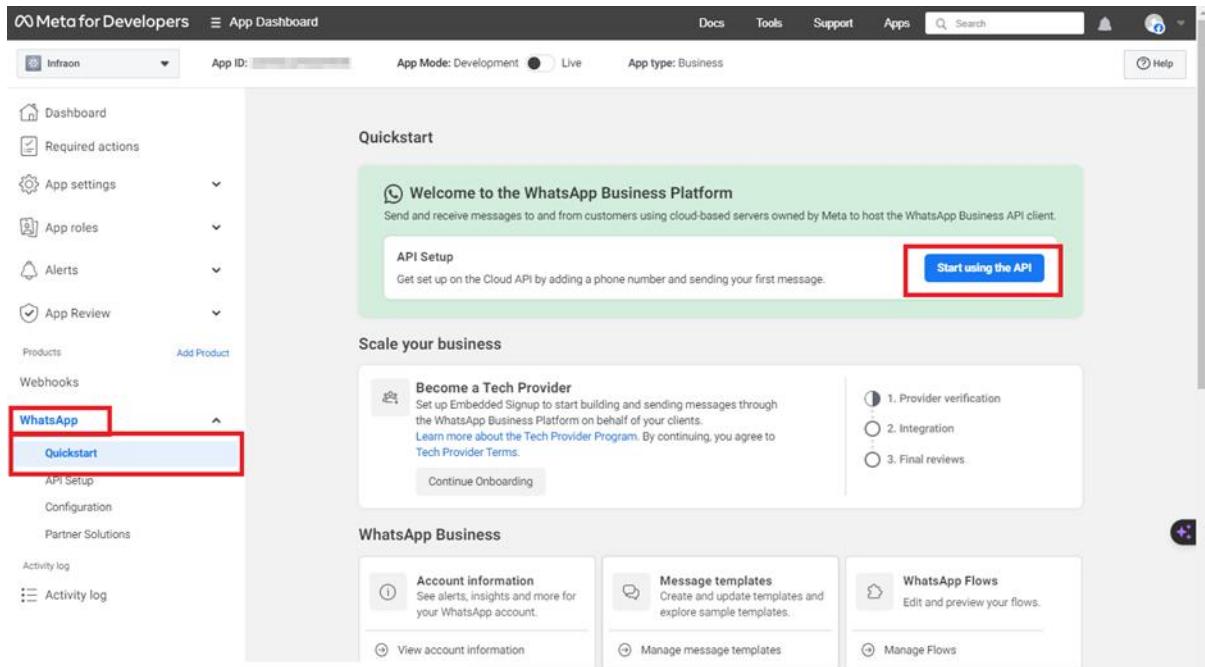
Enable API permissions

STEP 3.6: Once the app is created, click "**WhatsApp > Set up.**"



Follow the steps carefully:

STEP 3.7: Select “WhatsApp > Quick Start” on the left panel to set up the API. Click on the “Start Using the API” tab to continue.



Follow the necessary steps to complete the setup.

STEP 3.8: Copy the Phone Number ID and WhatsApp Business Account ID and paste them on STEP 3.

The screenshot shows the Metafor Developers App Dashboard with the 'API Setup' tab selected. On the left sidebar, under the 'WhatsApp' section, 'API Setup' is highlighted. In the main content area, there's a 'Temporary access token' section with a copy button and a note about expiration. Below it is a 'Send and receive messages' section. Under 'Step 1: Select phone numbers', there are fields for 'From' (Test number: +1 555 013 4677) and 'To' (Select a recipient phone number). The 'Phone number ID' and 'WhatsApp Business Account ID' fields are highlighted with a red border and a red arrow points to them. At the bottom, there's a terminal window showing a curl command for sending a message.

(NOTE: We will not copy the temporary access token because this is only valid for the first 24 hours, we will generate a permanent token number in the following steps.)

Generating Permanent Token Number

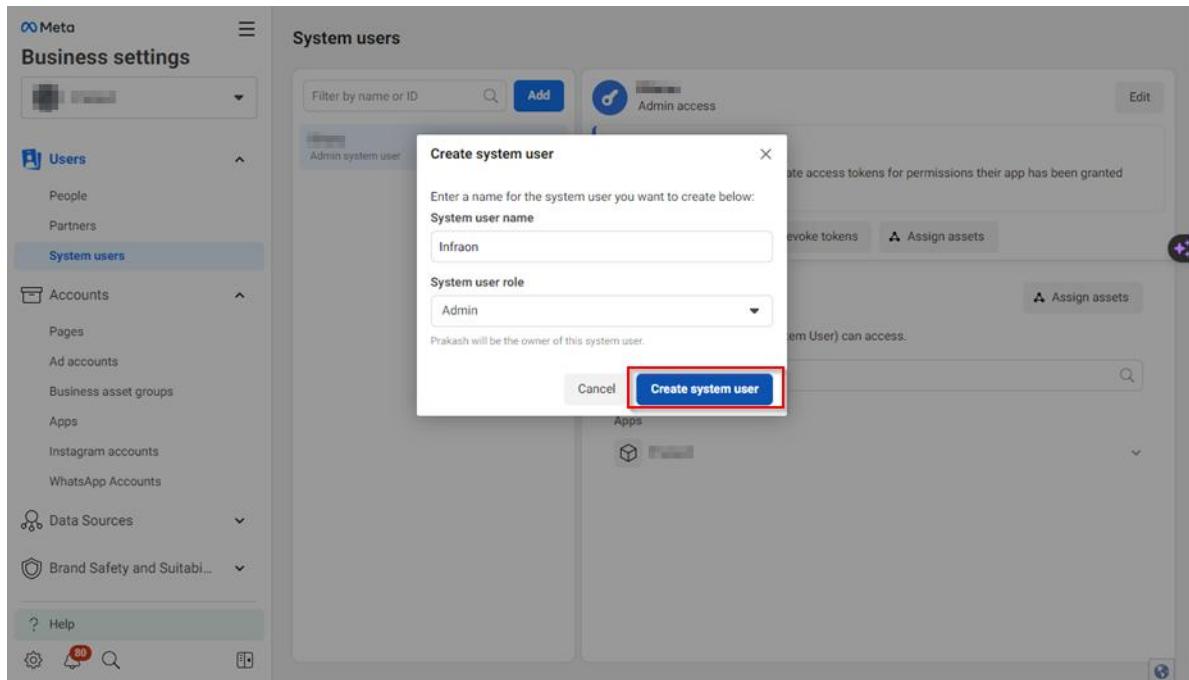
STEP 3.9: Go to "STEP 3.2" and click on the **business name** in blue colored, created earlier.

The screenshot shows the Meta for Developers Apps dashboard. On the left, there's a sidebar with filters for 'All Apps (2)', 'Archived (1)', and 'Required actions'. Below that is a 'Business Account' dropdown set to 'No Business Account selected'. The main panel displays the 'Infrastructure' app details. A red arrow points to the 'Business' field, which is currently set to 'Personal'. Other details shown include App ID: 3286522900C9E95, Mode: In development, and Type: Business.

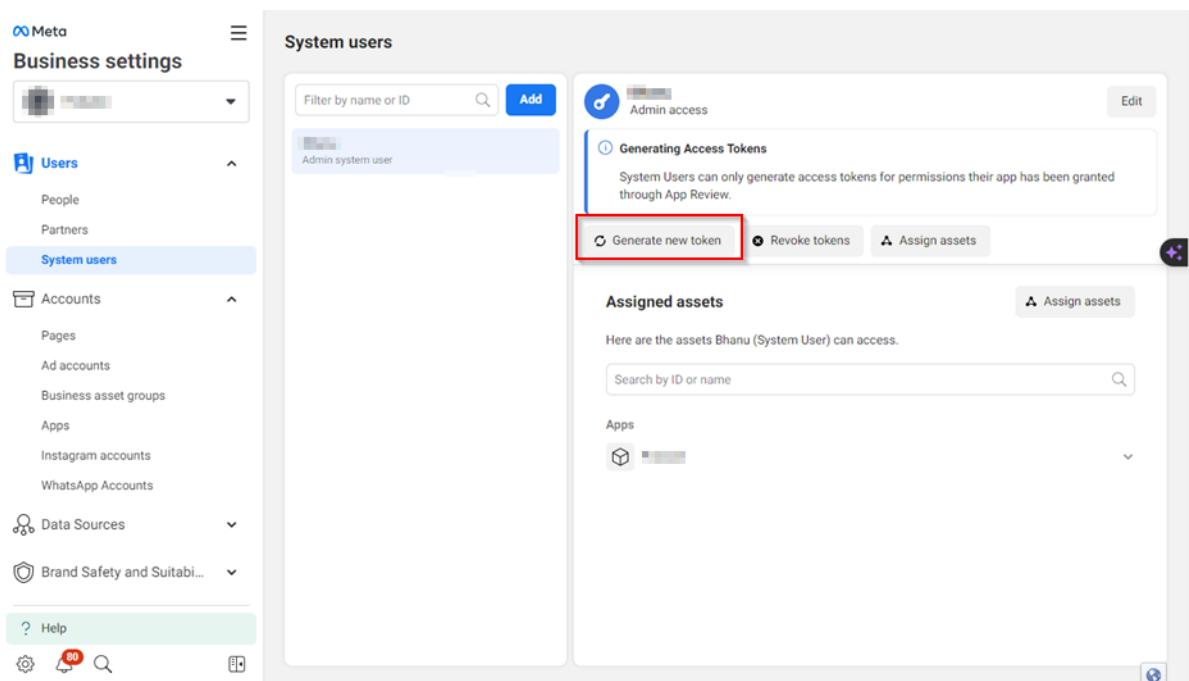
STEP 3.10: On the left panel, select “**System Users**” and click “**Add**” to continue.

The screenshot shows the Meta Business settings interface. On the left, under 'Users', the 'System users' option is highlighted with a red box and labeled '1'. On the right, the 'System users' page is displayed. The 'Add' button is highlighted with a red box and labeled '2'. The page also shows an 'Admin access' section and a 'Generating Access Tokens' section. On the far right, there's an 'Assigned assets' section with a 'Search by ID or name' input field.

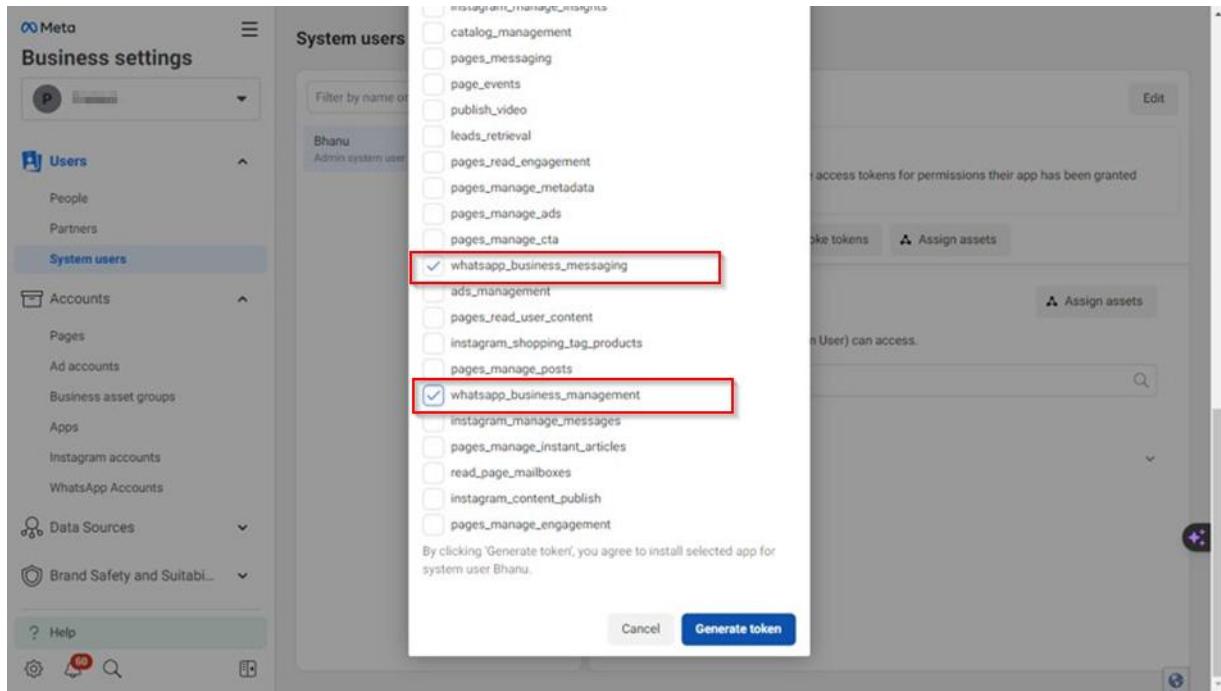
STEP 3.11: Enter the name of your “**System user**” and Click “**Select User Role > Admin.**”
Click “**Create System User**” to continue.



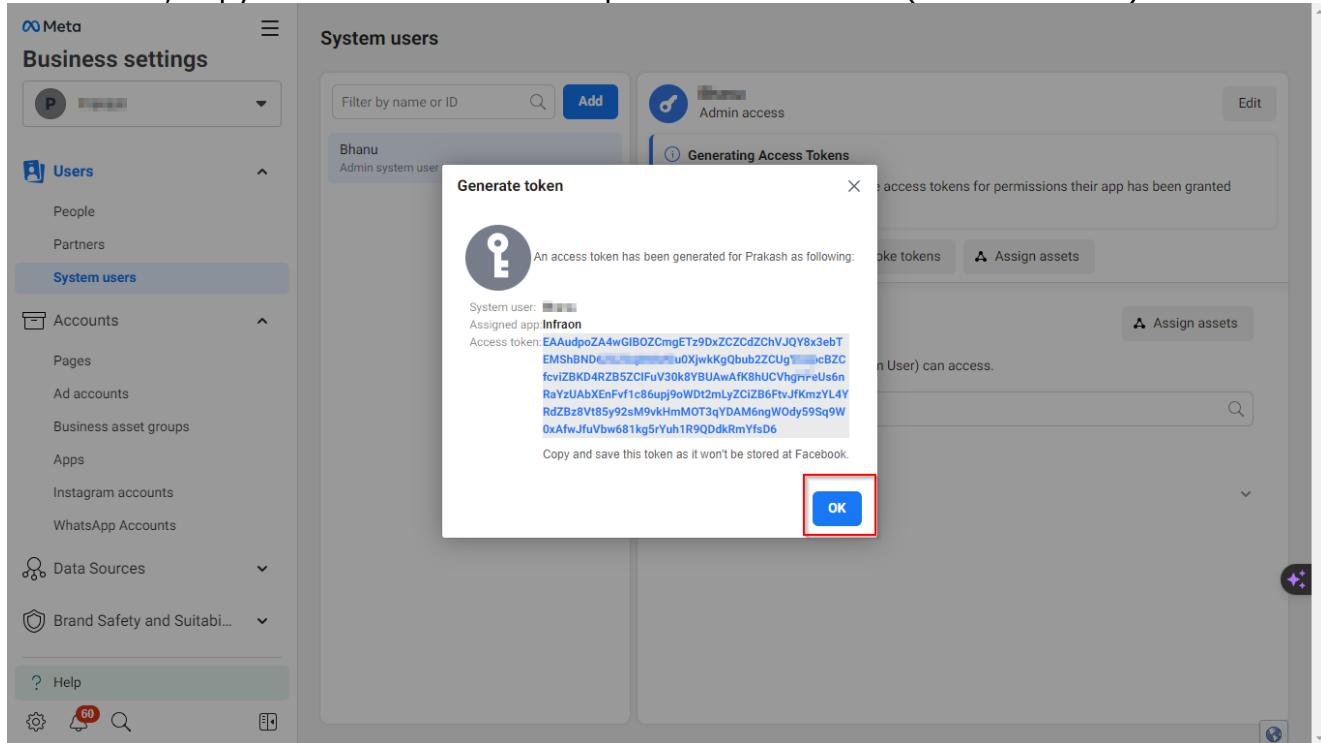
STEP 3.12: Click on the "Generate New Token"



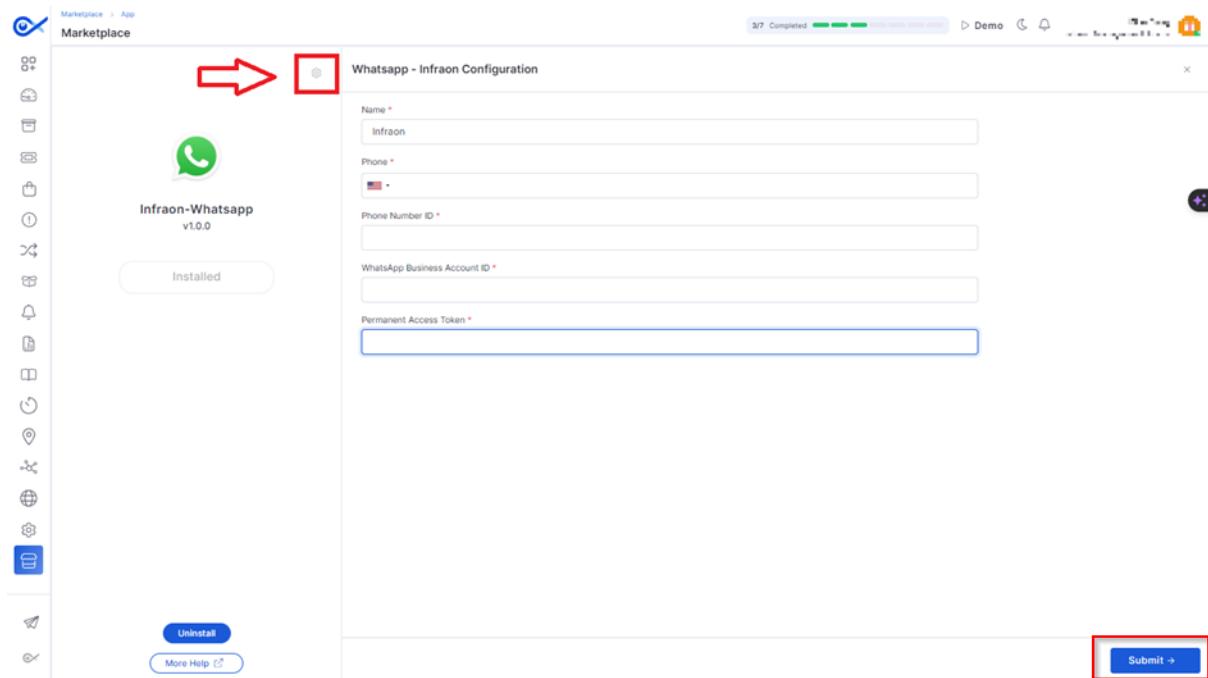
STEP 3.13: Tick the "whatsapp_business.messaging" and "whatsapp_business.management" and click "Generate Token."



Once done, copy the token number and paste it into **STEP 3** (refer to above).

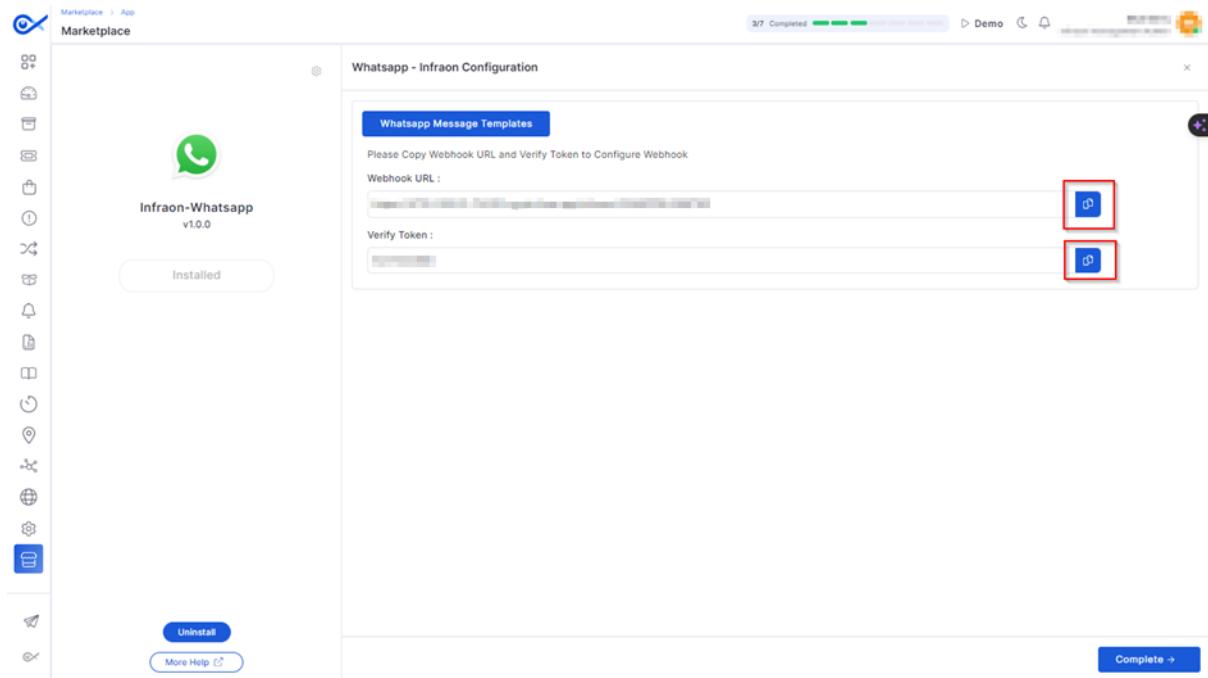


STEP 4: Once you have entered the credentials, continue by clicking on the “Submit”.



Configuring the webhooks

STEP 5: Copy the “**Webhook URL**” and “**Verify Token**” and go to “**STEP 3.8.**”



STEP 5.1: Click on the “**Configure webhooks**”

The screenshot shows the Meta for Developers App Dashboard. On the left, there's a sidebar with options like Dashboard, Required actions, App settings, App roles, Alerts, App Review, Products, Webhooks, WhatsApp, Quickstart, API Setup (which is selected), Configuration, and Partner Solutions. The main area has tabs for Docs, Tools, Support, Apps, and Help. The App Mode is set to Development (Live) and the App type is Business. A code editor window shows a JSON message template for WhatsApp. Below it, there are sections for Step 3: Configure webhooks to receive messages (with a red box around the 'Configure webhooks' button), Step 4: Learn about the API and build your app, Step 5: Add a phone number (with a red box around the 'Add phone number' button), and Step 6: Add payment method (with a red box around the 'Add payment method' button).

STEP 5.2: Click “**Edit**” and paste the “**Callback URL**” and “**Verify token**” from *STEP 5*.

“**Click Verify and Save**” to proceed.

The screenshot shows the Meta for Developers App Dashboard with the Configuration tab selected in the sidebar. A modal window titled "Edit webhook's callback URL" is open. It contains fields for "Callback URL" (with a value of "https://eims.com.ng/api/v1/webhook") and "Verify token" (with a value of "TestNotification123456"). There are "Edit" and "Cancel" buttons, and a prominent "Verify and save" button which is highlighted with a red box. Below the modal, there are sections for "Permanent token", "Phone numbers", and a "Manage phone numbers" button.

STEP 5.3: Click on “**Webhook fields > Manage**.”

The screenshot shows the Meta for Developers App Dashboard under the 'Configuration' tab. On the left sidebar, 'WhatsApp' is selected. In the main area, the 'Webhook' section is displayed. A red box highlights the 'messages' field in the 'Webhook fields' list. Below it, the 'Permanent token' and 'Phone numbers' sections are shown. At the bottom, there's a 'Test account' section with a 'Delete your business' link.

STEP 5.4: Select “Messages” toggle and click “Done” to continue.

This screenshot shows the 'Webhook fields' configuration dialog from the previous step. The 'messages' row is highlighted with a red box. The 'Subscribe' checkbox next to it is checked. In the bottom right corner of the dialog, a 'Done' button is highlighted with a red box.

Verify your personnel details

STEP 5.5: Proceed with “Step 5” by clicking the “Add phone number” tab.

The screenshot shows the Meta for Developers App Dashboard. On the left, there's a sidebar with options like Dashboard, Required actions, App settings, App roles, Alerts, App Review, Products, Webhooks, WhatsApp (selected), Quickstart, API Setup (selected), Configuration, and Partner Solutions. The main area has tabs for Docs, Tools, Support, Apps, and Help. The search bar at the top right contains the text "Search". The central content area is titled "Step 5: Add a phone number". It includes a code snippet for a WhatsApp message template, a "Run in Postman" button, and a "Send message" button. Below this, there are sections for Step 3 (Configure webhooks), Step 4 (Learn about the API and build your app), Step 5 (Add a phone number, with a red box around the "Add phone number" button), and Step 6 (Add payment method). A "Help" icon is located in the bottom right corner of the main content area.

STEP 5.6: Enter your “Business name”, “Business Website” and “Country” and click “Next”.

This screenshot shows the "Add phone number" step in the Meta for Developers App Dashboard. The sidebar and top navigation are identical to the previous screenshot. The main content area now displays a modal dialog titled "Fill in your business information". It contains three fields: "Business name" (set to "Infraon", highlighted with a red box), "Business website or profile page" (set to "https://infraon.io/", highlighted with a red box), and "Country" (set to "United States", highlighted with a red box). Below the modal, the "Next" button is also highlighted with a red box. The background shows the steps 5 and 6 of the setup process.

STEP 5.7: Once done, verify your Phone number by Text message or phone call.

Click “Next” to continue.

To send a test message, copy this command, paste it into Terminal, and press enter. To create your own message template, click [here](#).

```
1 curl -X POST
2 https://graph.facebook.com/v17.0/172261879297998/messages
```

Add phone number

This is the number people will see when they chat with you. [Learn how to use a number that's already on WhatsApp](#).

Phone number

US +1

You'll receive a code to verify this number.

Choose how you would like to verify your number:
If you are using a landline number, choose phone call.

Text message Phone call

[Back](#) [Next](#)

Add Payment Method

STEP 5.8: Now click on the “**Add Payment Method**”.

Review the developer documentation to learn how to build your app and start sending messages. [See documentation](#).

Step 5: Add a phone number

To start sending messages to any WhatsApp number, add a phone number. To manage your account information and phone number, [see the Overview page](#).

[Add phone number](#)

Step 6: Add payment method

Add a payment method to send business-initiated messages to your customers. After you use 1000 free user-initiated conversations each month, you will also need to have a payment method.

[Add payment method](#)

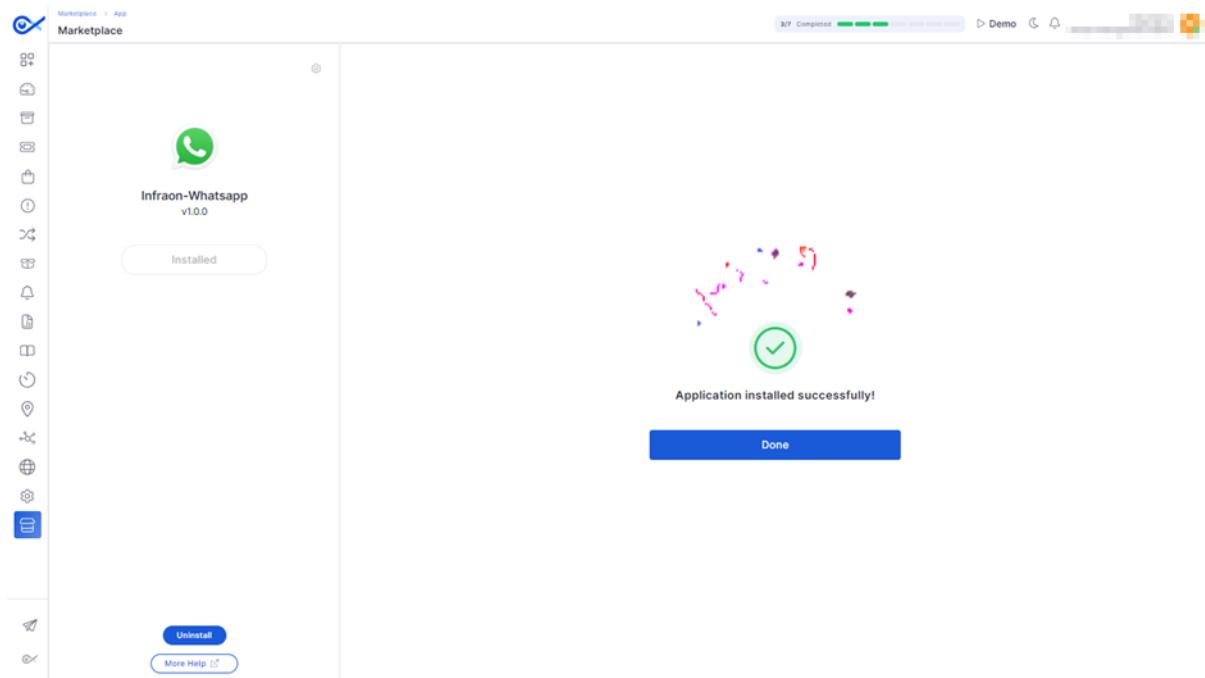
STEP 5.9: Enter the required details for your payment mode by clicking “Add.”

The screenshot shows the "WhatsApp Accounts" section within the "Business settings" of the Meta Business Center. On the left, there's a sidebar with "Accounts" selected. The main area displays a "Test WhatsApp Business Account" card with basic information like "Owned by" and "Remove" options. Below the card, tabs for "People", "Settings", and "Pages" are visible, with "Settings" currently selected. Under "Business information", fields for "Tax ID number", "Address", "Currency", "Time Zone", "Business name", and "Business verification" (status "In progress") are listed. A "Payment method" section is also present.

STEP 6: Once all the steps for the API Setup are completed, go to *STEP 5* and click “Complete.”

The screenshot shows the "Infraon-WhatsApp v1.0.0" app configuration page in the Marketplace. The left sidebar has various icons. The main panel shows the app logo and status "Installed". It includes fields for "Name", "Phone", "Phone Number ID" (with value "1147XXXX5066816"), "WhatsApp Business Account ID" (with value "0763XXXX6066746"), and "Permanent Access Token". At the bottom right is a red-bordered "Submit" button.

The Infraon-WhatsApp integration is now complete!!



Infraon Ring Central

Description

The Infraon Ring Central marketplace integration creates a seamless connection between the requester and the technicians while resolving tickets. This will be achieved through a cloud-based communication system that will combine calling features with collaboration tools, allowing for faster issue resolution and ultimately leading to faster issue resolution for customers.

How to Install

STEP 1: Installing the integration

STEP 1.1: Log in to your Infraon account. On the left panel, click on the Marketplace tab and select “**Ring Central**” integration.

Getting Started

Integrate your favorite apps to experience infinity possibilities with infraon

Azure AD

Slack

VendorIntegrations

Teams

WhatsApp

Jamf

GoogleWorkspace

RingCentral

RingCentral combines phone, video, messaging, and contact center, streamlining business communication with AI analytics and app integrations.

STEP 1.2: After clicking the tab, click on Install.

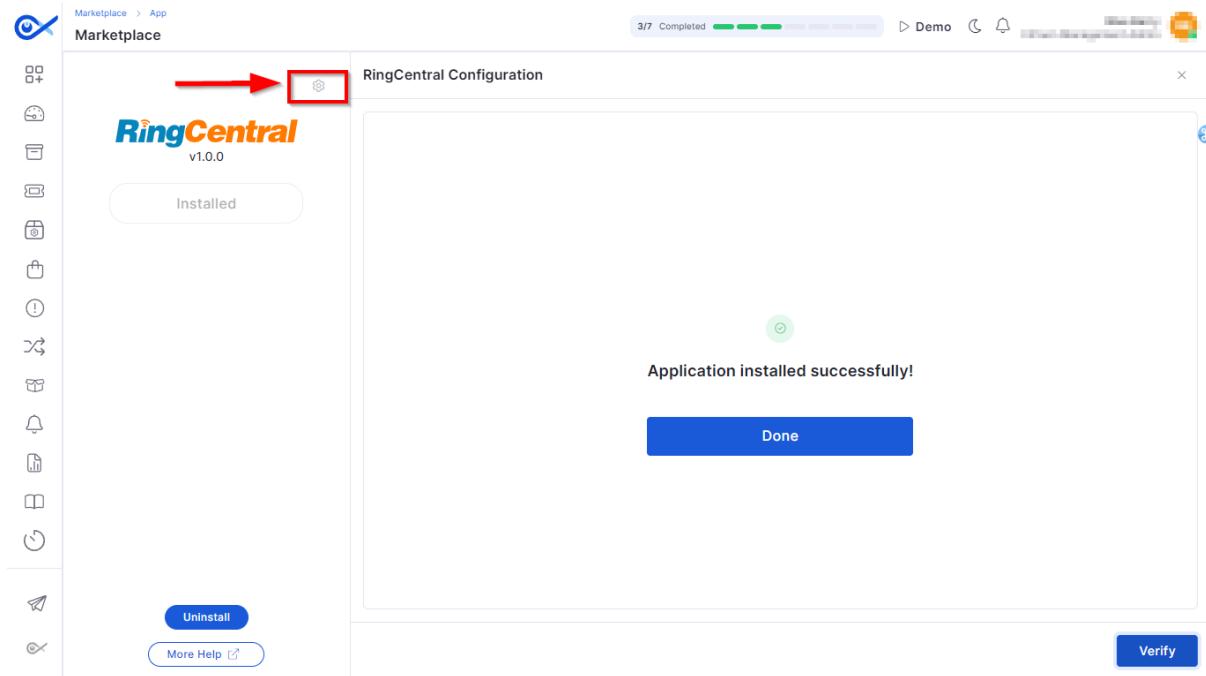
Marketplace

RingCentral v1.0.0

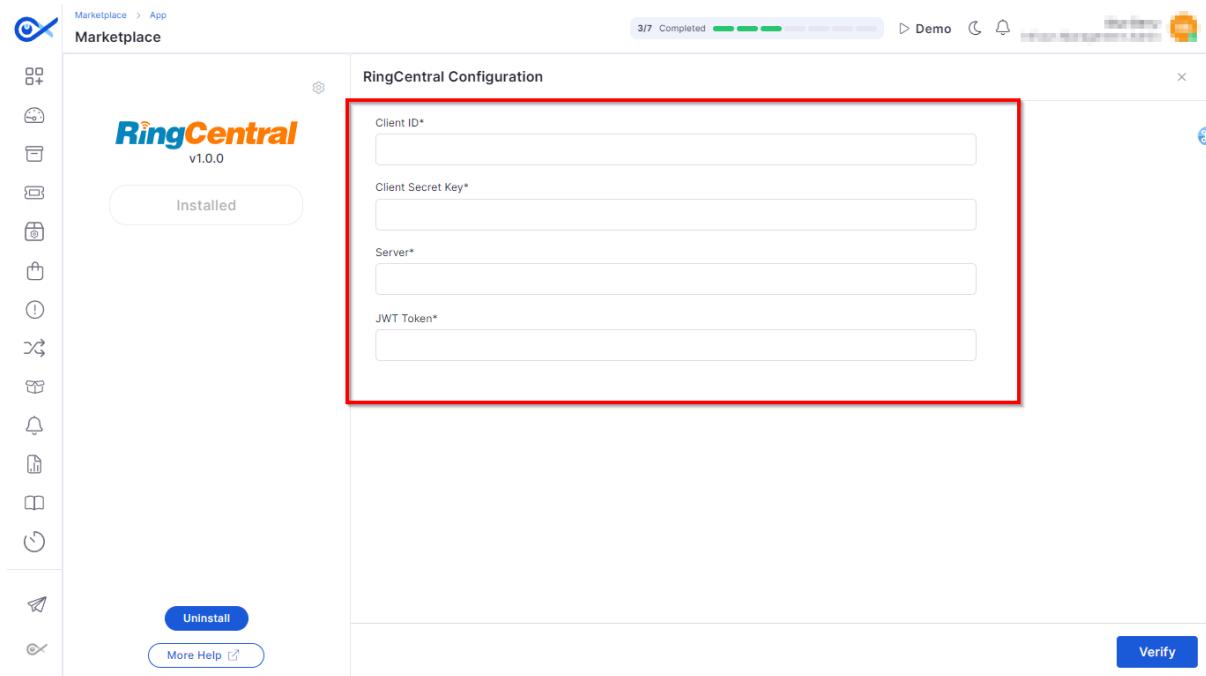
Install

Description How to install

STEP 1.3: Once the installation is done, click on the Ring Central-INFRAON configuration tab.



STEP 1.4: Now, enter the credentials as prompted in the respective call-out boxes.

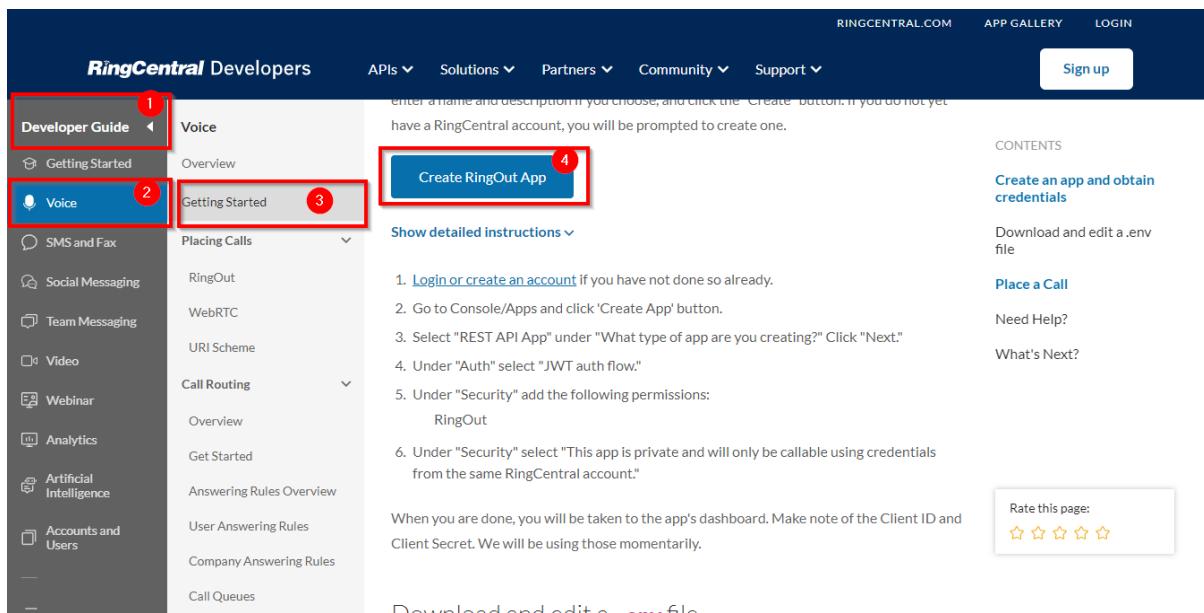


Follow the below steps to add the credentials.

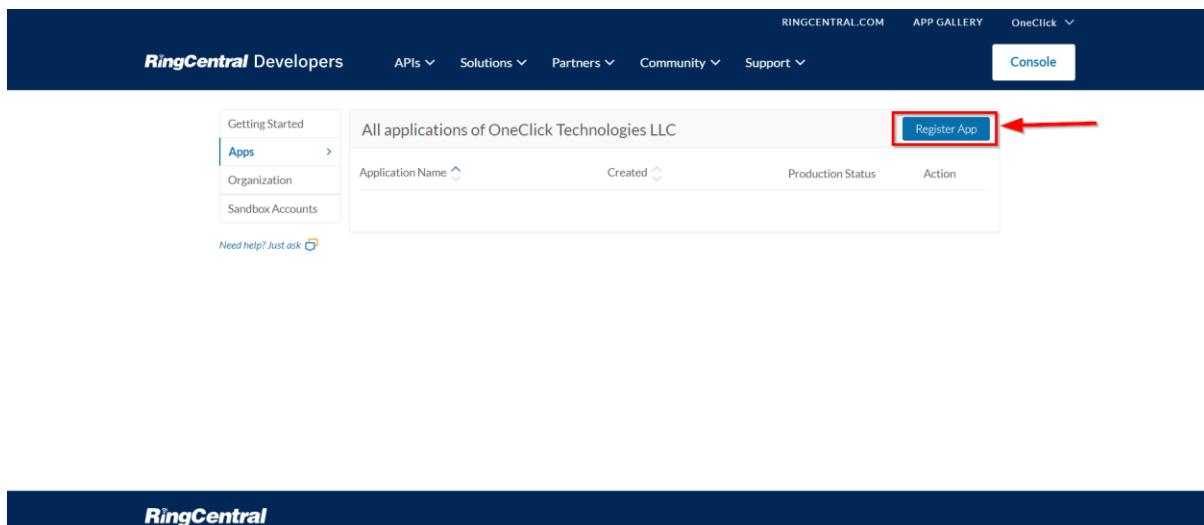
STEP 2: Register an App

STEP 2.1: Log in to the Ring Central webpage.

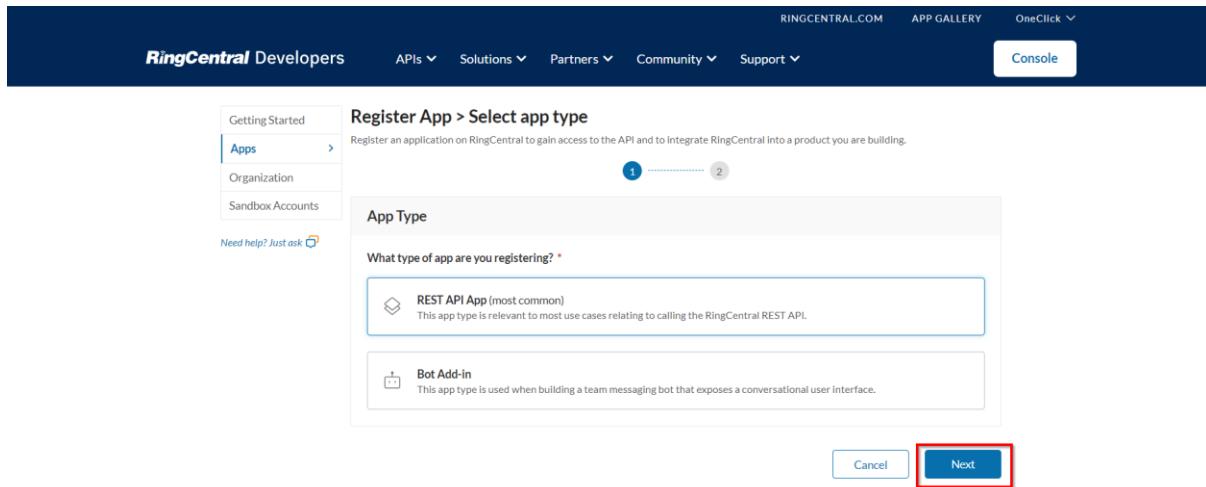
STEP 2.2: Upon logging in, head to the developer guides. Navigate to the "Voice" section and find the "Getting Started" page. There, click the "**Create RingOut App**" button to begin.



STEP 2.3: Begin the app registration process by clicking "**Register App.**"



STEP 2.4: Select the app type and click on '**Next'** to continue.



STEP 2.5: Now, enter the app name, description, and primary contact information in the 'Add properties' section. Click on the **(i)** button for more details.

The screenshot shows the 'App Properties (internal-use only)' section. It includes fields for 'App Name' (with a red box and arrow), 'App Description' (with a red arrow pointing to it from the left), 'Primary Contact' (a dropdown menu), and a question about promoting the app to the RingCentral App Gallery with 'Yes', 'No', and 'I don't know' options. The entire section is highlighted with a large red box.

STEP 2.6: In the 'App Card' section, shape the app's appearance on the App Gallery. Use these fields to configure its presentation. For more help, click on the **(i)** button to learn how to customize profiles for partners' app galleries.

App Card

Use the fields below to configure how your application will be presented within our App Gallery. Consult our [App Gallery Best Practices](#) guide to learn how to customize your profiles for our partners' app galleries.

Display Name (i)

Summary (i)

Enter a short summary of your app (max. 140 characters)

App Icon (i)

Image must be a square
File format supported: jpg, png, svg or gif
Size: less than 2MB

Choose

App card preview

[Display name]
OneClick Technologies LLC
[Summary will appear here]

Auth

STEP 2.7: In the 'Auth' section, locate and choose the authentication type that aligns with the organization's security protocols.

Select '**Yes**' to issue refresh tokens.

Auth

For apps that must authenticate directly to the platform, select the authentication method your app will use.

3-legged OAuth flow authorization code
This common OAuth flow requires users to log into the application via the RingCentral website, and to exchange an auth token for an access key.

JWT auth flow
This OAuth flow is recommended for server-side apps that do not have a user interface (e.g. scripts, cronjobs, daemons, and other command-line tools), as well as applications that are accessed by way of an "API key."

Issue refresh tokens? *

When this is enabled, RingCentral will issue a refresh token to allow sessions to be extended beyond their original lifetime, without having to reauthenticate.

Yes **No**

Security

Application Scopes (i)

Start typing to add scopes (optional)

Who will be authorized to access your app? *

This app is public and will be callable via any RingCentral customer. [Advanced settings](#)

STEP 2.8: Add the required security scopes and configure security by specifying access levels in the security section. "**Public**" grants unrestricted access, while "**Private**" limits access only to authorized users.

Yes No

Security

Application Scopes ⓘ

Ring Out ✖️ VoIP Calling ✖️ Call Control ✖️ Read Contacts ✖️ Read Messages ✖️

Who will be authorized to access your app? *

This app is public and will be callable via any RingCentral customer. Advanced settings ⓘ

This app is private and will only be callable using credentials from the same RingCentral account. ⓘ

App Features

Interactive Messages

Select this option if your app posts interactive messages to RingCentral Team Messaging chats. Interactive messages include elements such as buttons, form input fields, and other interactive elements.

Back Create

RingCentral

STEP 2.9: Select the app features as per the requirements and click “**Create**” to register the app.

Yes No

Security

Application Scopes ⓘ

Ring Out ✖️ VoIP Calling ✖️ Call Control ✖️ Read Contacts ✖️ Read Messages ✖️

Who will be authorized to access your app? *

This app is public and will be callable via any RingCentral customer. Advanced settings ⓘ

This app is private and will only be callable using credentials from the same RingCentral account. ⓘ

App Features

Interactive Messages

Select this option if your app posts interactive messages to RingCentral Team Messaging chats. Interactive messages include elements such as buttons, form input fields, and other interactive elements.

Back Create

RingCentral

The app has now been registered.

STEP 3: Obtaining the Access Credentials

STEP 3.1: Navigate to Step XX and click the newly created app to access its details.

The screenshot shows the RingCentral Developers console interface. At the top, there's a navigation bar with links for RINGCENTRAL.COM, APP GALLERY, OneClick, and a Console button. Below the navigation is a sidebar with options like Getting Started, Apps (which is selected and highlighted with a blue border), Organization, and Sandbox Accounts. The main content area displays a table titled "All applications of OneClick Technologies LLC". The table has columns for Application Name, Created, Production Status, and Action. One row in the table is highlighted with a red box and contains the text "Infraon RingOut App", "Mar 11, 2024 3:19:13 PM", "Graduated", and an edit icon. At the bottom left of the main area, there's a "Need help? Just ask" button.

STEP 3.2: On the panel, select the credentials tab.

The screenshot shows the detailed view of the "Infraon RingOut App". The top navigation bar shows "Apps > Infraon RingOut App". The left sidebar has tabs for Dashboard, Settings, **Credentials** (which is selected and highlighted with a red border), App Gallery, Rate limits, Analytics, and API history. The main content area is titled "Credentials" and contains sections for "Sandbox Environment" and "Production Environment". Under "Application Credentials", it shows "Main Company Number" dropdowns for both environments. Below that is a section for "User Credentials".

STEP 3.3: Now copy and paste the **API server URL**, **Client ID**, and **Client Secret** into the Infraon portal's configuration page. (STEP XX)

The screenshot shows the 'Credentials' page for the 'Infraon RingOut App'. The left sidebar includes links for Dashboard, Settings, Credentials (which is selected), App Gallery, Rate limits, Analytics, and API history. A 'Need help? Just ask' button is also present. The main content area is titled 'Credentials' and contains two tabs: 'Sandbox Environment' and 'Production Environment'. Under 'Main Company Number', dropdown menus show 'Main Company Number' and 'Main Company Name'. The 'Application Credentials' section is highlighted with a red box and contains fields for 'API Server URL' (with values 'https://[REDACTED].com' and 'https://[REDACTED].com'), 'Client ID' (with dropdowns for 'Client ID' and 'Client Secret'), and 'Client Secret' (with 'Click to see' links). Below this, 'User Credentials' and 'Tools' sections are shown, each with their own sub-fields.

STEP 4: Generating the JWT Token

STEP 4.1: On the same credential page, click on the “**Download**” option to generate the JWT token.

This screenshot shows the same 'Credentials' page as the previous one, but the focus is on the 'Tools' section. It includes fields for 'Account Admin Portal' (with 'Login' and 'Logout' buttons) and 'Tools' (with 'Logout' buttons). The 'Credentials JSON' button is highlighted with a red box and has a red arrow pointing to it from the left.

STEP 4.2: Now open the same downloaded JSON file, access the JWT token, and paste it into the Infraon portal's configuration page.

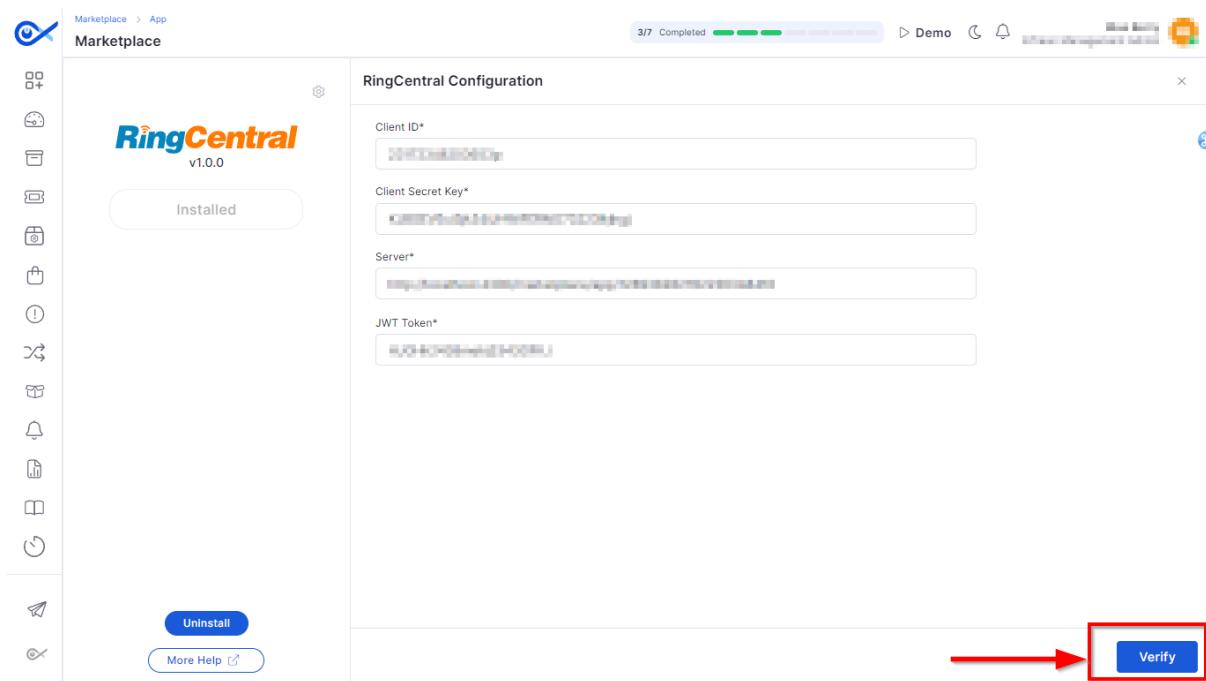
```

1 {
2   "clientId": "REDACTED",
3   "clientSecret": "REDACTED",
4   "server": "REDACTED",
5   "jwt": "REDACTED"
6 }
7
8

```

The screenshot shows a code editor interface with several tabs at the top: yarn.lock, CONTRIBUTING.md, TS index.ts, JS index.7bf66316.js, rc-credentials (3).json, and rc-credentials (4).json. The main pane displays a JSON object with fields for clientId, clientSecret, server, and jwt. The jwt field contains a long string of characters. A red arrow points to this jwt field.

STEP 4.3: To complete the Ring Central and Infraon integration, click "**Verify**" after adding the required credentials.



The above process is now completed.

Infraon LDAP

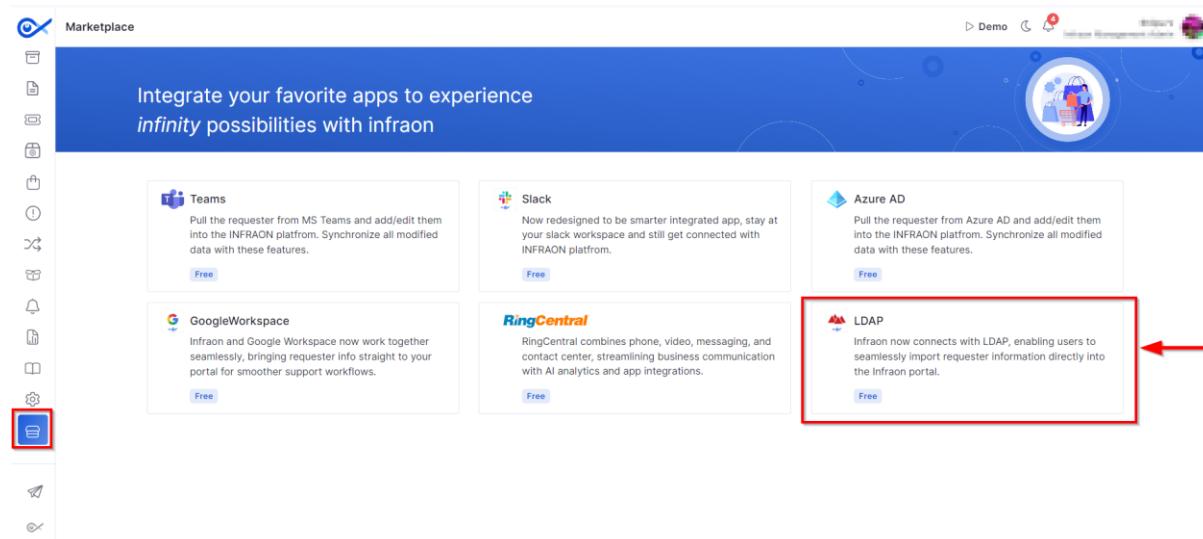
Description

Infraon Infinity is now integrating with LDAP to streamline user management. This integration will allow users to directly add end-users from LDAP to the Infraon portal, eliminating the need for manual data entry. Additionally, users will be able to view requester details directly within the Infraon platform, improving visibility and simplifying the approval process.

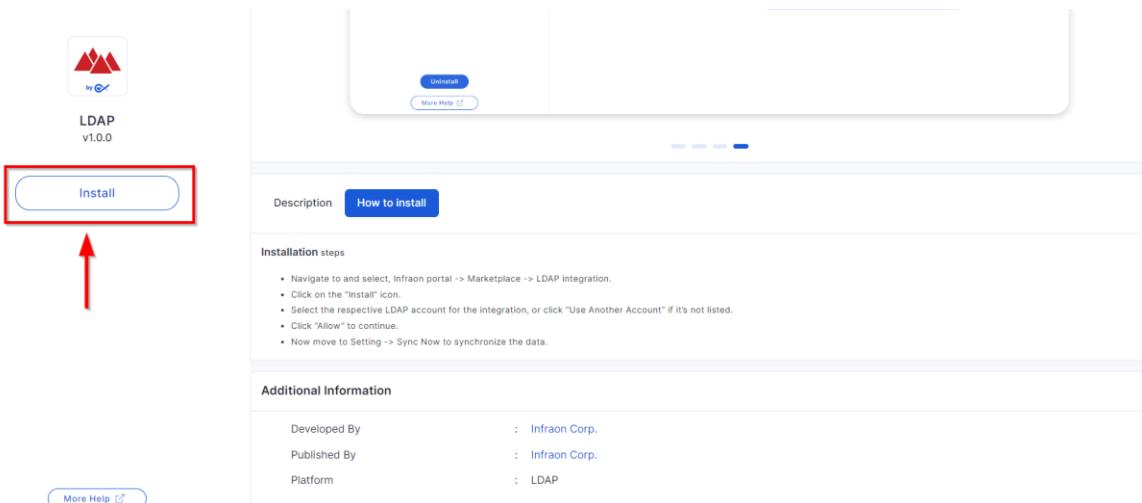
How to Install

Installation Steps:

STEP 1: Log in to your Infraon Infinity account. On the left panel, click on the 'Marketplace' tab and select "LDAP" integration.



STEP 2: After clicking the tab, click on Install.



STEP 3: Now, in the LDAP configuration tab, enter the credentials, LDAP URL/ IP Address, Port, User Name, Password, Base DN, Advance Search, and Role as prompted in the respective call-out boxes.

The screenshot shows the 'LDAP Configuration' page. On the left, there's a card for 'LDAP v1.0.0' with an 'Install' button. The main area has tabs for 'Configuration' (selected) and 'Requester'. A large red box highlights the input fields for 'LDAP URL / IP Address*', 'Port*', 'User Name*', 'Password*', 'Base DN*', 'Advance Search', and 'Role'. At the bottom right is a 'Verify' button.

STEP 4: Once the credentials have been filled, click 'Verify' to proceed.

LDAP Configuration

Configuration Requester

LDAP URL / IP Address*

Port*

User Name*

Password*

Base DN*

Advance Search

Role

More Help

Verify

STEP 5: In the Requester tab, select the adjacent fields dropdown to begin column mapping with the related fields on Infraon Infinity.

The same data can be previewed in the next column.

Marketplace > App Marketplace

LDAP v1.0.0

Installed

Uninstall

Requester Details

LDAP details

Full Name*

Email*

Phone Number

Landline

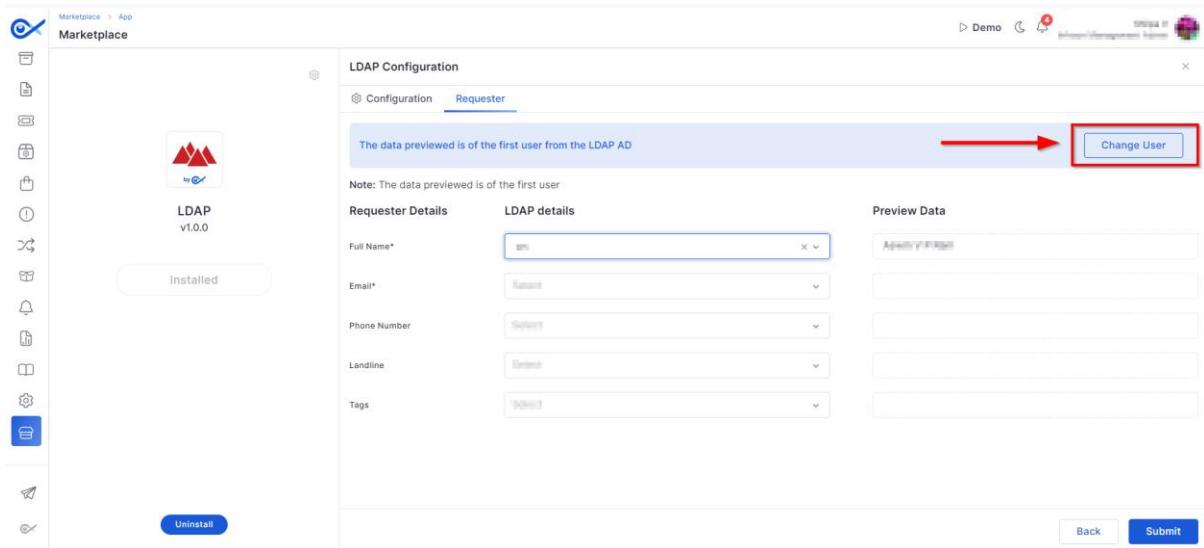
Tags

Preview Data

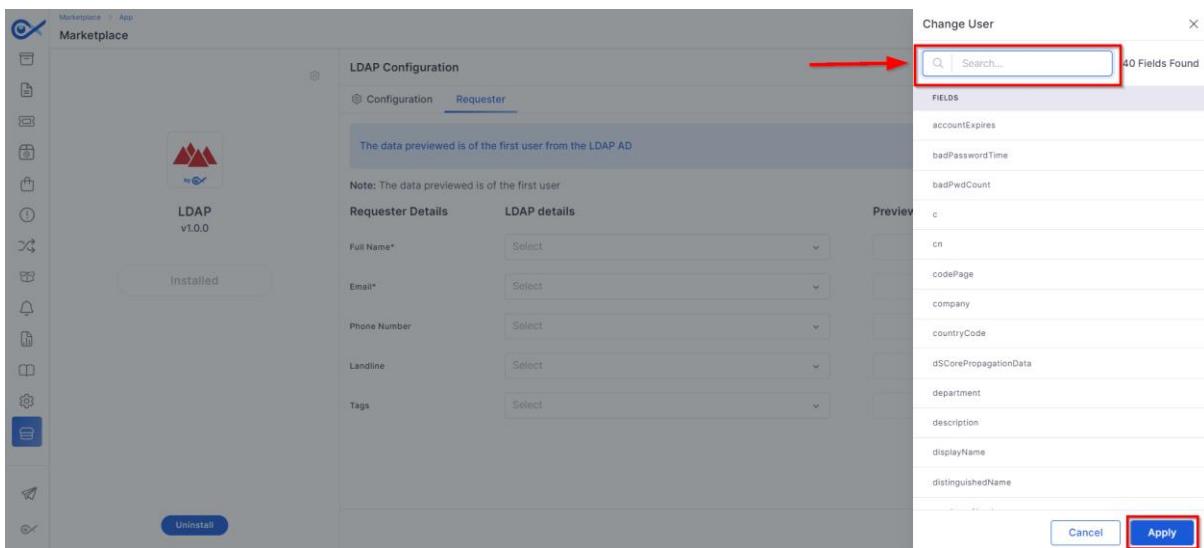
Change User

Back Submit

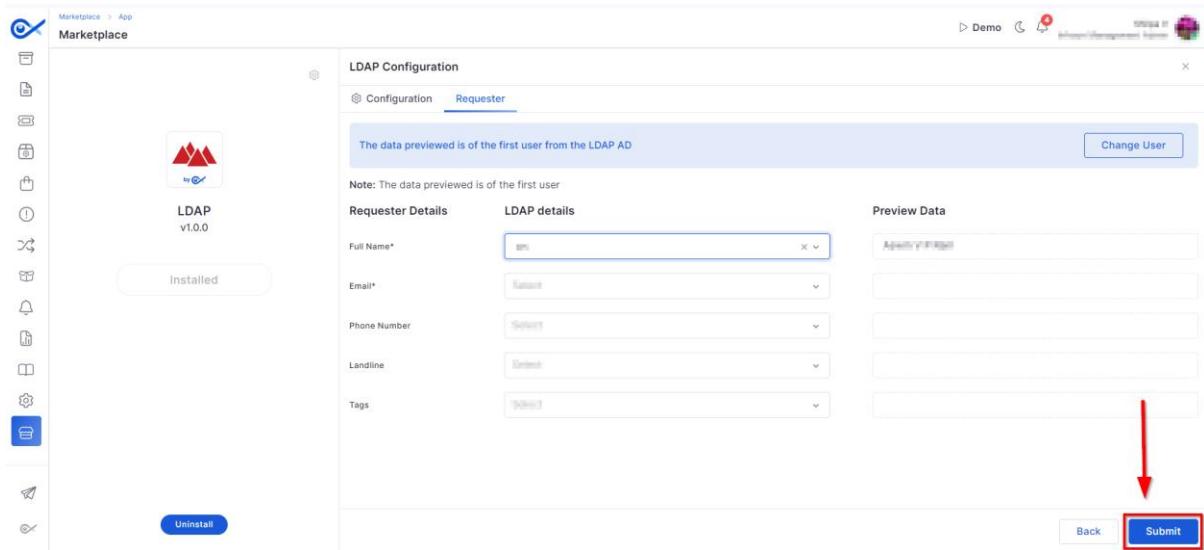
NOTE: Clicking 'Change User' provides a way to preview data from another user's perspective. This can be helpful for troubleshooting access issues, understanding user experience, or verifying data accuracy across different accounts."



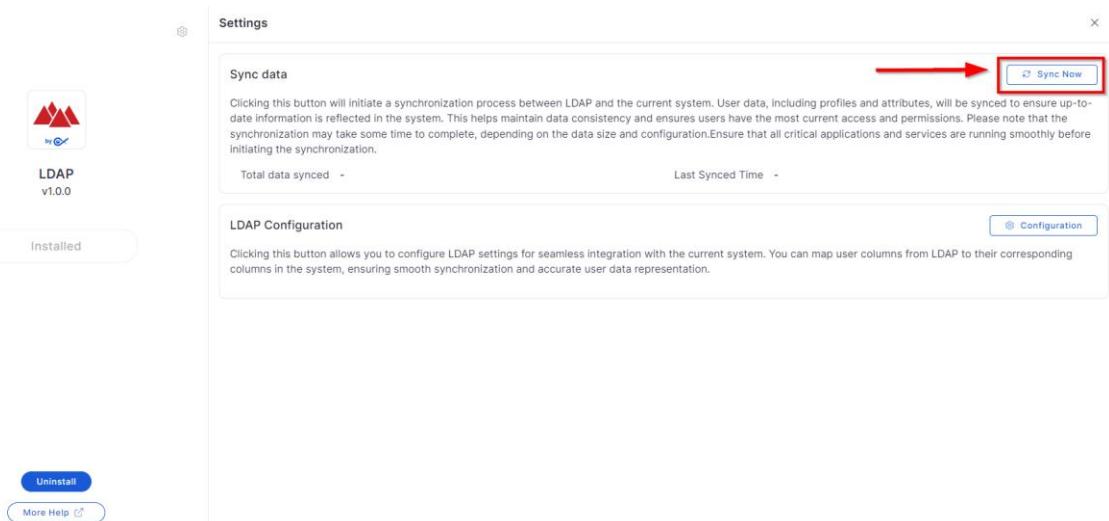
Select a user to import their default profile information. Once selected, click 'Apply' to make changes.



STEP 6: Once all the necessary details have been filled in, clicking the "Submit" button will finalize the configuration process for this integration.



STEP 7: After completing the configuration, initiate the synchronization by clicking "Sync Now" to import requester data into Infraon Infinity. Clicking "Sync Now" will trigger the import process.



The integration is now completed.

Infraon JIRA

Description

By integrating JIRA with the Infraon marketplace, IT assets in Infraon Infinity will automatically sync with JIRA. This two-way connection means any issues created for a specific asset in JIRA will appear in a dedicated "JIRA Tickets" section within the corresponding asset's details on Infraon.

How to Install

Installation steps

Installing the integration:

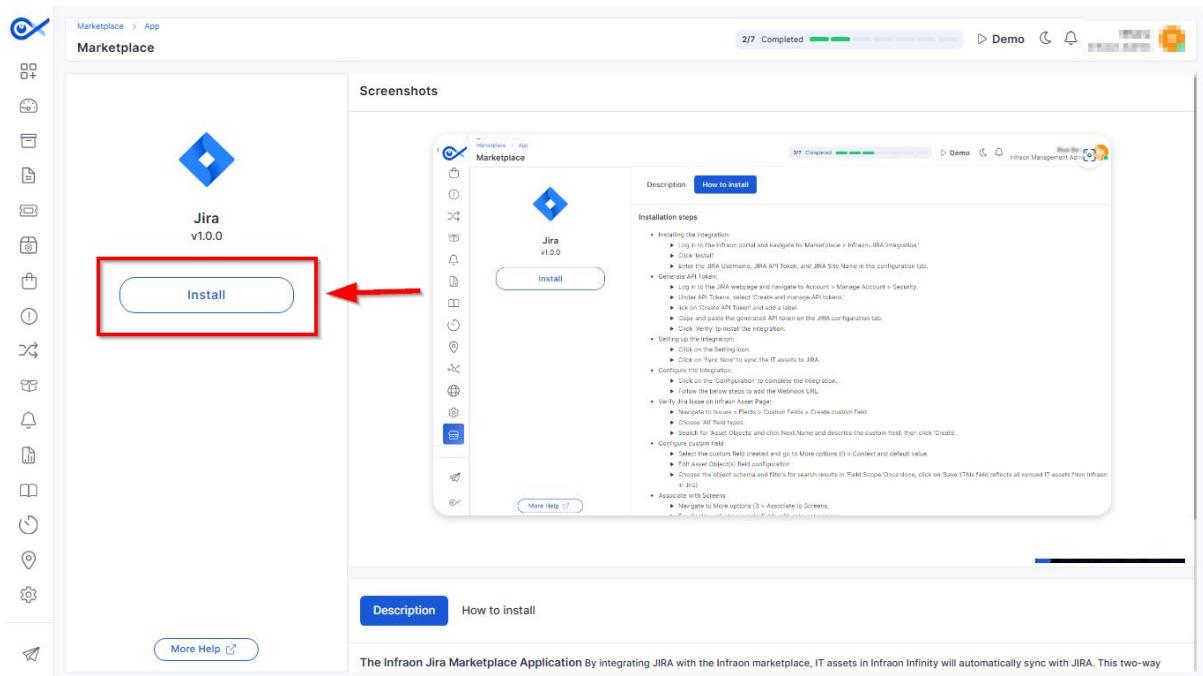
STEP 1: Log in to your Infraon account. On the left panel, click on the Marketplace tab and select "JIRA" integration.

The screenshot shows the Infraon Marketplace page. On the left, there is a vertical sidebar with various icons. One icon, which looks like a document with a grid, is highlighted with a blue square and a red border. The main content area has a blue header bar with the text "Integrate your favorite apps to experience infinity possibilities with infraon". Below this, there are several cards representing different integrations:

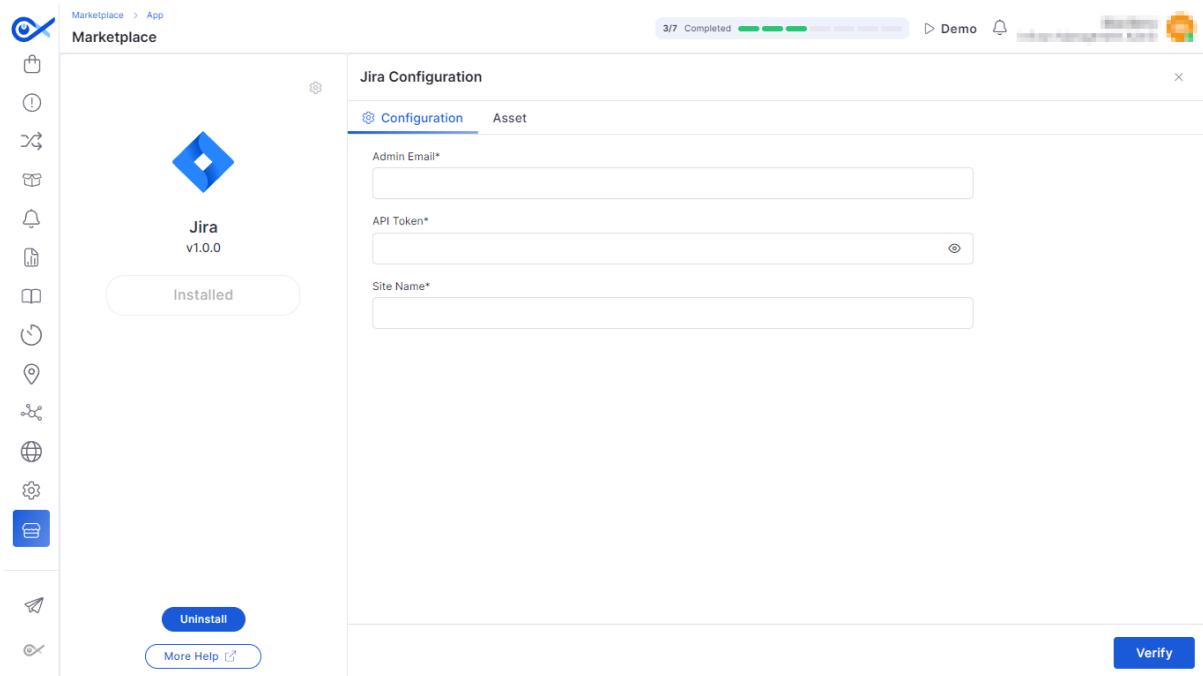
- Azure AD**: Pull the requester from Azure AD and add/edit on INFRAON platform. **Free**
- Slack**: Now redesigned to be smarter integrated app, stay at your slack workspace and still get connected with INFRAON platform. **Free**
- VendorIntegrations**: Now redesigned to be smarter integrated app, using vendor integrations stay connected with INFRAON platform. **Free**
- Teams**: Pull the requester from MS Teams and add/edit them into the INFRAON platform. Synchronize all modified data with these features. **Free**
- Whatsapp**: Now redesigned to be smarter integrated app, using whatsapp stay connected with INFRAON platform. **Free**
- Jamf**: Pull the devices from Jamf and add/edit them into the INFRAON platform. Synchronize all modified data with these features. **Free**
- RingCentral**: RingCentral combines phone, video, messaging, and contact center, streamlining business communication with AI analytics and app integrations. **Free**
- LDAP**: Infraon now connects with LDAP, enabling users to seamlessly import requester information directly into the Infraon portal. **Free**
- Jira**: JIRA integration with Infraon Infinity syncs IT assets. Create JIRA issues for an IT asset and see them in a dedicated "JIRA Tickets" section in Infraon Infinity. **Free**

A red box highlights the "Jira" integration card. A red arrow points upwards from the bottom right towards the "Jira" card, indicating it is the target of the selection.

STEP 2: After clicking the tab, click on Install.



STEP 3: After installing the Infraon JIRA integration, configure it by providing your JIRA credentials. This includes JIRA Admin Email, JIRA API Token, and JIRA Site Name.



Follow the below steps to add the credentials.

Generate API Token:

STEP 4: Log in to the [JIRA admin account](#) webpage.

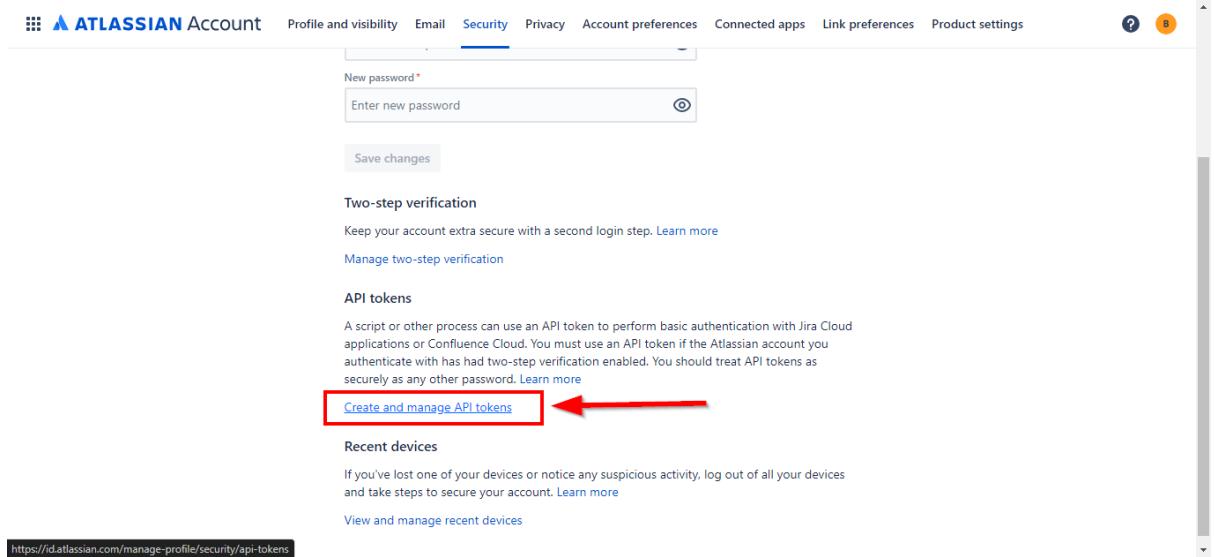
STEP 5: After logging in to JIRA, find your user account menu in the top right corner. It might be represented by your initials or avatar. Click on it, and then select "Manage Account" from the options.

The screenshot shows the JIRA web interface. At the top right, there is a user icon (initials 'B'). A red arrow points from this icon to a dropdown menu. The dropdown menu is titled 'ACCOUNT' and contains the following items: 'Bhanu' (with an orange profile picture), 'Manage account' (which is highlighted with a red box), 'UPGRADE', 'JIRA', 'Profile', 'Personal settings', 'Notifications', and 'Theme'. On the left side, there's a sidebar with sections like 'Queues', 'STARRED', 'TEAM PRIORITY', and 'Open tasks'. The main area shows 'Open tasks' with a search bar and a large orange speech bubble icon. Below it, there's a section titled 'All of your requests will show up here' with a 'Create a request' button.

STEP 6: Click "Security" in the top menu for more details.

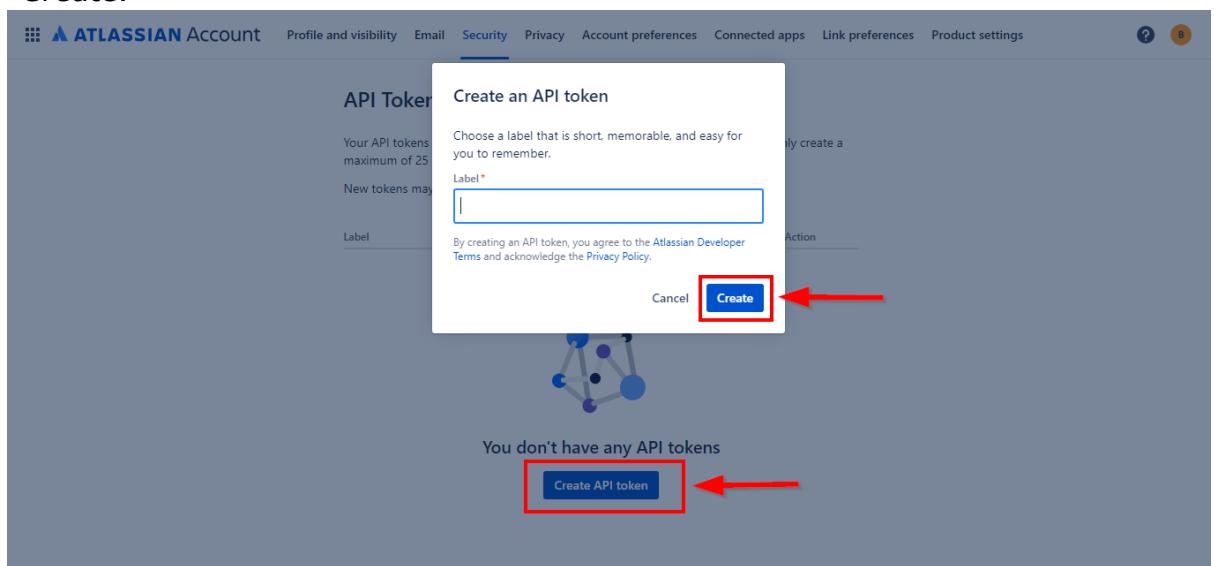
The screenshot shows the Atlassian Account security settings page. At the top, there is a navigation bar with tabs: 'Profile and visibility', 'Email', 'Security' (which is highlighted with a red box), 'Privacy', 'Account preferences', 'Connected apps', 'Link preferences', and 'Product settings'. A red arrow points from the 'Security' tab to the 'Privacy' section below. The 'Privacy' section is titled 'Profile and visibility' and contains instructions: 'Manage your personal information, and control which information other people see and apps may access.' It also includes links to 'Learn more about your profile and visibility' and 'View our privacy policy'. Below this, there's a 'Profile photo and header image' section with a yellow placeholder image featuring a white circle with the letter 'B'. To the right, there's a 'Who can see your profile photo?' dropdown set to 'Anyone'. Further down, there's an 'About you' section with a 'Full name' field and a 'Who can see this?' dropdown.

STEP 7: To proceed, locate "API Tokens" and select "Create and manage API tokens" to generate a new API token.



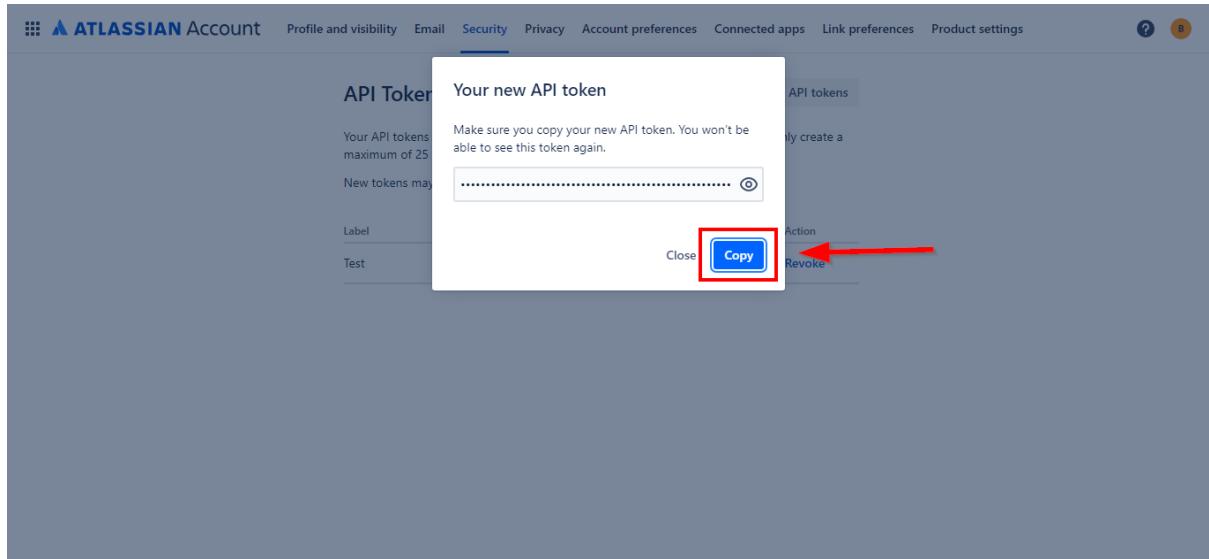
The screenshot shows the Atlassian Account Security settings page. The 'Security' tab is selected. Under the 'Two-step verification' section, there is a link 'Create and manage API tokens' which is highlighted with a red box and an arrow pointing to it. Below this section, there is a 'Recent devices' section with a link 'View and manage recent devices'. The URL in the address bar is https://id.atlassian.com/manage-profile/security/api-tokens.

STEP 8: To generate a new API token, click on "Create API Token," enter the necessary Label in the designated field, and confirm by clicking on "Create."



The screenshot shows the 'Create an API token' dialog box. It has a 'Label' input field where the user can enter a label for the API token. There is a 'Create' button at the bottom right of the dialog box, which is highlighted with a red box and an arrow pointing to it. In the background, the main page shows a message 'You don't have any API tokens' and a 'Create API token' button, which is also highlighted with a red box and an arrow pointing to it.

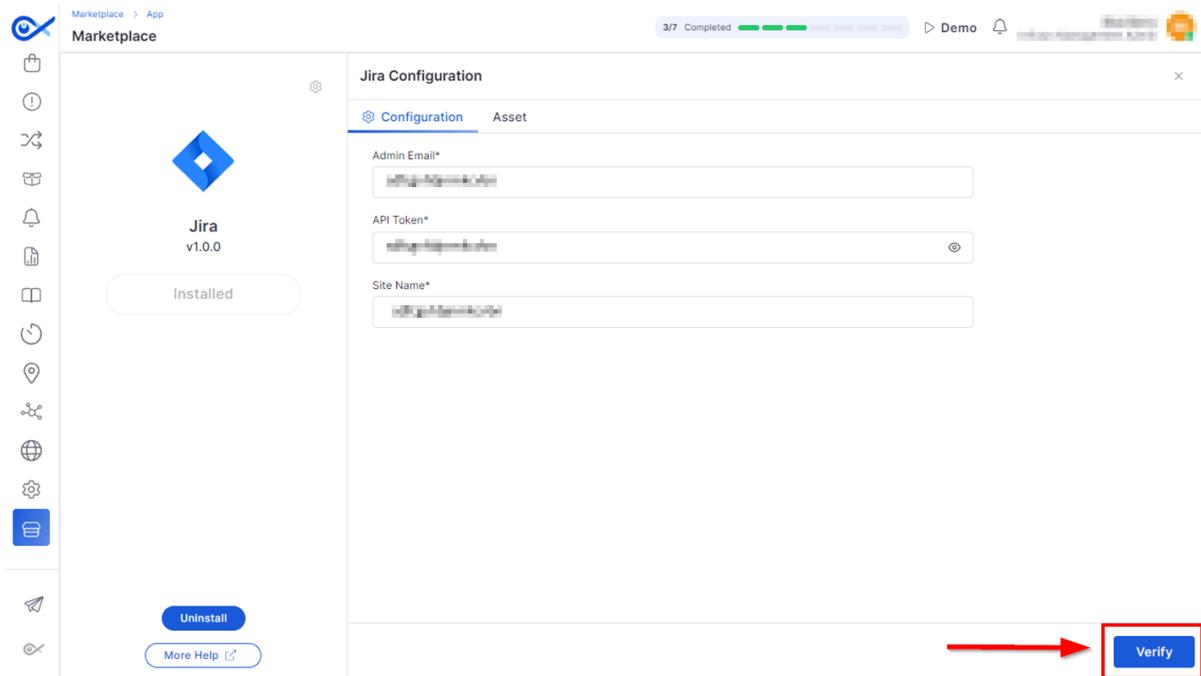
STEP 9: Once you have the API token, copy and paste it in the appropriate field on the Infraon configuration page.



NOTE: Locate the Site Name and Admin Email from the snippet provided below.

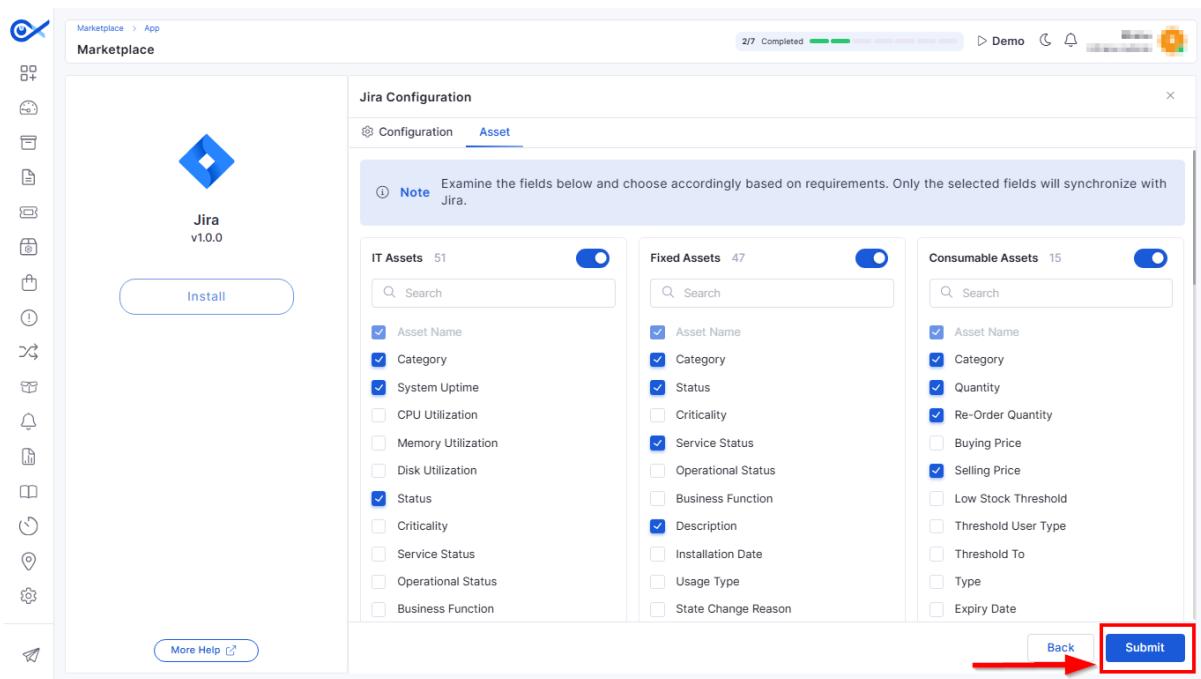
A screenshot of the Jira Service Desk interface. The URL in the address bar is partially redacted. On the left sidebar, there is a red box around the URL and a red arrow pointing down to the 'Site Name' label. On the right sidebar, there is a red box around the 'Admin Email' label, which is preceded by a red arrow pointing from the right.

STEP 10: To confirm your configuration and activate the integration, click "Verify" after entering all credentials.



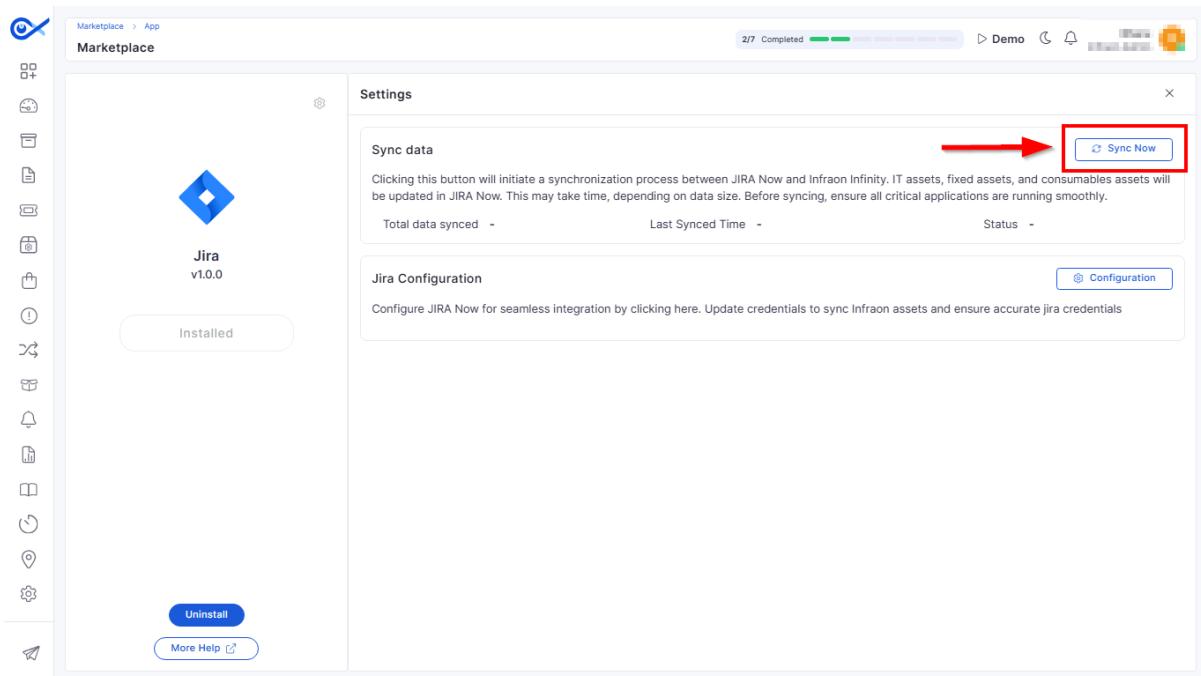
Configure Assets:

STEP 11: The "Assets" tab allows you to define which asset data will be synchronized on the JIRA platform. Choose the type of asset (IT Assets, Fixed Assets, or Consumable Assets) and then select the specific fields relevant to that asset type that you want to sync to JIRA. Once configured, click "Submit" to apply your settings.

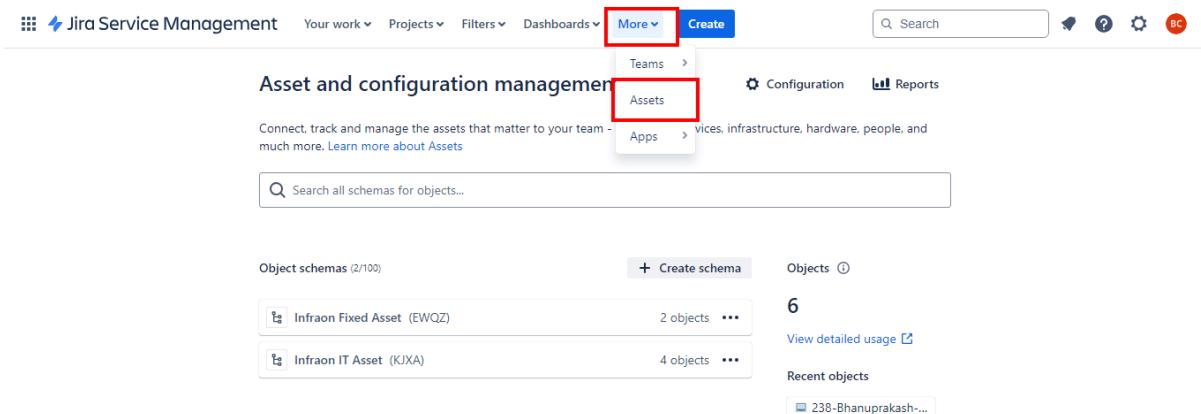


Setting up the Integration:

STEP 12: On the "Settings" tab, click "Sync Now" to manually trigger the synchronization between JIRA and Infraon Infinity.



NOTE: After successful synchronization, access the synced assets and their types within JIRA. Go to the "More" menu in the top navigation bar, then select "Assets" (also known as "Object Schemas" in JIRA)



Integration is Installed successfully.

Verify Jira Issue on Infraon Asset Page:

Create a custom field

STEP 1: To manage issue settings and create custom fields, navigate to the settings menu (represented by a gear icon) in the top right corner and select "Issues."

Manage your IT and non-IT as high-velocity teams

Get your team the data they need, when they need it with Assets. Try Premium connect and consolidate your data, then surface it inside issues, Confluence

Try it now Learn more

IT Assets

Hardware

Laptops

Charlie's laptop

Jane's laptop

Omar's laptop

Jeff's laptop

Owner: Charlie

Status: ORDERED

Purchase date: Aug 21, 2023

Location: Sydney

https://assetmanagement.atlassian.net/jira/setting/issues/issue-types

STEP 2: Within JIRA's Issues view, look for the "Custom fields" section on the left sidebar. Then, click on the "Create custom field" button in the top right corner to create a custom field.

Issues

Issue types

Issue type schemes

Sub-tasks

WORKFLOWS

Workflows

Workflow schemes

SCREENS

Screens

Screen schemes

Issue type screen schemes

FIELDS

Custom fields

Field configurations

Field configuration schemes

Custom fields

Active Trashed

Filter by name or description

Name : Type Screens and contexts : Projects : Last used :

Actual end Date Time Picker 6 screens, 1 context 2 projects No information

Actual start Date Time Picker 6 screens, 1 context 2 projects No information

Affected hardware Text Field (single line) 6 screens, 1 context 2 projects No information

Affected services LOCKED Unknown 22 screens, 1 context 2 projects Not tracked

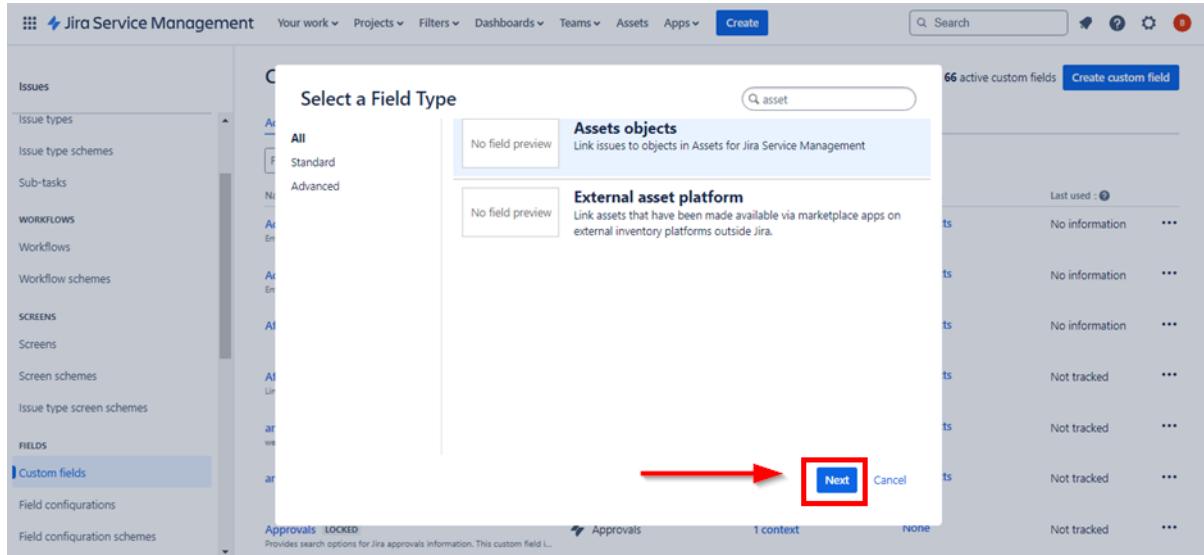
Assets objects Assets objects 67 screens, 1 context 2 projects Not tracked

Approvals LOCKED Approvals 1 context None Not tracked

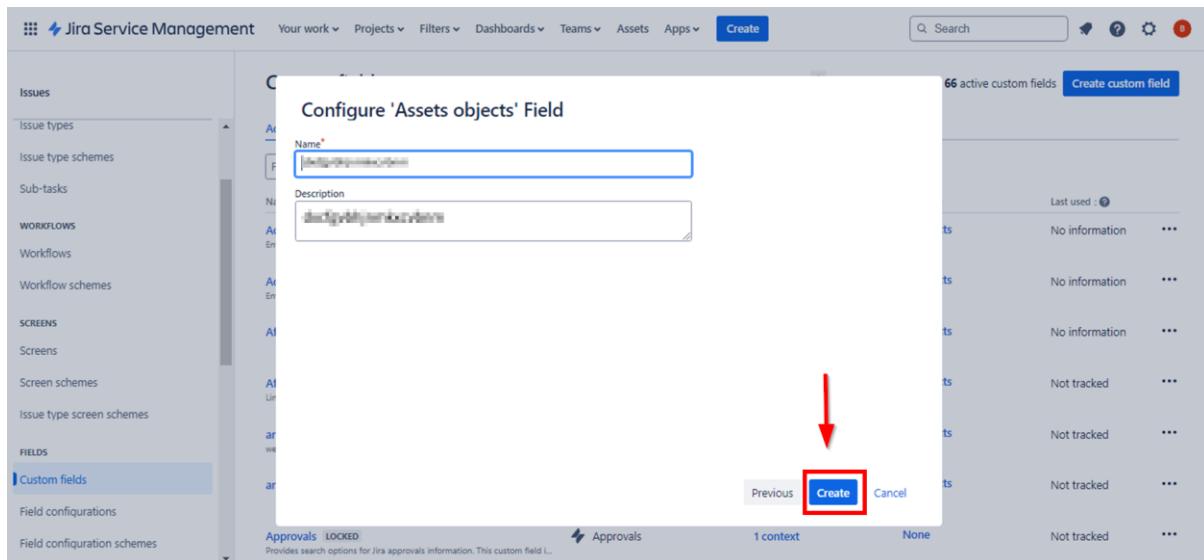
You currently have 66 active custom fields

Create custom field

STEP 3: From the pop-up window, search for and choose "Assets objects" (select "All" fields to view all options). Once selected, click "Next" to continue creating the custom field.



STEP 4: Complete the custom field configuration by entering a descriptive name and adding an optional explanation in the description field. Click "Create" to save your new field.



Configure custom field

STEP 5: To configure the newly created custom field, click the more info icon (:) and choose "Contents and default value."

The screenshot shows the 'Custom fields' section in Jira Service Management. On the left is a sidebar with various management options like Issues, New issue search transition, ISSUE TYPES, WORKFLOWS, SCREENS, etc. The main area shows a table of custom fields. One row is selected: 'Name : Infraon IT Asset', 'Type : Assets objects', 'Screens and contexts : 1 context', 'Projects : None', and 'Last used : Not tracked'. A context menu is open next to the row, with a red arrow pointing to the 'Contents and default value' option. Other menu items include 'Edit details', 'Translation options', 'Associate to Screens', and 'Move to trash'. The URL in the browser bar is assetmanagement.atlassian.net/secure/admin/ConfigureCustomField/default.jspa?cus....

STEP 6: Edit which asset details appear in the custom field by selecting "Edit Asset Object/s field configuration" under "Default Configuration Schema for Infraon IT Asset."

The screenshot shows the 'Configure Custom Field: Infraon IT Asset' page. The sidebar on the left is identical to the previous screenshot. The main content area is titled 'Configure Custom Field: Infraon IT Asset'. It contains a section for 'Default Configuration Scheme for Infraon IT Asset'. This section includes a 'Default configuration scheme generated by Jira' and a 'Scheme' dropdown set to 'Edit Configuration'. Below this, it lists 'Applicable contexts for scheme:' and 'Issue type(s): Global (all issues)'. A red arrow points to the 'Edit Asset object/s field configuration' link. Further down, there are sections for 'Object schema: None', 'Filter scope (AQL): None', 'Filter issue scope (AQL): None', 'Allow search filtering by these attributes: None', 'Object attributes to display on issue view: None', 'Field can store multiple objects: No', and 'Display a default object when this field appears in a customer portal: No'.

- STEP 6.1.** In the “Field Scope” section, select the desired object schema from the drop-down menu. You can also refine your search results by applying filters.

Jira Service Management

Issues

New issue search transition

ISSUE TYPES

Issue type hierarchy

Issue types

Issue type schemes

Sub-tasks

WORKFLOWS

Workflows

Workflow schemes

SCREENS

Screens

Screen schemes

Assets objects field configuration - Infraon IT Asset (customfield_10054)

Field scope →

Choose which object schema to use, and which filters to apply on the results shown when searching for objects in the field.

Object schema *

- Infraon IT Asset
- Infraon Fixed Asset
- Infraon IT Asset
- Services

Filter issue scope (AQL)

Filter the values that will appear in this custom field using the value of Assets custom fields or Jira System fields in this screen. [Learn more about Filter Issue Scope](#).

i Filter issue scope (AQL) is not supported when running automation rules

User interaction

Configure how your field will function for users, and how it will display on the issue view.

- STEP 6.2.** Customize the user experience and appearance of your custom field. Select the display attributes that will determine how the field appears on the issue view page.

Jira Service Management

Issues

New issue search transition

ISSUE TYPES

Issue type hierarchy

Issue types

Issue type schemes

Sub-tasks

WORKFLOWS

Workflows

Workflow schemes

SCREENS

Screens

Screen schemes

Filter the values that will appear in this custom field using AQL. [Learn more about Filter Scope](#).

Filter issue scope (AQL)

Filter the values that will appear in this custom field using the value of Assets custom fields or Jira System fields in this screen. [Learn more about Filter Issue Scope](#).

i Filter issue scope (AQL) is not supported when running automation rules

User interaction →

Configure how your field will function for users, and how it will display on the issue view.

Display and search across these attributes in the custom field

- Name
- Category

Display these attributes in the issue view

- Name
- Category

Field can store multiple objects

Display a default object when this field appears in a customer portal

Cancel Save

STEP 7: Review your selections and click "Save" to confirm the changes to your custom field.

Jira Service Management

Issues

New issue search transition

ISSUE TYPES

Issue type hierarchy

Issue types

Issue type schemes

Sub-tasks

WORKFLOWS

Workflows

Workflow schemes

SCREENS

Screens

Screen schemes

Custom fields

User interaction

Filter issue scope (AQL)

Filter issue scope (AQL) is not supported when running automation rules

Name Category

Display these attributes in the issue view

Name Category

Field can store multiple objects

Display a default object when this field appears in a customer portal

Cancel Save

(This field reflects all synced IT assets from Infraon in Jira)

Associate with Screens

STEP 8: To add the associate screens to the custom field, click the more info icon (:) and choose "Associate to Screens."

Jira Service Management

Issues

New issue search transition

ISSUE TYPES

Issue type hierarchy

Issue types

Issue type schemes

Sub-tasks

WORKFLOWS

Workflows

Workflow schemes

SCREENS

Screens

Screen schemes

Custom fields

Active Trashed

infra

Name	Type	Screens and contexts	Projects	Last used
Infra IT Asset	Assets objects	6 screens, 1 context	None	Not tracked

Associate to Screens

Edit details

Contexts and default value

Translation options

Move to trash

STEP 9: Make the field visible on relevant screens. Select the screens where you want the "Infraon IT Assets" field to appear. Remember, a field needs to be associated with a screen to be visible. Click "Update" to save your selections.

	Field Tab
JIRA Service Desk Pending Reason screen	<input checked="" type="checkbox"/>
JIRA Service Desk Pending Reason screen - 2	<input checked="" type="checkbox"/>
JIRA Service Desk Pending Reason screen - 3	<input checked="" type="checkbox"/>
JIRA Service Desk Pending Reason screen - 4	<input checked="" type="checkbox"/>
JIRA Service Desk Resolve Issue Screen	<input checked="" type="checkbox"/>
JIRA Service Desk Resolve Issue Screen - 2	<input checked="" type="checkbox"/>
JIRA Service Desk Resolve Issue Screen - 3	<input checked="" type="checkbox"/>
JIRA Service Desk Resolve Issue Screen - 4	<input checked="" type="checkbox"/>
Jira Service Desk Resolve Issue Screen	<input checked="" type="checkbox"/>
Jira Service Desk Resolve Issue Screen - 2	<input checked="" type="checkbox"/>
Jira Service Desk Resolve Issue Screen - 3	<input checked="" type="checkbox"/>
Jira Service Desk Resolve Issue Screen - 4	<input checked="" type="checkbox"/>
Resolve Issue Screen	<input checked="" type="checkbox"/>
Workflow Screen	<input checked="" type="checkbox"/>
Workflow Screen - 2	<input checked="" type="checkbox"/>
Workflow Screen - 3	<input checked="" type="checkbox"/>
Workflow Screen - 4	<input checked="" type="checkbox"/>
Workflow Screen - 5	<input checked="" type="checkbox"/>

Update **Cancel**

Create Issue

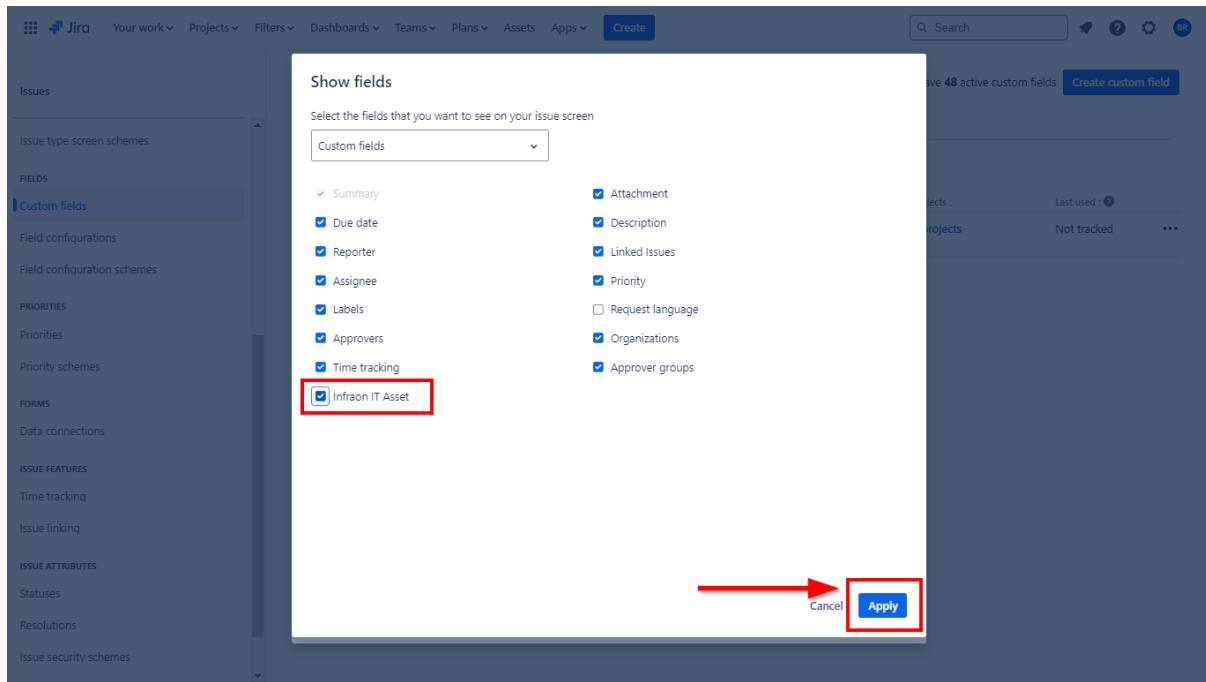
STEP 1: To Make the custom field visible on the issue view by clicking the ellipsis (...) menu and selecting "Show fields."

The 'Create issue' dialog shows the following fields:

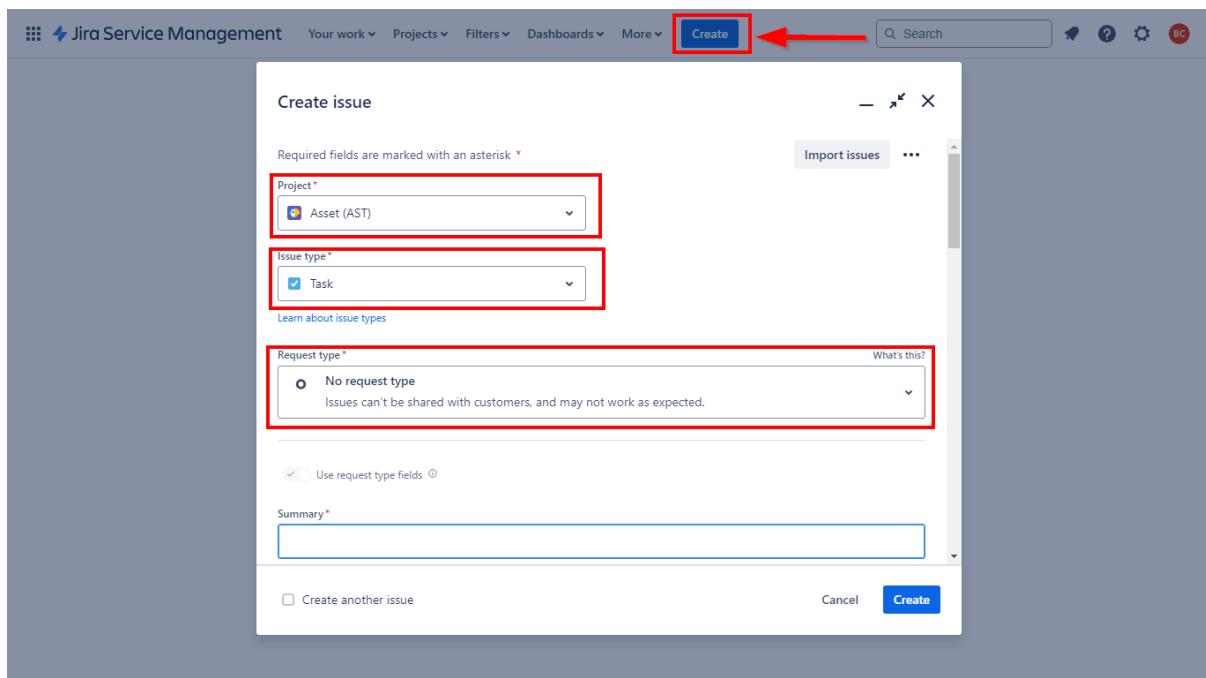
- Project: Asset (AST)
- Issue type: Task
- Request type: No request type (Note: Issues can't be shared with customers, and may not work as expected.)

In the top right corner of the dialog, there is a button labeled "Show fields". A red box highlights this button, and a red arrow points to it from the text above.

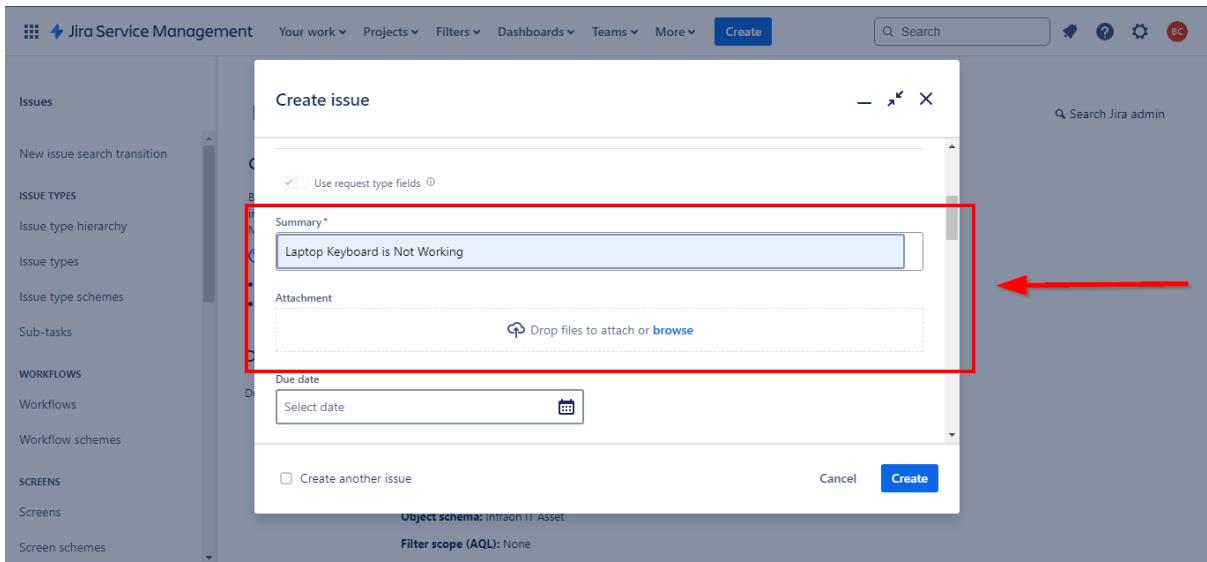
STEP 2: To make your custom field visible on the issue screen, choose it from the list and click "Apply" to confirm the changes.



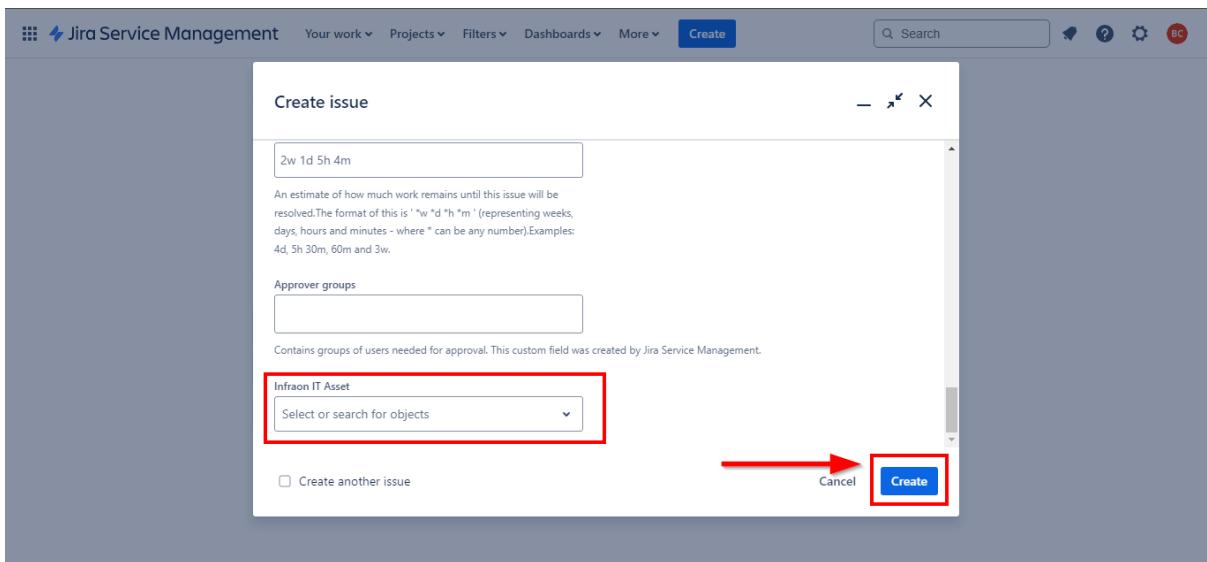
STEP 3: To create a new issue, click the "Create" button in the top panel. Then, select the Project, Issue Type, and Request Type for your issue.



STEP 4: Briefly summarize the issue and attach any files (optional).



STEP 5: Choose the relevant IT asset from the "Infraon IT Assets" field (the custom field we created earlier). Click the drop-down menu, select the asset, and then click "Create" to add the issue.



Viewing JIRA Issues in Infraon Infinity

STEP 1: Start by accessing the IT asset list within the Infraon Infinity portal to view the linked JIRA issue.

The screenshot shows the Infraon Infinity IT Assets list. On the left, there's a sidebar with various icons and a 'Categories' section. The 'All Assets' category is highlighted with a red box. The main area lists several assets, with the asset named '238-B...' highlighted with a red box. A large red arrow points upwards from this highlighted row towards the next step.

STEP 2: On the IT asset details page, find the "Ticket" section located in the left navigation bar. Once there, look for "Ticket Source" in the top right corner and select "JIRA Tickets."

The screenshot shows the Infraon Infinity IT Asset Details page for asset '238-B...'. The left sidebar has a 'Tickets' section highlighted with a red box. In the top right corner, there's a 'Ticket Source' dropdown menu with options: 'Infraon Tickets', 'Jira Tickets' (which is highlighted with a red box), and 'Service Now Tickets'. A red arrow points from the 'Tickets' section in the sidebar towards the 'Jira Tickets' option in the dropdown.

The Infraon Infinity portal provides a seamless way to view JIRA issues, even though they are created on a JIRA platform.

The screenshot displays the Infraon Infinity portal interface. On the left, a sidebar titled "IT Assets > View" shows a tree structure with sections like Details, Asset Life Cycle, Hardware, Software, Events, and Tickets. The "Tickets" section is currently selected. The main panel is titled "Jira Tickets" and lists two items:

- AST-2**: Status: Open, Priority: Medium. Ticket Type: Task. Description: Laptop Keyboard Is Not Working.
- AST-1**: Status: Open, Priority: Medium. Ticket Type: Task. Description: Key Board Is Not Working.

At the bottom of the main panel, it says "Showing 1-2 of 2". There are navigation icons for back, forward, and search. A "Show [10 entries]" button is also present.