Cisco DNA Spaces Configuration Guide

First Published: 2018-12-18
Last Modified: 2019-11-20

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
The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

Notwithstanding any other warranty herein, all document files and software of these suppliers are provided “as is” with all faults. Cisco and the above-named suppliers disclaim all warranties, expressed or implied, including, without limitation, those of merchantability, fitness for a particular purpose and noninfringement or arising from a course of dealing, usage, or trade practice. In no event shall Cisco or its suppliers be liable for any indirect, special, consequential, or incidental damages, including, without limitation, lost profits or loss or damage to data arising out of the use or inability to use this manual, even if Cisco or its suppliers have been advised of the possibility of such damages.

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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2019 Cisco Systems, Inc. All rights reserved.
Preface

This preface describes the audience, organization, acronyms, and conventions used in the document. This document contains the following sections:

- Audience, on page iii
- Document Organization, on page iii
- Document Conventions, on page v
- List of Acronyms and Abbreviations, on page v

Audience

This guide is meant for account administrators who manage the Cisco Digital Network Architecture (DNA) Spaces user accounts and perform the configurations required for Cisco DNA Spaces. This guide is also meant for business and store administrators who use Cisco DNA 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

<table>
<thead>
<tr>
<th>Chapter Number</th>
<th>Chapter Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 1</td>
<td>Cisco DNA Spaces Prerequisites</td>
<td>Provides information about various Cisco DNA Spaces features and the prerequisites to deploy Cisco DNA Spaces.</td>
</tr>
<tr>
<td>Chapter 2</td>
<td>Getting Started</td>
<td>Provides an overview about Cisco DNA Spaces and its features. This chapter also describes the process flow, system requirements, and how to start working with Cisco DNA Spaces.</td>
</tr>
<tr>
<td>Chapter 3</td>
<td>Location Hierarchy in Cisco DNA Spaces</td>
<td>Provides information about how to define Cisco DNA Spaces location hierarchy.</td>
</tr>
<tr>
<td>Chapter Number</td>
<td>Chapter Title</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>---------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Chapter 4</td>
<td>Behavior Metrics</td>
<td>Provides information about Behavior Metrics reports.</td>
</tr>
<tr>
<td>Chapter 5</td>
<td>Location Analytics</td>
<td>Provides information about how to view Location Analytics report.</td>
</tr>
<tr>
<td>Chapter 6</td>
<td>Impact Analysis</td>
<td>Provides information on using the Impact Analysis app.</td>
</tr>
<tr>
<td>Chapter 7</td>
<td>Working with the Captive Portal App</td>
<td>Provides information about how to create captive portals, configure support features such as SMS gateway, and display the captive portal using the captive portal rules.</td>
</tr>
<tr>
<td>Chapter 8</td>
<td>Sending Notifications with the Engagements App</td>
<td>Provides information about engagement rules that you can define to send notifications to customers and business users.</td>
</tr>
<tr>
<td>Chapter 9</td>
<td>Creating Tags with the Location Personas App</td>
<td>Provides information about profile rules that you can define to create tags or to modify the existing tags.</td>
</tr>
<tr>
<td>Chapter 10</td>
<td>Working with the Cisco DNA Spaces Operation Insights App</td>
<td>Provides an overview of the Operation Insights app.</td>
</tr>
<tr>
<td>Chapter 11</td>
<td>Monitoring and Support</td>
<td>Provides information about the app details mentioned in the Monitoring section, and how to use the Support feature.</td>
</tr>
<tr>
<td>Chapter 12</td>
<td>Managing Cisco DNA Spaces Users and Accounts</td>
<td>Provides information about how to manage Cisco DNA Spaces users, Cisco DNA Spaces accounts, and Cisco Connected Mobile Experiences (CMX) accounts.</td>
</tr>
<tr>
<td>Chapter 13</td>
<td>Setup Wireless Network</td>
<td>Describes the setup required for using Cisco DNA Spaces.</td>
</tr>
<tr>
<td>Chapter 14</td>
<td>Configuring Cisco Unified Wireless Network (Cisco Catalyst) for Cisco DNA</td>
<td>Describes the configurations required in the Cisco Unified Wireless Network (CUWN) to use Cisco DNA Spaces.</td>
</tr>
<tr>
<td>Chapter 15</td>
<td>Configuring Cisco Meraki for Cisco DNA Spaces</td>
<td>Describes the configurations required in Cisco Meraki to use Cisco DNA Spaces.</td>
</tr>
</tbody>
</table>
Document Conventions

This document uses the following conventions:

Table 1: Document Conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boldface</td>
<td>Commands, command options, and keywords are in boldface.</td>
</tr>
<tr>
<td>Italics</td>
<td>Arguments for which you supply values are in italics.</td>
</tr>
<tr>
<td>Option &gt; Option</td>
<td>Used to describe a series of menu options.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Expansion</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL</td>
<td>Access Control List</td>
</tr>
<tr>
<td>BLE</td>
<td>Bluetooth Low Energy</td>
</tr>
<tr>
<td>CUWN</td>
<td>Cisco Unified Wireless Network</td>
</tr>
<tr>
<td>CNA</td>
<td>Captive Network Assistant</td>
</tr>
<tr>
<td>RSSI</td>
<td>Received Signal Strength Indicator</td>
</tr>
<tr>
<td>SSID</td>
<td>Service Set Identifier</td>
</tr>
<tr>
<td>UUID</td>
<td>Universally Unique Identifier</td>
</tr>
</tbody>
</table>
Cisco DNA Spaces Prerequisites

This chapter describes the system requirements for Cisco Digital Network Architecture (DNA) Spaces, the bandwidth requirements to deploy Cisco DNA Spaces, and ports and IP addresses for Cisco DNA Spaces. This chapter contains the following sections:

- System Requirements, on page 1
- Bandwidth Requirements to Deploy Cisco DNA Spaces, on page 2
- Accessible Ports and IP Addresses, on page 5
- Cisco DNA Spaces Compatibility Matrix, on page 6

System Requirements

The System requirements for Cisco DNA Spaces is described in the following table.

Table 3:

<table>
<thead>
<tr>
<th>Item</th>
<th>System Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>• Microsoft Windows XP or later</td>
</tr>
<tr>
<td></td>
<td>• Mac OS X 10.6 or later</td>
</tr>
<tr>
<td>Browser</td>
<td>Windows OS</td>
</tr>
<tr>
<td></td>
<td>• Firefox Version 30 or later</td>
</tr>
<tr>
<td></td>
<td>• Chrome Version 34 or later</td>
</tr>
<tr>
<td></td>
<td>• Safari Version 5.1.7 or later</td>
</tr>
<tr>
<td></td>
<td>Mac OS</td>
</tr>
<tr>
<td></td>
<td>• Firefox Version 30 or later</td>
</tr>
<tr>
<td></td>
<td>• Chrome Version 34 or later</td>
</tr>
<tr>
<td></td>
<td>• Safari Version 5.1.7 or later</td>
</tr>
<tr>
<td>Cisco Wireless Controller</td>
<td>8.3 or later</td>
</tr>
</tbody>
</table>
### System Requirements

<table>
<thead>
<tr>
<th>Item</th>
<th>System Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Connected Mobile Experiences (CMX) - this is required only for Cisco AireOS/Catalyst Controllers used with Cisco CMX.</td>
<td>10.6 or later</td>
</tr>
<tr>
<td>Cisco DNA Spaces Connector (Only applicable for Cisco AireOS/Catalyst Controllers)</td>
<td>• vCPU: 2/4/8</td>
</tr>
<tr>
<td></td>
<td>• RAM: 4/8/16 GB</td>
</tr>
<tr>
<td></td>
<td>• Hard Disk: 60 GB</td>
</tr>
</tbody>
</table>

### Bandwidth Requirements to Deploy Cisco DNA Spaces

The following table shows the Internet bandwidth requirements for Cisco DNA Spaces Connector and Cisco Wireless Controller Direct Connect to send location updates.

**Table 4: Bandwidth Requirements for Location Updates**

<table>
<thead>
<tr>
<th>Test Data</th>
<th>Type</th>
<th>Required Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>5k-APs,60k-Clients</td>
<td>Cisco Wireless Controller Direct Connect</td>
<td>250 Kbps</td>
</tr>
<tr>
<td>5k-APs,60k-Clients</td>
<td>Cisco DNA Spaces Connector</td>
<td>4 Mbps</td>
</tr>
</tbody>
</table>

The following table shows the bandwidth requirements for loading the captive portal.

**Table 5:**

<table>
<thead>
<tr>
<th>Bandwidth</th>
<th>Number of Users</th>
<th>Response (In Seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Mbps</td>
<td>1</td>
<td>9.2</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>10.41</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>12.18</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>13.5</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>16.56</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>17.84</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>Number of Users</td>
<td>Response (In Seconds)</td>
</tr>
<tr>
<td>-----------</td>
<td>----------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>2 Mbps</td>
<td>1</td>
<td>9.06</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>9.15</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>10.48</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>11.28</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>12.06</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>12.34</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>13.5</td>
</tr>
<tr>
<td></td>
<td>8</td>
<td>15.5</td>
</tr>
<tr>
<td></td>
<td>9</td>
<td>15.7</td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>16.85</td>
</tr>
<tr>
<td></td>
<td>11</td>
<td>17.7</td>
</tr>
<tr>
<td>5Mbps</td>
<td>5</td>
<td>9.34</td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>11.56</td>
</tr>
<tr>
<td></td>
<td>11</td>
<td>11.92</td>
</tr>
<tr>
<td></td>
<td>12</td>
<td>11.51</td>
</tr>
<tr>
<td></td>
<td>13</td>
<td>12.5</td>
</tr>
<tr>
<td></td>
<td>14</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td>15</td>
<td>13.82</td>
</tr>
<tr>
<td></td>
<td>16</td>
<td>13.18</td>
</tr>
<tr>
<td></td>
<td>17</td>
<td>14.91</td>
</tr>
<tr>
<td></td>
<td>18</td>
<td>16.72</td>
</tr>
<tr>
<td></td>
<td>19</td>
<td>15.96</td>
</tr>
<tr>
<td></td>
<td>20</td>
<td>16.98</td>
</tr>
<tr>
<td></td>
<td>21</td>
<td>17.41</td>
</tr>
<tr>
<td>Bandwidth</td>
<td>Number of Users</td>
<td>Response (In Seconds)</td>
</tr>
<tr>
<td>-----------</td>
<td>----------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>7Mbps</td>
<td>25</td>
<td>13.93</td>
</tr>
<tr>
<td></td>
<td>30</td>
<td>15.41</td>
</tr>
<tr>
<td></td>
<td>31</td>
<td>15.21</td>
</tr>
<tr>
<td></td>
<td>32</td>
<td>15.64</td>
</tr>
<tr>
<td></td>
<td>33</td>
<td>16.31</td>
</tr>
<tr>
<td></td>
<td>34</td>
<td>18.92</td>
</tr>
<tr>
<td>9Mbps</td>
<td>30</td>
<td>10.56</td>
</tr>
<tr>
<td></td>
<td>35</td>
<td>12.11</td>
</tr>
<tr>
<td></td>
<td>40</td>
<td>14.79</td>
</tr>
<tr>
<td></td>
<td>41</td>
<td>14.7</td>
</tr>
<tr>
<td></td>
<td>42</td>
<td>13.27</td>
</tr>
<tr>
<td></td>
<td>43</td>
<td>13.93</td>
</tr>
<tr>
<td></td>
<td>44</td>
<td>15.68</td>
</tr>
<tr>
<td></td>
<td>45</td>
<td>16.81</td>
</tr>
<tr>
<td></td>
<td>46</td>
<td>16.13</td>
</tr>
<tr>
<td></td>
<td>47</td>
<td>19.25</td>
</tr>
<tr>
<td>11 Mbps</td>
<td>35</td>
<td>9.57</td>
</tr>
<tr>
<td></td>
<td>40</td>
<td>10.07</td>
</tr>
<tr>
<td></td>
<td>50</td>
<td>11.85</td>
</tr>
<tr>
<td></td>
<td>55</td>
<td>13.51</td>
</tr>
<tr>
<td></td>
<td>56</td>
<td>13.96</td>
</tr>
<tr>
<td></td>
<td>57</td>
<td>14.67</td>
</tr>
<tr>
<td></td>
<td>58</td>
<td>15.86</td>
</tr>
<tr>
<td></td>
<td>59</td>
<td>16.36</td>
</tr>
<tr>
<td></td>
<td>60</td>
<td>16.08</td>
</tr>
<tr>
<td></td>
<td>61</td>
<td>17.11</td>
</tr>
</tbody>
</table>
Accessible Ports and IP Addresses

Cisco DNA Spaces is a cloud-based solution, and there is no physical installation involved. So, there is no need to open any port to deploy Cisco DNA Spaces for cloud-based wireless networks such as Cisco Meraki. For some networks such as Cisco AireOS or Cisco Catalyst that are not cloud-based, you must have to open the required ports to establish a connection between your wireless network and Cisco DNA Spaces. You can establish this connection through a public IP or VPN. In addition, certain Cisco DNA Spaces IP addresses must be allowed in the customer infrastructure. For more information on the IP addresses to be allowed, see the Allow Cisco DNA Spaces IP Addresses, on page 5. For a default Cisco Unified Wireless Network installation, ports 80 and 443 must be open to be publicly accessible.

Cisco CMX must be publicly accessible in the following scenarios where Cisco DNA Spaces has to establish a connection with Cisco CMX:

• Connecting to Cisco CMX
• Importing location and access points
• Viewing Cisco CMX maps
• Viewing Cisco DNA Spaces reports

Allow Cisco DNA Spaces IP Addresses

To establish a connection between Cisco DNA Spaces and Cisco Unified Wireless Network (Cisco Catalyst), you must allow certain Cisco DNA Spaces IP addresses in your network infrastructure. To view the IP addresses that should be allowed, in the Cisco DNA Spaces dashboard, click the Configure Manually link in the SSIDs window that is accessible from the Captive Portal app.

Contact Cisco DNA Spaces support team for establishing a VPN connection.

---

**Note**

You do not require a publicly resolvable domain name to connect to Cisco DNA Spaces.

Certain domain names must also be allowed in a customer’s infrastructure for the Cisco CMX instances that are deployed in a customer’s network is able to communicate with the Cisco DNA Spaces analytical and notification servers. To know the domain names that should be allowed, in the Cisco DNA Spaces dashboard, click the Configure Manually link in the SSIDs window.
## Cisco DNA Spaces Compatibility Matrix

**Table 6: Cisco DNA Spaces Compatibility Matrix**

<table>
<thead>
<tr>
<th>Application</th>
<th>AireOS Controller</th>
<th>Cisco Catalyst 9800 Series Wireless Controller</th>
<th>Cisco Embedded Wireless Controller</th>
<th>3375 Appliance</th>
<th>Cisco Prime/ Cisco DNA Center</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco DNA Spaces (with Detect and Locate, Captive Portal, Engagements, Location Personas, Behavior Metrics)</td>
<td>• Cisco Wireless Controller Native Cloud Connector- 8.3 or later (except 8.3.102 for Presence) • Cisco DNA Spaces Connector- 8.0.119 or later.</td>
<td>16.10 or later</td>
<td>16.11.1s or later</td>
<td>NA</td>
<td>3.0 or later for maps</td>
</tr>
</tbody>
</table>

**Note**
- Cisco Prime support is not there for maps on Cisco Embedded Wireless Controller.
Gettings Started

This chapter provides an overview of Cisco Digital Network Architecture (DNA) Spaces, its features, the process flow, license packages, and system requirements for Cisco DNA Spaces.

This chapter contains the following sections:
- **Overview of Cisco DNA Spaces**, on page 7
- **Cisco DNA Spaces Dashboard**, on page 8
- **Cisco DNA Spaces Features**, on page 9
- **Cisco DNA Spaces License Packages**, on page 12
- **Process Flow for Cisco DNA Spaces**, on page 12
- **Single Sign-On for Cisco DNA Spaces**, on page 13
- **Start Working with Cisco DNA Spaces**, on page 13

Overview of Cisco DNA Spaces

Cisco DNA Spaces is a multichannel engagement platform that enables you to connect, know, and engage with visitors at their physical business locations. It covers various verticals of business such as retail, manufacturing, hospitality, healthcare, education, financial services, enterprise work spaces, and so on. Cisco DNA Spaces also provides solutions for monitoring and managing the assets in your premises.

The following are the major features of Cisco DNA Spaces:
- A common platform for managing visitor engagements, assets and resources, and beacons.
- A single setup section to complete all the platform setups.
- Support to display promotions and offers to the customers connecting to your SSIDs.
- Support to target the customers individually or as a group based on their location, tag, visit frequency, visit duration, and so on using rules.
- Support to engage with multiple wireless networks simultaneously.
- Provision to view your business performance.
- App to create captive portals, and to display them to the customers based on rules.
- App to send notifications to the customers when they are in your business premises.
- App to inform the employees when customers are near your business premises.
• App to group the customers, and create tags.
• App to log in to Operational Insights.
• Provision to add third party partner apps.
• Support to import location hierarchy in the same structure as in your wireless network.
• Provision to create Cisco DNA Spaces users with different privileges and location access.
• Provision to monitor the performance status of Cisco DNA Spaces and its apps and latencies.

In the ABC shopping mall, to get free Wi-Fi, the customers must connect to an SSID once they enter the mall. ABC wanted to provide a personalized experience to each customer who connects to the Wi-Fi based on their purchase history and visit frequency. After installing Cisco DNA Spaces, ABC could collect the Wi-Fi user’s details through the captive portals, and utilize this details to send notifications to the customers regarding the offers and services available for them. The customers once connected to the Wi-Fi are taken to a captive portal, where they are provided with an option to register themselves by filling details such as name, e-mail address, telephone number, and so on. This information captured is stored in Cisco DNA Spaces. When customers re-visit the mall, promotional offers are sent to the customers through SMS, or e-mail.

Cisco DNA Spaces can also be configured to notify business users such as employees regarding customer activities. For example, you can identify and tag repeat customers as platinum members on Cisco DNA Spaces dashboard. When a platinum customer enters a restaurant and their device is detected by a wireless access point, the restaurant representatives would receive alerts on their devices, and can provide personalized services to the customer.

**Cisco DNA Spaces Dashboard**

The dashboard that appears after you log into Cisco DNA Spaces is shown in the following figure.
Cisco DNA Spaces Features

The major features of Cisco DNA Spaces includes:

**Digitization Stats**

On the Home page of the Cisco DNA Spaces dashboard, the following Cumulative Statistics values are displayed at the top of the page.

- **Locations**: The total network locations configured in Cisco DNA Spaces for various wireless networks.

- **Access Points**: The total number of APs added to Cisco DNA Spaces

- **Location Updates**: The total number of location updates received from the wireless networks from the date of deployment of Cisco DNA Spaces.

- **Square Foot**: The total area configured for network locations in the Location Info option in Location Hierarchy. However, if total area is not configured for network locations in the Location Hierarchy, then the Square Foot value will be displayed based on number of APs.

- **Visitors**: The total number of unique visitors that have visited your business locations from the date of deployment of Cisco DNA Spaces.

- **Visits**: The total number of visits (including repeated visits of unique visitors) that occurred in your business locations from the date of deployment of Cisco DNA Spaces.
If a location is removed or modified from the location hierarchy, the corresponding change in the Visitor, Visit, and location update count are not updated in the Digitization Stats section.

Apps

Cisco DNA Spaces provides various task-oriented apps. You can also add partner apps to Cisco DNA Spaces.

Cisco DNA Spaces provides the following apps:

Captive Portal App

The Captive Portal app enables you to create captive portals, and display them to your customers based on Captive Portals Rules.

Captive Portals

The captive portal refers to the portal that appears for a user who accesses your Wi-Fi from a particular location with a specific Wi-Fi network ID (SSID). The customers of this captive portal are internet users who connect to the Wi-Fi from your business locations.

You can enhance the portals with various features such as welcome messages, notices, promotions, apps, videos, help line, and so on using the various portal modules provided in Cisco DNA Spaces. For more information on creating and managing portals, see the “Creating and Managing Portal” section.

Captive Portal Rule

Cisco DNA Spaces enables you to create Captive Portal Rules to display the captive portals based on various parameters. You can configure to display a captive portal based on the location, number of visits made by the customer, type of customer, app status of the customer, and so on.

You can also use this rule to manage the internet provisioning for the customers, and to send customer information to an external API.

For more information, see the “Captive Portal Rule” section.

Engagements App

Cisco DNA Spaces also functions as a Wi-Fi based beacon that facilitates you send appropriate notification to your customers, who has a Wi-Fi enabled device, when the customer is in and around your business premises. The Engagements app enables you to reach out to your customers individually with different promotions and offers. You can remind the customers about the offers available for them and their membership details. You can also set to provide offers only in certain outlets.

You can configure to send the notifications using the Engagement Rule app. Cisco DNA Spaces enables you to send the notification when a customer connects to a Wi-Fi.

Cisco DNA Spaces enables you to send the notifications in the following ways:

- SMS
- E-mail
- API notifications
• Cisco Webex Teams

For more information, see the Creating an Engagement Rule section.

Location Personas App

Cisco DNA Spaces enables you create tags by grouping the customers. You can create the tags using the Location Personas app. You can also use the Location Personas app to add additional customers to an existing tag, or remove certain customers from an existing tag. For more information on creating tags, see the “Creating or Modifying Tags Using a Location Personas App” section.

Behavior Metrics App

The Behavior Metrics app enables you to view various reports that provide insights about the performance of your business. You can compare your business performance with the industry performance. By default, the report includes the data from the date of installation of Cisco DNA Spaces. The report will be shown for all the locations for which you have access. You can filter to view the report for a particular location, month or tag. For more information on Behavior Metrics report, see the “Overview of Behavior Metrics” section.

Location Analytics App and Impact Analysis App

The Location Analytics app enables you to view reports of visits in your locations. Impact Analysis is a way of measuring the effect of any action you made based on before and after analytics. For more information on these apps, see the respective chapters.

Operational Insights App

The Operational Insights app enables you to monitor assets and optimize the performance of your assets, sensors, alerting system, and operational work flows. The app provides a range of tags and sensors to continually integrate, monitor, and manage your connected operations. Using its cloud-based interface, you can define the profile, category, and ownership of each assets. You can establish business rules to define work flows, and the expected operating range of your assets and sensors.

Partner Apps

Cisco DNA Spaces enables you to integrate third party apps to Cisco DNA Spaces. The third party apps will be listed as partnership apps in the Cisco DNA Spaces dashboard.

Location Hierarchy

The Location Hierarchy feature enables you to define your business locations in Cisco DNA Spaces. You can import the locations in the same structure in which they are defined it your wireless network. The apps such as Engagements, Captive Portals, and Location Personas Rules depend on the location hierarchy defined. Cisco DNA Spaces provides universal account, and you can add the locations of multiple wireless networks to the location hierarchy.

The APs that you can add to the location hierarchy depends on the type of Cisco DNA Spaces license you own.

For more information, see the “Location Hierarchy in Cisco DNA Spaces” section.
Monitoring and Support

The Monitoring section enables you to monitor the performance status of Cisco DNA Spaces, and its apps. It also displays the app latencies and anomalies. For more information, see the “Monitoring” section.

Admin Management

The Admin Management feature enables you to create Cisco DNA Spaces users. You can restrict the privileges for each user based on their role. For more information, see the “Managing Cisco DNA Spaces Users and Accounts” section.

Setup

Wireless Networks

Displays features and instructions to connect Cisco DNA Spaces to a particular wireless network through various methods. For more information, see Setting Up Cisco DNA Spaces to Work with Various Wireless Networks.

Map Service

Enables you to upload the map of locations for CMX tethering.

Wireless Network Status

The Wireless Network Status option enables you to view the synchronization status of your wireless network. You can view the time at which the last synchronization happened.

Cisco DNA Spaces License Packages

Cisco DNA Spaces is available in three different license packages namely, See (Base), Act (Advance), and Extend. The features available for your account depends on the type of Cisco DNA Spaces license package you own. In the Cisco DNA Spaces dashboard, the apps are displayed based on the license type for which it will be available.

Process Flow for Cisco DNA Spaces

The process flow for Cisco DNA Spaces is as shown in the following figure.
Single Sign-On for Cisco DNA Spaces

Cisco DNA Spaces supports Single Sign-On (SSO) so that the users can login to Cisco DNA Spaces using their SSO credentials. For example, if the domain Cisco is SSO-enabled, the Cisco employees, who have Cisco DNA Spaces account, can access Cisco DNA Spaces using their Cisco e-mail address and password. If a Cisco employee is already logged in to Cisco domain through any particular website or application, that Cisco employee can access Cisco DNA Spaces by simply specifying the Cisco e-mail address.

When you click the **Login** button, only the **e-mail ID** field will appear in the **Login** window along with a **Continue** button. If the user is already logged into the SSO-enabled domain, then the user will be directly taken to the Cisco DNA Spaces dashboard after clicking the **Continue** button. If the particular Cisco DNA Spaces account supports multiple customer names, then the **Select Customer** window will be displayed. If the user has not logged into the domain, then the user will be redirected to the IDP page for login authentication, and user can login by specifying the SSO credentials.

To enable single sign-on, certain configuration must be done in Cisco DNA Spaces. These configurations will be done by the Cisco DNA Spaces support team. To enable SSO for your Cisco DNA Spaces account, contact the Cisco DNA Spaces support team.

Start Working with Cisco DNA Spaces

Before starting working with Cisco DNA Spaces ensure that you have the prerequisites mentioned in the “Cisco DNA Spaces Prerequisites” section.
Initially, you must contact Cisco DNA Spaces support team for creating a Cisco DNA Spaces account. You will get an invite to activate your Cisco DNA Spaces account through e-mail. Click the **Accept Activate** button, and in the window that appears configure the log in credentials, and click **Activate Account**. You are now logged into Cisco DNA Spaces. If you are a **Dashboard Admin**, you can now invite other Cisco DNA Spaces users.

To start working with Cisco DNA Spaces, perform the following steps:

---

**Step 1**

Log in to Cisco DNA Spaces.

**Note** You can enable Single Sign-On for Cisco DNA Spaces. For more information see, [Single Sign-On for Cisco DNA Spaces](#), on page 13.

**Step 2**

Connect to your wireless network and configure the wireless network for Cisco DNA Spaces referring to the instructions in the **Setup** section of the Cisco DNA Spaces dashboard.

The setup instructions are also available in the following sections of this guide:

- **Meraki**: For configuring a Cisco Meraki network, see the "Configuring Cisco DNA Spaces for Meraki" section.

- **Cisco Unified Wireless Network with Cisco CMX**: For connecting Cisco DNA Spaces with Cisco AireOS Controller through Cisco CMX, see the “**Connecting Cisco DNA Spaces to Cisco Wireless Controller through Cisco CMX**, on page 199” section.

- **Cisco AireOS Wireless Controller or Cisco Catalyst 9800 Series Wireless Controller (without Cisco CMX)**.

**Note** Connecting through the Cisco Wireless Controller Direct Connection method is only recommended for small scale deployments. All large scale production deployment require a Cisco DNA Spaces Connector.

- **Using Cisco Wireless Controller Direct Connect**: For configuring Cisco DNA Spaces with Cisco Wireless Controller using Wireless Controller Direct Connect, see the **Connecting Cisco Catalyst 9800 Series Wireless Controller or Cisco Wireless Controller to Cisco DNA Spaces Using WLC Direct Connect or Cisco DNA Spaces Connector**, on page 212 section.

- **Using Cisco DNA Spaces Connector**: For configuring a Cisco DNA Spaces with Cisco AireOS Wireless Controller or Cisco Catalyst 9800 Series Wireless Controller using Cisco DNA Spaces Connector, see the **Connecting Cisco DNA Spaces to Cisco AireOS Wireless Controller or Cisco Catalyst 9800 Series Wireless Controller using Cisco DNA Spaces Connector**, on page 231.

- **Using Cisco Embedded Wireless Controller**: For configuring a Cisco Unified Wireless Network using Cisco Embedded Wireless Controller, see the **Configuring Mobility Express to work with Cisco DNA Spaces** section.

**Note** Cisco DNA Spaces provides an universal account so that you can connect Cisco DNA Spaces to multiple wireless networks.

**Step 3**

Add your team members, and assign them roles and permissions. For more information on adding Cisco DNA Spaces users, see the “Managing Cisco DNA Spaces Users and Accounts” section.
| Step 4 | Import the location hierarchy defined in your wireless network to Cisco DNA Spaces. For more information on configuring the location hierarchy, see the “Location Hierarchy in Cisco DNA Spaces” section. |
| Step 5 | Import SSIDs to Cisco DNA Spaces. For more information on importing the SSIDs, see the “SSIDs” section. |
| Step 6 | Define Location Personas Rules to tag customers. For more information on creating a Location Personas Rule, see the “Creating or Modifying Tags Using a Location Persona App” section. |
| Step 7 | Configure supporting features such as SMS Gateways. Refer to the respective topic in this guide for configuration. |
| Step 8 | If required, create Captive Portals. For more information on creating the captive portals, see the “Creating and Managing Portal” section. |
| Step 9 | If required, create Captive Portal Rules to display the appropriate captive portal to various customers. For more information on creating Captive Portal Rules, see the “Captive Portal Rule” section. |
| Step 10 | If required, create Engagement Rules to send appropriate notifications to the customers. For more information on creating Engagement Rules, see the “Creating an Engagement Rule” section. |
| Step 11 | Analyze the Cisco DNA Spaces performance, and your business performance using apps such as Behavior Metrics, Location Analytics, and Impact Analysis. For more information on these apps, see the respective section. |
| Step 12 | Monitor the Cisco DNA Spaces domain and apps using the Monitoring and Support section. |
Start Working with Cisco DNA Spaces
CHAPTER 3

Location Hierarchy in Cisco DNA Spaces

This chapter describes the structure of the location hierarchy in Cisco Digital Network Architecture (DNA) Spaces, and how to define the location hierarchy in Cisco DNA Spaces.

- Overview of Location Hierarchy, on page 17
- Prerequisites for Defining the Location Hierarchy, on page 17
- Defining the Location Hierarchy, on page 18
- Managing the Location Hierarchy, on page 29
- Displaying Cumulative Count in Location Hierarchy, on page 48

Overview of Location Hierarchy

In Cisco DNA Spaces, you can import the locations in the same structure in which you have defined in your wireless network such as Cisco AireOS Wireless Controller, Cisco Catalyst 9800 Series Wireless Controller, or Cisco Meraki.

Each Cisco DNA Spaces customer is provided with a default customer name (root name), and this customer name acts as the root location of Cisco DNA Spaces location hierarchy.

As Cisco DNA Spaces provides universal account, you can import and manage the locations of multiple wireless networks. A proximity rule can include the locations of multiple wireless networks. You can create proximity rules such as Captive Portal rule, Engagement rule, and Location Personas rule, and view access points, users, and child locations for any location in the location hierarchy. The number of access points, proximity rules, child locations, and users for each location in the location hierarchy are displayed against that particular location. For example, the number of proximity rules, child locations, and users for a group are shown against that group in the location hierarchy. The count of these location parameters are shown in a cumulative manner.

Prerequisites for Defining the Location Hierarchy

To define the location hierarchy in the Cisco DNA Spaces dashboard, you must first define the required hierarchy structure in your wireless network such as Cisco Meraki, Cisco AireOS Wireless Controller or Cisco Catalyst 9800 Series Wireless Controller. In addition, you must establish connection between Cisco DNA Spaces and your wireless network.

- Configuring Cisco Meraki for Cisco DNA Spaces, on page 243
Defining the Location Hierarchy

Cisco DNA Spaces supports the following wireless networks:

- Cisco Meraki
- Cisco Wireless Controller with or without Cisco CMX
- Cisco Catalyst 9800 Series Wireless Controller

**Note**

For Cisco Wireless Controller without Cisco CMX and Cisco Catalyst 9800 Series Wireless Controller, you can ensure that appropriate data transfer happens between the Controller and Cisco DNA Spaces using a Cisco DNA Spaces Connector.

Based on your wireless network, choose the required instructions from the following:

**Defining the Location Hierarchy for Cisco Meraki**

To import the Cisco Meraki locations, first you must add the Cisco Meraki Organization under the customer name. You can then import Meraki networks. When you import a Meraki network, its floors, and access points are also imported. You can group the access points and create zones at network or floor level. You can group the locations at customer name, or organization level. You can also rename the customer name.

Before creating the location hierarchy, ensure that all the prerequisites are met. To know the prerequisites for creating the location hierarchy, see the Prerequisites for Defining the Location Hierarchy, on page 17.

**Note**

You must have Cisco Meraki credentials to import the locations. Thereafter, location hierarchy synchronizes with Cisco Meraki using a Meraki service account. So, you must configure the Cisco Meraki Service account in your Cisco Meraki Customer account for background network synchronization to keep the Location Hierarchy up-to-date. However, to connect Cisco DNA Spaces to Cisco Meraki, you must still use your Meraki customer account. For more information on configuring the Cisco Meraki service account, see Configuring Cisco Meraki Service Account, on page 243.

The location hierarchy for Cisco Meraki network is as follows:

Meraki > Organization > Network > Floor > Access Points.
The Location Hierarchy for Cisco Meraki is shown in the following figure.

*Figure 3: Location Hierarchy for Meraki*

If you do not have Meraki credentials you can import the locations using Meraki API keys. For more information on importing the locations from Meraki using the API keys, see Importing Cisco Meraki Locations Using the API Keys, on page 21.

If you have the Meraki credentials, to import the Meraki locations to Cisco DNA Spaces, perform the following steps:

---

**Note**

After defining the location hierarchy, ensure that you define timezones for locations. The timezone defined affects the Cisco DNA Spaces rules and reports.

---

**Adding a Cisco Meraki Organization**

To create the location hierarchy in Cisco DNA Spaces, first you must add the Cisco Meraki Organization of which you want to import the locations to the location hierarchy.

---

**Note**

Cisco DNA Spaces enables you to add multiple Cisco Meraki Organizations to the location hierarchy so that you can connect to the multiple Meraki organizations simultaneously.

---

**Step 1**

In the Cisco DNA Spaces dashboard, choose Location Hierarchy.

**Step 2**

In the Location Hierarchy window that appears, click More Actions for the customer name (root name).

**Step 3**

Choose Add a Wireless Network.

**Step 4**

From the Wireless Network drop-down list that appears, choose Cisco Meraki.

**Step 5**

Enter the user name and password for your Meraki account, and click Login.

**Step 6**

From the Organization drop-down list, choose the Cisco Meraki Organization from which you want to import the locations.
Adding a Network to Cisco Meraki Organization

Cisco DNA Spaces enables you to maintain the network, and floor structure followed for the location hierarchy in Cisco Meraki. After adding a Cisco Meraki Organization to the location hierarchy, you can import its networks, and the associated floors.

To import a network and its associated floors to the location hierarchy, perform the following steps:

**Step 1**
In the Cisco DNA Spaces dashboard, click **Location Hierarchy**.

**Step 2**
In the 'Location Hierarchy' window, click the **More Actions** icon at the far right of the Cisco Meraki Organization for which you want to add the network.

**Step 3**
Choose **Add Network**.

**Step 4**
In the **Add Network** window, select the networks that you want to add to the location hierarchy.

The **Add Network** window appears with all the available networks for that Cisco Meraki Organization.

**Step 5**
Click **Add**.

The networks added gets listed in the location hierarchy along with its associated floors.

**Note**
In Cisco Meraki application, ensure that the network name is not duplicated.

Creating Zones and Adding Access Points

You can group the access points of a network or floor using zones. You can create the zones at network or floor level.

**Note**
You cannot modify the access points for a floor.

To create a zone for a network or floor, perform the following steps:

**Step 1**
In the Cisco DNA Spaces dashboard, choose **Location Hierarchy**.

**Step 2**
In the **Locations** window, click the **More Actions** at the far right of the network or floor under which you want to create the zone.

**Step 3**
Choose **Add Zone**.

**Step 4**
In the **Add Zone** window that appears, perform the following steps:

a) In the **Zone Name** field, enter a name for the zone.

b) In the **Select Access Points** area, check the check box for the access points that you want to add to the zone.

c) Click **Add**.
Before creating the zones, locate the access points that you want to include in the zone in the Cisco Meraki dashboard.

When you add an access point of a network or floor to a zone, that access point will not be available for that network or floor. The access points added to a zone will not be available for other zones.

Importing Cisco Meraki Locations Using the API Keys

To import Cisco Meraki locations using the API keys, perform the following steps:

Step 1
In the Location Hierarchy window, click the More Actions icon for the customer name (root name), and click Add a Wireless Network.

Step 2
In the window that appears, from the Add a Wireless Network drop-down list, choose Cisco Meraki.

Step 3
Click the Import Organization using API link that appears when you select Cisco Meraki.

Step 4
In the API Key field, enter the API Key for Meraki, and click Fetch Organizations.

The organizations for that API key gets listed.

Step 5
Select the organization that you want to import, and click Add.

The organization gets listed in the Locations window.

Step 6
Add the networks under the organization using the Add Network in the More Actions menu for the organization.

When you import a network, the floors and access points under it also get imported.

Step 7
Create zones under the floors using the Add Zones in the More Actions menu for the floors.

Defining the Location Hierarchy for Cisco AireOS/ Cisco Catalyst Wireless Controller with Cisco CMX

Before creating the location hierarchy, ensure that all the prerequisites are met. To know the prerequisites for creating the location hierarchy, see the Prerequisites for Defining the Location Hierarchy, on page 17.

Cisco DNA Spaces supports only Cisco CMX 10.6 or later. If you are using Cisco AireOS/ Catalyst with Cisco CMX, you can import the locations using CMX Tethering.

The location hierarchy for Cisco AireOS/Catalyst Wireless Controller with a Cisco CMX installation is as follows:

Cisco CMX Node > Campus > Building(network) > Floor > Access Points

The location hierarchy for Cisco AireOS/Catalyst Wireless Controller with Cisco CMX is shown in the following figure.
After defining the location hierarchy, ensure that you define timezones for locations. The timezone defined affects the Cisco DNA Spaces rules and reports.

- CMX Tethering can be done using Map Services or by configuring Token in Cisco CMX.

**Connecting Cisco DNA Spaces to Cisco Wireless Controller or Cisco Catalyst 9800 Series Wireless Controller Using CMX Tethering**

If you are having Cisco CMX 10.6 or later, you can use the CMX tethering feature to connect Cisco DNA Spaces to the controller, import locations and to configure the location updates for notifications and reports.

Cisco DNA Spaces Network Sync Server supports AP synchronization for CMX Tethering. For CMX Tethering, the changes made to APs in Cisco Prime get updated in Cisco DNA Spaces location hierarchy. To synchronize the AP changes, do any of the following:

- In Cisco CMX, click **SYSTEM**. In the dashboard that appears, choose **Settings > Controllers and Maps Setup > Import** In the window that appears, provide Cisco Prime Username, Password and IP Address. Then click **Import Controllers and Maps** to get latest map changes. Click **Save**.
- Download updated map from Cisco Prime and upload it to Cisco CMX.
- Download updated map from Cisco Prime and upload it to Map Services in Cisco DNA Spaces.

You can do CMX Tethering in the following ways:

**CMX Tethering by Configuring Token in Cisco CMX**

To configure CMX Tethering through token, perform the following steps:

**Step 1** In the Cisco DNA Spaces dashboard, choose **Setup > Wireless Networks**.
**Step 2** In the **Connect your wireless network** window, click **Add New**.
**Step 3** Click **Select** for **Cisco AireOS/Catalyst**.
**Step 4** Click **Select** for **Connect Via CMX Tethering**.
The prerequisites for using this option are displayed.

Step 5  
Click Continue Setup.

The Connect Via CMX Tethering widget appears in the Connect your wireless network window.

Step 6  
Expand the widget Connect Via CMX Tethering.

Step 7  
Click Create New Token displayed at Step 2.

Step 8  
In the Create a new token window, enter a name and description for the Cisco CMX Tethering.

Step 9  
Click Save.

Step 10  
Click View Tokens displayed at Step 2.

The Cisco CMX Tethering instance added gets listed.

Step 11  
To generate token for connecting the Cisco DNA Spaces with Cisco CMX, in the CMX Tethering Tokens window, click the Key icon for the Cisco CMX Tethering instance for which you want to generate token.

Step 12  
Click Copy.

Step 13  
Log into Cisco CMX.

Step 14  
Choose Manage > Cloud Apps.

Step 15  
In the Cloud Applications window that appears, click Enable in the Actions column for Cisco DNA Spaces.

Step 16  
In the window that appears, configure the token copied from Cisco DNA Spaces dashboard.

Note To enable the Cisco DNA Spaces service in Cisco CMX, you must have a Cisco DNA Spaces account.

Step 17  
To import the CMX Node to the location hierarchy, click Add CMX at Step 3.

Step 18  
In the ADD CMX to Location Hierarchy, click the radio button for the CMX node that you want to add.

Step 19  
Click Next.

The campuses under this CMX node are displayed along with its building. If you do not want to import a particular campus, building, you can uncheck the corresponding check box. By default, all are selected.

Step 20  
In the Display Name field, enter the name that must appear for this CMX node in the location hierarchy.

Step 21  
Click Import.

Step 22  
Create Zones and group access points, if required. For more information on creating zones, see Creating Zones and Adding Access Points, on page 25.

The CMX Node imported is displayed in the Location Hierarchy along with its campuses, buildings, and floors. You can now add campuses, building, and other child locations whenever required under this CMX node. For more information on adding campus, building, floors, and so on, see Managing the Location Hierarchy for Cisco Wireless Controller with CMX, on page 40.

You can import the CMX Node to the location hierarchy (Step 18 to Step 22) also using the Add a Wireless Network option in the More Actions menu for the root location. From the Wireless Network drop-down list, choose CMX On Prem. In the Display Name field, enter a name for the CMX node, and click Add.
What to do next

Note: When you configure CMX tethering using token, the location map for the particular CMX node appears in the Map Service window of the Cisco DNA Spaces dashboard.

CMX Tethering by Uploading the Location Map to Map Services

Note: The configurations done in the external applications that are not a part of Cisco DNA Spaces, and the menu path and names specified for the tabs, windows, options, and so on in this documentation are subject to change.

Step 1: Log into Cisco Prime Infrastructure.
Step 2: In the Settings/Getting Started window, click the circle icon near the top left of the window (near Cisco logo).
Step 3: In the window that appears, click Maps on the left pane.
Step 4: In the Wireless Maps area, click Site Maps (Deprecated).

Note: You can add new locations using the Site Maps (New) option.

Step 5: Click the drop-down list near Go, and choose Export Maps.
Step 6: Click Go.
Step 7: From the tree view of location maps, select the parent location (CMX node) that you want to export, and click Export.

Note: Ensure that the Include Map Information check box is checked.

Save the location map on your computer.

Note: You must download the map in the zip format and upload it in the Cisco DNA Spaces in the same format.

Step 8: In the Cisco DNA Spaces dashboard, choose Setup > Map Services.
Step 9: Click Maps Upload at the top left of the window, and select the location map downloaded from Cisco Prime Infrastructure.

Note: You can add a CMX Zone in Setup > Map Service using the square icon (below the Expand Collapse icon) displayed in the map.

Step 10: In the Cisco DNA Spaces dashboard, choose Location Hierarchy.
Step 11: Click the More Actions menu at the far right of the root location.
Step 12: Click Add a Wireless Network.
Step 13: From the Wireless Network drop-down list, choose CMX On Prem.
Step 14: In the Display Name field, enter a name for the CMX node.

CMX Tethering will be displayed under the title Add Network by.

Step 15: Click Add.
Step 16: Create Zones and group access points, if required. For more information on creating zones, see Creating Zones and Adding Access Points, on page 25.
The locations for the CMX node imported get displayed in the location hierarchy. You can now add campuses, building, and other child locations whenever required under this CMX node. For more information on adding campus, building, floors, and so on, see Managing the Location Hierarchy for Cisco Wireless Controller with CMX, on page 40.

Creating Zones and Adding Access Points

You can group the access points of a building or floor using zones. You can create the zones at building or floor level.

Note

You cannot modify the access points for a floor.

To create a zone for a building or floor, perform the following steps:

Step 1
In the Cisco DNA Spaces dashboard, choose Location Hierarchy.

Step 2
In the Location Hierarchy window, click More Actions at the far right of the building or floor under which you want to create the zone.

Step 3
Choose Add Zone.

Step 4
In the Add Zone window that appears, perform the following steps:

a) In the Zone Name field, enter a name for the zone.

b) In the Select Access Points area, select the check box for the access points that you want to add to the zone.

c) Click Add.

What to do next

When you add an access point of a building or floor to a zone, that access point will not be available for that building or floor. The access points added to a zone will not be available for other zones.

Defining the Location Hierarchy for Cisco Catalyst 9800 Series Wireless Controllers or Cisco Wireless Controller (without Cisco CMX)

You can connect a Cisco AireOS Wireless Controller (without CMX) or Cisco Catalyst 9800 Series Wireless Controller to Cisco DNA Spaces using any of the following connectors:

- Cisco WLC Direct Connect
- Cisco DNA Spaces Connector

For more information on features supported by these connectors, see Features Supported by Various Connectors, on page 198.
When you have connected the controller to Cisco DNA Spaces using Cisco WLC Direct Connect or Cisco DNA Spaces Connector, you can import the locations to the location hierarchy using any of the following methods:

- **Access Point Prefix**: If you are using this option, you can add only networks, groups, and zones in the location hierarchy. For more information on connecting the Cisco Wireless Controller to Cisco DNA Spaces, and importing the location hierarchy to the Cisco DNA Spaces dashboard, see Importing the Locations using Access Point Prefix, on page 26. Alternatively, you can also refer to the configurations steps for Connect WLC/Catalyst 9800 Directly in Setup > Wireless Networks of Cisco DNA Spaces dashboard.

- **Importing from Maps**: If you use this option, you can import the locations in the same hierarchical structure as in Cisco Prime, Campus-Building-Floor. In this method, you must import the location map from Cisco Prime Infrastructure and upload the map to the Map Services option in the Cisco DNA Spaces dashboard. You can then import that locations to the location hierarchy. For more information on importing the locations using Map Services, see Importing Locations to the Location Hierarchy Using Map Services, on page 27.

**Note**

If you were using Cisco DNA Spaces earlier with Cisco CMX, and if you are moving to use Cisco DNA Spaces directly with Cisco Wireless Controller, the Reports and proximity rules will be affected. The Reports will be shown based on the new location configurations. You also have to re-configure the proximity rules to display captive portals or to send notifications.

**Importing the Locations using Access Point Prefix**

**Step 1**
To import the locations to the Cisco DNA Spaces, click the three-line menu icon at the top-left of the Cisco DNA Spaces dashboard,

**Step 2**
Choose Location Hierarchy.

**Step 3**
In the Location Hierarchy window, click More Actions at the far right of the customer name(root name).

**Step 4**
Click Add a Wireless Network.

**Step 5**
From the Wireless Network drop-down list, choose WLC Direct Connect.

**Step 6**
Click the Access Point Prefix radio button.

The imported Cisco Wireless Controllers get listed.

**Note**
The Cisco Wireless Controllers get listed only if you configure the Cisco Wireless Controller for importing them to Cisco DNA Spaces.

**Step 7**
Select the Cisco Wireless Controller, and click Next.

This Cisco Wireless Controller will act as the primary Cisco Wireless Controller.

**Step 8**
Select another Cisco Wireless Controller as secondary controller, and click Next.

**Note**
This feature helps you manage Cisco DNA Spaces with a secondary Cisco Wireless Controller with the same APs if the primary controller is down.

The secondary controller is optional. You can move to the next screen without selecting a secondary controller by clicking the Skip button.
Step 9 Select the networks that you want to add.

**Note** Cisco DNA Spaces will automatically group the APs based on the prefix of their names, and creates networks. The APs that are not grouped under a network will be listed under the name “Unconfigured”.

**Note** If you are not selecting a network, the APs in that network will be added to the location hierarchy under the name “Unconfigured”.

Step 10 Click Done.

The APs of the primary and secondary controllers selected will get listed in the location hierarchy.

Step 11 In the location hierarchy, click the More Actions icon at the far right of the network, and click Add Zone.

Step 12 In the window that appears, enter a name for the zone, and select the APs to be included in the zone.

Step 13 Similarly, create all the required zones.

**Tip** If you were using Cisco DNA Spaces with Cisco CMX, create zones in the same structure as created earlier with the Cisco CMX.

Step 14 If you have created the location hierarchy earlier using the Cisco CMX, delete that location hierarchy, and re-configure the rules such as captive portal rules, engagement rules and location personas rules.

**Note**

- After defining the location hierarchy, ensure that you define timezones for locations. The timezone defined affects the Cisco DNA Spaces rules and reports.

- When adding the APs in the Cisco Wireless Controller, follow proper naming conventions (with appropriate prefix) to ease auto-network creation in Cisco DNA Spaces.

- In the Cisco Wireless Controller, if new APs are added to the Cisco Wireless Controller, those APs get automatically imported during the next Cisco Wireless Controller synchronization. If an imported AP is deleted from the Cisco Wireless Controller, the changes will be reflected in Cisco DNA Spaces only after 48 hours.

---

**What to do next**

You can change the primary controller, and add more secondary controllers. You can also add APs of multiple prefixes to a single network. For more information, see the Managing the Location Hierarchy for Cisco Wireless Controller or Cisco Catalyst 9800 Series Controller(with WLC Direct Connect or Cisco DNA Spaces Connector), on page 45.

**Importing Locations to the Location Hierarchy Using Map Services**

If a Cisco Wireless Controller or Cisco Catalyst 9800 Series Wireless Controller is connected to Cisco DNA Spaces through WLC Direct Connect or Cisco DNA Spaces Connector, you can import the locations to the location hierarchy using the Map Services. If you are using this option, you can import the locations in the same hierarchial structure, Campus- Building-floor.

To import the to the location hierarchy using the Map Services, perform the following steps:

Step 1 Log into Cisco Prime Infrastructure.

Step 2 In the Settings /Getting Started window, click the circle icon near the top-left of the window (near Cisco logo).
Step 3  In the window that appears, click Maps on the left pane.

Step 4  In the Wireless Maps area, click Site Maps (Deprecated).

**Note**  You can add new locations using the Site Maps (New) option.

Step 5  Click the drop-down list near Go, and choose Export Maps.

Step 6  Click Go.

Step 7  From the tree view of location maps, select the parent location (CMX node) that you want to export, and click Export.

**Note**  Ensure that the Include Map Information check box is checked.

Step 8  Save the location map on your computer.

**Note**  You must download the map in the gzip format and upload it in the Cisco DNA Spaces in the same format.

Step 9  In the Cisco DNA Spaces dashboard, choose Setup > Map Services.

Step 10 Click Upload at the top left of the window, and select the location map downloaded from Cisco Prime Infrastructure.

The location map gets uploaded to the Map Services.

Step 11 In the Cisco DNA Spaces dashboard, choose Location Hierarchy.

Step 12 In the Location Hierarchy window, click More Actions at the far right of the root location.

Step 13 Click Add a Wireless Network.

The Add a Wireless Network window appears.

Step 14 From the Add a Wireless Network drop-down list, choose WLC Direct Connect.

Step 15 Click the Import from Maps radio button.

The campuses and its associated buildings and floors that are available in the location map imported to Map Services are displayed.

Step 16 In the Display Name field, enter a name for the parent location that must appear under the root location.

Step 17 Check the campuses that you want to import.

When you check a campus, its associated buildings and floors also get selected. If you do not want to import a particular building, uncheck that building's check box. However, you cannot uncheck a particular floor.

Step 18 Click Import.

A message Locations imported Successfully is shown.

You can now view the imported locations in the location hierarchy

**Note**  If you are adding new locations in the wireless network, you have to import them manually to the location hierarchy following the same procedure.

After defining the location hierarchy, ensure that you define timezones for locations. The timezone defined affects the Cisco DNA Spaces rules and reports.
Managing the Location Hierarchy

Renaming a Customer

To rename a customer, perform the following steps:

1. In the Cisco DNA Spaces dashboard, click Location Hierarchy.
2. In the Location Hierarchy window, click More Actions at the far right of the customer name.
3. Click Rename <root name>.
4. In the Rename root window that appears, enter the customer name you want.
5. Click Rename.

Adding a Wireless Network

Cisco DNA Spaces supports Cisco AireOS Wireless Controller (Cisco Wireless Controller), Cisco Catalyst 9800 Series Wireless Controller and Cisco Meraki. You can add multiple wireless networks to the location hierarchy using the Add a Wireless Network option.

In the Add a Wireless Network window, the Add a Wireless Network drop-down list will be having the following three options:

- **Meraki**—To define the location hierarchy for Meraki network.
- **CMX On Prem**—To define the location hierarchy for Cisco AireOS Wireless Controller with Cisco CMX.
- **WLC Direct Connect**—To define the location hierarchy for Cisco Catalyst 9800 Series Wireless Controller or Cisco Wireless Controller without Cisco CMX.

For more information on adding a Cisco CMX node, Cisco Meraki Organization, or Cisco Wireless Controller access points using the Add a Wireless Network option, see Defining the Location Hierarchy, on page 18.

Adding Metadata for a Location

You can group the locations using metadata. You can use this metadata when defining the proximity rules. You can also use this metadata also for defining the brands for the Behavior Metrics app.

To add metadata for a location, perform the following steps:

1. In the Cisco DNA Spaces dashboard, choose Location Hierarchy.
2. In the Location Hierarchy window, click the More Actions icon for the location for which you want to add metadata.
3. Click Add/Edit Metadata.
4. In the Add Metadata for <location> window that appears, perform the following steps:
   a) In the Key field, enter a metadata key.
b) In the value field, enter a value for the key.
c) Click **Save**.

---

**What to do next**

**Note**
Similarly, add the metadata for other locations that must have this metadata.

---

**Updating Metadata for a Location**

To update the metadata for a location, perform the following steps:

**Step 1** In the **Location Hierarchy** window, click **More Actions** at the far right of the location for which you want to update the location metadata.

**Step 2** Click **Add/Edit Metadata**.

**Step 3** In the **Add Metadata for <location>** window that appears, click the metadata that you want to update.

**Step 4** Make necessary changes, and click **Update**.

---

**What to do next**

**Note**
You can delete a location metadata by clicking the Delete button for that metadata.

---

**Defining or Changing the Time Zone for Locations**

You can define the time zone for various locations in the location hierarchy. To define the time zone for a location, perform the following steps:

**Step 1** In the Cisco DNA Spaces dashboard, choose **Location Hierarchy**.

**Step 2** In the **Location Hierarchy** window, click **More Actions** for the location for which you want to define the time zone.

**Step 3** Click **Time Zone**.

The **Change TimeZone** window appears. In the **Current Time Zone** field, the time zone configured for the location appears. For a location for which the time zone is not yet defined, **No Time Zone** appears in the **Current Time Zone** field.

**Step 4** From the **Select Timezone** drop-down list, choose the time zone that you want to configure for this location.

**Step 5** Click **Change**.
The time zone is defined for the location.

**What to do next**

| Note | The notifications are sent for the locations based on the configured time zones. |

**Adding the Information of a Location**

You can specify the information such as address of each separately location in the location hierarchy.

To add the location information for a location, perform the following steps:

**Step 1** Click the three-line menu icon at the top-left of the Cisco DNA Spaces dashboard.

**Step 2** Choose **Location Hierrachy**.

**Step 3** In the **Location Hierarchy** window, click the location for which you want to add the information.

**Step 4** On the **Location Info** tab, click **Edit** for **Location Data**.

**Step 5** In the **Location Information** window that appears, enter the information for the particular location.

You can add the following information about the location:

- Brand
- Country
- State
- City
- Zip /Postal Code
- Address
- Time Zone
- Area in Square Feet or Square Meter
- Occupancy Limit (Max Capacity)

**Step 6** Click **Update**.

The location information added will now gets listed in the **Location Data** area on the **Location Info** tab.

**Note** If you are not specifying the location information for a location, that location will inherit the information of its parent location. Location information inherited from the parent location will appear in Orange. However, we recommend you to update the location information for each location.
Searching for a Location

You can search for a location in the location hierarchy using its name. To search for a location in the location hierarchy, perform the following steps:

**Step 1**
In the Cisco DNA Spaces dashboard, choose **Location Hierarchy**.

The **Location Hierarchy** window appears.

**Step 2**
In the Search field, enter the name of the location that you want to search.

The location gets highlighted in the location hierarchy.

Searching for an Access Point

You can search for an access point using its name or Mac address.

To search for an access point in the location hierarchy, perform the following steps:

**Step 1**
In the Cisco DNA Spaces dashboard, choose **Location Hierarchy**.

The **Location Hierarchy** window appears.

**Step 2**
In the Search field, enter the name or Mac address of the access point that you want to search.

The access point gets highlighted.

Managing the Maps for a Location

The maps are displayed by default based on the map configuration in the wireless network.

To view the map for a location, perform the following steps:

**Step 1**
In the Cisco DNA Spaces dashboard, choose **Location Hierarchy**.

The **Location Hierarchy** window appears with the location hierarchy.

**Step 2**
In the location hierarchy, click the location for which you want to view the map.

**Step 3**
Click the **Maps** tab.

The map appears in the **Maps** tab.

Managing the Access Points

You can add or remove access points to a zone.
Adding an Access Point to a Zone

To add access points to a zone, perform the following steps:

**Step 1**
In the Cisco DNA Spaces dashboard, choose Location Hierarchy.

The Location Hierarchy window appears with the location hierarchy.

**Step 2**
In the location hierarchy, click the zone to which you want to add the access point.

**Step 3**
Click Modify Access Points

**Step 4**
Select the check box for the access point that you want to add.

**Step 5**
Click Add.

The access point gets added to the zone.

---

**What to do next**

**Note**
If there are no access points under that zone, the button name will be Add Access Points.

**Note**
For Cisco Unified Wireless Network, to import the access points, the Cisco CMX must be publicly accessible. For a default Cisco Unified Wireless Network installation, the ports 80 and 443 must be open. For more information, see the “Bandwidth Requirements to Deploy Cisco DNA Spaces” section.

---

Removing an Access Point from a Zone

To remove an access point from a zone, perform the following steps:

**Step 1**
In the Cisco DNA Spaces dashboard, choose Location Hierarchy.

The Location Hierarchy window appears with the location hierarchy.

**Step 2**
In the location hierarchy, click the zone from which you want to delete the access point.

**Step 3**
Click Modify Access Points.

**Step 4**
Uncheck the check box for the access point that you want to delete.

**Step 5**
Click Add.

The access point gets deleted from the zone.

---

Viewing the Access Points for a Location

You can view the access points under each location. Ideally, the access points belong to a floor or zone.
To view the access points for a location, perform the following steps:

---

**Step 1**
In the Cisco DNA Spaces dashboard, choose **Location Hierarchy**.
The **Location Hierarchy** window appears with the location hierarchy.

**Step 2**
In the location hierarchy, click the location for which you want to view the access points.

**Step 3**
Click the **Access Points** tab.
The access points associated with that location are displayed.

---

**What to do next**

---

**Note**
The **Access Points** link for a location is enabled only if at least one access point exists for that location.

---

**Managing the Groups**
Cisco DNA Spaces enables you to rename a group name, edit a group, and delete an independent group.

**Creating Groups**
Grouping enables you to create proximity rules specific to a set of locations. You can create groups at the higher levels in the location hierarchy.

For Cisco Unified Wireless Network, you can group the CMX nodes or campuses in the location hierarchy. For example, you can group the Campus1 and Campus 2 under one group and Campus 3 and Campus 4 under another group. You can also create sub groups under these groups. For Meraki, you can group the Cisco Meraki Organizations or networks in the location hierarchy. For example, you can group the Network 1 and Network 2 under one group and Network 3 and Network 4 under another group. You can also create sub groups under these groups.

You can also create a group including the wireless network nodes of both Cisco Unified Wireless Network and Meraki. However, you cannot group the lower level locations of Cisco Unified Wireless Network and Meraki. For example, you cannot group a campus and a Meraki network.

To create a group for a location, perform the following steps:

---

**Step 1**
In the Cisco DNA Spaces dashboard, click **Location Hierarchy**.

**Step 2**
In the **Location Hierarchy** window, click **More Actions** at the far right of the location under which you want to add the group.

**Step 3**
Click **Create Group**.

**Step 4**
In the window that appears, perform the following steps:

a) Enter a name for the group.

b) Select the locations that you want to add under this group.
The locations available for selection depends upon where you are adding the group in the location hierarchy. When you add a group under the customer name (root level), the first level locations (For example, CMX node, Cisco Meraki Organization) are available for selection. When you add a group under a CMX node, only the campuses under that CMX node are available for selection.

c) Click Add.

What to do next

Tip
If you want to have a parent group without any location, and sub groups with location, then you first create the parent group with all the required locations that must become the part of its sub groups. Then you create a sub group under the parent group. The locations added to the parent group are available for selection. Select the locations that you want to add under the sub group. Similarly, you can create more sub groups under the parent group.

Note
You can add more locations to a group at any time.

Renaming a Group

To rename a group, perform the following steps:

Step 1
In the Cisco DNA Spaces dashboard, choose Location Hierarchy. The Location Hierarchy window appears with the location hierarchy.

Step 2
In the location hierarchy, click More Actions for the group that you want to rename.

Step 3
Click Rename "group name".

Step 4
In the Rename group window that appears, enter the new name for the group.

Step 5
Click Rename.

Editing a Group

You can add or remove the locations from a group.

To edit a group, perform the following steps:

Step 1
In the Cisco DNA Spaces dashboard, choose Location Hierarchy. The Location Hierarchy window appears with the location hierarchy.

Step 2
In the location hierarchy, click More Actions for the group that you want to edit.

Step 3
Click Edit group.

Step 4
In the Edit Group window that appears, check the check box for the locations that you want to be part of the group.
Deleting a Group

To delete a group, perform the following steps:

**Step 1**
In the Cisco DNA Spaces dashboard, choose Location Hierarchy. The Location Hierarchy window appears with the location hierarchy.

**Step 2**
In the location hierarchy, click More Actions at the far-right of the group that you want to delete.

**Step 3**
Click Delete group.

**What to do next**

---

**Note**
To delete a group, first you have to delete the locations and sub groups under that group, if any.

---

**Note**
You cannot delete a group that is associated with the proximity rules.

Managing the Zones

You can rename and delete the zones created for Cisco Unified Wireless Network or Meraki.

Renaming a Zone

To rename a zone, perform the following steps:

**Step 1**
In the Cisco DNA Spaces dashboard, choose Location Hierarchy. The Location Hierarchy window appears.

**Step 2**
In the location hierarchy, click More Actions for the zone that you want to rename.

**Step 3**
Click Rename "zone name".

**Step 4**
In the Rename-zone window that appears, enter the new name for the zone.

**Step 5**
Click Rename.

Deleting a Zone

To delete a zone, perform the following steps:
**Step 1**  
In the Cisco DNA Spaces dashboard, choose **Location Hierarchy**.  
The **Location Hierarchy** window appears.

**Step 2**  
In the location hierarchy, click **More Actions** for the zone that you want to delete.

**Step 3**  
Click **Delete zone**.

<table>
<thead>
<tr>
<th>What to do next</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Note</strong> You cannot delete any zone that is associated with the proximity rules.</td>
</tr>
</tbody>
</table>

### Managing the Location Hierarchy for Meraki

You can rename, and delete the locations under Meraki.

#### Adding Floors to a Network

To add a floor to a network, perform the following steps:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In the Cisco DNA Spaces dashboard, choose <strong>Location Hierarchy</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>In the <strong>Location Hierarchy</strong> window, click <strong>More Actions</strong> at the far right of the network under which you want to create the floor.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the <strong>Add Floor</strong> window that appears, select the floor that you want to add under the network.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click <strong>Add</strong>.</td>
</tr>
</tbody>
</table>

The floor gets added to the network.

### Renaming a Cisco Meraki Organization

To rename a Cisco Meraki Organization, perform the following steps:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In the Cisco DNA Spaces dashboard, choose <strong>Location Hierarchy</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>In the location hierarchy, click <strong>More Actions</strong> for the organization that you want to rename.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click <strong>Rename &quot;Organization Name&quot;</strong>.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the <strong>Rename-Meraki</strong> window that appears, enter the new name for the Cisco Meraki Organization.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click <strong>Rename</strong>.</td>
</tr>
</tbody>
</table>
Deleting a Cisco Meraki Organization

To delete a Cisco Meraki Organization, perform the following steps:

**Step 1**
In the Cisco DNA Spaces dashboard, choose Location Hierarchy.

The Location Hierarchy window appears with the location hierarchy.

**Step 2**
In the location hierarchy, click More Actions for the Cisco Meraki Organization that you want to delete.

**Step 3**
Click Delete Organization.

---

**What to do next**

**Note**
To delete an organization, first you have to delete the locations and groups under that organization, if any.

- You cannot delete any organization that is associated with the proximity rules.

Renaming a Network

To rename a network, perform the following steps:

**Step 1**
In the Cisco DNA Spaces dashboard, choose Location Hierarchy.

The Location Hierarchy window appears with the location hierarchy.

**Step 2**
In the location hierarchy, click More Actions for the network that you want to rename.

**Step 3**
Click Rename "network name".

**Step 4**
In the Rename-location window that appears, enter the new name for the location.

**Step 5**
Click Rename.

---

Deleting a Network

To delete a network, perform the following steps:

**Step 1**
In the Cisco DNA Spaces dashboard, choose Location Hierarchy.

The Location Hierarchy window appears with the location hierarchy.

**Step 2**
In the location hierarchy, click More Actions for the network that you want to delete.

**Step 3**
Click Delete network.
What to do next

Note
To delete a network, first you have to delete the floors and access points under that network, if any.

• You cannot delete any network that is associated with a proximity rule.

Renaming a Floor

To rename a floor, perform the following steps:

Step 1 In the Cisco DNA Spaces dashboard, choose Location Hierarchy.
The Location Hierarchy window appears with the location hierarchy.

Step 2 In the location hierarchy, click More Actions for the floor that you want to rename.

Step 3 Click Rename "floor name".

Step 4 In the Rename-floor window that appears, enter the new name for the floor.

Step 5 Click Rename.

Deleting a Floor

To delete a floor, perform the following steps:

Step 1 In the Cisco DNA Spaces dashboard, choose Location Hierarchy.
The Location Hierarchy window appears with the location hierarchy.

Step 2 In the location hierarchy, click More Actions for the floor that you want to delete.

Step 3 Click Delete floor.

What to do next

Note
If the floor that you delete has any zone under it, that zone is moved under the network after the deletion of the floor.

Note
You cannot delete any floor that is associated with a proximity rule.
Managing the Location Hierarchy for Cisco Wireless Controller with CMX

Adding a Campus to the Location Hierarchy

Cisco DNA Spaces enables you to maintain the campus, building, and floor structure followed for the location hierarchy in the Cisco CMX. After adding a CMX node to the location hierarchy, you can import its campuses, and the associated buildings, floors, and access points.

To import a campus and its associated buildings, floors, and access points to the location hierarchy, perform the following steps:

1. In the Cisco DNA Spaces dashboard, choose Location Hierarchy.
2. In the Location Hierarchy window, click More Actions at the far right of the CMX node for which you want to add the campus.
3. Click Add Campus.
4. In the Add Campus window that appears, select the campuses that you want to add to the location hierarchy.
   
   *Note* If you do not want to add a particular building or floor of a campus to the location hierarchy, you can remove it by unchecking the corresponding check box. If required, you can add it to the location hierarchy any time later. For more information on adding a building to a campus, see the Adding a Building to a Campus, on page 40. For more information on adding a floor to a building, see the Adding a Floor to a Building, on page 41.
5. Click Add.

The campuses added gets listed in the location hierarchy along with its associated buildings and floors.

*Note* In the Cisco CMX, ensure that there is no duplicate for a building name under a campus.

Adding a Building to a Campus

To add a building to a campus, perform the following steps:

1. In the Cisco DNA Spaces dashboard, click Location Hierarchy.
2. In the Location Hierarchy window, click More Actions at the far right of the campus to which you want to add the building.
3. Click Add Building.
4. In the Add Building window that appears, select the building that you want to add under the campus.
5. Click Add.

The building gets listed under the campus in the location hierarchy.
Adding a Floor to a Building

To add a floor to a building, perform the following steps:

**Step 1**  
In the Cisco DNA Spaces dashboard, click **Location Hierarchy**.

**Step 2**  
In the **Location Hierarchy** window, click **More Actions** at the far right of the building to which you want to add the floor.

**Step 3**  
Click **Add Floor**.

**Step 4**  
In the **Add Floor** window that appears, select the floor that you want to add under the building.

**Step 5**  
Click **Add**.  
The floor gets listed under the building.

Renaming a CMX Node

To rename a CMX node, perform the following steps:

**Step 1**  
In the Cisco DNA Spaces dashboard, choose **Location Hierarchy**.  
The **Location Hierarchy** window appears with the location hierarchy.

**Step 2**  
In the location hierarchy, click **More Actions** for the CMX node that you want to rename.

**Step 3**  
Click **Rename <Cisco CMX Node>**.

**Step 4**  
In the window that appears, enter the new name for the CMX node.

**Step 5**  
Click **Rename**.

What to do next

**Note**  
The renaming is not reflected in the Cisco CMX.

Deleting a CMX Node

To delete a CMX node from the location hierarchy, perform the following steps:

**Step 1**  
In the Cisco DNA Spaces dashboard, choose **Location Hierarchy**.  
The **Location Hierarchy** window appears with the location hierarchy.

**Step 2**  
In the location hierarchy, click **More Actions** for the CMX node that you want to delete from the location hierarchy.

**Step 3**  
Click the option to delete the CMX node.
Renaming a Campus

To rename a campus, perform the following steps:

**Step 1**
In the Cisco DNA Spaces dashboard, choose **Location Hierarchy**.

The **Location Hierarchy** window appears with the location hierarchy.

**Step 2**
In the location hierarchy, click **More Actions** for the campus that you want to rename.

**Step 3**
Click **Rename <campus name>**.

**Step 4**
In the **Rename-campus** window that appears, enter the new name for the campus.

**Step 5**
Click **Rename**.

Deleting a Campus

To delete a campus, perform the following steps:

**Step 1**
In the Cisco DNA Spaces dashboard, choose **Location Hierarchy**.

The **Location Hierarchy** window appears with the location hierarchy.

**Step 2**
In the location hierarchy, click **More Actions** for the campus that you want to delete.

**Step 3**
Click **Delete campus**.

What to do next

<table>
<thead>
<tr>
<th>Note</th>
<th>To delete a campus, first you have to delete the locations under that campus, if any.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note</td>
<td>You cannot delete a campus that is associated with proximity rules.</td>
</tr>
</tbody>
</table>
Renaming a Building

To rename a building, perform the following steps:

**Step 1**
In the Cisco DNA Spaces dashboard, choose **Location Hierarchy**.

The **Location Hierarchy** window appears with the location hierarchy.

**Step 2**
In the location hierarchy, click **Location Hierarchy** for the building that you want to rename.

**Step 3**
Click **Rename <building name>**.

**Step 4**
In the **Rename -network** window that appears, enter the new name for the building.

**Step 5**
Click **Rename**.

Deleting a Building

To delete a building, perform the following steps:

**Step 1**
In the Cisco DNA Spaces dashboard, choose **Location Hierarchy**.

The **Location Hierarchy** window appears with the location hierarchy.

**Step 2**
In the location hierarchy, click **More Actions** for the building that you want to delete.

**Step 3**
Click **Delete building**.

What to do next

---

**Note**
To delete a building, first you have to delete the floor or zones under that building, if any.

**Note**
You cannot delete a building that is associated with a proximity rule.

Renaming a Floor

To rename a floor, perform the following steps:

**Step 1**
In the Cisco DNA Spaces dashboard, choose **Location Hierarchy**.

The **Location Hierarchy** window appears with the location hierarchy.

**Step 2**
In the location hierarchy, click **More Actions** for the floor that you want to rename.

**Step 3**
Click **Rename "floor name"**.

**Step 4**
In the **Rename-floor** window that appears, enter the new name for the floor.
Deleting a Floor

To delete a floor, perform the following steps:

Step 1 In the Cisco DNA Spaces dashboard, choose **Location Hierarchy**.

The **Location Hierarchy** window appears with the location hierarchy.

Step 2 In the location hierarchy, click **More Actions** for the floor that you want to delete.

Step 3 Click **Delete floor**.

---

What to do next

**Note**

If the floor that you delete has any zone under it, that zone is moved under the building after the deletion of the floor.

Adding a CMX Zone

Cisco DNA Spaces dashboard supports to import the CMX Zones added to **Cisco CMX** and **Map Service**. CMX Zones can be added under floors. CMX Zones will just have X,Y coordinates, and will not have any access points associated with them.

Ideally, Cisco DNA Spaces will automatically add, update, and delete the CMX Zones in the location hierarchy based on the changes made in Cisco CMX or Map Service. However, for the existing locations in Cisco DNA Spaces, if any CMX Zone was created in Map Services before this CMX Zone support, that CMX Zone will not be imported automatically during synchronization. You have to manually add it to the location hierarchy. Once added, all the updates done for this particular CMX Zone will be synchronized automatically.

**Note**

CMX Zone support is not applicable if the wireless network is Meraki.

To add a CMX Zone manually to the location hierarchy, perform the following steps:

Step 1 In the Cisco DNA Spaces dashboard, choose **Location Hierarchy**.

Step 2 In the **Location Hierarchy** window, click the **More Actions** icon for the floor under which you want to add the CMX Zone.

Step 3 Click **Add CMX Zone**.

Step 4 In the **Add CMX Zone** window that appears, select the CMX Zones that you want to add.

**Note** The CMX Zones added to Map Service or Cisco CMX are available for selection.

Step 5 Click **Add**.
The CMX Zone gets listed under the particular floor. Now all the updates done for this particular CMX Zone will be synchronized automatically.

**Note**  You can add a CMX Zone in Setup > Map service using the square icon (below the Expand Collapse icon) displayed in the map.

---

### Managing the Location Hierarchy for Cisco Wireless Controller or Cisco Catalyst 9800 Series Controller (with WLC Direct Connect or Cisco DNA Spaces Connector)

#### Adding Networks Automatically for a Primary Controller

If you have skipped to select the networks when importing the Cisco Wireless Controller, you can add the networks automatically at any time later.

To add network automatically for a Cisco Wireless Controller or Cisco Catalyst 9800 Series Wireless Controller, perform the following steps:

1. In the Cisco DNA Spaces dashboard, choose **Location Hierarchy**.
2. In the **Location Hierarchy** window, click the **More Actions** icon for the wireless controller for which you want to add networks.
3. Click **Edit**.
4. In the **Edit Controller** window that appears, select the **Auto Network Creation** check box.
5. Click **Done**.

The APs with similar prefix are grouped, and networks are formed automatically. The APs that are not added to the auto-created networks are listed under the network name “unconfigured”.

---

### What to do next

**Note**  Only the APs added to the wireless controller after configuring the auto network are grouped. Existing APs under the “unconfigured” network name will not be grouped automatically based on this configuration. However, if any new AP gets added to the wireless controller with the same prefix of an existing AP in the “unconfigured” network, then the existing AP gets grouped with the new AP added.

---

### Manually Adding Networks for a Primary Controller

To manually add network for a Cisco Wireless Controller or Cisco Catalyst 9800 Series Wireless Controller, perform the following steps:
Location Hierarchy in Cisco DNA Spaces

Adding APs of Multiple Prefixes to a Network

You can add APs of multiple prefixes to a network. For example, if you have APs with prefixes, AB, BC, and CA, and if you want to group the APs with AB and BC under one wireless network, you can do so.

To add APs of multiple prefixes to a network of a Cisco Wireless Controller or Cisco Catalyst 9800 Series Wireless Controller, perform the following steps:

**Step 1**  
In the Cisco DNA Spaces dashboard, click the three-line menu icon at the top-left of the window.

**Step 2**  
Choose **Location Hierarchy**.

**Step 3**  
In the **Location Hierarchy** window, click the network to which you want to add APs of multiple prefixes.

**Step 4**  
In the **Location Info** tab, click **Edit** for **Access Points Prefix Used**.

**Step 5**  
In the **Edit Prefix** window that appears, click **Edit** for **Prefix**. The APs with the prefix entered get listed.

**Step 6**  
Click **Add Prefix**. Now the newly added prefix gets listed under **Added Prefixes** in the right pane of the window. **Add Prefix** will be enabled only if there are APs with the Prefix entered.

**Step 7**  
Click **Save**. After adding the prefix, the APs under the **unconfigured** network with this prefix will be moved to this network. To delete a prefix, hover over that prefix under **Added Prefixes**, and click the **Delete** icon that appears.
The Access Points Prefix Used option will be available in the Location Info tab only for the network locations. However, the Access Points Prefix Used option will not be available for the Unconfigured network.

### Adding Additional Secondary Controller

If you have skipped to add a secondary controller when importing the Cisco Wireless Controller, you can add it any time later. Even if you have configured a secondary controller, you can add more than one secondary controllers.

To add a secondary controller for a Cisco Wireless Controller, perform the following steps:

**Step 1** In the Cisco DNA Spaces dashboard, choose Location Hierarchy.

**Step 2** In the Location Hierarchy window, click the More Actions icon for the Cisco Wireless Controller for which you want to add secondary controller.

**Step 3** Click Edit.

**Step 4** In the Edit Controller window that appears, click Add More for Additional Controllers.

**Step 5** In the Add additional controller window that appears, select the Cisco Wireless Controller that you want to configure as secondary controller.

**Note** The Cisco Wireless Controllers similar to the primary controller (having same APs) will be top in the list.

**Step 6** Click Add.

Now the newly configured Cisco Wireless Controller has become the secondary controller.

**Note** You can add more than one Cisco Wireless Controller as secondary controller. However, you can add only one at a time.

### Deleting a Secondary Controller

To delete a secondary controller, perform the following steps:

**Step 1** Click the three-line menu icon displayed at the top-left of the Cisco DNA Spaces dashboard.

**Step 2** Choose Location Hierarchy.

**Step 3** In the location hierarchy, click the More Actions icon for the Primary Controller of which you want to delete the secondary Cisco Wireless Controller.

**Step 4** Click Edit.

In the Edit Controller window that appears, the secondary controllers added for that PrimaryController will be listed under Additional Controllers.

**Step 5** Click the Delete icon for the secondary controller that you want to delete.

**Step 6** In the window that appears, confirm the deletion.
Now, the secondary controller is deleted.

What to do next

Note When you delete a secondary controller, the APs that are unique for this secondary controller (APs not in the primary controller or its other secondary controllers) also will be deleted.

Renaming the Primary Controller

To rename the primary controller, perform the following steps:

Step 1 In the Cisco DNA Spaces dashboard, choose Location Hierarchy.
Step 2 In the location hierarchy, click the More Actions icon for the Cisco Wireless Controller that you want to rename.
Step 3 Click Rename <cisco wireless controller>.
Step 4 In the Rename WLC window that appears, enter the name required, and click Rename.

Now the name of the Cisco Wireless Controller is changed to the new name specified.

Note The name change is not reflected in the Cisco Wireless Controller.

Displaying Cumulative Count in Location Hierarchy

In the location hierarchy, the count of APs, Proximity Rules, and child locations for the locations will be shown as cumulative. The count for a location will be the total of its count and the count of all its child locations. For example, the total count of APs for a floor will be the sum total of APs for the floor and the APs for each zone under that floor.

The locations with zero count will not have a link to view the details. You can view the APs, Proximity Rules, Locations, and Users of a location by clicking that location. You can view the details of a location parameter only from the associated location.

For the proximity rules, only the unique rules are counted. For example, if two zones of a floor are included in an engagement rule, when counting the rule for the floor, that engagement rule will be counted only once.
CHAPTER 4

Behavior Metrics

This chapter describes the Behavior Metrics reports.

• Overview of Behavior Metrics, on page 49
• Viewing the Behavior Metrics Report, on page 49

Overview of Behavior Metrics

The Behavior Metrics app enables you to view various reports that provide insights about the performance of your business. By default, the report includes the data for the previous month. You can filter to view the report for a particular location and month. You can also filter the report based on tags.

After installation of Cisco Digital Network Architecture (DNA) Spaces, it will take a month to show the initial report. You can view the sample report during this period. You can also see the how your report is building up by switching to the “My Data” option during this period. After the report is ready, you will get a notification.

The Behavior Metrics app provides the following type of reports:

• Behavior Metrics (Business Metrics), on page 52

Viewing the Behavior Metrics Report

To view the various reports the Behavior Metrics app provides, perform the following steps:

Step 1 In the Cisco DNA Spaces dashboard, click Behavior Metrics.
The Behavior Metrics report is displayed.
**Step 2** Specify the location, tag, and month for which you want to view the report in the corresponding drop-down list at the top of the page.

---

**What to do next**

- By default, the report is displayed for the entire organization. If you do not have access at the organization level, the report is shown for the top-level location to which you have access. You can filter the locations up to the network level.

- The percentage or count described in the report for a filtered location will be total or average of all its child locations. For example, if the filtered location is a network, the number of visits shown for the network will be total of the number of visits for all the floors in that network.

- If the customer is having retail business, the title **Retail** appears along with **Behavior Metrics** at the top of the **Behavior Metrics** window. For the **Workspaces** vertical, the title **Workspaces** appears along with **Behavior Metrics**. For other businesses, it will be **Generic**.

---

**Benchmarks**

**Organization Benchmark**: Displays the average value for the entire organization. For example, if the organization is Cisco, the Organization Benchmark for “Average Visit Duration” shows the “average visit duration” for Cisco.
**Industry Benchmark**: Displays the average value for the industry to which your business belongs. For example, if you are in retail sector, in the Visit Duration Distribution graph, the average visit duration for retail is displayed. The industry benchmark average value is restricted to the data obtained from other clients who have installed Cisco DNA Spaces.

**Country Benchmark**: Displays the average value for the locations tagged under the particular country. For example, if you choose US as tag, in the Average Visit Duration graph, a bar corresponding to US is displayed which is the average visit duration for all the locations tagged under US. The total number of locations associated with the country tag is also displayed. If the locations under the particular country tag is associated with any other tag, in certain graphs such as Average Visit Duration, the average value for that tag is also shown.

**State Benchmark**: Displays the average value for the locations tagged under that particular state. If you select a state tag, in certain reports two additional bars appear in the graph. One displays the average value with the state name, and the other bar displays the same average value with total number of locations in the state. For example, Average Visit Duration graph.

**Brand Benchmark**: Displays the average value for the brand name. A brand name can be used as metadata only for the locations of a particular state. If you choose a brand, in certain graphs such as Average Visit Duration, the average value for the state to which the brand is tagged is also displayed.

**Filtered Location Benchmark**: Displays the average value for the filtered location. It appears only if you filter a particular location. For example, if “Cisco San Fransisco” is filtered in the location hierarchy, the “Average Visit Duration” for Cisco San Fransisco is shown along with the organization average. The total number of locations under the filtered location is also displayed.

**Top and Bottom 3 locations**: Displays the top tree and bottom three child locations.

**Important Locations**: Displays the child locations that are top in overall ranking for various parameters such as intent rate, acquisition rate, visit distribution, visit frequency, and so on. The top five important locations will be shown in the graphs.

---

**Note**

- The country, state, and brand benchmarks are displayed based on the data for the particular customer.
- When you filter the report for a brand, do not filter a state name that is not associated with it.
- Do not filter the report for two brands simultaneously.
- By default, the report is shown for top and bottom three locations. You can view the report for the important locations by clicking the toggle switch at the top right of the page.
- You can tag the locations under country, state, and brand benchmarks by defining metadata for the locations.

---

**Report Tabs**

The Behavior Metrics report has the following tabs:

**Group Tab**

By default the report is shown for Group View, and displays the report for the entire organization.
Historical Tab
Displays the report that shows the average values for the last twelve months. In most of the reports, average of the last twelve months is shown along with the average for each month. The industry and organization average are also shown based on the report. You can access the Historical view, by clicking the Toggle Historical View button at the far right of the Behavior Metrics window.

Comparative Tab
When you filter a location, the Comparative tab appears, and the report is displayed for that particular location along with the organization benchmark.

Behavior Metrics (Business Metrics)
Performance Benchmarking: Performance on Core Metrics related to Peers

Note
The Behaviour Metrics report for the Workspaces vertical will be different from the following one. For information on the Behaviour Metrics report for the Workspaces vertical, see Workspaces Vertical (Behavior Metrics), on page 55

Visit Duration
Visit Duration: Across Locations
Displays a line graph with the average visit duration for all your business locations. This report enables you to identify the time visitors are spending on various locations. The average visit duration for the industry and organization are also displayed in the graph.

Visit Duration: Key Locations
Displays a bar graph that represents the average duration of visits in key locations. The top and bottom 3 locations or important locations are shown in this report along with the industry and organization benchmark. If you are filtering a location, the average value for the filtered location is also shown in the report.

Visit Duration: By Sub-brand
Displays a bar graph that shows the average visit duration for various brands in your business. The industry and organization benchmarks are also displayed in the graph.

Visit Duration: Distribution
Displays a bar graph that displays the total number of visits for various Visit Duration ranges. Organization and industry average are shown in the report.

Visit Frequency
Visit Frequency represents the “number of visits made by the visitors” by “number of visitors”.

Visit Frequency: Across Locations
Displays a line graph with average visit frequency for all your business locations. This report enables you to identify how often the visitors are visiting your locations. The average visit frequency for the industry and organization are also displayed in the graph.

**Visit Frequency: Key Locations**
Displays a bar graph that represents the average visit frequency in key locations. The top and bottom 3 locations in visit frequency or important locations with highest visit frequency are shown in this report along with the industry and organization benchmarks. If you are filtering a location, the average value for the filtered location is also shown in the report.

**Visit Frequency: By Sub-brand**
Displays a bar graph that shows the average visit frequency for various brands in your business. This report enables you to identify which brand is more often visited. The industry and organization benchmarks are also displayed in the graph.

**Visit Frequency: Distribution**
Displays a bar graph that displays the total number of visits for various Visit Frequency ranges. Organization and industry average are shown in the report.

**Diagnostics: Factors that Impact or are impacted by the Core Metrics**

**Visit Duration by Visit Number**
Displays a bar graph that shows the time the visitors spent in the locations for various number of visits. This report helps you to identify the change that happens to the visit duration based on the visit count.

Each bar represents the average visit duration of the visitors for various visit numbers. For example, the bar for 7 represents the average visit duration of the visitors who has visited the locations 7 times during the specified month.

**Repeat Visitors: Across Locations**
Displays a line graph that shows the percentage of repeat visitors for all the locations. The organization and industry benchmarks for repeat visitors are also shown in the report.

**Repeat Visitors: Key Locations**
Displays a bar graph that shows the repeat visitor percentage for key locations. The top and bottom 3 locations in repeat visitors or important locations with highest repeat visitors are shown in this report along with the industry and organization benchmarks for repeat visitors. If you are filtering a location, the average value for the filtered location is also shown in the report.

**Visit Recency: Across Locations**
This report displays a line graph that shows the gap between the visits of the repeat visitors for various locations. The visit recency is shown in number of days. The industry and organization benchmark for the visit recency are also shown in the report.

**Visit Recency: Key Locations**
This report displays a bar graph that shows the gap in number days between the visits of the repeat visitors for key locations. The top and bottom 3 locations in visit recency or important locations are shown in this report along with the industry and organization benchmarks.

**Repeat Visitors: By Sub-brand**
Displays a bar graph that shows the percentage of repeat visitors for various brands in your business. This report enables you to identify the location with which brand is repeatedly visited the most. The industry and organization benchmarks for repeat visitors are also displayed in the graph.

**Visit Recency- By Sub-Brand**

Displays a bar graph that shows the visit recency (gap in days between the two visits of a repeat visitor) for various brands in your business. The industry and organization benchmarks for visit recency are also displayed in the graph.

**Visit Distribution: Hour of the Day**

Displays a bar graph that represents the daily visits in the organization (average of all the location of the organization) during various hours of a day. This report enables you to identify at what hour of the day there are more visits in the locations.

Each bar in the graph represents “the percentage of visits that occurs at that particular hour of the day” among “the total daily visits”. For example, the bar for 2 pm represents the percentage of visits that occurs at 2 pm among the average total daily visits.

**Visit Distribution: Day of the Week**

Displays a bar graph that represents the average daily visits in the organization during various days of a week. This report enables you to identify on which day of the week there are more visits.

Each bar in the graph represents “the percentage of visits that occurs at that particular day of the week” among “the average total weekly visits”. For example, the bar for “THU” represents the “percentage of visits that occurs on Thursdays” among “the total number of weekly visits”.

**Size of the Store and Visit Duration**

Displays a graph that shows the visit duration based on the square foot area of the locations. This report enables you to identify the influence the size of a location has on the time spent by visitors in the location.

The blue dot denotes the three child locations that have highest visit duration and the three child locations that have the lowest visit duration. The grey dot in the graph represents other child locations. Each dot represents the total square foot area of that particular child location and its average visit duration.

**Size of the Store and No. of Visits**

Displays a graph that shows the number of visits based on the square foot area of the locations. This report enables you to identify the influence the size of a location has on the repeat visits in the location.

The blue dot denotes the three child locations that have highest number of visits and the three child locations that have the lowest number of visits. The grey dot in the graph represents other child locations. Each dot represents the total square foot area of that particular child location and its average number of visits.

**Retail Experience Grid**

Displays a graph that provides a consolidated report of the visit duration and visit frequency for the entire month from all the locations. The graph will be displayed only for root locations and group locations. The visit duration will be displayed in the X-axis and the visit frequency will be displayed in the Y-axis. **Retail Experience Grid** will be available only for the Retail vertical.
Workspaces Vertical (Behavior Metrics)

Core Metrics: How do individual workspace locations perform along key metric

The Behavior Metrics window for Workspaces vertical will have the following information:

**Workday Duration**

- **Workday Duration: Across Locations**: The average number of hours the employees spent in the workspace are shown in this report. The average work duration for all your business locations under the filtered location are shown in this report.

- **Workday Duration: Key Locations**: The average work duration for key business locations under the filtered location are shown in this report. The average work duration for top and bottom three locations are displayed along with industry and organization average.

**Employee Frequency**

- **Employee Frequency: Across Locations**: The average frequency at which the employees visited the workspaces are shown in this report. The average visit frequency for all your business locations under the filtered location are shown in this report.

- **Employee Frequency: Key Locations**: The average visit frequency of employees in key locations under the filtered location are shown in this report. The average visit frequency for top and bottom three locations are displayed along with industry and organization average.

**Workspace Density**

- **Workspace Density: Across Locations**: The average density (employees in a squarefoot of workspace) of employees in the workspaces are shown in this report. The average workspace density for all your business locations under the filtered location are shown in this report.

- **Workspace Density: Key Locations**: The average workspace density at key locations under the filtered location are shown in this report. The average workspace density for top and bottom three locations are displayed along with industry and organization average.

**Occupancy Rate**

- **Occupancy Rate: Across Locations**: The average percentage of actual man hours the employees spent at the workspaces out of the prescribed average man hours are shown in this report. The average occupancy rate for all your business locations under the filtered location are shown in this report.

- **Occupancy Rate: Key Locations**: The average occupancy rate at key locations under the filtered location are shown in this report. The average occupancy rate for top and bottom three locations are displayed along with industry and organization average.

Diagnostics: Analysis of factors that impact or are impacted by the core metrics

**Entry Time**

- **Entry Time: Across Locations**: The average time at which employees enter the workspaces are shown in this report. The average entry time for all your business locations under the filtered location are shown in this report.
• **Entry Time: Key Locations**: The average entry time at key locations under the filtered location are shown in this report. The average entry time for top and bottom three locations are displayed along with industry and organization average.

**Exit Time**

• **Exit Time: Across Locations**: The average time at which employees exit the workspaces are shown in this report. The average exit time for all your business locations under the filtered location are shown in this report.

• **Exit Time: Key Locations**: The average exit time at key locations under the filtered location are shown in this report. The average exit time for top and bottom three locations are displayed along with industry and organization average.

**Entry Time Distribution**

Displays the percentage of employees that has entered the locations at various hours of a day along with the industry and organization average percentage for each hour of the day.

**Exit Time Distribution**

Displays the percentage of employees that has exited the locations at various hours of a day along with the industry and organization average percentage for each hour of the day.

**Employee Presence: Hour of Day**

Displays the percentage of employees that were present at the workspaces at various hours of a day along with the industry and organization average percentage for each hour of the day.

**Visitor Presence: Hour of Day**

Displays the percentage of visitors that were present at the workspaces at various hours of a day along with the industry and organization average percentage for each hour of the day.

**Employee Presence: Day of the Week**

Displays the percentage of employees that were present at the workspaces at various days of a week along with the industry and organization average percentage for each day of the week.

**Visitor Presence: Day of the week**

Displays the percentage of visitors that were present at the workspaces at various days of a week along with the industry and organization average percentage for various days of a week.

**Workspace Presence: Across Locations**

• **Workspace Presence: Across Locations**: The average time employees spent within the workspace as a percentage of prescribed work duration is shown in this report. The average workspace presence for all your business locations under the filtered location are shown in this report.

• **Workspace Presence: Key Locations**: The average workspace presence at key locations under the filtered location are shown in this report. The average workspace presence for top and bottom three locations are displayed along with industrial and organization average.

**Visitor Index**

• **Visit Index: Across Locations**: The average number of visitors who have visited the workspace as percentage of the employees of that workspace is shown in the report. The average visit index for all your business locations under the filtered location are shown in this report.
• **Visit Index : Key Locations:** The average visit index at key locations under the filtered location are shown in this report. The average visit index for top and bottom three locations are displayed along with industrial and organization average.

### Pin a Location

If you want to add certain locations as favorites, you can pin those locations. You can pin maximum three locations at a time. If you have added pin locations, all the graphs by default will show the value for the pinned locations. In bar charts there will be a bar for each pin location.

To pin a location, perform the following steps:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In the <strong>Behavior Metrics</strong> window, click the <strong>Pin Locations</strong> button at the far right of the window.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>In the <strong>Pin Locations</strong> window you can select the locations that you want to pin.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click <strong>Apply</strong>.</td>
</tr>
</tbody>
</table>
Location Analytics Report

This chapter describes the Location Analytics Report.

- Overview, on page 59
- Viewing Location Analytics Report, on page 59
- Location Analytics Report, on page 61
- Creating Custom Reports, on page 62

Overview

The Location Analytics app enables you to view reports of visits in your locations. The visits of your employees are also counted in the report.

Viewing Location Analytics Report

To view the location analytics report, perform the following steps:

Step 1  In the Cisco DNA Spaces dashboard, choose Home.
Step 2  In the window that appears, click Location Analytics.

The Location Analytics report appears.

By default, the report is shown for the root location from January 01, 2019 till todate. You can filter the report by location, date, and SSID. Report is not shown if there is no data.

Step 3  From the Filter by Location drop-down list, choose the parent location for which you want to view the report.

Note  For ACT and EXTEND licenses, you can view the report for floors and zones. However for the SEE licenses, you can filter only network locations.

Step 4  From the Filter by date drop-down list, choose the date range for which you want to view the report.

In the Choose date range window, you can specify an available time period or you can specify a custom date range by specifying the start date and end date. Click Apply.

The following periods will be available for selection by default:

- Today: The report displays the total number of visits on each hour of the particular day.
• **Yesterday**: The report displays the total number of visits on each hour of the previous day.

• **Current Week**: The report displays the total number of visits on each day of the current week.

• **Previous Week**: The report displays the total number of visits on each day of the previous week.

• **Current Month**: The report displays the total number of visits on each day of the current month.

• **Previous Month**: The report displays the total number of visits on each day of the previous month.

• **Last 15 days**: The report displays the total number of visits on each day of the previous 15 days.

• **Last 30 days**: The report displays the total number of visits on each day of the previous 30 days.

• **Last 3 Months**: The report displays the total number of visits on each day of previous 3 months.

• **Last 6 Months**: The report displays the total number of visits on each day of previous 6 months.

• **Custom**: The report displays the total number of visits on each day of the time range specified.

To view the visit details for a particular day, hover over that day on the graph.

**Step 5**

From the **Filter by SSID** drop-down list, choose the SSID for which you want to view the report.

The following SSID options will be available for selection:

• **All SSIDs**: Displays the visit data in the filtered locations for the specified period captured using the SSIDs in those locations.

• **Without SSIDs**: Displays the visit data in the filtered locations for the specified period that are not captured through SSIDs. For example, the visitors who have visited a filtered location, but not connected to any of the SSIDs in the filtered location during the time period specified. For example, the visit data captured from location updates. However, the visits of those visitors who have connected at least once to any of the SSIDs previously only will be counted.

• **Custom SSID configured in Cisco DNA Spaces**: Displays the visit data in the filtered locations for the specified period captured using the particular SSID.

**Note**

The report gets displayed for the filters applied. You can apply the filters only if you are an **ACT** license user. The **SEE** license users cannot use the SSID filter. However, they can use the date range filter, and filter the locations except the network, floor and zone locations.
You can view the following information in the Location Analytics report:

- **Visitors**: Displays total number of unique visitors in the filtered location during the period specified. The count for New Unique Visitors and Repeat Unique Visitors are shown separately along with their percentage. Also a graph is shown that displays the unique visitor count for each day of the specified period.
  - **New Visitors**: Total number of unique visitors who visit the filtered location for the first time.
  - **Repeat Visitors**: Total number of unique visitors who have visited the filtered location more than once.

- **Visits**: Displays total number of visits in the filtered location during the period specified. The count for New Visits and Repeat Visits are shown separately along with their percentage. Also a graph is shown that displays the visit count for each day of the specified period.
  - **New Visits**: Total number of unique first time visit in the filtered location.
  - **Repeat Visits**: Total number of unique visits that occurred more than once in the filtered location.

- **Dwell Time**: Displays the average dwell time for the visits occurred in the filtered location during the period specified. The average dwell time for New Visits and Repeat Visits are shown separately along with their percentage. A graph that displays the average dwell time of visits on each day is also shown.

- **Dwell Time Breakdown**: Displays the total number of visits for various dwell time ranges for the filtered location and period. For example, the count for 0-5 min represents the total number of visits of the duration 0 to 5 minutes in the filtered locations.
You can create custom reports with widgets with different filters.

Creating Custom Reports

In addition to the default report displayed for location analytics, you can create custom reports by applying widget filters. Each custom report can have multiple widgets. You can create widgets with different combinations of report types, locations, time period, SSIDs, visit ranges, and View By options. You can add more than one widget with same report type in a custom report.

To create a custom report, perform the following steps:

**Step 1**
In the Cisco DNA Spaces dashboard, choose **Home**.

**Step 2**
In the window that appears, click **Location Analytics**.

**Step 3**
Click the three-parallel line icon displayed at the top-left of the window.

**Step 4**
In the window that appears, click **My Reports**.

**Step 5**
Click **Create New Report**.

**Step 6**
In the **Create New Report** window that appears, enter a name and description for the report.

**Step 7**
Click **Create**.

**Step 8**
Click **Add New Widget**.

**Step 9**
In the **Add a Widget** wizard, do the following:

a) In the **Name of the widget** field, enter a name for the widget.

b) Click the type of report that needs to be added in the custom report.

   The report types available for selection will be the ones available for default report.

   You can select only one report type for a widget.

c) Click **Next**.

d) In the **Choose Locations** window, check the locations for which you want to view the report.

   **Note**
   • If you are selecting the report types as "Visitors", you can choose only one location. For other report types, you can filter more than one location.
   • You can choose only upto network locations for filtering. You cannot choose floors and zones for filtering.

e) Click **Next**.

f) In the **Filter by** window, specify the time period for which you want to view the report by specifying the values in **From** and **To** fields.

**g) From the SSID drop-down list, choose the SSID for which you want to view the report.**

The following SSID options will be available for selection:

• **All SSIDs**: Displays the visit data in the filtered locations for the specified period captured using the SSIDs in those locations.

• **Without SSIDs**: Displays the visit data in the filtered locations for the specified period that are not captured through SSIDs. For example, the visitors who have visited a filtered location, but not connected to any of the SSIDs in the filtered location during the time period specified. However, the visits of those visitors who have connected atleast once to any of the SSIDs previously only will be counted.
Custom SSID configured in Cisco DNA Spaces: Displays the visit data in the filtered locations for the specified period captured using the particular SSID.

Note: You can apply the filters only if you are an ACT license user. The SEE license users cannot use the SSID filter. However, they can use the date range filter, and filter the locations except the network, floor and zone locations.

h) From the Visit Range drop-down list, choose the time for which you want to view the report. For example, if you choose Mid Night, the report shows the details of visits happened at mid night on the selected locations during the specified period.

The following options will be available for selection:

- All Day: The visits happened during the entire day (12 am to 11:59 pm) will be included in the report.
- Mid Night: Only the visits during mid night (12 am to 2:59 am) will be included in the report.
- Early Morning: Only the visits during early morning (3 am to 4:59 am) will be included in the report.
- Morning: Only the visits during morning (5 am to 8:59 am) will be included in the report.
- Business Hours: Only the visits during business hours (9 am to 4:59 pm) will be included in the report.
- Evening: Only the visits during evening (5 pm to 8:59 pm) will be included in the report.
- Late Evening: Only the visits during late evening (9 pm to 11:59 pm) will be included in the report.
- AM: Only the visits during early morning (12 am to 11:59 am) will be included in the report.
- PM: Only the visits during late evening (12 pm to 11:59 pm) will be included in the report.

i) From the View By drop-down list, choose the order in which data must be displayed in the report.

- by day: The report displays the visit data for each day of the specified period.
- by Hour of Day: The report displays the visit data for each hour of the day. The visit count for a particular hour will be total visits occurred during the specified period at that particular hour. For example, in the "by hour of day" report for November 2019, the visit count displayed at 2 pm will be the total of number of visits occurred between 2.00 pm and 2:59 pm during the entire month of November 2019.
- by Week: The report displays the visit data for each week in the specified period.
- by Day of Week: The report displays the visit data for each week in the specified period with visit count for each day on that particular week.
- by Month: The report displays the visit data for each month in the specified period.

j) Click Add.

The new widget gets added to the custom report.

Step 10: Similarly, you can add multiple widgets to a custom report using the Add New Widget icon.

The custom report created gets listed in the My Reports window.
Note  ACT (Advanced) subscription customers are allowed to apply all filters (Location, SSID, Time Ranges, and Visit Range) in the widgets. SEE (Base) subscription customers are restricted to apply SSID and Visit Ranges filters, and cannot filter network locations.
Impact Analysis

This chapter describes how to work with the Impact Analysis app.

• Impact Analysis Overview, on page 65
• Adding an Impact Campaign(Event), on page 66
• Viewing an Impact Analysis Report, on page 67

Impact Analysis Overview

Impact Analysis is a way of measuring the effect of any action you made based on before and after analytics. The Impact Analysis app enables you to do impact analysis. For example, assume that you have provided a discount offer to all the visitors visiting in your location A on November 2019. Now you can measure the impact of this discount offer by comparing the metrics during the offer period with the metrics of the last 365 days.

This app will be available for SEE, ACT, and Extend license types.

You can create an event with a particular time period, and can do any of the following:

• Compare the metrics for the event period with the metrics of Daily Average during Past 365 days (Period During EVENT).

• Compare the metrics for same duration before and after the specified event period. (Period AFTER Event)

You can compare the following metrics:

• Visit duration

• Visit Count
Adding an Impact Campaign (Event)

**Note**
- You cannot add, edit or modify a campaign, if you are new Cisco DNA Spaces customer and there is no data for your Cisco DNA Spaces account.
- If you are having only read-only access to a Cisco DNA Spaces account, you can view the Impact Analysis reports for the existing campaigns for that account, but you cannot add, modify, or delete a campaign.

To add an Impact Campaign (Event), perform the following steps:

**Step 1**
In the Cisco DNA Spaces dashboard, choose Impact Analysis.

**Step 2**
In the Impact Analysis window that appears, click Add Impact Campaign.

The Add Impact Campaign window appears.

**Step 3**
In the Event Name field, enter a name for the event.

**Step 4**
From the Business Location drop-down list, choose the location for which the event is created.

You can choose only network locations.

**Step 5**
In the Choose the event period that you like to measure area (Compared To drop-down list in the Edit window), choose the event period.

The following options will be available:

- **Period DURING Event**: This option enables you to compare "the data for the event period specified" with "the data for daily average of last 365 days". For example, if you are selecting the event period as December 10, 2019 to December 20, 2019, the graph in the Impact Analysis report displays 2 bar charts, one with "data for December 10, 2019 to December 20, 2019" and the other with "daily average data for December 21, 2018 to December 20, 2019".

- **Period AFTER Event**: This option enables you to compare "the data for the same duration before the date range specified" with "the data for the the same duration after the date range specified". For example, if you are specifying the event duration as "January 01, 2020 to January 10, 2020" (10 days), the graph in the Impact Analysis report displays 2 bar charts, one with the "data for the time period December 22, 2019 to December 31, 2019 (10 days)" and other with the "data for the time period January 10, 2020 to January 19, 2020 (10 Days)".

**Note**
The graphs for Visit Duration and Visit Count are shown separately. In the Visit Duration graph, the difference in visit duration between two bar charts are displayed in minutes. In the Visit Count graph, the difference in visit count between two bars are displayed in percentage.

**Step 6**
In the EVENT DURATION area, specify the start date and end date for the event in the From and To fields respectively.

**Step 7**
Click See Impact.

Now the campaign is added.

- To edit a campaign, from the campaigns listed in the Impact Analysis window, click the campaign that you want to edit. Click Edit Campaign at the top-right of the window, and make necessary changes. Click Update to save the changes.
• To delete a campaign, from the campaigns listed in the Impact Analysis window, click the campaign that you want to delete. Click Delete displayed at the top-right of the window. In the Delete Impact Campaign window, click Delete to confirm the deletion. To delete multiple campaigns (events) at a time, in the Impact Analysis window, check the check boxes corresponding to the campaigns that you want delete, and click Delete that appears at the bottom of the window.

---

### Viewing an Impact Analysis Report

To view an Impact Analysis report, perform the following steps:

**Step 1**  
In the Cisco DNA Spaces dashboard, choose Impact Analysis.  
The Impact Analysis window appears. All the campaigns created will be listed in the window.

**Step 2**  
Click the campaign/event for which you want to view the report.  
The Impact Analysis report for the selected campaign is displayed. The report will have the following charts:

- **Impact on Visit Duration**: Displays a bar chart with the average visit duration for the event, and the average visit duration for the selected time window, in minutes.

- **Impact on Visit Count**: Displays a bar chart with the average visit count for the event and the average visit count for the selected time window, in percentage.

**Note**  
Report will be not be displayed if you have created the event with a future time period.
Right Now

This chapter describes about the Right Now app.

- Right Now Overview, on page 69

Right Now Overview

The Right Now app provides you the Right Now report that shows the details of visitors currently present at your locations. Using the Right Now app, you can also create Density Rules through which you can send notifications to the business users such as employees based on the visitor density or device count in the business locations.

Right Now Report

The Right Now report displays the details of the visitors currently present at your locations.

By default, the report shows the details of visitors currently present at all the locations. You can filter upto floor level.

This app will be available for SEE, ACT, and Extend license types.

Note

- The report for last 10 minute active users has a passive duration of 10 minutes. So, a visitor will be shown as active user until the passive duration crosses for that visitor. For example, if a visitor in a location is moving from 1st floor to 2nd floor, the visitor will be shown in both 1st and 2nd floor. For 1st floor, the visitor count will be updated only after the passive duration is met.

- If a location is removed or modified from the location hierarchy, the location name and count are not updated in the Right Now report.

Viewing the Right Now Report

To view the Right Now report, perform the following steps:

Step 1 In the Cisco DNA Spaces dashboard, choose Right Now.
The **Right Now** window appears.

**Step 2**

From the **Location** drop-down list, choose the network location for which you want to view the report.

The Right Now report for the selected network location is displayed.
The local time of your system is displayed under the **Right Now** section at the top of the report.

The report will have the following charts:

- **Visitors seen during the last 10 minutes:** All locations: Displays the total number of visitors in the filtered location including its child location during the last 10 minutes.
- **Visitors seen during the last 10 minutes:** All Locations: Displays the total number of visitors during last 10 minutes for each location separately. If the number of locations is more than 15, only the visitors count of top three and bottom three locations will be shown.
- **Cumulative Visitors:** All Locations: Displays the total number of visitors for each hour of the day in a cumulative manner.
- **First Time and Repeat Visitors:** Displays the percentage of new and repeat visitors among the active visitors.
- **Guests and Employees:** Displays the percentage of guests and employees among the active visitors.
- **Visitors:** By Location: Displays location-wise count of active visitors in the child locations of the filtered location.
  - Map View: The child locations of the filtered location are shown in the world map along with the total number of visitors in each of those child locations.
  - List View: The child locations of the filtered location are listed, and the number of current visitors for each location is shown against that location.

**Note**
- An "active visitor" can be any visitor who is present at the location during the last 10 minutes with connected to the network (WLAN/SSID) or a visitor who is present at the location during the last 10 minutes without connected to the network, but has connected on any of the previous visit.
- Average value for the last 51 weeks is shown as historical data for each chart in the report.

### Right Now on Camera

The Right Now on Camera option shows the Right Now report for your locations based on the data captured by the Meraki Cameras installed in your locations. This report will be available only if you have configured Meraki Camera for Cisco DNA Spaces using the **Camera** option in Setup. For more information on configuring Meraki Camera, see Setting up Cisco DNA Spaces to Work with Cisco Meraki Camera, on page 255.

### Viewing Right Now Report for Meraki Camera

To view the Right Now report for Meraki Camera, perform the following steps:

**Step 1**
In the Cisco DNA Spaces dashboard, choose **Right Now**.

The **Right Now** window appears.

**Step 2**
Click the three-line menu icon displayed at the top-left of the window, and choose **Right Now on Camera**.

The **Right Now on Camera** window appears with the Right Now report for Meraki Camera.
Figure 7: Right Now on Camera Report
Step 3

If required, from the **Location** drop-down list, choose the location for which you want to view the report.

**Note**  
By default, the report will be show for the root location.

The report will be having the following details:

- Your local time will be displayed at the top of the window, and the data in the report will be shown for this time.

- **# of people present**: Displays a bar graph that shows the total number of people currently present at the selected location and its child locations. The average number of people that were present at this time during the last 51 weeks at the selected location and its child locations is shown as Historical Average. The total number of people currently present will "Total number of people entered during the last 15 minutes through the tripwire entry for the cameras in the location" - "Total number of people exited during the last 15 minutes through the tripwire exit for the cameras in the location"

- **# of people present: Key Locations**: Displays a bar graph that shows the total number of people currently present at each of the child locations. If the total number of locations are more than or equal to 15, it will display the count for top and bottom three locations. In such cases, you can pin upto three locations to view the current presence count for the locations of your choice. This graph will appear only for the locations other than Network, Floor and Zone. The total number of people currently present will "Total number of people entered during the last 15 minutes through the tripwire entry for the cameras in the child locations" - "Total number of people exited during the last 15 minutes through the tripwire exit for the cameras in the child locations".

  **Note**  
The option to pin location will be available only if the number of locations are more than or equal to 15.

- **# of the people present: Key Cameras**: Displays a bar graph that shows the total number of people currently present for each Camera in the filtered location. If the total number of Cameras are more than Six, it will display the count for top and bottom three Cameras. In such cases, you can pin upto three cameras to view the current presence count for the cameras of your choice. This graph will appear only for network, floor and zone level locations.

  **Note**  
The option to pin cameras will be available only if the number of Cameras are more than Six.

- **# of the people present: Key Cameras Zones**: Displays a bar graph that shows the total number of people currently present for each camera zones defined for the cameras in the filtered location. If the total number of Camera Zones are more than Six, it will display the count for top and bottom three Camera Zones. In such cases, you can pin upto three camera zones to view the current presence count for the camera zones of your choice. This graph will appear only for network, floor and zone level locations.

  **Note**  
The option to pin camera zones will be available only if the number of Camera Zones are more than Six.

- **Cumulative Footfall during the day**: Displays a line graph that shows the total footfall during each hour of the day on which the Right Now report is viewed, in a cumulative manner. For example, the total number of footfall at 3 am will be total number of footfall that occurred from 00 am to 3 am.

  **Note**  
The graph is shown based on the time zone of the Network, Floor and Zone level locations. For example, if the root location XYZ has network locations in California, Tokyo and Bangalore, the report will display the data for these networks based on their current time. When it is 8.am at India, Japan will be at 11.30 am on the same day and California will still be on previous day 7.30 pm. So if your are viewing the **Right Now on Camera** report at 8.am IST, two graphs will be shown in the **Cumulative Footfall during the day** section. One with cumulative footfall count for Bangalore at 8.am and Tokyo at 11.30 am (as both are on same day), and another graph with cumulative footfall count for California at 7.30 pm on 19/07/2020.

- **Presence: By Location**: The location selected for the report, and its child locations are displayed in the Global Map, along with the count of visitors currently present at these locations in the **Map View**. You can also know the present visitor count as a hierarchy using the **List View**.
The # of the people present: Key Cameras Zones chart will be based on the people on camera's vicinity, and all the remaining charts will be based on entry and exit of people through tripwire line drawn for the cameras.

For information on pinning a location, camera, or camera zone, see Pinning a Location, Camera, or Camera Zone, on page 74.

---

**What to do next**

You can go back to the Right Now report using the Right Now on WiFi option in the three-line menu that appears at the top-left of the window.

---

### Pinning a Location, Camera, or Camera Zone

To pin a location, camera, or camera zone, perform the following steps:

---

**Step 1**

In the Right Now on Camera window, click the Pin icon displayed at the top right of the window.

The Pin window appears.

**Step 2**

Do the following based on your requirement:

- To pin a location, in the Pin Location area, select the check box for the locations that you want to pin, and click Apply. The locations selected will be displayed in the Pinned Locations area. You can pin a maximum of 3 locations.

- To pin a camera, in the Pin Cameras area, click the Cameras tab, and select the check box for the cameras that you want to pin, and click Apply. The cameras selected will be displayed in the Pinned Cameras area. You can pin a maximum of 3 cameras.

- To pin a camera zone, in the Pin Cameras area, click the Camera Zones tab, and select the check box for the camera zones that you want to pin, and click Apply. The camera zones selected will be displayed in the Pinned Camera Zones area. You can pin a maximum of 3 camera zones.

**Note**

You can search for a particular location, camera, or camera zone using the Search option displayed in the respective area.

---

### Density Rules

**Density Rule** enables you to track the density of unique devices or visitors in your business locations. This option is available only for the ACT license.

The Density Rule option allows you to create rules that triggers notifications to the business users such as building administrators based on the density of visitors, count of unique devices, or occupancy in the business locations. You can configure to send notifications through SMS, e-mail, Cisco Webex Teams, or using Trigger API.

This rule can be used to monitor the visitors in your locations to maintain the COVID 19 protocols, and can also be used to measure the impact of COVID 19 in your locations.
To create a Density Rule, perform the following steps:

**Step 1**
In the Cisco DNA Spaces dashboard, choose **Right Now**.
The **Right Now** window appears.

**Step 2**
Click the three-line menu icon displayed at the top-left of the window, and choose **Density Rules**.

**Step 3**
In the **Density Rule** window that appears, click **Create New Rule** displayed at the top-right of the window.
The **Create Density Rule** window is displayed.

**Step 4**
In the **Rule Name** field, enter a name for the Density Rule.

**Step 5**
In the **Sense** area, choose the required filter criteria from the **When a user is connect to WiFi and** drop-down list:

- **density**: Choose this option if you want to send the notifications based on the visitors density in a particular area. You can configure the area in square feet or square meter. If you choose this option, do the following configurations.
  - Set the density limit using the adjacent drop-down lists. You can configure the density limit as "more than" or "less than" a particular value, or as a value range using "between". You can choose "more than", "less than" or "between" from the first drop-down list, and manually enter the "value" or can choose the "value" from the drop-down list in the second field.
  - In the **per** field, specify the area of which the density limit is to be considered by manually entering the value or using the drop-down list. Then, from the adjacent drop-down list, choose the measurement scale. You can specify the measurement in square feet or square meter.

- **count**: Choose this option if you want to send the notifications based on the unique device count in a particular location type such as campus, building (network), floor or zone. If you choose this option, do the following configurations.
  - Set the device count limit using the adjacent drop-down lists. You can configure the device count limit as "more than" or "less than" a particular value, or as a value range using "between". You can choose "more than", "less than" or "between" from the first drop-down list, and you can manually enter the "value" or can choose the "value" from the drop-down list in the second field.
  - From the **at any** drop-down list, choose the location type of which the device count limit is to be considered.

**Note**
Cisco Meraki network and Cisco AireOS/ Cisco Catalyst connected through **Cisco DNA Spaces Connector** or **WLC Direct Connect** will not have **Campus** as a location type. So for these networks, if you are selecting **Campus** as location type, the rule will not be executed.

- **occupancy**: Choose this option if you want to send the notifications based on the occupancy in a particular location. You can define the occupancy limit for each location in the **Adding the Information of a Location** window in **Location Hierarchy**. You can configure to trigger the notification when the occupancy in a location reaches a certain percentage of the occupancy limit defined for that location. If you choose this option, do the following configurations.
  - Set the occupancy limit percentage at which the notification is to be triggered using the adjacent drop-down lists. You can configure the occupancy limit percentage as "more than" or "less than" a particular value, or as a percentage range using "between". You can choose "more than", "less than" or "between" from the first drop-down list, and you can manually enter the "percentage" or can choose the "percentage" from the **percent** drop-down list.

**Step 6**
In the Locations area, specify the locations for which you want to apply the rule.
You can configure to apply the rule for the entire location hierarchy, or a single or multiple locations such as group, floor, or zone. You can add the locations of multiple network types such as Cisco Meraki, Cisco AireOS or Cisco Catalyst in a Density rule. For more information on creating the location hierarchy, see the Defining the Location Hierarchy section.

You can again filter the locations based on the metadata defined for the selected location, or its parent or child locations. For more information on configuring the metadata for the locations, see the Adding Metadata for a Location section. You can either apply the rule for the locations with a particular metadata or exclude the locations with a particular metadata. For more information on filtering the locations, see the Filtering by Location.

**Step 7**

In the Schedule area, specify the period for which you want to apply the rule.

a) Check the **Set a date range for the rule** check box, and in the fields that appear, specify the start date and end date for the period for which you want to apply the Density rule.

b) Check the **Set a time range for the rule** check box, and in the fields that appear, specify the time range for which you want to apply the Density rule.

c) If you want to apply the rule only on particular days, check the **Filter by days of the week** check box, and from the list of days that appears, click the days on which you want to apply the rule.

**Step 8**

In the Actions area, specify the notification frequency and notification mode.

a) From the Notify drop-down list, choose any of the following:

   • Only Once: The notification is sent only once to the business user.

   • Once In: The notification is sent more than once based on the interval specified. If you choose this option, from the every drop-down list choose the interval value, and from the adjacent drop-down list, choose any of the following interval duration:

   - Hour(s)— To send the notification once in the number of hours specified.

   - Day(s)—To send the notification once in the number of days specified.

   - Week(s)— To send the notification once in the number of weeks specified.

   - Month(s)— To send the notification once in the number of months specified.

b) Specify the mode for sending notification.

You can send the notification to the customers through Cisco Webex Teams, e-mail, SMS, or to an external API. For more information on notification types, see Notification Type for a Business User, on page 170.

The summary of the rule is shown in the right side of the window.

**Note**

- If you are using the Via Email option, you must ensure to add the e-mail ID entering in the From field in the allowed list of e-mail IDs. To include the e-mail ID in the allowed list, contact the Cisco DNA Spaces support team. If you do not want to use a specific e-mail ID, you can use the default allowed e-mail ID no-reply@dnaspaces.io. However, the default ID is not displayed in the dashboard automatically. So, you have to enter it manually.

**Step 9**

Click Save and Publish.

The rule gets published, and is listed in the Density Rules window.
If you do not want to publish the rule now, you can click the Save button. You can publish the rule at any time later by opening the rule, and clicking the Save and Publish button. Also, you can publish the rule by clicking the Make Rule Live icon at the far right of the rule in the Density Rules window.

---

**What to do next**

You can go back to the Right Now report using the Right Now on WiFi option in the three-line menu that appears at the top-left of the window.

---

**Modifying a Density Rule**

To modify a Density rule, perform the following steps:

**Step 1**
In the Cisco DNA Spaces dashboard, click Right Now.

The Right Now window appears.

**Step 2**
Click the three-line menu icon that appears at the top-left of the window.

**Step 3**
Choose Density Rules.

The Density Rules window appears with all the existing Density rules listed.

**Step 4**
Click the Edit Rule icon that appears at the far right of the Density rule that you want to modify.

**Step 5**
Make necessary changes.

**Step 6**
To save the changes, click Save or to publish the changes, click Save and Publish.

*Note* A live rule will have only the Save and Publish button. When you click the Save and Publish button, the rule gets published with the changes.

---

**Pausing a Density Rule**

To pause a Density rule, perform the following steps:

**Step 1**
In the Cisco DNA Spaces dashboard, click Right Now.

The Right Now window appears.

**Step 2**
Click the three-line menu icon that appears at the top-left of the window.

**Step 3**
Choose Density Rules.

The Density Rules window appears with all the existing Density rules listed.

**Step 4**
Click the Pause Rule icon that appears at the far right of the Density rule that you want to pause.

**Step 5**
In the window that appears, confirm pausing.

The Density rule is paused.
What to do next

To pause multiple Density rules, check the check box for the Density rules that you want to pause, and click the Pause button that appears at the bottom of the page.

Note

[Note]

Restarting a Density Rule

To restart a Density rule, perform the following steps:

Step 1  In the Cisco DNA Spaces dashboard, click Right Now.

Step 2  Click the three-line menu icon that appears at the top-left of the window.

Step 3  Choose Density Rules.

Step 4  Click the Make Rule Live icon that appears at the far right of the Density rule that you want to restart.

Note  By default the icon name will be Pause Rule for all rules. Only for those rules that are paused the icon name changes to Make Rule Live.

The Density rule is restarted.

What to do next

To restart multiple Density rules, check the check box for the Density rules that you want to restart, and click the Make Live button that appears at the bottom of the window.

Deleting a Density Rule

To delete a Density rule, perform the following steps:

Step 1  In the Cisco DNA Spaces dashboard, click Right Now.

Step 2  Click the three-line menu icon that appears at the top-left of the window.

Step 3  Choose Density Rules.

Step 4  Click the Delete Rule icon that appears at the far right of the Density rule that you want to delete.

Step 5  In the dialog box that appears, click Delete Rule.
The Density Rule gets deleted.

**What to do next**

**Note**
To delete multiple Density rules, check the check box for the Density rules that you want to delete, and click the **Delete** button that appears at the bottom of the window.
Deleting a Density Rule
Chapter 8

Working with the Captive Portal App

This chapter describes how to create a captive portal using Cisco DNA Spaces.

• Creating and Managing Portal, on page 81
• Captive Portal Rule, on page 112
• Reports, on page 117
• SSIDs, on page 120
• Access Codes, on page 123
• User Management, on page 130
• Social Authentication for Portals, on page 131
• Configuring an SMS Gateway in Cisco DNA Spaces, on page 133
• Certified Device List for Portals, on page 139
• Cisco DNA Spaces Captive Portal Behavior, on page 140
• Authentication Steps for Customers, on page 144
• Smart Links and Text Variables for Captive Portals, on page 152

Creating and Managing Portal

A portal is the user interface that appears when a Wi-Fi user connects to an SSID. You can create the captive portals using Cisco DNA Spaces, and enhance the portals using the various portal modules provided by Cisco DNA Spaces.

Cisco DNA Spaces also allows you to have your own portals (Enterprise Captive Portals) to onboard end users who connect to Wi-Fi. For more information on Enterprise Captive Portals, see Enterprise Captive Portals.

Prerequisites for Creating a Portal

• To specify the locations for which the portal is applicable, you must define the location hierarchy. For more information on defining the location hierarchy, see the "Overview of Location Hierarchy" section.

• If you want to configure social authentication for the portal, you must do certain configuration in your social app, and then add that social app to Cisco DNA Spaces. For more information on configuring for social authentication, see the "Social Authentication for Portals" section.
• If you want to configure SMS-based authentication for the portal, you must configure the SMS gateway. For more information on configuring the SMS gateway, see the "Configuring an SMS Gateway in Cisco DNA Spaces" section.

Sample Portals

Cisco DNA Spaces provides sample portals for various authentication types.

• Email Authentication with Data Capture
• Inline SMS with password verification & data capture
• Inline Social Authentication
• SMS with password verification & data capture
• SMS with link verification
• Email authentication
• User Agreements

In addition, sample portals are provided to meet COVID-19 requirements.

To view and make a copy of the sample portal, perform the following steps:

Step 1  In the Cisco DNA Spaces dashboard, choose Home.
Step 2  In the window that appears, choose Captive Portal.
Step 3  In the Captive Portal window that appears, choose Portal in the left pane.
The sample portal for various authentication types are displayed at the bottom of the portal list.
Step 4  Click the Make a Copy icon at the far right of the sample portal that you want.
Step 5  In the portal wizard screen that appears, specify a name for the captive portal.
Step 6  If required, do the necessary customizations to the portal configuration,
Step 7  Save the portal.

Creating a Portal

When defining a portal, you can also configure the locations for which the portal must be available.

To create a portal, perform the following steps:

Step 1  In the Cisco DNA Spaces dashboard, choose Home.
Step 2  In the window that appears, choose Captive Portal.
Step 3  In the Captive Portal window that appears, choose Portal in the left pane.
Step 4  Click Create New.
The Portal wizard appears.
Step 5  In the **Portal Name** field, enter a name for portal.

Step 6  If you want this portal to be available only for certain locations, uncheck the **Enable this portal for all locations** check box.

**Note**  By default, the **Enable this portal for all locations** check box is checked so that the portal will be available for all the location in the location hierarchy.

Step 7  Click **Next**.

The **Authentication** window appears.

Step 8  From the **Authentication Type** drop-down list, choose the authentication type that you want apply for the portal.

Based on the authentication type selected additional fields appear. For more information on various authentication types, see the Configuring Authentication for a Portal, on page 87.

Step 9  After specifying the details for the authentication type, click **Next**.

The **Data Capture** window appears.

**Note**  For the “Social Sign In” authentication, you will be directed to the “User Agreements” screen as there is no Data Capture for Social Sign In. For Social Sign In, skip step 10 to step 12.

Step 10  If you want to add Data Capture form for this portal, check the **Enable Data Capture** check box.

Step 11  Configure the Data Capture form. Add the fields required for the Data Capture form using the **+Add Field Element** button. For more information on adding fields to the Data Capture form, see the Adding a Data Capture Form to a Portal, on page 95.

Step 12  Click **Next**.

The **User Agreements** window appears.

Step 13  In the **Terms & Condition Message** field, enter the “Terms & Conditions” for the portal.

**Note**  By default, the **Enable Terms & Conditions** check box is checked. If you do not want to specify any “Terms & Conditions”, uncheck the **Enable Terms & Conditions** check box.

Step 14  If you want to display privacy policy along with the Terms & Conditions, check the **Enable Privacy Policy** check box, and in the **Privacy Policy** field that appears, enter the privacy policy.

If you specify the privacy policy, during customer acquisition, the privacy policy also appears along with the “Terms & Conditions”.

Step 15  From the **How frequently do you want users to accept agreements** drop-down list, choose the frequency at which the customer must accept the “Terms & Conditions” to access the internet.

Step 16  In the **User Accepts Terms In** area, choose how the “Terms & Conditions” must appear during customer acquisition.

- **1-Click**—Choose this option, if you want display only the **Terms & Conditions** link. If you select this option, during customer acquisition, the customer can proceed further by clicking the “Accept Terms and Continue” button.

- **2-Click**—Choose this option, if you want to display a check box also along with the **Terms & Conditions** link. If you select this option, during customer acquisition, the customer has to select the check box, and click the **Accept Terms and Continue** button to proceed further.

**Note**  The 2-Click option is provided in Cisco DNA Spaces to meet the legal requirements of certain countries.
Step 17  If you want to restrict the internet access to the customers below certain age, select the **Enable Age gating** check box, and then choose the required age gating method from the following:

- **Moderate**: If you choose this option, during customer acquisition, the customer has to acknowledge that the age is 16 or above to proceed further.

- **Strict**: If you choose this option, during customer acquisition, the customer has to specify the month and year of the birth to access the internet. If the customer provides the age as less than 16, an alert message is shown, and the customer cannot proceed further to access the internet. However, the customer will be provided an option to change the age, if required.

Step 18  Click **Save and Configure Portal**.

A message **Portal saved successfully** appears, and the **Portal** window opens with the portal modules on the left and portal preview on the right.

Step 19  Add features to the portal using the **Portal Modules**, on page 84.

Step 20  Click **Save** to save the changes made to each module.

**Note**  When creating the portal, you can save the portal after specifying the name and locations for the portal. The new portal gets listed in the **Portals** window. You can configure authentication type, Terms & Conditions, Data Capture form, and so on at any time later using the Edit Portal button for that portal.

**Note**  To capture the details such as name, phone number, and so on of the customers connecting to the SSID using the captive portal, ensure that you add a “Data Capture form” in the captive portal. During customer acquisition (runtime), before provisioning the internet, the data capture form is displayed to the customer. The captured customer details are stored in Cisco DNA Spaces.

**Note**  A portal becomes live when you associate it with a Captive Portal Rule, and publish that rule.

---

### Portal Modules

The following are the portal modules of Cisco DNA Spaces:

- **Brand Name**—Define your brand name in the portal using this module. You can add the brand name as text or a logo image.

- **Welcome Message**—Add a welcome message in the portal using this module. You can configure to show different welcome messages for first time users and repeat users.

- **Notice**—Add a notice in the portal using this module. This helps you display notices to the portal users whenever required. You can set to provide the notice in the thicker text, text, or text with an image format.

- **Authentication**—Based on the authentication type selected when creating the portal, an Authentication module appears for the portal. The name of the module will be based on the authentication type. For example, if you have selected “SMS with link verification” as authentication type for a portal, the authentication module for that portal will be named as “SMS Authentication”. The Authentication module will have provision to configure the landing page URL for the portal. The Authentication module will not be available for the authentication type, “No Authentication”, if both “Data Capture” and “User Agreements” are not enabled.

- **Venue Map**—Add a label and icon for the Venue Map using this module. The venue map is uploaded in the portal from your wireless network based on the location.
• **Videos**—Add YouTube videos in the portal using this module. You can also add an appropriate caption and icon for the video section in the portal. You can also view the preview of the video when uploading.

• **Feedback**—Add the feedback questions in the portal using this module. You can add multiple choice and rating questions. This module also lets you customize the labels for the “Submit” button, “Thank You” message, and “Post Submission” button. You can also set whether the customers are to be provided a text box to add the comments. You can also specify the e-mail addresses and subject for feedback.

• **Help**—Add a help line number that the customer can contact for assistance using this module. You can customize the caption and icon for Help.

• **Get Apps**—Add apps to the portal using this module. You can add appropriate caption and icon for each app using this module.

• **Get Internet**—Add the external URL to which customer can navigate from the Get Internet section in the portal. To navigate to this URL, the customer has to accept the terms and conditions provided.

• **Promos & Offers**—Add the promotions and offers to display through the portal using this module. You can modify the title of the promotion. For each promotion you can add appropriate captions and images, and specify the URL to the promotion details. Promos are displayed as carousels.

• **Add Module**—Add customized content and menu items to the portal using this module. All the modules mentioned earlier are the default modules provided by Cisco DNA Spaces. You can add additional items to a portal based on your requirements using the “Add Module” button.

## Configuring a Language for a Portal

In Cisco DNA Spaces, you can configure the language in which the module captions and static content in the portal are to display. To display the static content in any language other than English, you must upload the corresponding text to Cisco DNA Spaces. Cisco DNA Spaces does not support to enter the content in any language other than English. The default language is set to English. You can change the default language.

You cannot translate the content prepared in one language to another using Cisco DNA Spaces.

To configure a language in which the portal content is to display, perform the following steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>To display the static content such as messages, country names, and so on in a language other than English, upload the key values in that language. For more information on uploading the key values for a language, see the <a href="#">Uploading Static Content Key Values for a Language</a>, on page 86</td>
</tr>
<tr>
<td>Step 2</td>
<td>Open the portal for which you want to configure the language.</td>
</tr>
</tbody>
</table>
| Step 3 | Click the **Languages** (Globe) icon at the top of the **Portal** window.  
The **Add Language** window appears. |
| Step 4 | Click **Add Language**. |
| Step 5 | In the search field that appears, enter the language.  
If this language is supported by Cisco DNA Spaces, then the language name appears in the drop-down list. |
| Step 6 | Click the **Add** button that appears adjacent to the language name. |
Setting a Default Language

To set a default language, do the following:

Step 1 In the portal, click the Languages icon at the top right of the window.
Step 2 In the Add Language window, from the “Default Language” drop-down list, choose the default language.
Step 3 Click Add.

Uploading Static Content Key Values for a Language

To set to display the static content in any language other than English, perform the following steps:

Step 1 In the portal, click the Languages icon at the top right of the window.
Step 2 In the Add Language window, click Download to download and save the template.
Step 3 Open the template.

The template contains keys for various static messages and the message that appears if your language is English. The column for English has “en” as first row.

Step 4 In the column adjacent to the English column, enter the language identifier for the language in which you want to display the static content.

For example, if you want to display the content in Arabic, enter “AR” in the first row.

Step 5 In the remaining rows, enter the text that must appear for the corresponding key.
Step 6 Save the file.
Step 7 In the Add Language window, use the Upload button to upload the window.
Step 8 Click Add.

What to do next

To know how to display the static content in a language, see the Configuring a Language for a Portal, on page 85.
The language code for various languages are shown in the following figure.

Figure 8: Language Code

Configuring Authentication for a Portal

To secure your portal from hacking or misuse, you can configure various authentication options for your portal. The customer is provided access only if the authentication is success.

You can authenticate the internet provisioning through SMS, e-mail, access code, or social networks such as Facebook, Twitter, or LinkedIn. Cisco DNA Spaces supports the SMS gateway of the third party vendors for SMS authentication. You can configure to provide SMS authentication through “SMS with password verification” or “SMS with link verification”. For “SMS with password verification”, you can define a custom verification code for a portal or you can configure to auto-generate the verification code.

During customer acquisition, the authentication process is initiated when the customer click any menu item in the portal. However, you can configure for inline authentication also, so that the Authentication module will be shown in the captive portal. For more information on inline authentication, see the Inline Authentication, on page 94.

Cisco DNA Spaces supports the following authentication types:

- **SMS with password verification** — For this authentication type, validation of mobile number is mandatory. When the customer enters a valid mobile number, an SMS is sent to that mobile number, which contains a link and verification code. The customer can access the internet by providing the verification code. The customer is not allowed to proceed further until the verification code is entered. Some use cases for this authentication type are SMS-based engagement campaigns, country specific requirements to verify the users connecting to internet, and so on. To know the authentication steps during customer acquisition, see Steps for SMS with Password Verification Authentication, on page 146. For more information, see the Configuring a Portal for SMS with Password Verification, on page 89 section.

- **SMS with link verification** — For this authentication type, validation of mobile number is optional. When the customer provides a valid mobile number, an SMS is sent to that mobile number with verification link. The customer can complete the validation by clicking the verification link in the SMS. However, customer can skip the validation process and proceed further. This authentication type can be used if the validation of the mobile number is not mandatory. To know the authentication steps during customer acquisition, see Steps for SMS with Link Verification Authentication, on page 144. For more information, see the Configuring a Portal for SMS with Link Verification, on page 88 section.
Email — The customer has to provide a valid e-mail ID to access the internet. To know the authentication steps during customer acquisition, see Steps for Email Authentication, on page 148. For more information on configuring e-mail authentication, see the Configuring a Portal for Email Authentication, on page 92 section.

Social Sign In — The internet access is provided only if the customer is logged in to a social site configured for authentication. You must configure at least one social site to use this option. To know the authentication steps during customer acquisition, see Steps for Social Authentication, on page 151. For more information on configuring the Social Sign In authentication, see the Configuring a Portal for Social Sign In Authentication section.

Access Code — The customer has to provide a valid access code to access the internet. To know the authentication steps during customer acquisition, see Steps for Access Code Authentication, on page 149. For more information on configuring Access code authentication, see the Configuring a Portal for Access Code Authentication, on page 93 section.

No Authentication — The internet access is provided without any authentication process. To know the authentication steps during customer acquisition, see Steps for No Authentication with Terms and Conditions, on page 150. For more information on configuring a portal for No Authentication, see the Configuring a Portal with No Authentication, on page 94 section.

The Opt In option is not available for “SMS with link verification” and “Social Sign In” authentication types. You can configure the Data Capture form for all the authentication types, except “Social Sign In”. For more information on configuring the Data Capture form, see the Adding a Data Capture Form to a Portal, on page 95. For more information on Opt In feature, see the “Opted In Option for Users” section.

Configuring a Portal for SMS with Link Verification

To configure a portal for “SMS with link verification”, do the following:

Step 1 When creating a portal, from the Authentication Type drop-down list, choose SMS with Link verification.

Step 2 If you want to configure inline authentication for this portal, and display the “Data Capture form” and “User Agreements” in the home page, check the Display Authentication, Data Capture, and User Agreements on portal home page check box. For more information on inline authentication, see the Inline Authentication, on page 94.

Step 3 In the SMS field, enter the text message that must appear in the SMS sent to the customer.

Note To display the link through which the customer can access the captive portal, ensure that “{Link}” is not removed when editing the text message.

Step 4 From the Default Country drop-down list, choose the country for which this setting is applicable.

Step 5 From the SMS Gateway drop-down list, choose the SMS gateway.

The SMS Gateways configured in the Settings option are available for selection. You can also use the Demo Gateway provided by Cisco that is chargeable.

Note For more information on configuring the SMS gateway, see the Configuring an SMS Gateway in Cisco DNA Spaces, on page 133.

Step 6 Save the changes.
Configuring a Portal for SMS with Password Verification

To configure a portal for “SMS with password verification”, perform the following steps:

Step 1 When creating a portal, from the Authentication Type drop-down list, choose **SMS with password verification**.

Step 2 If you want to configure inline authentication for this portal, and display user agreements on portal home page, check the **Display Authentication and User Agreements on portal home page** check box. For more information on inline authentication, see the **Inline Authentication**, on page 94.

Step 3 If you want the customers to provide an option to opt for receiving notifications, check the “Allow users to Opt in to receive message” check box.

Step 4 If the “Allow users to Opt in to receive message” check box is checked, the following fields appear:

- **Opt in Message**: Enter an opt in message.

- **Default Opt-In Check Box Behavior**
  - **Checked**: Click this option if you want the **Opt In** check box to be displayed as checked by default, during customer acquisition.
  - **Unchecked**: Click this option if you want the **Opt In** check box to be displayed as unchecked by default, during customer acquisition.

Step 5 Click the required Password Type.

- **Auto Generated password**— To auto-generate the password for each authentication request. The auto-generated password is sent to the customer.

- **Fixed Password**— To define a password for authentication. For all of the customers, this password is sent whenever there is an authentication request. In the “Password” field that appears when you click the “Fixed Password” option, enter the password that is to send to the customers.

Step 6 In the **SMS field** field, enter the text that must appear in the SMS that is sent to the customer.

**Note** To display the link through which the customer can access the captive portal, ensure that “{Link}” is not removed when editing the text message. Similarly, to display the password in the message, ensure that the “{Password}” is not removed.

Step 7 From the **Default Country** drop-down list, choose the country for which this setting is applicable.
Step 8  
From the SMS Gateway drop-down list, choose the SMS Gateway. The SMS Gateways configured in the Settings option are available for selection. You can also use the Demo Gateway provided by Cisco that is chargeable.

Note  
The SMS Gateway window appears where you can configure the required SMS gateway. For more information on configuring the SMS gateway, see the Configuring an SMS Gateway in Cisco DNA Spaces, on page 133.

Step 9  
Save the changes.

---

**What to do next**

Note  
Portals with SMS with password verification authentication type will have an authentication module named SMS Authentication. For more information on the Authentication module, see the Authentication Module, on page 95.

---

Note  
If you have not configured the authentication type when creating the portal, you can specify it at any time using the Edit Portal button for that portal in the Portals window.

### Configuring a Portal for Social Sign In Authentication

Cisco DNA Spaces supports the authentication through the following social networks:

- Facebook
- Twitter
- LinkedIn
- Instagram

Note  
- Currently, there is no dashboard support for Instagram authentication. For more information on configuring the Instagram authentication, see Configurations for Instagram Authentication, on page 91.
- To authenticate the access to the internet through a social network, you must configure the app for that social network in Cisco DNA Spaces. You can configure the social app in Cisco DNA Spaces through the Settings option. For more information, see the Adding Social Apps for Social Authentication, on page 133.

To authenticate the access to a portal through social sign in, perform the following steps:

Step 1  
When creating a portal, from the Authentication Type drop-down list, choose Social Sign In. The social networks that are supported by Cisco DNA Spaces for authentication appear along with the configured social apps.
Step 2 If you want to configure inline authentication for this portal, and display user agreements in the portal home page, check the Display Authentication and Users Agreements on portal home page check box. For more information on inline authentication, see the Inline Authentication, on page 94.

Step 3 Select the check box adjacent to the social networks through which you want to authenticate access to the internet.

The social networks configured in the Social Apps option under the Settings section will be available for selection. For more information on configuring the Social Apps, see the Adding Social Apps for Social Authentication, on page 133.

Step 4 Save the changes.

---

**What to do next**

**Note** Portals with Social Sign In authentication type will have an authentication module named Social Authentication. For more information on the Authentication Module, see the Authentication Module, on page 95.

**Note** The +Add button takes you to the Social Apps window where you can configure the customized apps.

**Note** If you have not configured the authentication type when creating the portal, you can specify it at any time using the Edit Portal button for that portal in the Portals window.

---

### Configurations for Instagram Authentication

Cisco DNA Spaces allows you to provide internet authentication to your captive portals through Instagram credentials. Currently, the Cisco DNA Spaces dashboard does not have the provision to configure Instagram authentication in the captive portal. So after creating the Instagram app, you must contact the Cisco DNA Spaces support team for configuring the captive portal for Instagram authentication.

**Note** You must have a Facebook developer account.

To configure Instagram authentication for your portals, do the following:

**Step 1** Go to developers.facebook.com.
**Step 2** Choose Products > Add Instagram > Setup > Basic Display.
**Step 3** Click Create New App.
**Step 4** Enter your facebook account name as Display name, and in the Valid OAuth Redirect URIs field, configure the valid website URL. For example, https://cisco.wifi-mx.com/p/instagram_auth.

You can now view the Instagram app ID and secret key in the Basic Display window under Products > Instagram.
Step 5
You can enable your Instagram app to be accessed by your Facebook app when it is in Development Mode. For that, perform the following steps:

This is not applicable for already activated Instagram apps.

a) In the Facebook developer app, choose Roles > Roles.
b) In the window that appears, scroll down to the Instagram Testers section.
c) Click Add Instagram Testers.
d) Enter your Instagram account’s username, and send the invitation.
e) Open a new web browser, and go to www.instagram.com.
f) Sign into your Instagram account to which you are invited.
g) In the Instagram home page, click the Profile icon.
h) Choose Edit Profile > Apps and Websites > Tester Invites.
i) Accept the invitation.

Alternatively for step e to i, click https://www.instagram.com/accounts/manage_access/, sign in, and in the Tester Invites tab, click Accept for the invite.

Step 6
Contact Cisco DNA Spaces support team, and share the Instagram app ID and secret key for configuring Instagram authentication in the portal.

The Cisco DNA Spaces support team now will do the necessary settings from the backend to make the text fields for entering the Instagram credentials in the captive portals.

Step 7
In the wireless network, configure to allow the following Instagram domains.

- instagram.com
- *.instagram.com
- api.instagram.com
- d36xtkk24g8jdx.cloudfront.net
- www.facebook.com
- connect.facebook.net
- *.akamaihd.net

For more information on configuring wireless network for Instagram authentication, see Configuring the Wireless Network for Social Authentication, on page 131.

Configuring a Portal for E-mail Authentication

To configure a portal for e-mail authentication, do the following:

Step 1
When creating a portal, from the Authentication Type drop-down list, choose Email.

Step 2
If you want to configure inline authentication for this portal, check the Display Authentication and User Agreements on portal home page check box. For more information on inline authentication, see the Inline Authentication, on page 94.
Step 3 If you want to provide the customer an option to opt for receiving notifications, check the Allow users to Opt in to receive message check box.

Step 4 If the Allow users to Opt in to receive message check box is checked, the following fields appear:

• **Opt in Message**: Enter an “opt in” message

  • **Default Opt-In Check Box Behavior**
    • **Checked**—Click this option if you want the **Opt In** check box to be displayed as checked by default, during customer acquisition.
    • **Unchecked**—Click this option if you want the **Opt In** check box to be displayed as unchecked by default, during customer acquisition.

Step 5 Save the changes.

---

**What to do next**

**Note** Portals with **Email** authentication type will have an authentication module named **Email**. For more information on the Authentication Module, see the Authentication Module, on page 95.

---

**Configuring a Portal for Access Code Authentication**

To configure a portal for the Access Code authentication, do the following:

Step 1 When creating a portal, from the **Authentication Type** drop-down list, choose **Access Code**.

Step 2 If you want to configure inline authentication for this portal, and display user agreements on portal home page, check the **Display Authentication and User Agreements on portal home page** check box. For more information on inline authentication, see the Inline Authentication, on page 94.

Step 3 If you want the customers to provide an option to opt for receiving notifications, check the Allow users to Opt in to receive message check box.

Step 4 If the Allow users to Opt in to receive message check box is checked, the following fields appear:

• **Opt in Message**: Enter an opt in message.

  • **Default Opt-In Check Box Behavior**
    • **Checked**—Click this option if you want the **Opt In** check box to be displayed as checked by default, during customer acquisition.
    • **Unchecked**—Click this option if you want the **Opt In** check box to be displayed as unchecked by default, during customer acquisition.

Step 5 Save the changes.
You can create access codes and share it with your customers using the **Access Code** option displayed in the left pane of the **Captive Portals** app. For more information on creating and sharing the access codes, see **Access Codes, on page 123**.

---

**What to do next**

**Note**

Portals with **Access Code** authentication type, provided **Data Capture** or **User Agreements** is enabled. For more information on the Authentication module, see the **Authentication Module, on page 95**.

---

**Configuring a Portal with No Authentication**

To configure a portal for No Authentication, perform the following steps:

**Step 1**  When creating a portal, from the **Authentication Type** drop-down list, choose **No Authentication**.

**Step 2**  If you want to display data capture and user agreements on portal home page, check the **Display Data Capture and User Agreements on portal home page** check box.

**Step 3**  If you want the customers to provide an option to opt for receiving notifications, check the **Allow users to Opt in to receive message** check box.

**Step 4**  If the **Allow users to Opt in to receive message** check box is checked, the following fields appear:

- **Opt in Message**: Enter an “opt in” message.
- **Default Opt-In Check Box Behavior**
  - **Checked**: Click this option if you want the **Opt In** check box to be displayed as checked by default, during customer acquisition.
  - **Unchecked**: Click this option if you want the **Opt In** check box to be displayed as unchecked by default, during customer acquisition.

**Step 5**  Save the changes.

---

**Inline Authentication**

In the Captive Portal, you can add authentication as an inline module along with other modules. That is, the authentication option is displayed before the customer click any link in the captive portal, thus reducing the number of clicks required to initiate the authentication process.

To configure inline authentication, in the Authentication screen, select the check box provided for configuring inline authentication.

For the **SMS with Link verification** and **SMS with password verification** authentication types, the authentication section will have a field to enter the mobile number, along with a Connect button. For Email authentication, the authentication section will have a field to enter the email ID. For social authentication, the authentication section will have relevant buttons for each social network configured for the portal, using which the customer can complete the authentication through that social network.
Authentication Module

When you select the authentication type for a portal, an authentication module is created for the portal based on the authentication type selected.

If you select the authentication type No Authentication or Access Code for a portal, that portal will not have an authentication module, if either “Data Capture” or “User Agreements” is not enabled.

The Authentication module will have a field to specify the alternate landing page for the portal.

Adding a Data Capture Form to a Portal

If you choose an authentication type other than Social Sign In for the portal, you can add a Data Capture form in the captive portal. You can add fields to the Data Capture form when creating the portal. You can configure the fields to capture the details such as first name, last name, mobile number, and so on of the customer. You can also add business tags based on which you can filter your customers.

Note

The business tags defined in the Data Capture form are available in the “Add Tags” option available in the rules such as Captive Portal Rule, Engagement Rule, and Profile Rule.

To configure a Data Capture form in a captive portal, perform the following steps:

Step 1
When creating a portal, after specifying the Terms and Conditions, click Next.

Step 2
Enable the Data Capture check box.

Step 3
Click Add Field Element.

You can add the following field elements to the Data Capture form:

• **Title**—To specify how to address the customer. For example, Mr, Ms. If you configure this field, during customer acquisition (runtime), the titles, Mr and Ms will be available for selection in the Data Capture form for the customer.

• **Email**—To specify the e-mail ID of the customer.

• **Mobile Number**—To specify the mobile number of the customer. You can specify a default country for the mobile number so that during customer acquisition, the code for the default country is displayed in the data capture form.

• **First Name**—To specify the first name of the customer.

• **Last Name**—To specify the last name of the customer.

• **Gender**—To specify the gender of the customer.

• **Date of Birth**: To specify the date of birth of the customer. If you add the Date of Birth field, you are not allowed to select the Moderate option in the Enable Age Gating area in the User Agreements window.

• **Business Tags**—To provide an answer of customer’s choice for the business tag question. This business tags help you in categorizing the customers.

• **Country Specific Fields**
  • **ZIP/Postal Code**—To provide the postal code of your address.
• CPF—To provide the CPF (This is applicable only for Brazil).

Note The Email field element is not available for Email authentication as the e-mail information is already collected during authentication. The Mobile Number field element is not available for the SMS with password verification authentication as the customer has to provide the mobile number during authentication.

Step 4 Click the corresponding option to add the fields.

General Fields
• In the Place Holder field, enter the text that must appear as place holder for the field.
• Check the Make this field mandatory check box to make the field mandatory.

Element-Specific Fields
• For the mobile number field element, choose the default country so that the country code for this country appears in the data capture form during customer acquisition.
• For the Zip/Postal Code field element, from the Country drop-down list, choose the country, so that the data capture form allows the customer to add the postal codes of that particular country. To support the postal codes of more than one country, click Add Country, and add another country.
• For the Business Tag field element, you must configure the following additional fields:
  • In the Name field, enter a name for the business tag.
  • In the Field Label field, enter the question that you want to ask the customer.
  • Click +Add Option.
  • In the field that appears, enter an answer that you want to provide to the customers to opt.
  • Similarly, add the remaining answer choices also using the +Add Option.

Note You can delete an added option using the corresponding Delete icon.
Note When the customers access the Data Capture form during authentication process, the answers you specify are available in a drop-down list. They can choose the required value. You can use this value for filtering the customers in the proximity rules.

Step 5 Save the changes.

Note During customer acquisition, the value entered in the CPF field in the Data Capture form will be converted to the "000.000.000-00" format. The number will be formatted automatically as the user enters the CPF number value. So the captive portal users do not have to add dots or hyphen manually to maintain the required format.

---

Defining a Brand Name for a Portal

Cisco DNA Spaces enables you to add your brand name in the portal using the Brand Name module. You can add the brand name as text or image. For example, you can use your company logo as a brand name.

To define a brand name in the portal, perform the following steps:
Working with the Captive Portal App

Adding a Welcome Message to a Portal

You can add a welcome message to a portal using the Welcome module. The welcome message added is displayed when a customer accesses your portal. You can configure to display different welcome messages for first time user and repeat user.

To add a welcome message to a portal, perform the following steps:

Step 1 Open the portal in which you need to add the welcome message.
Step 2 Click the Welcome Message module.
Step 3 In the First time visitor welcome text field, enter the welcome message that must appear when a customer accesses your portal for the first time. You can include the location details using the smart link variables. For more information on smart link, see the Smart Links and Text Variables for Captive Portals, on page 152.
Step 4 If you want to display a different welcome message for Repeat Visitors check box is checked, and in the adjacent text box, enter the welcome message for the repeat user. You can include the name and location details using the smart link variables. The variables “firstName” and “lastName” will be available for selection only if you have configured a Data Capture module in the portal with the fields, First Name and Last Name. The variables “firstName”, and “lastName” will be available for the authentication types other than “Social Sign In”. For more information on smart link, see the Smart Links and Text Variables for Captive Portals, on page 152.
Step 5 Click Save.
The welcome message is successfully defined for the portal.

What to do next

**Note**
If you are modifying a portal that is already associated with a published captive portal, click the **Save and Publish** button to immediately publish the changes. The **Save and Publish** button appears only if the portal is associated with a captive portal rule. For more information on creating a captive portal rule, see the *Creating a Captive Portal Rule to Display Captive Portals*, on page 113.

## Adding a Notice to a Portal

The Notice module enables you to provide notices in your portal. This module is useful when you want to pass any important information to your customers. You can add ticker and text notices. You can also add images along with text notices.

You can configure the date up to which the notice is to be displayed in the portal.

To add notices in a portal from the dashboard, do the following:

**Step 1**
Open the portal in which you want to add notice.

**Step 2**
Click the **Notice** module.

The **Notice** window appears.

**Step 3**
Click the type of notice you want. The following options are available:

- **Ticker Text Only**—The notice appears in a moving text format. For **Ticker Text Only**, in the **Notice** field that appears, enter the notice text.

- **Text Only**—The notice appears in the text format. For **Text Only**, in the **Notice** field that appears, enter the notice text.

- **Text with Image**—The notice appears as a text along with an uploaded image. For **Text with Image**, do the following:
  - In the **Notice** field, enter the notice text.
  - In the **Notice image** area, click the **Upload** button, and upload the image that must appear with the notice.

**Step 4**
In the **Hide After** field, choose the date up to which the notice is to display in the portal.

**Step 5**
Click **Save**.

The notice is successfully added to the portal.
What to do next

Note
If you are modifying a portal that is already associated with a published captive portal, click the Save and Publish button to immediately publish the changes. The Save and Publish button appears only if the portal is associated with a captive portal rule. For more information on creating a captive portal rule, see Creating a Captive Portal Rule to Display Captive Portals, on page 113.

Providing the Venue Details in a Portal

You can provide the venue details in a portal using the Venue Map module. You can define a label name, upload an icon image, and display a map for the venue using this module.

The default name of the module is Venue Map. The module name changes based on the changes you make in the Label field.

To add the venue details for a portal, perform the following steps:

Step 1
Open the portal in which you want to add the venue details.

Step 2
Click the Venue Map module.

The VENUE MAP window appears.

Step 3
In the Label field, enter the venue map label name that must appear in the portal.

Note
The Venue Map module name gets changed to the name you specify in the Label field.

Step 4
In the Icon area, upload the map icon that must appear adjacent to the map label using the Upload button.

Note
You can delete the icon using the Delete icon.

Step 5
In the Store Map area, the map for this venue as in the wireless network appears.

Note
The map appears only if the portal is associated with a location for which the map is defined in the wireless network (CUWN, Meraki). The map of the location where the customer is currently present is shown.

Step 6
Click Save.

The venue map is configured for the portal.

What to do next

Note
If you are modifying a portal that is already associated with a published captive portal, click the Save and Publish button to immediately publish the changes. The Save and Publish button appears only if the portal is associated with a captive portal rule. For more information on creating a captive portal rule, see the Creating a Captive Portal Rule to Display Captive Portals, on page 113.
Uploading Videos to a Portal

You can upload the videos to Cisco DNA Spaces portals using the Videos module. In this module, you can add a label and image for the area where the video appears in the portal, and specify the Youtube URL of the video.

The default name of the module is Videos. The module name changes based on the changes you make in the Label field.

Note

You can show only the YouTube videos in your portal.

To upload videos to a portal, perform the following steps:

**Step 1**
Open the portal in which you want to upload the video.

**Step 2**
Click the Videos module.

The VIDEOS window appears.

**Step 3**
In the Label field, enter the label that must appear for the area where the video appears in the portal.

Note

The Videos module name gets changed to the name you specify in the Label field.

**Step 4**
In the Icon area, upload the video icon that must appear adjacent to the video label using the Upload button.

Note

You can delete the icon using the Delete icon.

**Step 5**
Click Add a Video.

**Step 6**
In the YouTube URL field that appears, enter the YouTube URL of the video that you want to display in the portal.

**Step 7**
Click Save.

The video is successfully uploaded to the portal.

What to do next

Note

If you are modifying a portal that is already associated with a published captive portal, click the Save and Publish button to immediately publish the changes. The Save and Publish button appears only if the portal is associated with a captive portal rule. For more information on creating a captive portal rule, see the Creating a Captive Portal Rule to Display Captive Portals, on page 113.

Providing a Feedback Section in a Portal

The Feedback module in Cisco DNA Spaces enables you to collect the feedback from the customers of your portals. This module enables you to add multiple questions in the feedback section. These questions can be with multiple choice answers or rating-based answers. You can also provide a text box where the customers can add their comments.
To add a feedback section in a portal, perform the following steps:

**Step 1** Open the portal in which you need to add the feedback section.

**Step 2** Click the **Feedback** module.

The **FEEDBACK** window appears.

**Step 3** In the **Label** field, enter a name that must appear for the feedback section.

**Step 4** In the **Icon** area, upload the icon image that must appear adjacent to the feedback label using the **Upload** button.

**Step 5** In the **Question field**, enter a question for which you want the answer from the customer.

**Step 6** In the **Question Image** area, upload an image that must appear adjacent to the question using the **Upload** button.

**Step 7** In the **Question Type** area, choose any of the following:

- **Rating**: The customer can answer the question through rating.
- **Multiple Choice**: The customer can answer from the multiple choices provided. If you have chosen this option, enter the multiple choice of answers in the **Option 1** and **Option 2** fields. If you want to provide more choices, add the choice options using the “Add option” button.

**Note** You can add more questions to the feedback section using the “Add question” button.

**Step 8** In the **Submit Button Label** field, enter the name for the submit button, using which the customer must submit the answer.

**Step 9** In the **Thank You/Success message** field, enter the message that must appear to the customer after the customer submits the answer.

**Step 10** In the **Post Submission button label** field, enter the name for the button that appears once the customer’s answer is submitted. This button leads the customer to the Cisco DNA Spaces dashboard.

**Step 11** If you want to provide a text box for the customer to enter the comments, select the **Add a text box for additional comments from end user?** check box.

**Step 12** In the **Email to** field, enter the e-mail address to which the feedback is to be e-mailed.

**Step 13** In the **Email from** field, enter the **From** e-mail address to display to the receiver of the e-mail for the feedback e-mails.

**Step 14** In the **Email Subject** field, enter the subject for the e-mails with the feedback.

**Step 15** Click **Save**.

The feedback section is successfully created in the portal.

---

**What to do next**

**Note** If you are modifying a portal that is already associated with a published captive portal, click the **Save and Publish** button to immediately publish the changes. The **Save and Publish** button appears only if the portal is associated with a captive portal rule. For more information on creating a captive portal rule, see the Creating a Captive Portal Rule to Display Captive Portals, on page 113.
Adding a Help Option to a Portal

You can add a help line in your Cisco DNA Spaces portal using the Help module. The customers can use this help line to contact you, if they need any assistance. In this module, you can add a label and image for the area where the Help line appears in the portal, and you can specify the number to contact if the customer needs any assistance.

The default name of the module is Help. The module name changes based on the changes you make in the Label field.

To add a Help option to a portal, perform the following steps:

Step 1: Open the portal in which you need to add a help option.
Step 2: Click the Help module.
   The HELP window appears.
Step 3: In the Label field, enter the label that must appear for the area where the help line appears in the portal.
   Note: The Help module name gets changed to the name you specify in the Label field.
Step 4: In the Icon area, upload the help icon that must appear adjacent to the help label using the Upload button.
   Note: You can delete the icon using the Delete icon.
Step 5: In the Contact field, enter the help line number.
Step 6: Click Save.
   The help option is successfully defined for the portal.

What to do next

Note: If you are modifying a portal that is already associated with a published captive portal, click the Save and Publish button to immediately publish the changes. The Save and Publish button appears only if the portal is associated with a captive portal rule. For more information on creating a captive portal rule, see the Creating a Captive Portal Rule to Display Captive Portals, on page 113.

Adding Apps to a Portal

You can add apps to your Cisco DNA Spaces portal using the Apps module. You can add apps from both iOS app store and Play Store. In this module, you can add a label and image for the area where the apps appear in the portal.

The default name of the module is Get Apps. The module name changes based on the changes you make in the Button Label field.

To add an app to a portal, perform the following steps:
Step 1  Open the portal in which you need to add an app.
Step 2  Click the Get Apps module.
        The GET APPS window appears.
Step 3  In the Label field, enter the label that must appear for the area where the app appears in the portal.
        The Get Apps module name gets changed to the name you specify in the Label field.
Step 4  In the Icon area, upload the app icon that must appear adjacent to the app label using the Upload button.
        You can delete the icon using the Delete icon.
Step 5  Click Add an App.
Step 6  In the Add App area, do the following:
        a) From the Platform drop-down list, choose the app platform.
        b) In the App Store URL field, enter the URL of the app store from which you want to add app.
        c) In the App URL Scheme field, enter the URL scheme for your app that you receive when you install an app on your device.
        d) To provide a different URL for the desktops and laptops, check the Show this URL for Desktops and Laptops check box.
        e) If you have checked the Show this URL for Desktops and Laptops check box, enter the URL for desktops and laptops.
        To add more apps, use the Add an app button.
Step 7  Click Save.
        The app is successfully added to the portal.

What to do next

If you are modifying a portal that is already associated with a published captive portal, click the Save and Publish button to immediately publish the changes. The Save and Publish button appears only if the portal is associated with a captive portal rule. For more information on creating a captive portal rule, see the Creating a Captive Portal Rule to Display Captive Portals, on page 113.

Providing Access to the Internet from a Portal

You can provide access to the internet from a portal using the Get Internet module. You can add an external URL to a portal using the Get Internet module. In this module, you can add a label and image for the area where the internet link appears in the portal.

The default name of the module is Get Internet. The module name changes based on the changes you make in the Button Label field.
If inline authentication is configured for the captive portal, the Get Internet module will not be shown during customer acquisition, even if it is configured. For more information on inline authentication, see the Inline Authentication, on page 94.

To provide access to the internet from a portal, perform the following steps:

---

**Step 1**
Open the portal in which you need to provide a link to the internet.

**Step 2**
Click the Get Internet module.

The GET INTERNET window appears.

**Step 3**
In the Label field, enter the label that must appear for the area where the internet link appears in the portal.

**Note**
The Get Internet module name gets changed to the name you specify in the “Label” field.

**Step 4**
Upload the icon that must appear adjacent to the internet link using the Upload button.

**Note**
You can delete the image using the Delete icon.

**Step 5**
To change the landing page, ensure that the Change Landing page URL check box is checked.

**Step 6**
In the Launch Page field, enter the URL to connect to the internet from the portal.

**Step 7**
Click Save.

An option to access the internet is successfully configured in the portal.

---

**What to do next**

**Note**
If you are modifying a portal that is already associated with a published captive portal, click the Save and Publish button to immediately publish the changes. The Save and Publish button appears only if the portal is associated with a captive portal rule. For more information on creating a captive portal rule, see the Creating a Captive Portal Rule to Display Captive Portals, on page 113.

---

**Adding Promotions and Offers to a Portal**

The Promos & Offers module enables you add promotions and offers that you want to provide to the customers in your portal. You can add various promotion items in your portal that can be linked to different promotion URLs. The module enables you add a label, icon, and web URL for each promotion.

**Note**
The promotions are displayed as carousels.

To add promotions and offers to a portal, perform the following steps:
Step 1  Open the portal in which you want to add the promotions and offers module.
Step 2  Click the Promos & Offers module.
The PROMOS & OFFERS window appears.
Step 3  In the Label field, enter the label that must appear for the area in which the promotions and offers appear.
Step 4  Click Add a Promotion.
Step 5  In the Promo Name field, enter a name for the promotion link.
Step 6  In the Promo Image area, upload the icon that must appear adjacent to the promotion link using the Upload button.
Step 7  In the Link Promo to URL field, enter the URL that links to the promotion web page.
Step 8  Click Save.
The promotions and offers link is successfully added to the portal.

What to do next

Note  You can add more than one promotion to your portal using the Add a Promotion button.

Note  If you are modifying a portal that is already associated with a published captive portal, click the Save and Publish button to immediately publish the changes. The Save and Publish button appears only if the portal is associated with a captive portal rule. For more information on creating a captive portal rule, see the Creating a Captive Portal Rule to Display Captive Portals, on page 113.

Deleting a Promotion and an Offer for a Portal

Cisco DNA Spaces enables you to remove a promotion from a portal after the required time line.
To delete a promotion from your portal, perform the following steps.

Step 1  Open the portal from which you want to delete the promotion.
Step 2  Click the Promos & Offers module.
The PROMOS & OFFERS window appears with the promotions added to that portal.
Step 3  Click the Delete icon that appears at the top right of the promotion that you want to delete.

Adding Custom Content and Menu Items to a Portal

The “Add Module” module enables you to add custom content and menu items in your portal according to your requirements. You can add various menu items to your portal that can be linked to different web pages.
The module enables you to add a label, icon, and web URL for each menu item. You can also enable a Back button, if the web page linked to is compatible.

To add a customized menu item to a portal, perform the following steps:

**Step 1**
Open the portal in which you need to add custom menu item.

**Step 2**
Click **Add Module**.

**Step 3**
Choose any of the following:

- **Custom Content**—To include additional customized text in the portal.
- **Menu Item**—To include Menu Items that links to a web page, in the portal.

The custom module gets added to the portal module list, and opens the page for it. The fields that appears for the custom module depends on custom module type.

**Step 4**
For “Custom Content”, enter the following details for the custom module.

- In the **HTML Module Name** field, enter a name for the module.
- In the Rich field, add the content.

**Step 5**
For **Menu Item** field, enter the following details for the custom module.

a) In the **Label** field, enter the label that must appear for the custom menu item.

   **Note** The Menu Item module name gets changed to the name you specify in the Label field.

b) In the Icon area, upload the icon that must appear adjacent to the menu item using the **Upload** button.

   **Note** You can delete the icon using the Delete icon.

c) In the **Link to URL** field, enter the URL to which the menu item is to link.

   **Note** You can enhance your URL using the smart link option. Click the **Add Variable** drop-down list to view the variables that you can add. For more information on creating a smart link, see the Smart Links and Text Variables for Captive Portals, on page 152.

**Step 6**
To enable a back button in the linked web page, check the **Enable Back button** check box.

**Step 7**
Click Save.

The customized content or menu item is successfully added to the portal.

---

**What to do next**

---

**Note** The menu items added appear as text in the preview of the portal, but appear as links in the runtime.
If you are modifying a portal that is already associated with a published captive portal, click the **Save and Publish** button to immediately publish the changes. The **Save and Publish** button appears only if the portal is associated with a captive portal rule. For more information on creating a captive portal rule, see Creating a Captive Portal Rule to Display Captive Portals, on page 113.

### Exporting a Portal

Cisco DNA Spaces enables you to export a portal created using the portal modules.

To export a portal, perform the following steps:

**Step 1** Open the portal that you want to export.

**Step 2** Click the **Export Portal** icon at the top of the **Portal** window.

The Export Portal dialog box appears.

**Step 3** Click **Download**.

**Step 4** In the window that appears, do any of the following:

a) To open the exported file directly, choose **Open**.

b) To save the portal file on your computer, choose **Save File**.

The portal zip file is saved in the “Downloads” folder on your computer.

**Note** The portal is exported in the zip format.

### Editing the Portal Style Sheet

The Style Sheet Editor option in Cisco DNA Spaces enables you to update the style sheet of a portal. This helps you to change the font properties and outlook of your portal.

To edit a portal style sheet, perform the following steps:

**Step 1** Open the portal of which you want to edit the style sheet.

**Step 2** Click **Stylesheet Editor** at the top of the **Portal** window.

**Step 3** In the **CSS Editor** tab, make necessary changes in the style sheet.

**Step 4** Click **Save**.

**What to do next**

You can upload the style sheet from an external source. For example, the CSS designed for another portal.

You can also download the style sheet to make necessary updates and upload the edited style sheet. For example, if you want a CSS designer to edit the portal, you can download the style sheet using the **Download** option.
Adding Assets to the Style Sheet

To improve the outlook of your portal, you can add assets such as images and fonts to the Stylesheet Editor of your portal. You can add image files such as jpeg, png, and tif. Edit your style sheet to incorporate these assets in the portal.

To add assets to a portal style sheet, perform the following steps:

Step 1: Open the portal of which you want to edit the style sheet.
Step 2: Click Stylesheet Editor.
Step 3: Click the Assets Library tab.
Step 4: Drag and drop the asset file, or upload it using the Choose File button.

The file gets added to the assets list.

What to do next

You can copy the URL of an asset using the Copy Asset url button displayed for an asset at the bottom of the asset. To add this asset in your portal, add the URL in the style sheet in the appropriate location.

You can delete an asset using the delete icon displayed for the asset in the assets list.

Importing a Portal

Cisco DNA Spaces enables you import a portal from an external path. For example, if you want to enhance a portal using an external application, you can export the portal using the Export Portal icon, make necessary enhancements, and import the portal file to Cisco DNA Spaces using the Import Portal option.

To import a portal, perform the following steps:

Step 1: In the Cisco DNA Spaces dashboard, choose Home.
Step 2: In the window that appears, click Captive Portal.
Step 3: In the Captive Portal window, choose Portal in the left pane.

The Captive Portal window appears.

Step 4: Click Import Portal at the top-right of the window.
Step 5: In the Import Portal window that appears, do the following:

a) In the Portal Name field, enter a file name for the portal.
b) Drag the drop the portal file to the window, or click the Choose file button, and choose the file that you want to import.
c) If you want this portal to be available for all the location, ensure that the Add all locations to this portal check box is checked. If you want the portal to be available only for the selected locations, uncheck the Add all locations to this portal check box, and select the locations for which the portal must be available.

The selected locations appear at the right side of the window.
Step 6  Click Import.

What to do next

Note  The portal is uploaded in the zip format.

Deleting a Portal

To delete a portal, perform the following steps:

Step 1  In the Cisco DNA Spaces dashboard, choose Home.
Step 2  In the window that appears, click Captive Portal.
Step 3  In the Captive Portal window, choose Portal in the left pane.
         The Captive Portal window appears with the list of available portals in Cisco DNA Spaces.
Step 4  Click the Delete icon that appears at the far right of the portal that you want to delete.
Step 5  In the Delete Portals window that appears, click Yes.
         The portal gets deleted from Cisco DNA Spaces.
Note  You can delete multiple portals simultaneously by selecting the check boxes adjacent to the portals that you want to delete, and clicking the Delete button that appears at the bottom of the window.
Note  You cannot delete a portal that is associated with a captive portal rule.

Editing a Portal

To edit a portal, perform the following steps:

Step 1  In the Cisco DNA Spaces dashboard, choose Home.
Step 2  In the window that appears, click Captive Portal.
Step 3  In the Captive Portal window, choose Portal in the left pane.
         The Captive Portal window appears with the list of available portals in Cisco DNA Spaces.
Step 4  Click the Edit icon that appears at the far right of the portal that you want to edit.
Step 5  Make necessary changes and save the changes made for each module.
Step 6  To publish the changes, click the Save and Publish button for the portal.
Editing the Locations for a Portal

To edit the locations for a portal, perform the following steps:

- **Step 1**: In the Cisco DNA Spaces dashboard, choose **Home**.
- **Step 2**: In the window that appears, click **Captive Portal**.
- **Step 3**: In the **Captive Portal** window, choose **Portal** in the left pane.
- **Step 4**: In the **Captive Portal** window that appears, check the check box for the portal for which you want to edit the locations.
- **Step 5**: Click **Add to Locations** that appears at the bottom of the window.
- **Step 6**: In the **Add Locations to Portals** window that appears, select the locations for the portal, and click **Save Changes**.
- **Step 7**: To publish the changes, click the **Save and Publish** button for the portal.

E-mailing a Portal Preview URL

You can e-mail the preview URL of a portal, so that the receiver can use this URL to preview the portal. To e-mail the preview URL of a portal, perform the following steps:

- **Step 1**: Open the portal of which you want to e-mail the preview URL.
  - The portal appears.
- **Step 2**: Click the **Link** icon in the **Portal Preview** area at the far right of the window.
- **Step 3**: In the **Email Portal URL** field, enter the e-mail ID to which you want to e-mail the portal preview URL.
- **Step 4**: Click **Send**.
  - A message appears stating the URL is sent to the e-mail address specified.

Previewing a Portal Using QR Code

Cisco DNA Spaces enables you to preview the portal using the QR code for a portal. To use this feature, you need to have a QR code reader app installed on your mobile.

To scan the QR code of a portal, perform the following steps:

- **Step 1**: Open the portal of which you want to scan the QR Code.
- **Step 2**: Click the **Link** icon in the **Portal Preview** area at the far right of the window.
- **Step 3**: Open the QR code reader app on your mobile.
- **Step 4**: In the portal, focus the mobile on the area labeled **Scan with QR code reader on your mobile device**.
  - The mobile scans the QR code and displays the message whether to open the URL.
- **Step 5**: Click **Ok**.
The portal is opened in your mobile screen.

---

**Previewing a Portal**

Cisco DNA Spaces enables you to view the outlook of the captive portal. Cisco DNA Spaces enables you to preview each module in the captive portal separately. The default preview is of the Captive Portal home screen. The preview of authentication module simulates the customer acquisition (runtime) flow. The preview of modules appear as carousels.

To preview a captive portal, perform the following steps:

**Step 1**
Open the portal of which you want to view the preview.

The preview of the portal home screen appears in the **Portal Preview** area.

**Step 2**
Click the right arrow to navigate to the next screen.

---

**Previewing the Portal in Various Devices**

Cisco DNA Spaces enables you to view the outlook of the captive portal in various devices. You can preview the portals for mobile, tablets, and laptops. Cisco DNA Spaces enables you to preview each module in the captive portal separately. The default preview is of the Captive Portal home screen.

To preview a captive portal for a device, perform the following steps:

**Step 1**
Open the portal of which you want to view the preview in various devices.

The preview of the portal home screen appears at the devices are displayed in the right side of the portal. The **CSS Editor** window appears with device preview in the right pane.

**Step 2**
Do any of the following:
- **a)** To view the preview of the portal for mobile, click the tab for the mobile.
- **b)** To view the preview of the portal for tablet, click the tab for the tablet.
- **c)** To view the preview of the portal for laptop, click the tab for the laptop.

The preview of the captive portal home page for the selected device appears.

**Step 3**
To preview a particular module in the captive portal, from the adjacent drop-down list, select the module.

**Note**
In the preview window, to view the preview of other devices, click the corresponding tabs. You can also scan the QR code, e-mail the portal URL, and change the orientation from the preview window.
Display, Hide or Reorder the Modules in a Captive Portal

The portal administrators can display or hide a module added to a portal by switching the ON/OFF toggle switch at the top left of the module. To reorder the modules, drag and drop the modules to the required location. The preview section reflects the changes.

Captive Portal Rule

The Captive Portal Rule enables you to manage the captive portal display and internet provisioning for the customers connecting to your SSIDs.

Using a Captive Portal Rule you can manage the captive portal display and internet provisioning in the followings ways:

• **Show Captive Portal**—When a customer filtered for the rule connects to the SSID configured for the rule, a captive portal is displayed. The customer can access the internet by clicking any menu item in the portal after completing the required authentication steps. You can configure to show different captive portals to the customers that suits them based on their location, number of visits, tags they belong to, number of visits made in your location, duration of their visits, and so on. You can restrict the duration for which internet must be provided for each session. Also, you can define the bandwidth required for the internet for this captive portal rule.

• **Direct Internet Access**—When a customer filtered for the rule connects to the SSID configured for the rule, the internet is provisioned immediately without any authentication process. The captive portal is not shown in this case.

• **Deny Internet Access**—When a customer filtered for the rule tries to connect to the SSID, connection cannot be established as internet is denied.

In addition, the Captive Portal rule enables you to do the following:

• Create tags or modify existing tags based on rule filtering.

• Send the details of the customers that are signed in to the captive portal to an external API.

In a Captive Portal rule, you can configure the actions to be performed, when the conditions defined are met. You can filter the customers for the rule based on various parameters such as locations, tags, number and duration of visits of the customers, app status, and so on.

This chapter describes how to create the captive portal rules.

Prerequisites for Creating a Captive Portal Rule

• To specify the locations for which the captive portal rule is applicable, you must define the location hierarchy. For more information on defining the location hierarchy, see the “Overview of Location Hierarchy” section.

• For the **CMX On Prem** option, ensure that all the required APs are added to the Cisco CMX.

• To specify the SSID for which you want to display the captive portal, you must import the SSIDs created in your wireless network system to Cisco DNA Spaces. For more information on importing the SSIDs, see the Importing the SSIDs from a Wireless Network, on page 121.
• To display a captive portal based on the captive portal rule, you must create the portal. For more information on creating the captive portal, see the Creating and Managing Portal, on page 81.

• To specify the tags for which the rule is applicable, you must define the tags. For more information on creating the tags, see the "Creating or Modifying Tags Using a Location Personas App" section.

• To send to an external API the details such as first name, last name, and so on of the customers who have signed into the captive portal, you must configure the Data Capture form in the captive portal. Without the Data Capture form, only the information such as device mac address will be sent to the external API. For more information on configuring a data capture form, see the Adding a Data Capture Form to a Portal, on page 95.

• RADIUS authentication is highly recommended for captive portals. RADIUS authentication is mandatory for **Seamlessly Provision Internet**, **Deny Internet**, and for extending Session Duration and Bandwidth. To manage internet provisioning and RADIUS authentication, do the required configurations in your wireless network.

  • If your wireless network is Meraki, do the configurations mentioned in Configuring Cisco Meraki for RADIUS Authentication, on page 244.

  • If your wireless network is CUWN (Cisco AireOS), do the configurations mentioned in Configuring Cisco Wireless Controller for Internet Provisioning and RADIUS Authentication, on page 208.

### Creating a Captive Portal Rule to Display Captive Portals

Before creating a captive portal rule, ensure that all the prerequisites are met. To know the prerequisites for creating a captive portal rule, see the Prerequisites for Creating a Captive Portal Rule, on page 112.

You can filter the customers for whom you want to apply the rule based on their location, whether the customer is an opted in or not opted in user, the tags the customers belong to, first time or repeat user, the number of visits made by the customer and so on. You can filter the locations in which the rule is to be applied based on the locations or the metadata associated with the locations. You can also apply the rule based on the number of visits made by the customer to the specified locations during the specified time. You can also configure to apply the rule only during a particular time with in a particular period, and only for certain days of a week.

The Captive Portal Rule also allows you to configure to provide direct internet connection when the customers filtered for the rule connects to your SSID. In this case, the captive portal is not displayed, but the customer will get access to the internet. You can also configure to deny the internet access to the customers filtered for a Captive Portal Rule.

Using a Captive Portal Rule, you can create new tags or modify existing tags with the customers filtered for the rule. The Captive Portal Rule also allows you send the details of the customers, connected to the SSID configured for the rule, to an external API.

---

**Note**

If Cisco Wireless Controller is connected through Cisco CMX, ensure that all the required APs are added to the Cisco CMX for the Captive Portal rules to function. After defining the location hierarchy, if you are adding new APs to the Cisco CMX, the newly added APs get automatically displayed in the location hierarchy.

---

To create a captive portal rule to show a portal, perform the following steps:
Creating a Captive Portal Rule to Display Captive Portals

**Step 1**  
In the Cisco DNA Spaces dashboard, click the Captive Portal app.

**Step 2**  
In the Captive Portal window that appears, Click Captive Portal Rule in the left pane of the dashboard.

**Step 3**  
Click Create New Rule on the far right of the window.

**Step 4**  
In the Rule Name field, enter a name for the captive portal rule.

**Step 5**  
In the Sense area, perform the following steps:

a) From the drop-down list after When a user is on WiFi, choose WiFi.

b) From the drop-down list after and connected to, choose the SSID for which you want to apply the rule.

   **Note**  
   The SSIDs are available for selection only if you have imported/configured the SSIDs. If the required SSID is not imported/configured, you can import/configure it using the Configure SSID button listed in the drop-down list. When you select the Configure SSID button, you are redirected to the Import/Configure SSID window. For more information on importing/configuring the SSIDs, see the Importing the SSIDs from a Wireless Network, on page 121.

**Step 6**  
In the Locations area, specify the locations for which you want to apply the rule.

You can configure to apply the rule for the entire location hierarchy, or a single or multiple locations such as group, floor, or zone. You can add the locations of both Meraki and CUWN in a Captive Portal rule. For more information on creating the location hierarchy, see the Defining the Location Hierarchy section.

You can again filter the locations based on the metadata defined for the selected location, or its parent or child locations. For more information on configuring the metadata for the locations, see the “Defining or Editing Metadata for a Location” section. You can either apply the rule for the locations with a particular metadata or exclude the locations with a particular metadata. For more information on filtering the locations, see the Filtering by Location, on page 137.

**Step 7**  
In the IDENTIFY area, specify the type of customers for whom you want to apply the rule.

**Note**  
You can filter the customers for whom you want to apply the rule based on the on-boarding status of the customer, whether the customer is an opted in or not opted in user, the tags the customers belong to, and the number of visits made by the customer. You can apply all these filters or any of them based on your requirement.

To specify the customers for whom the Captive Portal rule is to apply, perform the following steps:

a) If you want to filter the customers based on the on-boarding status of the customer, check the “Filter by On boarding Status” check box. If you want to filter the on-boarded customers (the customers who have completed the authentication process) for the rule, click the Onboarded Visitor radio button. If you want to filter the customers who have not on-boarded (the customers who have not completed the authentication process) for the rule, click the Not Onboarded Visitor radio button.

b) If you want to filter the customer by the Opt In Status, check the Filter by Opt-In Status check box, and specify whether you want to filter the opted in users or not opted in users. For more information on opted in users, see the “Opted In Option for Users” section on page 6-5.

c) If you want to filter the customers based on tags, check the Filter by Tags check box.

   **Note**  
   You can filter the tags in two different ways. Either you can specify the tags for which the rule must be applied or you can specify the tags for which the rule must not be applied. You can choose the best filtering method based on your requirement. For example, if you want to apply the rule for the customers in all the tags except for one tag, it is easy to opt the exclude option, and mention that particular tag for which you do not want to apply the rule.

   - To include the tags so that the rule is applied to the customers in the selected tags, use the Add Tags button for Include.
• To not apply the rule to the customers in the tags that are excluded, use the Add Tags button for Exclude.

For more information on using the tag filter, see the “Filtering by Tag” section.

d) If you want to filter the customers based on the number of visits made by the customer in the selected locations, check the Filter by Previous Visits check box.

Click the Add Locations button. In the Choose Locations window, specify the locations of which the customer visit needs to consider for filtering. In the following fields, mention the number of visits and duration for filtering. For more information on the visits and duration that you can configure, see the “Previous Visit Criteria” section.

Step 8

In the Schedule area, specify the period for which you want to apply the rule.

a) Check the Set a date range for the rule check box, and in the fields that appear, specify the start date and end date for the period for which you want to apply the captive portal rule.

b) Check the Set a time range for the rule check box, and in the fields that appear, specify the time range for which you want to apply the captive portal rule.

c) If you want to apply the rule only on particular days, check the Filter by days of the week check box, and from the list of days that appears, click the days on which you want to apply the rule.

Step 9

In the Actions area, configure the actions to be performed when the preceding conditions are met:

a) To manage the internet provisioning for the customers filtered for the rule, choose the required option from the following:

• Show Captive Portal—Choose this option to display a captive portal when the customers filtered for the Captive Portal rule connects to the SSID configured for the rule. From the Select Captive Portal drop-down list, choose the captive portal that you want to show when the conditions defined in this rule are met.

Note The portals that you have created for the chosen locations are available for selection. If you have not created the required portal, you can create it using the Create Portal button that is available in the Select Captive Portal drop-down list. When you select the Create Portal button, you are redirected to the Create Portal window. For more information on creating a portal, see the Creating a Portal, on page 82.

• If you want to limit the period for which internet is to be provided for a session, check the Session Duration check box, and in the field that appears enter the session duration. You can specify the session duration in minutes, hours, or days.

• If you want to restrict the bandwidth for the internet provided for the customers based on this captive portal rule, check the Bandwidth check box, and in the bandwidth bar that appears, specify the bandwidth. You can define the bandwidth within a range of 1 kbps and 1 tbps.

Note The session duration defined here overrides the session expiry configuration in your wireless network such as CUWN or Meraki. So, you can define more session duration for a captive portal than the one configured in your wireless network using this option.

• Seamlessly Provision Internet: Choose this option if you want to provide internet to your customers immediately after they connect to your SSID. In this case, the customer does not have to complete any authentication steps. To use this option, you must do certain configurations in your wireless network such as CUWN or Meraki as mentioned in the Prerequisites for Creating a Captive Portal Rule, on page 112. The data that is to be entered for this option depends on your wireless network.

• In the Rule/Policy Name field, enter a name for the policy. You must specify the same name that you have defined in the Wireless Network.

Note This field is not required for the CUWN.
To specify the session duration, check the Session Duration check box, and in the **Enter Session Duration** field, mention the duration for which you want to provide the internet access for each connection.

To specify the bandwidth, check the Bandwidth the Limit check box, and specify the bandwidth using the bandwidth bar that appears. You can specify a maximum bandwidth of 1 tbps.

**Note**  
The bandwidth field is not required for Meraki as the bandwidth configured in Meraki will be considered.

**Deny Internet**: Choose this option if you want to deny the internet to the customers filtered for the rule when they try to connect to your SSID. In this case, the customers are not allowed to connect to the SSID.

b) To create a tag for the customers who are filtered based on this captive portal rule or to add or remove the filtered customers from an existing rule, click the **Add Tags** button. For more information on using the tag filter, see the “Filtering by Tag” section.

c) If you want to send to an external API the details such as first name, last name, mobile number, and so on of the customers who have signed up to the captive portal configured for this rule, check the **Trigger API** check box, and do the necessary API configurations. For more information on API configurations, see **Trigger API Configuration for Notification**.

**Note**  
The summary of the rule is shown on the right side of the window.

**Step 10**  
Click **Save and Publish**.

The rule gets published and listed in the **Captive Portal Rules** window.

**Note**  
If you do not want to publish the rule now, you can click the **Save** button. You can publish the rule at any time later by opening the rule, and clicking the **Save and Publish** button. Also, you can publish the rule by clicking the **Make Rule Live** icon at the far right of the rule in the **Captive Portal Rules** window.

**Use Case: Captive Portal Rule**

XYZ is a business group that is engaged in different stream lines of business from mobile stores to supermarkets. XYZ has 5 mobile stores and 4 supermarkets at various locations in New York. The SSID name of XYZ in New York is XYZID. XYZ wants to show a captive portal C1, that displays the offers available for various items in the supermarket, when the customers connect to XYZID from XYZ’s supermarkets. Similarly, a captive portal, C2, must be shown to customers who connect to the XYZID from XYZ’s mobile stores. The captive portal must be shown to the users that are not opted in.

**Locations with super markets**: L1, L2, L3, L4, L5

**Locations with mobile stores**: L7, L8, L9, L10

To achieve the preceding scenario, perform the following steps:

**Step 1**  
In the Cisco Wireless Controller, define the mode for access points, create the ACLs, and create the SSID, XYZID. For more information on the Cisco Wireless Controller configurations, see the **Importing the SSIDs for Cisco Meraki**, on page 122.

**Step 2**  
Log in to Cisco DNA Spaces.

**Step 3**  
Add XYZID to Cisco DNA Spaces using the Import SSID option.

**Step 4**  
Create the location hierarchy for XYZ. In the location hierarchy, all the supermarkets and mobile store of XYZ in New York must be defined as locations under the location, New York. Add a location metadata for the locations L1, L2, L3,
L4, and L5 with key as StoreType and value as SM. Add a location metadata for the locations L7, L8, L9, and L10 with key as StoreType and value as MS. For more information on defining the location metadata, see the “Defining or Editing Metadata for a Location” section.

**Step 5** Create portal C1 for super market and portal C2 for mobile stores. For more information on creating the portals, see the Creating a Portal, on page 82.

**Step 6** In the Cisco DNA Spaces dashboard, choose Home.

**Step 7** In the window that appears, choose Captive Portal.

**Step 8** In the Captive Portal window, choose Captive Portal Rule in the left pane.

**Step 9** Click Create New Rule.

**Step 10** In the RULE NAME enter the name, R1, for the captive portal rule.

**Step 11** From the When a user is on drop-down list, choose WiFi, and from the add Connected to drop-down list, choose XYZID.

**Step 12** In the Locations area, perform the following steps:

- a) Click the Add Locations button, and in the Choose Locations window that appears, select the location for New York, and click Ok.
- b) Check the Filter by metadata check box, and click the Add Metadata button for Filter.
- c) In the Choose Location Metadata window, choose the key, StoreType, and choose the value SM.

  **Note** As the location metadata StoreType is defined for the locations that are under the location New york, it will be available for selection in the Choose Location Metadata window.

**Step 13** In the Identify area, check the Filter by Opt-In Status check box, and choose Only for not opted-in Visitor.

**Step 14** In the Schedule area, check the Set a date range for the rule check box, and specify the start date as today’s date and end date as last date of this year.

**Step 15** In the Actions area, choose Show Captive Portal, and from the Select Captive Portal drop-down list, choose C1.

**Step 16** Click Save and Publish.

The rule gets published.

**Step 17** Similarly, create another rule, R2, for the Mobile Group, with the location metadata key as StoreType and value as MS, and the captive portal, C2.

Now, when a customer visits XYZ’s super market and connects to XYZID, C1 is shown. When the same customer connects to XYZID from XYZ’s mobile store, C2 is shown.

---

### Reports

Cisco DNA Spaces provides the following captive portal reports:

By default, the report is provided for all the location for the last one year. You can filter the location and duration for the report.

To view the report, click Reports on the left pane of the Captive Portal window.
Device Onboarding

The Device Onboarding report provides information about the devices that have connected to your SSIDs. If a customer is connecting to your SSID from more than one device, each such device is counted to calculate the number of devices.

Onboarding Journey

This section displays the count of unique devices for the selected location and period.

- **Connected to SSID**—The total number of unique devices that have connected to your SSIDs from the selected location during the time period specified.

- **Shown Captive Portal**—The total number of unique devices that have connected to your SSIDs, and got the captive portal loaded successfully, from the selected location during the time period specified.

- **Provisioned Internet**—The total number of unique devices that got internet provisioned from the selected location during the specified period. This metrics for all the locations from the date of deployment of Cisco DNA Spaces is shown at the top of the report for **Total Unique Devices Provisioned Internet**.

Daily Trend: New v/s Returning Devices Connected to the SSID

This section displays the daily trend of the new and returning unique devices that have connected to your SSIDs from the location for the specified time period.

- **New Devices**—The total number of new unique devices that have connected to your SSIDs from the selected location during the specified time period. The percentage of new unique devices out of the total number of devices is also shown.

- **Returning Devices**—The total number of unique devices that have connected to your SSIDs from the selected location more than once during the specified period. The percentage of unique returning devices out of the total number of unique devices connected is also shown.

The graph represents the unique New v/s Returning devices connected from the selected location on each day of the specified period. X-axis of the graph represents the days in the selected period, and Y-axis represents the number of unique devices. The color indicators for new and returning unique devices are displayed at the top of the graph.

Menu Button Clicks in Captive Portal

This section displays the details of daily engagements of customers through promotions and offers. Daily engagement through promotions and offers is calculated based on the menu buttons that the customers have clicked during the specified period.

- **Menu buttons**—The total number of menu buttons that were clicked at least once from the selected location during the specified period.

- **Clicks**—The total number of clicks made in the captive portals from the selected location during the specified period.
Customer Acquisition

This report provides insights on the unique customers acquired newly from the selected location during the specified period, and the data (personal and demographic) collected from the acquired customers.

If a new customer connects to your location using multiple devices, and uses the same personal identity (mobile number, e-mail, or social ID), the customer is counted only once.

Customer Acquisition

This report will not count the customers who are acquired through the authentication types, "No Authentication" and "Access Code".

- **New Devices Connected to SSID**: The total number of new unique devices that have connected to your SSIDs from the selected location during the specified time period. The percentage of new unique devices out of the total number of devices is also shown.

- **New Customers Identified**: The total number of unique new customers that got acquired through any of personal identifiers such as mobile number, e-mail, or social ID from the selected location during the specified period. The percentage of new unique customers acquired out of the total new unique devices connected is also shown. This metrics for all the locations from the date of installation of Cisco DNA Spaces is shown at the top of this report for “Customers Identified”.

- **Customers Opted In**: The total number of “unique new customers acquired” who have opted in for subscription from the selected location during the specified period. The percentage of opted-in “unique new customers acquired” out of the total number of “unique new customers acquired” is also shown. For more information on opted-in users, see the “Opted In Option for Users” section.

- **Completed Data Capture**: The total number of “unique new customers acquired through any of personal identifiers such as mobile number, e-mail, or social ID”, and have completed the data capture form from the specified location during the specified period. The percentage of “unique new customers acquired” who have completed the data capture out of the total number “unique new customers acquired” is also shown.

Daily Customer Acquisition

This section displays a bar graph that shows the count of “unique new devices connected to your SSIDs” and “unique new customers acquired through any of personal identifiers such as mobile number, e-mail, or social ID”, from the selected location during the specified period. It also shows the daily count of “unique new customers acquired” who have opted-in for subscription and completed the data capture. X-axis represents the days in the selected period. Y-axis represents the count. The color indicators are shown at the top of the graph. Mouse-over the graph to view the count for a particular day.

This report will not count the customers who are acquired through the authentication types, “No Authentication” and “Access Code”.

Note

This report will not count the customers who are acquired through the authentication types, “No Authentication” and “Access Code”.
Captured Data

This section displays the number of e-mail addresses, phone numbers, names, gender details, and so on captured from the selected location during the specified period.

- **Phone Number**—The total number of unique phone numbers captured from the specified location during the specified period.

- **Emails**—The total number of unique e-mail addresses captured from the specified location during the specified period.

- **Social ID**—The total number of unique social IDs captured, through social authentication, from the specified location during the specified period.

- **Names**—The total number of customers/devices from which the names (first name/last name) are captured from the specified location during the specified period.

- **Gender**—The total number of customers/devices from which gender is captured from the specified location during the specified period.

Customer Distribution

This section displays the profile details such as country, gender, and language captured newly from the selected location during the specified period.

**Countries**: Displays a pie chart with the percentage of customers from different countries out of the total number of customers for whom the country data is collected. The total number of countries is displayed at the center of the pie chart. The countries with highest number of customers are displayed below the pie chart with the count of customers. You can view all the countries, with at least one customer, by clicking the “Show All” button. Country names are derived based on the country code of the phone numbers specified during the authentication process.

**Languages**: Displays a pie chart with the percentage of customers who used various languages out of the total number of customers for whom the language data is collected. The languages that are used the most by customers are displayed below the pie chart with the count of customers. You can view all the languages, used at least by one customer, by clicking the “Show All” button. Language count is derived based on the language selected by the customer in the captive portal.

**Gender**: Displays a pie chart with the percentage of male, female, and "gender not specified" customers out of the total number of customers. The total percentage of the customers that has provided the gender details is displayed at the center of the pie chart. The count of the male, female, and unknown gender customers are displayed at the bottom of the pie chart.

SSIDs

The SSID refers to wireless network ID your customers connect to access the internet. You might be having multiple SSIDs for your business locations. Cisco DNA Spaces allows to display different captive portals for same SSID or various SSIDs in your business locations based on your requirement.

The SSIDs are defined in the Wireless Network System. For example, Cisco Wireless Controller for Cisco Unified Wireless Network. To define the captive portals to be displayed for an SSID, you must import the SSID to Cisco DNA Spaces.
The imported SSIDs will be shown in grid view. Each Meraki SSID will have a “Detail” link using which you can configure the SSID in Meraki. If required, you can delete the imported SSID for a wireless network from the grid.

The Configure Manually link for a SSID leads you to the manual configuration instructions for the corresponding wireless network. For example, the “Configure Manually” link for the Meraki SSIDs lead to the configuration instructions for Cisco Meraki.

Prerequisites for Importing or Configuring the SSIDs

To import/configure the SSIDs to Cisco DNA Spaces, you must do the following:

- Create the location hierarchy. For more information on creating the location hierarchy, see the “Overview of Location Hierarchy” section.
- Create the SSIDs in the Wireless Network System.
  - For creating the SSIDs for the CUWN, see the Configuring Cisco Wireless Controllers and Cisco Catalyst 9800 Series Controllers for Cisco DNA Spaces, on page 197 chapter.
  - For creating the SSIDs for Meraki, see the Enabling SSIDs in Cisco Meraki, on page 244 section.
- For Meraki, to import the SSIDs, Cisco DNA Spaces and Meraki must be connected. The connection is usually established when defining the location hierarchy. You can also connect to Meraki using the Wi-Fi icon at the top right of the Cisco DNA Spaces dashboard.

Importing the SSIDs from a Wireless Network

Before trying to import an SSID, ensure that the prerequisites are met. For more information on the prerequisites to import an SSID, see the Prerequisites for Importing or Configuring the SSIDs, on page 121.

Note

To create a captive portal rule for an SSID, you must import that SSID from the CUWN or Meraki.

For CUWN, you must manually import the SSIDs.

Importing the SSIDs for Cisco Wireless Controller or Cisco Catalyst 9800 Series Wireless Controller

Note

For Cisco Wireless Controller or Cisco Catalyst 9800 Series Wireless Controller, you must manually add the SSIDs to Cisco DNA Spaces. The SSID name you specify in Cisco DNA Spaces must match with the SSID name configured in the Controller. You can view the SSID name in the Controller dashboard.

Note

For Cisco Wireless Controller or Cisco Catalyst 9800 Series Wireless Controller with CMX, the SSIDs are configured in the Cisco Wireless Controller, not in the Cisco CMX.
To manually import the SSIDs to Cisco DNA Spaces, perform the following steps:

**Step 1** In the Cisco DNA Spaces dashboard, choose **Home**.

**Step 2** In the **My Apps** area, click **Captive Portal**.

**Step 3** In the **Captive Portal** window that appears, choose **SSIDs** in the left pane.

**Step 4** Click **Import/Configure SSID**.

**Step 5** In the **Import/Configure SSID** window that appears, from the **Wireless Network** drop-down list choose **CUWN (CMX/WLC)**.

**Step 6** In the **SSID** field, enter the name of the SSID you want to import, and click **Add**.

The imported SSID appears in the **SSID**s window.

---

**What to do next**

**Note** As Cisco DNA Spaces needs to synchronize with the Controller to load the imported SSIDs, you may need to refresh the window to view the imported SSIDs.

---

**Importing the SSIDs for Cisco Meraki**

To create the Captive Portal rules for an SSID of Meraki, you must import that SSID from the Meraki network. After importing the SSIDs, in the Meraki dashboard, you must configure the SSID for working with Cisco DNA Spaces.

**Note** You can import the SSIDs only for those locations that are imported to the location hierarchy.

To import the SSIDs, perform the following steps:

**Step 1** In the Cisco DNA Spaces dashboard, choose **Home**.

**Step 2** In the **My Apps** area, click **Captive Portal**.

**Step 3** In the **Captive Portal** window that appears, choose **SSIDs** in the left pane.

**Step 4** Click **Import/Configure SSID**.

**Step 5** In the **Import/Configure SSID** window that appears, from the **Wireless Network** drop-down list, choose **Meraki**.

**Step 6** From the Organization drop-down list, choose the organization of which you want to import the SSID.

The SSIDs enabled in Meraki for the selected organization are available for selection.

**Step 7** Check the check box for the SSID that you want to import, and click **Import**.

The imported SSID appears on the **SSID**s window.

**Step 8** In the grid for that SSID, click the **Detail** link.
Step 9  On the window that appears, click **Activate** for the SSID to update the Cisco DNA Spaces configurations for the SSID in Meraki.

The **SSID Configuration Sync** window appears with the SSID updates that need to be configured in Meraki.

Step 10  Click **Update**.

**Note**  You can manually also configure the SSIDs in Meraki. To know how to manually configure the SSIDs in Meraki, see the “Manually Configuring SSIDs for Cisco Meraki” section.

---

### What to do next

**Note**  As Cisco DNA Spaces needs to synchronize with the Meraki network to load the imported SSIDs, you may have to refresh the window to view the imported SSIDs.

---

### Access Codes

Cisco DNA Spaces enables you to control the internet provisioning in your business premises using access codes. You can create access codes for your various locations and restrict the internet access for these locations using the access codes. That is, the customers can access the internet only after providing an access code configured for that location. This section describes how to create and manage the access codes using Cisco DNA Spaces.

To use this feature, you must configure access code authentication for your captive portals. For more information on configuring access code authentication for captive portals, see [Configuring a Portal for Access Code Authentication](#), on page 93.

Cisco DNA Spaces enables you to share with the customers the access codes that you have created. You can specify the validity period for an access code. You can configure to have a single code value for an access code, or to change the code value weekly or monthly. You can manually specify the code values for an access code or choose to auto-generate. You can define the time for which the customers can access the internet using an access code. Cisco DNA Spaces also enables you set the download and upload bandwidth limits for access codes, when accessing the internet using a particular access code.

You can define multiple access codes for a single location. For example, if you want to provide a high speed internet only for your platinum members, you can create an access code with maximum bandwidth and create another access code with limited bandwidth. You can then share the access codes based on the type of the customer.

To know the authentication steps for an access code authentication, see [Steps for Access Code Authentication](#), on page 149.
Creating an Access Code

To create an access code, perform the following steps:

Step 1
In the Cisco DNA Spaces dashboard, click Captive Portals.

Step 2
In the window that appears, click the three line menu icon in the top left of the window.

Step 3
Click Access Code.

Note
The Access Code option will be available in the Cisco DNA Spaces dashboard only if you are a Cisco DNA Spaces Account Admin or Access Code Manager user. For more information on creating a Cisco DNA Spaces user, see the Inviting a Cisco DNA Spaces User, on page 191.

Step 4
From the drop-down list, choose the location for which you want to define the access code.

Step 5
Click Create Access Code.

Step 6
In the Create Access Code window, choose the type of access code that you want to create.

• Fixed: The code value remains the same till the time the access code is valid.
• Weekly: The code value for the access code changes every week
• Monthly: The code value for the access code changes every month.

The remaining fields that appear depends on the access code type that you have selected.

If you choose the access code type as Fixed, enter the following details:

a) In the Access Code Name field, enter a name for the access code.
b) If you want to define your own code values for the access code, check the Set your own access code? check box.
c) In the Access Code field that appears, enter the code value.
d) Specify the time for which the customer could access the internet using the access code by adjusting the Limit session by time bar. This time is for a single session.
e) If you want to define a validity period for the access code, check the Define a validity period for this access code check box. Specify the start date and end date by clicking the respective buttons.
f) If you want to limit the bandwidth when the customer accesses the internet using this access code, check the Limit bandwidth check box.
g) Specify the maximum bandwidth that must be provided to the customer when accessing the internet using this access code by adjusting the Bandwidth Limit bar.
h) Click the Show More link, and specify the upload and download limits.
i) From the Number of times access code can be used drop-down list, choose the maximum number of times a customer can access the internet using this access code.
If you choose the access code type as **Weekly**, enter the following details:

a) In the **Access Code Name** field, enter a name for the access code.
b) Specify how to generate the access code.

- If you want to specify your own code values for all the weeks, check the **Upload access codes from the csv file** check box. You can download the access code template by clicking the link in the message box. After entering all the code values for all the required weeks in the template, you can upload the template as a csv file using the **Upload** button.

- If you want to generate the code values for all the weeks automatically, specify the period for which this access code is valid in weeks by adjusting the “Access Code Validity time period” bar.

**Note**  
The **Access Code Validity time period** bar will be available only if you have not selected the **Upload access codes from the csv file** check box. If you have selected the **Upload access codes from csv File** check box, the validity period is considered based on the number of code values entered in the csv file. For example, if you define three code values in the csv file, then the access code is valid for three weeks. The code values mentioned in the csv file are considered sequentially for each week.

c) Specify the time for which the customer could access the internet using the access code by adjusting the **Limit session by time** bar. This time is for a single session.
d) Click the **Start Date** button, and specify the date from which the access code is valid.
e) If you want to limit the bandwidth when the customer accesses the internet using this access code, check the **Limit bandwidth** check box.
f) In the **Bandwidth limit** bar that appears, specify the maximum bandwidth that must be provided to the customer when accessing the internet using this access code by adjusting the bar.
g) Click the **Show More** link and specify the upload and download limits.
h) From the **Number of times access code can be used** drop-down list, choose the maximum number of times a customer can access the internet using this access code.

If you choose **Monthly**, enter the following details:

a) In the **Access Code Name** field, enter a name for the access code.
b) Specify how to generate the access code.

- If you want to specify your own code values for all the months, check the **Upload access codes from the csv file** check box. You can download the access code template by clicking the link in the message box. After entering all the code values for all the required months in the template, you can upload the template as a csv file using the **Upload** button.

- If you want to generate the code values for all the months automatically, specify the period for which this access code is valid in months by adjusting the **Access Code Validity time period** bar.

**Note**  
The **Access Code Validity time period** bar will be available only if you have not checked the **Upload access codes from csv File** check box. If you have checked the **Upload access codes from the csv file** check box, the validity period is considered based on the number of code values entered in the csv file. For example, if you define three code values in the csv file, then the access code is valid for three months. The code values mentioned in the csv file are considered sequentially for each month.

c) Specify the time for which the customer could access the internet using the access code by adjusting the **Limit session by time** bar. This time is for a single session.
d) Click the **Start Date** button, and specify the date from which the access code is valid.
e) If you want to limit the bandwidth when the customer accesses the internet using this access code, select the Limit bandwidth check box.

f) In the Bandwidth limit bar that appears, specify the maximum bandwidth that must be provided to the customer when accessing the internet using this access code by adjusting the bar.

g) Click the Show More link, and specify the upload and download limits.

h) From the Number of times access code can be used drop-down list, choose the maximum number of times a customer can access the internet using this access code.

Step 7 Click Create.

---

**Viewing an Access Code**

You can view all the access codes for a location of which the validity period has not yet expired.

To view the access codes defined for a location in the Cisco DNA Spaces, perform the following steps:

---

**Step 1** In the Cisco DNA Spaces dashboard, click Captive Portals.

**Step 2** In the window that appears, click the three line menu icon in the top left of the window.

**Step 3** Click Access Code.

**Note** The Access Code option will be available in the Cisco DNA Spaces dashboard only if you are a Cisco DNA Spaces Account Admin or Access Code Manager user. For more information on creating a Cisco DNA Spaces user, see the Inviting a Cisco DNA Spaces User, on page 191.

**Step 4** In the Access Code window that appears, from the drop-down list, choose the location for which you want to view the access codes.

The access codes defined for the location appear.

For the location selected, the total number of access codes available, the total number of expired access codes, and number of active and inactive access codes among them are displayed.

In addition, the following details of the access codes defined for the location are displayed:

- **Status**: Whether the access code name is active or not.
- **Name**: The name of the access code.
- **Code**: The code value for the access code name at the time of viewing the access code. The code value changes if it is set to change weekly or monthly.
- **Type**: The access code type. The access code type can be fixed, or that changes weekly or monthly.
- **Expiry Date**: The period for which the access code is valid.
- **Actions**: The actions such as edit, share, and delete that you can perform for an access code.
Editing an Access Code

To edit an access code, perform the following steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the Cisco DNA Spaces dashboard, click Captive Portals.</td>
</tr>
<tr>
<td>Step 2</td>
<td>In the window that appears, click the three line menu icon in the top left of the window.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click Access Code.</td>
</tr>
</tbody>
</table>

**Note** The Access Code option will be available in the Cisco DNA Spaces dashboard only if you are a Cisco DNA Spaces Account Admin or Access Code Manager user. For more information on creating a Cisco DNA Spaces user, see the Inviting a Cisco DNA Spaces User, on page 191.

<table>
<thead>
<tr>
<th>Step 4</th>
<th>In the Access Code window that appears, select the location for which you want to edit the access code. The access codes defined for that location appear.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 5</td>
<td>In the Active Access Codes area, for the access code that you want to edit, click the Edit button.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Make necessary changes, and click Update.</td>
</tr>
</tbody>
</table>

Sharing an Access Code

The Cisco DNA Spaces enables you to share the access codes with your customers.

To share an access code, perform the following steps:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In the Cisco DNA Spaces dashboard, click Captive Portals.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>In the window that appears, click the three line menu icon in the top left of the window.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click Access Code.</td>
</tr>
</tbody>
</table>

**Note** The Access Code option will be available in the Cisco DNA Spaces dashboard only if you are a Cisco DNA Spaces Account Admin or Access Code Manager user. For more information on creating a Cisco DNA Spaces user, see the Inviting a Cisco DNA Spaces User, on page 191.

<table>
<thead>
<tr>
<th>Step 4</th>
<th>In the Access Code window that appears, select the location for which you want to share the access code. The access codes defined for that location appear.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 5</td>
<td>In the Active Access Codes area, for the access code that you want to share, click the Share button.</td>
</tr>
<tr>
<td>Step 6</td>
<td>In the Share Access Code window that appears, enter the e-mail ID of the person to whom you want to share the access code, and click Invite.</td>
</tr>
</tbody>
</table>

Deleting an Access Code

To delete an access code, perform the following steps:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In the Cisco DNA Spaces dashboard, click Captive Portals.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>In the window that appears, click the three line menu icon in the top left of the window.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click Access Code.</td>
</tr>
</tbody>
</table>

**Note** The Access Code option will be available in the Cisco DNA Spaces dashboard only if you are a Cisco DNA Spaces Account Admin or Access Code Manager user. For more information on creating a Cisco DNA Spaces user, see the Inviting a Cisco DNA Spaces User, on page 191.

<table>
<thead>
<tr>
<th>Step 4</th>
<th>In the Access Code window that appears, select the location for which you want to delete the access code. The access codes defined for that location appear.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 5</td>
<td>In the Active Access Codes area, for the access code that you want to delete, click the Delete button.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Make necessary changes, and click Update.</td>
</tr>
</tbody>
</table>
Deactivating an Access Code

To deactivate an access code, perform the following steps:

Step 1 In the Cisco DNA Spaces dashboard, choose **Home**.
Step 2 Click **Captive Portals**.
Step 3 In the window that appears, click **Access Code** in the left pane.

**Note** The Access Code option will be available in the Cisco DNA Spaces dashboard only if you are a Cisco DNA Spaces Account Admin or Access Code Manager user. For more information on creating a Cisco DNA Spaces user, see the Inviting a Cisco DNA Spaces User, on page 191.

Step 4 In the Access Code window that appears, select the location for which you want to deactivate the access code.

The access codes defined for that location appear.

Step 5 In the **Active Access Codes** area, for the access code that you want to deactivate, click the **Delete** button.

Step 6 In the **Delete** window that appears, click **Yes** to confirm the deletion.

**Note** You can delete multiple access codes simultaneously. A check box will appear for each access code so that you can select multiple access codes at a time, and delete them simultaneously. You can also delete the expired access codes.

Reactivating an Access Code

By default, an access code is in the active mode when it is created. Once you deactivate it, you can activate it whenever required, provided the validity period for the access code is not expired.

To reactivate an access code, perform the following steps:
Exporting Access Codes

Cisco DNA Spaces enables you to export access codes created for a location to a .csv file or as a PDF.

To export the access codes defined for a location in the Cisco DNA Spaces, perform the following steps:

Step 1 In the Cisco DNA Spaces dashboard, click Captive Portals.
Step 2 In the window that appears, click the three line menu icon in the top left of the window.
Step 3 Click Access Code.

Note The Access Code option will be available in the Cisco DNA Spaces dashboard only if you are a Cisco DNA Spaces Account Admin or Access Code Manager user. For more information on creating a Cisco DNA Spaces user, see the Inviting a Cisco DNA Spaces User, on page 191.

Step 4 In the Access Code window that appears, select the location for which you want to export the access codes.

For the location selected, the total number of access codes available, total number of expired access codes, and number of active and inactive access codes among them are displayed.

Step 5 Do any of the following based on the format required:

• To export the access codes as a PDF file, choose Export > Export as PDF.

• To export the access codes as a .csv file, choose Export > Export as CSV.

Step 6 In the window that appears, click OK to save the file.

The access codes get downloaded to the Downloads folder in your computer in the format specified.

Note Only the access codes that are active get exported.
What to do next

If you want to export expired access codes or if you want to export the access codes that are valid during a particular period, you can do it using the Filter option.

Filtering Access Codes to Export

To filter the access codes to be exported, perform the following steps:

Step 1 In the Access Code window, from the drop-down list, choose the location for which you want to export the access codes.

Step 2 Click Filter.

- All Access Codes: Exports all the access codes created for the selected location, including active and expired.

- Filter by: Exports the access codes based on the filter applied. You can choose to filter the access codes that expires on the current week, current month, or on a particular date range. Similarly, you can also filter the access codes that expired during current week, current month, or during a particular date range. You can simultaneously include both expired and active access codes using Expires in and Expired options.

Step 3 Click Apply.

The filtered access code gets displayed in the Filtered Access Codes window.

Step 4 Do any the following based on the format required:

- To export the access codes as a PDF file, choose Export > Export as PDF.

- To export the access codes as a .csv file, choose Export > Export as CSV.

Step 5 In the window that appears, click OK to save the file.

The access codes get downloaded to the Downloads folder in your computer in the format specified.

User Management

The User Management option allows you to invite Captive Portal users with the user roles, Creative User or AccessCodeManager. Only a user with read and write permission on Captive Portals app can invite other users using the User Management option.

- Creative User: This user can create, view, and edit the captive portals in the locations for which access rights are provided. This user will not have access to any other feature of Cisco DNA Spaces. This role is basically for captive portal designers.

- AccessCodeManager: This user can create access codes and manage the access codes for the location for which access rights are provided. This user will have access only to the Captive Portals app. This role is basically for access code managers.

The roles are listed on the Roles tab. You cannot edit the roles from the Roles tab.

To define an Access Code Manager or Creative User, perform the following steps:
Step 1  In the Cisco DNA Spaces dashboard, choose Home.
Step 2  Click Captive Portals.
Step 3  In the window that appears, click User Management in the left pane.

Note  The User Management option will be available in the Cisco DNA Spaces dashboard only for a user with read and write permission on Captive Portals app. For more information, see Inviting a Cisco DNA Spaces User, on page 191.

Step 4  Click Invite User.
Step 5  In the Invite User window, enter the e-mail address of the user whom you want to invite, and click Next.
Step 6  From the Role drop-down list, choose Creative User or AccessCodeManager.
Step 7  Click Location.
Step 8  In the Location Hierarchy area, check the check boxes for the locations for which you want to give access to this particular user.
Step 9  Click Done.
Step 10  Click Send Invitation.

An invitation is sent to the user. The user name gets listed in the Users tab. You can search for a user using the Find Users field.

Social Authentication for Portals

To enable social authentication for the portals, perform the following steps:

• Configuring a Portal for Social Sign In Authentication, on page 90

Configuring the Wireless Network for Social Authentication

For social authentication, you must do some configurations in your wireless network such as Meraki and CUWN. For more information, refer the following links:

• Configuring Cisco Meraki for Social Authentication, on page 247
• Configuring Cisco Wireless Controller for Social Authentication, on page 210

Configuring the Apps for Social Authentication

The configuration required in the apps for the social-authentication through various networking sites is described in this section.

Facebook

To configure the Facebook app for the social-authentication, perform the following steps:
**Twitter**

To configure the Twitter app for the social-authentication, perform the following steps:

1. Log in to apps.twitter.com.
2. Click the app that you want to configure in Cisco DNA Spaces for social-authentication.
3. Click the **Settings** tab.
4. In the **Callback URL** field, enter the callback URL.
   - Global Redirect URL: https://cisco.wifi-mx.com/p/twitter_auth
   - Redirect URL for EU: https://cmxcisco.eu/p/twitter_auth
5. Uncheck the **Enable Callback Locking** check box.
6. Check the **Allow this application to be used to Sign in with Twitter** check box.

**LinkedIn App**

1. Log in to developer.linkedin.com.
2. Click **My Apps**.
3. Click the app that you want to configure for the social-authentication.
4. Click **Authentication**.
5. In the Default Application Permissions area, select the **r_basicprofile** and **r-emailaddress** check boxes.
6. In the Authorized Redirect URLs field, enter the redirect URL, and click **Add**.
What to do next

Note: The domain changes based on Cisco DNA Spaces setup (live, beta, and so on) where the portal is created.

Adding Social Apps for Social Authentication

To manage authentication to the portals through the social network sites, you need to configure the corresponding social app in Cisco DNA Spaces. For example, if you need to authenticate access to a portal for customers that are signed in to Facebook, you need to configure the Facebook app in Cisco DNA Spaces. You can add the apps of the following social network sites to Cisco DNA Spaces:

- Facebook
- Twitter
- LinkedIn

To configure the social apps in Cisco DNA Spaces, perform the following steps:

Step 1: In the Cisco DNA Spaces dashboard, choose Home.
Step 2: In the window that appears, click Captive Portal.
Step 3: In the Captive Portal window that appears, click Settings in the left pane.
Step 4: In the Settings window, choose Social Apps.
Step 5: Click the Add button corresponding to the social networking site for which you want to configure the app. The fields for configuring the app appear.
Step 6: Enter the app name, app ID, and app secret key in the respective fields.
Step 7: Click Save.

Configuring an SMS Gateway in Cisco DNA Spaces

To send SMS notifications, and to manage the portal authentication through SMS, you must configure SMS gateways. Cisco DNA Spaces enables you to use the SMS Gateways of third-party vendors. To configure an SMS gateway in Cisco DNA Spaces, perform the following steps:

Step 1: In the Cisco DNA Spaces dashboard, choose Home.
**Managing Captive Portal Rules**

You can pause a captive portal rule, and make it live again, whenever required. You can modify a captive portal rule, and delete it if required. You can also view the captive portal rules configured for a location.

**Pausing a Captive Portal Rule**

To pause a captive portal rule, perform the following steps:

**Step 1** In the Cisco DNA Spaces dashboard, choose **Home**.
Step 2 In the My Apps area, choose Captive Portal.
Step 3 In the Captive Portal window, choose Captive Portal Rule.
The captive portal rules created get listed.
Step 4 Check the check box for the captive portal rule that you want to pause.
Step 5 Click the Pause button that appears at the bottom of the window.
Step 6 In the window that appears, click Pause Rule to confirm the pause.
The captive portal rule is paused.

What to do next

Note To pause multiple captive portal rules, check the check boxes for the captive portal rules that you want to pause, and click the Pause button that appears at the bottom of the window.

Restarting a Captive Portal Rule

To restart a captive portal rule that is paused, perform the following steps:

Step 1 In the Cisco DNA Spaces dashboard, choose Home.
Step 2 In the My Apps area, choose Captive Portal.
Step 3 In the Captive Portal window, choose Captive Portal Rule.
The captive portal rules created get listed.
Step 4 Check the check box for the captive portal rule that you want to restart.
Click the Make Live button that appears at the bottom of the window.

What to do next

Note To restart multiple captive portal rules, check the check boxes for the captive portal rules that you want to restart, and click the Make Live button that appears at the bottom of the window.

Modifying a Captive Portal Rule

To modify a captive portal rule, perform the following steps:

Step 1 In the Cisco DNA Spaces dashboard, choose Home.
Step 2 In the My Apps area, choose Captive Portal.
Step 3 In the **Captive Portal** window, choose **Captive Portal Rule**.
The captive portal rules created get listed.

Step 4 Click the **Edit Rule** icon for the captive portal rule that you want to modify.

Step 5 Make necessary changes.

Step 6 To save the changes, click **Save** or to publish the changes, click **Save and Publish**.

**Note** A live rule will have only the **Save and Publish** option. When you click the **Save and Publish** button, the rule gets published with the changes.

### Deleting a Captive Portal Rule

To delete a captive portal rule, perform the following steps:

**Step 1** In the Cisco DNA Spaces dashboard, choose **Home**.

**Step 2** In the **My Apps** area, choose **Captive Portal**.

**Step 3** In the **Captive Portal** window, choose **Captive Portal Rule**.
The captive portal rules created get listed.

**Step 4** Click the **Delete Rule** icon that appears at the far right of the captive portal rule that you want to delete.

**What to do next**

**Note** To delete multiple captive portal rules, select the check box for the captive portal rules that you want to delete, and click the Delete button that appears at the bottom of the window.

### Viewing the Captive Portal Rules for a Location

To view a captive portal rule for a location such as group, building, floor, and so on, perform the following steps:

**Step 1** In the Cisco DNA Spaces dashboard, choose **Location Hierarchy**.
The **Location Hierarchy** window appears with the location hierarchy.

**Step 2** Click the location for which you want to view the captive portal rule.

**Step 3** Click the **Proximity Rule** tab.

**Step 4** Click the **Captive Portal Rule** tab.
The captive portal rules for the location gets listed.
What to do next

Note: The **Proximity Rules** link for a location is enabled only if at least one proximity rule exists for that location.

Filtering by Location

For the Cisco DNA Spaces Rules such as Captive Portal Rule, Engagement Rule, Location Personas Rule, and Density Rule, you can filter the locations in which you want to apply a rule. You can also filter the locations by the metadata defined for the selected locations.

To specify the locations in which you want to apply the rule, perform the following steps:

---

**Step 1** Click the **Add Locations** button.

**Step 2** In the **Choose Locations** window that appears, select the locations for which you want to apply the rule.

**Step 3** Click **Done**.

You can again filter the locations using the metadata defined for the locations. Only the metadata defined for the selected locations and their parent or child locations will be available for selection.

---

Apply the rule for locations with a particular metadata

To apply the rule for locations with a particular metadata, perform the following steps:

---

**Step 1** Select the **Filter by Metadata** check box.

**Step 2** In the Filter area, click the **Add Metadata** button.

The **Choose Location Metadata** window appears.

**Step 3** From the drop-down list, choose the metadata variable, and choose the value for the variable in the adjacent field.

**Step 4** Click **Done**.

---

Exclude the locations with a particular metadata

To exclude the locations with a particular metadata, perform the following steps:

---

**Step 1** Select the **Filter by Metadata** check box.

**Step 2** In the Exclude area, click the **Add Metadata** button.

The **Choose Location Metadata** window appears.

**Step 3** From the drop-down list, choose the metadata variable, and choose the value for the variable in the adjacent field.

**Step 4** Click **Done**.
Trigger API Configurations

To configure to send notifications or customer details to an external API using the Cisco DNA Spaces rules, perform the following steps:

- From the Method drop-down list, choose the method for triggering API.

**Note**

You can include the data such as first name, last name, and so on of the customer in the notification message or the customer details sent to the API by adding the smart link variables in the API URI or by adding variables in the method parameters.

- GET—To send notification or customer details to the API using the GET method. If you choose this method, additional fields appear where you can mention the request parameters to include additional details such as first name, last name, mobile number, and so on of the customer. You can add the request parameter keys defined in your API, and mention the values for them using variables. The value can be a hard-coded value or a variable. When you click the “Value” field, the variables that you can add get listed. For more information on variables, see the Smart Links and Text Variables for Captive Portals, on page 152. You can add more “get parameters” using the **Add** button.

- POST FORM—To send notification or customer details to the API using the POST FORM method. If you choose this method, additional fields appear where you can mention the form parameters to include additional details such as first name, last name, mobile number, and so on of the customer. You can add the form parameter keys defined in your API, and mention the values for them. The value can be a hard-coded value or a variable. When you click the “Value” field, the variables that you can add get listed. For more information on variables, see the Smart Links and Text Variables for Captive Portals, on page 152. You can add more “form parameters” using the **Add** button.

- POST JSON—To send notification or customer details to the API using the POST JSON method. If you choose this method, a text box appears where you can mention the JSON data that is to send to the API. You can mention the JSON values for various JSON fields defined in your API. The value can be a hard-coded value or a variable. To add a variable as JSON, click the “JSON Data” text box. The variables get listed. Select the variable that you want to add. For more information on variables, see the Smart Links and Text Variables for Captive Portals, on page 152.

- POST BODY—To send notification or customer details to the API using the POST BODY method. If you choose this method, an additional field appears where you can mention the content that must be sent to the API. You can add variables in the content. To add a variable as BODY, click the “Post Body Data” text box. The variables get listed.

  - In the URI field, enter the URI for the API. You can include additional details of the customers in the notification or customer data sent to the API using the smart links. Click the “URI” field to view the variables that you can add. For more information on variables, see the Smart Links and Text Variables for Captive Portals, on page 152.

**Note**

Only those data that you have configured to capture using the Data Capture form in the portal are included.
Certified Device List for Portals

The following table lists the devices and operating systems that are tested and certified for the portals.

Table 7:

<table>
<thead>
<tr>
<th>Device</th>
<th>OS Version</th>
<th>Browser/ Captive Network Assistant (CNA) (where site loads and works fine)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mobile Device</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Moto G2</td>
<td>6.0</td>
<td>CNA and Google Chrome</td>
</tr>
<tr>
<td>Sony Experia SP</td>
<td>4.3</td>
<td>Google Chrome</td>
</tr>
<tr>
<td>Samsung S2</td>
<td>4.1.2</td>
<td>Google Chrome</td>
</tr>
<tr>
<td>Samsung Galaxy S5</td>
<td>6.0.1</td>
<td>Google Chrome</td>
</tr>
<tr>
<td>Samsung S6</td>
<td>6.0.1</td>
<td>Google Chrome</td>
</tr>
<tr>
<td>Micromax</td>
<td>5.0 and 4.4.4</td>
<td>Google Chrome</td>
</tr>
<tr>
<td>Google Nexus 6</td>
<td>6.0.1</td>
<td>CNA and Google Chrome</td>
</tr>
<tr>
<td>Moto X Play</td>
<td>6.0.1</td>
<td>Google Chrome</td>
</tr>
<tr>
<td>iPhone 4s</td>
<td>7.1.2</td>
<td>CNA Safari</td>
</tr>
<tr>
<td>iPhone 5s</td>
<td>9.3.5 and 9.3.4</td>
<td>CNA, Safari</td>
</tr>
<tr>
<td>iPhone 6</td>
<td>9.3.4</td>
<td>CNA, Safari</td>
</tr>
<tr>
<td>iPhone 6s</td>
<td>9.3.4</td>
<td>CNA, Safari</td>
</tr>
<tr>
<td>iPhone 6 Plus</td>
<td>9.3.2</td>
<td>CNA, Safari</td>
</tr>
<tr>
<td>Huwaei Honur</td>
<td>6.0.1 and 6.0</td>
<td>Google Chrome</td>
</tr>
<tr>
<td>Huwaei P8</td>
<td>5.0.1</td>
<td>Google Chrome</td>
</tr>
<tr>
<td>Microsoft Lumia 950</td>
<td>Windows 10</td>
<td>CNA and Native Browser</td>
</tr>
<tr>
<td>Nokia Lumia 1320</td>
<td>Windows 8.1</td>
<td>CNA and Native Browser</td>
</tr>
<tr>
<td><strong>iPads/Tablets</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Samsung Galaxy Tab2</td>
<td>4.1.2</td>
<td>Google Chrome</td>
</tr>
<tr>
<td>Samsung Galaxy Tab 3 Neo</td>
<td>4.2.2</td>
<td>Google Chrome</td>
</tr>
<tr>
<td>iPad Mini</td>
<td>8.3</td>
<td>CNA and Safari</td>
</tr>
<tr>
<td>iPad 2</td>
<td>9.3.2</td>
<td>CNA and Safari</td>
</tr>
</tbody>
</table>
Cisco DNA Spaces Captive Portal Behavior

The captive portal behavior for various devices is as follows:

**Apple iOS 7.x to 11.x**

When a customer connects to an SSID configured with the captive portal URL, the Captive Network Assistant (CNA) window appears. The CNA loads and displays the content for the portal.

When the customer click any menu or link in the portal, a Log In screen appears with the content based on the authentication type configured for the portal. For more information on configuring the authentication for portal, see the Configuring Authentication for a Portal, on page 87. The customer must follow the authentication steps which can be just accepting terms and conditions, an SMS verification, an e-mail verification, or social-authentication. For more information on the authentication steps for various authentication types, see the Authentication Steps for Customers, on page 144. After completing the required authentication steps, Cisco DNA Spaces sends a request to the wireless network (CUWN, Meraki) to provision internet for that particular device. After successful provisioning of the internet, the CNA window is dismissed, and the Mobile Safari is opened. The web page for the menu or link that customer the clicked earlier appears in the Mobile Safari.

**Note**

For iOS11.0 to 11.3, after internet provisioning, the CNA window will not close automatically. A message is displayed that asks the customer to close the CNA window by clicking the Done button.

Alternatively, if CNA is bypassed, and the customer accesses any URL that is not white-listed (not in Access Control List or Walled Garden Range) using the Mobile Safari or Chrome browser, then the customer is redirected to the configured captive portal URL. The browser loads and displays the content for the captive portal. When the customer click any menu or link in the portal, the Log In screen appears where the customer has to complete the authentication steps as described earlier to provision the internet.

**Note**

After the internet is provisioned, the customer can navigate through any of the menus or links in the portal without any more authentications.

<table>
<thead>
<tr>
<th>Device</th>
<th>OS Version</th>
<th>Browser/ Captive Network Assistant (CNA) (where site loads and works fine)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Laptops/Desktops</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows Lap HP ProBook</td>
<td>Windows 7</td>
<td>Chrome/ Firefox/IE</td>
</tr>
<tr>
<td>Windows Lap Lenovo</td>
<td>Windows 10</td>
<td>Chrome/ Firefox/IE</td>
</tr>
<tr>
<td>Macbook Pro 13-inch</td>
<td>Mac OS X EI Capitan 10.11.6</td>
<td>CNA</td>
</tr>
<tr>
<td>Macbook Pro 13-inch Retina display</td>
<td>Mac OS X EI Capitan 10.11.6</td>
<td>CNA</td>
</tr>
</tbody>
</table>
If any error occurs during the internet provisioning, the captive portal re-appears.

**Note**

If you configure the authentication module as an inline module in the captive portal, you can initiate the authentication process without clicking any link in the portal. For more information on configuring the Authentication module as an inline module, see the Inline Authentication, on page 94.

### Android 5.x and Later (Using CNA)

When the customer connects to an SSID configured with a captive portal URL, an option to 'Sign in to {SSID name}' appears in the notification area. On clicking the notification, devices with Android 5.x or later launches the CNA window. The CNA loads the content from the portal URL and displays the portal. When the customer click any menu or link in the portal, a Log In screen appears with the content based on the authentication type configured for the portal. For more information on configuring the authentication for portal, see the Configuring Authentication for a Portal, on page 87. The customer must follow the authentication steps which can be just accepting terms and conditions, an SMS verification, an e-mail verification, or social-authentication. For more information on the authentication steps for various authentication types, see the Authentication Steps for Customers, on page 144. After completing the required authentication steps, Cisco DNA Spaces sends a request to the wireless network (CUWN, Meraki) to provision internet for that particular device. After successful provisioning of the Internet, the CNA window is dismissed.

Alternatively, the customer can ignore the notification and go ahead using the native or Chrome browser. When the customer accesses any URL that is not white-listed (not in Access Control List or Walled Garden Range), the customer is redirected to the configured captive portal URL. The browser loads and displays the content for the captive portal. When the customer click any menu or link in the portal, the Log In screen appears where the customer has to complete the authentication steps as described earlier to provision the internet. After successful provisioning of the internet, the web page for the menu or link that customer clicked earlier appears.

**Note**

After the internet is provisioned, the customer can navigate through any of the menus or links in the portal without any more authentications.

**Note**

If any error occurs during the internet provisioning, the captive portal re-appears.

**Note**

If you configure the authentication module as an inline module in the captive portal, you can initiate the authentication process without clicking any link in the portal. For more information on configuring the Authentication module as an inline module, see the Inline Authentication, on page 94.
Android 4.x and Earlier

When the customer connects to an SSID configured with a captive portal URL, an option to 'Sign in to {SSID name}' appears in the notification area. On clicking the notification, devices with Android 4.x or earlier launches the default browser. The browser tries to load a URL that is generated by the device. As this URL is not white-listed (not in Access Control List or Walled Garden Range), the customer is redirected to the captive portal. When the customer click any menu or link in the portal, a Log In screen appears with the content based on the authentication type configured for the portal. For more information on configuring the authentication for portal, see the Configuring Authentication for a Portal, on page 87. The customer must follow the authentication steps which can be just accepting terms and conditions, an SMS verification, an e-mail verification, or social-authentication. For more information on the authentication steps for various authentication types, see the Authentication Steps for Customers, on page 144. After completing the required authentication steps, Cisco DNA Spaces sends a request to the wireless network (CUWN, Meraki) to provision internet for that particular device. After successful provisioning of the internet, the web page for the menu or link that customer clicked earlier appears in the same browser.

Note

After the internet is provisioned, the customer can navigate through any of the menus or links in the portal without any more authentications.

Note

If any error occurs during the internet provisioning, the captive portal re-appears.

Note

If you configure the authentication module as an inline module in the captive portal, you can initiate the authentication process without clicking any link in the portal. For more information on configuring the Authentication module as an inline module, see the Inline Authentication, on page 94.

Windows Phone

When the customer connects to an SSID configured with a captive portal URL, the Captive Network Assistant (CNA) appears. The CNA loads and displays the content for the captive portal URL. When the customer click any menu or link in the portal, a Log In screen appears with the content based on the authentication type configured for the portal. For more information on configuring the authentication for portal, see the Configuring Authentication for a Portal, on page 87. The customer must follow the authentication steps which can be just accepting terms and conditions, an SMS verification, an e-mail verification, or social-authentication. For more information on the authentication steps for various authentication types, see the Authentication Steps for Customers, on page 144. After completing the required authentication steps, Cisco DNA Spaces sends a request to the wireless network (CUWN, Meraki) to provision internet for that particular device. After successful provisioning of the Internet, the CNA window is dismissed.

Note

If any error occurs during the internet provisioning, the captive portal re-appears.
If you configure the authentication module as an inline module in the captive portal, you can initiate the authentication process without clicking any link in the portal. For more information on configuring the Authentication module as an inline module, see the Inline Authentication, on page 94.

**Note**

Windows PCs and Laptops

After successfully connecting to an SSID configured with a captive portal URL, when the customer browses any URL that is not white-listed (not in Access Control List or Walled Garden Range), the customer is redirected to the captive portal page configured for that SSID. When the customer click any menu or link in the portal, a Log In screen appears with the content based on the authentication type configured for the portal. For more information on configuring the authentication for portal, see the Configuring Authentication for a Portal, on page 87. The customer must follow the authentication steps which can be just accepting terms and conditions, an SMS verification, an e-mail verification, or social-authentication. For more information on the authentication steps for various authentication types, see the Authentication Steps for Customers, on page 144.

After completing the required authentication steps, Cisco DNA Spaces sends a request to the wireless network (CUWN, Meraki) to provision internet for that particular device. After successful provisioning of the internet, the web page for the menu or link that customer clicked earlier appears in the same browser.

For windows 10, when the customer connects to an SSID configured with a captive portal URL, the Captive Network Assistant (CNA) appears. The CNA loads and displays the content for the captive portal URL. When the customer click any menu or link in the portal, a Log In screen appears with the content based on the authentication type configured for the portal. For more information on configuring the authentication for portal, see the Configuring Authentication for a Portal, on page 87. The customer must follow the authentication steps which can be just accepting terms and conditions, an SMS verification, an e-mail verification, or social-authentication. For more information on the authentication steps for various authentication types, see the Authentication Steps for Customers, on page 144. After completing the required authentication steps, Cisco DNA Spaces sends a request to the wireless network (CUWN, Meraki) to provision internet for that particular device. After successful provisioning of the internet, the CNA window is dismissed.

**Note**

After the internet is provisioned, the customer can navigate through any of the menus or links in the portal without any more authentications.

**Note**

If any error occurs during the internet provisioning, the captive portal re-appears.

**Note**

If you configure the authentication module as an inline module in the captive portal, you can initiate the authentication process without clicking any link in the portal. For more information on configuring the Authentication module as an inline module, see the Inline Authentication, on page 94.
When the customer connects to an SSID configured with a captive portal URL, the Captive Network Assistant (CNA) window appears. The CNA loads and displays the content for the captive portal. When the customer click any menu or link in the portal, a Log In screen appears with the content based on the authentication type configured for the portal. For more information on configuring the authentication for portal, see the Configuring Authentication for a Portal, on page 87. The customer must follow the authentication steps which can be just accepting terms and conditions, an SMS verification, an e-mail verification, or social-authentication. For more information on the authentication steps for various authentication types, see the Authentication Steps for Customers, on page 144. After completing the required authentication steps, Cisco DNA Spaces sends a request to the wireless network (CUWN, Meraki) to provision the internet for that particular device. After successful provisioning of the internet, the web page for the menu or link that customer clicked earlier appears in the default browser of the customer. Apart from the link that the customer has clicked, the browser opens another tab with the home page that is in CNA.

Alternatively, the customer can dismiss the captive portal window and go ahead using the browser. When the customer accesses any URL that is not white-listed (not in Access Control List or Walled Garden Range), the customer is redirected to the configured captive portal URL. The browser loads and displays the content for the captive portal URL. When the customer click any menu or link in the portal, the Log In screen appears where the customer has to complete the authentication steps as described earlier to provision the internet. After successful provisioning of the internet, the web page for the menu or link that customer clicked earlier appears in the same browser.

Note
After the internet is provisioned, the customer can navigate through any of the menus or links in the portal without any more authentications.

Note
If any error occurs during the internet provisioning, the captive portal re-appears.

Note
If you configure the authentication module as an inline module in the captive portal, you can initiate the authentication process without clicking any link in the portal. For more information on configuring the Authentication module as an inline module, see the Inline Authentication, on page 94.

Authentication Steps for Customers
The authentication steps that a customer has to complete to provision the internet for various authentication types are as follows:

Steps for SMS with Link Verification Authentication
To complete the “SMS with link verification” authentication, perform the following steps:
Step 1
In the captive portal, click/tap any menu item.

Step 2
In the Log In screen that appears, enter the mobile number.

Note
If a Data Capture module is configured, the data capture form appears along with the mobile number field.

Step 3
Enter the mobile number, and all the mandatory fields in the Data Capture form, and press Accept Terms and Continue.

The internet is provisioned, and a SMS with a link to access the portal is sent to the mobile number provided.

Step 4
Click the link in the SMS for finger print verification.

For more information on fingerprint verification, see the Fingerprint Verification, on page 146.

Note
If the customer does not click the link in the SMS within a time frame, a “Skip” button appears. The customer can click the “Skip” button to proceed further without fingerprint verification. When the customer tries to access the internet next time, a blank “mobile number” field is shown to provide the mobile number again. This occurs for every internet access till the customer completes the fingerprint verification.

Authentication Steps for a Repeat User for SMS with Link Verification

The authentication steps for a repeat user for various scenarios are as follows:

- Completed the fingerprint verification (Data Capture module is not configured): When the customer click/tap any menu item, internet is provisioned.

- Completed the fingerprint verification (Data Capture module is configured, the Data Capture form is filled): When the customer click/tap any menu item, internet is provisioned.

- Completed the fingerprint verification, but Data capture form is not filled or partially filled (for non mandatory fields): When the customer click/tap any menu item, internet is provisioned. However, the data capture form is shown if there is any change in the data capture form.

- Not completed the fingerprint verification, but filled the Data Capture form: When the customer click/tap any menu item, the mobile number field appears along with the pre-filled Data Capture form. The customer has to enter the mobile number again for accessing the internet. This continues for all the internet access attempts till the customer completes the fingerprint verification.

- Mobile number verification process was not completed during previous internet access: If the verification process is not complete within a limited time, the internet is provisioned even for invalid mobile numbers. For such a repeat user, when the captive portal loads, and the customer click any menu item or link in the portal, the log in screen appears with the mobile number field. The customer has to enter a valid mobile number.

- The Data Capture module is configured, and the registration details are outdated: When the captive portal loads, and the customer click any menu item or link in the portal, the registration form appears with the previously filled data. The customer can update the form, and press Connect to get access to the internet.

The following are some of the scenarios when the registration details become outdated:

- Added new mandatory fields: Added a new mandatory field in the Data Capture module. For example, you configured the Data Capture module without a Gender field. The customer completes registration. Later on, you added the Gender field to the Data Capture module and marked it as mandatory.
• **Optional field becomes mandatory**: Modified the Data Capture module to make an optional field that the customer skipped during registration as a mandatory field. For example, you have configured a Data Capture module with the last name as optional. The customer connected to the SSID and completed the registration without mentioning the last name. Now, you modified the Data Capture module and made the last name mandatory for registration.

• **Modified the choice options**: Removed or replaced a choice option that was available for selection. For example, you have configured a mandatory business tag “Age Criteria” with choice options as “Child” and Adult”. The customer completes registration by selecting Age Criteria as Child. Later on, you modified to display the choices as “Kids”, and “Adult”.

**Note**

In all the above scenarios, if there is any change in the Terms and Conditions defined, the “Accept Terms and Continue” button is displayed. The customer must press the “Accept Terms and Continue” button to get access to the internet or to move to the next authentication step.

**Fingerprint Verification**

When a customer provides the mobile number for the “SMS with link verification” authentication, a message with a link is sent to the mobile number provided, and the internet is provisioned. The Fingerprint verification happens when the customer click the link in the message. If the customer is not clicking the link within a pre-defined time, a temporary page with a “SKIP” option is shown to the customer. The customer can click the Skip option to access the internet without fingerprint verification.

The fingerprint verification status for various scenarios is as follows:

- When the customer click the link in the message, if fingerprint matches, then customer acquisition will happen and the customer will be redirected to the portal page. The customer will be considered as repeat user on next visit.

- When the customer click the link in the message, if the fingerprint verification fails (For example, if the customer opens the link in a different browser than the one used for initiating the SMS authentication, then the fingerprint verification fails.), a confirmation page appears for the customer. If the customer click “Confirm”, the customer acquisition will happen, and the customer will be redirected to the portal page. The customer will be considered as repeat user on next visit.

- When the customer click the link in the message, if fingerprint verification fails, a confirmation page appears for the customer. If the customer click “Cancel”, the customer will be considered as first time user on next visit, and the log in screen appears with a blank mobile number field.

- If the customer click “Skip” in the temporary page displayed, the customer is considered as first time user on next visit, and the log in screen appears with a blank mobile number field.

**Steps for SMS with Password Verification Authentication**

To complete the “SMS with password verification” authentication, perform the following steps:

**Step 1**

In the captive portal, click/tap any menu item.

**Step 2**

In the Log In screen that appears, enter the mobile number.
Step 3  
If the customer wants to unsubscribe from receiving notifications, uncheck the Opt In to Receive notification check box.

**Note**  
The “Opt In to receive notification” check box appears in the Log In screen only if you have selected the “Allow users to Opt in to receive message” check box in the Authentication screen when configuring the authentication details for the portal.

Step 4  
Press Accept Terms and Continue.

Step 5  
In the screen that appears, enter the verification code received through the SMS.

Step 6  
Press Verify.

After successful verification of the verification code, the Data Capture form appears, if Data Capture is enabled.

Step 7  
Enter all the mandatory fields in the Data Capture form, and press Connect.

**Note**  
If all the fields are optional, there will be two buttons Skip and Connect. The customer can click the Skip button to proceed without filling the data. If the customer click Skip, the data capture form will appear for that customer only if there is any change in the form.

After successful registration, the internet provisioning process is initiated, and the internet is provisioned.

**Note**  
If the Data Capture module is not enabled, the internet is provisioned immediately after the verification code validation.

---

**Authentication Steps for a Repeat User for SMS with Password Verification**

The authentication steps for a repeat user for various scenarios are as follows:

- **Data Capture is not configured**: When the captive portal loads, and the customer click any menu item or link in the portal, the internet is provisioned.

- **Data Capture is configured, and the customer completed the registration**: When the captive portal loads, and the customer click any menu item or link in the portal, the internet is provisioned.

- **Data Capture is configured, and the registration details are outdated**: When the captive portal loads, and the customer click any menu item or link in the portal, the Data Capture form appears with the previously filled data. The customer can update the form, and press the “Connect” button to get access to the internet.

The following are some of the scenarios when the registration details become outdated:

- **Added new mandatory fields**: Added a new mandatory field in the Data Capture form. For example, you configured the Data Capture form without a Gender field. The customer completes registration. Later on, you added the Gender field to the Data Capture form and marked it as mandatory.

- **Optional field becomes mandatory**: Modified the Data Capture form to make an optional field that the customer skipped during registration as a mandatory field. For example, you have configured a Data Capture form with the last name as optional. The customer connected to the SSID and completed the registration without mentioning the last name. Now, you modified the Data Capture form and made the last name mandatory in the form.

- **Modified the choice options**: Removed or replaced the choice options that was available for selection. For example, you have configured a mandatory business tag “Age Criteria” with choice options as “Child” and “Adult”. The customer completes registration by selecting Age Criteria as “Child”. Later on, you modified to display the choices as “Kids”, and “Adult”.

---
Steps for E-mail Authentication

To complete the e-mail authentication, perform the following steps:

Step 1  In the captive portal, click/tap any menu item.
Step 2  In the Log In screen that appears, enter the e-mail ID.
Step 3  If the customer wants to unsubscribe from receiving notifications, uncheck the Opt In to Receive notification check box.

Note  The Opt In to Receive notification check box appears in the Log In screen only if you have checked the Allowed users to Opt in to receive message check box for the Email authentication type when configuring the authentication details for the portal.

Step 4  Press Accept Terms and Continue.
If the e-mail ID entered is valid, the internet is provisioned.

Step 5  If the Data Capture is enabled in the Authentication screen of the captive portal, a Data Capture form appears when the customer press Accept Terms and Continue.

Step 6  Enter all the mandatory fields in the Data Capture form, and press Connect.

Note  If all the fields are optional, there will be two buttons Skip and Connect. The customer can click the Skip button to proceed without filling the data. If the customer click “Skip”, the Data Capture form will appear for the repeat user only if there is any change in the form.

The internet provisioning process is initiated, and the internet is provisioned.

Authentication Steps for a Repeat User for Email Verification

The authentication steps for a repeat user for various scenarios are as follows:

• Entered invalid e-mail ID during previous log in: When the captive portal loads, and the customer click any menu item or link in the portal, the log in screen appears with the invalid e-mail ID mentioned during previous login. The customer has to enter a valid e-mail ID to proceed further.

• Data Capture is not enabled - When the captive portal loads, and the customer click any menu item or link in the portal, the internet is provisioned.

• Data Capture is enabled, and the customer completed the registration - When the captive portal loads, and the customer click any menu item or link in the portal, the internet is provisioned.
Data Capture is enabled, and the registration details are outdated—When the captive portal loads, and the customer click any menu item or link in the portal, the Data Capture form appears with the previously filled data. The customer can update the form, and press “Connect” to get access to the internet.

The following are some of the scenarios when the registration details become outdated:

- **Added new mandatory fields** - Added a new mandatory field in the Data Capture form. For example, you configured the Data Capture form without a Gender field. The customer completes registration. Later on, you added the Gender field to the Data Capture form and marked it as mandatory.

- **Optional field becomes mandatory** - Modified the Data Capture form to make an optional field that the customer skipped during registration as a mandatory field. For example, you have configured a Data Capture form with the last name as optional. The customer connected to the SSID, and completed the registration without mentioning the last name. Now, you modified the Data Capture form and made the last name mandatory in the form.

- **Modified the choice options** - Removed or replaced a choice option that was available for selection. For example, you have configured a mandatory business tag “Age Criteria” with choice options as “Child” and “Adult”. The customer completes registration by selecting Age Criteria as Child. Later on, you modified to display the choices as “Kids”, and “Adult”.

---

**Note**

In all the above scenarios, if there is any change in the Terms & Conditions defined, the **Accept Terms and Continue** button is displayed. The customer must press the “Accept Terms and Continue” button to get access to the internet or to move to the next authentication step.

---

**Steps for Access Code Authentication**

To complete the “Access Code” authentication, perform the following steps:

**Step 1**
In the captive portal, click/tap any menu item.

**Step 2**
In the Log In screen that appears, enter the access code.

**Step 3**
If the customer wants to unsubscribe from receiving notifications, uncheck the **Opt In to Receive notification** check box.

**Note**

The “Opt In to receive notification” check box appears in the Log In screen only if you have selected the “Allow users to Opt in to receive message” check box in the Authentication screen when configuring the authentication details for the portal.

**Step 4**
Press **Accept Terms and Continue**.

**Step 5**
Press **Verify**.

After successful verification of the access code, the Data Capture form appears, if Data Capture is enabled.

**Step 6**
Enter all the mandatory fields in the Data Capture form, and press **Connect**.

**Note**

If all the fields are optional, there will be two buttons **Skip** and **Connect**. The customer can click the **Skip** button to proceed without filling the data. If the customer click **Skip**, the data capture form will appear for that customer only if there is any change in the form.

After successful registration, the internet provisioning process is initiated, and the internet is provisioned.
Authentication Steps for a Repeat User for Access Code Authentication

The authentication steps for a repeat user for various scenarios are as follows:

- **Data Capture is not configured**: When the captive portal loads, and the customer click any menu item or link in the portal, the internet is provisioned.

- **Data Capture is configured, and the customer completed the registration**: When the captive portal loads, and the customer click any menu item or link in the portal, the internet is provisioned.

- **Data Capture is configured, and the registration details are outdated**: When the captive portal loads, and the customer click any menu item or link in the portal, the Data Capture form appears with the previously filled data. The customer can update the form, and press the “Connect” button to get access to the internet.

The following are some of the scenarios when the registration details become outdated:

- **Added new mandatory fields**: Added a new mandatory field in the Data Capture form. For example, you configured the Data Capture form without a Gender field. The customer completes registration. Later on, you added the Gender field to the Data Capture form and marked it as mandatory.

- **Optional field becomes mandatory**: Modified the Data Capture form to make an optional field that the customer skipped during registration as a mandatory field. For example, you have configured a Data Capture form with the last name as optional. The customer has connected to the SSID and completed the registration without mentioning the last name. Now, you modified the Data Capture form and made the last name mandatory in the form.

- **Modified the choice options**: Removed or replaced the choice options that was available for selection. For example, you have configured a mandatory business tag “Age Criteria” with choice options as “Child” and Adult”. The customer completes registration by selecting Age Criteria as “Child”. Later on, you modified to display the choices as “Kids”, and “Adult”.

- **Entered invalid e-mail ID during previous log in**: When the captive portal loads, and the customer click any menu item or link in the portal, the Data Capture form appears with the invalid e-mail ID mentioned during previous login. The customer has to enter a valid e-mail ID to proceed further.

In all the above scenarios, if there is any change in the Terms and Conditions defined, the Accept Terms and Continue button is displayed. The customer must press the Accept Terms and Continue button to get access to the internet, or to move to the next authentication step.

Steps for No Authentication with Terms and Conditions

You can configure to provision the internet to the customers if they accept just the terms and conditions mentioned.

To complete the authentication that requires only the acceptance of the terms and conditions, perform the following steps:
Step 1  In the captive portal, click/tap any menu item.

Step 2  In the Log In screen that appears, press Accept Terms and Continue.

The internet provisioning process is initiated, and the internet is provisioned.

**Authentication Steps for a Repeat User with Terms and Conditions Authentication**

When the captive portal loads, and the customer click any menu item or link in the portal, the internet is provisioned.

---

**Note**

If there is any change in the Terms and Conditions defined, the “Accept Terms and Continue” button is displayed. The customer must press the “Accept Terms and Continue” button to get access to the internet or to move to the next authentication step.

---

**Steps for Social Authentication**

To complete the social authentication for a portal, perform the following steps:

---

**Step 1**

When the customer click any menu item or link in the captive portal, a screen appears with all the social sign in options available for the portal.

**Note**

The Sign in option appears only for those social networks that are configured for the portal. For more information on configuring the social network for a portal, see the Configuring a Portal for Social Sign In Authentication, on page 90.

**Step 2**

Click the sign in option for the social network through which you want to complete the authentication. The log in page for the social network appears.

For example, click the sign in option for Linked In, then the log in screen for Linked In appears.

**Step 3**

Enter the log in credentials for the social network, and press the log in button.

**Step 4**

In the screen that appears, press Allow.

The redirect URI gets loaded, and the Terms and Conditions screen appears.

**Step 5**

Press Accept Terms and Continue.

**Note**

For Facebook and Twitter, it is not required to configure the redirect URI. The Redirect URI must be configured for Linked In. For more information on configuring the redirect URI for Linked In, see the Configuring the Apps for Social Authentication, on page 131.

**Step 6**

After provisioning the internet, a Continue window appears.

**Step 7**

Press Continue to view the page for the link that you have clicked earlier.
Authentication Steps for a Repeat User with Social Authentication

When the captive portal loads, and the customer click any menu item or link in the portal, the options to connect with all the configured social networks appear. The social networks the customer has used earlier for authentication will be labeled as “Continue with [social network]. For example, if the customer has used Facebook authentication earlier to access the internet through the captive portal, the option for Facebook will be labeled as “Continue with Facebook”. For the social networks that are not used earlier for authentication, a sign in option appears. For example, “Signin with Linkedin”.

• If the customer continues to use a social network that was used earlier for authentication, the internet is provisioned without any authentication process. However, if there is any change in the Terms and Conditions, the Terms and Conditions screen is shown. Then, the customer must press the “Accept Terms and Continue” button to get access to the internet.

• If the customer signs in using a social network that was not used earlier for authentication, the customer has to complete the entire authentication process for that social network. If the customer has accessed the internet using social authentication through any of the social network, the Terms and Conditions screen is not shown during the authentication process. However, if there is any change in the terms and conditions, the Terms and Conditions screen appears during the authentication process. Then, the customer must press the “Accept Terms and Continue” button to get access to the internet.

Smart Links and Text Variables for Captive Portals

Smart Links

The Smart Link option enables you to provide your customers personalized web pages and messages. Using the Smart Link option, you can customize the URLs for the custom menu links in the captive portals to provide a personalized view. You can personalize your site pages for each user or group of users.

For example, you can configure the parameter “optedinstatus” for a custom menu item in your portal. Then you configure the web page for this custom menu item to display different content for “opted in” and “not opted in” users. When a customer who is an opted in user click the custom menu link in the captive portal, the content for the opted in user is shown. When a customer who is not an opted in user click the same custom menu link, the content for the not opted in user is shown.

To use these parameters to display the personalized view to the customers, you have to configure your web pages accordingly.

In the Captive Portals app, You can include the smart links in the following options:

• The links added in the custom menu items added to the portal.

• URL added in the URI field in Trigger API.

Text Variables

Using text variables, you can add personal details of the customers such as name, mobile number, gender, and so on in the messages sent to an API end point using Trigger API. By default, the message will have first name and last name of the customer. You can add additional customer details using the variables.
For example, assume that you have created a Trigger API notification and configured the variables “mobile” and “gender” in the message text box for the SMS notification. Now, when a customer receives a SMS message based on this engagement rule, the mobile number and gender details of the customer are also shown in the message.

You can add variables in the following options:

- The message sent to an API end point using Trigger API.
- Welcome Messages for first time and repeat user.
- Notices added to the portal (Only backend support).

Cisco DNA Spaces captures the personal details of the customers using the Data Capture form. That is, to include the personal details such as first name, last name, gender, and so on in the smart link or as text variable, you must configure the Data Capture form in the portal. For more information on adding a Data Capture form to a captive portal see the Adding a Data Capture Form to a Portal section.

The URL of the captive portal that is included in the “SMS with link verification” and “SMS with password verification” messages are not supported with the smart link feature.

Cisco DNA Spaces provides certain predefined variables. You must use these variables to provide personalized view for you web pages and to add customer details in the notification messages.

You can include static and dynamic variables in a smart link or text.

The static parameters that you can include in the smart link or text are as follows:

<table>
<thead>
<tr>
<th>Static Variable Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>$location</code> or <code>$locationName</code></td>
<td>Name of the location for which the rule is triggered.</td>
</tr>
<tr>
<td><code>$Address</code></td>
<td>The address configured for the location in the Location Info window in Location Hierarchy.</td>
</tr>
<tr>
<td><code>$State</code></td>
<td>The state configured for the location in the Location Info window in Location Hierarchy.</td>
</tr>
<tr>
<td><code>$Country</code></td>
<td>The country configured for the location in the Location Info window in Location Hierarchy.</td>
</tr>
<tr>
<td><code>$City</code></td>
<td>The city configured for the location in the Location Info window in Location Hierarchy.</td>
</tr>
<tr>
<td><code>$TotalAreaValue</code></td>
<td>The total area configured for the location in the Location Info window in Location Hierarchy.</td>
</tr>
<tr>
<td><code>$firstName</code> (Not applicable for First Time Visitor in the Welcome module.)</td>
<td>First name of the customer.</td>
</tr>
<tr>
<td><code>$lastName</code> (Not applicable for First Time Visitor in the Welcome module.)</td>
<td>Last name of the customer.</td>
</tr>
</tbody>
</table>
The following variables are not applicable for the **Welcome** module, but only for Custom modules and Trigger API.

<table>
<thead>
<tr>
<th>Static Variable Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$email</td>
<td>E-mail address of the customer.</td>
</tr>
<tr>
<td>$mobile</td>
<td>Mobile number of the customer.</td>
</tr>
<tr>
<td>$gender</td>
<td>Gender of the customer.</td>
</tr>
<tr>
<td>$URL</td>
<td>URL link value.</td>
</tr>
<tr>
<td>$macaddress</td>
<td>The mac address of the device.</td>
</tr>
<tr>
<td>$encryptedMacAddress</td>
<td>The encrypted mac address of the device.</td>
</tr>
<tr>
<td>$deviceSubscriberId</td>
<td>The subscriber ID for the device in the database.</td>
</tr>
<tr>
<td>$optinStatus</td>
<td>The opt in status for the customer.</td>
</tr>
</tbody>
</table>

In addition, you can include the following dynamic variables in a smart link or text:

**Table 9: Dynamic Variable List**

<table>
<thead>
<tr>
<th>Dynamic Variable Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Tags</td>
<td>The business tag to which the customer belongs to. The business tags configured in the Data Capture form are listed as variables. For more information on creating a business tag, see the <a href="#">Adding a Data Capture Form to a Portal</a> section.</td>
</tr>
<tr>
<td>Location Metadata</td>
<td>The location metadata for the customer location. The location metadata keys defined in the location hierarchy are listed as variables. For more information on defining the location metadata, see the <a href="#">Adding Metadata for a Location</a> section.</td>
</tr>
</tbody>
</table>

To include a smart link in a URL, or variable in a text, perform the following steps:

**Step 1**
Click anywhere in the URL field or text box or click the corresponding **Add Variable** drop-down list.

The variables that you can include get listed.

**Step 2**
Choose the variables that you want to include.
Cisco DNA Spaces functions as a Wi-Fi Beacon that identifies the customers in a Cisco DNA Spaces enabled premises and sends notifications to the customers and business users, based on the engagement rule defined.

This chapter describes how to create the engagement rules that enable you to send notifications to the customers when they are near your business premises. A customer can be a user who has purchased from your business premises earlier, a potential buyer, or a visitor. You can also configure engagement rules to send notifications to your business users such as employees or to an API end point. For example, you can configure an engagement rule that informs your customer care representative when a privileged customer enters the premises so that the customer care representative can provide value added services to the customer.

You can configure to send the notification based on the customers connectivity to your Wi-Fi.

**Note**

An engagement rule is applied for all the SSIDs defined for the locations specified in the rule.

- Prerequisites for Creating an Engagement Rule, on page 155
- Creating an Engagement Rule, on page 156
- Managing Engagement Rules, on page 163
- Engagement Rule Report, on page 165
- Visitor Engagement, on page 166
- Engagement URL, on page 166
- Previous Visit Criteria, on page 166
- Notification Types, on page 168
- Notification Frequency, on page 168
- Location Filter for an Engagement Rule, on page 168
- Notification Type for a Consumer, on page 169
- Notification Type for a Business User, on page 170
- Trigger API Configuration for Notification, on page 173

**Prerequisites for Creating an Engagement Rule**

- To send notifications, you must do certain configurations in your wireless network system.
  - If your wireless network is Cisco Meraki, do the configurations mentioned in Configuring Cisco Meraki for Notifications and Reports, on page 246.
• If your wireless network is Cisco AireOS or Cisco Catalyst, do the configurations mentioned in Configuring Cisco Wireless Controller (without Cisco CMX) for Notification and Reports, on page 215

• If your wireless network is Cisco Catalyst, do any of the following configurations based on the mode and connector.
  • Configuring Cisco Catalyst 9800 Series Wireless Controller (Local Mode) for Captive Portals and Engagements Apps Using CLI, on page 217
  • Configuring Cisco Catalyst 9800 Series Wireless Controller GUI (Local Mode) for Captive Portals and Engagements Apps, on page 221
  • Configuring Cisco Catalyst 9800 Series Wireless Controller GUI (Flex Mode or Mobility Express) for Captive Portals and Engagements Apps, on page 225

• To specify the locations for which the engagement rule is applicable, you must define the location hierarchy. For more information on defining the location hierarchy, see the Overview of Location Hierarchy, on page 17.

• To specify the tags for which the rule is applicable, you must define the tags. For more information on creating the tags, see the Creating or Modifying Tags Using a Location Personas App, on page 175.

• To send to an external API the details such as first name, last name, and so on of the customers who have signed into the captive portal, you must configure the Data Capture form in the captive portal. Without the Data Capture form, only the information such as device mac address will be send to the external API. For more information on configuring a data capture form, see the Adding a Data Capture Form to a Portal, on page 95.

Creating an Engagement Rule

The Engagement Rule refers to the conditions based on which the notifications are sent to the target users. You can create the engagement rule for your customers and business users such as employees or API endpoints.

You can set the frequency at which the notification is to send. You can also define the criteria that must match to send the notification. You can configure to send the notification to a single user or a group of users in multiple locations.

For customers, you can send the notifications through SMS or e-mail. For business users, you can send the notifications through Cisco Webex Teams, SMS, e-mail, or to an external API. For customers and business users, you can configure to send the notifications based on the connectivity of the customer to an SSID. You can configure more than one notification type for an engagement rule, so that the user gets notification in more than one format. This increases the probability of notifications to be noticed by the user.

Creating an Engagement Rule for a Consumer

You can send the notifications to a customer through SMS or e-mail.

To define an engagement rule to send notifications to the customers, perform the following steps:

Step 1 In the Cisco DNA Spaces dashboard, choose Engagements.
Step 2  On the Engagements window that appears, click Create New Rule.

Step 3  In the Rule Name field, enter a name for the engagement rule.

Step 4  From the When a user is on WiFi and drop-down list, choose any of the following:

- **Entering a Location**: Choose this option if you want to send the notification when a visitor connected to the Wi-Fi enters the location.

- **Away from the Location**: Choose this option if you want to send the notification when a visitor connected to the Wi-Fi is away from the location for a specified time. If you are selecting this option, from the For scroll list, choose the number of minutes a visitor needs to be away from the location for sending notifications.

  **Note**  - The Exiting Location option is no more available. If you are editing an existing Engagement Rule with Exiting Location configured, the Choose User Activity drop-down list will appear without any selection. You must choose the required option from the Choose User Activity drop-down list to save the rule successfully.

  - Even if a visitor is physically present in the location, but gets disconnected from the Wi-Fi for the minutes specified in the For scroll list, the visitor will be considered for sending notification.

  - **Present at Location**: Choose this option if you want to send notifications to a visitor who is connected to the Wi-Fi and is present at the location for a specified duration or at a particular time. If you choose this option, additional fields appear where you can mention the duration or time that needs to be met by the customer to get filtered for this rule.

Step 5  In the Locations area, specify the locations for which you want to send the notifications.

You can configure to send notifications for the entire customer name or a single or multiple locations such as group, floor, or zone. You can add the locations of different wireless networks such as Cisco Meraki, Cisco Wireless Controller, and so on in an Engagement rule.

You can again filter the locations for which the notification is to send based on the metadata defined for the selected location or its parent or child locations. You can either send the notifications for the locations with a particular metadata or exclude the locations with a particular metadata. For more information on defining the locations for the engagement rule, see the Location Filter for an Engagement Rule, on page 168.

Step 6  In the IDENTIFY area, specify the type of customers for whom you want to send the notifications.

**Note**  You can filter the customers for whom you want to send the notifications based on whether the customer is an opted in or not opted in user, the tags the customers belong to, and the number of visits made by the customer. You can apply all these filters or any of them based on your requirement.

To specify the customers for whom the notification is to send, perform the following steps:

a) If you want to filter the customers by the Opt In Status, check the Filter by Opt-In Status check box, and choose whether you want to send the notifications for opted in users or not opted in users.

b) If you want to filter the customers based on tags, check the Filter by Tags check box.

  **Note**  You can filter the tags in two different ways. Either you can specify the tags for which the notifications are to send or you can specify the tags for which the notifications must not be sent. You can choose the best filtering method based on your requirement. For example, if you want to send the notifications for all tags expect for one tag, it is easy to opt the exclude

c) If you want to filter the customers based on the number of visits made by the customer in the selected locations, check the Filter by Previous Visits check box. Click the Add Locations button. In the Choose Locations window, specify
Use Case: Engagement Rule for Customers

The retail store ABC has outlets across Europe. As part of its summer sale, ABC has decided to provide some offers to its customers. The offer is only for the customers visiting the ABC outlets at location A and floor 1 at location B. All the customers who had visited any outlet of ABC at least 5 times in the current year are eligible for the offer. ABC wants to send notifications regarding the offers to the customers who had visited any of its outlets minimum 5 times during the current year. The notifications need to send when the customer enters location A or Floor 1 of location B with connected to the Wi-Fi. The notification is to send only on weekends as the offer is only for weekends. The notifications are to send only for a fortnight for the opted-in users. ABC wants to send the notifications during each visit through e-mail.

To meet the preceding scenario, perform the following steps:

Step 1 Log in to Cisco DNA Spaces.
Step 2  Create the location hierarchy with all the locations of ABC.

Step 3  In the Cisco DNA Spaces dashboard, click Engagements.

Step 4  On the Engagements page that appears, click Create New Rule.

Step 5  In the Rule Name field, enter a name for the engagement rule.

Step 6  From the When a user is on WiFi and drop-down list, choose Entering Location.

Step 7  In the Locations area, click the Add Locations button for choosing the location, and select location A, and Floor 1 of location B.

Step 8  In the Identify area, do the following:
   a) Check the Filter by Opt-In Status check box, and choose Only for opted-in Visitor.
   b) Check the Filter by Previous Visits check box, and click the Add Locations button. Check the customer name (root name) check box to consider the visit to all of the locations of ABC, and click Done.
   c) From the following drop-down lists, choose Atleast, 5 Times in This Year.

Step 9  In the Schedule area, do the following:
   a) Check the Set a date range for the rule check box, and specify the date range for the fortnight for which you want to provide the offer. Set the time also, if required.
   b) Check the Filter by days of the week check box, and click Sat and Sun.

Step 10  In the Actions area, do the following:
   a) From the Notify drop-down list, choose Consumer.
   b) From the adjacent three drop-down lists, choose Once in, 1, and Visits, respectively.
   c) Check the Via Email check box.
   d) In the From Name field, enter the email name that must be displayed to the customer, and in the From Email field, enter the email ID that must be displayed to the customer.
   e) In the Subject field enter a subject for the email. If required, edit the message in the following text box.
   f) Check the Via SMS check box, specify the SMS gateway. If required, edit the content in the following text box.

   Note This configuration is to send the notification even if the app notification fails. In addition, the customers who are not an app user, get the notification through SMS.

Step 11  Click Save and Publish.

The rule gets published.

Creating an Engagement Rule for a Business User

Before creating an engagement rule, ensure that the prerequisites are met. For more information on the prerequisites to create an engagement rule, see the “Prerequisites for Creating an Engagement Rule” section.

You can send the notifications to the business users such as employees through Cisco Webex Teams, SMS, or e-mail. You can also send notifications to an external API.

To define an engagement rule to send notifications to the business users or an external API, perform the following steps:

Step 1  In the Cisco DNA Spaces dashboard, choose Engagements.

Step 2  On the Engagements window that appears, click Create New Rule.
Creating an Engagement Rule for a Business User

Step 3
In the Rule Name field, enter a name for the engagement rule.

Step 4
From the When a user is on WiFi and drop-down list, choose any of the following:

- **Entering a Location**: Choose this option if you want to send the notification to the business user, when a visitor connected to the Wi-Fi enters the location.

- **Away from the Location**: Choose this option if you want to send the notification to the business user, when a visitor connected to the Wi-Fi is away from the location for a specified time. If you are selecting this option, from the For scroll list, choose the number of minutes a visitor needs to be away from the location for sending notifications.

  **Note**
  - The Exiting Location option is no more available. If you are editing an existing Engagement Rule with Exiting Location configured, the Choose User Activity drop-down list will appear without any selection. You must choose the required option from the Choose User Activity drop-down list to save the rule successfully.
  - Even if a visitor is physically present in the location, but gets disconnected from the Wi-Fi for the minutes specified in the For scroll list, the visitor will be considered for sending notification.

- **Present at Location**: Choose this option if you want to send notification to the business user, when a visitor who is connected to the Wi-Fi is present at the location for a specified duration or at a particular time. If you choose this option, additional fields appear where you can mention the duration or time that needs to be met by the customer to get filtered for this rule.

Step 5
In the Locations area, specify the locations for which you want to send the notifications.

You can configure to send notifications for the entire customer name or a single or multiple locations such as group, floor, or zone. You can add the locations of different wireless networks such as Cisco Meraki, Cisco Wireless Controller, and so on in an Engagement rule.

You can again filter the locations for which the notification is to send based on the metadata defined for the selected location or its parent or child locations. You can either send the notifications for the locations with a particular metadata or exclude the locations with a particular metadata. For more information on defining the locations for the engagement rule, see the Location Filter for an Engagement Rule, on page 168.

Step 6
In the Identify area, specify the type of customers for whom you want to send the notifications to the business users.

**Note**
You can filter the customers for whom you want to send the notifications to the business users based on whether the customer is an opted in or not opted in user, the tags the customers belong to, and the number of visits made by the customer. You can apply all these filters or any of them based on your requirement.

To specify the customers for whom the notification is to send to the business user, perform the following steps:

a) If you want to filter the customers by the opt in status, check the Filter by Opt-In Status check box, and choose whether you want to send the notifications for opted in users or not opted in users.

b) If you want to filter the customers based on tags, check the Filter by Tags check box.

   You can filter the tags in two different ways. Either you can specify the tags for which the notifications are to send or you can specify the tags for which the notifications must not be sent. You can choose the best filtering method based on your requirement. For example, if you want to send the notifications to the business users for all tags except for one tag, it is easy to opt the exclude option, and mention that particular tag for which you do not want to send the notifications.

   c) If you want to filter the customers based on the number of visits made by the customer in the selected locations, check the Filter by Previous Visits check box.
Click the **Add Locations** button. In the **Choose Locations** window, specify the locations of which the customer visit needs to consider for filtering. In the following fields, mention the number of visits and duration required to send notifications. For more information on the visits and duration you can configure, see the “Previous Visit Criteria” section.

**Step 7**

In the **Schedule** area, specify the period for which you want to apply the engagement rule.

a) Check the **Set a date range for the rule** check box, and in the fields that appear specify the start date and end date for the period for which you want to apply the engagement rule.

b) Check the **Set a time range for the rule** check box, and in the fields that appear specify the time range for which you want to apply the engagement rule, within the date range specified.

c) If you want to apply the rule only on particular days, check the **Filter by days of the week** check box, and from the list of days that appears, click the days on which you want to apply the engagement rule.

**Step 8**

In the **Actions** area, perform the following steps:

a) From the Notifiy drop-down list, choose **Business**, and from the adjacent drop-down list choose any of the following:

   • **Only Once** — The notification is sent only once to a business user.

   • **Once In** — The notification is sent more than once to a business user based on the notification frequency specified. In the additional fields that appear when you choose this option, specify the notification frequency. For more information on the notification frequency, see the “Notification Frequency” section.

   • Specify the mode of notification. You can send the notification to the customers through Cisco Webex Teams, e-mail, SMS. You can also send the notification to an external API. For more information on notification types, see **Notification Type for a Business User**, on page 170


**Note**

To display the variables such as first name, last name, mobile number, and so on in the notification message, you must configure the data capture form in the portal. For more information on configuring the data capture form in the portal, see the “Adding a Data Capture Form to a Portal” section.

**Note**

The summary of the rule is shown in the right side of the page.

**Step 9**

Click **Save and Publish**.

The rule gets published and listed in the Engagement Rules page.

**Note**

If you do not want to publish the rule now, you can click the **Save** button. You can publish the rule at any time later by opening the rule, and clicking the **Save and Publish** button. Also, you can publish the rule by clicking the **Make Rule Live** icon at the far right of the rule in the Engagement Rules page.

---

**Use Case: Engagement Rule for a Business User**

ABC is a hotel group with hotels around the globe. ABC has many privilege customers, mainly business people, who use its hotels. As part of its 25th anniversary, ABC wants to provide some special gifts to its platinum loyalty members who visits its first hotel at location A. ABC considers all the customers who had visited its hotels at location A or location C minimum 10 times in the last 2 years as platinum loyalty members.

ABC wants its customer care representative to directly go and meet the customer, and gift the customers. ABC wants to send notifications to its customer care representative regarding the arrival of the platinum loyalty members through SMS. The notifications need to send for the opted in users when the customer enters
the location. The notifications are to send only for the current month. ABC wants to send the notifications only once for a customer.

To meet the preceding scenario, perform the following steps:

**Step 1**
Log in to Cisco DNA Spaces.

**Step 2**
Create the location hierarchy with all the locations of ABC.

**Step 3**
Create a tag for the platinum loyalty members, **Platinum**, using the Profile Rule. The rule must be to filter the customers visited the location A or location C at least 10 times in last 2 years.

**Step 4**
In the Cisco DNA Spaces dashboard, click **Engagements**.

**Step 5**
On the **Engagements** window that appears, click **Create New Rule**.

**Step 6**
In the **RULE NAME** field, enter a name for the engagement rule.

**Step 7**
In the **When a user is on WiFi and** drop-down list, choose **Entering Location**.

**Step 8**
In the Locations area, click the **Add Locations** button, and select location A, the location where ABC wants to provide the gifts to the customers.

**Step 9**
In the **Identify** area, do the following:
   a) Check the **Filter by Opt-In Status** check box, and choose **Only for opted-in Visitor**.
   b) Check the **Filter by Tags** check box, and click the **Add Tags** button for Include.
   c) In the **Choose Tags** window, click the **Include** radio button for **Platinum1**, created at step 3, and click **Done**.

**Step 10**
In the Schedule area, do the following:
   a) Check the **Set a date range for the rule** check box, and specify the start date and end date of the current month for which ABC want to provide the offer.

**Step 11**
In the Actions area, do the following:
   a) From the Notify drop-down list, choose **Business**.
   b) From the adjacent drop-down list, choose **Only Once**.
   c) Check the **Via Email** check box. In the From field, specify the From e-mail ID that must appear in the e-mail, in the “To” field, enter the e-mail ID of the business user to whom you want to send the notification, and in the Subject field, enter a subject for the notification e-mail. If required, edit the notification message displayed in the following text editor.

The e-mail ID entered in the **From** field must be included in the allowed list for e-mail IDs. To include the e-mail ID in the allowed list, contact Cisco DNA Spaces support team.

**Step 12**
Click **Save and Publish**.

The engagement rule is published.

---

**What to do next**

Now, when an opted in platinum loyalty member enters the premises of location A, a notification is sent to the customer care representative of location A.
Managing Engagement Rules

Pausing an Engagement Rule

To pause an engagement rule, perform the following steps:

Step 1
In the Cisco DNA Spaces dashboard, click Engagements.

The Engagements window appear with all the engagements rules listed.

Step 2
Click the Pause Rule icon that appears at the far right of the engagement rule that you want to pause.

Step 3
In the window that appears, confirm pausing.

The engagement rule is paused.

What to do next

Note
To pause multiple engagement rules, check the check box for the engagement rules that you want to pause, and click the Pause button that appears at the bottom of the page.

Restarting an Engagement Rule

To restart an engagement rule, perform the following steps:

Step 1
In the Cisco DNA Spaces dashboard, click Engagements.

The Engagements window appear with all the engagements rules listed.

Step 2
Click the Make Rule Live icon that appears at the far right of the engagement rule that you want to restart.

The engagement rule is restarted.

What to do next

Note
To restart multiple engagement rules, check the check box for the engagement rules that you want to restart, and click the Make Live button that appears at the bottom of the window.
Modifying an Engagement Rule

To modify an engagement rule, perform the following steps:

**Step 1**
In the Cisco DNA Spaces dashboard, click **Engagements**.
The **Engagements** window appears with all the engagements rules listed.

**Step 2**
Click the **Edit Rule** icon that appears at the far right of the engagement rule that you want to modify.

**Step 3**
Make necessary changes.

**Step 4**
To save the changes, click **Save** or to publish the changes, click **Save and Publish**.

*Note* 
A live rule will have only the **Save and Publish** button. When you click the **Save and Publish** button, the rule gets published with the changes.

Deleting an Engagement Rule

To delete an engagement rule, perform the following steps:

**Step 1**
In the Cisco DNA Spaces dashboard, click **Engagements**.
The **Engagements** window appears with all the engagements rules listed.

**Step 2**
Click the **Delete Rule** icon that appears at the far right of the engagement rule that you want to delete.

**Step 3**
In the window that appears, confirm deletion.

What to do next

*Note*
To delete multiple engagement rules, check the check box for the engagement rules that you want to delete, and click the **Delete** button that appears at the bottom of the window.

Viewing an Engagement Rule for a Location

To view an engagement rule for a location such as group, building, floor, and so on, perform the following steps:

**Step 1**
Click the three-line menu icon at the top-left of the Cisco DNA Spaces dashboard.

**Step 2**
Choose **Location Hierarchy**.

The **Location Hierarchy** window appears with the location hierarchy.

**Step 3**
Click the location for which you want to view the engagement rule.
Step 4 Click the **Rules** tab.

Step 5 Click the **Engagement Rule** tab.

The engagement rules for the location gets listed.

### What to do next

You can also access the **Rules** tab by clicking the **Rules** link that appears for each location in the location hierarchy. The **Rules** link for a location is enabled only if at least one proximity rule exists for that location.

### Engagement Rule Report

Cisco DNA Spaces allows you to view the report that is specific to each engagement rule. This report displays the details of the rule activity and the user engagement for a specific rule.

To view the Engagement Rule report for an engagement rule, perform the following steps:

1. In the Cisco DNA Spaces dashboard, choose **Home**.
2. In the My Apps area, choose **Engagements**.
   
   Click the rule for which you want to the Engagement Rule Report.

3. In the Filter area, choose the period for which you want to view the report.

   The report is filtered for the specified period.

   The Engagement Rule report has the following sections.

### Rule Activity

This section displays the details of notifications sent based on the particular engagement rule.

- **Daily Engagements**—Displays the ratio “the total number of notifications sent” to “the unique customers to whom the notifications are sent”, on each day based on the particular engagement rule. X-axis represents the days in the filtered period. Y-axis represents the number of notifications sent. You can view the data for a particular day by hovering the mouse in the graph in the area for the day.

- **Engagements**—This section displays the total number of notifications sent for each of the targeted locations.

- **Engagement by Time of Day**—This bar graph displays the number of notifications sent to the customers during various timings in a day. This helps you to identify at what time the customers filtered for the rule are present in your business premises, and target them accordingly.
Visitor Engagement

The Visitor Engagement report shows the details of engagements with the visitors based on the Engagement Rule you have configured. To access the Visitor Engagement report, in the Engagements window, click the three-line menu icon at the top-left of the window, and then click Visitor Engagement.

Engagements

Total Engagements - The total number of engagements (through SMS or e-mail notifications) with the visitors, who have visited the selected location, during the specified period. This metrics for all the locations from the date of installation of the Cisco DNA Spaces is shown at the top of the report for “Total Engagements with Visitors”.

Via SMS - The total number of engagements through SMS to the visitors who have visited the selected during the specified period. The percentage of engagements through SMS out of total engagements is also displayed.

Via Email - The total number of engagements through e-mail to the visitors who have visited the selected during the specified period. The percentage of engagements through e-mail out of total engagements is also displayed.

Daily Trends of Engagements

This section displays a line graph that shows the number of engagements from the location on each day of the specified period through various notification types such as SMS, e-mail and so on. The color indicators for various notification types are displayed at the top of the graph. Mouse-over the graph to view the engagement details for a particular day.

Engagement Rule Report

This section lists the report for various Engagement Rules. The date on which the rule is published is shown along with the total number of engagements made based on the rule. You can view the detailed report for a particular Engagement rule by clicking the corresponding rule. For more information on Engagement rule report, see Engagement Rule Report, on page 165.

Engagement URL

The Engagement URL refers to the URL that is provided in the SMS and e-mail notification messages that are sent to the customers. For business users, you can add the engagement URL in the SMS notifications. The users can click this URL to view a site page that is relevant to the notification. For example, you can provide a site page with more information on the discounts and offers available to the customer. You can create this site page using any site development application.

Previous Visit Criteria

You can define various criteria for filtering the customers based on their previous visits.

• Atleast ..Times — The rule is applied when the number of customer visits meets the number specified.
• Last 1 day — The rule is applied if the number of customer visits in the last one day meets the number specified.
• **Last 7 days**—The rule is applied if the number of customer visits in the last 7 days meets the number specified.

• **Last 15 days**—The rule is applied if the number of customer visits in the last 15 days meets the number specified.

• **Last 30 days**—The rule is applied if the number of customer visits in the last 30 days meets the number specified.

• **Last 90 days**—The rule is applied if the number of customer visits in the last 90 days meets the number specified.

• **This Weekend**—The rule is applied if the number of customer visits in the current week meets the number specified.

• **This Month**—The rule is applied if the number of customer visits in the current month meets the number specified.

• **This Year**—The rule is applied if the number of customer visits in the current year meets the number specified.

• **Date Range**—The rule is applied if the number of customer visits during a particular period meets the number specified. If you choose this option, additional fields appear where you can mention the start date and end date for the period.

• **Between, . Times**—The rule is applied when the number of customer visits comes within the number range specified.

  • **Last 1 day**—The rule is applied if the number of customer visits in the last one day comes with in the number range specified.

  • **Last 7 days**—The rule is applied if the number of customer visits in the last 7 days comes with in the number range specified.

  • **Last 15 days**—The rule is applied if the number of customer visits in the last 15 days comes with in the number range specified.

  • **Last 30 days**—The rule is applied if the number of customer visits in the last 30 days comes with in the number range specified.

  • **Last 90 days**—The rule is applied if the number of customer visits in the last 90 days comes with in the number range specified.

  • **This Week**—The rule is applied if the number of customer visits in the current week comes with in the number range specified.

  • **This Month**—The rule is applied if the number of customer visits in the current month comes with in the number range specified.

  • **This Year**—The rule is applied if number of customer visits in the current year comes with in the number range specified.

  • **Date Range**—The rule is applied if the number of customer visits during a particular period comes with in the number range specified. If you choose this option, additional fields appear where you can mention the start date and end date for the period.
Notification Types

Cisco DNA Spaces enables you to send the notifications in the following formats:

- **SMS**—To send the notification as an SMS. For business users, you can define the mobile number to which you want to send the notification.
- **Email**—To send the notification as an e-mail. For business users, you can define the e-mail address to which you want to send the notification.
- **API Notifications**—To send an API notification to an external application. Cisco DNA Spaces enables you to send the notification to a third party application. This notification type is not applicable for customers.
- **Cisco Webex Teams**—To send the notification to the Webex Team account of the business user. This notification type is not applicable for customers. To use this notification type, you must have a Cisco Webex account.

Notification Frequency

The frequency at which you want to send the notification for an engagement rule. You can configure the engagement rule for the following notification frequencies:

- **Only Once**—To send the notification only once to a user.
- **Once in**—To send the notification once in the interval specified.
  - **Visits**—To send the notification when the number of customer visits meet the number specified.
  - **Hours**—To send the notification once in the number of hours specified.
  - **Days**—To send the notification once in the number of days specified.
  - **Weeks**—To send the notification once in the number of weeks specified.
  - **Months**—To send the notification once in the number of months specified.

Location Filter for an Engagement Rule

To specify the locations for which you want to send the notifications, perform the following steps:

1. Click the **Add Locations** button.
2. In the **Choose Locations** window that appears, check the check box for the locations for which you want to send the notifications.
3. Click **Done**.

You can again filter the locations using the metadata defined for the locations. Only the metadata defined for the selected locations and their parent or child locations will be available for selection.
To send notifications only for the locations with a particular location metadata, perform the following steps:

1. Check the **Filter by Metadata** check box.
2. In the **Filter** area, click the **Add Metadata** button.
   
   The **Choose Location Metadata** window appears.
3. From the drop-down list, choose the metadata variable, and choose the value for the variable in the adjacent field.
4. Click **Done**.

To exclude to send notifications for the locations with a particular metadata, perform the following steps:

1. Check the **Filter by Metadata** check box.
2. In the **Exclude** area, click the **Add Metadata** button.
   
   The **Choose Location Metadata** window appears.
3. From the drop-down list, choose the metadata variable, and choose the value for the variable in the adjacent field.
4. Click **Done**.

---

**Notification Type for a Consumer**

In the Engagement rule, under the Actions area, specify the modes through which you want to send the notifications to the customer.

- If you want to send the notification through SMS, check the “Via SMS” check box. From the “SMS Gateway” drop-down list, choose the SMS gateway through which you want to send the SMS notification. You can use the **Demo Gateway** provided by Cisco, which is chargeable. For information on adding the SMS gateways, see the message content that is sent to the customer is displayed in the following text box. You can enhance the message content using variables. By default, the first name and last name of the customer, and engagement URL are added as variables. You can add more text variables in the message using the variables that lists below the text box when you click the text box. For more information on adding a text variable, see the **Smark Links and Text Variables for Engagements Rule and Density Rule** section.

   If required, in the Link field, enter the engagement URL that must appear in the notification. For more information on creating the engagement URL, see the **Engagement URL, on page 166** section.

- If you want to send the notification through e-mail, check the **Via Email** check box. In the **From Name** field, specify the name from which the customer receives the e-mail, in the **From Email** field, specify the e-mail ID from which the customer receives the e-mail, and in the **Subject** field, enter the subject for the notification e-mail. The message content that is sent to the customer is displayed in the following text box. You can enhance the message content using the text variables. By default, the first name and last name of the customer, and engagement URL are added as variables. You can add more text variables in the message using the variables that lists below the text box when you click the text box. For more information on adding a text variable, see the **Smark Links and Text Variables for Engagements Rule and Density Rule** section.
If required, in the Link field, enter the engagement URL that must appear in the notification. For more information on creating the engagement URL, see the Engagement URL, on page 166 section.

Note

- If you are using the Via Email option, you must ensure to add the e-mail ID entering in the From field in the allowed list of e-mail IDs. To include the e-mail ID in the allowed list, contact the Cisco DNA Spaces support team. If you do not want to use a specific e-mail ID, you can use the default allowed e-mail ID no-reply@dnaspaces.io. However, the default ID is not displayed in the dashboard automatically. So, you have to enter it manually.

- The variable “$firstName” is to display the first name of the customer, “$lastName” is to display the last name of the customer, “$email” is to display the e-mail address of the customer, “$mobile” is to display the mobile number of the customer”, “$URL” is to display the engagement URL, “$gender” is to display the gender of the customer”, and “$locationName” is to display the location from which the message is sent.

- To display the variables such as first name, last name, mobile number, and so on in the notification message, you must configure the data capture form in the portal. For more information on configuring the data capture form in the portal, see the Adding a Data Capture Form to a Portalsection.

Notification Type for a Business User

You can send notifications to the business users through Cisco Webex Teams, SMS and e-mail. You can also send the notifications to an API end point.

- If you want to send the notification through Cisco Webex Teams, check the Via Cisco Webex Teams check box. From the Webex Accounts drop-down list, choose the Webex account to which you want to send the notifications. You can add a Webex account using the Add Webex Account option. To add a webex account, you must specify the webex developer account, and you must generate a token for the particular account using the Webex Developer site. Then you must configure the token in the Add Webex Account window within the timeout period shown for the token in the developer site. As an alternate to the default token, you can create Bots in the developer site, and can generate tokens without timeout limitations.

The message content that is sent to the business users is displayed in the Notification Message text box. You can enhance the message using the text variables. By default, the first name and last name of the customer, and the engagement URL are added as variables. You can add more text variables in the message using the variables that lists below the text box when you click the text box. For more information on adding a text variable, see the Smark Links and Text Variables for Engagements Rule and Density Rule section.

- If you want to send the notification through SMS, check the Via SMS check box. From the SMS Gateway drop-down list, choose the SMS gateway through which you want to send the SMS notification. You can use the Demo Gateway provided by Cisco, which is chargeable. In the To field that appears, enter the mobile number (with country code) of the business user to whom you want to send the notifications. If required, in the Link field, enter the engagement URL that must appear in the notification. For more information on configuring the engagement URL, see the Engagement URL, on page 166.

The message content that is sent to the business users is displayed in the following text box. You can enhance the message using the text variables. By default, the first name and last name of the customer, and the engagement URL are added as variables. You can add more text variables in the message using
the variables that lists below the text box when you click the text box. For more information on adding a text variable, see the Smark Links and Text Variables for Engagements Rule and Density Rule section.

- If you want to send the notification through e-mail, check the Via Email check box. In the From field, specify the “From e-mail ID” that must appear in the e-mail, in the To field, enter the e-mail ID of the business user to whom you want to send the notification, and in the Subject field, enter a subject for the notification e-mail.

  Note
  The e-mail ID entered in the From field must be included in the allowed list for e-mail IDs. To include the e-mail ID in the allowed list, contact Cisco DNA Spaces support team. If you do not want to use a specific e-mail ID, you can use the default allowed e-mail ID no-reply@dnaspaces.io. However, the default ID is not displayed in the dashboard automatically. So, you have to enter it manually.

  The message content that is sent to the business user is displayed in the following text box. By default, the first name and last name of the customer, and the engagement URL are added as variables. You can add more text variables in the message using the variables that lists below the text box when you click the text box. For more information on adding a text variable, see the Smark Links and Text Variables for Engagements Rule and Density Rule section. If required, in the Link field, enter the engagement URL that must appear in the notification. For more information on configuring the engagement URL, see the Engagement URL, on page 166.

  • If you want to send the notification to an external API, check the Trigger API check box. For more information on the configurations for Trigger API, see the “Trigger API Configuration for Notification” section.

Smark Links and Text Variables for Engagements Rule and Density Rule

In Engagement Rules and Density Rules, you can add text variables in the notification messages sent for all notification types (Via Cisco Webex Teams, Via SMS, Via Email, and Trigger API), and can create smart links for Trigger API URI. The varilables enable you to display the customer, location and device details in the notification message or Trigger API URI. By default, the notification message will have first name and last name of the customer. You can add additional additional details using the variables.

For example, assume that you have created an engagement rule to send SMS notifications to the customers and have configured the variables “mobile” and “gender” in the message text box for the SMS notification. Now, when a customer receives a SMS message based on this engagement rule, the mobile number and gender details of the customer are also shown in the message.

Note
Cisco DNA Spaces captures the personal details of the customers using the Data Capture form. That is, to include the personal details such as first name, last name, gender, and so on in the smart link or as text variable, you must configure the Data Capture form in the portal. For more information on adding a Data Capture form to a captive portal see the Adding a Data Capture Form to a Portal section.

You can include static and dynamic variables in the notification message and URLs.

The static variables that you can include in the notification message are as follows:
## Table 10: Static Variable List

<table>
<thead>
<tr>
<th>Static Variable Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$firstName</td>
<td>First name of the customer.</td>
</tr>
<tr>
<td>$lastName</td>
<td>Last name of the customer.</td>
</tr>
<tr>
<td>$email</td>
<td>E-mail address of the customer.</td>
</tr>
<tr>
<td>$mobile</td>
<td>Mobile number of the customer.</td>
</tr>
<tr>
<td>$gender</td>
<td>Gender of the customer.</td>
</tr>
<tr>
<td>$URL</td>
<td>URL link value.</td>
</tr>
<tr>
<td>$TotalAreaValue</td>
<td>The total area configured for the location in the <strong>Location Info</strong> window in <strong>Location Hierarchy</strong>.</td>
</tr>
<tr>
<td>$TotalAreaUnit</td>
<td>The total area unit configured for the location in the <strong>Location Info</strong> window in <strong>Location Hierarchy</strong>.</td>
</tr>
<tr>
<td>$TotalCapacity</td>
<td>The total capacity configured for the location in the <strong>Location Info</strong> window in <strong>Location Hierarchy</strong>.</td>
</tr>
<tr>
<td>$locationName</td>
<td>Name of the location for which the rule is triggered.</td>
</tr>
<tr>
<td>$buildingName (Only for Density Rules)</td>
<td>Building name of the location for which the notification is triggered.</td>
</tr>
<tr>
<td>$floorName (Only for Density Rules)</td>
<td>Floor name of the location for which the notification is triggered.</td>
</tr>
<tr>
<td>$zoneName (Only for Density Rules)</td>
<td>Zone name of the location for which the notification is triggered.</td>
</tr>
<tr>
<td>$deviceCount (Only for Density Rules)</td>
<td>Device count for the location for which the notification is triggered.</td>
</tr>
<tr>
<td>$locationPath (Only for Density Rules)</td>
<td>The location path (parent hierarchy) for the location for which the rule is triggered. The locations in the hierarchy will be separated by ‘&gt;’ (Sample Format: Account&gt;CMXNode&gt;Campus&gt;Building&gt;Floor&gt;Zone).</td>
</tr>
</tbody>
</table>

The **Trigger API** notification type will be having the following additional variables for both Engagements Rules and Density Rules.

<table>
<thead>
<tr>
<th>Static Variable Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$macaddress</td>
<td>The mac address of the device.</td>
</tr>
<tr>
<td>$encryptedMacAddress</td>
<td>The encrypted mac address of the device.</td>
</tr>
<tr>
<td>$deviceSubscriberId</td>
<td>The subscriber ID for the device in the database.</td>
</tr>
<tr>
<td>$optinStatus-</td>
<td>The opt in status for the customer.</td>
</tr>
</tbody>
</table>
The dynamic variables that you can include in the notification message and URLs for Engagements Rule and Density Rule are as follows:

**Table 11: Dynamic Variable List**

<table>
<thead>
<tr>
<th>Dynamic Variable Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Tags</td>
<td>The business tag to which the customer belongs to. The business tags configured in the Data Capture form are listed as variables. For more information on creating a business tag, see the Adding a Data Capture Form to a Portal section.</td>
</tr>
<tr>
<td>Location Metadata</td>
<td>The location metadata for the customer location. The location metadata keys defined in the location hierarchy are listed as variables. For more information on defining the location metadata, see the Adding Metadata for a Location section.</td>
</tr>
</tbody>
</table>

To include a smart link in the URL or text variable in the notification message, perform the following steps:

**Step 1**
To include smart link, click anywhere inside the URI field. To include text variable, click anywhere inside the notification message text box. To include text variable for Via Email, click the Smartlinks drop-down list in the rich text editor. The variables that you can include get listed.

**Step 2**
Choose the variables that you want to include.

**Trigger API Configuration for Notification**

To send notifications to an external API through the rules, in the Create [Rule Name] window, in the Actions area, perform the following steps:

1. Check the **Trigger API** check box.
2. From the **Method** drop-down list, choose the method for triggering API.

**Note**
You can add the customer details in the notification message, by adding the link variables in the API URI or text variables in the method parameters.

- **Get** — To send notification or customer details to the API using the “GET” method. If you choose this method, additional fields appear where you can mention the GET request headers and parameters to include additional details such as first name, last name, mobile number, and so on of the customer in the notification. You can add the request parameter keys defined in your API and mention the values for them using text variables. The value can be a hard-coded value or a variable. You can view the variables that you can add by clicking the “Value” field. You can add more **GET** headers and parameters using the corresponding **Add** button.
• **Post Form** — To send notification or customer details to the API using the “POST FORM” method. If you choose this method, additional fields appear where you can mention the POST FORM request headers and parameters to include additional details such as first name, last name, mobile number, and so on of the customer. You can add the form parameter keys defined in your API and mention the values for them. The value can be a hard-coded value or a variable. You can view the variables that you can add by clicking the “Value” field. You can add more “form parameters” using the **Add** button.

• **Post JSON** — To send notification or customer details to the API using the “POST JSON” method. If you choose this method, request header fields appear, along with a text box where you can mention the JSON data that is to send as notification message to the API. You can mention the values for various JSON request header fields defined in your API. The value can be a hard-coded value or a variable. You can view the variables that you can add by clicking the “Value” field. You can view the variables that you can add to the JSON Data by clicking the text box.

• **Post Body** — To send notification or customer details to the API using the "POST BODY" method. If you choose this method, an request header fields appear where you can mention the content that must be included in the notification sent to the API, along with a **Post Body Data** field. You can mention the values for various Body request header fields defined in your API. The value can be a hard-coded value or a variable. You can view the variables that you can add by clicking the “Value” field. You can view the variables that you can add to the **Post Body Data** field when you clicking the field.

---

**Note**

Only those data that you have configured to capture using the Data Capture form in the portal are included in the notifications.

3. In the URI field, enter the URI for the API. You can include additional details of the customers in the notification message using the smart links. To view the variables that you can include in the URI, click the **URI** field.

   • For information on variables that you can add for the Captive Portal Rule, see **Smart Links and Text Variables for Captive Portals**, on page 152

   • For information on variables that you can add for the Engagement or Density Rule, see **Smart Links and Text Variables for Engagements Rule and Density Rule**, on page 171
CHAPTER 10

Creating Tags with the Location Personas App

Cisco Digital Network Architecture (DNA) Spaces enables you to group the customers using tags. You can then use these tags in the Cisco DNA Spaces rules such as Engagement Rules. In Cisco DNA Spaces, you can create tags using the Location Personas app. You can also use the Location Personas app to add more customers to the existing tags, or to remove certain customers from an existing tag. You can group a customer under multiple tags.

When you are creating a tag, you can use the existing tags to filter the customers from the selected locations. For example, if you want to create a tag with location A and location B, but only for android users, you can use the tag filter to remove the tag for iOS.

- Creating or Modifying Tags Using a Location Personas App, on page 175
- Use Case: Location Personas Rule (Profile Rule), on page 177
- Managing Location Personas Rules, on page 180
- Location Personas Rule Report, on page 182

Creating or Modifying Tags Using a Location Personas App

To create a tag, or to include the customers to or exclude the customers from an existing tag, perform the following steps:

Step 1 In the Cisco DNA Spaces dashboard, click Location Personas.
Step 2 In the Location Personas window that appears, click Create New Rule.
Step 3 In the Rule Name field, enter a name for the Location Personas / Profile rule.
Step 4 From the When a user is on WiFi and drop-down list, choose any of the following:
  - Entering a Location: Choose this option if you want to tag the visitors with Wi-Fi connected, when they enter the location.
  - Away from the Location: Choose this option if you want to tag the visitors with Wi-Fi connected and are away from the location for a specified time. If you are selecting this option, from the For scroll list, choose the number of minutes a visitor needs to be away from the location for tagging based on the this rule.
• The **Exiting Location** option is no more available. If you are editing an existing **Location Personas** rule with **Exiting Location** configured, the **Choose User Activity** drop-down list will appear without any selection. You must choose the required option from the **Choose User Activity** drop-down list to save the rule successfully.

• Even if a visitor is physically present in the location, but gets disconnected from the Wi-Fi for the minutes specified in the **For** scroll list, the visitor will be considered for tagging for this rule.

**Step 5**

In the **Locations** area, specify the locations of which you want to filter the customers for the rule.

You can choose the entire customer name or single or multiple locations such as group, campus, building, floor, or zone. You can add the locations of both CUWN and Cisco Meraki.

You can again filter the locations based on the metadata defined for the selected location or its parent or child locations. You can either choose the locations with a particular metadata or exclude the locations with a particular metadata. For more information on configuring the location for the profile rule, see the Location Filter for a Location Persons Rule, on page 179

**Step 6**

In the **Identify** area, specify the type of customers that you want to filter for the rule.

**Note**

You can filter the customers based on whether the customer is an opted in or not opted in user, the tags the customers belong to, the number of visits made by the customer, and the status of the app in the customer’s device. You can apply all these filters or any of them based on your requirement.

To specify the customers whom you want to filter for the rule, perform the following steps:

a) If you want to filter the customers by the **Opt In Status**, check the **Filter by Opt-In Status** check box, and choose whether you want to filter the opted in users or not opted in users for the rule.

**Note**

For more information on opted in users, see the Opted In Option for Users, on page 179.

b) If you want to filter the customers based on the tags, check the **Filter by Tags** check box.

**Note**

You can filter the customers by including or excluding existing tags. You can filter the tags in two different ways. Either you can specify the existing tags of which you want to include the customers for the rule or the existing tags of which you want to exclude the customers for the rule. You can choose the best filtering method based on your requirement. For example, if you want to add the customers of all the existing tags expect one tag, it is easy to opt the exclude option, and mention that particular tag of which you want to exclude the customers.

For more information on using the tag filter, see the Filtering by Tag, on page 178.

c) If you want to filter the customers based on the number of visits made by the customer in the selected locations, check the **Filter by Previous Visits** check box.

Click the **Add Locations** button. In the **Choose Locations** window, specify the locations of which the customer visit needs to consider for filtering. In the following fields, mention the number of visits and duration required to be met by the customers to be filtered for the rule.

d) If you want to filter the customers based on the customer’s app status, check the **Filter by App Status** check box, and choose whether you want to filter the app user or non app user for the rule.

**Step 7**

In the **Schedule** area, specify the period for which you want to apply the rule for filtering the customers.
Only those customers who meet the preceding conditions during the period specified are filtered for the rule.

a) Check the **Set a date range for the rule** check box, and in the fields that appear, specify the start date and end date for the period for which you want to apply the profile rule.

b) Check the **Set a time range for the rule** check box, and in the fields that appear, specify the time range for which you want to apply the profile rule.

c) If you want the rule to be executed only on particular days, check the **Filter by days of the week** check box, and from the list of days that appears, click the days on which you want to apply the rule.

**Step 8**

In the Actions area, specify whether you want to create a new tag by including or excluding the customers filtered based on the preceding conditions, or to include or exclude the filtered customers from an existing tag.

a) Click the **Add Tags** button.

- If you want to add or remove the filtered customers from the existing tags, mention the tags to which you want to include the filtered customers and the tags from which you want to exclude the filtered customers.

- To add the customers that are filtered based on this profile rule to an existing tag, choose the Add radio button for the tags to which you want to add the customers.

- To remove the customers that are filtered based on this profile rule from an existing tag, choose the Remove radio button for the tags from which you want to remove the customers.

**Note**

In the **Choose Tags** window, you can search for a tag using the Search option. The tags selected are displayed on the right side of the window.

- If you want to create a new tag with the rule, click the **Create New Tag** button. In the “Enter the tag name” field that appears, enter a name for the tag, and click **Add**. The newly created tag gets listed in the tag list. Choose whether you want to include or exclude the filtered customers from the tag.

b) Click **Done**.

**Note**

Using a profile rule, you can create a tag by including or excluding the filtered customers, or you can modify an existing tag by including or excluding the filtered customers, simultaneously. You can also create more than one tag for a rule.

**Note**

The summary of the rule is shown on the right side of the page.

**Step 9**

Click **Save and Publish**.

The rule gets published and listed in the Profile Rules page.

**Note**

If you do not want to publish the rule now, you can click the Save button. You can publish the rule at any time later by clicking the **Save and Publish** button. Also, you can publish the profile rule by clicking the **Make Rule Live** icon at the far right of the rule on the **Location Personas** window.

---

**Use Case: Location Personas Rule (Profile Rule)**

ABC hotel group as part of its 25th anniversary wants to provide some special gifts to its platinum loyalty members. ABC considers all the customers who had visited its hotels at location A or location C minimum 10 times in the last 2 years as platinum loyalty members. All the visitors who have connected to the Wi-Fi at least 45 minutes are to consider as customers. ABC wants to create a tag for its platinum loyalty members.
The opted in customers who meet the previous conditions within the end of the current month are to add to the tag.

To meet the preceding scenario, perform the following steps:

**Step 1** Log in to Cisco DNA Spaces.
**Step 2** Create the location hierarchy with all the locations of ABC.
**Step 3** In the Cisco DNA Spaces dashboard, click **Location Personas**.
**Step 4** In the **Location Personas** window that appears, click **Create New Rule**.
**Step 5** In the **Rule Name** field, enter a name for the profile rule.
**Step 6** From the **When a user is on WiFi and** drop-down list, choose **Present at Location**, and from the drop-down list that appears, choose **45 Minutes**.
**Step 7** In the Locations area, click the **Add Locations** button, and select location A, and location C.
**Step 8** In the **Identify** area, do the following:
   a) Check the **Filter by Opt-In Status** check box, and choose **Only for opted-in Visitor**.
   b) Check the **Filter by Previous Visits** check box, and click the **Add Locations** button, and add Location A, and Location C.
   c) In the following fields, choose **At least**, **10** times in, and **Date Range**, respectively.
   d) In the date range fields, enter the start date and end date for the last two years.
**Step 9** In the Schedule area, check the **Set a date range for the rule** check box, and specify the start date as today’s date and end date as last date of the current month.
**Step 10** In the Actions area, do the following:
   a) Click the **Add Tags** button.
   b) In the **Create Tags** window, Click **Create New Tag**.
   c) In the **Enter the tag name** field, enter **Platinum1**, and click **Add**. In the Tag list, click the **Include** radio button for Platinum1, and click **Done**.
**Step 11** Click **Save and Publish**.
The profile rule is published.

---

**Filtering by Tag**

You can either opt to include or exclude the tags for filtering.

**Including a Tag**

To include a tag, perform the following steps:

**Step 1** In the **Filter by Tags** area of the proximity rule (captive portal rule, engagement rule, profile rule), click the **Add Tags** button for **Include**.
**Step 2** In the **Choose Tags** window, click the **Include** radio button for the tag that you want to include.
**Step 3** Click **Done**.
Excluding a Tag

To exclude a tag, perform the following steps:

**Step 1** In the Filter by Tags area of the proximity rule (captive portal rule, engagement rule, profile rule), click the Add Tags button for Exclude.

**Step 2** In the Choose Tags window, click the Exclude radio button for the tag that you want to exclude.

**Step 3** Click Done.

Searching for a Tag

To search for a tag, perform the following steps:

**Step 1** In the window to create a new rule, in the Filter by Tags area, click the Add Tags button for Include or Exclude.

**Step 2** In the Choose Tags window, enter the name of the tag that you want to search.

The tag list gets filtered with the search results.

Clearing a Tag

If you choose an include or exclude radio button for a tag, you can clear the selection using the Clear Selection option for that tag.

Opted In Option for Users

Cisco DNA Spaces enables you to provide an option in the captive portal for the customers to opt out from the notification subscriptions.

In the portal, check the Allow users to opt in to receive message check box to provide an option for the customers to opt for the subscriptions. The option Allow users to opt in to receive message is available for the authentication types SMS with password verification or Email.

By default, the customers are opted in for subscription. The customers can opt out from subscription when accessing the captive portal. When a customer accesses the captive portal by connecting to an SSID, the opt in check box is displayed to the customer.

Location Filter for a Location Persons Rule

To specify the locations, perform the following steps:

1. Click the Add Locations button.
2. In the Choose Location window that appears, select the locations for the profile rule.
3. Click OK.
You can again filter the locations using the metadata defined for the locations. Only the metadata defined for the selected locations and their parent or child locations will be available for selection.

To include a locations with a particular metadata, perform the following steps:

**Step 1** Select the **Filter by Metadata** check box.

**Step 2** In the Filter area, click the **Add Metadata** button.

The **Choose Location Metadata** window appears.

**Step 3** From the drop-down list, choose the metadata variable, and choose the value for the variable in the adjacent field.

**Step 4** Click **Done**.

To exclude a location with a particular metadata, perform the following steps:

**Step 1** Select the **Filter by Metadata** check box.

**Step 2** In the Exclude area, click the **Add Metadata** button.

The **Choose Location Metadata** window appears.

**Step 3** From the drop-down list, choose the metadata variable, and choose the value for the variable in the adjacent field.

**Step 4** Click **OK**.

### Managing Location Personas Rules

You can pause a Location Personas (Profile) Rule and make it live again, whenever required. You can modify a Location Personas rule, and delete it if required. You can create Location Personas rules specific to a location, and view them from the location hierarchy.

### Pausing a Location Personas Rule

To pause a Location Personas rule, perform the following steps:

**Step 1** In the Cisco DNA Spaces dashboard, click **Location Personas**.

The **Location Personas** window appears with all the existing Location Personas rules.

**Step 2** Click the **Pause Rule** icon that appears at the far right of the Location Personas rule that you want to pause.

The Location Personas rule is paused.
What to do next

Note To pause multiple Location Personas rules, check the check box for the Location Personas rules that you want to pause, and click the Pause button that appears at the bottom of the window.

Restarting a Location Personas Rule

To restart a Location Personas rule, perform the following steps:

Step 1 In the Cisco DNA Spaces dashboard, click Location Personas.
The Location Personas window appears with all the existing Location Personas rules.

Step 2 Click the Make Rule Live icon that appears at the far right of the Location Personas rule that you want to restart.
The Location Personas rule is restarted.

What to do next

Note To restart multiple Location Personas rules, check the check box for the Location Personas rules that you want to restart, and click the Make Live button that appears at the bottom of the window.

Modifying a Location Personas Rule

To modify a Location Personas rule, perform the following steps:

Step 1 In the Cisco DNA Spaces dashboard, click Location Personas.
The Location Personas window appears with all the existing Location Personas rules.

Step 2 Click the Edit Rule icon for the Location Personas rule that you want to modify.

Step 3 Make necessary changes.

Step 4 To save the changes, click Save or to publish the changes, click Save and Publish.

Note A live rule will have only the Save and Publish option. When you click the Save and Publish button, the rule gets published with the changes.

Deleting a Location Personas Rule

To delete a Location Personas rule, perform the following steps:
Step 1  In the Cisco DNA Spaces dashboard, click Location Personas.
The Location Personas window appears with all the existing Location Personas rules.
Step 2  Click the Delete Rule icon that appears at the far right of the Location Personas rule that you want to delete.

What to do next

Note  To delete multiple Location Personas rules, check the check box for the Location Personas rules that you want to delete, and click the Delete button that appears at the bottom of the window.

Viewing a Location Personas Rule for a Location

To view an Location Personas rule for a location such as group, building, floor, and so on, perform the following steps:

Step 1  Click the three-line menu icon at the top-left of the Cisco DNA Spaces dashboard.
Step 2  Choose Location Hierarchy.
The Locations window appears with the location hierarchy.
Step 3  Click the location for which you want to view the Location Personas rule.
Step 4  Click the Rules tab.
Step 5  Click the Profile Rule tab.
The Location Personas rules for the location gets listed.

What to do next

Note  You can also access the Rules tab by clicking the Rules link that appears for each location in the location hierarchy. The Rules link for a location is enabled only if at least one proximity rule exists for that location.

Location Personas Rule Report

The Location Personas Rule report shows the performance of Location Personas rules. It is specific to a Location Personas rule.
To view the Location Personas (Profile) Rule report for a Location Personas rule, perform the following steps:
Step 1  In the Cisco DNA Spaces dashboard, click **Location Personas**.
The **Location Personas** window appears with all the existing Location Personas rules.

Step 2  Click the rule for which you want to the Location Personas Rule Report.

Step 3  In the Filter area, choose the period for which you want to view the report.

- **Total Devices Tagged**—The total number of devices tagged for the Location Personas rule from the day on which the Location Personas rule is created.

- **Total Users Tagged**—The total number of visitors tagged for the particular Location Personas rule from the day on which the Location Personas rule is created.

- **Total Tags Removed**—The total number of visitors removed from the tags mentioned in the Location Personas rule from the day on which Location Personas rule is created.

---

**Rule Activity**

This section displays the number of customers and devices tagged based on the particular Location Personas rule during the specified period.

- **Tagging Trends**—Displays the total number of devices and customers tagged for the particular rule during the specified period. Also displays the number the customers removed from the tags based on the particular Location Personas rule. The line graph represents the total number of tags added or removed on each day of the specified period. If the duration specified is less than a week, the data will be shown in a bar graph. If the duration specified is not more that 2 days, the graph displays the number of customers tagged at various timings of each day.

- **Tags Added**—Displays the total number of tags created for the rule.

- **Device Tags added by Location**—Displays the number of devices tagged from each location during the specified period.

- **Tags Removed by Location**—This section will be displayed only if it is specified in the Location Personas rule to remove the filtered devices from a particular tag. The total number of devices untagged from each location based on the particular Location Personas rule during the particular period is shown.

- **Tagging by Time of Day**—This bar graph displays the number of customers added to various tags based on the Location Personas rule, at various timings of a day, during the specified period. This helps in identifying the time at which the customers targeted by this rule visits the targeted locations the most.
Cisco DNA Spaces Asset Locator App

The Cisco DNA Spaces Asset Locator app enables you to monitor assets and optimize the performance of your assets, sensors, alerting system, and operational work flows.

- Working with the Cisco DNA Spaces Asset Locator App, on page 185

Working with the Cisco DNA Spaces Asset Locator App

The Cisco DNA Spaces Asset Locator app provides a range of tags and sensors to continually integrate, monitor, and manage your connected operations. Using its cloud-based interface, you can define the profile, category, and ownership of each assets. You can establish business rules to define work flows, and the expected operating range of your assets and sensors.

For more information on Cisco DNA Spaces Asset Locator, see Asset Locator.
Working with the Cisco DNA Spaces Asset Locator App
CHAPTER 12

Monitoring

This chapter describes the monitoring details that are displayed in Cisco DNA Spaces.

To access the Monitor window, in the Cisco DNA Spaces dashboard, click the three-line menu icon at the top-left, and choose Monitor.

- Monitoring, on page 187
- App Latency, on page 190
- Enterprise Apps, on page 190
- Partner Apps, on page 190

Monitoring

This section describes Cisco DNA Spaces health details that are displayed in the Monitor section.

The Monitor section of Cisco DNA Spaces is shown in the following figure:
The header of the monitoring section will be having the following details:

- **All Locations connected**: Displays the current location update status for the locations to which you have access. This section will be marked as up if location updates are received from all the locations, and the status will be **All Locations Connected**. If there is any location update issue, this section will be marked as down, and the total number of locations that have location update issue will be displayed.

- **No Anomalies Reported**: Displays the current status of location updates and internet provisioning (this is applicable only if you have configured customer acquisition through captive portals) in the locations. This section is marked as up if location updates and internet provisioning are happening for all the locations without any issues. If any of them is not happening for any location, the status will be down. If both location update and internet provisioning are not happening for a location, such locations will be listed out.

- **DNA Apps**: Displays the current status of Cisco DNA Spaces apps. This section is marked as up if all the Cisco DNA Spaces apps are currently active.

- **Partner apps**: Displays the current status of partner apps that you have integrated with Cisco DNA Spaces. This section is marked as up if the partner apps that are integrated with Cisco DNA Spaces are functioning as expected. This section will be marked as down, if you have not integrated any partner app with Cisco DN Spaces or if the partner apps are not functioning as expected.

- **Enterprise Apps**: Displays the current status of enterprise apps that you have integrated with Cisco DNA Spaces. This section is marked as up if the enterprise apps that are integrated with Cisco DNA Spaces are functioning as expected. This section will be marked as down, if you have not integrated any enterprise app with Cisco DNA Spaces or if the enterprise apps are not functioning as expected.

- **App Latency**: This area displays the current latency status for the apps.
**Location Updates**

The locations for which the location updates are not happening currently are listed in this area. This area also displays a bar that shows location update status for the last 30 days. Each line in the bar represents a day of last 30 days. For days having location update issues the corresponding line in the bar appears in red.

**Anomalies**

This area displays the location updates issues and internet provisioning issues (this is applicable only of you have configured customer acquisition through captive portals) currently occurring in the locations. The total number of anomalies for your Cisco DNA Spaces account will be listed.

The following details for each anomaly will be displayed:

- **ID**— The ID for anomaly.
- **Description**— Describes whether it is a location update or internet provisioning issue.
- **CreatedTime**— The time at which the anomaly is recorded.

**DNA Apps**

This area displays the status of the apps provided by Cisco DNA Spaces for last 30 days. The following details of each Cisco DNA Spaces app will be shown.

The status of the following apps will be shown:

- **Captive Portal**—Displays the status of the Captive Portal app.
- **Engagement**—Displays the status of the Engagement app.
- **Location Analytics**—Displays the status of the location updates for all your locations.
- **Location Personas**—Displays the status of the Location Personas app.
- **Cisco DNA Spaces**—Displays the status of the Cisco DNA Spaces domain. The status of the Cisco DNA Spaces domain will be active only if all the associated apps are active.

---

**Note**

Cisco DNA Spaces domain will be marked as up, only if the domain is working for all the Cisco DNA Spaces customers.

The following details will be shown for each app:

- **Description**— The name of the app.
- **Uptime %**— With in the last 30 days, the percentage of period for which the app was up. For example, if the app was active for all the last 30 days without any health issues, the Uptime % value will be 100%.
- **Status**— Displays the current status of the app.

The following health properties will be considered to decide the status of the apps:
• **Captive Portal app**— Portal Health, Rule Engine Health, Subscriber Health, Email Verifier health, SMS Health, and database health.

• Cisco DNA Spaces— Vault health, Dashboard health, DMS health, TMS health.

• **Engagement app**— Dashboard health, Subscriber health, Server health, Location Receiver health, DMS health, Email Verifier health, SMS health, and Database health.

• **Location Analytics**— Dashboard health, Subscriber health, Server health, Location Receiver health, and Database health.

• **Location Personas**— Dashboard Health, Subscriber Health, Server health, Location Receiver health, and Database health.

**App Latency**

This area displays the status of latencies associated with the apps for the last 30 days.

The following app latency details will be shown:

• **Description**— The name of the app. For example, Kafka server.

• **Latency**— During the last 30 days, the percentage of period for which the app latency status was up. For example, if the Kafka server has an app latency on 1 day during the last 30 days, the latency value will be 96.6%.

• **Status**— The current status of the app latency.

**Enterprise Apps**

This area displays the status of the enterprise apps for the last 30 days.

The following enterprise app details will be shown:

• **Description**— Name of the Enterprise app.

• **Uptime Percentage**— During the last 30 days, the percentage of period for which the Enterprise app was up.

• **Status**— The current status of the enterprise app.

**Partner Apps**

This area displays the status of the partner apps for the last 30 days.

The following partner app details will be shown:

• **Description**— Name of the partner app.

• **Uptime Percentage**— During the last 30 days, the percentage of period for which the partner app was up.

• **Status**— The current status of the partner app.
Managing Cisco DNA Spaces Users and Accounts

This chapter explains how to invite and manage Cisco DNA Spaces users.

- Managing Cisco DNA Spaces Users, on page 191
- Managing the Cisco DNA Spaces Accounts, on page 194

Managing Cisco DNA Spaces Users

Cisco DNA Spaces provides its users different rights and privileges based on the role they perform.

Inviting a Cisco DNA Spaces User

When a Cisco DNA Spaces account is created, a Dashboard Admin Role user is created for the account with the e-mail ID provided. This Dashboard Admin can invite other users for Cisco DNA Spaces.

Cisco DNA Spaces provides only one default user role, Dashboard Admin Role. By default, Dashboard Admin Role will have read and write access rights only to the role types, DNASpaces (including menu items in the left pane, of the dashboard, and the apps Behavior Metrics, OpenRoaming, Location Analytics, Engagements, and Location Personas), CaptivePortals, and OperationsInsights.

- If the Dashboard Admin Role requires access to any other role types (apps) such as BLEManager, you must contact the Cisco DNA Spaces support team.

- By default, a Dashboard Admin Role for the SEE (Base) license will have access only to DNASpaces.

Cisco DNA Spaces allows you to define user roles with different access rights to different apps. For example, you can create a user role with read and write permissions in Captive Portals app, and read only permission in Operational Insights app.

You can include the following role types (apps) in a user role, if that particular service is enabled for your account.

- DNASpaces: This role type provides access to all the menu items in the left pane of the Cisco DNA Spaces dashboard such as Location Hierarchy, Admin Management, Monitoring and Support, Setup,
and so on. In addition, this role type provides access to the apps such as Behavior Metrics, OpenRoaming, Location Analytics, Engagements, and Location Personas.

- **CaptivePortal**: This role type provides access rights to the Captive Portals app.
- **OperationalInsights**: This role type provides access rights to the Operational Insights app.
- **BeconManager**: This role type provides access rights to the BLE Manager app.
- **MobileSDK**: This role type provides access rights to the Location SDK app.
- **Location**: This role type provides access rights to the Detect and Locate app.

To invite a Cisco DNA Spaces user, perform the following steps:

**Step 1**
In the Cisco DNA Spaces dashboard, choose **Admin Management**.

**Step 2**
Click **Invite Admin**.

**Step 3**
In the **Invite Admin** window, enter the following details:

a) In the **Email** field, enter the e-mail address of the user to add.

b) From the **Role Name** drop-down list, choose the user role that you want to provide to this user.

    The default user role, and the user roles defined earlier appears in the drop-down list for selection. If the required user role is not there, you can define a user role using **Create New Role**. For more information on creating a new user role, see the **Creating a User Role** section. The user roles defined all get listed on the **Roles** tab.

c) Click **Invite**.

**Note**
- The **Invite Admin** button is available only for Cisco DNA Spaces Admins with Read and Write permissions.
- Certain apps such as Captive Portals have provision to manage the users for that particular app. For example, a Captive Portals app user with read/write permission can invite users with user roles **Creative User** or **AccessCodeManger** from the **User Management** option in the Captive Portals app. Admin Management users will be displayed in the User Management window. However, from the **User Management** option in the Captive Portals app, you cannot modify an user account created through **Admin Management**.

---

**Creating a User Role**

To create a Cisco DNA Spaces user role, perform the following steps:

**Step 1**
In the Cisco DNA Spaces dashboard, click **Admin Management**.

**Step 2**
Click the **Roles** tab, and click **Create Role**.

**Note**
You can also click **Create New Role** in the **Role Name** drop-down list in the **Invite Admin** window.

**Step 3**
In the **Create New Role** window, enter the following details:

a) In the **ROLE NAME** field, enter a name for the user role.
Managing Cisco DNA Spaces Users and Accounts

Editing Cisco DNA Spaces User

A Dashboard Admin user with read and write permission can change the user role of a user. For example, a Dashboard Admin Read can be promoted to a Dashboard Admin Read and Write user.

To edit the user privileges of a Cisco DNA Spaces user, perform the following steps:

Step 1 In the Cisco DNA Spaces dashboard, choose Admin Management. The Admin page appears with the list of e-mail IDs of the Cisco DNA Spaces users.

Step 2 Click the Edit icon at the far right of the e-mail ID of the user whom you want to edit. The Invite Admin window appears.

Step 3 From the Role Name drop-down list, choose the type of access that you want to provide to the user. The default user roles, and the user roles defined earlier appears in the drop-down list for selection. If the required user role is not there, you can define a user role using Create New Role. For more information on creating a new user role, see the "Creating a User Role" section.

Step 4 Click Update.

Deleting a Cisco DNA Spaces User

If a user no more needs access to the Cisco DNA Spaces, we recommend that such users to be deleted from the Cisco DNA Spaces user list. A Dashboard Admin Role user can delete other users.

To delete an existing Cisco DNA Spaces user, perform the following steps:

Step 1 In the Cisco DNA Spaces dashboard, choose Admin Management. The Admins page appears with the list of the Cisco DNA Spaces users.
Step 2  Click the **Delete** icon at the far right of the e-mail ID of the user whom you want to delete.

If you want to delete multiple users, select the check box for the corresponding e-mail IDs, and click **Delete Admins** that appears on top right of the window.

---

**God Admin**

Cisco DNA Spaces provides a **God Admin** user role to access the God Admin dashboard, which is available only for Cisco Internal users. Currently, the number of God Admin accounts possible at a time is restricted. The Team option does not support to create God Admin user roles. It is created internally by Cisco DNA Spaces team. The God Admin dashboard provides a report that is generated based on the data for all the Cisco DNA Spaces customers, and helps Cisco to analyze the overall performance of Cisco DNA Spaces.

The data displayed in the God Admin dashboard includes:

- Total No of Locations
- Total Number of APs
- Total number of location updates.
- Total sq.ft area covered by Cisco DNA Spaces.
- Total number of Visits and Visitors.
- Visitors by location in Map View and List View.
- Top 5 Locations.
- Visit Duration for various visit ranges.
- Visit Counts for various Visit ranges.
- Graph for Hourly Visits.
- Count of Mobile Numbers, Email IDs, Names captured along with the number of visitors for which gender is captured.
- Count of Opt In users.

---

**Managing the Cisco DNA Spaces Accounts**

This section describes how to manage the Cisco DNA Spaces Accounts.

**Changing the Cisco DNA Spaces Password**

We recommend you to change the Cisco DNA Spaces password at frequent intervals to ensure more security for your application.

To change the password of your Cisco DNA Spaces account, perform the following steps:
Step 1  In the Cisco DNA Spaces dashboard, click the User Account icon that appears at the far-right of the dashboard.

Step 2  Click Change Password.

Step 3  In the window that appears, do the following:
   a)  In the Current Password field, enter the current password for your Cisco DNA Spaces account.
   b)  In the New Password field, enter the new password that you want for your Cisco DNA Spaces account.
   c)  In the Confirm Password field, reenter the new password for confirmation.
   d)  Click Change Password.

Password Strength

   The Cisco DNA Spaces password requires the following parameters:
      • Atleast 8 characters.
      • Atleast 1 upper case letter (A-Z)
      • Atleast 1 lower case letter (a-z)
      • Atleast 1 special character
      • Atleast 1 numeric character(0-9)

Signing Out of Cisco DNA Spaces

   To sign out of Cisco DNA Spaces, perform the following steps:

   Step 1  In the Cisco DNA Spaces dashboard, click the User Account icon that appears in the far right of the dashboard.
   Step 2  Click Logout.
CHAPTER 14

Configuring Cisco Wireless Controllers and Cisco Catalyst 9800 Series Controllers for Cisco DNA Spaces

This chapter describes the configurations to be done in the Cisco Wireless Controller (Cisco AireOS) or Cisco Catalyst 9800 Series Controllers to work with Cisco DNA Spaces. The configurations required differ based on the wireless controller type and connector you use.

- You cannot connect a Cisco Wireless Controller with hyper location with Cisco DNA Spaces and Cisco CMX simultaneously.

- If you want to connect a Cisco Wireless Controller with both Cisco CMX and Cisco DNA Spaces simultaneously, you must use a Cisco DNA Spaces Connector. Check the limitations for the number of NMSP connections your Cisco Wireless Controller can support, and ensure that your Cisco Wireless Controller can support the addition of a new connection to Cisco DNA Spaces Connector, especially if there are existing connections to multiple Cisco CMX servers.

- You cannot use a Cisco Wireless Controller simultaneously with Cisco WLC Direct Connect and Cisco DNA Spaces Connector. Disable the Cisco WLC Direct Connect before using the Cisco DNA Spaces Connector.

- It is recommended to use Cisco DNA Spaces Connector rather than Cisco WLC Direct Connect, especially when you are using a lower version of Cisco Wireless Controller. Also, certain apps such as Operation Insights, Detect and Locate, and so on are supported only by Cisco DNA Spaces Connector.

- It is not recommended to compare the data displayed in your wireless network with the data shown in Cisco DNA Spaces reports as it is expected to defer as per the design.

The configurations are done in the external applications that are not a part of Cisco DNA Spaces, and the menu path and names specified for the tabs, windows, options, and so on in this documentation are subject to change.

The features supported by various connector types, and the configurations for various combinations of wireless controllers and connectors are as follows:
### Features Supported by Various Connectors

The following table lists the features supported by each type of connector. You can opt the connector based on the feature or app that you want to use. Cisco DNA Spaces Connector is recommended if you want to use the apps such as Operational Insights and Open Roaming.

**Table 12: Connectors-Feature Support**

<table>
<thead>
<tr>
<th>Features/Apps</th>
<th>Cisco DNA Spaces Connector</th>
<th>Cisco WLC Direct Connect (Recommended only for small scale deployments)</th>
<th>Defining the Location Hierarchy for Cisco AireOS/ Cisco Catalyst Wireless Controller with Cisco CMX</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco DNA Spaces dashboard</td>
<td>Cisco DNA Spaces Dashboard</td>
<td>Cisco DNA Spaces Dashboard</td>
<td>Cisco DNA Spaces Dashboard</td>
</tr>
<tr>
<td>Captive Portals</td>
<td>Working with the Captive Portal App</td>
<td>Working with the Captive Portal App</td>
<td>Working with the Captive Portal App</td>
</tr>
<tr>
<td>Engagements</td>
<td>Sending Notifications with the Engagements App</td>
<td>Sending Notifications with the Engagements App</td>
<td>Sending Notifications with the Engagements App</td>
</tr>
<tr>
<td>Location Personas</td>
<td>Creating Tags with the Location Personas App</td>
<td>Creating Tags with the Location Personas App</td>
<td>Creating Tags with the Location Personas App</td>
</tr>
<tr>
<td>Location Analytics</td>
<td>Location Analytics Report</td>
<td>Location Analytics Report</td>
<td>Location Analytics Report</td>
</tr>
<tr>
<td>Impact Analysis</td>
<td>Impact Analysis</td>
<td>Impact Analysis</td>
<td>Impact Analysis</td>
</tr>
<tr>
<td>Behaviour Metrics</td>
<td>Behavior Metrics</td>
<td>Behavior Metrics</td>
<td>Behavior Metrics</td>
</tr>
<tr>
<td>Operational Insights</td>
<td>Supported</td>
<td>Not Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Open Roaming</td>
<td>Supported</td>
<td>Not Supported</td>
<td>Not Supported</td>
</tr>
<tr>
<td>IoT Services</td>
<td>Supported</td>
<td>Not Supported</td>
<td>Not Supported</td>
</tr>
</tbody>
</table>
### Defining the Location Hierarchy for Cisco AireOS/Cisco Catalyst 9800 Series Wireless Controller with Cisco CMX

**CiscoWLCDirectConnect** *(Recommended only for small scale deployments)*

**Connecting Cisco DNA Spaces to Cisco Wireless Controller Using Cisco WLC Direct Connect**

**Connecting Cisco DNA Spaces to Cisco Catalyst 9800 Series Wireless Controller Using Cisco WLC Direct Connect**

<table>
<thead>
<tr>
<th>Features/Apps</th>
<th>Cisco DNA Spaces Connector</th>
<th>Cisco WLC Direct Connect <em>(Recommended only for small scale deployments)</em></th>
<th>Defining the Location Hierarchy for Cisco AireOS/ Cisco Catalyst 9800 Series Wireless Controller with Cisco CMX</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detect and Locate</td>
<td>Supported</td>
<td>Limited Support <em>(Associated Clients only)</em></td>
<td>Supported</td>
</tr>
<tr>
<td>Hyperlocation</td>
<td>Supported</td>
<td>Not Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Fastlocate</td>
<td>Supported</td>
<td>Not Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Scale Support</td>
<td>Best suited for scaling</td>
<td>Scale supported for AireOS Controller 8.8 MR2 and Cisco Catalyst 9800 Series 16.12.1. Up to 50 clients.</td>
<td>Supports the scale that Cisco CMX can handle.</td>
</tr>
</tbody>
</table>

**Note**

- Connecting through the Cisco Wireless Controller Direct Connection method is only recommended for small scale deployments. All large scale production deployment require a Cisco DNA Spaces Connector.
- As the **Open Roaming** app is in Beta, currently documentation is not available for this app. For any information related to **Open Roaming**, contact the Cisco DNA Spaces support team.

### Connecting Cisco DNA Spaces to Cisco Wireless Controller through Cisco CMX

When you want to use Cisco DNA Spaces with Cisco Wireless Controllers with a Cisco CMX installation, you must use the **CMX On Prem** option in the **Add a Wireless network** window of Location Hierarchy.

For Cisco Unified Wireless Network with Cisco CMX, the following configurations are required to work with Cisco DNA Spaces:
• The configuration for internet provisioning and RADIUS authentication is required only if you need radius-authentication. This configuration is required only if you need social authentication for your portals.

**Configuring Access Point Mode, SSIDs, ACLs, Splash URLs, and Virtual Interface in the WLC**

To create a Captive Portal rule, you must initially define the mode for access points, and create the SSIDs and ACLs in the Cisco Wireless Controller. You must also ensure that the splash URL for the SSID is configured in the Cisco Wireless Controller.

**Note**

The SSIDs and ACLs are created in the Cisco Wireless Controller and not in the Cisco CMX.

The Cisco Wireless Controller configurations for the local and flexconnect modes are different.

**Note**

The configurations are done in the Cisco Wireless Controller that is not a part of Cisco DNA Spaces, and the menu path and names specified for the tabs, windows, options, and so on in this documentation are subject to change.

**Local Mode Configurations for Using Cisco DNA Spaces**

To configure the Cisco Wireless Controller to use with Cisco DNA Spaces in the local mode, perform the following steps:

**Configure the Local Mode for an Access Point**

To configure a local mode for an access point, perform the following steps:

**Step 1**
Log in to the Cisco Wireless Controller with your Wireless Controller credentials.

**Step 2**
In the Cisco Wireless Controller main window, click the **Wireless** tab.

All of the access points are listed.

**Step 3**
Click the access point for which you want to configure the mode to local.

**Step 4**
Click the **General** tab.

**Step 5**
From the **AP Mode** drop-down list, choose **Local**, and click **Apply**.
Create SSIDs in Cisco Wireless Controller

The SSIDs are created in the Cisco Wireless Controller, not in the Cisco CMX.

To create the SSIDs in the Cisco Wireless Controller, perform the following steps:

**Step 1**
In the Cisco Wireless Controller main window, click the **WLANs** tab.

**Step 2**
To create a WLAN, choose **Create New** from the drop-down list at the right side of the window, and click **Go**.

**Step 3**
In the **New** window that appears, enter the WLAN details like Type, Profile Name, SSID, and so on.

**Step 4**
Click **Apply**.
The **Edit <SSID Name>** window appears.

**Step 5**
Add the SSID to the Cisco DNA Spaces dashboard.

**Step 6**
In the Cisco Wireless Controller main window, on the **General** tab, uncheck the **Broadcast SSID** check box.

*Note*  
The SSID Broadcasting is interrupted to avoid any customer accessing the SSID before completing the configurations.

**Step 7**
Choose **Security > Layer 2**, and check the **MAC Filtering** check box.

**Step 8**
In the **Layer 3** tab, do the following configurations:

a) From the **Layer 3 security** drop-down list, choose **Web Policy**.

*Note*  
**Web Policy** is the Layer 3 security option that enables you to configure captive portal in the Cisco Wireless Controller.

b) Choose the **On Mac Filter Failure** radio button.

c) In the **Preauthentication ACL** area, from the **IPv4** drop-down list, choose the ACL previously defined.

d) Check the **Enable** check box for the Sleeping Client.

*Note*  
Enabling sleeping client is not mandatory. But if enabled, the customer who is in sleeping mode after authentication gets connected without authentication if is waken up within the specified time. The clients with guest access that had successful web authentication are allowed to sleep and wake up without having to go through another authentication process through the login page. You can configure the duration for which the sleeping clients are to be remembered for before re-authentication becomes necessary. The valid range is 1 hour to 720 hours (30 days), with the default being 12 hours. Ideally, this should be similar to session timeout.

e) Check the **Enable** check box for the Override Global Config.

*Note*  
Enabling **Override global config** allows you to redirect the customer to the Cisco DNA Spaces URL, which is an external URL.

f) From the **Web Auth Type** drop-down list, choose **External (Redirect to External Server)**.

*Note*  
The **Web Auth Type** must be **External** as the Cisco DNA Spaces page is hosted in the external server, and not in the controller.

g) In the **URL** field that appears, enter the Cisco DNA Spaces splash URL.
To view the splash URL for your CUWN or AireOS account, in the Cisco DNA Spaces dashboard, the **Configure Manually** link for a AireOS SSID in the **SSIDs** window. The Configure Manually link appears only after adding a Cisco AireOS SSID.

**Note** You must configure the splash page for the customer to be redirected to the Cisco DNA Spaces web page during on-boarding.

h) Click **Apply**.

**Step 9**
Click the **Advanced** tab.

**Step 10**
In the **Enable Session Timeout** field, enter the required session timeout value in seconds. For example, for session timeout of 30 minutes, enter 1800.

**Step 11**
Click **Apply**.

**Step 12**
In the **General** tab, check the **Enabled** check box for the **Status** and **Broadcast SSID** options, to enable the SSID.

**Step 13**
Execute the following command in the command prompt to disable captive bypassing. Then, restart the Cisco Wireless Controller.

```
config network web-auth captive-bypass disable
Management > HTTP-HTTPS
```

**Note** If captive bypassing is enabled, the CNA will not pop up for iOS devices.

**Step 14**
In the **HTTP-HTTPS configuration** window that appears, do the following:

a) From the **HTTP Access** drop-down list, choose **Disabled**.

b) From the **HTTPS Access** drop-down list, choose **Enabled**.

c) From the **WebAuth SecureWeb** drop-down list, choose **Disabled**.

d) Click **Apply**.

**Step 15**
Choose **Security > Web Auth > Web Login Page**, and ensure that the Redirect URL after login field is blank.

**Note** The redirect URL field must be blank so that it won’t override the Cisco DNA Spaces splash URL configured in **Layer 3**.

---

**What to do next**

**Note**
If you have made any changes to the **Management** tab, then restart your Cisco Wireless Controller for the changes to take effect.

---

**Create Access Control Lists**

To restrict the Internet access for customers, and to allow access only to Cisco DNA Spaces splash page URL when connected to the SSID, the Cisco DNA Spaces IPs (wall garden ranges) must be configured in the ACL. Now when a customer connects to the SSID, the splash page appears for the customer.

If ACL is not configured with all the required IPs, the system considers the Cisco DNA Spaces as an external URL, and results into multiple redirection for customer.

To create the access control list, perform the following steps:

**Step 1**
Log in to the Cisco Wireless Controller with your Wireless Controller credentials.
Step 2 Choose Security > Access Control Lists > Access Control Lists.

Step 3 To add an ACL, click New.

Step 4 In the New window that appears, enter the following:
   a) In the Access Control List Name field, enter a name for the new ACL.
      Note You can enter up to 32 alphanumeric characters.
   b) Choose the ACL type as IPv4.
   c) Click Apply.

Step 5 When the Access Control Lists window reappears, click the name of the new ACL.

Step 6 In the Edit window that appears, click Add New Rule.

Step 7 Configure a rule for this ACL with the required wall garden ranges.

To view the wall garden ranges, in the Cisco DNA Spaces dashboard, click the Configure Manually link for a Cisco Unified Wireless Network SSID in the SSIDs window. The wall garden ranges are listed under the caption Creating the Access Control List. The Configure Manually link appears only after adding a Cisco AireOS SSID.

When defining the ACL rule, ensure to configure the values as follows:

- **Direction**: Any
- **Protocol**: Any
- **Source Port Range**: 0-65535
- **Destination Port Range**: 0-65535
- **DSCP**: Any
- **Action**: Permit

Step 8 If you want to provide social authentication for your portal, you must also configure the wall garden ranges for social authentication.

Note The wall garden ranges configured for social authentication allows the customers to access all the HTTPS web sites directly after connecting to your SSID, without using the captive portal.

---

Configure the Virtual Interface

To configure the virtual interface, perform the following steps:

Step 1 Choose Controller > Interfaces.

Step 2 Click the Virtual link.

Step 3 In the Interfaces > Edit window that appears, enter the following parameters:
   a) In the IP address field, enter the unassigned and unused gateway IP address, if any.
   b) In the DNS Host Name field, enter the DNS Host Name, if any.
      Note Ideally this field must be blank.
To ensure connectivity and web authentication, the DNS server must always point to the virtual interface. If a DNS hostname is configured for the virtual interface, then you must configure the same DNS hostname on the DNS servers used by the client.

c) Click **Apply**.

**Note**
If you have made any changes to the virtual interface, restart your Cisco Wireless Controller for the changes to take effect.

---

**FlexConnect Mode Configurations for Using Cisco DNA Spaces**

You can configure FlexConnect for central switch or local switch mode.

**FlexConnect Central Switch Mode**

To configure the Cisco Wireless Controller to use the Cisco DNA Spaces in the FlexConnect central switch mode, perform the following steps:

Configure the **FlexConnect Mode for an Access Point**

This configuration is applicable for FlexConnect central switch and local switch mode. To configure a FlexConnect Central switch mode for an access point, perform the following steps:

**Step 1**
In the Cisco Wireless Controller main window, click the **Wireless** tab. All of the access points are listed.

**Note**
For more details on the access points, see the Cisco Wireless Controller user guide.

**Step 2**
Click the access point for which you want to configure the mode to FlexConnect.

**Step 3**
Click the **General** tab.

**Step 4**
From the **AP Mode** drop-down list, choose **FlexConnect**.

**Step 5**
Click **Apply** to commit your changes and to cause the access point to reboot.

**Create SSIDs in the Cisco Wireless Controller for FlexConnect Central Switch Mode**

Create the SSID using the same steps as outlined for the local mode. For more information, see the **Create SSIDs in Cisco Wireless Controller**, on page 201.

**Create Access Control Lists for FlexConnect Central Switch Mode**

Create the Access Control List using the same steps as outlined for the local mode. For more information, see the **Create Access Control Lists**, on page 202.

**Configure the Virtual Interface**

To configure the virtual interface, perform the following steps:

**Step 1**
Choose **Controller > Interfaces**.
Step 2  Click the Virtual link.

Step 3  In the Interfaces > Edit window that appears, enter the following parameters:
   a) In the IP address field, enter the unassigned and unused gateway IP address, if any.
   b) In the DNS Host Name field, enter the DNS Host Name, if any.

   Note  Ideally this field must be blank.

   Note  To ensure connectivity and web authentication, the DNS server must always point to the virtual interface. If a DNS hostname is configured for the virtual interface, then you must configure the same DNS host name on the DNS servers used by the client.

   c) Click Apply.

   Note  If you have made any changes to the virtual interface, restart your Cisco Wireless Controller for the changes to take effect.

---

FlexConnect Local Switch Mode

To configure the Cisco Wireless Controller to use the Cisco DNA Spaces in the FlexConnect local switch mode, perform the following steps:

- Configure the FlexConnect Mode for an Access Point, on page 204

Configure the FlexConnect Mode for an Access Point

This configuration is applicable for FlexConnect central switch and local switch mode. To configure a FlexConnect Central switch mode for an access point, perform the following steps:

Step 1  In the Cisco Wireless Controller main window, click the Wireless tab.

   All of the access points are listed.

   Note  For more details on the access points, see the Cisco Wireless Controller user guide.

Step 2  Click the access point for which you want to configure the mode to FlexConnect.

Step 3  Click the General tab.

Step 4  From the AP Mode drop-down list, choose FlexConnect.

Step 5  Click Apply to commit your changes and to cause the access point to reboot.

---

Create SSIDs in the Cisco Wireless Controller for the FlexConnect Local Switch Mode

- The SSIDs are created in the Cisco Wireless Controller, not in the Cisco CMX.

To create the SSIDs in the CUWN for the FlexConnect local switch mode, perform the following steps:

Step 1  In the Cisco Wireless Controller main window, click the WLANs tab.
Step 2  
To create a WLAN, choose **Create New** from the drop-down list at the right side of the window, and click **Go**.

Step 3  
In the **New** window that appears, enter the WLAN details such as, Type, Profile Name, SSID, and so on.

Step 4  
Click **Apply**.  
The **Edit <SSID Name>** window appears.

Step 5  
Add the SSID to the Cisco DNA Spaces dashboard.

Step 6  
In the Cisco Wireless Controller main window, on the **General** tab, uncheck the **Broadcast SSID** check box.  
**Note**   
The SSID Broadcasting is interrupted to avoid any customer accessing the SSID before completing the configurations.

Step 7  
Choose **Security > Layer 2**, and check the **MAC Filtering** check box.

Step 8  
In the **Layer 3** tab, do the following configurations:

a)  
From the Layer 3 security drop-down list, choose **Web Policy**.  
**Note**  
**Web Policy** is the **Layer 3** security option that enables you to configure captive portal in the Cisco Wireless Controller.

b)  
Choose the **On Mac Filter Failure** radio button.

c)  
In the **Preauthentication ACL** area, from the **WebAuth FlexACL** drop-down list, choose the ACL previously defined.

d)  
Check the **Enable** check box for Sleeping Client.  
**Note**  
Enabling sleeping client is not mandatory. But if enabled, the customer who is in sleeping mode after authentication gets connected without authentication if is waken up within the specified time. The clients with guest access that had successful web authentication are allowed to sleep and wake up without having to go through another authentication process through the login window. You can configure the duration for which the sleeping clients are to be remembered for before re-authentication becomes necessary. The valid range is 1 hour to 720 hours (30 days), with the default being 12 hours. Ideally, this should be similar to session timeout.

e)  
Check the **Enable** check box for Override Global Config.  
**Note**  
Enabling **Override Global Config** enables you to redirect the customer to the Cisco DNA Spaces URL, which is an external URL.

f)  
From the **Web Auth Type** drop-down list, choose **External**.  
**Note**  
The **Web Auth Type** must be **External** as the Cisco DNA Spaces page is hosted in the external server, and not in the controller.

g)  
In the URL field that appears, enter the Cisco DNA Spaces Splash URL.  
To view the splash URL for your CUWN account, in the Cisco DNA Spaces dashboard, click the **Configure Manually** link for a CUWN SSID in the **SSIDs** window. The **Configure Manually** link appears only after adding a Cisco AireOS SSID.  
**Note**  
You must configure the splash page for the customer to be redirected to the Cisco DNA Spaces web page during on-boarding.

h)  
Click **Apply**.

Step 9  
Click the **Advanced** tab.

Step 10  
In the **Enable Session Timeout** field, enter the required session timeout value in seconds. For example, for session timeout of 30 minutes, enter 1800.
Step 11 In the **FlexConnect** area, check the **Enabled** check box for FlexConnect Local Switching, and click **Apply**.

Step 12 In the **General** tab, select the **Enabled** check box for the Status and Broadcast SSID options, to enable the SSID.

Step 13 Execute the following command in the command prompt to disable captive bypassing. Then, restart the Cisco Wireless Controller.

    config network web-auth captive-bypass disable

**Note** If captive bypassing is enabled, the CNA will not pop up for iOS devices.

Step 14 Choose **Management > HTTP-HTTPS**.

Step 15 In the **HTTP-HTTPS Configuration** window that appears, perform the following:

   a) From the **HTTP Access** drop-down list, choose **Disabled**.
   b) From the **HTTPS Access** drop-down list, choose **Enabled**.
   c) From the **WebAuth SecureWeb** drop-down list, choose **Disabled**.
   d) Click **Apply**.

Step 16 Choose **Security > Web Auth > Web Login Page**, and ensure that the **Redirect URL after login** field is blank.

**Note** The redirect URL field must be blank so that it will not override the Cisco DNA Spaces splash URL configured in Layer 3.

---

**Create Access Control Lists for FlexConnect Local Switch Mode**

To restrict the Internet access for customers, and to allow access only to Cisco DNA Spaces splash page URL when connected to the SSID, the Cisco DNA Spaces IPs (wall garden ranges) must be configured in the ACL. Now when a customer connects to the SSID, the splash page appears for the customer.

If ACL is not configured with all the required IPs, the system considers the Cisco DNA Spaces as an external URL, and results into multiple redirection for customer.

To create the access control list for the FlexConnect local switch mode, perform the following steps:

---

**Step 1** Log in to the Cisco Wireless Controller with your Wireless Controller credentials.

**Step 2** Choose **Security > Access Control Lists > FlexConnect ACLs**.

**Step 3** To add an ACL, click **New**.

**Step 4** In the **New** window that appears, enter the following:

   a) In the **Access Control List Name** field, enter a name for the new ACL.
      
      **Note** You can enter up to 32 alphanumeric characters.

   b) Click **Apply**.

**Step 5** When the **Access Control Lists** window reappears, click the name of the new ACL.

**Step 6** In the **Edit** window that appears, click **Add New Rule**.

The **Rules > New** window appears.

**Step 7** Configure a rule for this ACL with the required wall garden ranges.

To view the wall garden ranges, in the Cisco DNA Spaces dashboard, click the **Configure Manually** link for a CUWN SSID in the **SSIDs** window."
When defining the ACL rule, ensure to configure the values as follows:

- **Direction**: Any
- **Protocol**: Any
- **Source Port Range**: 0-65535
- **Destination Port Range**: 0-65535
- **DSCP**: Any
- **Action**: Permit

**Step 8**

If you want to provide social authentication for your portal, you must also configure the wall garden ranges for social authentication. To know the wall garden ranges that you must configure for social authentication, see the Configuring the Wireless Network for Social Authentication section.

**Note**

The wall garden ranges configured for social authentication allows the customers to access all the HTTPS web sites directly after connecting to your SSID, without using the captive portal.

---

**Configure the Virtual Interface**

To configure the virtual interface, perform the following steps:

**Step 1**

Choose **Controller > Interfaces**.

**Step 2**

Click the **Virtual** link.

**Step 3**

In the **Interfaces > Edit** window that appears, enter the following parameters:

- a) In the **IP address** field, enter the unassigned and unused gateway IP address, if any.
- b) In the **DNS Host Name** field, enter the DNS Host Name, if any.

**Note**

Ideally this field must be blank.

**Note**

To ensure connectivity and web authentication, the DNS server must always point to the virtual interface. If a DNS hostname is configured for the virtual interface, then you must configure the same DNS host name on the DNS servers used by the client.

- c) Click **Apply**.

**Note**

If you have made any changes to the virtual interface, restart your Cisco Wireless Controller for the changes to take effect.

---

**Configuring Cisco Wireless Controller for Internet Provisioning and RADIUS Authentication**

We highly recommend to use RADIUS authentication for captive portals. The following features work only if you configure RADIUS authentication.

- Seamless Internet Provisioning.
- Extended session duration and Internet bandwidth.
- Deny Internet.

Also, for Customer onboarding by captive portal, internet provisioning configuration is required.

To configure radius authentication and seamless internet provisioning, perform the following steps:

**Step 1**
Log in to Cisco Wireless Controller with your Cisco Wireless Controller credentials.

**Step 2**
In the Cisco Wireless Controller main window, click the Security tab.

**Step 3**
Choose Radius > Authentication.

The Radius Authentication Servers window appears.

**Step 4**
From the Auth Called Station ID Type drop-down list, choose AP MAC Address:SSID.

**Step 5**
From the MAC Delimiter drop-down list, choose Hyphen.

**Step 6**
Click New.

**Step 7**
In the New window that appears, enter the details of the radius server for authentication, such as server IP address, port number, and secret key, select the Server Status as Enabled, and click Apply.

Port Number: 1812

**Note**
You can configure only the Cisco DNA Spaces radius servers. To view the radius server IP address and secret key, in the Cisco DNA Spaces dashboard, click the Configure Manually link for a CUWN SSID in the SSIDs window. The Configure Manually link appears only after adding a Cisco AireOS SSID. Configure both the primary and secondary radius server IPs. You can also contact the Cisco DNA Spaces support team.

**Step 8**
Choose Radius > Accounting.

The Radius Accounting Servers window appears.

**Step 9**
From Acct Called Station ID Type, choose AP MAC Address:SSID.

**Step 10**
From the MAC Delimiter drop-down list, choose Hyphen.

**Step 11**
Click New.

**Step 12**
In the New window that appears, enter the details of the radius server for accounting, such as server IP address, port number, and secret key, select the Server Status as Enabled, and click Apply.

Port Number: 1813

**Note**
You can configure only the Cisco DNA Spaces radius servers. You can configure only the Cisco DNA Spaces radius servers. To view the radius server IP address and secret key, in the Cisco DNA Spaces dashboard, click the “Configure Manually” link for a CUWN SSID in the SSIDs window.

**Step 13**
In the Cisco Wireless Controller main window, click the WLANs tab.

**Step 14**
Click the WLAN of the SSID for the Captive Portal rule.

**Step 15**
Choose Security.

**Step 16**
In the Layer 2 tab, select the MAC Filtering check box.

**Step 17**
In the Layer 3 tab, ensure that the following is configured.

In the Layer 3 security drop-down list, Web Policy is selected, and the On Mac Filter Failure radio button is selected.

**Note**
These configurations in the Layer 3 are done when creating the SSIDs.

**Step 18**
In the AAA Servers tab, in the Radius Servers area, do the following:
Configuring Cisco Wireless Controller for Social Authentication

For social authentication with Cisco Unified Wireless Network, you must do some configurations in the Cisco Wireless Controller.

To configure the Cisco Unified Wireless Network for social authentication, perform the following steps:

Step 1
Log in to Cisco Wireless Controller using your credentials.

Step 2
Choose Security > Access Control Lists > Access Control Lists.

Step 3
In the Access Control List window that appears, click the Access Control List configured for Cisco DNA Spaces.

Click Add New Rule and add additional two rules with following information.

<table>
<thead>
<tr>
<th>No</th>
<th>Action</th>
<th>Source IP Address/Netmask</th>
<th>Destination IP Address/Netmask</th>
<th>Protocol</th>
<th>Source Port Range</th>
<th>Destination Port Range</th>
<th>DSCP</th>
<th>Direction</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Permit</td>
<td>0.0.0.0/0.0.0.0</td>
<td>0.0.0.0/0.0.0.0</td>
<td>TCP</td>
<td>HTTPS</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
</tr>
<tr>
<td>2</td>
<td>Permit</td>
<td>0.0.0.0.0/0.0.0.0</td>
<td>0.0.0.0.0/0.0.0.0</td>
<td>TCP</td>
<td>Any</td>
<td>HTTPS</td>
<td>Any</td>
<td>Any</td>
</tr>
</tbody>
</table>

Note
This wall garden ranges configured for social authentication will allow the customers to access all the HTTPS web sites directly after connecting to your SSID, without using the captive portal.

Step 4
Add social platform specific domains as ACLs based on the social networks that you want to use for authentication. To add social domains as ACLs, perform the following steps:

a) In the Cisco Wireless Controller dashboard, choose Security > Access Control Lists.

b) Click More Actions for the Access Control List configured for Cisco DNA Spaces.

c) Click Add Remove URL.
d) Enter a social URL name, and click **Add**.

e) Repeat steps c and d for each domain.

**Note** These domain names are managed by the social networks and can change at any time. Also, these domain names are subjected to change based on country/region. If you are facing any issue, contact the Cisco DNA Spaces support team.

The commonly used domain names for various social platforms are as follows:

**Table 13:**

<table>
<thead>
<tr>
<th>Social Domains</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Facebook</strong></td>
</tr>
<tr>
<td>facebook.com</td>
</tr>
<tr>
<td>static.xx.fbcdn.net</td>
</tr>
<tr>
<td><a href="http://www.gstatic.com">www.gstatic.com</a></td>
</tr>
<tr>
<td>m.facebook.com</td>
</tr>
<tr>
<td>fbcdn.net</td>
</tr>
<tr>
<td>fbsbx.com</td>
</tr>
<tr>
<td><strong>LinkedIn</strong></td>
</tr>
<tr>
<td><a href="http://www.linkedin.com">www.linkedin.com</a></td>
</tr>
<tr>
<td>static-exp1.licdn.com</td>
</tr>
<tr>
<td><strong>Twitter</strong></td>
</tr>
<tr>
<td>abs.twimg.com</td>
</tr>
<tr>
<td>syndication.twitter.com</td>
</tr>
<tr>
<td>twitter.com</td>
</tr>
<tr>
<td>analytics.twitter.com</td>
</tr>
<tr>
<td><strong>Instagram</strong></td>
</tr>
<tr>
<td>instagram.com</td>
</tr>
<tr>
<td>*.instagram.com</td>
</tr>
<tr>
<td>api.instagram.com</td>
</tr>
<tr>
<td>d36xtkk24g8jdx.cloudfront.net</td>
</tr>
<tr>
<td><a href="http://www.facebook.com">www.facebook.com</a></td>
</tr>
<tr>
<td>connect.facebook.net</td>
</tr>
</tbody>
</table>
To import the locations from Cisco 9800 Series Wireless Controller or Cisco Wireless Controller (without CMX) to Cisco DNA Spaces, you must first connect the Controller to Cisco DNA Spaces through one of the connectors.

The connectors, **Cisco WLC Direct Connect** and **Cisco DNA Spaces Connector** can be used for both Cisco Wireless Controller and Cisco Catalyst 9800 Series Wireless Controller.

**Note**

- If you want to connect a Cisco Wireless Controller with both Cisco CMX and Cisco DNA Spaces simultaneously, you must use a Cisco DNA Spaces Connector. However, it is not recommended to connect a single Controller to both Cisco DNA Spaces and Cisco CMX simultaneously.

- It is recommended not to compare the data displayed in Cisco DNA Spaces reports such as Behavior Metrics with the data displayed in Cisco Wireless Controller or Cisco CMX, as it is expected to differ as per design.

- For importing a Controller to Cisco DNA Spaces, ensure that atleast one AP is connected to that particular Controller.

- In the Controller, if new APs are added to the Controller, those APs get automatically imported during the next Controller synchronization. If an imported AP is deleted from the Controller, the changes will be reflected in Cisco DNA Spaces only after 48 hours. However, an AP without updates will be deleted after 48 hours only if updates are coming from other APs. For example, if there are 10 APs that are configured, and if 2 APs are removed from Controller, these 2 APs will be removed from Cisco DNA Spaces only when updates are received from other 8 APs.

- If an AP is disassociated from the Controller, it is not immediately removed from Cisco DNA Spaces to release the AP count. The APs will be removed from Cisco DNA Spaces only after 48 hours.

The configurations required for various combinations of Wireless Controllers and Connectors are as follows:
Connecting Cisco DNA Spaces to Cisco Wireless Controller Using Cisco WLC Direct Connect

To connect the Cisco Wireless Controller Version 8.3 or later (without Cisco CMX installation) to the Cisco DNA Spaces, and to import the Cisco Wireless Controller and its access points to the Cisco DNA Spaces, perform the following steps:

Before you begin

- You need Cisco Wireless Controller Version 8.3 or later
- For importing a Cisco Wireless Controller to Cisco DNA Spaces, ensure that at least one AP is connected to that particular Cisco Wireless Controller.
- The Cisco Wireless Controller must be able to reach Cisco DNA Spaces cloud over HTTPS.
- Cisco Wireless Controller must be able to reach out to the internet.
- To use Cisco DNA Spaces with anchor mode, you must have a network deployment with Cisco Wireless Controllers in both anchor controller mode and foreign controller mode. If the network deployment contains Cisco Wireless Controller in Anchor Controller mode and Foreign Controller mode, Cisco WLC Direct Connect must be enabled in both controllers using the commands described in this section. In addition, the Cisco Wireless Controllers in both modes must be able to reach the Cisco DNA Spaces cloud over HTTPS. However, Cisco DNA Spaces does not support Cisco Wireless Controller Version 8.3.102 in anchor mode.
- To connect the Cisco AireOS Wireless Controller Version 8.3 or later successfully to the Cisco DNA Spaces using Cisco WLC Direct Connect, you must have a root certificate issued by DigiCert CA. If the network deployment contains Cisco Wireless Controller in Anchor Controller mode and Foreign Controller mode, you must import the certificate to the Cisco Wireless Controllers in both modes.

Step 1

Import the DigiCert CA root certificate.

a) Download your root certificate from the following link:


b) Copy the root certificate content to a file with .cer extension, and save the file as {your_filename}.cer.

c) Copy the {your_filename}.cer file to the default directory on your TFTP.

d) Log in to the Cisco Wireless Controller CLI, and execute the following commands:

   transfer download datatype cmx-serv-ca-cert
   transfer download mode tftp
   transfer download filename {your_filename}.cer
   transfer download serverip {your_tftp_server_ip}
   transfer download start

   e) Type Y to start the upload

f) After the new root certificate has been uploaded successfully, execute the following commands to disable, and then enable your Cisco CMX Cloud Services:

   config cloud-services cmx disable
   config cloud-services cmx enable
After uploading the root certificate, Cisco Wireless Controller will prompt for reboot. Rebooting is recommended, but not mandatory. The certificate will be installed in either case.

If you try to connect the Wireless Controller to Cisco DNA Spaces using a root certificate not issued by DigiCert CA, you will get the following error:

https:SSL certificate problem: unable to get local issuer certificate

**Step 2**

In the Cisco Wireless Controller CLI mode, execute the following commands:

```plaintext
config cloud-services cmx disable
config cloud-services server url https://{Customer Path Key}.{LB Domain} {LB IP Address}
config cloud-services server id-token <Customer JWT Token>
config network dns serverip <dns server ip>
config cloud-services cmx enable
```

**Note**

To view the {Customer Path Key}, {LB Domain}, {LB IP Address}, and {Customer JWT Token}, log in to Cisco DNA Spaces dashboard, and click the three-line menu icon that is displayed at the top-left of the dashboard. Choose **Setup > Wireless Networks**. Then expand **Connect WLC / Catalyst 9800 Directly**, and click **View Token**. Click the WLC tab, and you can view the {Customer Path Key}, {LB Domain}, and {LB IP Address} at Step 1b and {Customer JWT Token} at Step 1c.

**Step 3**

Check the summary using the following command:

```plaintext
show cloud-services cmx summary
```

The result appears.

Now in the Cisco DNA Spaces dashboard, when you choose **CUWN-WLC** in the **Add a Wireless Network** window, the WLC will be listed. So, you can import the APs of that WLC to the Cisco DNA Spaces.

**Example:**

**Sample Result**

(Cisco Controller) >show cloud-services cmx summary

CMX Service
Server ............................... https://$customerpathkey.dnaspaces.io
IP Address ............................ <Local System IP Address>
Connectivity .......................... https: UP
Service Status .......................... Active
Last Request Status .................... HTTP/1.1 200 OK
Heartbeat Status ........................ OK

Now the Cisco Wireless Controller will be available for import in the Cisco DNA Spaces location hierarchy. You can import the locations using Map services or Access Point Prefix.

- To import the locations based on Access Point prefix, see **Importing the Locations using Access Point Prefix**, on page 26
- To import the locations using Map Services, see **Importing Locations to the Location Hierarchy Using Map Services**, on page 27
What to do next

For social authentication, radius authentication, and internet provisioning, refer to the following sections:

- Configuring Cisco Wireless Controller for Internet Provisioning and RADIUS Authentication
- Configuring Cisco Wireless Controller for Internet Provisioning and RADIUS Authentication

Configuring Cisco Wireless Controller (without Cisco CMX) for Notification and Reports

Without Cisco CMX, you can connect Cisco Wireless Controller to Cisco DNA Spaces using the connectors **WLC Direct Connect** and **Cisco DNA Spaces Connector**. In these cases, the configurations required for notifications and reports will be done automatically when you import the Cisco Wireless Controller.

**Note**

If you are using Cisco DNA Spaces with **WLC Direct Connect** or **Cisco DNA Spaces Connector**, the Controller must be in “Foreign controller” mode.

Connecting Cisco DNA Spaces to Cisco Catalyst 9800 Series Wireless Controller Using Cisco WLC Direct Connect

**Before you begin**

- For importing a Cisco Catalyst 9800 Series Wireless Controller to Cisco DNA Spaces, ensure that at least one AP is connected to that particular Cisco Catalyst 9800 Series Wireless Controller.
- Cisco Catalyst 9800 Series Wireless Controller must be able to reach Cisco DNA Spaces cloud over HTTPS.
- Cisco Catalyst 9800 Series Wireless Controller must be able to reach out to the internet.
- To connect the Cisco Catalyst 9800 Series Wireless Controller successfully to the Cisco DNA Spaces using Cisco WLC Direct Connect, you must have a root certificate trusted by Cisco.

To connect the Cisco Catalyst 9800 Series Controller to Cisco DNA Spaces, and to import that controller and its access points to the Cisco DNA Spaces, perform the following steps:

**Step 1**

Import the Cisco External Trusted Root Store to install the DigiCert Global Root CA on the Controller.

a) Download the root certificate using the following command:

```
(config)#crypto pki trustpool import url http://www.cisco.com/security/pki/trs/ios.p7b
```

b) verify the certificate installation using the following command:

```
#show crypto pki trustpool | section DigiCert Global Root CA
cn=DigiCert Global Root CA
cn=DigiCert Global Root CA
```

**Note**

You must check the output to verify correct trustpool installation.
Step 2  On Cisco Catalyst 9800 Series Controller, enable DNS to resolve the Cisco DNA Spaces URL using the following commands:

a. `(config)#ip name-server <Primary IP> <Secondary IP>`
b. `(config)#ip domain lookup`  
c. `(config)#ip route 0.0.0.0 0.0.0.0 <default_gw_ip_addr>`

Step 3  Enable `nmsp` cloud-services on Cisco Catalyst 9800 Series Controller to communicate with Cisco DNA Spaces Cloud over HTTPS.

a. `(config)#nmsp cloud-services server url <URL>`
b. `(config)#nmsp cloud-services server token <Customer JWT TOKEN>`
c. `(config)#nmsp cloud-services http-proxy <proxy ip_addr> <proxy port>`  -This command is optional, and must be used only if the proxy server needs to reach the internet.
d. `(config)#nmsp cloud-services enable`

Note  To view the server URL and token, log in to Cisco DNA Spaces dashboard, and click the three-line menu icon that is displayed at the top-left of the dashboard. Choose `Setup > Wireless Networks`. Then expand `Connect WLC / Catalyst 9800 Directly`, and click `View Token`. Click the `Cisco Catalyst 9800` tab, and you can see the URL at Step 2b and token at Step 2c.

Step 4  Confirm the connection between Cisco Catalyst 9800 Series Controller and Cisco DNA Spaces Cloud by executing the following command:

```
#show nmsp cloud-services summary
```

The result must be as follows.

**Example:**

**Sample Result**

Server : https://abc.dnaspaces.io

CMX Service : Enabled

Connectivity : https: UP

Service Status : Active

Last IP Address : <Local System IP Address>

Last Request Status : HTTP/1.1 200 OK

Heartbeat Status : OK

Now the Cisco Catalyst 9800 Series Wireless Controller will be available for import in the Cisco DNA Spaces location hierarchy.

Step 5  To view the breif summary of active/inactive Cisco CMX cloud connections, execute the following command:

```
#show nmsp status
```

**Note**  You can see the state of the connection to Cisco DNA Spaces Cloud connection.

Step 6  To view aggregated subscriptions summary for all active Cisco DNA Spaces cloud connections, execute the following command:

```
# show nmsp subscription summary
```

**Note**  You can view the services that Cisco DNA Spaces Cloud is subscribed to, after the connection is established.
Step 7  Import the locations to the Cisco DNA Spaces dashboard. For more information on importing the location, see Defining the Location Hierarchy for Cisco Catalyst 9800 Series Wireless Controllers or Cisco Wireless Controller (without Cisco CMX), on page 25.

Step 8  If you want to use the Captive Portals and Engagements apps, do the required configuration from the following:

### Configuring Cisco Catalyst 9800 Series Wireless Controller (Local Mode) for Captive Portals and Engagements Apps Using CLI

#### Note

The minimum supported Cisco Catalyst 9800 Series Wireless Controller Version is 16.10.20181030.

To configure Cisco Catalyst 9800 Series Wireless Controller for Captive Portals and Engagements app, perform the following steps:

#### Step 1

In the Cisco DNA Spaces dashboard, configure a Cisco Catalyst SSID. For more information on configuring the SSIDs, see the Importing the SSIDs for Cisco Wireless Controller or Cisco Catalyst 9800 Series Wireless Controller section.

**Note**  You can define any name for the SSID. You must use the same SSID name when configuring the Cisco Catalyst 9800 Series Wireless Controller.

#### Step 2

On Cisco Catalyst 9800 Series Wireless Controller, enable HTTP and HTTPS as follows:

- `ip http server`
- `ip http secure-server`

#### Step 3

Configure parameter maps for client redirection.

- `parameter-map type webauth <map name>`
- `type consent`
- `timeout init-state sec 600`
- `redirect for-login <splash page URL>`
- `redirect append ap-mac tag ap_mac`
- `redirect append wlan-ssid tag wlan`
- `redirect append client-mac tag client_mac`
- `redirect portal ipv4 <IP Address>`
- `logout-window-disabled`
- `success-window-disable`

**Note**  For Splash URL and IP address, in the Cisco DNA Spaces dashboard, click the Captive Portal app. Click SSIDs, and then click the Configure Manually link for the Cisco Catalyst SSID created in Step 1. The splash URL for your CUWN account will be listed in the Creating the SSIDs in CUWN-WLC section. The IP address will be listed in the Creating the Access Control List section. You must use only any one IP address from the list. You can also contact the Cisco DNA Spaces support team.

#### Step 4

Configure virtual IP address for client redirection.
parameter-map type webauth global
virtual-ip ipv4 192.0.2.0
intercept-https-enable

**Note**
- Instead of `IPv4 192.0.2.0`, you can configure any virtual IP. The virtual-ip should be a non-routable and a not used IP address.
- You must have a valid SSL certificate for the virtual IP/Domain installed in Cisco Catalyst 9800 Series Wireless Controller controller.

**Step 5** Configure FQDN URL filtering.
For central switch wlans, the URL filter list is attached to the policy-profile:

```
urlfilter list social_login_fqdn_central
action permit
url <splash page domain>
```

**Note** Configure the domain configured at Step 3 for "redirect for-login".

```
url *.fbcdn.net
url *.licdn.com
url *.licdn.net
url *.twimg.com
url *.gstatic.com
url *.twitter.com
url *.akamaihd.net
url *.facebook.com
url *.facebook.net
url *.linkedin.com
url ssl.gstatic.com
url *googleapis.com
url static.licdn.com
url *.accounts.google.com
url *.connect.facebook.net
url oauth.googleapis.com
```
wireless profile policy default-policy-profile
urlfilter list pre-auth-filter social_login_fqdn_central
For flex WLANs the URL filter list is attached to the flex-profile
urlfilter list social_login_fqdn_flex
action permit
url <splash page domain>

**Note**  Configure the domain configured at Step 3 for "redirect for-login".

url *.fbcdn.net
url *.licdn.com
url *.licdn.net
url *.twimg.com
url *.gstatic.com
url *.twitter.com
url *.akamaihd.net
url *.facebook.com
url *.facebook.net
url *.linkedin.com
url ssl.gstatic.com
url *.googleapis.com
url static.licdn.com
url *.accounts.google.com
url *.connect.facebook.net
url oauth.googleusercontent.com
urlfilter list social_login_fqdn_central
wireless profile flex default-flex-profile
acl-policy <WA-sec<<ip>>
urlfilter list social_login_fqdn_flex
description "default flex profile"

**Step 6** Configure Radius Accounting.

aaa new-model
aaa group server radius <group name>
server name <radius server name>
subscriber mac-filtering security-mode mac
mac-delimiter hyphen
aaa accounting login <authentication> group <group name>
aaa authorization network <Authorization> group <Group Name>
aaa accounting identity <Accounting> start-stop group <Group Name>
aaa server radius dynamic-author
client <Radius Server IP> server-key <Radius Secret>
aaa session-id common
radius-server attribute wireless accounting call-station-id ap-macaddress-ssid
radius server <Radius Name>
address ipv4 <Radius Server IP> auth-port 1812 acct-port 1813
key <Radius Secret>

**Note** You can configure only the Cisco DNA Spaces radius servers. To view the IPv4 IP address, secret key, and port for radius server configuration, in the Cisco DNA Spaces dashboard, click the **Captive Portal** app. Click **SSIDs**, and then click the **Configure Manually** link for the Cisco Catalyst SSID created in Step 1. The radius server details will be listed in the **Radius Server Configuration** section. Configure both the primary and secondary radius server IPs. You can also contact the Cisco DNA Spaces support team.

**Step 7** Configure Policy Profile.

wireless profile policy default-policy-profile
aaa-override
accounting-list <Accounting Server>
autoqos mode voice
description "default policy profile"
service-policy input platinum-up
service-policy output platinum
urlfilter list pre-auth-filter <url filter>
vlan <id>
no shutdown

**Step 8** Configure WLAN.

wlan <WLAN name>
ip access-group web <ACL Name>
no security wpa
no security wpa akm dot1x
no security wpa wpa2 ciphers aes
security web-auth
security web-auth authentication-list default
security web-auth parameter-map <map name>
no shutdown

**Note** Ensure that the WLAN name you mention here matches with the SSID name you configured in Cisco DNA Spaces at step 1.

**Step 9** Enable DNS resolution and make sure you have a default gateway configured on the Cisco Catalyst 9800 Series Wireless Controller.

ip name-server <dns_ip_address>
ip domain-lookup
ip route 0.0.0.0 0.0.0.0 <default_gw_ip_addr>

You can then import the SSIDs to Cisco DNA Spaces, and configure captive portals for SSIDs using the Captive Portal Rule.

Configuring Cisco Catalyst 9800 Series Wireless Controller GUI (Local Mode) for Captive Portals and Engagements Apps

Note The minimum supported Cisco Catalyst 9800 Series Wireless Controller Versions are 16.10.1E and 16.10.11.

To configure Cisco Catalyst 9800 Series Wireless Controller for Captive Portals and Engagements apps, perform the following steps:

Step 1 In the Cisco DNA Spaces dashboard, configure a Cisco Catalyst SSID. For more information on configuring the SSIDs, see the Importing the SSIDs for Cisco Wireless Controller or Cisco Catalyst 9800 Series Wireless Controller section.

Step 2 Create the Parameter Map:
   a) Log into Cisco Catalyst 9800 Series Wireless Controller.
   b) Choose Configuration > Security > Web Auth.
   c) On the Web Auth Parameter Map tab, click Add.
   d) In the Parameter-map name field, enter parameter-map name.
   e) From the Type drop-down list, choose consent, and click Apply to Device.
      The newly created Parameter Map gets listed on the Web Auth Parameter Map tab.
   f) Click the newly created Parameter Map.
   g) On the General tab, check the Disable Success Window check box, and the Disable Logout Window check box.
   h) On the Advanced tab, do the following:
      • In the Redirect for log-in field, enter the splash page URL https://<domain>/p2/<customerPathKey>.
      • In the Redirect Append for AP MAC Address field, enter ap_mac.
      • In the Redirect Append for Client MAC Address field, enter client_mac.
      • In the Redirect Append for WLAN SSID field, enter wlan.
      • In the Portal IPV4 Address field, enter the Cisco DNA Spaces IP to be allowed.

   Note To view the IP address to be allowed, in the Cisco DNA Spaces dashboard, click the Captive Portals app. Click SSIDs, and then click the Configure Manually link for the Cisco Catalyst SSID. The IP addresses will be listed in the Creating the Access Control List section. You must use only any one IP address from the list. The remaining IPs are specified when creating the ACL. The Configure Manually link appears only after adding a Cisco Catalyst SSID.
   i) Click Update and Apply.

Step 3 Install the web-auth certificate and configure the global parameter map.
You must have a valid SSL certificate for the virtual IP/Domain installed in Cisco Catalyst 9800 Series Wireless Controller. You can purchase any wild card certificate.

a) Log into Cisco Catalyst 9800 Series Wireless Controller.
b) In the Cisco Catalyst 9800 Series Wireless Controller dashboard, choose Configuration > Security > Web Auth.
c) Click the Parameter map name, global.
d) Configure Maximum Http connections as 100.
e) Configure Init-State Timeout(Secs) as 120.
f) On the General tab, from the Type drop-down list, choose Webauth.
g) Specify virtual IPv4 address (virtual IP) or virtual IPv4 Host name (domain) in the respective field.
h) Configure Watch List Expiry Timeout(Secs) as 600.
i) Check the Web Auth intercept HTTPS check box.
j) Click Update & Apply.
k) Convert the certificate into pkcs12.
   The file format will be .p12.
l) Copy the file into the tftp server.
m) Download the certificate copied to the tftp server using the following steps:
   • In the Cisco Catalyst 9800 Series Wireless Controller CLI, enter the following command:
     
     crypto pki import <name> pkcs12 tftp://<tftp server ip>:/ password <certificate password>
   
   • To confirm the tftp server IP, enter yes.
   
   • Enter the certificate file name. For example, wildcard.wifi-mx.com.p12.
     
     The certificate gets downloaded.

n) To verify the installed certificate, in the Cisco Catalyst 9800 Series Wireless Controller dashboard, choose Configuration > Web Auth > Certificate.
   
The downloaded certificate appears as the last certificate in the list.
o) To map the installed certificate with webauth parameter map, in the Cisco Catalyst 9800 Series Wireless Controller CLI, execute the following commands:
   
   • Conf t

   • parameter-map type webauth global

   • trustpoint <installed trustpool name > ex: trustpool name

   • end

   • wr (to save the configuration)

   Reload Cisco Catalyst 9800 Series Wireless Controller.

Step 4
Create the ACL by adding URL filters.
a) Choose Configuration > Security > URL Filter.
b) In the URL Filters window, click Add.
c) In the List Name field, enter the list name.
d) Change the status of Action to Permit.
e) In the URLs field, enter the splash page domain configured at Step 2h (Parameter Map).

   Add the following domains, if you want to enable social authentication:
f) Choose Configuration > Tags and Profiles > Policy.
g) In the Policy Profile window, click default-policy-profile.
h) In the Edit Policy Profile window, click the Access Policies tab.
i) In the URL Filters area, from the Pre Auth drop-down list, choose the previously created ACL.
j) Click Update & Apply to Device.

Step 5 Create the SSID.
a) Choose Configuration > Tags and Profiles > WLANs.
b) Click Add.
a) On the General tab, in the Profile Name field, enter the profile name.
b) In the SSID field, enter the SSID name defined at Step 1.
c) Set the status as Enabled.
d) Click the Security tab, and then click the Layer2 tab.
e) From the Layer 2 Security Mode drop-down list, choose None.
f) Click the Layer3 tab.
g) Check the Web Policy check box.
h) From the WebAuth Parameter Map drop-down list, choose the Web Auth Parameter Map created at step 2.
i) Click Show Advanced Settings.
j) In the Preauthentication ACL area, from the IPv4 drop-down list, choose the ACL created at step 4.
k) Click Save & Apply to Device.

Step 6 Configure the RADIUS server.
We highly recommend to use RADIUS authentication for captive portals. The following features work only if you configure RADIUS authentication.

- Seamless Internet Provisioning.
- Extended session duration.
- Deny Internet.

Note

a) Choose Configuration > Security > AAA.
b) In the Authentication Authorization and Accounting window, click the Servers/Groups tab.
c) Choose Radius > Servers, and click Add.
d) In the Name field, enter a name for the radius server.
e) In the IPv4 / IPv6 Server Address field, enter the radius server address.

Note

You can configure only the Cisco DNA Spaces radius servers. To view the radius server IP address and secret key, in the Cisco DNA Spaces dashboard, click the Captive Portal app. Click SSIDs, and then click the Configure Manually link for the Cisco Catalyst SSID created at Step 1. In the window that appears, the radius server details will be listed in the Radius Server Configuration section. Configure both the primary and secondary radius server IPs. You can also contact the Cisco DNA Spaces support team.

f) In the Key field, enter the key, and confirm it in the Confirm Key field.
g) In the Auth Port field, enter 1812.
h) In the Acct Port field, enter 1813.
i) Click Save & Apply to Device.

The server added will be available in Servers list.
j) Choose Radius > Server Groups, and click Add.
k) In the Name field, enter a name.
l) From the MAC-Delimiter drop-down list, choose hyphen.
m) From the MAC-Filtering drop-down list, choose mac.
n) Move the radius server previously created from “Available Servers” to “Assigned Servers” using the arrow button.
o) Click Save & Apply to Device.
p) In the Authentication Authorization and Accounting window, click the AAA Method List tab.
q) Click Authentication, and click Add and specify the following details:

1. In the Method List Name field, enter the method list name.
2. From the Type drop-down list, choose Login
3. From the Group Type drop-down list, choose Group.
4. Move the server group created earlier (step j to step o) from Available Server Groups to Assigned Server Groups, and click Save & Apply to Device.

r) On the AAA Method List tab, click Authorization, and click Add, and specify the following details:

1. In the Method List Name field, enter the method list name.
2. From the Type drop-down list, choose Network.
3. From the Group Type drop-down list, choose group.
4. Move the server group previously created (step j to step o) from Available Servers to Assigned Servers using the arrow button, and click Save & Apply to Device.
s) On the AAA Method List tab, click Accounting, and click Add, and specify the following details:

1. In the Method List Name field, enter the method list name.
2. From the Type drop-down list, choose Identity.
3. From the Group Type drop-down list, choose group.
4. Move the server group previously created (step j to Step o) from Available Servers to Assigned Servers using the arrow button, and click Save & Apply to Device.

Step 7

Enable L3 and L2 authentication (Mac Filtering).

Make sure Type is selected as webauth in parameter-map for RADIUS Authentication.

Note

To configure L3 and L2 authentication, ensure that you have created the SSIDs and have done all the configurations at step 5. You can then import the SSIDs to Cisco DNA Spaces, and configure captive portals for SSIDs using the Captive Portal Rule.

a) Choose Configuration > Tags and Profiles > WLANs.
b) Click the SSID for which you want to configure L2 and L3 Authentication.
c) In the Edit WLAN window, click the Security tab.
d) On the Layer3 tab, from the Authentication drop-down list, choose the radius authentication configured previously (step 6q).
e) On the Layer2 tab, to enable Mac Filtering, check the MAC Filtering check box.
f) From the Authorization List drop-down list that appears, choose the authorization server created previously (step 6r).
g) Click Show Advanced Settings.
h) Check the On Mac Filter Failure check box.
i) Click Update & Apply to Device.
j) Choose Configuration > Tags and Profiles > Policy.
k) Click default-policy-profile.
l) On the Advanced tab, in the AAA Policy area, check the Allow AAA Override check box.
m) Ensure that default aaa policy is selected from the Policy Name drop-down list.
n) Click Update & Apply to Device.

Step 8

Enable Radius Accounting.

a) Choose Configuration > Tags and Profiles > Policy.
b) Click default-policy-profile.
c) On the Advanced tab, from the Account List drop-down list, choose the accounting server created at Step 6s.
d) Click Update & Apply to Device.

Configuring Cisco Catalyst 9800 Series Wireless Controller GUI (Flex Mode or Mobility Express) for Captive Portals and Engagements Apps

Note

The minimum supported Cisco Catalyst 9800 Series Wireless Controller Versions are 16.10.1E and 16.10.11.
To configure "Cisco Catalyst 9800 Series Wireless Controller in Flex mode" or "Cisco Catalyst 9800 Series Wireless Controller with Mobility Express" for Captive Portals and Engagements apps, perform the following steps:

**Step 1**
To configure the Cisco Catalyst 9800 Series Wireless Controller in Flex mode, ensure that the following configurations are done:

This configuration is not required for Mobility Express.

a) Log into Cisco Catalyst 9800 Series Wireless Controller.
b) Choose Configuration > Tags > Site.
c) Select the required site name.
d) Uncheck the Enable Local Site check box.
e) Click Update & Apply to Device.
f) Choose Configuration > Policy.
g) Select the required policy name.
h) Disable Central Switching.
i) Click Update & Apply to Device.

*Note* AP might reboot and rejoin the wireless controller on changing from Local Mode to Flex mode.

**Step 2**
In the Cisco DNA Spaces dashboard, configure a Cisco Catalyst SSID. For more information on configuring the SSIDs, see the Importing the SSIDs for Cisco Wireless Controller or Cisco Catalyst 9800 Series Wireless Controller section.

**Step 3**
Create the Parameter Map:

a) Log into Cisco Catalyst 9800 Series Wireless Controller.
b) Choose Configuration > Security > Web Auth.
c) On the Web Auth Parameter Map tab, click Add.
d) In the Parameter-map name field, enter parameter-map name.
e) From the Type drop-down list, choose consent, and click Apply to Device.
   The newly created Parameter Map gets listed on the Web Auth Parameter Map tab.
f) Click the newly created Parameter Map.
g) On the General tab, check the Disable Success Window check box, and the Disable Logout Window check box.
h) On the Advanced tab, do the following:
   • In the Redirect for log-in field, enter the splash page URL https://<domain>/p2/<customerPathKey>.
   • In the Redirect Append for AP MAC Address field, enter ap_mac.
   • In the Redirect Append for Client MAC Address field, enter client_mac.
   • In the Redirect Append for WLAN SSID field, enter wlan.
   • In the Portal IPV4 Address field, enter the Cisco DNA Spaces IP to be allowed.

*Note* To view the IP address to be allowed, in the Cisco DNA Spaces dashboard, click the Captive Portals app. Click SSIDs, and then click the Configure Manually link for the CUWN/Catalyst SSID. The IP addresses will be listed in the Creating the Access Control List section. You must use only any one IP address from the list. The remaining IPs are specified when creating the ACL. The Configure Manually link appears only after adding a Cisco Catalyst SSID.

i) Click Update and Apply.
Step 4

Install the web-auth certificate and configure the global parameter map.

You must have a valid SSL certificate for the virtual IP/Domain installed in Cisco Catalyst 9800 Series Wireless Controller. You can purchase any wild card certificate.

a) Log into Cisco Catalyst 9800 Series Wireless Controller.
b) In the Cisco Catalyst 9800 Series Wireless Controller dashboard, choose Configuration > Security > Web Auth.
c) Click the Parameter map name, global.
d) Configure Maximum Http connections as 100.
e) Configure Init-State Timeout(Secs) as 120.
f) On the General tab, from the Type drop-down list, choose Webauth.
g) Specify virtual IPv4 address (virtual IP) or virtual IPv4 Host name (domain) in the respective field.
h) Configure Watch List Expiry Timeout(Secs) as 600.
i) Check the Web Auth intercept HTTPS check box.
j) Click Update & Apply.
k) Convert the certificate into pkcs12.
   The file format will be .p12.
l) Copy the file into the tftp server.
m) Download the certificate from the tftp server using the following steps:
   • In the Cisco Catalyst 9800 Series Wireless Controller CLI, enter the following command:
     crypto pki import <name> pkcs12 tftp://<tftp server ip>:/<password> <certificate password>
   • To confirm the tftp server IP, enter yes.
   • Enter the certificate file name. For example, wildcard.wifi-mx.com.p12.
   The certificate gets downloaded.

n) To verify the installed certificate, in the Cisco Catalyst 9800 Series Wireless Controller dashboard, choose Configuration > Web Auth > Certificate.
   The downloaded certificate appears as the last certificate in the list.
o) To map the installed certificate with webauth parameter map, in the Cisco Catalyst 9800 Series Wireless Controller CLI, execute the following commands:
   • Conf t
   • parameter-map type webauth global
   • trustpoint <installed trustpool name > ex: trustpool name
   • end
   • wr (to save the configuration)

Reload Cisco Catalyst 9800 Series Wireless Controller.

Step 5

Create the ACL by adding URL filters.

a) Choose Configuration > Security > URL Filter.
b) In the URL Filters window, click Add.
c) In the List Name field, enter the list name.
d) Change the status of Action to Permit.
e) In the URLs field, enter the splash page domain configured at Step 3h (Parameter Map).
Add the following domains, if you want to enable social authentication:

- *.fbcdn.net
- *.licdn.com
- *.licdn.net
- *.twimg.com
- *.gstatic.com
- *.twitter.com
- *.akamaihd.net
- *.facebook.com
- *.facebook.net
- *.linkedin.com
- ssl.gstatic.com
- *.googleapis.com
- static.licdn.com
- *.accounts.google.com
- *.connect.facebook.net
- oauth.googleusercontent.com

f) Choose Configuration > Tags and Profiles > Policy.
g) In the Policy Profile window, click default-policy-profile.
h) In the Edit Policy Profile window, click the Access Policies tab.
i) In the URL Filters area, from the Pre Auth drop-down list, choose the previously created ACL.
j) Click Update & Apply to Device.
k) Choose Configuration > Tags and Profiles > Flex.
l) Click the Profile in use.
m) In the Edit Flex Profile window that appears, click Policy ACL tab.
n) Click Add.
o) From the ACL Name drop-down list, choose WA-sec-<ip>.
p) From the Pre Auth URL Filter drop-down list, choose URL filter ACL created previously (Step 5a to 5e).
q) Click Save.
r) Click Update & Apply to Device.

**Step 6**

Create the SSID.

a) Choose Configuration > Tags and Profiles > WLANs.
b) Click Add.
a) On the General tab, in the Profile Name field, enter the profile name.
b) In the SSID field, enter the SSID name defined at Step 2.
c) Set the status as Enabled.
d) Click the Security tab, and then click the Layer2 tab.
e) From the Layer 2 Security Mode drop-down list, choose None.
f) Click the Layer3 tab.
g) Check the Web Policy check box.
h) From the WebAuth Parameter Map drop-down list, choose the Web Auth Parameter Map created at step 3.
i) Click Show Advanced Settings.
j) In the Preauthentication ACL area, from the IPv4 drop-down list, choose the ACL created at step 4.
k) Click Save & Apply to Device.

Step 7
Configure the RADIUS server.

Note We highly recommend to use RADIUS authentication for captive portals. The following features work only if you configure RADIUS authentication.

- Seamless Internet Provisioning.
- Extended session duration.
- Deny Internet.

a) Choose Configuration > Security > AAA.
b) In the Authentication Authorization and Accounting window, click the Servers/Groups tab.
c) Choose Radius > Servers, and click Add.
d) In the Name field, enter a name for the radius server.
e) In the IPv4 / IPv6 Server Address field, enter the radius server address.

Note You can configure only the Cisco DNA Spaces radius servers. To view the radius server IP address and secret key, in the Cisco DNA Spaces dashboard, click the Captive Portal app. Click SSIDs, and then click the Configure Manually link for the Cisco Catalyst SSID created at Step 2. In the window that appears, the radius server details will be listed in the Radius Server Configuration section. Configure both the primary and secondary radius server IPs. You can also contact the Cisco DNA Spaces support team.

f) In the Key field, enter the key, and confirm it in the Confirm Key field.
g) In the Auth Port field, enter 1812.
h) In the Acct Port field, enter 1813.
i) Click Save & Apply to Device.
   The server added will be available in Servers list.
j) Choose Radius > Server Groups, and click Add.
k) In the Name field, enter a name.
l) From the MAC-Delimiter drop-down list, choose hyphen.
m) From the MAC-Filtering drop-down list, choose mac.

m) Move the radius server previously created from “Available Servers” to “Assigned Servers” using the arrow button.
o) Click Save & Apply to Device.
p) In the Authentication Authorization and Accounting window, click the AAA Method List tab.
q) Click Authentication, and click Add and specify the following details:
   1. In the Method List Name field, enter the method list name.
   2. From the Type drop-down list, choose Login
   3. From the Group Type drop-down list, choose Group.
4. Move the server group created earlier (step j to Step o) from Available Server Groups to Assigned Servers Groups, and click Save & Apply to Device.

r) On the AAA Method List tab, click Authorization, and click Add, and specify the following details:
   1. In the Method List Name field, enter the method list name.
   2. From the Type drop-down list, choose Network.
   3. From the Group Type drop-down list, choose group.
   4. Move the server group previously created (step j to Step o) from Available Servers to Assigned Servers using the arrow button, and click Save & Apply to Device.

s) On the AAA Method List tab, click Accounting, and click Add, and specify the following details:
   1. In the Method List Name field, enter the method list name.
   2. From the Type drop-down list, choose Identity.
   3. From the Group Type drop-down list, choose group.
   4. Move the server group previously created (step j to Step o) from Available Servers to Assigned Servers using the arrow button, and click Save & Apply to Device.

Step 8
Enable L3 and L2 authentication (Mac Filtering).
Make sure Type is selected as webauth in parameter-map for RADIUS Authentication.

Note To configure L3 and L2 authentication, ensure that you have created the SSIDs and have done all the configurations at step 6. You can then import the SSIDs to Cisco DNA Spaces, and configure captive portals for SSIDs using the Captive Portal Rule.

a) Choose Configuration > Tags and Profiles > WLANs.
   b) Click the SSID for which you want to configure L2 and L3 Authentication.
   c) In the Edit WLAN window, click the Security tab.
   d) On the Layer3 tab, from the Authentication drop-down list, choose the radius authentication configured previously(step 7q).
   e) On the Layer2 tab, to enable Mac Filtering, check the MAC Filtering check box.
   f) From the Authorization List drop-down list that appears, choose the authorization server created previously(step 7r).
   g) Click Show Advanced Settings.
   h) Check the On Mac Filter Failure check box.
   i) Click Update & Apply to Device.
   j) Choose Configuration > Tags and Profiles > Policy.
   k) Click default-policy-profile.
   l) On the Advanced tab, in the AAA Policy area, check the Allow AAA Override check box.
   m) Ensure that default aaa policy is selected from the Policy Name drop-down list.
   n) Click Update & Apply to Device.

Step 9
Enable Radius Accounting.

a) Choose Configuration > Tags and Profiles > Policy.
   b) Click default-policy-profile.
   c) On the Advanced tab, from the Account List drop-down list, choose the accounting server created at Step 7s.
Connecting Cisco DNA Spaces to Cisco AireOS Wireless Controller or Cisco Catalyst 9800 Series Wireless Controller using Cisco DNA Spaces Connector

Cisco Wireless Controller with Cisco DNA Spaces Connector

To connect Cisco AireOS Wireless Controller to Cisco DNA Spaces using a Cisco DNA Spaces Connector, and to configure captive portal authentication or notifications, do the following:

- Connect Cisco AireOS Wireless Controller to Cisco DNA Spaces using a Cisco DNA Spaces Connector referring the procedure mentioned in Cisco DNA Spaces: Connector Configuration Guide.
- After connecting Cisco AireOS Controller to Cisco DNA Spaces, configure radius authentication and internet provisioning as described in Configuring Cisco Wireless Controller for Internet Provisioning and RADIUS Authentication.
- If Captive Portal Authentication is required, import SSIDs, create captive portal with the required authentication type, and configure Captive Portal rule based on the procedure mentioned in chapter Working with the Captive Portal App, on page 81.
- If social authentication is required for captive portal, configure social authentication as described in Configuring Cisco Wireless Controller for Social Authentication, on page 210.
- If you want to send notifications using Cisco DNA Spaces, configure the engagement rules based on the procedure mentioned in chapter Sending Notifications with the Engagements App, on page 155.

Cisco Catalyst 9800 Series Wireless Controller with Cisco DNA Spaces Connector

To connect Cisco Catalyst 9800 Series Wireless Controller to Cisco DNA Spaces using a Cisco DNA Spaces Connector, and to configure captive portal authentication or notifications, do the following:

- To connect Cisco Catalyst 9800 Series Wireless Controller to Cisco DNA Spaces using a Cisco DNA Spaces Connector, refer the procedure mentioned in Cisco DNA Spaces: Connector Configuration Guide.
- After connecting Cisco Catalyst 9800 Series Wireless Controller to Cisco DNA Spaces, for social authentication, radius authentication, and internet provisioning (for using the Captive Portals app and Engagements app), refer to a matching section from the following:
  - Configuring Cisco Catalyst 9800 Series Wireless Controller (Local Mode) for Captive Portals and Engagements Apps Using CLI, on page 217
  - Configuring Cisco Catalyst 9800 Series Wireless Controller GUI (Local Mode) for Captive Portals and Engagements Apps, on page 221
  - Configuring Cisco Catalyst 9800 Series Wireless Controller GUI (Flex Mode or Mobility Express) for Captive Portals and Engagements Apps, on page 225.
- To configure Captive Portal Authentication, import SSIDs, create captive portal with the required authentication type, and configure Captive Portal rule based on the procedure mentioned in chapter Working with the Captive Portal App, on page 81.
- If you want to send notifications using Cisco DNA Spaces, configure the engagement rules based on the procedure mentioned in chapter Sending Notifications with the Engagements App, on page 155.
Configuring Mobility Express to work with Cisco DNA Spaces

This section describes the configurations to be done in the Mobility Express Controller for using Cisco DNA Spaces.

The configurations required for various Mobility Express versions are different. The configurations for various Mobility Express versions are as follows:

Configuring Mobility Express 8.7 or Later for Cisco DNA Spaces

To configure the Mobility Express 8.7 or later for Cisco DNA Spaces, perform the following steps:

Creating SSIDs in the Mobility Express

To create SSIDs in the Mobility Express, perform the following steps:

Step 1 Log in to Mobility Express with your credentials.
Step 2 In the main window, click Wireless Settings in the left pane.
Step 3 Click WLANs.
Step 4 To create a WLAN, click Add new WLAN/RLAN.
Step 5 In the window that appears, in the General tab, enter the WLAN details like Type, Profile Name, SSID, and so on.
Step 6 Click Apply.

The Add new WLAN/RLAN window appears.

Step 7 Click WLAN Security.
Step 8 Enable the Guest Network toggle switch.
Step 9 Enable the Captive Network Assistant toggle switch.
Step 10 From the Captive Portal drop-down list, choose External Splash Page.
Step 11 From the Access Type drop-down list, choose Web Consent.
Step 12 In the Captive Portal URL field that appears, enter the Cisco DNA Spaces splash URL.

To view the splash URL for your ME account, in the Cisco DNA Spaces dashboard, click the Configure Manually link for a CUWN SSID in the SSIDs window.

Step 13 Click Apply.
Step 14 To enable and broadcast the SSID, in the General tab, from the Admin drop-down list, choose “Enabled”, and enable the “Broadcast SSID” toggle switch.
Step 15 Execute the following command in the command prompt to disable the secure webauth mode. Then, restart the ME.

```
config network web-auth secureweb disable
```

Step 16 Execute the following command in the command prompt to change the webauth login success page from Default to None.

```
config custom-web webauth-login-success-page none
```

Configuring RADIUS Authentication in Mobility Express 8.7 or Later

To configure radius authentication in the Mobility Express 8.7 or later, perform the following steps:
Step 1: Log in to Mobility Express with your credentials.

Step 2: In the ME main window, click Switch to Expert View in the top right of the window.

Step 3: In the pop up window that appears, select OK.

Step 4: In the left pane, click Management > Admin Accounts.

Step 5: In the window that appears, click the Radius tab.

Step 6: Click Add RADIUS Authentication Server.

In the Add/ Edit Radius Authentication Server window appears, enter the following radius server details:

   a) In the Server IP Address field, enter the IP address of the radius server.
   b) In the Shared Secret field, enter your radius secret key.
   c) In the Confirm Shared Secret field, re-enter the radius secret key.

Note: You can configure only the Cisco DNA Spaces radius servers. To view the IP address and secret key for radius server configuration, in the Cisco DNA Spaces dashboard, click the Captive Portal app. Click SSIDs, and then click the Configure Manually link for a Cisco Unified Wireless Network (Cisco AireOS) SSID. Click the Configure SSID in CUWN-WLC tab. The radius server details will be listed in the Radius Server Configuration section. Configure both the primary and secondary radius server IPs. You can also contact the Cisco DNA Spaces support team.

Step 7: Click Apply.

Step 8: In the Mobility Express main window, click Wireless Settings in the left pane.

Step 9: Click WLANs.

The WLAN/RLAN Configuration window appears with the SSIDs list.

Step 10: Click the Edit icon for the SSID created previously.

Step 11: In the Edit WLAN window that appears, click the WLAN Security tab.

Step 12: From the Access Type drop-down list, choose Radius.

Step 13: Click the Radius Server tab, and click Add RADIUS Authentication Server.

Step 14: From the Server IP Address drop-down list, select your Radius Server, and click Apply.

Step 15: In the Edit WLAN window, click Apply.

Now the Mobility Express 8.7 or later is configured for radius server authentication.

Creating Access Control Lists in Mobility Express 8.7 or Later

To create Access Control Lists in the Mobility Express 8.7 or later, perform the following steps:

Step 1: Log in to Mobility Express with your credentials.

Step 2: In the Mobility Express main window, click the Wireless Settings in the left pane.

Step 3: Click WLANs.

The WLAN/RLAN Configuration window appears with the SSIDs list.

Step 4: Click the Edit icon for the SSID created previously.
In the **Edit WLAN** window that appears, click the **WLAN Security** tab.

**Step 5** Click the **Pre Auth ACLs** tab.

**Step 6** Click **Add IP Rules**.

**Step 7** In the Add/Edit IP ACLs, create rules with the following configuration:

<table>
<thead>
<tr>
<th>Action</th>
<th>Source IP Address/Netmask</th>
<th>Destination IP Address/Netmask</th>
<th>Protocol</th>
<th>Source Port Range</th>
<th>Dest Port Range</th>
<th>DSCP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permit</td>
<td>34.235.248.212/255.255.255</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
</tr>
<tr>
<td>Permit</td>
<td>0.0.0.0/0.0.0.0</td>
<td>34.235.248.212/255.255</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
</tr>
<tr>
<td>Permit</td>
<td>54.77.207.183/255.255.255</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
</tr>
<tr>
<td>Permit</td>
<td>54.77.207.183/255.255.255</td>
<td>54.77.207.183/255.255</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
</tr>
</tbody>
</table>

**Note** For EU region, **34.235.248.212, 52.55.235.39** must be replaced with **54.77.207.183,34.252.175.120**.

When defining the ACL rule, ensure to configure the values as follows:

- **Protocol**: Any
- **DSCP**: Any
- **Action**: Permit

**Step 8** Click **Apply**.

---

**Configuring Mobility Express 8.7 or Later for Social Authentication**

To configure the Mobility Express for Social Sign authentication for captive portals, perform the following steps:

**Step 1** Log in to Mobility Express with your credentials.

**Step 2** In the **Mobility Express** main window, click the **Wireless Settings** in the left pane.

**Step 3** Click **WLANs**.

The **WLAN/RLAN Configuration** window appears with the SSIDs list.

**Step 4** Click the **Edit** icon for the SSID created previously.

In the **Edit WLAN** window that appears, click the **WLAN Security** tab.

**Step 5** Click the **Pre Auth ACLs** tab.

**Step 6** Click **Add IP Rules**.

**Step 7** In the Add/Edit IP ACLs, configure the following two rules in addition to the existing ACL rules:

<table>
<thead>
<tr>
<th>Action</th>
<th>Source IP Address/Netmask</th>
<th>Destination IP Address/Netmask</th>
<th>Protocol</th>
<th>Source Port Range</th>
<th>Dest Port Range</th>
<th>DSCP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permit</td>
<td>0.0.0.0/0.0.0.0</td>
<td>0.0.0.0/0.0.0.0</td>
<td>TCP</td>
<td>HTTPS</td>
<td>Any</td>
<td>Any</td>
</tr>
</tbody>
</table>
### Allowing the URLs in the Mobility Express 8.7 or Later

To allow a URL in the Mobility Express 8.7 or later, perform the following steps:

<table>
<thead>
<tr>
<th>Action</th>
<th>Source IP Address/Netmask</th>
<th>Destination IP Address/Netmask</th>
<th>Protocol</th>
<th>Source Port Range</th>
<th>Dest Port Range</th>
<th>DiffServ</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permit</td>
<td>0.0.0.0/0.0.0.0</td>
<td>0.0.0.0/0.0.0.0</td>
<td>TCP</td>
<td>Any</td>
<td>HTTPS</td>
<td>Any</td>
</tr>
</tbody>
</table>

**Step 1** Log in to ME with your credentials.

**Step 2** In the ME main window, click the **Wireless Settings** in the left pane.

**Step 3** Click **WLANs**.

   The **WLAN/RLAN Configuration** window appears with the SSIDs list.

**Step 4** Click the **Edit** icon for the SSID created previously.

**Step 5** In the **Edit WLAN** window that appears, click the **WLAN Security** tab.

**Step 6** Click the **Pre Auth ACLs** tab.

**Step 7** Click **Add URL Rules**.

**Step 8** In the **Add/Edit URL ACLs** window that appears, configure the URL that you want to include in the allowed list.

When defining the URL rule, ensure to configure the values as follows:

- **URL**: domain
- **Action**: Permit

**Step 9** Click **Update**.

### Configuring Mobility Express for Notifications and Reports

If you are using Mobility Express with WLC connect, to configure for location updates, perform the following steps:

**Step 1** In the **Cisco Wireless Controller CLI**, execute the following commands:

- a. `config cloud-services cmx disable`
- b. `config cloud-services server url https://{Customer Path Key}.{LB Domain} {LB IP Address}`
- c. `config cloud-services server id-token {Customer JWT Token}`
- d. `config network dns serverip <dns server ip>`
- e. `config cloud-services cmx enable`
To view the {Customer Path Key}, {LB Domain}, {LB IP Address}, and {Customer JWT Token}, in the Cisco DNA Spaces dashboard, click the Configure Manually link for a CUWN SSID in SSIDs window. You can also contact the Cisco DNA Spaces support team. Ensure that there are no trailing or leading spaces.

Step 2  Check the summary using the following command:

```sh
show cloud-services cmx summary
```

The result appears.

Now in the Cisco DNA Spaces dashboard, when you choose CUWN-WLC in the Add a Wireless Network window, the WLC will be listed. So, you can import the APs of that WLC to the Cisco DNA Spaces.

**Sample Result**

```sh
(Cisco Controller) >show cloud-services cmx summary
CMX Service
Server ....................................... https://$customerpathkey.dnaspaces.io
IP Address.................................... 50.16.12.224
Connectivity.................................. https: UP
Service Status ............................... Active
Last Request Status........................... HTTP/1.1 200 OK
Heartbeat Status ............................. OK
```

---

**What to do next**

Now the Cisco Wireless Controller will be available for importing to the Cisco DNA Spaces location hierarchy. For more information on importing the Cisco Wireless Controller and its access points, follow from Step 4 of the procedure mentioned in Connecting Cisco DNA Spaces to Cisco Wireless Controller Using Cisco WLC Direct Connect, on page 213.

---

**Configuring Mobility Express 8.6 or Earlier for Cisco DNA Spaces**

To configure Mobility Express 8.6 or earlier for Cisco DNA Spaces:

**Creating SSIDs in Mobility Express 8.6 or Earlier**

The steps to create SSIDs in Mobility Express 8.6 or earlier are same as that for Mobility Express 8.7 or later. To know the configuration steps, see the Creating SSIDs in the Mobility Express, on page 232.

**Configuring RADIUS Authentication for Mobility Express 8.6 or Earlier**

In Mobility Express 8.6 or earlier, you cannot configure radius servers individually.

To configure Mobility Express 8.6 or earlier for RADIUS authentication, perform the following steps:

**Step 1**  Log in to Mobility Express with your credentials.

**Step 2**  In the Mobility Express main window, click Wireless Settings in the left pane.

**Step 3**  Click WLANs.
The WLAN/RLAN Configuration window appears with the SSIDs list.

**Step 4**  Click the **Edit** icon for the SSID created previously.

**Step 5**  In the **Edit WLAN** window that appears, click the WLAN Security tab.

**Step 6**  From the **Access Type** drop-down list, choose **Radius**.

**Step 7**  To add the radius server, click **Add**.

**Step 8**  In the window that appears, enter the following radius server details:

- a. In the **Server IP Address** field, enter the IP address of the radius server.

- b. In the **Shared Secret** field, enter your radius secret key.

- c. In the **Confirm Shared Secret** field, re-enter the radius secret key.

- d. Click **Apply**.

**Note**  You can configure only the Cisco DNA Spaces radius servers. To view the IP address and secret key for radius server configuration, in the Cisco DNA Spaces dashboard, click the **Captive Portal** app. Click **SSIDs**, and then click the **Configure Manually** link for a Cisco Unified Wireless Network (Cisco AireOS) SSID. Click the **Configure SSID in CUWN-WLC** tab. The radius server details will be listed in the **Radius Server Configuration** section. Configure both the primary and secondary radius server IPs. You can also contact the Cisco DNA Spaces support team.

**Step 9**  In the **Edit WLAN** window, click **Apply**.

Now, the Mobility Express is configured for radius server authentication of Cisco DNA Spaces captive portals.

---

**Creating ACLs for Mobility Express 8.6 or Earlier**

Mobility Express 8.6 or earlier does not provide user interface to configure Access Control Lists. So for creating ACLs, and configuring social authentication, you must use the command prompt. For the commands to use for these ACL configurations, see the “Mobility Express Command Reference Guide”.

Now the Cisco Wireless Controller will be available for import in Cisco DNA Spaces location hierarchy. For more information on importing the Cisco Wireless Controller and access points to the Cisco Wireless Controller, follow from Step 3 of the procedure mentioned in Connecting Cisco DNA Spaces to Cisco Wireless Controller Using Cisco WLC Direct Connect, on page 213.

**Configuring Mobility Express for Notifications and Reports**

If you are using Mobility Express with WLC connect, to configure for location updates, perform the following steps:

**Step 1**  In the **Cisco Wireless Controller CLI**, execute the following commands:

- a. `config cloud-services cmx disable`

- b. `config cloud-services server url https://{Customer Path Key}.{LB Domain} {LB IP Address}`

- c. `config cloud-services server id-token {Customer JWT Token}`

- d. `config network dns serverip <dns server ip>`

- e. `config cloud-services cmx enable`
To view the Customer Path Key, LB Domain, LB IP Address, and Customer JWT Token, in the Cisco DNA Spaces dashboard, click the **Configure Manually** link for a CUWN SSID in SSIDs window. You can also contact the Cisco DNA Spaces support team. Ensure that there are no trailing or leading spaces.

**Step 2**  
Check the summary using the following command:

```
show cloud-services cmx summary
```

The result appears.

Now in the Cisco DNA Spaces dashboard, when you choose **CUWN-WLC** in the **Add a Wireless Network** window, the WLC will be listed. So, you can import the APs of that WLC to the Cisco DNA Spaces.

**Sample Result**

(Cisco Controller) > show cloud-services cmx summary

CMX Service

Server ....................................... https://$customerpathkey.dnaspaces.io

IP Address.................................... 50.16.12.224

Connectivity.................................. https: UP

Service Status ............................... Active

Last Request Status ......................... HTTP/1.1 200 OK

Heartbeat Status ......................... OK

---

**What to do next**

Now the Cisco Wireless Controller will be available for importing to the Cisco DNA Spaces location hierarchy. For more information on importing the Cisco Wireless Controller and its access points, follow from Step 4 of the procedure mentioned in [Connecting Cisco DNA Spaces to Cisco Wireless Controller Using Cisco WLC Direct Connect](#), on page 213.

### Configuring Aironet 4800 Series Mobility Express Controller 8.10.150.0 for Cisco DNA Spaces

To configure AireOS 4800 Series Mobility Express Controller 8.10.150.0 for Cisco DNA Spaces:

#### Configuring Mobility Express 8.10.150.0

To configure Mobility Express 8.10.150.0 for Cisco DNA Spaces, perform the following steps:

**Step 1**  
Log in to **Mobility Express** with your credentials.

**Step 2**  
Go to **Advanced > Security Settings**.

**Step 3**  
Click **Add New ACL**.

**Step 4**  
In the **Add ACL Rule** window, enter the ACL details:

a) From the **ACL Type** drop-down list, choose **IPv4**.

b) In the **ACL name field**, enter a name for the ACL.

c) Click **Add URL Rules**.

The **Add /Edit URL ACLs** window appears.
d) In the **URL** field, enter splash page URL domain.

e) From the **Action** drop-down list, choose **Permit**.

f) To enable social authentication, add the following domains in the ACL:

   - *.facebook.com
   - *.facebook.com
   - ssl.gstatic.com
   - static.licdn.com
   - *.fbcdn.net
   - *.akamaihd.net
   - *.twitter.com
   - *.twimg.com
   - oauth.googleusercontent.com
   - *.googleapis.com
   - *.accounts.google.com
   - *.gstatic.com
   - *.linkedin.com
   - *.licdn.net
   - *.licdn.com

This step is required only if you want to enable social authentication.

g) Click **Update**.

### Step 5

To add radius server configuration, perform the following steps:

a) Create an ACL.

b) Enable **Expert** view.

c) Go to **Management > Admin Accounts > Radius**

d) From the **Authentication Call Station ID Type** drop-down list, choose **AP MAC Address:SSID**.

e) From the **Authentication MAC Delimiter** drop-down list, choose **Hyphen**.

f) From the **Accounting Call Station ID Type** drop-down list, choose **AP MAC Address:SSID**.

g) From the **Accounting MAC Delimiter** drop-down list, choose **Hyphen**.

h) From the **Fallback Mode** drop-down list, choose **Off**.

i) Click **Apply**.

### Step 6

Click **Add Radius Authentication Server**, and in the **Add/Edit Radius Authentication Server** that appears, enter the following details:

a) Disable **CoA**.

b) In the **Server Ip Address** field, enter the radius server IP address.

c) In the **Shared Secret** field, enter the secret key.

d) In the **Confirm Shared Secret** field, enter the secret key to confirm

e) Click **Apply**.
Added radius server will be listed under the Radius Servers list.

**Note** You can configure only the Cisco DNA Spaces radius servers. To view the IP address and secret key for the radius server configuration, in the Cisco DNA Spaces dashboard, click the Captive Portals app. Click SSIDs, and then click the Configure Manually link for a Cisco Unified Wireless Network (Cisco AireOS) SSID. The radius server details will be listed in the Radius Server Configuration section. Configure both the primary and secondary radius server IPs. You can also contact the Cisco DNA Spaces support team.

### Step 7
To configure WLAN for radius server, perform the following steps:

a) In the Cisco Aironet ME dashboard, choose Wireless Settings > WLAN.

b) Click the General tab.

c) In the Profile Name field, enter the SSID name.

d) From the Admin State drop-down list, choose Enabled.

e) From the Radio Policy drop-down list, choose ALL.

f) Click the WLAN Security tab.

g) Enable Guest Network.

h) Enable Captive Network Assistant.

i) In the Captive Portal URL field, enter the captive portal URL.

**Note** To view the Captive Portal URL, in the Cisco DNA Spaces dashboard, click the Captive Portals app. Click SSIDs, and then click the Configure Manually link for a Cisco Unified Wireless Network (Cisco AireOS) SSID. Go to the Creating the SSIDs in WLC Direct Connect section. The URL is displayed at Step 7g.

j) From the Access Type, choose RADIUS.

k) In the ACL Name (IPV4), choose the ACL name configured at Step 4b.

l) For radius server, click Add Radius Authentication Server

m) Select Radius server IP added at Step 6b from the list.

### Step 8
For Radius L2 Authentication, enable MAC Filtering and ON MAC Filter failure.

### Step 9
Click Apply.

---

### Configuring Mobility Express for Notifications and Reports

If you are using Mobility Express with WLC connect, to configure for location updates, perform the following steps:

### Step 1
In the Cisco Wireless Controller CLI, execute the following commands:

a. config cloud-services cmx disable

b. config cloud-services server url https://{Customer Path Key}.LB Domain {LB IP Address}

c. config cloud-services server id-token {Customer JWT Token}

d. config network dns serverip <dns server ip>

e. config cloud-services cmx enable
To view the \{Customer Path Key\}, \{LB Domain\}, \{LB IP Address\}, and \{Customer JWT Token\}, in the Cisco DNA Spaces dashboard, click the \textbf{Configure Manually} link for a CUWN SSID in SSIDs window. You can also contact the Cisco DNA Spaces support team. Ensure that there are no trailing or leading spaces.

\textbf{Step 2} Check the summary using the following command:

\texttt{show cloud-services cmx summary}

The result appears.

Now in the Cisco DNA Spaces dashboard, when you choose \textbf{CUWN-WLC} in the \textbf{Add a Wireless Network} window, the WLC will be listed. So, you can import the APs of that WLC to the Cisco DNA Spaces.

\textbf{Sample Result:}

(Cisco Controller) \texttt{>show cloud-services cmx summary}

\begin{verbatim}
CMX Service
Server ....................................... https://$customerpathkey.dnaspaces.io
IP Address................................. 50.16.12.224
Connectivity.............................. https: UP
Service Status .............................. Active
Last Request Status....................... HTTP/1.1 200 OK
Heartbeat Status ......................... OK
\end{verbatim}

\textbf{What to do next}

Now the Cisco Wireless Controller will be available for importing to the Cisco DNA Spaces location hierarchy. For more information on importing the Cisco Wireless Controller and its access points, follow from Step 4 of the procedure mentioned in \textbf{Connecting Cisco DNA Spaces to Cisco Wireless Controller Using Cisco WLC Direct Connect} , on page 213.

\textbf{Cisco DNA Spaces Scale Benchmark}

\textit{Table 14: Scale Summary}

<table>
<thead>
<tr>
<th>SNO</th>
<th>Cisco DNA Spaces Connector</th>
<th>Cisco WLC Direct Connect</th>
<th>CMX Tethering Connector</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platforms</td>
<td>Cisco AireOS</td>
<td>Cisco AireOS</td>
<td>Cisco Catalyst 9800 Series</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SNO</td>
<td>Cisco DNA Spaces Connector</td>
<td>Cisco WLC Direct Connect</td>
<td>CMX Tethering Connector</td>
</tr>
<tr>
<td>-----</td>
<td>---------------------------</td>
<td>--------------------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>Max Scale on supported appliance.</td>
<td>12.5K APs, 250K clients</td>
<td>50 APs and 50 Clients</td>
<td>60K clients, 5K APs, and 50k RFID tags</td>
</tr>
<tr>
<td></td>
<td>Incoming NMSP should not be more than 10.5K messages/sec.</td>
<td>50 APs and 50 Clients</td>
<td>Maps with 1BLDG-100 Floors and each floor with 50 APs</td>
</tr>
<tr>
<td>Scale supported releases</td>
<td>Connector version 2.1.1 with docker v2.0.204</td>
<td>8.8MR2</td>
<td>16.12, 17.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>8.8MR2 with CMX 10.6 (high end)</td>
</tr>
</tbody>
</table>

**Note**
Currently, scaling is not available for Mobility Express.
CHAPTER 15

Configuring Cisco Meraki for Cisco DNA Spaces

This chapter describes the configurations required in Cisco Meraki for using Cisco DNA Spaces.

- Configuring Cisco Meraki Service Account, on page 243
- Enabling SSIDs in Cisco Meraki, on page 244
- Configuring Cisco Meraki for RADIUS Authentication, on page 244
- Configuring Cisco Meraki for Notifications and Reports, on page 246
- Configuring Cisco Meraki for Social Authentication, on page 247
- Manually Configuring SSIDs for Cisco Meraki, on page 247

Configuring Cisco Meraki Service Account

The details of Meraki network such as organization, networks, APs and so on can be fetched to Cisco DNA Spaces using a Meraki Service account.

To avail this support, you must invite the Meraki service account from your Meraki customer account. You can contact the Cisco DNA Spaces support team for the e-mail ID of Meraki Service account.

Note

- However, to connect Cisco DNA Spaces to Cisco Meraki, you must still use your Meraki customer account. The customer's Meraki account is used for importing the networks into location hierarchy, for which the user has access to. The service account is used for background network synchronization to keep the Location Hierarchy up-to-date.
- As Cisco Meraki is not a part of the Cisco DNA Spaces, the menu path and menu names are subject to change.

To configure a Cisco Meraki Service account in Cisco Meraki, perform the following steps:

Step 1 Go to https://meraki.cisco.com.
Step 2 Log in to the application using the login credentials for your Cisco Meraki account.
Step 3 From the Cisco Merkai Organization drop-down list, choose the organization for which you want to configure the Meraki Service account.
Step 4 Choose Organization > Administrators > Add Admin.
Step 5 Enter the name and e-mail ID for the Cisco Meraki service account.
Step 6  From the Organization Access drop-down list, choose Full.
Step 7  Click Create Admin.

The Cisco Meraki service account is now configured for the filtered organization.

---

Enabling SSIDs in Cisco Meraki

To import the SSIDs to the Cisco DNA Spaces to configure them for the Captive Portal Rules, you must enable those SSIDs in Cisco Meraki.

Note: As Cisco Meraki is not a part of the Cisco DNA Spaces, the menu path and menu names are subject to change.

To enable the SSIDs in Cisco Meraki, perform the following steps:

Step 1  Go to https://meraki.cisco.com.
Step 2  Log in to the application using the login credentials for your Cisco Meraki account.
Step 3  Click the Cisco Meraki Organization in which you want to enable the SSIDs, and choose the required network.
Step 4  Choose Wireless > Configure > SSIDs.

The SSIDs available for the network appears.

Step 5  Rename the SSID and enable it.
Step 6  Click Edit Settings, and in the Splash page option, click the Click-Through radio button.
Step 7  Click Save Changes.

The SSID is successfully enabled in Cisco Meraki.

---

Configuring Cisco Meraki for RADIUS Authentication

To provide more security to your portals, the Cisco DNA Spaces provides radius-authentication for the portals. Also, certain configurations are required in Cisco Meraki to manage the seamless internet provisioning that can be configured using the Captive Portal Rule.

The Radius Server Configurations required when configuring for the seamless internet provisioning is different from that of the standard radius server configuration.

Configuring Cisco Meraki for RADIUS Authentication (Without Seamless Internet Configurations)

To configure Cisco Meraki for radius authentication, perform the following steps:
Configuring Cisco Meraki for RADIUS Authentication and Seamless Internet Provisioning

To configure Cisco Meraki for RADIUS authentication and Seamless Internet Provisioning, do the following configurations in Cisco Meraki:

Step 1  Log in to Cisco Meraki with your Meraki credentials.
Step 2  Choose Wireless Access Control.
Step 3  Choose the SSID for the captive portal rule.
Step 4  In the Association requirements area, choose Open.
Step 5  In the Splash page area, choose Sign-on with, and from the drop-down list select my RADIUS server.
Step 6  In the Radius servers area, click Add a server, and in the fields that appear mention the radius server details for authentication.

• Port: 1812

Note You can configure only the Cisco DNA Spaces radius servers. To view the radius server IP address and secret key, in the Cisco DNA Spaces dashboard, click the Configure Manually link for a Meraki SSID in the SSIDs page.

Step 7  From the Radius accounting drop-down list, choose Radius Accounting is enabled.
Step 8  In the Radius accounting servers area, click Add a server, and in the fields that appear mention the radius server details for accounting.

• Port: 1813

Note You can configure only the Cisco DNA Spaces radius servers. You can configure only the Cisco DNA Spaces radius servers. To view the radius server IP address and secret key, in the Cisco DNA Spaces dashboard, click the Configure Manually link for a Meraki SSID in the SSIDs page.

Step 9  Configure the Wall Garden ranges. To view the wall garden ranges, in the Cisco DNA Spaces dashboard, click the Configure Manually link for a Meraki SSID in the SSIDs page.

Step 10  Save the changes.

Configuring Cisco Meraki for Cisco DNA Spaces

Configuring Cisco Meraki for RADIUS Authentication and Seamless Internet Provisioning
You can configure only the Cisco DNA Spaces radius servers. To view the radius server IP address and secret key, in the Cisco DNA Spaces dashboard, click the **Configure Manually** link for a Meraki SSID in the SSIDs page.

**Step 7**
From the **Radius accounting** drop-down list, choose **Radius Accounting is enabled**.

**Step 8**
In the **Radius accounting servers** area, click **Add a server**, and in the fields that appear mention the radius server details for accounting.

- Port: 1813

**Note**
You can configure only the Cisco DNA Spaces radius servers. To view the radius server IP address and secret key, in the Cisco DNA Spaces dashboard, click the **Configure Manually** link for a Meraki SSID in the SSIDs page.

**Step 9**
From the **Radius attribute specifying group policy name** drop-down list, choose **Filter-Id**.

**Step 10**
Save the changes.

**Step 11**
In the Cisco Meraki dashboard, click **Network-wide Group Policies**.

**Step 12**
Click **Add a Group**.

**Step 13**
In the **New group** window that appears, enter a name for the group.

**Note**
You have to configure this name as the policy name in the Cisco DNA Spaces dashboard. If you are specifying the group name as **CaptiveBypass**, this policy name will act as the default policy name for all the Captive Portal rules. That is, if you are not specifying a policy name for a Captive Portal rule for which the “Seamlessly Internet Provision” is opted, the policy name **CaptiveBypass** will be applied for that rule.

**Step 14**
From the **Bandwidth** drop-down list, choose the required option, and specify the Internet bandwidth to be provisioned for the customers.

**Step 15**
From the Splash drop-down list, choose **Bypass**.

**Step 16**
Click **Apply**.

**Step 17**
Configure the Wall Garden ranges. To view the wall garden ranges, in the Cisco DNA Spaces dashboard, click the **Configure Manually** link for a Meraki SSID in the SSIDs page.

---

### Configuring Cisco Meraki for Notifications and Reports

To send notifications using the Cisco DNA Spaces and to view the Cisco DNA Spaces reports, you must do certain configurations in Cisco Meraki.

To configure Cisco Meraki for sending notifications using the Cisco DNA Spaces or to view the Cisco DNA Spaces reports, perform the following steps:

**Step 1**
Log in to Cisco Meraki using the credentials for your Meraki account.

**Step 2**
Click the organization in which you want to enable SSIDs, and choose the required network.

**Step 3**
Choose **Network-wide > Configure > General**.

**Step 4**
In the CMX area, do the following:

a) From the **Analytics** drop-down list, choose **Analytics is enabled**.

b) From the **Scanning API** drop-down list, choose **Scanning API enabled**.
c) Click Add a Post URL, and enter the post URL details in the respective fields.

To view the post URL details, in the Cisco DNA Spaces dashboard, click the Configure Manually link for a Meraki SSID in the SSIDs window.

**Step 5** Click Save Changes.

---

**Configuring Cisco Meraki for Social Authentication**

For social authentication with Cisco Meraki, you must do some configurations in meraki.cisco.com.

To configure Cisco Meraki for social-authentication, perform the following steps:

**Step 1** In the Cisco Meraki dashboard, choose Wireless > Configure > Access Control.

The Access Control window appears.

**Step 2** From the SSID drop-down list, choose the SSID for which you want to configure the social authentication.

**Step 3** In the Wall Garden Ranges field, enter the social networking domain names listed in the following table, and click Save Changes.

<table>
<thead>
<tr>
<th>Social Networking Domain Names</th>
<th>Facebook</th>
<th>Twitter</th>
<th>LinkedIn</th>
<th>Instagram</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>.facebook.com</td>
<td>.twitter.com</td>
<td>.linkedin.com</td>
<td>instagram.com</td>
</tr>
<tr>
<td></td>
<td>.fbcdn.net</td>
<td>.twimg.com</td>
<td>.licdn.net</td>
<td>.instagram.com</td>
</tr>
<tr>
<td></td>
<td>.akamaihd.net</td>
<td>.licdn.com</td>
<td></td>
<td>api.instagram.com</td>
</tr>
<tr>
<td></td>
<td>.connect.facebook.net</td>
<td></td>
<td></td>
<td>d36xkk24g8jdx.cloudfront.net</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td><a href="http://www.facebook.com">www.facebook.com</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>connect.facebook.net</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>* .akamaihd.net</td>
</tr>
</tbody>
</table>

Social Authentication for Cisco Meraki is successfully configured.

---

**Manually Configuring SSIDs for Cisco Meraki**

To manually configure an SSID in Cisco Meraki, you have to initially import that SSID in the Cisco DNA Spaces. For more information, see the "Importing the SSIDs for Cisco Meraki section .

To configure the SSID manually in Cisco Meraki, perform the following steps:
Manually Configuring SSIDs for Cisco Meraki

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Log in to Cisco Meraki using the credentials for your Meraki account.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Choose the required Cisco Meraki organization and network from the respective drop-down list.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Choose Wireless &gt; Access Control.</td>
</tr>
<tr>
<td>Step 4</td>
<td>From the SSID drop-down list, choose the SSID that you want to configure for the Cisco DNA Spaces.</td>
</tr>
<tr>
<td>Step 5</td>
<td>In the splash page area, choose Click-through.</td>
</tr>
<tr>
<td>Step 6</td>
<td>From the Wall garden drop-down list, choose Wall garden is enabled.</td>
</tr>
<tr>
<td>Step 7</td>
<td>In the Wall garden ranges field, enter the required wall garden ranges.</td>
</tr>
</tbody>
</table>

To view the wall garden ranges, in the Cisco DNA Spaces dashboard, click the Configure Manually link for a Meraki SSID in the SSIDs window.

| Step 8 | Click Save Changes. |
| Step 9 | Choose Wireless > Splash page. |
| Step 10 | For the previously selected SSID, in the Custom Splash URL area, choose Or provide a URL where customers will be redirected, and in the adjacent field enter the splash URL. |

**Note** When you import an SSID to the Cisco DNA Spaces, the splash page URL for the SSID is generated in the Cisco DNA Spaces. To view the splash URL for an SSID, in the Cisco DNA Spaces dashboard, click the Configure Manually link for that Meraki SSID in the SSIDs page.

| Step 11 | In the Splash Behavior area, click the The URL they were trying to fetch radio button under Where should users go after the splash page. |
| Step 12 | Click Save Changes. |
| Step 13 | Repeat steps 3-12 for all the SSIDs that you want to use in the Cisco DNA Spaces. |

What to do next
PART I

Setup

• Setup Wireless Network, on page 251
• Setup Meraki Camera, on page 255
Setup Wireless Network

This chapter provides an overview on how to view the configuration instructions for various wireless networks, and how to configure the wireless network through various methods.

- Setting Up Cisco DNA Spaces to Work with Various Wireless Networks, on page 251

Setting Up Cisco DNA Spaces to Work with Various Wireless Networks

To work with Cisco DNA Spaces, you must connect it with your wireless network. You can use Cisco DNA Spaces with Cisco AireOS (Catalyst) or Cisco Meraki. Cisco DNA Spaces provides instructions along with the required features to connect to various networks.

To connect Cisco DNA Spaces to a wireless network, perform the following steps:

Step 1 In the Cisco DNA Spaces dashboard, choose Setup > Wireless Networks.

Step 2 In the Connect your wireless Network window, click Add New.

A window appears with the options Cisco AireOS/Catalyst and Cisco Meraki.

Note For new Cisco DNA Spaces accounts, the button name will be Get Started.

Step 3 Click Select for your wireless network.

Displays different methods through which you can connect to your wireless network.

- For Cisco AireOS/Catalyst, configurations for the following methods will be available:
  - Via Spaces Connector: To connect Cisco DNA Spaces to Cisco Wireless Controller using a Cisco DNA Spaces Connector.
  - Connect WLC Directly: To connect Cisco DNA Spaces to Cisco Wireless Controller using a Cisco Wireless Controller Direct Connect.
  - Via CMX On-Prem: To connect Cisco DNA Spaces to Cisco Wireless Controller using Cisco CMX.

- For Cisco Meraki, configurations for the following methods will be available:
  - Connect via Meraki Login: To connect Cisco DNA Spaces to Cisco Meraki using a Cisco Meraki account.
• **Connect via API Key**: To connect Cisco DNA Spaces to Cisco Meraki using a Cisco Meraki API Key.

**Step 4**  
Click Select for the method through which you want to connect to Cisco DNA Spaces.  
The prerequisites for connecting to the wireless network using the selected method is displayed. Ensure that the prerequisites are met.

**Step 5**  
Click Customize Setup.  
The message Successfully saved the configuration is shown.

**Step 6**  
A bar corresponding to the wireless network configuration method selected appears in the **Connect your wireless network** window. For example, if you select **Via Spaces Connector**, a bar **Connect via Spaces Connector** appears.

**Step 7**  
To view the instructions, and configure the wireless network, click the drop-down button at the far right of the bar.  
The instructions, and the features to connect to the particular network using the particular method is displayed.

**Step 8**  
Follow the instructions to add the wireless network.

---

**Wireless Network Bars**

Any of the following bars will be displayed for Cisco AireOS based on the connection method selected:

- **Connect via Spaces Connector**: Displays step-by-step instructions to connect Cisco DNA Spaces to Cisco Wireless Controller using a Cisco DNA Spaces Connector. You can add connectors using the Create a new token option provided at Step 2. You can add Cisco Wireless Controllers using the Add Controllers option provided at Step 3. You can then import the added Cisco Wireless Controller to the Cisco DNA Spaces location hierarchy using the Import Controllers option at Step 4. You can view the Cisco DNA Spaces Connectors and Cisco Wireless Controllers added using View Connectors and View Controllers options respectively. You can view the location hierarchy using the View Location Hierarchy option. For the OpenRoaming app, you can configure the hotspots through the Add OpenRoaming Hotspot option provided at Step 2. You can also view the configurations for the OpenRoaming app for various controllers separately using the OpenRoaming Controller Configuration option provided at Step 2.


- **Connect via CMX Manual Upload**: Displays step-by-step instructions to configure location hierarchy using a JSON file and to configure location updates for these locations for notifications and reports. You can upload the JSON file using the Upload Json option at Step 3.

- **Connect via CMX Tethering**: Displays step-by-step instructions to configure location updates for a Cisco CMX node using CMX tethering with token. You can create the token using the Create New Token option at Step 2, and configure it in Cisco CMX. Then you can add the tethered Cisco CMX node to the location hierarchy using the Add CMX option at Step 3.

- **Connect via CMX On-Prem Auto Sync**: Displays step-by-step instructions to configure location updates for Cisco DNA Spaces by connecting to a Cisco CMX account using VPN. You can connect to Cisco CMX using Add CMX On-Prem provided at Step 2.
Any of the following tab will be displayed for Cisco Meraki based on your selection.

- **Connect via Meraki Login**: Displays instructions to connect Cisco DNA Spaces to Cisco Meraki network using a Meraki account. You can connect to Cisco Meraki using the Connect option provided at Step 1. You can import a Meraki Organization and its child locations to the location hierarchy using the Import Networks option at Step 3.

- **Connect via Meraki API Key**: Displays instructions to connect Cisco DNA Spaces to Cisco Meraki network using a Meraki API Key. You can import a Meraki Organization and its child locations to the location hierarchy using the Import Networks option at Step 3.

**View Configuration Steps**: Redirects to the documentation for the particular wireless network.

**System Requirements**: Provides the system requirements for Cisco DNA Spaces.

**Frequently asked questions**: Provides the link to the frequently asked questions for Cisco DNA Spaces.

**Cisco AireOS/Catalyst**: Displays instructions to import a CMX Node (CMX On-Prem) to the Location Hierarchy window.

**Cisco Meraki**: Displays instructions to import a Meraki Organization to the Location Hierarchy window.
CHAPTER 17

Setup Meraki Camera

This chapter provides information on the configurations required in Cisco DNA Spaces for Meraki Camera.

- Setting up Cisco DNA Spaces to Work with Cisco Meraki Camera, on page 255

Setting up Cisco DNA Spaces to Work with Cisco Meraki Camera

Cisco DNA Spaces enables you determine the number of visitors visiting your locations using a Cisco Meraki Camera. To avail this feature you must have a Meraki log in and must have installed Cisco Meraki Cameras in your locations. Meraki Camera can be connected to existing Cisco AireOS or Cisco Catalyst network as long as the camera can reach Meraki cloud server. Also, you must have valid Meraki MV Sense licenses.

You can capture the following details using the Camera feature:

- The total number of visits entering a location.
- The total number of visits leaving a location.
- The total number of visitors currently present at a location.

Note
If a visitor exits the tripwire line and enters the tripwire line again, the new entry is counted as a separate visit.

You can view the visitor count using the Camera Metrics and Right Now apps available in the Cisco DNA Spaces dashboard.

Configuring a Meraki Camera

To configure the Meraki Camera, perform the following steps:

Step 1 In the Cisco Meraki dashboard, configure the cameras on required Meraki Network. For more information on configuring the cameras on the Meraki network, see Configuring Cameras.

Step 2 Configure Cisco Meraki Service account. For more information on configuring Cisco Meraki Service account, see Configuring Cisco Meraki Service Account, on page 243.
Step 3 In the Cisco DNA Spaces dashboard, click the three-line menu icon displayed at the top-left of the dashboard.

Step 4 Choose Setup > Camera.

The Connect your Camera window appears.

Step 5 Click Get Started.

Note If you have connected to the Cisco Meraki earlier, the widget corresponding to the connection method used will be displayed automatically in the Connect your Camera window. In such cases, Get Started will not be displayed. If you want to connect to Cisco Meraki using same connection method(Login, API Key) for configuring Meraki camera, you can skip Step 4 to Step 6. However if you want to connect through the alternate connection method, you can add the corresponding widget using Add New. If you have added widgets for both connection methods (through login and API key), Add New will be disabled.

Step 6 Click Select to indicate the method that you wish to connect Cisco Meraki to Cisco DNA Spaces.

The window displays the prerequisites for the selected method. For more information on the methods, see Setting Up Cisco DNA Spaces to Work with Various Wireless Networks, on page 251.

Step 7 Click Continue Setup.

In the Connect your wireless network window, a widget now appears that allows you to connect the camera.

The widget that appears depend on the method you selected at Step 6. For the Connect Via Meraki Login method, the widget displayed will be Meraki Camera for analytics via Meraki Login. For the Connect via API Key method, the widget displayed will be Meraki Camera for analytics via Meraki API Key.

Step 8 In the expanded widget, click Connect displayed at Step 1.

If you are already connected to the Cisco Meraki network using the same connection method, the instruction for Step 1 gets replaced with the message that you are connected, and the Connect link will not be displayed. In such cases, you can skip this step.

a) For the Meraki Camera for analytics via Meraki Login widget, a window appears with fields to enter e-mail and password for login. Enter the login credentials, and click Submit. After connecting successfully, the content in Step 1 gets replaced with the message "Connected as [e-mail using which you have connected]."

b) For the Meraki Camera for analytics via Meraki API Key widget, a window appears with a API Key field. Enter the API Key, and click Submit. After connecting successfully, the content in Step 1 gets replaced with the message "Connected with [ masked API key]."

Step 9 Click Import Networks displayed at Step 2 in the Connect your Meraki Camera window.

And if the camera network is already imported to the location hierarchy section, then you can skip Step 9 to Step 13.

Step 10 In the Import Networks window, select the Meraki Organization (in which the Meraki Camera Networks are configured) that you want to import.

Step 11 From the Choose Networks area, select the check boxes for the Meraki networks that you want to import.

Step 12 Click Import.

The total number of Meraki networks and cameras that are imported are displayed.

Step 13 Click Finish.

Now, the Meraki Camera configurations in Cisco Meraki will get automatically synchronized with Cisco DNA Spaces. Typically, it gets auto configured in 48 hours. If you are facing any delay, manually configure the MQTT server details in Cisco Meraki as explained in the following step.
If want to manually configure the MQTT Server details in Cisco Meraki, perform the following:

Host and port of the MQTT server are account-specific and are displayed in Step 3 within the Cisco DNA Spaces Connect your Meraki Camera window. You must configure these MQTT server details in Cisco Meraki.

a) Log in to Cisco Meraki dashboard.
b) From the menu in the left pane of the dashboard, choose Cameras > Cameras.
c) In the Name field, click the link for the camera for which you want configure the MQTT server.

The details of the selected camera are displayed. The Video tab for the camera is displayed by default.

d) Click the Settings tab, and click Sense.
e) To the right of Sense API, click Enabled.
f) Click the Add or Edit MQTT Brokers link.
g) In the Edit MQTT Brokers window, click New MQTT Broker.
h) In the Edit MQTT Broker window that appears, enter the MQTT server details.

i) Click Save.

To configure the Entry/Exit line for the camera, click Draw Trip Wire at Step 4 in the Connect your Meraki Camera window.

Currently camera metrics are calculated only at location level. Please ensure that there is a camera at every entrance to a location where metrics are desired and that the tripwire is drawn for each of those cameras. To ensure accuracy, cameras should be placed in close proximity to an entrance with a clear view of the entire entry/exit point. Tripwire should be drawn several feet off the floor at the point of entry/exit. Do not draw a trip wire for any cameras at a location that are not located at a location level entry/exit point.

Note

In the Draw Trip-Wire window that appears, click Select Locations, choose the location in which the camera is configured, and click Done.

In the Select a camera you wish to draw the trip-wire area, select the radio button for the camera for which you want to set the trip wire, and click Next.

Create the trip-wire by drawing a line on the camera preview image using +.

By default, the entry and exit arrows will appear in the middle of the trip-wire. The green arrow represents Entry and the red arrow represents Exit. Ensure that the entry and exit arrows are pointing in the direction as shown in the following images. If the arrows are not positioned properly, hover over the line, and click the arrow that appears to flip the line.
The tripwire will function only if you have configured Meraki Service account.

**Step 19**

Ensure to click both the end points of the line to configure the XY coordinates. After clicking the end points of the line, the XY coordinates for the entry and exit arrows will be displayed automatically in the **Trip-wire status** area, and status gets changed to **Set**. By default, the status will be **Not Set**.

**Note** The status will be changed to **Set** only if you click both the end points of the line.

**Step 20**

Click **Finish**.

Now the camera is configured to use in Cisco DNA Spaces.

---

**What to do next**

Cisco DNA Spaces **Right Now** app will also report zone level presence data, if you have configured camera zones in Cisco Meraki. To define zones for each camera, refer to Cisco Meraki documentation.

---

**Editing the Trip Wire for a Camera**

To edit the XY coordinates of trip wire for a camera, perform the following steps:

**Step 1**

In the Cisco DNA Spaces dashboard, click the three-line menu icon displayed at the top-left of the dashboard.

**Step 2**

Choose **Settings > Camera**.

The **Connect your Meraki Camera** window appears.
Step 3 Click **View Cameras** displayed at Step 4 in the **Connect your Meraki Camera** window.

The Cameras imported to Cisco DNA Spaces are displayed. You can filter to view the cameras for a particular location.

Step 4 Click the **Edit** icon that is displayed far-right of the camera for which you want to edit the trip wire.

Step 5 In the **Edit Trip Wire** window that appears, edit the trip wire details, and click **Done**.
Editing the Trip Wire for a Camera