Cisco Spaces: Asset Locator Configuration Guide

First Published: 2017-12-17

Last Modified: 2022-11-30

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

CONTENTS

PREFACE

CHAPTER 1

CHAPTER 2

CHAPTER 3

Preface

This preface describes the audience, organization, acronyms, and conventions used in the document.

> **Note** **Cisco DNA Spaces** is now **Cisco Spaces**. We are in the process of updating our documentation with the new name. This includes updating GUIs and the corresponding procedures, screenshots, and URLs. For the duration of this activity, you might see occurrences of both **Cisco DNA Spaces** and **Cisco Spaces**. We take this opportunity to thank you for your continued support.

This document contains the following sections:

Audience

This guide is meant for account administrators who manage the Cisco Spaces user accounts and perform the configurations required for Cisco Spaces. This guide is also meant for business and store administrators who use Cisco Spaces to create the proximity rules to send notifications to customers and business users.

Other target audience includes portal designers and access code managers.

Document Organization

Chapter Number	Chapter Title	Description
Chapter 1	**Cisco Spaces Prerequisites**	Provides information about various Cisco Spaces features and the prerequisites to deploy Cisco Spaces.

Chapter Number	Chapter Title	Description
Chapter 2	**Getting Started**	Provides an overview about Cisco Spaces and its features. This chapter also describes the process flow, system requirements, and how to start working with Cisco Spaces.
Chapter 3	**Cisco Spaces Home**	Provides information about about Cisco Spaces dashboard and its features.
Chapter 4	**Location Hierarchy in Cisco Spaces**	Provides information about how to define Cisco Spaces location hierarchy.
Chapter 5	**Location Hierarchy 2.0 in Cisco Spaces**	Provides information about Location Hierarchy 2.0 and its features in Cisco Spaces.
Chapter 6	**Integration**	Describes how to integrate with Cisco DNA Center and Service Now and other applications.
Chapter 7	**Monitor**	Provides information about the app details mentioned in the Monitoring section.
Chapter 8	**Admin Management**	Provides information about how to manage Cisco Spaces users, Cisco Spaces accounts, and Cisco Connected Mobile Experiences (CMX) accounts.
Chapter 9	**Setup**	Describes how to setup Wireless Network and Meraki Camera.

Document Conventions

This document uses the following conventions:

Table 1: Document Conventions

Convention	Description
Boldface	Commands, command options, and keywords are in boldface.
Italics	Arguments for which you supply values are in italics
Option > Option	Used to describe a series of menu options.

Note Means reader take note. Notes contain helpful suggestions or references to material not covered in this guide.

Tip Means *reader take tip*. Tips contain helpful suggestions to resolve issues.

List of Acronyms and Abbreviations

Table 2: List of Acronyms and Abbreviations

Acronym	Expansion
ACL	Access Control List
BLE	Bluetooth Low Energy
CUWN	Cisco Unified Wireless Network
CNA	Captive Network Assistant
RSSI	Received Signal Strength Indicator
SSID	Service Set Identifier
UUID	Universally Unique Identifier

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you’re looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions, and services, visit Cisco DevNet.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a gateway to the Cisco bug-tracking system, which maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. The BST provides you with detailed defect information about your products and software.

Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.

CHAPTER 1

Overview

Overview

Note **Cisco DNA Spaces** is now **Cisco Spaces**. We are in the process of updating our documentation with the new name. This includes updating GUIs and the corresponding procedures, screenshots, and URLs. For the duration of this activity, you might see occurrences of both **Cisco DNA Spaces** and **Cisco Spaces**. We take this opportunity to thank you for your continued support.

Asset Locator is more than an asset management tool. It is a comprehensive single resource for managing, monitoring, and optimizing your assets, Internet of Things (IoT) sensors, alerting system, and operational workflows. Using a technology-agnostic approach, the solution can use a wide range of tags and sensors, including Wi-Fi, RFID, and environmental monitors, to continually integrate, monitor, and manage your connected operations. Through its cloud-based interface, you can define the profile, category, and ownership of each of the assets. You can establish business rules to define workflows and the expected operating range of your assets and sensors.

Asset Locator then continually monitors data from the sensors attached to your assets—including telemetry data such as temperature and humidity. When any measure deviates from the norm established by your workflows, policies, and business rules, the solution swings into action. It can give you an immediate alert or, if you prefer, can trigger an automated action that is predefined by your workflows and business rules.

The cloud solution and mobile app give you real-time visibility into how your operations are functioning, enabling you to take immediate action and optimize operational processes. In addition, you have access to a wide range of historical reports and Key Performance Indicators (KPIs) to help you continually evaluate the effectiveness of operations and measure the impact of new processes.

Overview

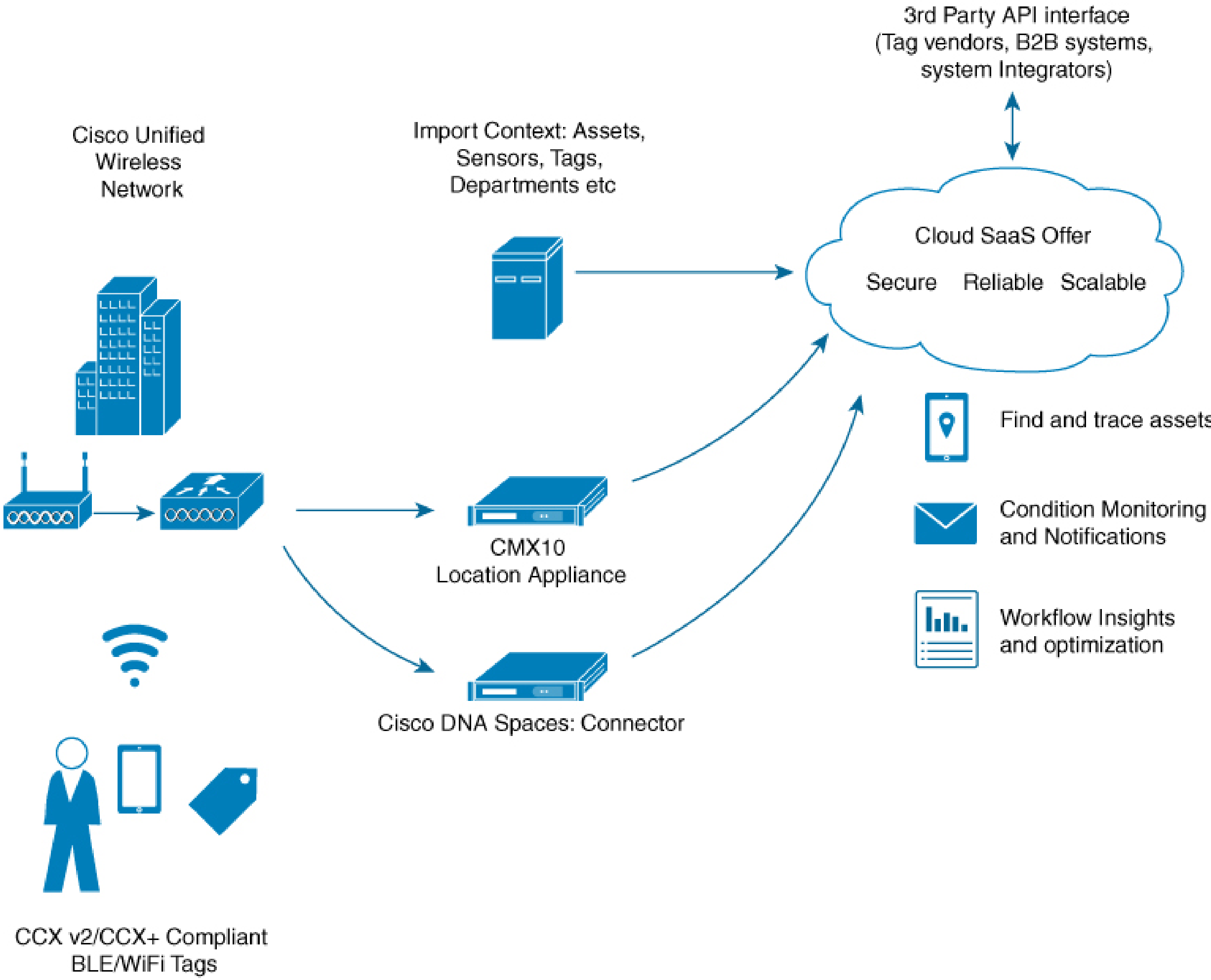
Here is a quick glance at the solution architecture:

- Asset Locator cloud account.
- Assets that are to be tracked.

- Tags (Wi-FI, BLE, or RFID) attached to the assets that need to be tracked.
- Cisco Access Points and Cisco Wireless Controllers.
- Cisco Connected Mobile Experiences device (Cisco CMX) OR Cisco Spaces: Detect and Locate deployed within the network.
- Floor Maps downloaded from Cisco Prime Infrastructure .

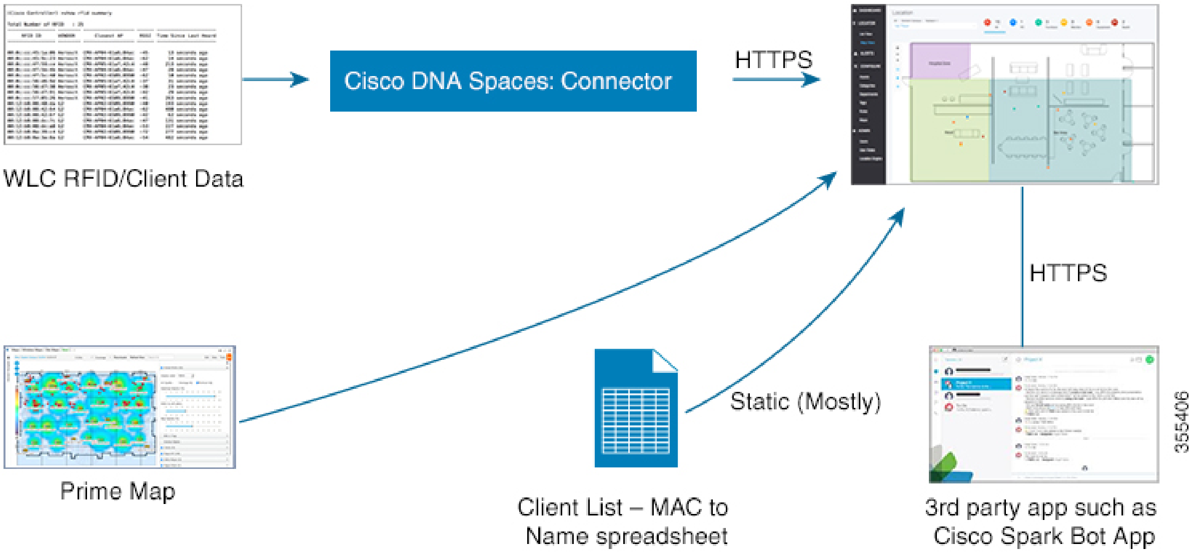
Solution Component	Description	Version supported
Cisco AireOS Wireless Controller	Control and Data	Any wireless controller version
Cisco Access Points	For Wi-FI tags. Location of assets based on RSSI information emananting from tag.	Any AP
Cisco Prime Infrastructure	For AP positioning and exporting maps. (Management)	Cisco PI Version 3.0 and above.
Cisco CMX OR Cisco Spaces: Detect and Locate	Configuration and management required for Asset Locator.	Cisco CMX 10.3.1.x and above.
Tags	Attached to assets that need to be tracked	CCX Compatible, Wi-Fi, BLE, RFID
Assets	Assets that need to be tracked	—
Maps	Building and floors maps exported from Cisco Prime Infrastructure	—
Cisco Asset Locator	Monitor, Track, and Manage assets	—

Figure 1: Information Flow


3rd Party API interface
(Tag vendors, B2B systems, system Integrators)
Cisco Unified Wireless Network
Import Context: Assets, Sensors, Tags, Departments etc
Cloud SaaS Offer
Secure
Reliable
Scalable
Find and trace assets
Condition Monitoring and Notifications
Workflow Insights and optimization
CMX10
Location Appliance
Cisco DNA Spaces: Connector
CCX v2/CCX+ Compliant BLE/WiFi Tags

Note Asset Locator requires a data path that includes either Cisco Spaces: Connector or Cisco CMX.

Figure 2: Information Flow


WLC RFID/Client Data
Cisco DNA Spaces: Connector
HTTPS
HTTPS
Prime Map
Static (Mostly)
Client List – MAC to Name spreadsheet
3rd party app such as Cisco Spark Bot App
355406

Features and Benefits

- **Use your existing wireless network** to provide better operational insights and efficiencies
- **Digitize and capture** indoor location, sensor telemetry and other contextual data from your assets
- **Save critical staff time** by easily managing and quickly locating assets in your facilities
- **Synthesize the collected data** via a sophisticated rules engine, apply business and workflow rules, and automatically trigger defined actions and alerts
- **Reduce manual processes** by tracking, managing, and monitoring Wi-Fi, RFID tags, and telemetry sensors attached to assets
- **Avoid inventory loss or stock outages** by monitoring assets and sensors in real time, applying business and workflow rules, and automatically triggering alerts
- **Automate KPI** monitoring through the web dashboard and reports, for real-time and historical insights to optimize operations
- **Provide connectivity to enterprise applications** via a flexible, API-driven platform
- **Gain unified visibility** across the entire organization from a single cloud-scaled dashboard while providing custom roles and permissions to users
- **Reduce CapEx and maintenance costs** with a SaaS subscription model

Table 3: Features and Benefits

Feature	Benefit
Cisco Compatible Extensions (CCX) compatibility	Provides support for multiple tag providers Helps reduce new investment when tag systems are already deployed
Cloud service	Reduces installation cost and time Improves scalability as demand grows Improves solution through continuous feature development and faster deployment
Asset track and trace, monitoring, and management	Improves efficiency of critical staff by reducing manual monitoring and tracking of assets Improves asset utilization by analyzing movement and utilization patterns Improves tactical operations through real-time visibility into all assets in a facility
Rules	Enables automated workflows through rules that address conditions such as asset location, motion status, environmental telemetry, and other business attributes Avoids inventory loss or stock outages through an alerting system Detects the temperature and humidity of refrigerators to maintain an acceptable range for temperature-sensitive assets Tracks assets based on entrance, exit, or motion-sensing events Improves safety and security by detecting panic button trigger
Alerting system	Reduces downtime by triggering alerts when asset condition exceeds threshold defined by business rules and workflows Helps keep staff informed through alerts sent by email or text message Automatically classifies assets based on rule conditions Manages alerts with built-in audit trail and alert management system Triggers secondary workflows through API triggers to other enterprise back-end systems

Feature	Benefit
Reporting	Reduces time spent collecting data, monitoring assets, and reporting Helps improve decision-making through automated and customizable KPI reports Enables compliance reporting with historic records on telemetry data (temperature, humidity, etc.) and asset status
Mobile app	Provides a user-friendly interface to help reduce time spent searching for assets inside a facility Uses the mobile device's location to further improve asset search by limiting results to nearby assets and alerts Improves response to and compliance with alerts through notifications and easy alert management Improves user experience and mobility for staff on the floor

Licensing

Cisco Spaces: Asset Locator is tag and sensor technology agnostic. Depending on your technology preferences, you can purchase sensors from any CCX-compliant tag vendor.

The web and mobile platforms give you the power to tailor the solution to your needs. How do you want to categorize your assets? What workflows are important to your operations? Through a single, cloud-based interface, you have complete control over each of these elements. And by automating your workflows and alerts, you no longer need to spend cycles on day-to-day monitoring, but rather can focus on continually improving your operations.

Asset Locator is a component of Cisco Spaces, a cloud-based and mobile solution that can be deployed easily and quickly. And its subscription model helps provide predictable, year-to-year operational expenses. Asset Locator is included in the Cisco Spaces ACT license.

Navigate to **Settings > Licenses** to find details of existing license.

- **Type—**Type of License (Evaluation or Advanced)
- **End Date—**Date of expiry of license
- **Days Remaining—**Number of days remaining for the license to expire.
- **Account Name—**Account Name of License
- **Account Number—**Account Number of License

CHAPTER 2

Setup

Setup

Request a Cisco Spaces: Asset Locator Account

Request an account on Cisco Spaces by sending an email to cisco-dnaspaces-support@external.cisco.com requesting for a demo or live account creation on the Cisco Spaces dashboard. For more information, see Getting Started with DNA Spaces Dashboard.

Setup Connectivity between Asset Locator and Cisco Spaces

Refer to Cisco Spaces: Connector Configuration Guide for more information.

Setup Connectivity between Asset Locator and Cisco CMX (Release 10.6 and above)

To set up connectivity between Asset Locator and Cisco CMX release 10.6 and greater, no configuration is necessary on Asset Locator. You can follow instructions in the Configuring Cisco CMX 10.6 and above.

Note You can use the **dnaspaces-stream** channel to track data flow from Cisco CMX to Asset Locator.

Setup Connectivity Between Asset Locator and Cisco CMX (Prior to Release 10.6)

To setup connectivity between Asset Locator and Cisco CMX prior to Release 10.6, no configuration is necessary on Asset Locator.

Step 1 Import maps from Cisco PI to Cisco CMX

Refer to *Import Maps from Cisco PI to Cisco CMX* section of the Appendix.

Step 2 Connect the Cisco CMX to Cisco Spaces.

Refer to *How to Obtain a token from Cisco Spaces* section of the Appendix.

Step 3 Configure notifications on Cisco CMX.

Refer to *Configuring Notifications on Cisco CMX 10.5 and below* section of the Appendix.

Setup Connectivity Between Asset Locator and Cisco Spaces: Detect and Locate

To setup connectivity between Asset Locator and Cisco Spaces: Detect and Locate, no configuration is necessary on Asset Locator. This is because the system auto-provisions the dnaspaces-stream during customer onboarding or asset provisioning

CHAPTER 3

Manage Maps

Manage Maps

Uploading Maps

One of the first setup tasks involved in setting up Asset Locator is uploading maps exported from Cisco Prime Infrastructure to Asset Locator.

Note If Asset Locator is launched through Cisco Spaces, maps are automatically synced into Asset Locator.

Before you begin

If you are using Cisco CMX release 10.5 or earlier, refer to Importing Maps from Cisco PI to Cisco CMX.

Step 1 Log in to the Asset Locator.

Step 2 From the left-navigation pane, click **Configure** > **Maps**, and then click **Upload** button.

Step 3 Browse to the location and select the maps exported previously from Cisco Prime Infrastructure .

Step 4 Verify if the maps were uploaded successfully by selecting the floor map.

Create Chokepoints (Monitors)

From the left-navigation pane, click **Configure** > **Maps**, and browse to the location where you need to create a chokepoint. Click the chokepoint icon from the toolbar to the left as shown and enter the details of the chokepoint before placing it on the map.

Create Zones

From the left navigation pane, click **Configure > Maps**, and browse to the location where you need to create a chokepoint. Click the Zone icon from the toolbar to the left as shown and add the name of the zone before placing it on the map. Once added, you can zoom into the zone and view it.

CHAPTER 4

Manage Assets

Manage Assets

Category

Categories and subcategories are customized classfiications for your assets. Add categories from the **Categories** tab in the left navigation pane. You can use Categories to group and classify your assets like wheelchairs, IV pumps, forklifts, carts, and so on.

Step 1 From the left navigation pane, click **Categories** and then **Add** in the main area of Asset Locator.

Step 2 In the **Category** dialog box click **General**, enter the name and select a **Department**. You can also configure **Subcategories** here.

Step 3 (Optional) Add custom asset field for the category and click **Save**.

Step 4 (Optional) Click **Upload Picture** tab and click the **Click to Upload** button, and browse for an image. Note that all assets that are assigned to the category are also assigned the same picture as an icon.

Departments

Adding Departments (and categories) are a prerequisite step to adding your assets manually, one after the other, to the Asset Locator.

Add departments using the **Configure** > **Departments** tab in the left-navigation pane. Departments can be created according to the team that owns the assets. Department is a mandatory configuration. Examples of departments are Sales, Finance, Kitchen, Human Resources (HR), Foundry, OR, and ICU.

Step 1 From the left navigation pane, click **Configure** > **Departments** and then **Add** in the main area of Asset Locator.

Step 2 In the **Name** field, enter a name for the department along with other information, and click **Save**.

Creating Assets Manually

From **Configure** > **Assets**, you can add your assets to the Asset Locator either individually or in bulk, using an asset upload CSV file. If you prefer to upload your assets in bulk, refer to Uploading Assets in Bulk, on page 13.

Note Department and Category must be configured in Asset Locator before assets can be manually added.

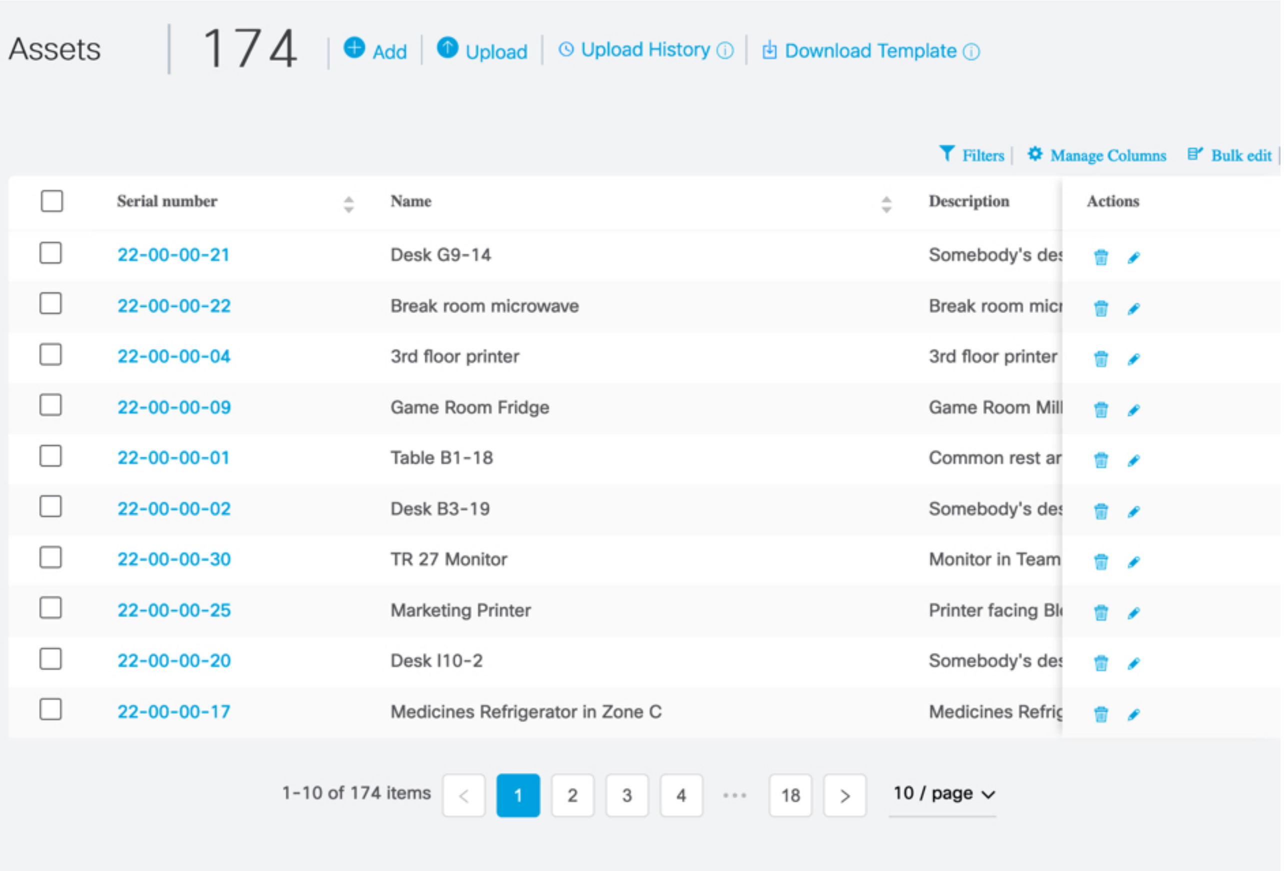
Adding Assets Individually

This task shows how to add assets individually. Note that, you must configure Categories and Departments before adding assets individually.

Step 1 Click **Add** to add assets individually. In the **Asset** Dialog box, enter the Asset details, select department, category and assign a tag. By default, the State of an asset is Active. Select Inactive only if the asset need not be tracked. For static assets (no location information being received), you can manually add the location under the **Static Location** tab. You can add an icon for the asset by clicking the **Upload Picture** tab. If the asset is assigned to a category which has an icon as well, this icon overrides that icon. You can add enable Telemetry from the **Tags** tab.

Note **Assigned Site** is an optional field defining where the asset belongs to in the region. Assigned Site can be Campus, Building or Floor level as per the uploaded maps. This field is used for the Role Based Access Control to prevent users from seeing assets from sites they are not assigned to. For your assets to be available for a particular site, the assets must be configured with the proper assigned site.

Step 2 Verify that your assets where added successfully by navigating to the asset tab on the navigation panel. To view the details of your asset and tag, navigate to the list view under Locator and click on an asset.



□	Serial number	Name	Description	Actions
□	22-00-00-21	Desk G9-14	Somebody's des	
□	22-00-00-22	Break room microwave	Break room micr	
□	22-00-00-04	3rd floor printer	3rd floor printer	
□	22-00-00-09	Game Room Fridge	Game Room Mill	
□	22-00-00-01	Table B1-18	Common rest ar	
□	22-00-00-02	Desk B3-19	Somebody's des	
□	22-00-00-30	TR 27 Monitor	Monitor in Team	
□	22-00-00-25	Marketing Printer	Printer facing Bl	
□	22-00-00-20	Desk I10-2	Somebody's des	
□	22-00-00-17	Medicines Refrigerator in Zone C	Medicines Refrig	

Step 3 Click **History** to see the details of Asset's location, telemetry, alerts and location on the map.

Uploading Assets in Bulk

Asset upload functionality allows you to upload new assets as well as update existing assets.

Note Asset Locator automatically creates categories and departments if they have not been created previously.

Ensure that the following mandatory fields are included in the Asset Upload CSV file for each asset.

- Serial Number
- Department Name
- Category Name
- Tag Type

Step 1 From Asset Locator, click **Configure** > **Assets** > **Download Template**. Fill the sample template downloaded and click **Upload**

Step 2 Verify the status of your asset upload clicking **Upload History**. You can view the status of upload even if the upload was not successful or if the upload process is ongoing. Once the status indicates success, verify if the assets are available on the **Assets** page.

CHAPTER 5

Manage Rules

Configuring Rules and Actions

Asset Locator rule engine allows to keep track of your assets using location and environmental monitoring. The rules keep track of your assets using the location and the status of the associated tags. You can have different types of rules that check for conditions like asset movement, change in asset location, entering or exting of asset into a specific bulding, floor, zone (logical area) or change in asset conditions like temperature or humidity or battery level (of associated tag). When the conditions are fulfilled, the rules trigger actions like sending SMS, Emails, HTTP notifications or even modification of asset attributes.

The Asset Locator rules can be configured and modified at any time. Asset Locator rules are meant to save massively on manual operations and give the business more assurace concerning the precision of their asset record and outright docility conditions.

Below are a few examples of usecases using rules:

- **Temperature**: Send notifications when the temperature of a tag attached to an asset goes **Below/Above** a temperature or **Between/Out of Range** of temperatures
- **Battery**: Send notifications when the battery levels of a tag attached to an asset goes **Below/Above** a percentage level or **Between/Out of Range** of percentage levels.
- **Humidity**: Send notifications when the humidity of a tag attached to an asset goes **Below/Above** a percentage level or **Between/Out of Range** of percentage levels
- **Missing**: Send notifications when a tag attached to an asset is uncommunicative. Also send notifications when the asset/tag reappears.
- **Location Dwell**: Send notifications when a tag attached to an asset is within a configured location, which could be a Campus, Building, Floor, Zone, or chokepoint.
- **Location Entrance**: Send notifications when a tag attached to an asset enters **From** a certain location **To** a certain location, where location could be a Campus, Building, Floor, Zone, or chokepoint. Note that both locations must be different for this notification.
- **Location Exit**: Send notifications when a tag attached to an asset exits **From** a certain location **To** a certain location, where location could be a Campus, Building, Floor, Zone, or chokepoint. Note that both locations must be different for this notification.

- **Button Press**: Send notifications when an emergency button on a tag (attached to an asset) is pressed, assuming that tag transmits immediately.
- **Motion**: Send notifications when a tag attached to an asset experiences one or more motion types. Motion type is tag-vendor dependent.
- **Attribute Condition**: Update the value of an attribute and observe the attribute updates on the Locator Tab. You can label assets based on their status. The available attribute types are displayed in the image. You can add a new attribute from **Assets>Columns>Add New Field**.

Step 1 In the left navigation pane, click **Configure>Rules>Add**.

Step 2 Enter a **Name** for the rule. This will be used in the content of notifiations sent via SMS, E-mail, API, or system alert.

Step 3 Choose a **Priority**.

Step 4 Enter a descrption for the rule.

Step 5 Click the **Enabled** button to activate or deactive the rule.

Step 6 (Optional) Click the **Advanced** button to enable the **ASSET FILTER** pane, which allows you to restrict the scope of the rule to a particular category, department, or asset. If disabled, the rule is applicable to all categories, department or assets.

a) In the **ASSET FILTER** pane, choose a **Category** or **Department** or specific asset(s) on which the rule is to be applied.

Step 7 Select the condition under which the rule is to be applied on:

- **Temperature**: You are notified when the temperature of a tag attached to an asset goes **Below/Above** a temperature or **Between/Out of Range** of temperatures. Supported units include Celsius and Fahrenheit.
- **Humidity**: You are notified when the humidity of a tag attached to an asset goes **Below/Above** a percentage level or **Between/Out of Range** of percentage levels.
- **Battery**: You are notified when the battery levels of a tag attached to an asset goes **Below/Above** a percentage level or **Between/Out of Range** of percentage levels.
- **Attribute**: You are notified based on the value of an attribute.

  Note Attributes support the date time format.

- **Missing**: You are notified when a tag attached to an asset is uncommunicative for over five minutes. You are also notified when the asset reappears.

  Note
  - Missing alert is generated when a tag is not heard for over five minutes. If the tag stays missing, you will receive another alert as per the configured **Repeat Notification Every** interval of the Action.
  - A reappearance alert is generated when the tag is heard from again.

- **Location**: You are notified according to location of an asset.

Note

- Use Location entrance to track an asset which moves between two different locations only. Alert is not triggered if an asset returns to a location after exiting the same location. Refer to the example below:

  a. Location Entrance condition is **From** Building B **To** Building A.

  b. Asset enters Building A.

  c. Asset leaves Building A for a time, say 30 minutes or eight hours.

  d. Asset returns to Building A. Alert is not triggered as Asset did not enter from Building B.

- **Repeat notification delay** value of an Action is ignored for Location **Exit** and **Entrance** conditions.

- For all other Location conditions, **Repeat notification delay** is pertinent. If an asset leaves a zone, re-enters a zone, and leaves the zone again before the **Repeat notification delay** time is up, you receive only an initial alert indicating that the asset is missing. The next alert is generated only after the **Repeat notification delay** interval is up.The example below illustrates the same:

  a. **Repeat notification delay** is configured for one hour.

  b. Asset leaves premises at 9:00 AM. An alert is generated.

  c. Asset returns to premises at 9:15 AM. No alert is generated.

  d. Asset leaves premises at 9:30 AM. No alert is generated until the hour is up.

If the **Trigger on Chokepoints** is enabled, alert is generated only when assets enter the range of a chokepoint.

- **Motion**: You are notified when a tag attached to an asset experiences one or more motion types. Motion type is tag-vendor dependent. For Centrak tags, valid types are **Stationary** and **Movement**.
- **Button Press**: You are notified as soon as an emergency button on a tag attached to an asset is pressed, and the tag beacons immediately. Button type is tag-vendor dependent. Users can label buttons as needed. Below is a list of third party tags and their respective mapping on the Asset Locator dashboard.
  - **Aeroscout**
    - **Button Press**: You are notified as soon as the button on a Aeroscout tag attached to an asset is pressed.
    - **Tampering**: You are notified as soon as an Aeroscout tag attached to an asset is tampered with.
  - **Centrak**
    - **Button 1**: You are notified as soon as the green button on a Centrak tag attached to an asset is pressed.
    - **Button 2**: You are notified as soon as the yellow button on a Centrak tag attached to an asset is pressed.
    - **Button 3**: You are notified as soon as the red button on a Centrak tag attached to an asset is pressed.

Step 8 Configure a delay for the actions to be performed when a rule condition occurs.

The delay can be of two types:

- **Trigger After Time**: Trigger an action only after a configured time delay. **IMMEDIATELY** triggers action at the next tag transmission. This field is dependent on the tag transmission period.

- **Trigger After Count**: Trigger an action only after a configured number of assets satisfy the condition.

Step 9 Configure an action to be triggered after a condition is met. An action can be of four types:

- Email: Send emails at a configured frequency.
    - **Subject:** Enter a heading for your Email.
    - **Message:** Enter a message body for your Email.
    - **User's Email:** Choose addresses already configured on the Asset Locator dashboard.
    - **Other email addresses:** Enter addresses not configured on the Asset Locator dashboard.
    - **Repeat notification delay:** Configure frequency at which alerts must be sent to the Email addresses.
    - **Location-based Alerting:** Enter phone numbers not configured on the Asset Locator dashboard.
- SMS: Send SMS at a configured frequency.
    - **Message:** Enter a message body for your SMSs.
    - **Repeat notification delay:** Configure the frequency at which SMSs must be sent to the phone numbers.
    - **Users:** Note that only users with validated phone numbers appear here. To validate the phone number of a user, login as the user and click **User Settings** from the gear drop-down in the top-right corner. In the page that opens, click on **Phone Validation** and complete the steps provided.
    - **Location-based Alerting:** You can enter phone numbers not configured on the Asset Locator dashboard. This allows individual users to receive location-based alerts.

      However, individual users must opt in their phone numbers for receving alerts by logging into their accouns on the Asset Locator dashboard. Follow the instructions frrom Opting Your Device for Location-Based Notifications, on page 19.

      Administrators must also enable user tracking on the Asset Locator dashboard by updating the user data with the device MAC addresss. Follow the instructions from Opting Your Device for Location-Based Notifications, on page 19.
- HTTP: Send messages to configured URLs at a configured frequency.
    - **URL:** Configure the URL of your server.
    - **Message:** Enter content for the body of the alert.
    - **Repeat notification delay:** Configure the frequency at which alerts are sent to the server.
    - **Disable Alerts:** Disables creation of alerts for a particular rule. This option can be used when notifications are forwarded to third party services for consumption.
- Asset Attribute: Update an attribute with a value.
    - **Asset Attribute:** Choose asset states, static fields, and custom fields configured for an asset on the Asset Locator dashboard.

Note

- Rules configured only with **Attribute update** action will not trigger alerts in the **Alerts** view.
- All other alerts (action: SMS, Email, HTTP) will trigger alerts in the **Alerts** view in addition to performing configured actions.
- You can assign **Open/In Progress/Done/Closed** status to an alert based on the progress of the alert.
- Closing an alert without any action on an alert does not mean that an alert is gone from the system. You can view the alert in the **Closed** widget.

Note

- If tag transmission rate is once an hour, you should configure the **Repeat notification value** of an **Action** to be an hour or more.
- **Trigger After** and **Repeat notification value** is dependent on Tag transmission rates.

Opting Your Device for Location-Based Notifications

This task is a prerequisite to enable location-based notifications to an individual user's email address or phone number. This task is necessary for the proper functioning of a rule configured with Location-based alerting.

Step 1 (Administrator Task) From the **User Management > App Users** tab, you, as an Administrator, can click the respective

📱 icon for a user. In the **User** dialog box that opens, enter a name and the MAC address of the user's mobile device or any device tag used to track the user.

Step 2 (User Task) From the Asset Locator dashboard, you, as an Asset Locator user, must click **User Settings** from the gear drop-down in the top right corner. In the page that opens, click on **Phone Validation** button.

Step 3 In the **Phone Validation** popup that is displayed, and follow the instructions displayed.

CHAPTER 6

Manage Reports

Manage Reports

Asset Locator provides detailed reports of asset inventory, alert history, battery information, temperature and humidity. You can download any report in the CSV or PDF format. You can subscribe to it or subscribe others to receive an email with the report. You can edit the reports and save them as your default view for the next time you need to consult them.

- Inventory report: List of all assets in the system right now.
- Low Battery Summary: List of all assets in the system right now with battery level less than the selected threshold.
- Alert History: Alert history as a table for a selected time range.
- Temperature: Formatted report with temp history as chart and table for a selected time range
- Humidity: Formatted report with humidity history as chart and table for a selected time range

This section takes you through the process of creating Reports using asset details.

Step 1 In the left-navigation pane, click **Reports > My Reports**.

Step 2 Click **Add** to add a new report.

Step 3 In the **Create Report** dialog box that is displayed, choose a report template.

- Click **Inventory Report>Create**. A report of all assets in the system is displayed.
- Click **Low Battery Summary>Create**. You can click the filter button on the right to modify the a **Battery Limit**. A battery report is displayed with all the assets having a tag battery percentage that is below the specified limit. You can modify the battery percentage value to modify the report.
- Click **Alert History>Create**. A report of all the alerts in the system over the past seven days is generated by default. You can modify the range of the report as required (last three days, yesterday, today) by clicking the filter button on the right. Maximum configurable time limit is 90 days.
- Click **Temperature** and choose to filter by departments or categories or individual assets and click **Create**. A preview of the report of the temperature of the surrounding environment of assets during the last week is displayed. Maximum configurable time limit is seven days.

- Click **Humidity** and choose to filter by departments or categories or individual assets and click **Create**. A report of the humidity of the surrounding environment of assets during the last week is displayed. Maximum configurable time limit is seven days.

Step 4 Enter a Title and Description for your report.

Step 5 Use the **Attributes** check boxes on the left to customize the columns displayed in the report. Once selected, they appear as objects in the Columns selected that can be you can drag and reordered as required to be displayed on the report.

Step 6 Click the filter button on the top right to customize the records displayed based on specific conditions. For example, display records that have battery values lower than a particular percentage.

Step 7 Note that you can already see partial results of your report. Click **Save** > **Run** to view the complete report.

Step 8 Configure E-mail subscriptions to your report by specifying E-mail addresses, the days and time on which the report needs to be sent, and the format used for the report, which can be PDF or CSV. You can also apply filters in this view.

Step 9 Now save any changes made to the report.

Step 10 Trigger the download of the report as PDF or CSV. The downloaded files appear in the **Recent Downloads** section on the top right, which includes links to all downloads triggered in the last 24 hours.

Step 11 Once done with a particular report, click the Back arrow to return to the Reports dashboard.

Step 12 From the Reports dashboard, you can perform different actions on individual reports. Choose from one of the following:

- Remove: Delete a report.
- Edit Report: Modify a report.
- Copy Report: Duplicate a report.
- Share Report: Pick users to share a report with. Only those users who have access rights to view the report can be selected. Other users are greyed out.
- View Report Subscribers: View the subscriptions active for this report.

Step 13 Click **Manage Columns** to modify the columns and the order of the columns of the reports dashboard.

Step 14 Click **Download History** to view the details of reports downloaded in the last 24 hours.

Step 15 Click **Reports**> **My Subscriptions** to view the subscriptions created by you or subscribed by you. From the first tab, you can delete subscriptions you have created, and from the second tab, you can unsubscribe from subscription you are part of.

CHAPTER 7

Manage Users

Manage Users

Managing users is done using the **User Management** tab which is further divided into four tabs

- **Administrators**—Lists information about administators defined on the Cisco Spaces dashboard with administrative access rights to the app.
- **App Users**—Lists information about users defined within the Cisco Spaces: Asset Locator application
- **User Roles**—Define role-based access control (RBAC), where users or groups of users are provided with various user roles.
- **Permissions**—Define an access profile for each User Role. A profile is a collection of controls and restrictions which can be then assigned to a user role

Configuring User Permissions, User Roles, and Users

The Asset Locator users are provided with Role-based access control (RBAC), where users or groups of users are provided with various User Roles. Some of the User Roles are AdminAccess and ReadOnlyAccess.

User Roles are differentiated by the permissions associated, departments, categories and sites. You can establish permissions for individual components of Asset Locator, allowing you to delegate and share responsibilities across your organization.

For instance, your floor staff might have require access rights to viewing or searching for assets, and executing reports. However, your IT staff will require access rights to add and edit assets and create new reports

Permissions are in the form of profiles that are associated with User Roles. A profile is a collection of controls and restrictions which can be then assigned to a User Role. Permissions are created by selecting checkboxes for various Asset Locator features like **Configure Assets**, and assigning permissions like view or edit to these features.

Before you begin

- Ensure that categories and departments are configured.
- Ensure that maps are uploaded.

Step 1 (Optional) In the left navigation pane, click **User Management>Permissions**.

a) Click **Add**.

b) In the **Permission** dialog box, enter **Name**, **Description**, and configure the necessary permissions by selecting the checkboxes and click **Save**.

Table 4: Default Permissions and Priviliges

Permissions	Privilige
AdminAccess	Read and write access to entire system.
ReadOnlyAccess	Read only access.

Step 2 In the left navigation pane, click **User Management>User Roles** and click **Add**.

Step 3 In the **Role** dialog box, do the following:

a) Name: Enter a Name for the user role.

b) Permission: Select a Permission from the drop-down list.

c) Select specific **Departments**, **Categories** or **Sites**.

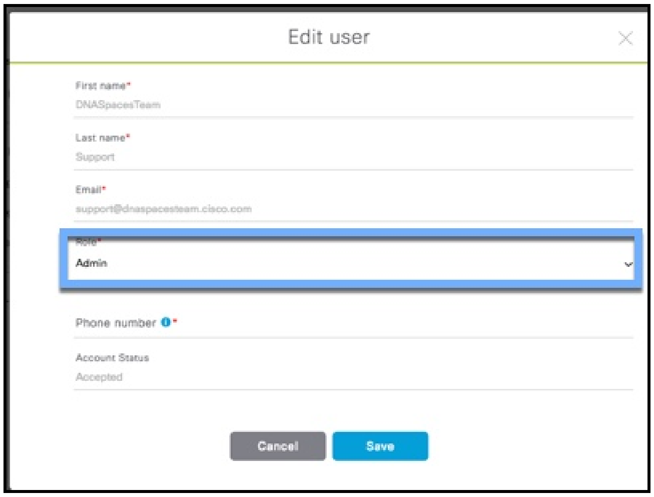
Step 4 Invite users by entering their email IDs and selecting **Role** as configured in Step 2.

Modifying Users and User Roles

You, as an administrator, cannot modify the personal details of a user. The users also cannot modify their personal details from the **User Management** tab.

The Asset Locator Administrator can modify user roles only. The Asset Locator Administrator can edit the role of a specific user by editing user details from **User Management>App Users**.

Figure 3: Adminstrator can only modify roles of each individual user



Edit user

First name*
DNASpacesTeam

Last name*
Support

Email*
support@dnaspacesteam.cisco.com

Role*
Admin

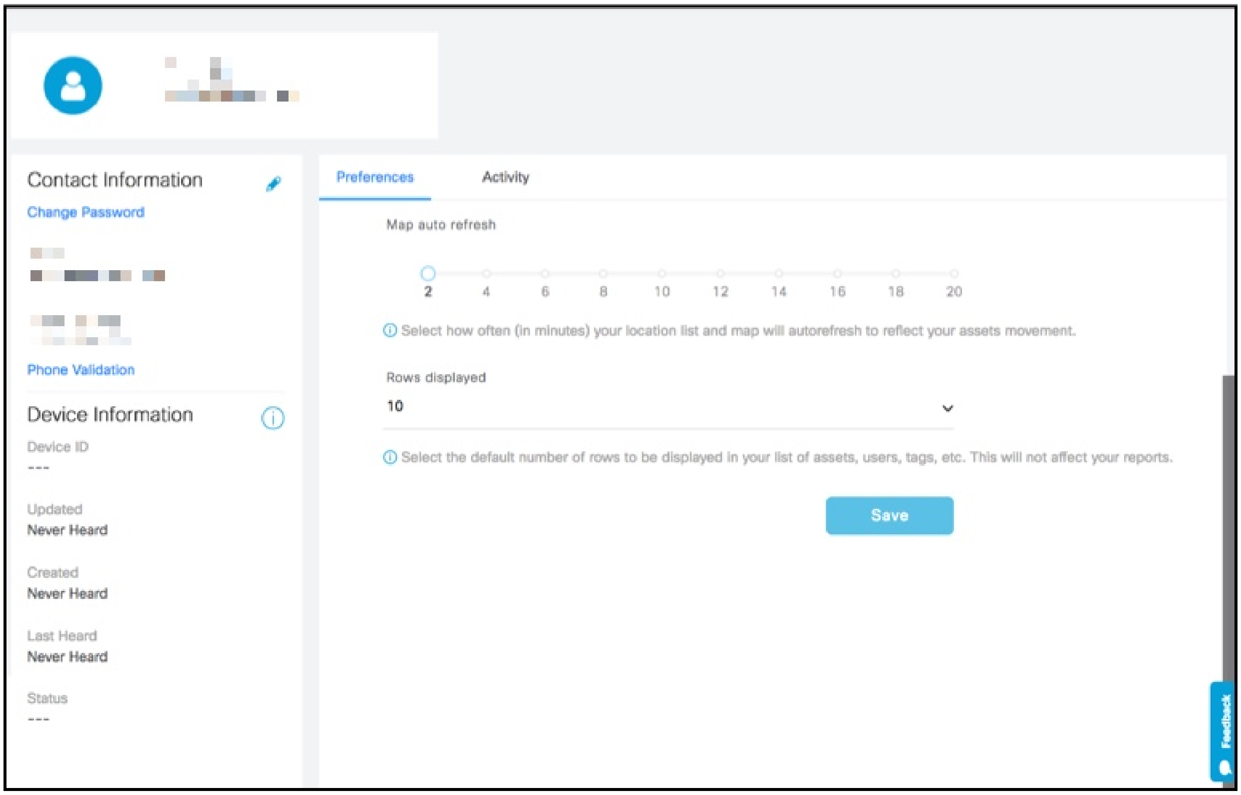
Phone number*

Account Status
Accepted

Users listed under **User Management** > **Administrators** are administrators defined in the Cisco Spaces dashboard. This type of user cannot be edited from Asset Locator, and can be edited from the Cisco Spaces dashboard only.

Step 1 To modify user details, users must log in to their respective accounts on the Asset Locator dashboard and click the profile button in the top right corner, and from the drop-down menu, click **User Settings**. Look for **Contact Information** and click the pencil icon beside it.

Figure 4: Users can modify personal details from User Settings



[redacted]

Contact Information

Change Password

[redacted]

Phone Validation

Device Information

Device ID

Updated
Never Heard

Created
Never Heard

Last Heard
Never Heard

Status

Map auto refresh: 2

ⓘ Select how often (in minutes) your location list and map will autorefresh to reflect your assets movement.

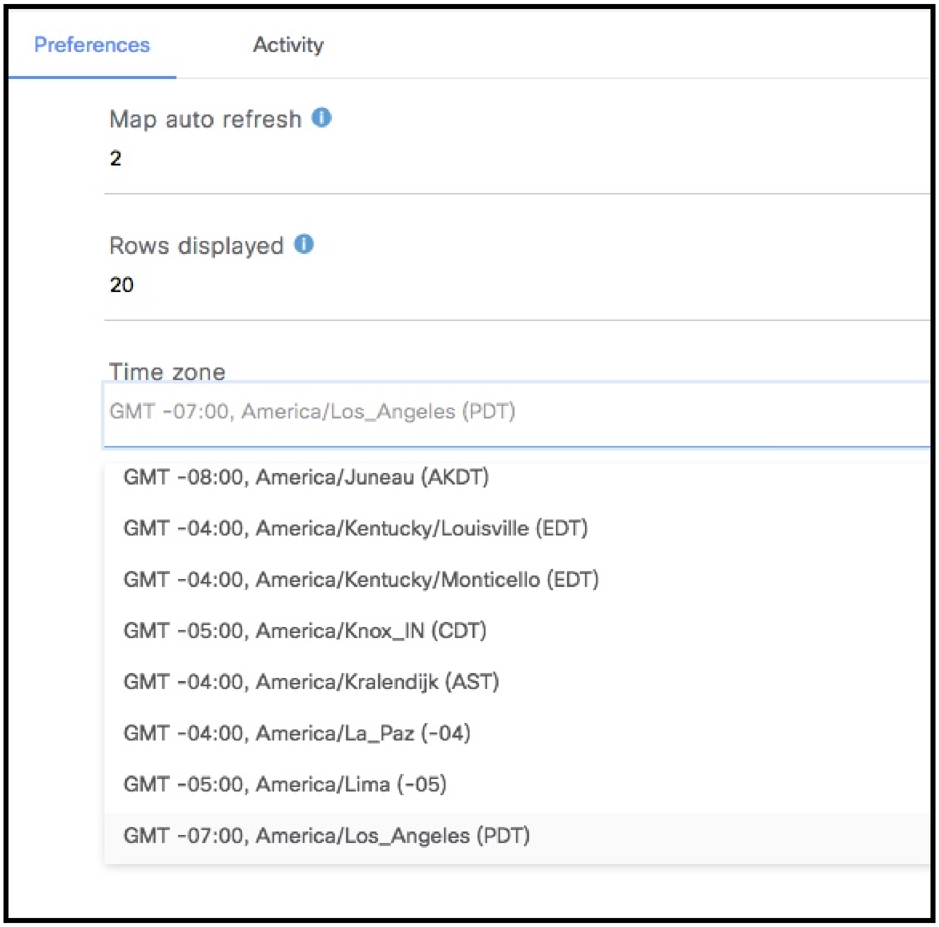
Rows displayed: 10

ⓘ Select the default number of rows to be displayed in your list of assets, users, tags, etc. This will not affect your reports.

Step 2 From the **Preferences** tab of this page, you can set the following:

- Map auto refresh: Select how often (in minutes) your location list and map auto refreshes to reflect your assets movement.
- Rows displayed: Select the default number of rows to be displayed in your list of assets, users, tags, and so on. This value does not affect your reports.
- Time zone: Select your time zone.

Figure 5: Time Zone Selection



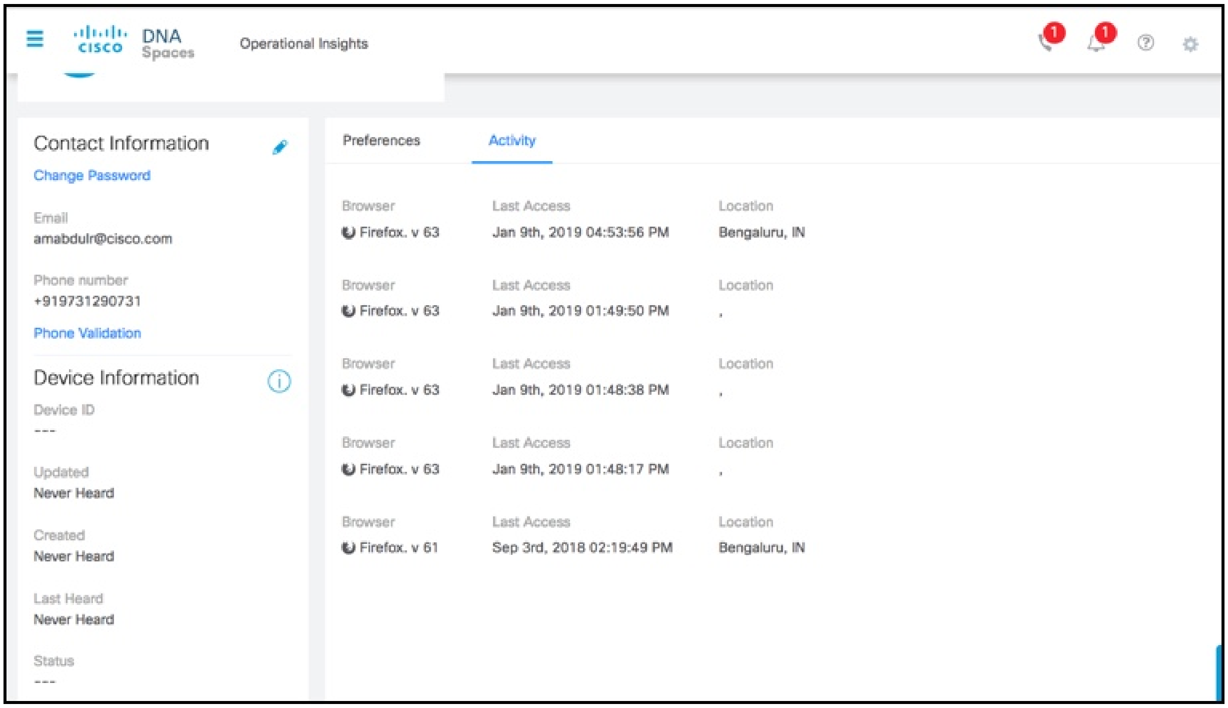
Map auto refresh
2

Rows displayed
20

Time zone
GMT -07:00, America/Los_Angeles (PDT)

GMT -08:00, America/Juneau (AKDT)
GMT -04:00, America/Kentucky/Louisville (EDT)
GMT -04:00, America/Kentucky/Monticello (EDT)
GMT -05:00, America/Knox_IN (CDT)
GMT -04:00, America/Kralendijk (AST)
GMT -04:00, America/La_Paz (-04)
GMT -05:00, America/Lima (-05)
GMT -07:00, America/Los_Angeles (PDT)

Step 3 From the **Activity** tab, you can observe dasboard access activity like browsers used, access time, and location.



Contact Information

Change Password

Email
amabdulr@cisco.com

Phone number
+919731290731

Phone Validation

Device Information

Device ID

Updated
Never Heard

Created
Never Heard

Last Heard
Never Heard

Status

Preferences | Activity

Browser	Last Access	Location
Firefox. v 63	Jan 9th, 2019 04:53:56 PM	Bengaluru, IN
Firefox. v 63	Jan 9th, 2019 01:49:50 PM	,
Firefox. v 63	Jan 9th, 2019 01:48:38 PM	,
Firefox. v 63	Jan 9th, 2019 01:48:17 PM	,
Firefox. v 61	Sep 3rd, 2018 02:19:49 PM	Bengaluru, IN

CHAPTER 8

Track and Trace

Track and Trace

Dashboard View

The dashboard shows the summary of all statistics associated with your account.

- Navigate to a location using the map and click a particular location and view the summary statistics by location.
- Navigate to a location using the drop-down menu on the top-left and view the summary statistics by location.
- For the selected location, view Assets by department, category, and sub-divided locations, and click to view the assets as a filtered list view of the Locator tab. The **No Location** pie is used to indicate those assets that have never been heard by the system and hence have no recorded location.
- For the selected location, view Alerts by department, category, rules, priority, and sub-divided locations, and click to view the alerts as a filtered view of the assets tab.

Locator

Asset Locator presents your assets and their details with the Locator Tab. You can view the assets on a List or Map view. You can further apply filters to this view and save for later use as customized widgets, or downloaded as CSV files.

You can click the assets in any of these views for a more detailed view or the Asset 360 view which inlcudes further details like telemetry information, activity on a particular date, playback of asset history for different dates, heatmaps and location trails.

Search

You can search for assets in the Locator: List View or Map View. You can search by the asset name, location, or any of the attributes associated with the asset.

Filter

You can filter **Manage Wideget** button to add a Canned widget, which is a widget based on an existing template. Alternatively, you can fliter your information and click **Save As New** to create a new widget.

Widget

Click the **Manage Wideget** button to add a Canned widget, which is a widget based on an existing template. Alternatively, you can fliter your information and click **Save As New** to create a new widget.

Locator: List View

The list view allows you to see a list of assets. These assets can be downloaded in CSV format.

Locator: The Map View

The map view allows you to create zones for creation of effective alerts.If assets are too close to one another, note that the map displays them as a clustered view.

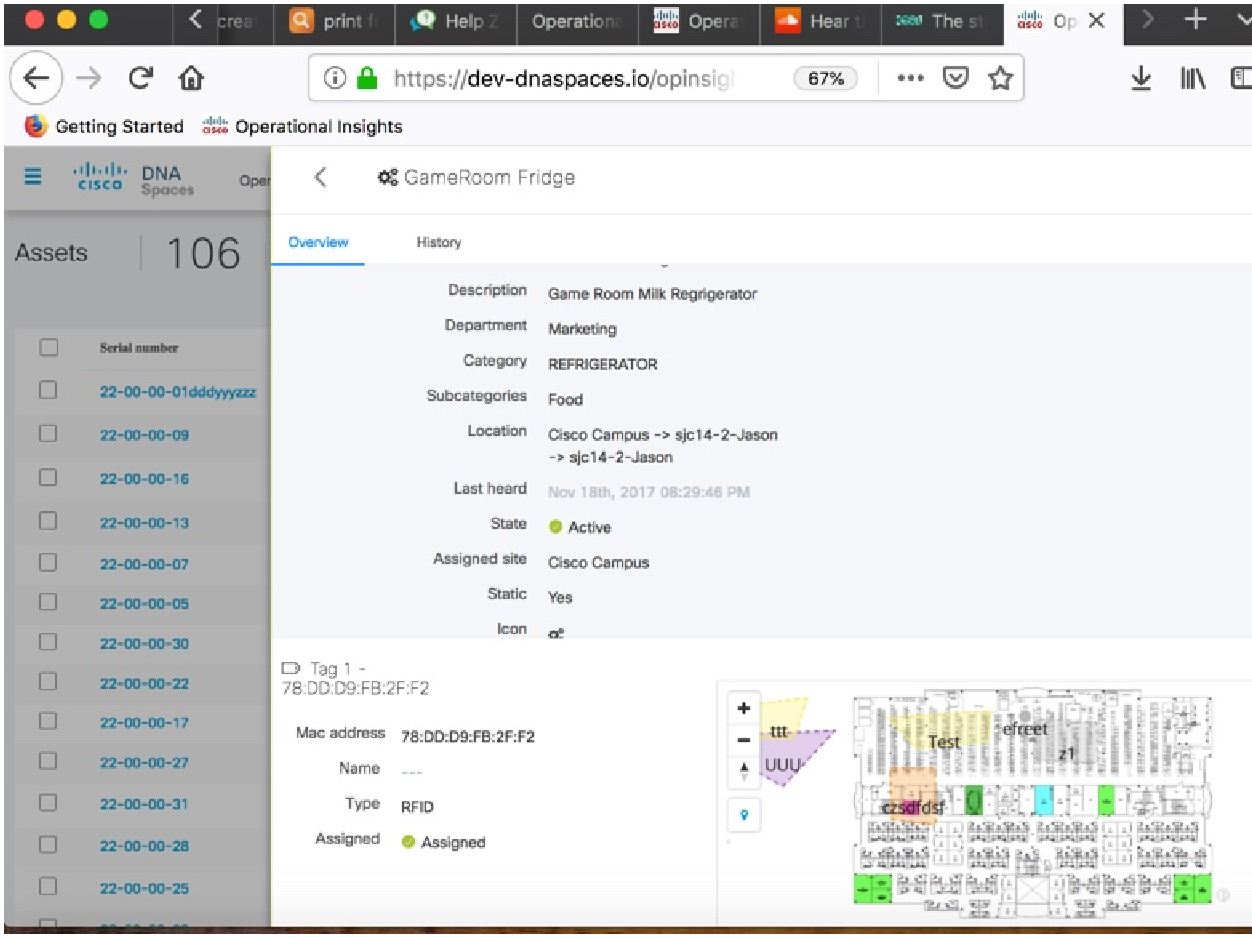
Manage Columns

Click the **Manage Columns** ⚙ icon to reorder, hide, or show the columns.

Asset 360: A Detailed View of Assets

You can click an asset from the Locator: List or Map View to view a complete and detailed view of the Asset or Asset 360 degree view. A map is displayed in this view with the asset positioned on the map.

- You can zoom in to the map using the **plus** and **minus** sign.
- You can click, hold, and rotate the compass icon to rotate the map.



Assets 106

☐	Serial number
☐	22-00-00-01dddyyyzzz
☐	22-00-00-09
☐	22-00-00-16
☐	22-00-00-13
☐	22-00-00-07
☐	22-00-00-05
☐	22-00-00-30
☐	22-00-00-22
☐	22-00-00-17
☐	22-00-00-27
☐	22-00-00-31
☐	22-00-00-28
☐	22-00-00-25

GameRoom Fridge

Description	Game Room Milk Regrigerator
Department	Marketing
Category	REFRIGERATOR
Subcategories	Food
Location	Cisco Campus -> sjc14-2-Jason -> sjc14-2-Jason
Last heard	Nov 18th, 2017 08:29:46 PM
State	● Active
Assigned site	Cisco Campus
Static	Yes
Icon	

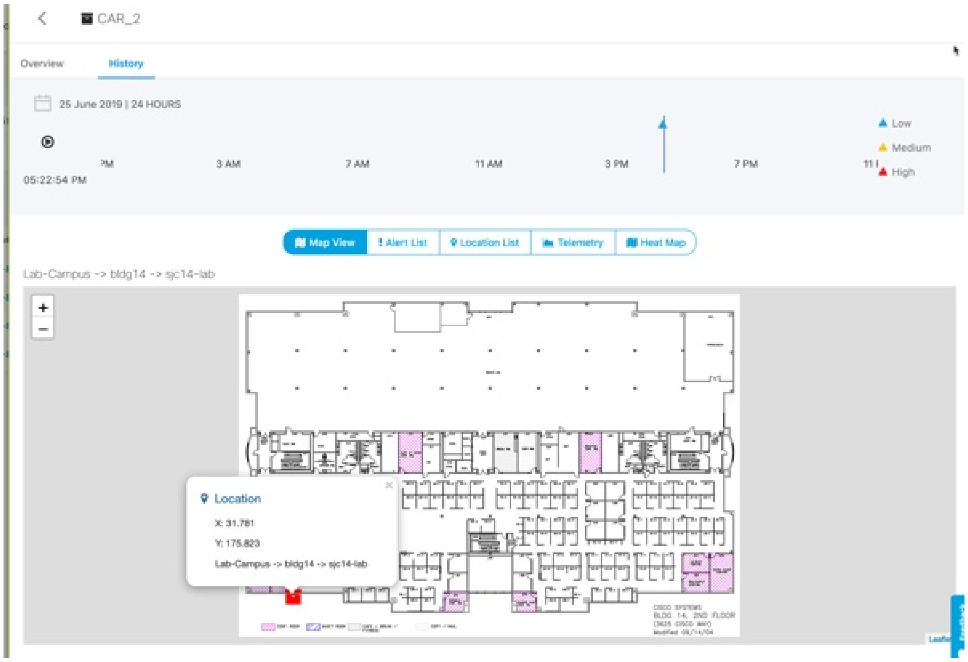
Tag 1 - 78:DD:D9:FB:2F:F2

Mac address	78:DD:D9:FB:2F:F2
Name	---
Type	RFID
Assigned	● Assigned

History View

Click on the History tab of the Asset 360 degree view to get a detailed view of the asset hisotry.

Figure 6: History: Location View



Lab-Campus -> bldg14 -> sjc14-lab

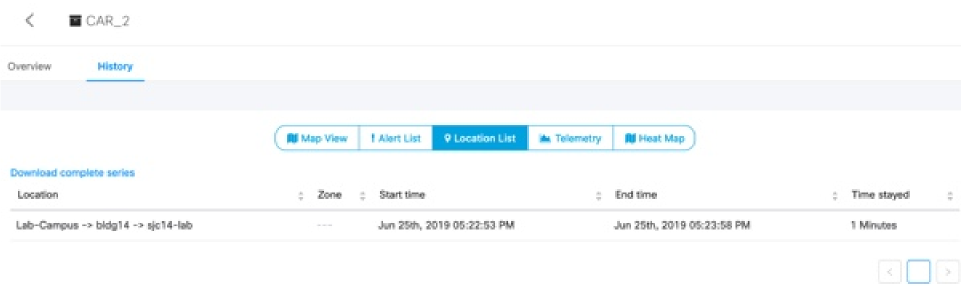
Location

X: 31.781

Y: 175.823

Lab-Campus -> bldg14 -> sjc14-lab

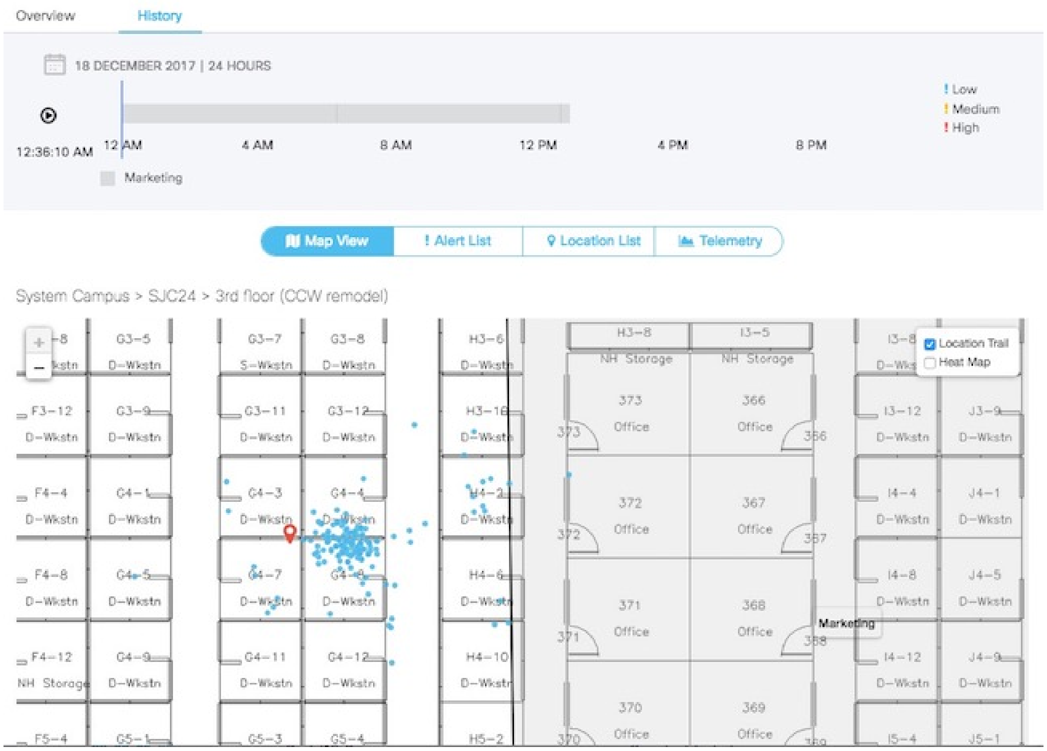
Figure 7: History: Alert List View



Download complete series

Location	Zone	Start time	End time	Time stayed
Lab-Campus -> bldg14 -> sjc14-lab	---	Jun 25th, 2019 05:22:53 PM	Jun 25th, 2019 05:23:58 PM	1 Minutes

Figure 8: History: Location Trail on Map View

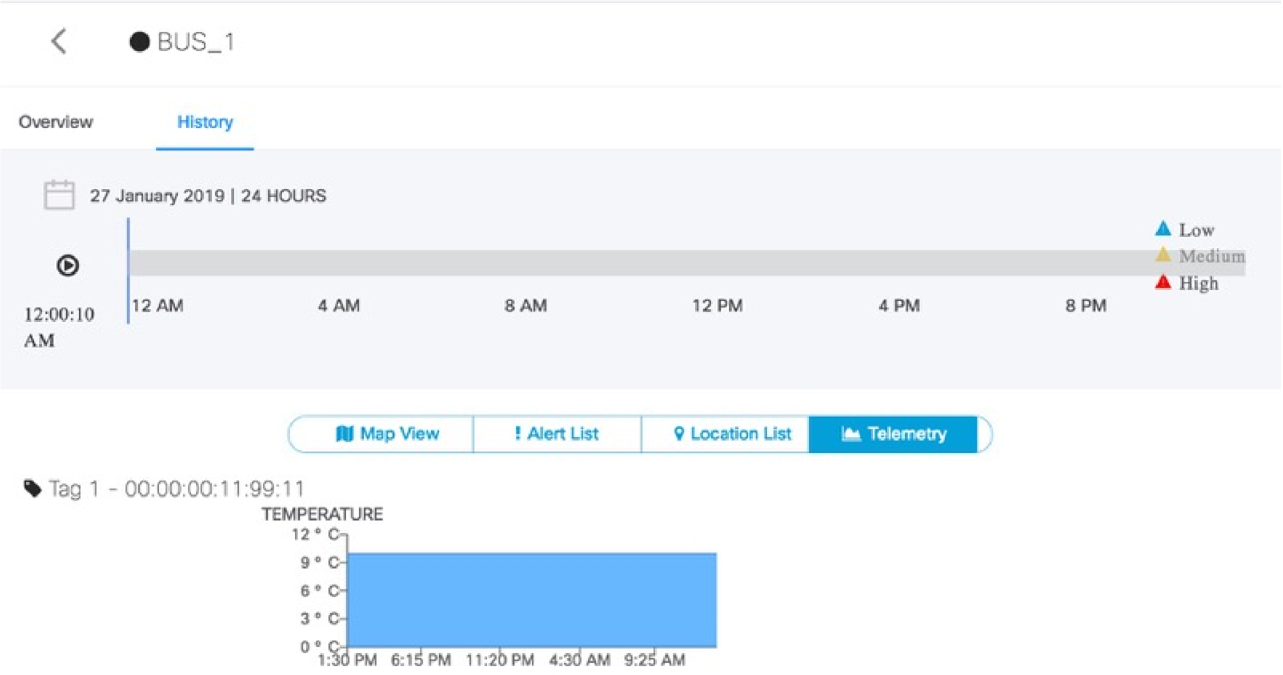


18 DECEMBER 2017 | 24 HOURS

System Campus > SJC24 > 3rd floor (CCW remodel)

☑ Location Trail
□ Heat Map

Figure 9: History: Telemetry View



Alerts View

The **Alerts** View has a list of alerts. The alerts are triggered when conditions of the rules configured in the **Rules** tab are satisifed. The view is organized by the widgets added by a user. Saving this filter will create a Widget.

Navigate to the **Alerts** View

- You can add widgets to this view
- You can download CSV files listing all the alerts.
- You can hide or change the order of columns
- You can add comments to an alert, or assign **Open/In Progress/Done/Closed** status to an alert based on the progress of the alert. Closing an alert without an action does not mean an alert is gone from the system. **Closed Alerts** is a widget that can provide a historic view of closed alerts.

- You can restrict the contents in this view by applying filters on various parameters. Saving this filter will create a widget.

Tag View

Choose **Configure > Tags** to open the tag view. The tags shown here are automatically discovered from CMX. The tag view displays the list of tags and, among other information, its last heard time and location. Tags can be modified individually or in bulk. Asset Locator can work with any CCX Compliant tags that send location, battery and telemetry data. Asset Locator can also work with BLE tags.

CHAPTER 9

Troubleshoot

Troubleshoot

Problem: Asset Tags not populated in Cisco Spaces: Asset Locator

Possible Cause Cisco CMX is unable to communicate with Cisco Spaces: Asset Locator.

- **Solution** Verify if the proxy is configured on the Cisco CMX device, by issuing the following command from the command line interface (CLI) of Cisco CMX.

  ```
  cmxos sysproxy show command
  ```

  - **Solution** If the proxy is not configured on the Cisco CMX, see *Configuring a Proxy on Cisco CMX for Cisco Spaces: Asset Locator*.
  - **Solution** If proxy is configured correctly on the Cisco CMX, issue one of the following CURL commands. If the command does not give an error and instead outputs many lines of text, then the proxy is able reach the external network and can allow Cisco CMX to communicate with Asset Locator.

    ```
    curl https://www.google.com
    ```

    OR

    ```
    curl http://www.dnaspaces.io
    ```

- **Solution** Verify that the correct floor map which was exported from Cisco Prime Infrastructure with APs detecting tags is uploaded in CMX.
- **Solution** Verify if the Floor ID of the Cisco CMX floor map is same as the Floor ID in the Asset Locator floormap (Floor ID is displayed on the floor map page in lower-left corner)
- **Solution** Verify if tags are visible on Cisco CMX floor maps

Problem: Assets do not display location information despite functional connectivity between Cisco CMX and Asset Locator

Floor ID mismatch between Cisco CMX and Asset Locator

- **Solution** Verify if the correct floor map was exported.

Problem: Last Heard Time in Asset Locator > Locator > List is longer than expected.

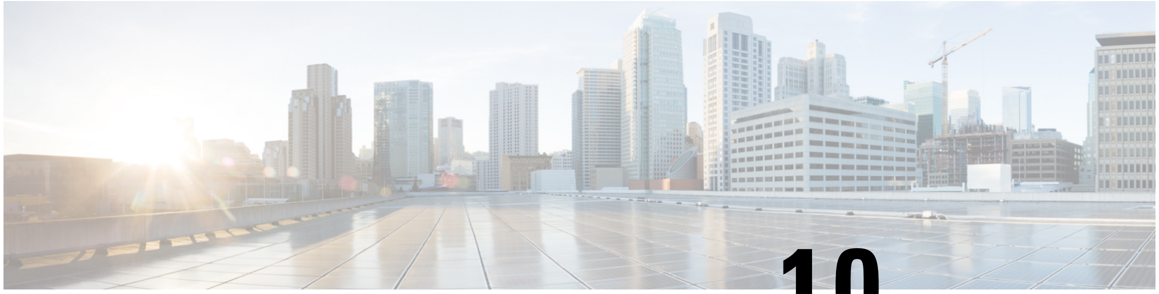
Tags may not be getting detected either on Cisco CMX or there is a problem with the connectivity between Cisco CMX and Asset Locator.

- **Solution** Ensure that the tags on Cisco CMX floor maps are updated at configured intervals.
- **Solution** Check **Location Engine** dnaspaces-stream to check if **Last Heard Time** is updated regularly. If not, check Cisco CMX and Cisco Spaces: Connector.
- **Solution** Verify that same floor maps are uploaded in Asset Locator.
- **Solution** Verify if the Floor ID in the Cisco CMX floor map is same as floor ID in the Asset Locator floor map. Floor ID is displayed in the lower-left corner of the **Map** page.
- **Solution** Verify tags are shown on Cisco CMX floor maps.

If the problem persists, contact the support team.

Problem: Alerts not received as SMS or email for an asset.

- **Solution** Verify if the email and phone numbers are configured correctly.
- **Solution** Asset Locator provides 100 SMS by default. To enable further SMSs, the Tropos account has to be setup.
- **Solution** Verify if the phone number is validated by the user.



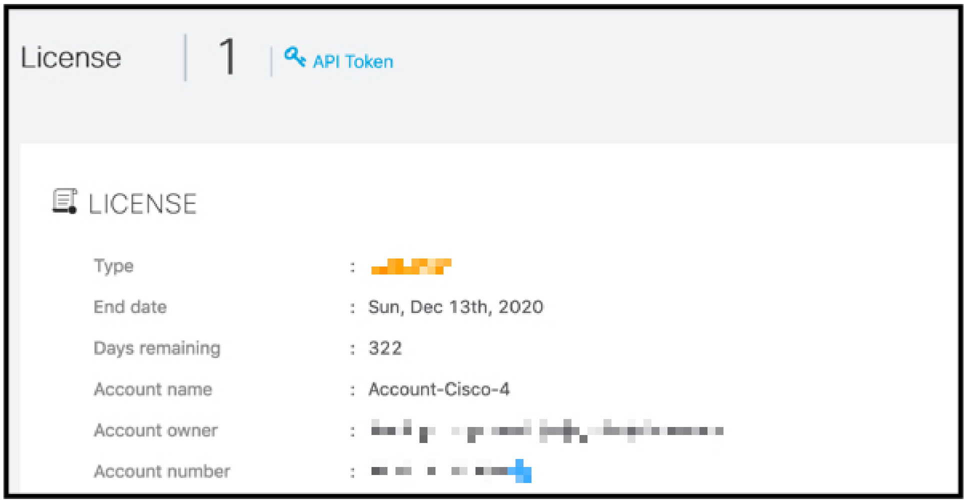
CHAPTER 10

APIs

APIs

The APIs have an asset fetch limit of 100 records. The API has a rate limit of five requests per second. You can generate an API token from the **Settings>Licenses** tab.

Figure 10: The License Tab



License | 1 | API Token

LICENSE

Type	: [redacted]
End date	: Sun, Dec 13th, 2020
Days remaining	: 322
Account name	: Account-Cisco-4
Account owner	: [redacted]
Account number	: [redacted]

Additional References

Cisco Spaces: Asset Locator API Reference: https://www.cisco.com/c/dam/en/us/td/docs/wireless/cisco-dna-spaces/tech-notes/asset-locator-api-ref.pdf

APPENDIX A

Appendix

- Appendix, on page 41

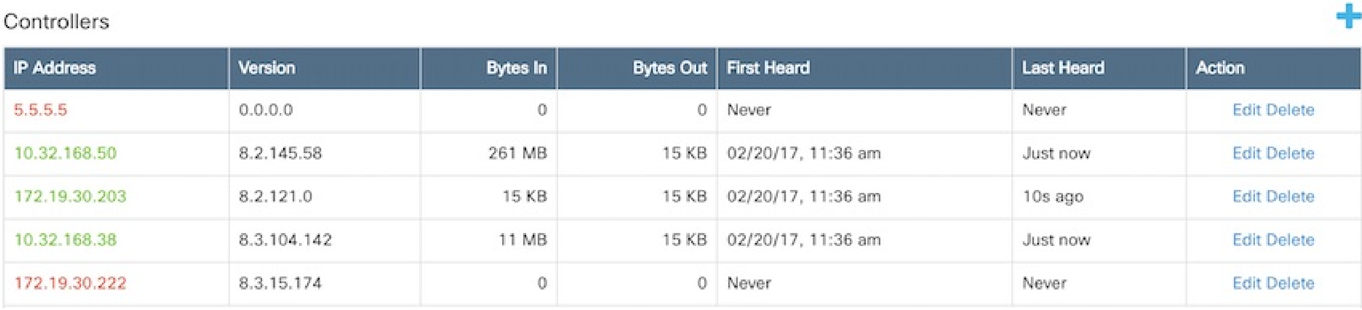
Appendix

Configuring Cisco CMX with wireless controller

Step 1 From the Cisco CMX navigation pane, choose **System>Settings>Controllers and Maps Setup>Advanced**.

Step 2 From the **Controllers** section, select the **IP address** from the drop-down and enter the wireless controller IP address. From the **Controller SNMP Write Community**, select a version and click **Save**.

Step 3 From the main area of the Cisco CMX dashboard, go to the, **Controller** area, and ensure that the wireless controller IP address is green. This indicates a successful connection between the wireless controller and Cisco CMX.



Controllers

IP Address	Version	Bytes In	Bytes Out	First Heard	Last Heard	Action
5.5.5.5	0.0.0.0	0	0	Never	Never	Edit Delete
10.32.168.50	8.2.145.58	261 MB	15 KB	02/20/17, 11:36 am	Just now	Edit Delete
172.19.30.203	8.2.121.0	15 KB	15 KB	02/20/17, 11:36 am	10s ago	Edit Delete
10.32.168.38	8.3.104.142	11 MB	15 KB	02/20/17, 11:36 am	Just now	Edit Delete
172.19.30.222	8.3.15.174	0	0	Never	Never	Edit Delete

Note If the wireless controller IP address is not green, refer to the instructions in the next task.

Configure a Hash Key on wireless controller

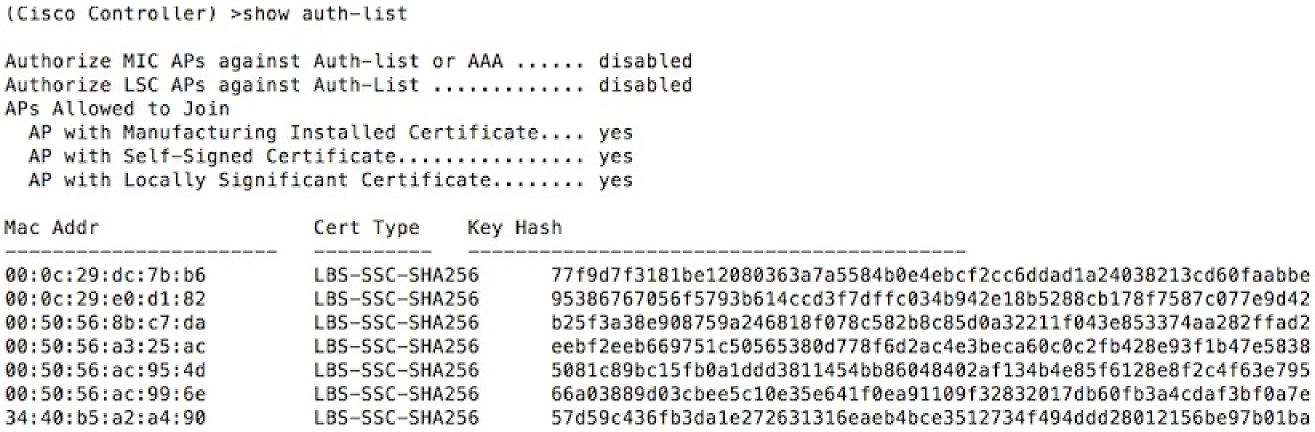
If the status of the wireless controller IP address is red, the wireless controller may have been added on Cisco CMX with a read community string. Perform the following troubleshooting task.

Step 1 From the Cisco CMX CLI, execute the **cmxctl config controllers show** command and copy the value of the SHA2 key:

```
[CMXadmin@CMX-jkp103 configuration]$ cmxctl config controllers show

+-------------+------------------------------------------------------------------+

| MAC Address | 00:50:56:ac:99:6e                                                |

+-------------+------------------------------------------------------------------+

| SHA1 Key    | d116d605fd88e72763a03871bc483786e463ae43                         |

+-------------+------------------------------------------------------------------+

| SHA2 Key    | 66a03889d03cbee5c10e35e641f0ea91109f32832017db60fb3a4cdaf3bf0a7e |

+-------------+------------------------------------------------------------------+
```

Step 2 From the wireless controller CLI, issue the **config auth-list add sha256-lbs-ssc** *<CMX-mac><sha2KeyHashString>* command using the SHA2 string from Step 1.

Step 3 At the wireless controller CLI, execute the **show auth-list** command:



```
(Cisco Controller) >show auth-list

Authorize MIC APs against Auth-list or AAA ...... disabled
Authorize LSC APs against Auth-List ............ disabled
APs Allowed to Join
  AP with Manufacturing Installed Certificate.... yes
  AP with Self-Signed Certificate................ yes
  AP with Locally Significant Certificate........ yes

Mac Addr                  Cert Type    Key Hash
-----------------------   ----------   ------------------------------------------
00:0c:29:dc:7b:b6         LBS-SSC-SHA256     77f9d7f3181be12080363a7a5584b0e4ebcf2cc6ddad1a24038213cd60faabbe
00:0c:29:e0:d1:82         LBS-SSC-SHA256     95386767056f5793b614ccd3f7dffc034b942e18b5288cb178f7587c077e9d42
00:50:56:8b:c7:da         LBS-SSC-SHA256     b25f3a38e908759a246818f078c582b8c85d0a32211f043e853374aa282ffad2
00:50:56:a3:25:ac         LBS-SSC-SHA256     eebf2eeb669751c50565380d778f6d2ac4e3beca60c0c2fb428e93f1b47e5838
00:50:56:ac:95:4d         LBS-SSC-SHA256     5081c89bc15fb0a1ddd3811454bb86048402af134b4e85f6128e8f2c4f63e795
00:50:56:ac:99:6e         LBS-SSC-SHA256     66a03889d03cbee5c10e35e641f0ea91109f32832017db60fb3a4cdaf3bf0a7e
34:40:b5:a2:a4:90         LBS-SSC-SHA256     57d59c436fb3da1e272631316eaeb4bce3512734f494ddd28012156be97b01ba
```

Configuring a Proxy on Cisco CMX 10.4 and above

This task shows you how to configure a proxy gateway on Cisco CMX (10.4 and above) to allow communication between a Cisco CMX server installed on a private network and an external cloud setup.

Step 1 **cmxos sysproxy proxy http://** *<proxy-gateway-address> <port>*

This command configures a proxy gateway that allows communication of an internal Cisco CMX with an external Asset Locator server.

Step 2 **cmxos sysproxy no_proxy localhost** *<website-address>*

This command prevents the use of proxy for IP addresses that are within the network.

Step 3 **cmxos sysproxy {enable | clear | disable}**

This command enables proxy.

Step 4 **cmxctl stop -a**

Step 5 **cmxcl agent start**

Step 6 **cmxctl start**

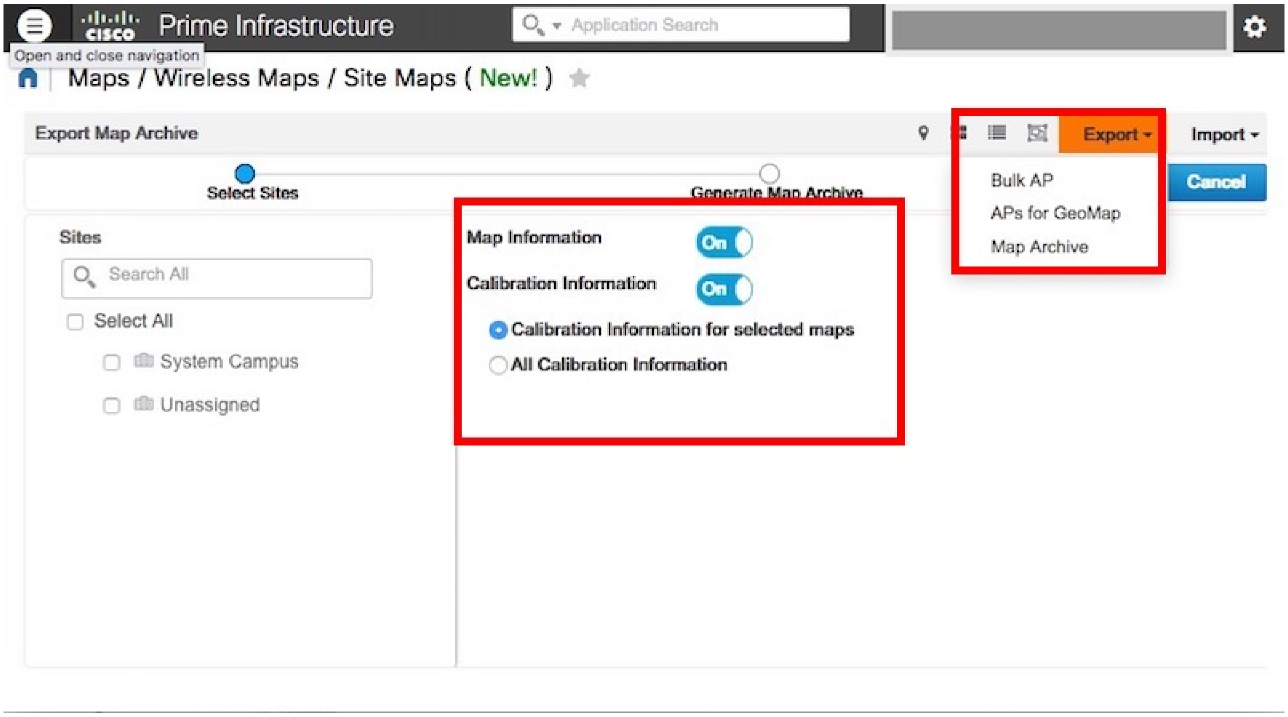
Step 7 Restart Cisco CMX to see the changes in effect.

Import Maps from Cisco PI to Cisco CMX

Step 1 Log in to Cisco PI using the URL *https://<PrimeInfrastructure_IP_address>*.

a) Choose **Maps>Wireless Maps>Site Maps**.

b) From the right navigation pane, choose **Export > Map Archive**. Ensure that all the default checks are retained, as shown in the figure.



Map Information On
Calibration Information On
● Calibration Information for selected maps
○ All Calibration Information

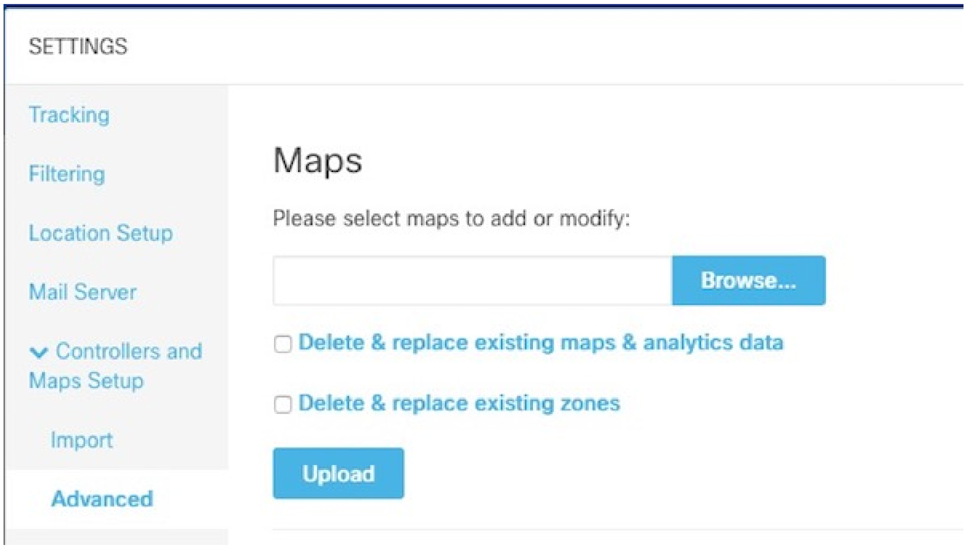
c) Select the map to be exported and click **Export**.

The selected map is downloaded to a compressed .tar file named `ImportExport_xxxx .tar.gz`, for example, `ImportExport_4575dcc9014d3d88.tar.gz`, in your browser's download directory.

Step 2 Log in to Cisco CMX dashboard using the URL *https://<CMX_IP_address>*.

a) Choose **System>Settings>Controllers and Map Setup>Advanced**.

b) Under **Maps**, click **Browse**, select the maps exported from Cisco PI (Step 1), and click **Upload**.



Maps

Please select maps to add or modify:

□ Delete & replace existing maps & analytics data

□ Delete & replace existing zones

Step 3 Log in to App dashboard

Step 4 Select **Maps** from the left menu.

Step 5 Click **Upload**. The map uploads to the App.

Step 6 Verify that the map uploaded to the App correctly.

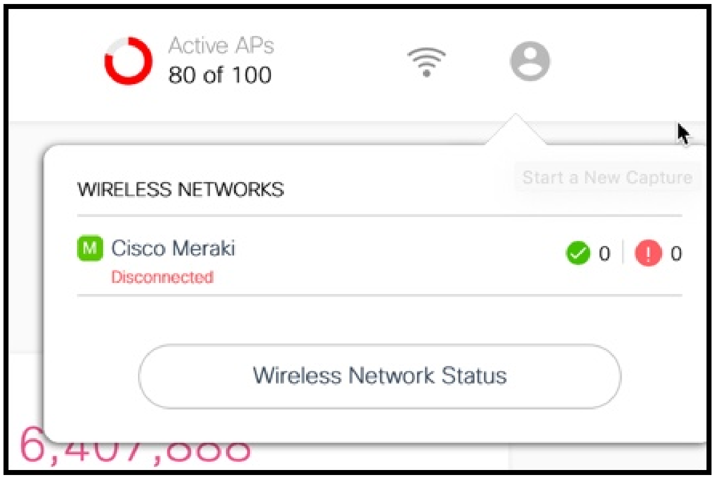
How to obtain a Cisco CMX token from Cisco Spaces

This appendix shows you how to add a Cisco CMX to your Cisco Spaces account and obtain a token for the same. You can configure this token on Cisco CMX. This step is a prerequiste for the proper functioning of Asset Locator.

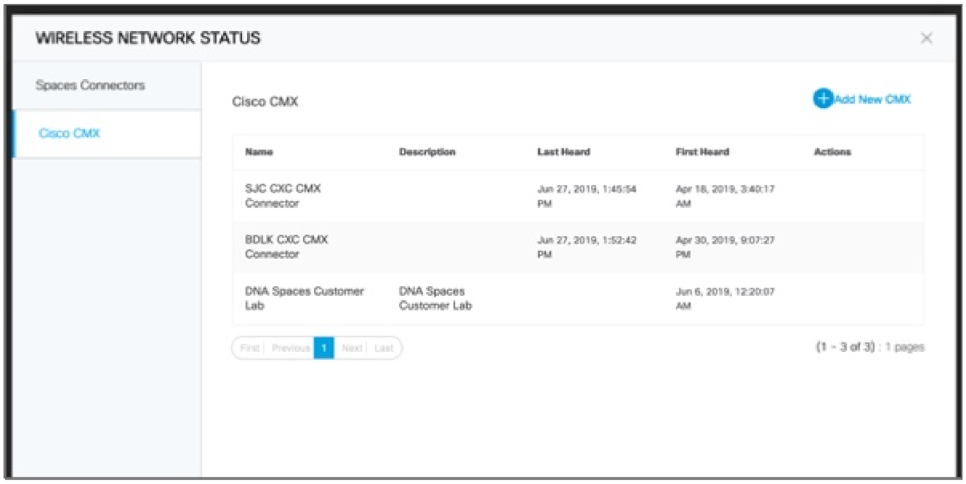
Step 1 Log in to your Cisco Spaces account.

Step 2 Click on the 📶 button in the top-right corner.

Step 3 Click **Wireless Network Status**.



Step 4 From the **Wireless Network Status** page that is displayed, click **Cisco CMX** and **Add New CMX**

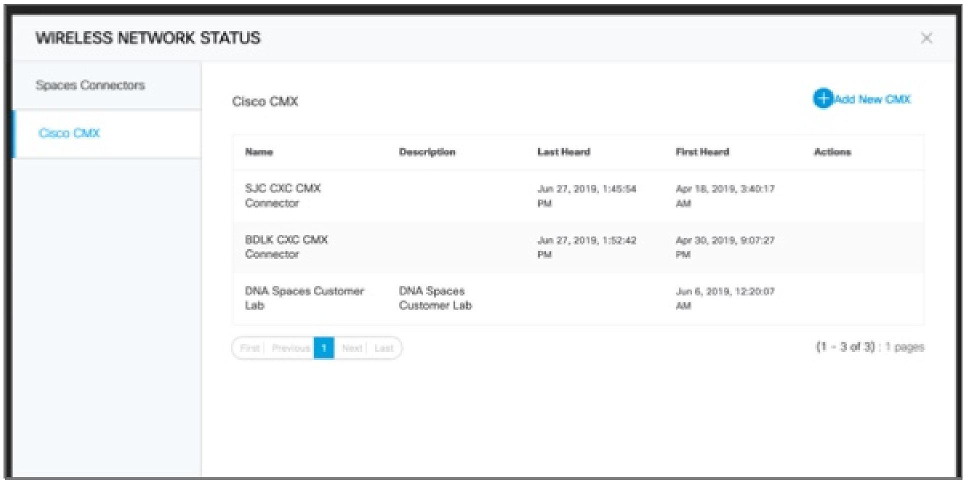


Cisco CMX

Name	Description	Last Heard	First Heard	Actions
SJC CXC CMX Connector		Jun 27, 2019, 1:45:54 PM	Apr 18, 2019, 3:40:17 AM	
BDLK CXC CMX Connector		Jun 27, 2019, 1:52:42 PM	Apr 30, 2019, 9:07:27 PM	
DNA Spaces Customer Lab	DNA Spaces Customer Lab		Jun 6, 2019, 12:20:07 AM	

(1 - 3 of 3) : 1 pages

Step 5 From the **Wireless Network Status** page that is displayed, click **Cisco CMX** and **Add New CMX**

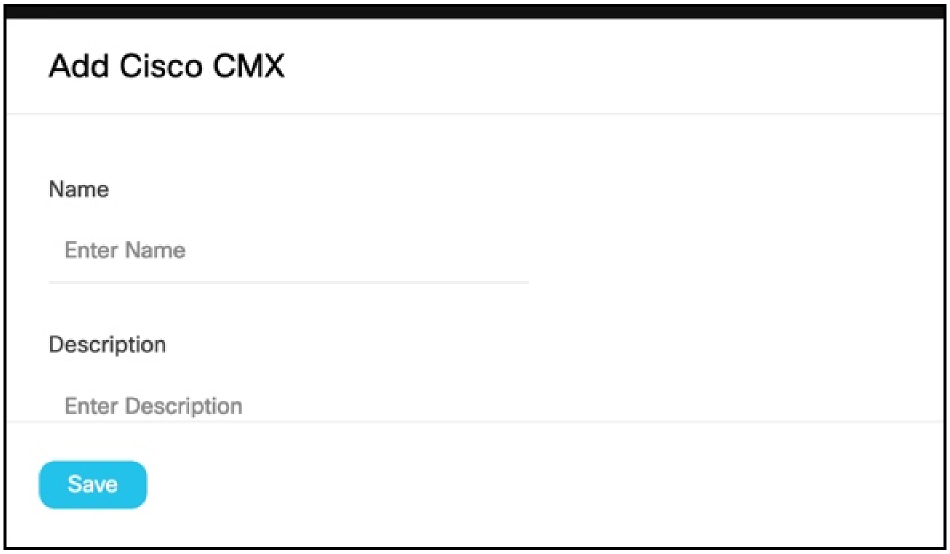


Cisco CMX

Name	Description	Last Heard	First Heard	Actions
SJC CXC CMX Connector		Jun 27, 2019, 1:45:54 PM	Apr 18, 2019, 3:40:17 AM	
BDLK CXC CMX Connector		Jun 27, 2019, 1:52:42 PM	Apr 30, 2019, 9:07:27 PM	
DNA Spaces Customer Lab	DNA Spaces Customer Lab		Jun 6, 2019, 12:20:07 AM	

(1 - 3 of 3) : 1 pages

Step 6 Enter a **Name** and **Description** for your Cisco CMX and click **Save**.



Add Cisco CMX

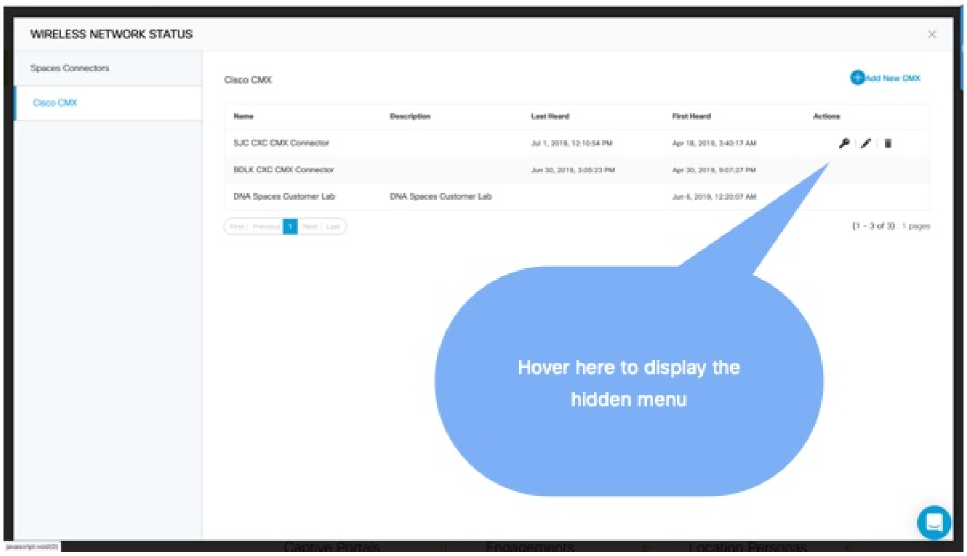
Name

Enter Name

Description

Enter Description

Step 7 Hover around the right extreme area of the Cisco CMX you added to display the respective hidden menu. Click on the Key button.



WIRELESS NETWORK STATUS

Spaces Connectors
Cisco CMX
Add New CMX
First | Previous | 1 | Next | Last
Hover here to display the hidden menu

Cisco CMX

Name	Description	Last Heard	First Heard	Actions
SJC CXC CMX Connector		Jul 1, 2019, 12:10:54 PM	Apr 18, 2019, 3:40:17 AM	
BDLK CXC CMX Connector		Jun 30, 2019, 3:05:23 PM	Apr 30, 2019, 9:07:27 PM	
DNA Spaces Customer Lab	DNA Spaces Customer Lab		Jun 6, 2019, 12:20:07 AM	

[1 - 3 of 3] : 1 pages

Step 8 Authenticate using your Cisco Spaces credentials when prompted and click **Submit**.

Step 9 When the Token is displayed, click **Copy**.

What to do next

You can now add this token on your Cisco CMX.

Location Services Using Cisco CMX

Configuring Cisco CMX 10.6 and Above

Configuring Notifications on Cisco CMX 10.6 and above

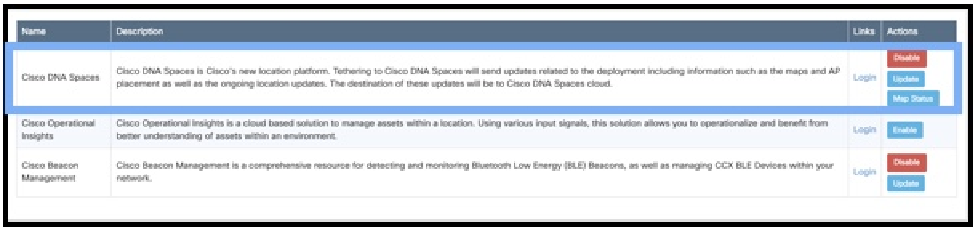
This step demonstrates how to configure HTTPS notifications in Cisco CMX to notify Application when a location update occurs for a tag.

Before you begin

Get the Application token. Refer to *How to Obtain a token from Cisco Spaces* of the Appendix.

Step 1 From the Cisco Spaces: Asset Locator dashboard, choose **Manage> Cloud Apps**.

Step 2 In the **Cloud Applications> Cisco Spaces** section, click **Enable**.

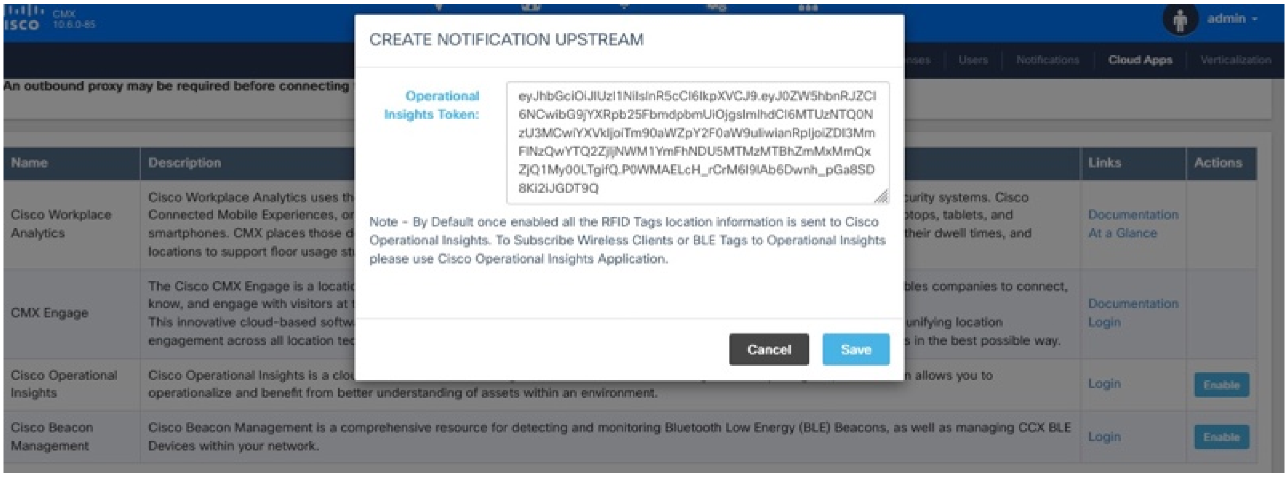


Name	Description	Links	Actions
Cisco DNA Spaces	Cisco DNA Spaces is Cisco's new location platform. Tethering to Cisco DNA Spaces will send updates related to the deployment including information such as the maps and AP placement as well as the ongoing location updates. The destination of these updates will be to Cisco DNA Spaces cloud.	Login	Disable Update Map Status
Cisco Operational Insights	Cisco Operational Insights is a cloud based solution to manage assets within a location. Using various input signals, this solution allows you to operationalize and benefit from better understanding of assets within an environment.	Login	Enable
Cisco Beacon Management	Cisco Beacon Management is a comprehensive resource for detecting and monitoring Bluetooth Low Energy (BLE) Beacons, as well as managing CCX BLE Devices within your network.	Login	Disable Update

Note **WARNING**

Do not enable Asset Locator if it is present. This is deprecated.

Step 3 In the **Create Notification Upstream** dialog box, enter the value of token obtained from Cisco Spaces.



An outbound proxy may be required before connecting

CREATE NOTIFICATION UPSTREAM

Operational Insights Token: eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ0ZW5hbnRJZCI6NCwibG9jYXRpb25FbmdpbmUiOjgsImlhdCI6MTUzNTQ0NzU3MCwiYXVkIjoiTm90aWZpY2F0aW9uIiwianRpIjoiZDI3MmFlNzQwYTQ2ZjljNWM1YmFhNDU5MTMzMTBhZmMxMmQxZjQ1My00LTgifQ.P0WMAELcH_rCrM6I9lAb6Dwnh_pGa8SD8Ki2iJGDT9Q

Note - By Default once enabled all the RFID Tags location information is sent to Cisco Operational Insights. To Subscribe Wireless Clients or BLE Tags to Operational Insights please use Cisco Operational Insights Application.

Name	Description	Links	Actions
Cisco Workplace Analytics	Cisco Workplace Analytics uses th … Connected Mobile Experiences, or … smartphones. CMX places those d … locations to support floor usage st … curity systems. Cisco … ptops, tablets, and … their dwell times, and	Documentation At a Glance	
CMX Engage	The Cisco CMX Engage is a locati … know, and engage with visitors at t … This innovative cloud-based softw … engagement across all location tec … bles companies to connect, … unifying location … s in the best possible way.	Documentation Login	
Cisco Operational Insights	Cisco Operational Insights is a clo … n allows you to operationalize and benefit from better understanding of assets within an environment.	Login	Enable
Cisco Beacon Management	Cisco Beacon Management is a comprehensive resource for detecting and monitoring Bluetooth Low Energy (BLE) Beacons, as well as managing CCX BLE Devices within your network.	Login	Enable

Configuring Cisco CMX 10.5 and Before

Configuring Notifications on Cisco CMX (Prior to Cisco CMX 10.6)

This procedure demonstrates how to configure HTTPS notifications in Cisco CMX to notify Application when a location update occurs for a tag.

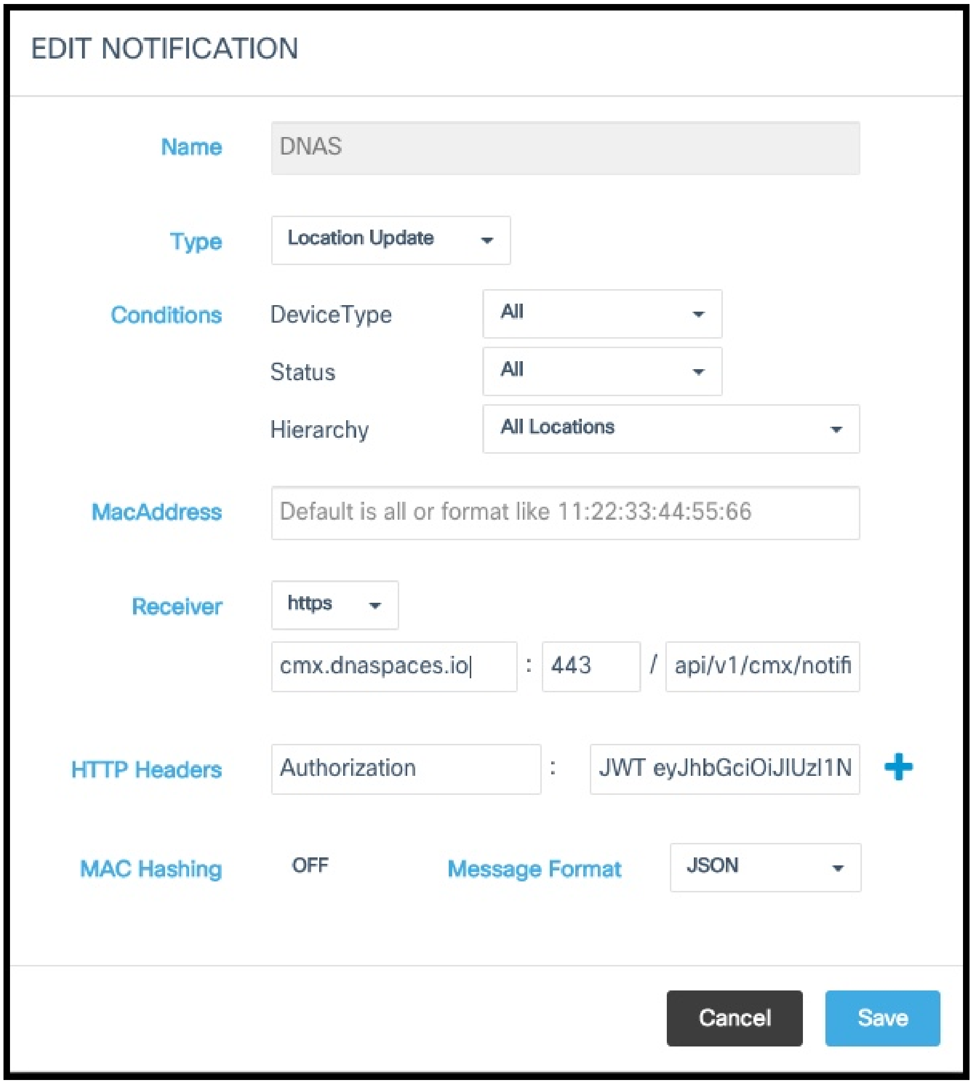
Before you begin

You can retreive a token from the Creating Cisco CMX Connector and Retrieving Token section of the Cisco CMX configuration guide.

Step 1 From the Cisco CMX dashboard, navigate to **Manage** > **Notification** > **+New Notification**.

Step 2 In the **Create New Notification** dialog box, enter a **Name** for your notification.

Figure 11: Create New Notification



EDIT NOTIFICATION

Name: DNAS

Type: Location Update

Conditions:
DeviceType: All
Status: All
Hierarchy: All Locations

MacAddress: Default is all or format like 11:22:33:44:55:66

Receiver: https
cmx.dnaspaces.io : 443 / api/v1/cmx/notifi

HTTP Headers: Authorization : JWT eyJhbGciOiJIUzI1N

MAC Hashing: OFF

Message Format: JSON

Step 3 Under **Conditions**, choose **All** from the **Device Type** and **Status** drop-down box, and choose **All Locations** from the **Heirarchy** drop-down box.

Step 4 Leave the **MAC address** field empty.

Step 5 From **Receiver** drop-down list, select **https** .

Step 6 From the information in the activation mail, fill the **host address** field with `https://cmx.dnaspaces.io` and port number as *443*.

Step 7 In the **url** field, enter ***`api/v1/cmx/notifications/locationUpdate`***

Step 8 Turn the **MAC hashing** option off.

Step 9 From the **Message Format** drop-down list, select **JSON**.

Step 10 Click **Create**.

Enabling Telemetry on Cisco CMX (Prior to 10.3)

This task enables Cisco CMX to send telemetry data to the Asset Locator. Telemetry data is nonlocation data such as temperature of humidity that is collected by the RFID tags and sent to Asset Locator through the Cisco CMX location engine.

Step 1 In the Cisco CMX CLI, navigate to the `/opt/cmx/etc/node.conf` and insert the following line under **location** section.

```
user_options=-Dpublish-telemetry=true
```

Step 2 Restart Cisco CMX.

```
cmxctl stop -a
cmxctl agent start
cmxctl start
```

Step 3 Ensure that Cisco CMX and all its services and processes are up and running.

```
cmxctl status
```