CONTENTS

Preface iii

Audience iii

Document Organization iv

Document Conventions v

List of Acronyms and Abbreviations v

Cisco DNA Spaces Prerequisites 1-1

System Requirements 1-1

Bandwidth Requirements to Deploy Cisco DNA Spaces 1-2

Accessible Ports and IP Addresses 1-4

Allow Cisco DNA Spaces IP Addresses 1-4

Cisco DNA Spaces Compatibility Matrix 1-5

Getting Started 2-1

Overview of Cisco DNA Spaces 2-1

Cisco DNA Spaces Dashboard 2-2

Cisco DNA Spaces Features 2-3

Digitization Stats 2-3

My Apps 2-4

Location Hierarchy 2-6

Monitoring and Support 2-6

Team 2-6

Setup 2-6

Wireless Network Status 2-6

Cisco DNA Spaces License Packages 2-7

Process Flow for Cisco DNA Spaces 2-7

Start Working with Cisco DNA Spaces 2-7

Location Hierarchy in Cisco DNA Spaces 3-1

Overview of Location Hierarchy 3-1

Prerequisites for Defining the Location Hierarchy 3-2
Contents

Report Tabs 4-3
Behavior Metrics (Business Metrics) 4-4
Performance Benchmarking: Performance on Core Metrics related to Peers 4-4
Visit Duration 4-4
Visit Frequency 4-4
Diagnostics: Factors that Impact or are impacted by the Core Metrics 4-5
WiFi Adoption 4-7
Right Now 4-8
Pin a Location 4-9

Working with the Captive Portal App 4-1
Creating and Managing Portal 4-1
Prerequisites for Creating a Portal 4-2
Sample Portals 4-2
Creating a Portal 4-3
Portal Modules 4-5
Configuring a Language for a Portal 4-6
Configuring Authentication for a Portal 4-9
Authentication Module 4-15
Adding a Data Capture Form to a Portal 4-15
Defining a Brand Name for a Portal 4-16
Adding a Welcome Message to a Portal 4-17
Adding a Notice to a Portal 4-18
Providing the Venue Details in a Portal 4-18
Uploading Videos to a Portal 4-19
Providing a Feedback Section in a Portal 4-21
Adding a Help Option to a Portal 4-22
Adding Apps to a Portal 4-23
Providing Access to the Internet from a Portal 4-24
Adding Promotions and Offers to a Portal 4-24
Deleting a Promotion and an Offer for a Portal 4-25
Adding Custom Content and Menu Items to a Portal 4-26
Exporting a Portal 4-27
Editing the Portal Style Sheet 4-27
Importing a Portal 4-28
Deleting a Portal 4-29
Editing a Portal 4-29
Editing the Locations for a Portal 4-30
E-mailing a Portal Preview URL 4-30
Previewing a Portal Using QR Code 4-30
Contents

4-31

Previewing a Portal

Previewing the Portal in Various Devices 4-31

Display, Hide or Reorder the Modules in a Captive Portal 4-32

Captive Portal Rule 4-32

Prerequisites for Creating a Captive Portal Rule 4-32

Creating a Captive Portal Rule to Display Captive Portals 4-33

Use Case: Captive Portal Rule 4-37

Reports 4-38

Device Onboarding 4-38

Customer Acquisition 4-39

SSIDs 4-41

Prerequisites for Importing or Configuring the SSIDs 4-41

Importing the SSIDs from a Wireless Network 4-41

Importing the SSIDs for Cisco Unified Wireless Network 4-42

Importing the SSIDs for Cisco Meraki 4-42

Social Authentication for Portals 4-44

Configuring the Wireless Network for Social Authentication 4-44

Configuring the Apps for Social Authentication 4-45

Adding Social Apps for Social Authentication 4-46

Configuring an SMS Gateway in Cisco DNA Spaces 4-46

Managing Captive Portal Rules 4-47

Certified Device List for Portals 4-51

Cisco DNA Spaces Captive Portal Behavior 4-52

Apple iOS 7.x to 11.x 4-53

Android 5.x and Later (Using CNA) 4-53

Android 4.x and Earlier 4-54

Windows Phone 4-55

Windows PCs and Laptops 4-55

Macbook 4-56

Authentication Steps for Customers 4-57

Authentication Steps for No Authentication with Terms and Conditions 4-57

Authentication Through SMS with Link Verification 4-57

Authentication Through SMS with Password Verification 4-59

Authentication Through E-mail 4-61

Authentication Steps for Social Authentication 4-62

Smart Links and Text Variables 4-63

4-65
Sending Notifications with the Engagements App 5-1
  Prerequisites for Creating an Engagement Rule 5-1
  Creating an Engagement Rule 5-2
    Creating an Engagement Rule for a Consumer 5-2
  Use Case: Engagement Rule for Customers 5-4
    Creating an Engagement Rule for a Business User 5-6
  Use Case: Engagement Rule for a Business User 5-8
Managing Engagement Rules 5-9
  Pausing an Engagement Rule 5-9
  Restarting an Engagement Rule 5-10
  Modifying an Engagement Rule 5-10
  Deleting an Engagement Rule 5-11
  Viewing an Engagement Rule for a Location 5-11
  Engagement Rule Report 5-11
    Rule Activity 5-12
    User Insight 5-12
Creating Tags with the Location Personas App 6-1
  Creating or Modifying Tags Using a Location Persona App 6-1
  Use Case: Profile Rule (Location Personas Rule) 6-3
Managing Location Personas Rules 6-7
  Pausing a Location Personas Rule 6-7
  Restarting a Location Personas Rule 6-7
  Modifying a Location Personas Rule 6-8
  Deleting a Location Personas Rule 6-8
  Viewing a Location Personas Rule for a Location 6-8
  Location Personas Rule Report 6-9
    Rule Activity 6-9
    User Insights 6-10
Working with the Cisco DNA Spaces Operation Insights App 7-1
  7-1
  Monitoring and Support 8-1
    Monitoring 8-1
      App Latency 8-3
      Enterprise Apps 8-3
      Partner Apps 8-4
    Support 8-4
      Ticket Status 8-4
Contents

Tickets 8-4

Managing Cisco DNA Spaces Users and Accounts 9-1
  Managing Cisco DNA Spaces Users 9-1
    Inviting a Cisco DNA Spaces User 9-1
    Editing User Privileges 9-2
    Deleting a Cisco DNA Spaces User 9-3
  Managing the Cisco DNA Spaces Accounts 9-3
    Changing the Cisco DNA Spaces Password 9-3
    Signing Out of Cisco DNA Spaces 9-4

Setup Wireless Network 10-1
  Setting Up Cisco DNA Spaces to Work with Various Wireless Networks 10-1

Configuring Cisco Unified Wireless Network (Cisco AireOS) for Cisco DNA Spaces 11-1
  Configurations for the CMX On Prem Option to work with Cisco DNA Spaces 11-2
    Configuring Access Point Mode, SSIDs, ACLs, Splash URLs, and Virtual Interface in the WLC 11-2
    Configuring Cisco Unified Wireless Network for Internet Provisioning and RADIUS Authentication 11-11
    Configuring Cisco Unified Wireless Network for Notifications and Reports 11-13
    Configuring Cisco CMX for Notification and Reports Using CMX Tethering (For Cisco CMX 10.6 or later) 11-15
    Configuring the Cisco Unified Wireless Network for Social Authentication 11-17
  Configurations for the WLC Direct Connect Option to work with Cisco DNA Spaces 11-17
    Connecting Cisco Wireless Controller to Cisco DNA Spaces Using Wireless Controller Cloud Connect 11-18
    Configuring Mobility Express to work with Cisco DNA Spaces 11-20
      Configuring Mobility Express 8.7 or Later for Cisco DNA Spaces 11-21
      Configuring Mobility Express 8.6 or Earlier for Cisco DNA Spaces 11-25
    Configuring eWLC to work with Cisco DNA Spaces 11-26
    Configuring eWLC(GUI) to work with Cisco DNA Spaces 11-30
  11-36

Configuring Cisco Meraki for Cisco DNA Spaces 12-1
  Enabling SSIDs in Cisco Meraki 12-1
    Configuring Cisco Meraki for RADIUS Authentication 12-2
      Configuring Cisco Meraki for RADIUS Authentication (Without Seamless Internet Configurations) 12-2
      Configuring Cisco Meraki for RADIUS Authentication and Seamless Internet Provisioning 12-3
Configuring Cisco Meraki for Notifications and Reports  12-4
Configurations Required in Cisco Meraki for Location Manager  12-4
Configuring Cisco Meraki for Social Authentication  12-5
Manually Configuring SSIDs for Cisco Meraki  12-5
Preface

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

- Audience, page iii
- Document Organization, page iv
- Document Conventions, page v
- List of Acronyms and Abbreviations, 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 1</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 4</td>
<td>Behavior Metrics</td>
<td>Provides information about Behavior Metrics reports.</td>
</tr>
<tr>
<td>Chapter 5</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 6</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 7</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 8</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 9</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 10</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 11</td>
<td>Configuring Cisco Unified Wireless Network (Cisco AireOS) for Cisco DNA Spaces</td>
<td>Describes the configurations required in the Cisco Unified Wireless Network (CUWN) to use Cisco DNA Spaces.</td>
</tr>
<tr>
<td>Chapter 12</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

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Boldface</strong></td>
<td>Commands, command options, and keywords are in <strong>boldface</strong>.</td>
</tr>
<tr>
<td><em>Italics</em></td>
<td>Arguments for which you supply values are in <em>italics</em>.</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>
<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, page 1-1
- Bandwidth Requirements to Deploy Cisco DNA Spaces, page 1-2
- Accessible Ports and IP Addresses, page 1-4

System Requirements

Before installing Cisco DNA Spaces, ensure that all of the following system requirements are met.

<table>
<thead>
<tr>
<th>Item</th>
<th>Supported 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>• Internet Explorer Version 9 or later</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>Mac OS</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 (only for Cisco Unified Wireless Network)</td>
<td>8.3 or later</td>
</tr>
<tr>
<td>Cisco Connected Mobile Experiences (CMX) - this is required only for Cisco Unified Wireless Network used with Cisco CMX.</td>
<td>10.0 or later</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 Cloud Connect to send location updates.

Table 1-2  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 Cloud 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 1-3  Bandwidth Requirements for Captive Portals

<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>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>
</tbody>
</table>
### Table 1-3  Bandwidth Requirements for Captive Portals

<table>
<thead>
<tr>
<th>Bandwidth</th>
<th>Number of Users</th>
<th>Response (In Seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>5Mbps</td>
<td>5</td>
<td>9.34</td>
</tr>
<tr>
<td>10</td>
<td>11.56</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>11.92</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>11.51</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>12.5</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>13.82</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>13.18</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>14.91</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>16.72</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>15.96</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>16.98</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>17.41</td>
<td></td>
</tr>
<tr>
<td>7Mbps</td>
<td>25</td>
<td>13.93</td>
</tr>
<tr>
<td>30</td>
<td>15.41</td>
<td></td>
</tr>
<tr>
<td>31</td>
<td>15.21</td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>15.64</td>
<td></td>
</tr>
<tr>
<td>33</td>
<td>16.31</td>
<td></td>
</tr>
<tr>
<td>34</td>
<td>18.92</td>
<td></td>
</tr>
<tr>
<td>9Mbps</td>
<td>30</td>
<td>10.56</td>
</tr>
<tr>
<td>35</td>
<td>12.11</td>
<td></td>
</tr>
<tr>
<td>40</td>
<td>14.79</td>
<td></td>
</tr>
<tr>
<td>41</td>
<td>14.7</td>
<td></td>
</tr>
<tr>
<td>42</td>
<td>13.27</td>
<td></td>
</tr>
<tr>
<td>43</td>
<td>13.93</td>
<td></td>
</tr>
<tr>
<td>44</td>
<td>15.68</td>
<td></td>
</tr>
<tr>
<td>45</td>
<td>16.81</td>
<td></td>
</tr>
<tr>
<td>46</td>
<td>16.13</td>
<td></td>
</tr>
<tr>
<td>47</td>
<td>19.25</td>
<td></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 Unified Wireless Network (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, page 1-4. 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.

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.

<table>
<thead>
<tr>
<th>Bandwidth</th>
<th>Number of Users</th>
<th>Response (In Seconds)</th>
</tr>
</thead>
<tbody>
<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>
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>
<thead>
<tr>
<th>Application</th>
<th>3504, 5520, 8500</th>
<th>eWLC</th>
<th>Mobility Express</th>
<th>3375 Appliance</th>
<th>Cisco Prime/ Cisco DNA Center</th>
</tr>
</thead>
</table>
| Cisco DNA Spaces (with Presence, Captive Portal, Engagements, Location Personas, Behavior Metrics) | - Cisco Wireless Controller Cloud Connector or- 8.3 or later (except 8.3.102 for Presence)  
- Cisco DNA Spaces Connector or- 8.0.119 or later  
- Cisco Wireless Controller 8.0 or later with Cisco CMX 10.0 or later | 16.10 or later | 1832 model with software version 8.5.135 | NA | 3.0 or later |
Getting 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, page 2-1
- Cisco DNA Spaces Dashboard, page 2-2
- Cisco DNA Spaces Features, page 2-3
- Process Flow for Cisco DNA Spaces, page 2-7
- Cisco DNA Spaces License Packages, page 2-7
- Start Working with Cisco DNA Spaces, page 2-7

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.
Cisco DNA Spaces Dashboard

- App to log in to BLE Manager.
- 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 push notifications, BLE notifications, 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 or BLE beacon, 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 Figure 2-1.
Cisco DNA Spaces Features

The major features of Cisco DNA Spaces includes:

- **Digitization Stats**, page 2-3
- **My Apps**, page 2-4
  - Captive Portal App, page 2-4
  - Engagements App, page 2-4
  - Profile Rules App, page 2-5
  - Behavior Metrics App, page 2-5
  - BLE Manager App, page 2-5
  - Operational Insights App, page 2-5
  - Partner Apps, page 2-5
- **Location Hierarchy**, page 2-6
- **Monitoring and Support**, page 2-6
- **Team**, page 2-6
- **Setup**
- **Wireless Network Status**, page 2-6

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 square foot area in your business locations that are covered by Cisco DNA Spaces.
- **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.

**Note**

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.
My 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, page 2-4
- Engagements App, page 2-4
- Profile Rules App, page 2-5
- Behavior Metrics App, page 2-5
- BLE Manager App, page 2-5
- Operational Insights App, page 2-5
- Partner Apps, page 2-5

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 on page 4-1.

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 on page 4-32.

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 beacon functionality 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 or when a customer is with in a beacon premises.

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

- SMS
- E-mail
- Push notifications using apps
- BLE Notifications
- API notifications
- Cisco Webex Teams

For more information, see the “Creating an Engagement Rule” section on page 5-2.

Profile Rules App

Cisco DNA Spaces enables you create tags by grouping the customers. You can create the tags using the Profile Rule. You can also use the Profile rule 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 Persona App” section on page 6-1.

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 on page 4-1.

BLE Manager App

The BLE Manager app enables you to detect and monitor the Cisco APs integrated with BLE, and other Beacons in your wireless network. BLE Manager is available only for CUWN. Currently, you must have a BLE Manager account to access this app.

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 in your wireless network. The apps such as Engagements, Captive Portals, and Profile 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 on page 3-1.

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. The Support section enables you to view the tickets raised by your customers. For more information, see the “Monitoring and Support” section on page 8-1.

Team

The Team feature enables you to create Cisco DNA Spaces users. You can restrict the privileges and locations for each user based on their role. For more information, see the “Managing Cisco DNA Spaces Users and Accounts” section on page 9-1.

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, page 10-1.

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. You can also add Cisco DNA Spaces connector through this option.
Cisco DNA Spaces License Packages

Cisco DNA Spaces is available in two different license packages namely, **Base** and **Advance**. The features available for your account depends on the type of Cisco DNA Spaces license package you own.

Process Flow for Cisco DNA Spaces

The process flow for Cisco DNA Spaces is as shown in Figure 2-2.

**Note**

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 an **Account 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.

**Step 2** Follow the instructions provided in the **Cisco DNA Spaces Setup Guide** that appears to connect Cisco DNA Spaces to your wireless network.

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

- **Cisco Meraki**
For configuring a Cisco Meraki network, see the “Configuring Cisco Meraki for Cisco DNA Spaces” section on page 12-1.

- **Cisco Unified Wireless Network with Cisco CMX**

  For configuring a Cisco Unified Wireless Network with Cisco CMX, see the “Configurations for the CMX On Prem Option to work with Cisco DNA Spaces” section on page 11-2.

- **Cisco Unified Wireless Network with Cisco Wireless Controller (without a Cisco CMX Connection)**
  - **Using Cisco DNA Spaces Connector**—For configuring a Cisco Unified Wireless Network with Cisco Wireless Controller using Cisco DNA Spaces Connector, see the Cisco DNA Spaces Connector Configuration Guide.
  - **Using Mobility Express**—For configuring a Cisco Unified Wireless Network using Mobility Express, see the “Configuring Mobility Express to work with Cisco DNA Spaces” section on page 11-20.
  - **Using eWLC**—For configuring a Cisco Unified Wireless Network using eWLC, see the “Configuring eWLC(GUI) to work with Cisco DNA Spaces” section on page 11-30.

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 on page 9-1.

**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 on page 3-1.

**Step 5**
Import SSIDs to Cisco DNA Spaces. For more information on importing the SSIDs, see the “SSIDs” section on page 4-41.

**Step 6**
Define Profile Rules (Location Persona Rules) to tag customers. For more information on creating a Profile Rule, see the “Creating or Modifying Tags Using a Location Persona App” section on page 6-1.

**Step 7**
Configure supporting features such as SMS Gateways, Apps, BLE Beacons, and so on. Refer to the respective topic in this guide for configuration.

**Step 8**
Create Captive Portals. For more information on creating the captive portals, see the “Creating and Managing Portal” section on page 4-1.

**Step 9**
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 on page 4-32.

**Step 10**
Create Engagement Rules to send appropriate notifications to the customers. For more information on creating Engagement Rules, see the “Creating an Engagement Rule” section on page 5-2.

**Step 11**
Analyze the Cisco DNA Spaces performance, and your business performance using Business Metrics. For more information on Business Metrics, see the “Overview of Behavior Metrics” section on page 4-1.

**Step 12**
Monitor the Cisco DNA Spaces domain and apps using the Monitoring and Support section.
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, page 3-1
- Prerequisites for Defining the Location Hierarchy, page 3-2
- Defining the Location Hierarchy, page 3-2
- Managing the Location Hierarchy, page 3-16
- Defining or Editing Metadata for a Location, page 3-24
- Defining or Changing the Time Zone for Locations, page 3-25
- Wireless Network Synchronization, page 3-26
- Managing the Maps for a Location, page 3-26
- Managing the Access Points, page 3-28
- Managing the Groups, page 3-29
- Managing the Zones, page 3-31
- Displaying Cumulative Count in Location Hierarchy, page 3-32

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 Unified Wireless Network (Cisco AireOS or Cisco Catalyst) 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. You can import the locations in the same structure in which they are defined in Cisco Unified Wireless Network or Cisco Meraki. For Cisco Unified Wireless Network, you can use Cisco DNA Spaces even without installing the Cisco CMX. However, this option will be having certain restrictions for the location hierarchy structure.

As Cisco DNA Spaces provides universal account, you can import and manage the locations of both Cisco Unified Wireless Network and Cisco Meraki. However, the wireless network specified when creating your customer account will be your base network. A proximity rule can include the locations of both Cisco Unified Wireless Network and Cisco Meraki.
You can create proximity rules such as captive portal rule, engagement rule, and profile rule, and view access points, BLE beacons, users, and child locations for any location in the location hierarchy. The number of access points, BLE beacons, 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 provider system such as Cisco Meraki or Cisco Unified Wireless Network. In addition, you must establish connection between Cisco DNA Spaces and your wireless network. When you try to add a wireless network in the location hierarchy, Cisco DNA Spaces asks you to provide the login credentials to connect to that wireless network. For the Cisco CUWN-WLC option, it is only required to ensure that the required access points are configured in the Cisco Wireless Controller.

Defining the Location Hierarchy

Cisco DNA Spaces supports the following wireless networks:

- **Cisco Meraki**—If your wireless network is Cisco Meraki, you can define the location hierarchy using the Cisco Meraki option.

- **Cisco Unified Wireless Network with Cisco CMX**—If your wireless Network is Cisco Unified Wireless Network and if you are having a Cisco CMX installed, you can define the location hierarchy using the CMX On Prem option.

- **Cisco Unified Wireless Network with Cisco Wireless Controller**—You can use Cisco DNA Spaces with Cisco Unified Wireless Network even if you don’t have installed the Cisco CMX. If your wireless Network is Cisco Unified Wireless Network, and if you are not having the Cisco CMX installed, you can define the location hierarchy using the WLC Direct Connect option.

**Note** For the WLC Direct Connect option, you can ensure that appropriate data transfer happens between Cisco Wireless 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, page 3-3
- Defining the Location Hierarchy for Cisco Unified Wireless Network with Cisco CMX, page 3-6
- Defining the Location Hierarchy for Cisco Unified Wireless Network with Wireless Controller (without Cisco CMX Installation), page 3-9
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, page 3-2.

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 Figure 3-1.

![Location Hierarchy](image)

You must have Cisco Meraki credentials to import the locations. 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 the “Importing Meraki Locations Using the API Keys” section on page 3-5.

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

1. Adding a Cisco Meraki Organization, page 3-3
2. Adding a Network to Cisco Meraki Organization, page 3-4
3. Creating Zones and Adding Access Points, page 3-4

**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.
To add a Cisco Meraki Organization 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 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 Meraki.

**Step 5** Enter the user name and password for your Meraki account, and click Connect account.

**Note** You can also connect to Meraki using the Wi-Fi icon in the left pane of the dashboard. If you are already connected to Meraki, the fields to enter the login credentials will not appear.

**Step 6** From the Organization drop-down list, choose the Cisco Meraki Organization from which you want to import the locations.

**Step 7** Click Add.

The organization that is added gets listed in the location hierarchy.

### 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 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 Meraki, 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.
Chapter 3  Location Hierarchy in Cisco DNA Spaces

Defining the Location Hierarchy

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 icon 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 Enter Zone Name Here 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.

Tip
Before creating the zones, locate the access points that you want to include in the zone in the Meraki dashboard.

Note
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 Meraki Locations Using the API Keys

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

Step 1
In the Locations 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 Meraki.

Step 3
Click the Import Organization using API link that appears when you select 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 Unified Wireless Network with Cisco CMX

If you have the Cisco CMX installed, you can use the Cisco CUWN - CMX option for defining the location hierarchy for Cisco Unified Wireless Network. The Cisco CUWN - CMX option enables you to import the locations in the same hierarchy in which you have defined them in the Cisco CMX. Initially, you must add CMX nodes to the location hierarchy under the customer name. You can then import campuses. When you import a campus, its buildings, floors, and access points are also imported. You can create zones at building or floor level by grouping the access points. You can group the locations at customer name (root name), CMX node, or campus level. You can also rename the customer name.

Note

The Cisco Wireless Controller must be able to reach Cisco DNA Spaces cloud over HTTPS.

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, page 3-2.

The location hierarchy for Cisco Unified Wireless Network with a Cisco CMX installation is as follows:

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

The location hierarchy of the Cisco Unified Wireless Network - CMX is shown in Figure 3-2.

Figure 3-2 Location Hierarchy

To create the location hierarchy for the Cisco CUWN - CMX option, perform the following steps:

1. Adding a CMX Node, page 3-7
2. Adding a Campus to the Location Hierarchy, page 3-7
3. Creating Zones and Adding Access Points, page 3-8
4. Creating Groups, page 3-29

If your Cisco CMX is not publicly accessible, you can manually import the locations. For more information on manually importing the locations, see the Creating the Location Hierarchy by Manually Uploading the Cisco CMX Details, page 3-8.
Chapter 3  Location Hierarchy in Cisco DNA Spaces

Defining the Location Hierarchy

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 CMX Node

Note
Cisco DNA Spaces supports CMX 10.0 or later.

To add a CMX node 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 More Actions at the far right of the customer name (root name).

Step 3
Choose Add a Wireless Network.

Step 4
From the Add a Wireless Network drop-down list that appears, choose Cisco CUWN - CMX.

Step 5
In the Display Name field, enter the name that must display for the CMX node in the location hierarchy.

Step 6
In the URL field, enter the URL to connect to Cisco CMX.

Step 7
In the User Name field, enter the user name to connect to Cisco CMX.

Step 8
In the Password field, enter the password to connect to Cisco CMX.

Step 9
Click Add.

The CMX node appears in the location hierarchy under the customer name.

Note
Cisco DNA Spaces will not allow you to add two CMX nodes with the same access point.

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:

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 CMX node for which you want to add the campus.

Step 3
Click Add Campus.

Step 4
In the Add Campus window that appears, select the campuses that you want to add to the location hierarchy.
The Add Campus window appears with all the available campuses for that CMX node. If you select a campus, its buildings and floors appears to the right of the campus.

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, page 3-18. For more information on adding a floor to a building, see the Adding a Floor to a Building, page 3-18.

Step 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.

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 Enter Zone Name Here 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.

Note 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.

Creating the Location Hierarchy by Manually Uploading the Cisco CMX Details

If you want to use the location hierarchy of a Cisco CMX that is not publicly accessible, you can import the location hierarchy to Cisco DNA Spaces by uploading the JSON file that contains the location hierarchy details.
For a location hierarchy created using the JSON file, you can rename and delete the locations such as building, floor, and so on, but you cannot edit the locations. You can create groups and zones in the location hierarchy.

**Note**
As this method has many limitations, we recommend you to use this option only if you cannot connect to the Cisco CMX from the Cisco DNA Spaces dashboard.

**Note**
As the wireless network information required for access point synchronization is not available, the access point synchronization will not happen if the locations are added to the location hierarchy using the JSON file. So after importing the JSON file if you make changes in the wireless network for the locations, those changes will not reflect in the location hierarchy.

To create a location hierarchy using a JSON file, perform the following steps:

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

**Step 2**
In the **Locations** window, click **More Actions** at the far right of the customer name.

**Step 3**
Click **Add Wireless Network**.

**Step 4**
From the **Add Wireless Network** drop-down list, choose **Cisco CUWN - CMX**.

**Step 5**
Select **Upload JSON**.

**Step 6**
Enter the name that must be displayed for the CMX node in the location hierarchy.

**Step 7**
Select the JSON file to upload using the **Browse** button.

**Step 8**
Click **Upload**.

The JSON file is uploaded and the location hierarchy is created for the Cisco CMX in the Cisco DNA Spaces dashboard.

**Note**
After uploading the JSON file, to update the location hierarchy, you must delete the location hierarchy manually, and then re-import the JSON file with new location details.

### Creating the JSON File for Locations

Create the JSON file for locations with following curl command:

```
curl -u 'userName:Password@123#' https://CMXPublicIP/api/config/v1/maps--insecuremseoutput.json
```

### Defining the Location Hierarchy for Cisco Unified Wireless Network with Wireless Controller (without Cisco CMX Installation)

You can use Cisco DNA Spaces with Cisco Unified Wireless Network, even without installing Cisco CMX. In such cases, you must use the **Cisco CUWN -WLC** option. However, for the **Cisco CUWN -WLC** option, you can add only networks, groups, and zones in the location hierarchy.
Defining the Location Hierarchy

Note If you were using Cisco DNA Spaces earlier with Cisco CMX, and if you are moving to use Cisco DNA Spaces 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.

To avail the Cisco CUWN -WLC option, you must configure the Cisco Wireless Controller to import the access points to the Cisco DNA Spaces dashboard. For more information on configuring the Cisco Wireless Controller for importing the access points to the Cisco DNA Spaces dashboard, see the Configurations for the WLC Direct Connect Option to work with Cisco DNA Spaces, page 11-17.

For Cisco Unified Wireless Network, to use Cisco DNA Spaces with Cisco Wireless Controller without a Cisco CMX installation, create the location hierarchy as following.

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 customer name.

Step 3 Click Add Wireless Network.

Step 4 From the Wireless Network drop-down list, choose Cisco CUWN -WLC.

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. For more information on configuring the Cisco Wireless Controller, see the “Configurations for the WLC Direct Connect Option to work with Cisco DNA Spaces” section on page 11-17.

Step 5 Select the Cisco Wireless Controller, and click Next.

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

Step 6 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 7 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 8 Click Done.

The APs of the primary and secondary controllers selected will get listed in the location hierarchy.
Step 9  In the location hierarchy, click the More Actions icon at the far right of the network, and click Add Zone.

Step 10 In the window that appears, enter a name for the zone, and select the APs to be included in the zone.

Step 11 Similarly, create all the required zones.

Tip If you are an existing Cisco CUWN - CMX user, create zones in the same structure as created earlier with the Cisco CMX.

Step 12 If you already have created the location hierarchy using the Cisco CMX earlier, delete that location hierarchy, and re-configure the proximity rules.

You can change the primary controller, and add more secondary controllers. For more information, see the “Managing the Cisco Wireless Controller and Access Points” section on page 3-11.

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

Note • 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.

Managing the Cisco Wireless Controller and Access Points

• Changing the Primary Controller, page 3-12
• Adding Additional Secondary Controller, page 3-12
• Adding Networks Automatically for a Primary Controller, page 3-13
• Manually Adding Networks for a Cisco Wireless Controller, page 3-13
• Creating Groups for a Cisco Wireless Controller, page 3-13
• Adding Metadata for a Cisco Wireless Controller or Network, page 3-14
• Renaming the Primary Controller, page 3-14
• Renaming a Network, page 3-15
• Deleting a Cisco Wireless Controller, page 3-15
• Deleting a Network, page 3-15
• Deleting a Secondary Cisco Wireless Controller, page 3-16
Changing the Primary Controller

To change the primary 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 that you want to change.
Step 3  Click **Edit**.
Step 4  In the **Edit Controller** window that appears, click **Change** for “Primary Controller”.
Step 5  In the **Change Primary Controller** window that appears, select the Cisco Wireless Controller that you want to configure as the Primary controller.
Step 6  Click **Change**.

Now the newly configured Cisco Wireless Controller has become the Primary Controller.

---

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.
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, 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, choose Location Hierarchy.</td>
</tr>
<tr>
<td>Step 2</td>
<td>In the Location Hierarchy window, click the More Actions icon for the Cisco Wireless Controller for which you want to add networks.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click Edit.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the Edit Controller window that appears, select the “Auto Network Creation” check box.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click Done.</td>
</tr>
</tbody>
</table>

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”.

Note
Only the APs added to the Cisco 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 Cisco 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 Cisco Wireless Controller

To manually add network for a Cisco Wireless Controller, 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, choose Location Hierarchy.</td>
</tr>
<tr>
<td>Step 2</td>
<td>In the Location Hierarchy window, click the More Actions icon for the Cisco Wireless Controller for which you want to define the network.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click Add Network.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the Network Name field that appears, enter a name for the network.</td>
</tr>
<tr>
<td>Step 5</td>
<td>In the Access Point prefix field that appears, enter the prefix the APs must have to group under the network, and click Fetch.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Click Done.</td>
</tr>
</tbody>
</table>

The network will be created with the APs having the prefix mentioned.

Creating Groups for a Cisco Wireless Controller

You can create groups under a Cisco Wireless Controller by grouping the networks.
To create a group 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 under which you want to create group.

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

**Step 4** In the **Add Group** window that appears, enter the following:

- In the **Enter a Group Name** field, enter a name for the group.
- In the **Select Location** area, select the networks that you want to add under this group.
- Click **Add**.

Now a group is created with the networks specified.

### Adding Metadata for a Cisco Wireless Controller or Network

You can group the Cisco Wireless Controllers and networks using metadata. You can use this metadata when defining the proximity rules.

To add a metadata for a Cisco Wireless Controller/network, 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 or network for which you want to add metadata.

**Step 3** Click **Add/Edit Metadata**.

**Step 4** In the **Add Metadata for [WLC controller/network]** window that appears, perform the following steps:

- In the **Key** field, enter a metadata key.
- In the **value** field, enter a value for the key.
- Click **Save**.

**Note** Similarly, add the metadata for other Cisco Wireless Controllers that must have this metadata.

### 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.

---

### Renaming a Network

To rename a network, 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 network that you want to rename.
- **Step 3**  Click **Rename [network]**.
- **Step 4**  In the **Rename network** window that appears, enter the name required, and click **Rename**.
Now the name of the network is changed to the new name specified.

---

### Deleting a Cisco Wireless Controller

To delete 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, click the **More Actions** icon for the Cisco Wireless Controller that you want to delete.
- **Step 3**  Click **Delete wlc**.
- **Step 4**  In the **Delete wlc** window that appears, confirm the deletion.
Now the Cisco Wireless Controller is deleted from Cisco DNA Spaces.

---

**Note**  You cannot delete a Cisco Wireless Controller that has networks or access points under it. Also, you cannot delete a Cisco Wireless Controller that is associated with a proximity rule.

---

### Deleting a Network

To delete a network, 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 network that you want to delete.
- **Step 3**  Click **Delete network**.
- **Step 4**  In the **Delete network** window that appears, confirm the deletion.
Deleting a Secondary Cisco Wireless Controller

To delete a secondary Cisco Wireless 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 of which you want to delete the secondary Cisco Wireless Controller.

**Step 3** Click **Edit**.

In the **Edit Controller** window that appears, the secondary controllers added for that Cisco Wireless Controller will be listed under “Additional Controllers”.

**Step 4** Click the **Delete** icon for the secondary controller that you want to delete.

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

Now, the secondary controller is deleted.

Note When you delete a secondary Cisco Wireless 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.

Managing the Location Hierarchy

- Renaming a Customer, page 3-16
- Adding a Wireless Network, page 3-17
- Defining or Editing Metadata for a Location, page 3-24
- Searching for an Access Point, page 3-17
- Managing the Location Hierarchy for Cisco Unified Wireless Network, page 3-18
- Managing the Location Hierarchy for Meraki, page 3-22

Renaming a Customer

To rename a customer, 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 customer name.
Step 3  Click **Rename** [root name].

Step 4  In the **Rename root** window that appears, enter the customer name you want.

Step 5  Click **Rename**.

### Adding a Wireless Network

Cisco DNA Spaces supports both Cisco Unified Wireless Network and Meraki. You can add both CMX nodes and Cisco Meraki Organizations using the Add a Wireless network option.

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

- **Meraki**—To define the location hierarchy for Meraki network.
- **Cisco CUWN - CMX**—To define the location hierarchy for the Cisco Unified Wireless Network, when the Cisco CMX is installed.
- **Cisco CUWN -WLC**—To define the location hierarchy for the Cisco Unified Wireless Network, when the Cisco CMX is not installed.

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 the respective topic from the following:

- **Adding a CMX Node**, page 3-7
- **Adding a Cisco Meraki Organization**, page 3-3
- **Defining the Location Hierarchy for Cisco Unified Wireless Network with Wireless Controller (without Cisco CMX Installation)**, page 3-9

### 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.
Managing the Location Hierarchy

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 Location Hierarchy for Cisco Unified Wireless Network

- Adding a Building to a Campus, page 3-18
- Adding a Floor to a Building, page 3-18
- Renaming a CMX Node, page 3-19
- Editing a CMX Node, page 3-19
- Deleting a CMX Node, page 3-19
- Renaming a Campus, page 3-20
- Deleting a Campus, page 3-20
- Renaming a Building, page 3-20
- Deleting a Building, page 3-21
- Renaming a Floor, page 3-21
- Deleting a Floor, page 3-21

Adding a Building to a Campus

To add a building to a campus, 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 campus to which you want to add the building.
Step 3 Click Add Building.
Step 4 In the Add Building window that appears, select the building that you want to add under the campus.
Step 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 “cmx name”.
Step 4  In the window that appears, enter the new name for the CMX node.
Step 5  Click Rename.

Note  The renaming is not reflected in the Cisco CMX.

Editing a CMX Node

You can edit the Cisco CMX connection credentials.
To edit 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 edit.
Step 3  Click the option to edit the CMX node.
Step 4  In the window that appears, provide the updated Cisco CMX log in credentials for the CMX node.
Step 5  Click Edit.

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.
Managing the Location Hierarchy

Step 3  Click the option to delete the CMX node.

Note  To delete a CMX node, first you have to delete the locations and groups under that CMX node, if any.

Note  You cannot delete a CMX node that is associated with the proximity rules.

Renaming a Campus

To rename a campus, perform the following steps:

Step 1  In the Cisco DNA Spaces dashboard, choose 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.

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

Step 3  Click Delete campus.

Note  To delete a campus, first you have to delete the locations under that campus, if any.

Note  You cannot delete a campus that is associated with proximity rules.

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 More Actions 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.

---

**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.

**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.
Managing 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.

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.

Managing the Location Hierarchy for Meraki

You can rename, and delete the locations under Meraki.

- Adding Floors to a Network, page 3-22
- Renaming an Cisco Meraki Organization, page 3-22
- Deleting a Cisco Meraki Organization, page 3-23
- Renaming a Network, page 3-23
- Deleting a Network, page 3-23
- Renaming a Floor, page 3-21
- Deleting a Floor, page 3-21

Adding Floors to a Network

To add a floor to a network, 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 network under which you want to create the floor.

Step 3 In the Add Floor window that appears, select the floor that you want to add under the network.

Step 4 Click Add.

The floor gets added to the network.

Renaming an Cisco Meraki Organization

To rename 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 organization that you want to rename.

Step 3 Click Rename “Organization Name”.

Step 4 In the Rename -meraki window that appears, enter the new name for the Cisco Meraki Organization.
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.

**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.
Defining or Editing Metadata for a Location

Cisco DNA Spaces enables you to define metadata for a location using variables. You can define the metadata at any level in the location hierarchy. You can use this metadata for filtering the locations when creating the proximity rules. For example, if you want to categorize your locations as corporate branch, division branch, and local branch, then you can define a location metadata with key as Branch and values as CB, DB, and LB, respectively. Then, you can use this metadata to filter the locations when creating the proximity rules.
To define a metadata for a location, perform the following steps:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In the Cisco DNA Spaces dashboard, click Location Hierarchy.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>In the Location Hierarchy window, click More Actions at the far right of the location for which you want to add the location metadata.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click Add/Edit Metadata.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the Add Metadata for [location] window that appears, perform the following steps:</td>
</tr>
<tr>
<td></td>
<td>a. Click the + button.</td>
</tr>
<tr>
<td></td>
<td>b. In the Key field, enter a name for the variable key.</td>
</tr>
<tr>
<td></td>
<td>c. In the Value field, enter a value for the variable key.</td>
</tr>
<tr>
<td></td>
<td>d. Click Save.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In the Location Hierarchy window, click More Actions at the far right of the location for which you want to update the location metadata.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Click Add/Edit Metadata.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the Add Metadata for [location] window that appears, click the metadata that you want to update.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Make necessary changes, and click Update.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>In the Cisco DNA Spaces dashboard, choose Location Hierarchy.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>In the Location Hierarchy window, click More Actions for the location for which you want to define the time zone.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click Time Zone.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Step 4</td>
<td>From the Select Timezone drop-down list, choose the time zone that you want to configure for this location.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click Change.</td>
</tr>
</tbody>
</table>
The time zone is defined for the location.

---

**Note**

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

---

**Wireless Network Synchronization**

To know the synchronization status of the locations, perform the following steps:

**Step 1**
In the Cisco DNA Spaces dashboard, click the Wi-Fi icon at the top-right.

**Step 2**
Click *Wireless Network Status*.

**Step 3**
Click the wireless network of which you want to see the synchronization status. For example, to view the synchronization status for Meraki, click *Meraki*.

The synchronization status is displayed.

---

**Managing the Maps for a Location**

The maps are displayed by default based on the map configuration in the wireless network. Cisco DNA Spaces enables you to display the Micello map for the floors and zones. Also, you can upload external maps for the floors and zones.

- Viewing the Maps for a Location, page 3-26
- Configuring a Micello Map, page 3-27
- Uploading an External Map, page 3-27

---

**Viewing the Maps for a Location**

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**
Choose the *Maps* tab.

The map appears in the Maps tab.
Configuring a Micello Map

Cisco DNA Spaces enables you to configure Micello map for a floor or zone.
To configure the Micello map, 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 window, click the floor or zone for which you want to configure the Micello map.
Step 3 Click the Maps tab.
Step 4 Click the Micello tab.
Step 5 In the Map Name field, enter a name for the map.
Step 6 In the Enter Micello details area, choose whether you want to configure the Map ID or Map URL to display the Micello map.
Step 7 In the following field, enter the Map ID or Map URL for the Micello map based on the previous selection.
Step 8 In the API Key field, enter the API key for the Micello map.
Step 9 Click Save.
The maps gets loaded from the Micello, and appears in the window.

Note To configure a Micello map, you must have a Micello account.

Uploading an External Map

Cisco DNA Spaces enables you to configure external maps of your choice for a floor or zone.
To configure an external map, 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 floor or zone for which you want to configure the external map.
Step 3 Click the Maps tab.
Step 4 Click the Image tab.
Step 5 In the Map Name field, enter a name for the map.
Step 6 Click the Choose File button and upload the image file for the map.
Step 7 Click Save.
Managing the Access Points

You can add or remove access points to a zone.

- Adding an Access Point to a Zone, page 3-28
- Removing an Access Point from a Zone, page 3-28
- Viewing the Access Points for a Location, page 3-29

Adding an Access Point to a Zone

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

1. In the Cisco DNA Spaces dashboard, choose Location Hierarchy. The Location Hierarchy window appears with the location hierarchy.
2. In the location hierarchy, click the zone to which you want to add the access point.
3. Click Modify Access Points.
4. Select the check box for the access point that you want to add.
5. Click Add.

The access point gets added to the zone.

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 on page 1-2.

Removing an Access Point from a Zone

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

1. In the Cisco DNA Spaces dashboard, choose Location Hierarchy. The Location Hierarchy window appears with the location hierarchy.
2. In the location hierarchy, click the zone from which you want to delete the access point.
3. Click Modify Access Points.
Managing the Groups

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

- Creating Groups, page 3-29
- Renaming a Group, page 3-30
- Editing a Group, page 3-31
- Deleting a Group, page 3-31

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.
Managing the 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.

---

**Note** 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**.

---

**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.

Step 5  Click Update.

---

**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.

---

**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, page 3-32
- Deleting a Zone, page 3-32
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**.

---

Note  You cannot delete any zone that is associated with the proximity rules.

Displaying Cumulative Count in Location Hierarchy

In the location hierarchy, the count of APs, BLE Beacons, 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, BLE beacons, 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.
Behavior Metrics

This chapter describes the Behavior Metrics reports.

• Overview of Behavior Metrics, page 4-1
• Viewing the Behavior Metrics Reports, page 4-1
• Pin a Location, page 4-9

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), page 4-4
• WiFi Adoption, page 4-7
• Right Now, page 4-8

Viewing the Behavior Metrics Reports

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

Step 1 In the Cisco DNA Spaces dashboard, choose Home.
Step 2 In the My Apps area, click Behavior Metrics.
The Behavior Metrics report is displayed.
Step 3 To view any other report, click the corresponding tab at the top right of the Behavior Metrics window.
Step 4 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.

Note

- 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 month and tag filters are not applicable for the Right Now report.
- 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 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 meta data 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 Francisco” is filtered in the location hierarchy, the “Average Visit Duration” for Cisco San Francisco 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 meta data 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

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 bench marks 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.
Viewing the Behavior Metrics Reports

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.

WiFi Adoption

The Wi-Fi Adoption report provides the metrics about the Wi-Fi Adoption in the filtered location. The data is shown for the filtered tag and month.

Intent Rate

The Intent Rate report displays the details of the visitors who intended to click the SSIDs. The bar graph represents the percentage of “footfalls that intended to click the SSID” among the “total number of footfalls”. This report enables you to identify how many visitors tried to access the Wi-Fi.

Acquisition Rate

The Acquisition Rate report displays a bar graph that represents the percentage of visitors who clicked the SSID, and got the internet provisioned. This report enables you to identify how many visitors are acquired.

Repeat Visitors

The Repeat Visitors shows the details of repeated visits in the locations. Displays a bar graph that represents the percentage of “visitors who have visited the locations more than once” among “the total number of visitors who have visited the locations”. This report enables you to analyze whether the visitors are coming again to your business locations.

WiFi Connected Distribution: Hour of the Day

Displays a bar graph that represents the distribution of Wi-Fi Connections during various hours of a day. This report enables you to identify at what hour of the day there are more Wi-Fi adoption. Each bar in the graph represents the “percentage of Wi-Fi connections that occurred at that particular hour of a day” among “the total Wi-Fi connections occurs on a day”. For example, the bar for 1 pm represents the “percentage of Wi-Fi connections that occurs at 1 pm” among “the total Wi-Fi connections that occurs on a day”.

WiFi Connected Distribution: Day of the Week

Displays a bar graph that represents the distribution of Wi-Fi Connections during various days of a week. This report enables you to identify on which day there are more Wi-Fi adoption. Each bar in the graph represents the “percentage of Wi-Fi connections that occurred at that particular day of the week” among
the “Wi-Fi connections occurs on a week”. For example, the bar for “Tues” represents the “percentage of Wi-Fi connections that occurred on Tuesdays” among the “total number Wi-Fi connections that occurs on a week”.

**AP Density**

Displays a bar graph that shows the average number of APs available per square foot.

| Note | There is no historical data shown for AP density. |

**Right Now**

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 your locations. You can filter the location for which you want to view the data using the Location drop-down list.

| Note | Do not compare the data displayed in Cisco DNA Spaces reports such as Behavior Metrics with the data displayed in Cisco Wireless Controller or Cisco CMX. |

The report includes the following details:

- **Total Active Visitors**—The total number of visitors currently present at the filtered location.
- **New VS Returning Visitors**—The pie chart displays the percentage of new visitors and the returning visitors (the visitors who have visited the location earlier) among the total number of visitors currently present at the filtered location. The count for new visitors and the count for returning visitors are also shown below the pie chart along with their percentage.
- **Top 5 locations**—The 5 locations that currently have more visitors are displayed along with the number of visitors.
- **Current visitors by their gender**—Displays pie charts with percentage of male, female, and gender-not-specified customers among the total number of visitors currently present at the location. The count for each gender is also displayed below the corresponding pie chart.
- **Current Visitors Profile Information**—The number of mobile number, e-mail IDs, names, and gender that are captured from the visitors currently present at the location. The number of current visitors opted in for subscription is also shown in this section.
- **Current visitors distribution based on their tags**—Displays the tags to which the current visitors belong to. A pie chart is displayed for each such tag showing the percentage of the current visitors for that tag. You can view all the tags to which at least one current visitor got added by clicking the “Show More” button.
- **Current visit duration**—The bar graph displays the duration for which the current visitors are present at the filtered location. The number of current visits for various visit duration ranges is shown. The average dwelling time is shown at the top of the bar graph.
- **Days Visited of the current visitors since last 30 days**—The bar graph displays the number of days the current visitors visited the filtered location in the last 30 days. The number of visits for various day ranges is shown. The average days visited by the currently present visitors at the filtered location is shown above the bar graph.
• **Current visitors by their locations**—Displays location-wise count of current visitors in the child locations of the filtered location. The location-wise count is displayed in Map view and list view.
  
  – **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**

• Right Now report has a passive duration of 10 minutes. So, a visitor will be shown in the Right Now report 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. For example, the Top Locations displayed in the Right Now report will be affected.

• If a visitor is appearing for more than 12 hours in a location that visitor is considered as an employee.

---

### 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:

| Step 1 | In the **Behavior Metrics** window, click the **Pin Locations** button at the far right of the window. |
| Step 2 | In the **Pin Locations** window you can select the locations that you want to pin. |
| Step 3 | Click **Apply**. |
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.

- Prerequisites for Creating a Portal, page 4-2
- Sample Portals, page 4-2
- Creating a Portal, page 4-3
- Portal Modules, page 4-5
- Configuring a Language for a Portal, page 4-6
- Configuring Authentication for a Portal, page 4-9
- Adding a Data Capture Form to a Portal, page 4-15
- Defining a Brand Name for a Portal, page 4-16
- Adding a Welcome Message to a Portal, page 4-17
- Adding a Notice to a Portal, page 4-18
- Providing a Feedback Section in a Portal
- Uploading Videos to a Portal, page 4-19
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 on page 3-1.

• 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 on page 4-44.

• 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 on page 4-46.

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

To view and make a copy of the sample portal, perform the following steps:
Creating and Managing 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 My Apps area, choose Captive Portal.
Step 3: In the Captive Portal window that appears, choose Portal in the left pane.
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 My Apps area, choose Captive Portal.
Step 3: In the Captive Portal window that appears, choose Portal in the left pane.
Step 4: Click Create New.
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.
Step 8: From the Authentication Type drop-down list, choose the authentication type that you want apply for the portal.
Step 9: After specifying the details for the authentication type, click Next.

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” section on page 4-15.

Step 12 Click Next.

The User Agreements screen 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.

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.

**Note**

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:

**Step 1**
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 Uploading Static Content Key Values for a Language, page 4-7

**Step 2**
Open the portal for which you want to configure the language.

**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.

The language gets added to the Added Languages list.

**Step 7**
Click Add.

In the portal, now a drop-down list appears adjacent to the Languages icon, and the newly added language gets listed in that drop-down list.

**Step 8**
From the drop-down list adjacent to the Languages icon, choose the language in which the static portal content is to display.

The captions of the modules are displayed in the chosen language.

### Setting a Default Language

To set a default language, do the following:
Creating and Managing Portal

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.

To know how to display the static content in a language, see the Configuring a Language for a Portal, page 4-6.
The language code for various languages are shown in Figure 4-1.
Figure 4-1 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, 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” section on page 4-14.

Cisco DNA Spaces supports the following authentication types:

- **No Authentication** — The internet access is provided without any authentication process. For more information on configuring a portal for No Authentication, see the “Configuring a Portal with No Authentication” section on page 4-9.

- **SMS with password verification** — The customer has to enter a valid mobile number to access the internet. Then, 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 in the SMS. For more information on configuring the “SMS with password verification”, see the “Configuring a Portal for SMS with Password Verification” section on page 4-12.

- **SMS with link verification** — The customer has to provide a valid mobile number to access the internet. Then, an SMS is sent to that mobile number. For more information, see the “Configuring a Portal for SMS with Link Verification” section on page 4-10.

- **Email** — The customer has to provide a valid e-mail ID to access the internet. For more information on configuring e-mail authentication, see the “Configuring a Portal for E-mail Authentication” section on page 4-14.

- **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. For more information on configuring the Social Sign In authentication, see the “Configuring a Portal for Social Sign In Authentication” section on page 4-13.

---

**Note**

The Opt In option is available only for “SMS with password verification”, “Email”, and “No Authentication” 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” section on page 4-15. For more information on Opt In feature, see the “Opted In Option for Users” section on page 6-5.

---

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.
Creating and Managing Portal

Chapter 4  Working with the Captive Portal App

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.

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**, page 4-14.

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” section on page 4-46.

Step 6  Save the changes.

**Note**  Portals with **SMS with link verification** authentication type will have an authentication module named **SMS Authentication**. For more information on the Authentication Module, see the “Authentication Module” section on page 4-15.
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 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, page 4-14.

**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, 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 “{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” section on page 4-46.

**Step 9** Save the changes.
Creating and Managing Portal

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” section on page 4-15.

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

Note

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” section on page 4-46.

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 User Agreements on portal home page check box. For more information on inline authentication, see the Inline Authentication, page 4-14.

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, page 4-46.

Step 4
Save the changes.

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” section on page 4-15.

Note

The +Add button takes you to the Social Apps window where you can configure the customized apps.
Creating and Managing Portal

Chapter 4      Working with the Captive Portal App

Creating and Managing Portal

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 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, page 4-14.
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.

Note
Portals with Email authentication type will have an authentication module named Email. For more information on the Authentication Module, see the “Authentication Module” section on page 4-15.

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** 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**.
The Data Capture screen appears.

**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.
- **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).
Creating and Managing Portal

Chapter 4      Working with the Captive Portal App

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 placeholder 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.

---

**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:

**Step 1**  Open the portal for which you want to define the brand name.

**Step 2**  Click the **Brand Name** module.

The **brand name** window appears.
Step 3  Choose the type of brand.
  a.  If you choose Text only, in the Brand Name field that appears, enter the brand name.
  b.  If you choose Logo, click the Upload button that appears, and upload the logo image.
Step 4  Click Save.
The brand name for the portal is successfully defined.

---

Note  If you are modifying a portal that is already associated with a published captive portal, click the Save & 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” section on page 4-33.

---

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.
The Welcome Message window appears.
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” section on page 4-63.
Step 4  If you want to display a different welcome message for the repeat users, ensure that the Add a custom 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” section on page 4-63.
Step 5  Click Save.
The welcome message is successfully defined for the portal.

---

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” section on page 4-33.
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.

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” section on page 4-33.

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.
Chapter 4 Working with the Captive Portal App

Creating and Managing Portal

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.

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” section on page 4-33.

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.
Creating and Managing 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.

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” section on page 4-33.
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.
Creating and Managing Portal

The feedback section is successfully created in the portal.

---

**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” section on page 4-33.

### 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.

---

**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” section on page 4-33.
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.

- **Note**  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.

- **Note**  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.

- **Note**  To add more apps, use the **Add an App** button.

**Step 7**  Click **Save**.

The app is successfully added to the portal.

- **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” section on page 4-33.
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.

Note
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, page 4-14.

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.

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” section on page 4-33.

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.
Creating and Managing Portal

Chapter 4      Working with the Captive Portal App

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.

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” section on page 4-33.

Deleting a Promotion and an Offer for a Portal

Cisco DNA Spaces enables you to remove a promotion from a portal after the required timeline.

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 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.
- 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.

- 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.

- 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” section on page 4-63

**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.

**Note** The menu items added appear as text in the preview of the portal, but appear as links in the runtime.
Creating and Managing Portal

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” section on page 4-33.

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 Portal**.

**Step 4**
In the window that appears, do any of the following:

- To open the exported file directly, choose **Open**.
- 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**.

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 Css** button. After making the necessary changes to the style sheet, you can upload it to Cisco DNA Spaces using the **Upload Css** button.
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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Open the portal of which you want to edit the style sheet.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click Stylesheet Editor.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click the Assets Library tab.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Drag and drop the asset file, or upload it using Choose File button.</td>
</tr>
</tbody>
</table>

The file gets added to the assets list.

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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>In the Cisco DNA Spaces dashboard, choose Home.</td>
</tr>
<tr>
<td>Step 2</td>
<td>In the My Apps area, click Captive Portal.</td>
</tr>
<tr>
<td>Step 3</td>
<td>In the Captive Portal window, choose Portal in the left pane.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click Import Portal at the top-right of the window.</td>
</tr>
<tr>
<td>Step 5</td>
<td>In the Import Portal window that appears, do the following:</td>
</tr>
<tr>
<td></td>
<td>a. In the Portal Name field, enter a file name for the portal.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

The selected locations appear at the right side of the window.
Step 6  Click **Import**.

---

**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 **My Apps** area, 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 **My Apps** area, 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 My Apps area, 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 following 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**, page 4-32
- **Creating a Captive Portal Rule to Display Captive Portals**, page 4-33
- **Use Case: Captive Portal Rule**, page 4-37
- **Managing Captive Portal Rules**, page 4-47

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 on page 3-1.
- For CUWN-CMX, 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” section on page 4-41.

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” section on page 4-1.

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 Persona App” section on page 6-1.

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” section on page 4-15.

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” section on page 12-2.

– If your wireless network is CUWN, do the configurations mentioned in “Configuring Cisco Unified Wireless Network for Internet Provisioning and RADIUS Authentication” section on page 11-11.

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” section on page 4-32.

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, the status of app in the customer’s device, 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.
Captive Portal Rule

Note

For CUWN-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:

---

### 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, 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” section on page 4-41.

---

### 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 on page 3-2.

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 on page 3-24. 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” section on page 4-50.

### 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, the number of visits made by the customer, and the status of app in the customer’s device. 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 on page 6-4.

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 on page 5-13.

e. If you want to filter the customers based on the customer’s app status, check the **Filter by App Status** check box, and choose the app status for which the rule is applicable.

**Step 8**
In the Schedule area, specify the period for which you want to apply the rule.

f. 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.

a. 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.

b. 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” section on page 4-3.
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” section on page 4-32. 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 the 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 on page 6-4”.

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 the“Trigger API Configurations” section on page 4-50.

**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 super
markets. 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 super market, when the customers connect to XYZID from XYZ’s super markets.
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
*Configuring Access Point Mode, SSIDs, ACLs, Splash URLs, and Virtual Interface in the WLC*,
page 11-2.

**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 on page 3-24.

**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**” section on page 4-3.

**Step 6** In the Cisco DNA Spaces dashboard, choose **Home**.

**Step 7** In the My Apps area, 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** field, 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 **and 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:

- **Device Onboarding**, page 4-38
- **Customer Acquisition**, page 4-39

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.
**Reports**

- **Provisioned Internet**—The total number of unique devices that got internet provisioned from the selected location during the specified period. This metric reflects the total number of unique devices that are able to access the internet from the specified period. This metric is crucial for understanding the overall connectivity and growth of devices in the selected location.

**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 selected location during the specified period.

- **New Devices**—The total number of new unique devices that have connected to your SSIDs from the selected location during the specified 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 identified newly from the selected location during the specified period, and the data (personal and demographic) collected from the identified customers.

**Note**

If a new customer connects to your location using multiple devices, and uses the same personal identity (mobile number, e-mail, and so on), the customer is counted only once.

**Customer Acquisition**

- **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 period. The percentage of new unique devices out of the total number of devices is also shown.
Chapter 4      Working with the Captive Portal App

Reports

• **New Customers Identified**—The total number of new unique customers that got identified through any of the personal identity (mobile number, e-mail, and so on) from the selected location during the specified period. The percentage of new unique customers identified out of the total unique new 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 identified” who have opted in for subscription from the selected location during the specified period. The percentage of opted-in “unique new customers identified” out of the total number of “unique new customers identified” is also shown. For more information on opted-in users, see the “Opted In Option for Users” section on page 6-5.

• **Completed Data Capture**—The total number of “unique new customers identified” who have completed the data capture form from the specified location during the specified period. The percentage of “unique new customers identified” who have completed the data capture out of the total number “unique new customers identified” 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 identified”, from the selected location during the specified period. It also shows the daily count of “unique new customers identified” 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.

**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.

**Device Languages**—Displays a pie chart with the percentage of customers who used various device languages out of the total number of customers for whom the device language data is collected. The device languages that are used the most by customers are displayed below the pie chart with the count of customers. You can view all the device languages, used at least by one customer, by clicking the “Show All” button. Device language count is derived based on the device language selected by the customer in the captive portal.

## 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 on page 3-1.
- Create the SSIDs in the Wireless Network System.
  - For creating the SSIDs for the CUWN, see the “Configuring Access Point Mode, SSIDs, ACLs, Splash URLs, and Virtual Interface in the WLC” section on page 11-2.
  - For creating the SSIDs for Meraki, see the “Enabling SSIDs in Cisco Meraki” section on page 12-1
- 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” section on page 4-41.
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 Unified Wireless Network, page 4-42
- Importing the SSIDs for Cisco Meraki, page 4-42

Importing the SSIDs for Cisco Unified Wireless Network

Note For CUWN, 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 Cisco Wireless Controller. You can view the SSID name in the Cisco Wireless Controller dashboard.

Note For CUWN-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 SSIDs window.

Note As Cisco DNA Spaces needs to synchronize with the CUWN 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 SSIDs 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 on page 12-5.

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.
Social Authentication for Portals

To enable social authentication for the portals, perform the following steps:

1. Configuring the Wireless Network for Social Authentication, page 4-44
2. Configuring the Apps for Social Authentication, page 4-45
3. Adding Social Apps for Social Authentication, page 4-46
4. Configuring a Portal for Social Sign In Authentication, page 4-13

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 the Cisco Unified Wireless Network for Social Authentication, page 11-17
- Configuring Cisco Meraki for Social Authentication, page 12-5
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, page 4-45
- Twitter, page 4-45
- LinkedIn App, page 4-45

Facebook

To configure the Facebook app for the social-authentication, perform the following steps:

Step 1 Go to developers.facebook.com.
Step 2 From the My Apps drop-down list, choose the app that you want configure in Cisco DNA Spaces for social-authentication.
Step 3 Click Settings.
Step 4 In the App Domains field, enter cisco.wifi-mx.com.

Note The domain changes based on Cisco DNA Spaces setup (live, beta, and so on) where the portal is created.

Twitter

To configure the Twitter app for the social-authentication, perform the following steps:

Step 1 Log in to apps.twitter.com.
Step 2 Click the app that you want to configure in Cisco DNA Spaces for social-authentication.
Step 3 Click the Settings tab.
Step 5 Uncheck the Enable Callback Locking check box.
Step 6 Check the Allow this application to be used to Sign in with Twitter check box.

Note The domain changes based on Cisco DNA Spaces setup (live, beta, and so on) where the portal is created.

LinkedIn App

Step 1 Log in to developer.linkedin.com.
Step 2 Click My Apps.
Chapter 4      Working with the Captive Portal App

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**.
Step 2 In the **My Apps** area, 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**.

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 **My Apps** area, 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 **Add**.
Step 3 In the Captive Portal window that appears, click Settings in the left pane.

Step 4 In the Settings window, choose SMS.

Step 5 Click Add SMS Gateway.

Step 6 From the SMS Gateway Type drop-down list, choose the SMS Gateway type that you want to use. Additional fields appear based on the SMS Gateway type selected.

Cisco DNA Spaces supports the following SMS Gateway types:

- REASON8
- SMPP
- WATERFALL
- MGAGE
- TWILIO
- PANACEA MOBILE
- DATAMETRIX
- TROPO
- NYY
- TRU
- PHIZZLE
- AWS_SNS
- PROXIMUS

Step 7 In the additional fields that appear based on the SMS Gateway type selected, specify the required values.

Step 8 Click Save.

Note The SMS Gateways created appears for selection in the SMS Gateway drop-down list for “SMS with password verification” and “SMS with link verification” authentication options in the portal. These SMS gateways also are available for selection when configuring the SMS notifications in the Engagement Rule.

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, page 4-48
- Restarting a Captive Portal Rule, page 4-48
- Modifying a Captive Portal Rule, page 4-48
- Deleting a Captive Portal Rule, page 4-49
- Viewing the Captive Portal Rules for a Location, page 4-49
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.
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.

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.
Step 4  Check the check box for the captive portal rule that you want to restart.
Step 5  Click the Make Live button that appears at the bottom of the window.

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.

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 Rules tab.

Step 4 Click the Captive Portal Rule tab.

The captive portal rules for the location gets listed.

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, and Profile 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:

a. Click the **Add Locations** button.

b. In the **Choose Locations** window that appears, select the locations for which you want to apply the rule.

c. 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 apply the rule for locations with a particular metadata, perform the following steps:

a. Select the **Filter by Metadata** check box.

b. In the Filter area, click the **Add Metadata** button.

The **Choose Location Metadata** window appears.

c. From the drop-down list, choose the metadata variable, and choose the value for the variable in the adjacent field.

d. Click **Done**.

To exclude the locations with a particular metadata, perform the following steps:

a. Select the **Filter by Metadata** check box.

b. In the Exclude area, click the **Add Metadata** button.

The **Choose Location Metadata** window appears.

c. From the drop-down list, choose the metadata variable, and choose the value for the variable in the adjacent field.

d. 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” section on page 4-63. 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” section on page 4-63. 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” section on page 4-63.

- **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” section on page 4-63.

**Certified Device List for Portals**

The following table lists the devices and operating systems that are tested and certified for the portals.

<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>Mobile Device</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>
</tbody>
</table>

**Note**

Only those data that you have configured to capture using the Data Capture form in the portal are included.
Cisco DNA Spaces Captive Portal Behavior

The captive portal behavior for various devices is as follows:

- **Apple iOS 7.x to 11.x**, page 4-53
- **Android 5.x and Later (Using CNA)**, page 4-53
- **Android 4.x and Earlier**, page 4-54
- **Windows Phone**, page 4-55
- **Windows PCs and Laptops**, page 4-55
- **Macbook**, page 4-56

Table 4-1 Certified Device List

<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>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 Honor</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>iPads/Tablets</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>
<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>
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” section on page 4-9. 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” section on page 4-57. 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.

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” section on page 4-14.

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” section on page 4-9. 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” section on
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” section on page 4-14.

### 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” section on page 4-9. 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” section on page 4-57. 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.
Chapter 4   Working with the Captive Portal App

Cisco DNA Spaces Captive Portal Behavior

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” section on page 4-14.

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” section on page 4-9. 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” section on page 4-57. 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.

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” section on page 4-9. 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” section on page 4-57. 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” section on page 4-9. 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” section on page 4-57. 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” section on page 4-14.

---

**Macbook**

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” section on page 4-9. 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” section on page 4-57. 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.
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” section on page 4-14.

Authentication Steps for Customers

The authentication steps that a customer has to complete to provision the internet for various authentication types are as follows:

- Authentication Steps for No Authentication with Terms and Conditions, page 4-57
- Authentication Through SMS with Link Verification, page 4-57
- Authentication Through SMS with Password Verification, page 4-59
- Authentication Through E-mail, page 4-61
- Authentication Steps for Social Authentication, page 4-62

Authentication 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.

Authentication Through SMS with Link Verification

To complete the “SMS with link verification” authentication, perform the following steps:

**Step 1**
In the captive portal, click/tap any menu item.
**Authentication Steps for Customers**

**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 fingerprint verification.

For more information on fingerprint verification, see the “Fingerprint Verification” section on page 4-59.

*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), and 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.
Authentication Steps for Customers

- **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 login 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 login screen appears with a blank mobile number field.**

### Authentication Through SMS with Password Verification

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.
Authentication Steps for Customers

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.
Authentication Steps for Customers

– **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.

**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.

**Authentication Through E-mail**

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 **Allow 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:
Authentication Steps for Customers

- **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.

Authentication 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” section on page 4-13.

**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” section on page 4-45.

Step 6  After provisioning the internet, a “Continue” screen 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, “Sign in 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

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 and the engagement URLs in the notification messages, 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.
Smart Links and Text Variables

Note To use these parameters to display the personalized view to the customers, you have to configure your web pages accordingly.

You can include the smart links in the following options:

• The links added in the custom menu items added to the portal.
• The engagement URLs in the SMS and e-mail notifications.

Using text variables, you can add personal details of the customers such as name, mobile number, gender, and so on in the notification messages sent to the customers and business users. By default, the notifications 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 an engagement rule to send SMS notifications to the customers 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 notification message sent to the customers and business users such as employees or API end point.
• Welcome Messages for first time and repeat user.
• Notices added to the portal.

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.

Note 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 your 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:

• macaddress-The mac address of the device.
• encryptedMacAddress-The encrypted mac address of the device.
• deviceSubscriberId-The subscriber ID for the device in the database.
• firstName- The first name of the customer.
• lastName- The last name of the customer.
• email- The e-mail ID of the customer.
• Mobile- The mobile number of the customer.
• gender- The gender of the customer.
• optinStatus- The opt in status for the customer.
Note
You can use the “macaddress”, “encryptedMacAddress”, “deviceSubscriberId”, and optinStatus variables only for API notifications and the engagement URLs in the notifications.

You can include the following dynamic variables in a smart link or text:

- Business Tags- 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 on page 4-15.

- Location Metadata- The location metadata for the customer location. The location metadata keys defined are listed as variables. For more information on defining the location metadata, see the “Defining or Editing Metadata for a Location” section on page 3-24.

To include a smart link in a URL, or variable in a text, perform the following steps:

Step 1
In the URL field or text box, enter $ 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.
Sending Notifications with the Engagements App

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 or closeness to a BLE Beacon.

An engagement rule is applied for all the SSIDs or BLE Beacons defined for the locations specified in the rule.

- Prerequisites for Creating an Engagement Rule, page 5-1
- Creating an Engagement Rule, page 5-2
- Managing Engagement Rules, page 5-9
- Engagement Rule Report, page 5-11

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” section on page 12-4
  - If your wireless network is CUWN, do the configurations mentioned in Configuring Cisco CMX for Notifications and Reports, page 11-13
- 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” section on page 3-1
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, e-mail, BLE Beacon, or app. For business users, you can send the notifications through Cisco Webex Teams, SMS, e-mail, or to an external API. For customers, you can configure to send the notifications based on the proximity of the customer to a BLE beacon or connectivity of the customer to an SSID. For 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, page 5-2
• Creating an Engagement Rule for a Business User, page 5-6
• Use Case: Engagement Rule for Customers, page 5-4
• Use Case: Engagement Rule for a Business User, page 5-8

Creating an Engagement Rule for a Consumer

You can send the notifications to a customer through SMS, e-mail, BLE Beacon, or app.

To define an engagement rule to send notifications to the customers, perform the following steps:

---

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

**Step 2**  In the **My Apps** area, choose **Engagements**.
Step 3 On the Engagements page that appears, click **Create New Rule**.

Step 4 In the Rule Name field, enter a name for the engagement rule.

Step 5 In the Sense area, from the **When a user is on** drop-down list, choose whether you want to send notifications based on the user’s connectivity to the Wi-Fi or proximity to the BLE Beacon. For more information on configuring the sense type and expected customer presence, see the “Sense Type for an Engagement Rule” section on page 5-15.

Step 6 In the Locations area, specify the locations for which you want to send the notifications.

You can configure to send notifications for the entire location hierarchy or single or multiple locations such as group, floor, or zone. You can add the locations of both Cisco Meraki and CUWN in an Engagement rule. For more information on creating the location hierarchy, see the “Defining the Location Hierarchy” section on page 3-2.

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. For more information on configuring the metadata for the locations, see the “Defining or Editing Metadata for a Location” section on page 3-24. 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” section on page 5-15.

Step 7 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, the number of visits made by the customer, and the status of app in the customer’s device. 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.

**Note**

For more information on opted in users, see the “Opted In Option for Users” section on page 6-5.

b. If you want to filter the customers based on tags, check the **Filter by Tags** check box.

**Note**

For more information on creating tags, see the “Creating or Modifying Tags Using a Location Persona App” section on page 6-1.

**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 option, and mention that particular tag for which you don’t want to send the notifications.

For more information on using the tag filter, see the “Filtering by Tag” section on page 6-4.

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 on page 5-13.

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 the notification is to send to app user or non app user.

**Step 8**

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

e. 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.

a. 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.

b. If you want to apply the engagement 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 send the notifications.

**Step 9**

In the Actions area, perform the following steps:

a. From the **Notify** drop-down list, choose **Consumer**, and from the adjacent drop-down list choose any of the following:

   - **Only Once**—The notification is sent only once to a customer.
   - **Once In**—The notification is sent more than once to a customer 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 on page 5-14.

b. Specify the mode of notification. You can send the notification to the customers through app, e-mail, SMS, or BLE Beacon. For more information on configuring the notification types, see the “Notification Type for a Consumer” section on page 5-16.

**Note**
The summary of the rule is shown on the right side of the page.

**Step 10**

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 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 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 its app, A1.

To meet the preceding scenario, perform the following steps:

**Step 1** Integrate the app, A1, with the Cisco DNA Spaces SDK. For configuring the SDK, contact the Cisco DNA Spaces support team.

**Step 2** Log in to Cisco DNA Spaces.

**Step 3** Create the location hierarchy with all the locations of ABC.

**Step 4** Configure the app, A1, in Cisco DNA Spaces. For configuring the app, contact the Cisco DNA Spaces support team.

**Step 5** In the Cisco DNA Spaces dashboard, choose Home.

**Step 6** In the My Apps area, click Engagements.

**Step 7** On the Engagements page that appears, click Create New Rule.

**Step 8** In the RULE NAME field, enter a name for the engagement rule.

**Step 9** From the When a user is on drop-down list, choose WiFi, and from the drop-down list that appears, choose Entering Location.

**Step 10** In the Locations area, click the Add Locations button for choosing the location, and select location A, and Floor 1 of location B.

**Step 11** 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 12** 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 13** 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 App Push Notification check box, and from the following drop-down list, choose A1. If required, edit the message in the following text box.

d. 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 14** Click Save and Publish.
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 on page 5-1.

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 Home.
Step 2 In the My App area, click Engagements.
Step 3 On the Engagements page that appears, click Create New Rule.
Step 4 In the Rule Name field, enter a name for the engagement rule.
Step 5 In the Sense area, from the When a user is on drop-down list, choose WiFi to send notifications to the business user based on the user’s connectivity to the Wi-Fi. For more information on configuring the sense type and expected customer presence, see the “Sense Type for an Engagement Rule” section on page 5-15.

Note For business users, you must not choose the sense as “Beacon”.

Step 6 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 both Cisco Meraki and CUWN in an Engagement rule. For more information on defining the location hierarchy, see the “Defining the Location Hierarchy” section on page 3-2.

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. For more information on configuring the metadata for the locations, see the “Defining or Editing Metadata for a Location” section on page 3-24. 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” section on page 5-15.

Step 7 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, the number of visits made by the customer, and the status of app in the customer’s device. You can apply all these filters or any of them based on your requirement.

The rule gets published.
Creating an Engagement Rule

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.

**Note**
For more information on opted in users, see the “Opted In Option for Users” section on page 6-5.

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 to the business users for all tags expect 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.

For more information on using the tag filter, see the “Filtering by Tag” section on page 6-4.

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 on page 5-13.

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 send the notifications for the app users or non app users.

**Step 8** In the Schedule area, specify the period for which you want to apply the engagement rule.

e. 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.

a. 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.

b. 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 9** In the Actions area, perform the following steps:

a. From the **Notify** 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 on page 5-14.

   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 configuring the notification types, see the “Notification Type for a Business..."
Creating an Engagement Rule

User” section on page 5-17.

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 on page 4-15.

Note The summary of the rule is shown in the right side of the page.

Step 10 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 at least 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. For more information on creating the tag for this condition, see the use case in the “Creating or Modifying Tags Using a Location Persona App” section on page 6-1.
Step 4 In the Cisco DNA Spaces dashboard, choose Home.
Step 5 In the My Apps area, click Engagements.
Step 6 On the Engagements page that appears, click Create New Rule.
Step 7 In the RULE NAME field, enter a name for the engagement rule.
Step 8 From the When a user is on drop-down list, choose WiFi, and from the drop-down list that appears, choose Entering Location.
Step 9  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 10 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 11 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 12 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.

Step 13 Click Save and Publish.

The engagement rule is published.

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, page 5-9
- Restarting an Engagement Rule, page 5-10
- Modifying an Engagement Rule, page 5-10
- Deleting an Engagement Rule, page 5-11
- Viewing an Engagement Rule for a Location, page 5-11

Pausing an Engagement Rule

To pause an engagement rule, perform the following steps:

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

Step 2 In the My Apps area, click Engagements.

The Engagements page appear with all the engagements rules listed.

Step 3 Click the Pause Rule icon that appears at the far right of the engagement rule that you want to pause.

Step 4 In the window that appears, confirm pausing.
Managing Engagement Rules

The engagement rule is paused.

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, choose Home.
Step 2 In the My Apps area, click Engagements.
The Engagements page appear with all the engagements rules listed.
Step 3 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.

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 page.

Modifying an Engagement Rule

To modify an engagement rule, perform the following steps:

Step 1 In the Cisco DNA Spaces dashboard, choose Home.
Step 2 In the My Apps area, click Engagements.
The Engagements page appear with all the engagements rules listed.
Step 3 Click the Edit Rule icon that appears at the far right of the engagement rule that you want to modify.
Step 4 Make necessary changes.
Step 5 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 an Engagement Rule

To delete an engagement rule, perform the following steps:

Step 1 In the Cisco DNA Spaces dashboard, choose Home.
Step 2 In the My Apps area, click Engagements.
The Engagements page appear with all the engagements rules listed.
Step 3 Click the Delete Rule icon that appears at the far right of the engagement rule that you want to delete.
Step 4 In the window that appears, confirm deletion.

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 page.

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 In the Cisco DNA Spaces dashboard, choose Location Hierarchy.
The Location Hierarchy page appears with the location hierarchy.
Step 2 Click the location for which you want to view the engagement rule.
Step 3 Click the Proximity Rules tab.
Step 4 Click the Engagement Rule tab.
The engagement rules for the location gets listed.

Note The Proximity 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:

Step 1 In the Cisco DNA Spaces dashboard, choose Home.
Step 2 In the My Apps area, choose Engagements.
Engagement Rule Report

Click the rule for which you want to the Engagement Rule Report.

Step 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, page 5-12
- User Insight, page 5-12

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 by Location**—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.

User Insight

This section show the details of the customers who were targeted by the particular rule.

- **User Profile**—This section displays the total number of customers to whom the notifications are sent for the particular engagement rule.

  The pie chat in this section displays the ratio of the tagged customers to the not tagged customers among the targeted customers. Tagged customers are those customers who are included in any of the tag created in Cisco DNA Spaces. Also, the percentage of the targeted customers in each of those tags is shown using pie charts.

  This section also displays the ratio of male to female customers among the customers targeted based on the rule.

- **Dwell Time Distribution**—This bar graph displays the duration of each visit in the targeted locations. The duration of visits that fall with in various dwell time ranges are shown. For example, the count for >8 hrs represents the number of visits that spent greater than 8 hours in the targeted locations. The average dwell time is shown at the top of the graph.

- **Repeat User Engagement**—This bar graph displays the number of times the notifications are sent to various customers filtered for the rule. The number of customers that falls with in various repeat user ranges are shown in this section. The average repeat user engagement is shown at the top of the graph.

- **Users by Visit Count**—This bar graph displays the number of visits made by each target customer on the targeted locations. The number of customers that falls with in various visit ranges are shown. The average number of visits made by the customers filtered for the particular engagement rule is shown at the top of the graph.
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 Week— 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.
- **Push Notification**— To send the notification as a push message from an app. If you choose this option, the SMS or e-mail notification for this rule is not sent even configured. However, if there is any failure in sending the push notification, Cisco DNA Spaces uses the other configured notification types for sending the notification. To use this option, you need to configure the app. This notification type is not applicable for business users.
- **BLE Notification**— To send the notification as BLE notification. You can use this notification method only if the “Sense” is selected as “BLE Beacon”. This notification type is not applicable for business users.
- **Email**— To send the notification as an e-mail. For business users, you can define the e-mail address to which you want the sent 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.
Sense Type for an Engagement Rule

a. If you choose “WiFi”, an additional field appears where you can choose any of the following:
   - **Entering Location**—The notification is sent when a customer connected to the Wi-Fi enters the location.
   - **Exiting Location**—The notification is sent when a customer connected to the Wi-Fi leaves the location.
   - **Present at location**—The notification is sent when the customer is connected to the Wi-Fi and 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 meet to send the notifications.

b. If you choose “Beacon”, an additional field appears where you can choose any of the following:
   - **Beacon Enter**—The notification is sent when the customer enters the beacon premises.
   - **Beacon Exit**—The notification is sent when the customer leaves the beacon premises.
   - **Present at location**—The notification is sent when the customer 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 meet to send the notifications.

**Note**
If you choose **Beacon**, the notification is sent only if the customer’s blue tooth is ON.

**Note**
If you choose **Sense** as **Beacon**, you can send the notification only as BLE notification. If you choose **Sense** as **WiFi**, you cannot send BLE notification.

**Note**
For business user, you can select only **WiFi** as sense type.

Location Filter for an Engagement Rule

To specify the locations for which you want to send the notifications, perform the following steps:

a. Click the **Add Locations** button.

b. In the **Choose Locations** window that appears, check the check box for the locations for which you want to send the notifications.

c. 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

a. Check the **Filter by Metadata** check box.

b. In the Filter area, click the **Add Metadata** button.

   The **Choose Location Metadata** window appears.

   c. From the drop-down list, choose the metadata variable, and choose the value for the variable in the adjacent field.
d. Click Done.

To exclude to send notifications for the locations with a particular metadata, perform the following steps:

a. Check the Filter by Metadata check box.

b. In the Exclude area, click the Add Metadata button.

The Choose Location Metadata window appears.

c. From the drop-down list, choose the metadata variable, and choose the value for the variable in the adjacent field.

d. 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 to the customers through an app as push notifications, check the “Via App Push Notification” check box. From the App drop-down list, choose the app through which the notification is to send. For configuring the app, contact the Cisco DNA Spaces support team. The message content that is sent to the customer is displayed in the following text box. You can enhance the message content using the smart links. By default, the first name and last name of the customer 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 creating a text variable, see the “Smart Links and Text Variables” section on page 4-63.

- If you want to send the notification as a BLE notification, check the “BLE Notification” check box. The message content that is sent to the customer is displayed in the following text box. By default, the first name and last name of the customer 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 creating a text variable, see the “Smart Links and Text Variables” section on page 4-63.

Note: To send BLE beacon notifications or push notifications, you must integrate the BLE Beacon or the app from which you want to send the notifications with the Cisco DNA Spaces SDK. For SDK integration, contact the Cisco DNA Spaces Support team.

- 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 creating a text variable, see the “Smart Links and Text Variables” section on page 4-63.

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” section on page 5-13.
• 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 creating a text variable, see the “Smart Links and Text Variables” section on page 4-63.

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” section on page 5-13.

Note 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.

Note If you opt for app notification, the SMS and e-mail notifications are not sent even if they are configured. In any case if the app notification fails, the SMS or e-mail notifications are sent, if configured.

Note You can send the BLE notification only if you choose sense as “Beacon”. You can send the notification as push notification, SMS, or e-mail, if you choose the sense as “WiFi”.

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 on page 4-15.

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.

• 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 of the business user to whom you want to send the notifications. 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” section on page 5-13.
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 creating a text variable, see the “Smart Links and Text Variables” section on page 4-63.

- 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.

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 creating a text variable, see the “Smart Links and Text Variables” section on page 4-63.

- 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 on page 5-18.

**Trigger API Configuration for Notification**

To send notifications to an external API through the engagement rules, in the Create Engagement Rule page, 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 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” text box. For more information on text variables, see the “Smart Links and Text Variables” section on page 4-63. You can add more “GET” headers and parameters using the corresponding “Add” button.

- **Post Form**- To send notification 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 in the notification. 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” text box. For more information on text variables, see the “Smart Links and Text Variables” section on page 4-63. You can add more “POST FORM” headers and parameters using the corresponding “Add” button.

- **Post JSON**- To send notification 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” text box. You can view the variables that you can add to the JSON Data by clicking the text box. For more information on text variables, see the “Smart Links and Text Variables” section on page 4-63. You can add more “JSON” request headers using the corresponding “Add” button.

- Post Body- To send notification 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 included in the notification sent to the API. If you choose this method, request header fields appear, along with a text box where you can mention the content that is to send as notification message to the API. 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” text box. You can view the variables that you can add to the Body content by clicking the text box. For more information on text variables, see the “Smart Links and Text Variables” section on page 4-63. You can add more “JSON” request headers using the corresponding “Add” button.

**Note**

Only those data that you have configured to capture using the Data Capture form in the portal are included in the notifications.

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 more information on smart link, see the “Smart Links and Text Variables” section on page 4-63.
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 Persona App, page 6-1
• Use Case: Profile Rule (Location Personas Rule), page 6-3
• Managing Location Personas Rules, page 6-7
• Location Personas Rule Report

Creating or Modifying Tags Using a Location Persona 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, choose Home.
Step 2 In the My Apps area, click Location Personas.
Step 3 On the Location Personas page that appears, click Create New Rule.
Step 4 In the Rule Name field, enter a name for the Location Personas / Profile rule.
Step 5 In the Sense area, from the When a user is on drop-down list, choose whether you want to filter the customers for the rule based on the customer’s connectivity to the Wi-Fi or access to the BLE Beacon. For more information on configuring the sense type for the profile rule, see the “Sense Type for a Profile Rule” section on page 6-5.
Step 6 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. For more information on defining the location hierarchy, see the “Defining the Location Hierarchy” section on page 3-2.
Creating or Modifying Tags Using a Location Persona App

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 on page 3-24. 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 Profile Rule” section on page 6-6.

Step 7 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” section on page 6-5.

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 except 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” section on page 6-4.

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. For more information on the visits and duration you can configure, see the “Previous Visit Criteria” section on page 5-13.

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

Note 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.

Cisco DNA Spaces Configuration Guide
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 9**
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.

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.

**Step 10**
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 **User Profiler** page.

---

**Use Case: Profile Rule (Location Personas 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, choose **Home**.
**Step 4** In the **My Apps** area, click **Location Personas**.
**Step 5** On the **Location Personas** page that appears, click **Create New Rule**.
**Step 6** In the **RULE NAME** field, enter a name for the profile rule.
**Step 7** From the **When a user is on** drop-down list, choose **WiFi, Present at Location**, and from the drop-down list that appears, choose **45 Minutes**.
**Step 8** In the Locations area, click the **Add Locations** button, and select location A, and location C.
**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 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 10** 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 11** 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 12** 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.
Excluding a Tag

To exclude a tag, perform the following steps:

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.
2. In the Choose Tags window, click the Exclude radio button for the tag that you want to exclude.
3. Click Done.

Searching for a Tag

To search for a tag, perform the following steps:

1. In the window to create a new rule, in the Filter by Tags area, click the Add Tags button for Include or Exclude.
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.

Sense Type for a Profile Rule

a. If you choose “WiFi”, an additional field appears where you can choose any of the following:
   – Entering Location—The customer connected to the Wi-Fi when enters the location is filtered for the rule.
Use Case: Profile Rule (Location Personas Rule)

- **Exiting Location**—The customer connected to the Wi-Fi when exits the location is filtered for the rule.
- **Present at location**—The customer who is present at the location with connected to the Wi-Fi during a specified time or a specified duration is filtered for the rule. If you choose this option, additional fields appear where you can mention the duration or time that needs to meet by the customer to get filtered.

b. If you choose “Beacon”, an additional field appears where you can choose any of the following:
- **Beacon Enter**—The customer who enters the beacon premises is filtered for the rule.
- **Beacon Exit**—The customer who exits the beacon premises is filtered for the rule.
- **Present at location**—The customer who is present at the beacon premises during a specified time or a specified duration is filtered for the rule. If you choose this option, additional fields appear where you can mention the duration or time that needs to meet to filter for the rule.

**Location Filter for a Profile Rule**

To specify the locations, perform the following steps:

a. Click the **Add Locations** button.

b. In the **Choose Location window** that appears, select the locations for the profile rule.

c. 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 meta data, 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 meta data, 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, page 6-7
- Restarting a Location Personas Rule, page 6-7
- Modifying a Location Personas Rule, page 6-8
- Deleting a Location Personas Rule, page 6-8
- Viewing a Location Personas Rule for a Location, page 6-8

Pausing a Location Personas Rule

To pause a Location Personas rule, perform the following steps:

---

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

Step 2  
In the **My Apps** area, click **Location Personas**.

The **User Profile** window appears with all the existing Location Personas rules.

Step 3  
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.

---

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 page.

Restarting a Location Personas Rule

To restart a Location Personas rule, perform the following steps:

---

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

Step 2  
In the **My Apps** area, click **Location Persona**.

The **User Profile** window appears with all the existing Location Personas rules.

Step 3  
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.

---
Modifying a Location Personas Rule

To modify a Location Personas rule, perform the following steps:

Step 1 In the Cisco DNA Spaces dashboard, choose Home.
Step 2 In the My Apps area, click Location Persona.
   The User Profile window appears with all the existing Location Personas rules.
Step 3 Click the Edit Rule icon for the Location Personas rule that you want to modify.
Step 4 Make necessary changes.
Step 5 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, choose Home.
Step 2 In the My Apps area, click Location Persona.
   The User Profile window appears with all the existing Location Personas rules.
Step 3 Click the Delete Rule icon that appears at the far right of the Location Personas rule that you want to delete.

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 page.

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

**Step 2** Click the location for which you want to view the Location Personas rule.

**Step 3** Click the **Proximity Rules** tab.

**Step 4** Click the **Profile Rule** tab.

The Location Personas rules for the location gets listed.

---

**Note**  
The “Proximity 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, choose **Home**.

**Step 2** In the **My Apps** area, choose **Location Persona**.

**Step 3** Click the rule for which you want to view the Location Personas Rule Report.

**Step 4** 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 customers 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 customers 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.

**User Insights**

This section show the details of the customers who are targeted by the particular Location Personas rule during the specified period.

• **User Profile**—Displays the percentage of male and female customers in the total number of customers tagged by the particular Location Personas rule. The total number of male and female customers are shown near to the corresponding pie chart. Displays the total number of customers tagged to each tag specified in the rule. The pie charts for tags represent the percentage of customers tagged based on this rule in each tag. The number of tagged customers for each tag is shown below the corresponding pie chart. If the customers tagged for the rule are part of other tags not specified in the rule, those tags are also shown with the number and percentage of those customers.

• **Dwell Time**—The bar graph displays the duration of the visits made in the targeted locations by the customers tagged by the particular rule. The duration of visits for various dwell time ranges are shown. For example, the count for >8 hrs represents the number of tagged customers who has spent greater than 8 hours in the targeted locations. Average dwell time of the customers tagged based on the particular Location Personas rule is shown at the top of the bar graph.

• **Number of Visits**—This bar graph displays the number of times the customers tagged based on the particular Location Personas rule has visited the targeted locations. The number of visits for various visit ranges are shown. The average number of visits made by the tagged customers are shown at the top of the bar graph.
Working with the Cisco DNA Spaces Operation Insights App

The Cisco DNA Spaces 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 asset. 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 Operation Insights, see the Cisco DNA Spaces Operational Insights Configuration Guide.
This chapter describes the monitoring details that are displayed in Cisco DNA Spaces. It also provides information on the Support section.

To access the Monitoring and Support window, in the Cisco DNA Spaces dashboard, choose Monitoring and Support.

- Monitoring, page 8-1
- Support, page 8-4

Monitoring

This section describes Cisco DNA Spaces health details that are displayed in the Monitoring section. The Monitoring section of Cisco DNA Spaces is shown in Figure 8-1.

![Monitoring](image)

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 if 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.
Chapter 8  Monitoring and Support

Monitoring

- **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 heath, Server Health, Location Receiver heath, and Database health.
- **Location Personas**- Dashboard Health, Subscriber Health, Server health, Location Receiver heath, and Database heath.

**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 a 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.

## Support

The Support option enables you to track tickets raised by your customers. The tickets will be managed by the Cisco DNA Spaces support team. The tickets raised in third party tools can be uploaded into the Cisco DNA Spaces dashboard.

## Ticket Status

This area displays the status of various tickets raised by your customers. The following details will be listed in the header:

- **Unresolved**—Displays the total number of unresolved tickets.
- **Urgent**—Displays the total number of tickets with “Urgent” Status.
- **High**—Displays the total number of tickets with “High” status
- **Normal** —Displays the total number of “Normal” tickets.
- **Low**—Displays the total number of “Low” tickets.

## Tickets

The tickets raised by your customers are displayed here. The following details of the tickets are displayed:

- **ID**- The ID of the ticket.
- **Description**- The subject matter for the ticket.
- **Severity**- The severity allocated for the ticket.
- **Create Time**- The time at which the ticket was created.
- **ETA**- The expected time line for resolving the ticket.
- **Ticket Status**- The current status of the report.
Managing Cisco DNA Spaces Users and Accounts

This chapter explains the various types of Cisco DNA Spaces users. It also describes how to manage Cisco DNA Spaces and Cisco Unified Wireless Network accounts.

- Managing Cisco DNA Spaces Users, page 9-1
- Managing the Cisco DNA Spaces Accounts, page 9-3

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, page 9-1
- Editing User Privileges, page 9-2
- Deleting a Cisco DNA Spaces User, page 9-3

Inviting a Cisco DNA Spaces User

The Account Admin user can add other users for the Cisco DNA Spaces, and grant the users the required admin rights. The users can be created for a particular location. The Cisco DNA Spaces enables you to define the following types of users:

- **Account Admin**—This user has complete administrative rights on the Cisco DNA Spaces dashboard.
- **Admin**—This user has all the privileges except user management on the specified location. For example, an admin user cannot invite a user to join the Cisco DNA Spaces.
- **Read Only Access**—This user has the access only to view the Cisco DNA Spaces dashboard for the specified location. That is, this user cannot edit the Cisco DNA Spaces configurations.
- **Installer**—This user has the access only to the basic features of the Cisco DNA Spaces such as Settings, SSIDs, Connectors, Wireless Networks, and Behavior Metrics.

To add a Cisco DNA Spaces user, perform the following steps:

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

**Step 2** Click **Invite a User**.
Managing Cisco DNA Spaces Users

Step 3 In the **Invite a User** window, enter the following details:

a. In the **Email** field, enter the e-mail address of the user to add.

b. From the **Privileges** drop-down list, choose the access type that you want to provide to this user.

   Based on your selection, an option to specify locations appear. The field is not displayed for Account Admin.

   • If you choose **Admin** or **Read Only Access**, the **Choose Location** button appears. Select the locations for which you want to provide access, and click **Done**.

c. Click **Send Invitation**.

---

**Note** The Invite a User button is available only for the Account Admin users.

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.

**Editing User Privileges**

The Cisco DNA Spaces enables you to change the privileges of an existing Cisco DNA Spaces user. For example, an account admin user can promote a portal user to an admin user.

To change the user privileges of a Cisco DNA Spaces user, perform the following steps:

---

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

   The **Team** page appears with the list of Cisco DNA Spaces users.

**Step 2** Click the user for whom you want to change the user privileges.
Managing the Cisco DNA Spaces Accounts

This section describes how to manage the Cisco DNA Spaces Accounts.

- Changing the Cisco DNA Spaces Password, page 9-3
- Signing Out of Cisco DNA Spaces, page 9-4

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.

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.

To delete an existing Cisco DNA Spaces user, perform the following steps:

Step 1 In the Cisco DNA Spaces dashboard, choose Team.
   The Team page appears with the list of the Cisco DNA Spaces users.
Step 2 Check the check box adjacent to the user that you want to delete.
Step 3 Click Delete User at the far right of that user ID.

Managing the Cisco DNA Spaces Accounts

The Edit Privileges window appears.

Step 3 From the Privileges drop-down list, choose the type of access that you want to provide to the user.
Step 4 If you choose Admin or Read Only Access from the Choose Location drop-down list that appears, select the locations for which you want to provide access to the user.
Step 5 Click Update.

Note An e-mail is sent to the user indicating the change in the user privileges.
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**.
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 networks.

- The setup enables you to connect Cisco DNA Spaces to Cisco AireOS through the following methods:
  - Connect through a Cisco DNA Spaces Connector.
  - Connect through a Cisco Wireless Controller Cloud Connect.
  - Connect through Cisco On Prem.
- You can connect Cisco DNA Spaces to Cisco Meraki using the following methods:
  - Connect through Cisco Meraki account.
  - Connect through 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.

- **Connect via AireOS WLC Direct Connector**: Displays step-by-step instructions to connect Cisco DNA Spaces to Cisco Wireless Controller using Cisco Wireless Controller Cloud Connect.

- **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.

- **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.

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.
Configuring Cisco Unified Wireless Network (Cisco AireOS) for Cisco DNA Spaces

This chapter describes the configurations to be done in the Cisco Unified Wireless Network (Cisco AireOS or Cisco Catalyst) for using Cisco DNA Spaces. The configurations required differs based on the channel you use.

In addition to the method-specific configurations, you must do certain additional configurations for social authentication, radius authentication, and internet provisioning if you need these features. These configurations are common for all the methods, except eWLC and Mobility Express. For these two methods, the configurations are covered along with the respective method configurations.

**Note**
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.

- Configuring the Cisco Unified Wireless Network for Social Authentication, page 11-17
- Configuring Cisco Unified Wireless Network for Internet Provisioning and RADIUS Authentication, page 11-11

The configurations specific to various methods are as follows:

- Configurations for the CMX On Prem Option to work with Cisco DNA Spaces, page 11-2.
- Configurations for the WLC Direct Connect Option to work with Cisco DNA Spaces, page 11-17.
  - Connecting Cisco Wireless Controller to Cisco DNA Spaces using Cisco DNA Spaces Connector.
  - Configuring Mobility Express to work with Cisco DNA Spaces, page 11-20.
  - Configuring eWLC to work with Cisco DNA Spaces, page 11-26.
  - Configuring eWLC(GUI) to work with Cisco DNA Spaces, page 11-30
Chapter 11    Configuring Cisco Unified Wireless Network (Cisco AireOS) for Cisco DNA Spaces

Configurations for the CMX On Prem Option to work with Cisco DNA Spaces

For Cisco Unified Wireless Network with Cisco CMX, the following configurations are required to work with Cisco DNA Spaces:

1. Configuring Access Point Mode, SSIDs, ACLs, Splash URLs, and Virtual Interface in the WLC, page 11-2
2. Configuring Cisco Unified Wireless Network for Notifications and Reports, page 11-13
3. Configuring Cisco Unified Wireless Network for Internet Provisioning and RADIUS Authentication, page 11-11 (This configuration is required only if you need radius-authentication.)
4. Configuring the Cisco Unified Wireless Network for Social Authentication, page 11-17 (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 WLC.

Note

The SSIDs and ACLs are created in the WLC and not in the Cisco CMX.

The WLC configurations for the local and flexconnect modes are different.

• Local Mode Configurations for Using Cisco DNA Spaces, page 11-3
• FlexConnect Mode Configurations for Using Cisco DNA Spaces, page 11-7
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:

1. Configure the Local Mode for an Access Point, page 11-3
2. Create SSIDs in Cisco Wireless Controller, page 11-3
3. Create Access Control Lists, page 11-5
4. Configure the Virtual Interface, page 11-6

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

Note: 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. For more information, see “Importing the SSIDs for Cisco Unified Wireless Network” section on page 4-42.
Step 6 In the Cisco Wireless Controller main window, on the General tab, uncheck the Broadcast SSID check box.
Step 7 Choose Security > Layer 2, and check the MAC Filtering check box.

Note If radius authentication is not required, choose None for Layer 2 security. The Layer 2 security is to provide the internet access without splash page. As you are already configuring splash page for Cisco DNA Spaces, there is no need of Layer 2 security in this case.

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.

Note If radius authentication is not required, you must choose the Passthrough 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**.

### 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:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Log in to the Cisco Wireless Controller with your Wireless Controller credentials.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Choose <strong>Security &gt; Access Control Lists &gt; Access Control Lists</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>To add an ACL, click <strong>New</strong>.</td>
</tr>
<tr>
<td>Step 4</td>
<td>In the <strong>New</strong> window that appears, enter the following:.</td>
</tr>
<tr>
<td></td>
<td>a. In the <strong>Access Control List Name</strong> field, enter a name for the new ACL.</td>
</tr>
<tr>
<td></td>
<td>Note You can enter up to 32 alphanumeric characters.</td>
</tr>
<tr>
<td></td>
<td>b. Choose the ACL type as <strong>IPv4</strong>.</td>
</tr>
<tr>
<td></td>
<td>c. Click <strong>Apply</strong>.</td>
</tr>
<tr>
<td>Step 5</td>
<td>When the <strong>Access Control Lists</strong> window reappears, click the name of the new ACL.</td>
</tr>
<tr>
<td>Step 6</td>
<td>In the <strong>Edit</strong> window that appears, click <strong>Add New Rule</strong>.</td>
</tr>
<tr>
<td></td>
<td>The <strong>Rules &gt; New</strong> window appears.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Configure a rule for this ACL with the required wall garden ranges.</td>
</tr>
<tr>
<td></td>
<td>To view the wall garden ranges, in the <strong>Cisco DNA Spaces</strong> dashboard, click the <strong>Configure Manually</strong> link for a Cisco Unified Wireless Network SSID in the <strong>SSIDs</strong> window. The wall garden ranges are listed under the caption <strong>Creating the Access Control List</strong>. The <strong>Configure Manually</strong> link appears only after adding a Cisco AireOS SSID.</td>
</tr>
<tr>
<td></td>
<td>When defining the ACL rule, ensure to configure the values as follows:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Direction</strong>: Any</td>
</tr>
<tr>
<td></td>
<td>• <strong>Protocol</strong>: Any</td>
</tr>
<tr>
<td></td>
<td>• <strong>Source Port Range</strong>: 0-65535</td>
</tr>
<tr>
<td></td>
<td>• <strong>Destination Port Range</strong>: 0-65535</td>
</tr>
<tr>
<td></td>
<td>• <strong>DSCP</strong>: Any</td>
</tr>
<tr>
<td></td>
<td>• <strong>Action</strong>: Permit</td>
</tr>
<tr>
<td>Step 8</td>
<td>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 “<strong>Configuring the Wireless Network for Social Authentication</strong>” section on page 4-44.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

**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 Mode Configurations for Using Cisco DNA Spaces**

You can configure FlexConnect for central switch or local switch mode.

- FlexConnect Central Switch Mode, page 11-7
- FlexConnect Local Switch Mode, page 11-7

---

**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:

2. Create SSIDs in the Cisco Wireless Controller for FlexConnect Central Switch Mode, page 11-8.

---

**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:

2. Create SSIDs in the Cisco Wireless Controller for the FlexConnect Local Switch Mode, page 11-8.
3. Create Access Control Lists for FlexConnect Local Switch Mode, page 11-10
4. Configure the Virtual Interface, page 11-6
Configurations for the CMX On Prem Option to work with Cisco DNA Spaces

Chapter 11      Configuring Cisco Unified Wireless Network (Cisco AireOS) for Cisco DNA Spaces

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” section on page 11-3.

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” section on page 11-5.

Create SSIDs in the Cisco Wireless Controller for the FlexConnect Local Switch Mode

**Note** 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. For more information, see “Importing the SSIDs for Cisco Unified Wireless Network” section on page 4-42.

Step 6  In the Cisco Wireless Controller main window, on the **General** tab, uncheck the **Broadcast SSID** check box.
Chapter 11  Configuring Cisco Unified Wireless Network (Cisco AireOS) for Cisco DNA Spaces

Configurations for the CMX On Prem Option to work with Cisco DNA Spaces

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.

Note  If RADIUS authentication is not required, choose None for Layer 2 security. The Layer 2 security is to provide the internet access without splash page. As you are already configuring splash page for Cisco DNA Spaces, there is no need of Layer 2 security in this case.

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.

Note  If RADIUS authentication is not required, you must choose the “Passthrough” radio button.

c.  In the Preauthentication ACL area, from the WebAuth FlexAC drop-down list, choose the ACL previously defined.

d.  Check the Enable check box for Sleeping Client.

Note  Enabling sleeping client is optional. 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 remembered 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:
Chapter 11  Configuring Cisco Unified Wireless Network (Cisco AireOS) for Cisco DNA Spaces

Configurations for the CMX On Prem Option to work with Cisco DNA Spaces

---

**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 on page 4-44.

  **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.

---

**Configuring Cisco Unified Wireless Network for Internet Provisioning and RADIUS Authentication**

To provide an additional layer of security for your portal, Cisco DNA Spaces supports RADIUS authentication for the internet provisioning on the captive portals. Also, certain configurations are required in the CUWN to manage the internet provisioning.

• Customer onboarding by captive portal
• To seamlessly provision internet
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.

**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. 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.
Configuring Cisco Unified Wireless Network for Notifications and Reports

The configurations required for Cisco Unified Wireless Network for notifications and reports depend on how the wireless network is connected to Cisco DNA Spaces. Access the respective link from the following based on your scenario:

- Configuring Cisco CMX for Notifications and Reports, page 11-13
- Configuring Cisco CMX for Notification and Reports Using CMX Tethering (For Cisco CMX 10.6 or later), page 11-15
- Configuring Cisco Unified Wireless Network with Cisco Wireless Controller for Notifications and Reports (Without a Cisco CMX Installation), page 11-20
- Configuring Mobility Express for Notifications and Reports, page 11-24

Configuring Cisco CMX for Notifications and Reports

To enable the Cisco DNA Spaces to send notifications, you must do certain configurations in the Cisco CMX.
Chapter 11 Configuring Cisco Unified Wireless Network (Cisco AireOS) for Cisco DNA Spaces

Configurations for the CMX On Prem Option to work with Cisco DNA Spaces

Note The Cisco DNA Spaces supports Cisco CMX 10.0 or later:

If you are having Cisco CMX 10.6 or later, you can automatically configure Cisco CMX for notification and reports. For more information, see Configuring Cisco CMX for Notification and Reports Using CMX Tethering (For Cisco CMX 10.6 or later), page 11-15.

To manually configure Cisco CMX 10.0 or later for notifications, perform the following steps:

Step 1 Log in to Cisco CMX using the login credentials for your Cisco CMX account.
Step 2 Choose Manage > Notifications.
Step 3 Click New Notification.
Step 4 In the CREATE NEW NOTIFICATION window, perform the following steps:
   a. In the Name field, enter a name for notification.
   b. From the Type drop-down list, choose Location Update.
   c. From the DeviceType drop-down list, choose All.
   d. From the Hierarchy drop-down list, choose All Locations.
   e. From the Receiver drop-down list, choose https, and in the field enter the following details of the Cisco DNA Spaces server:
      - Host address: location.dnaspaces.io
      - Port No: 443
      - URL: notifications/MSE/<customerIdentifier>
   f. Ensure that MAC Scrambling is set to OFF, and the message format is JSON.

Note If you select the DeviceType as All, the Cisco DNA Spaces gets the location updates for all the devices from the Cisco CMX.

Note If you select the Hierarchy as All locations, the Cisco DNA Spaces gets the location updates from all the locations associated with the Cisco CMX.

Note For the EU region, the host address must be location.dnaspaces.eu.

Note Choosing the Receiver as https enables you to secure the location updates sent from your Cisco CMX.

Note The customerIdentifier is customer-specific. To view your customerIdentifier, in the Cisco DNA Spaces dashboard, click the Configure Manually link for a CUWN SSID in the SSIDs window.
**Chapter 11 Configuring Cisco Unified Wireless Network (Cisco AireOS) for Cisco DNA Spaces**

**Configurations for the CMX On Prem Option to work with Cisco DNA Spaces**

---

**Note**

If the MAC Scrambling is set to **ON**, the Cisco Wireless Controller will not send the actual MAC address, and the Cisco DNA Spaces cannot identify the customers.

---

**Note**

Even though the Cisco DNA Spaces receives the location updates for the message format, **XML**, the Cisco DNA Spaces will process the location update data only if the format is **JSON**.

---

**Step 6**

Click **Create** to create the notification.

---

**Configuring Cisco CMX for Notification and Reports Using CMX Tethering (For Cisco CMX 10.6 or later)**

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

You can do CMX Tethering in the following ways:

- CMX Tethering by Manually Uploading the Location Map to Cisco DNA Spaces, page 11-15.
- CMX Tethering by Configuring Token in Cisco CMX, page 11-16.

---

**CMX Tethering by Manually Uploading the Location Map to Cisco DNA Spaces**

---

**Step 1**

Log into Cisco Prime Infrastructure.

**Step 2**

In the **Settings /Getting Started** window, click the circle icon near the top right 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 Upload at the top left of the window, and select the location map downloaded from Cisco Prime Infrastructure.
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 Add a Wireless Network window, under the Add Network by area, click the CMX Tethering radio button.
Step 15 In the Display Name field, enter a name for the CMX node.
Step 16 Click Add.

The locations for the CMX node tethered gets displayed in the location hierarchy.

CMX Tethering by Configuring Token in Cisco CMX

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

Step 1  Generate token in the Cisco DNA Spaces dashboard, and configure Token in the Cisco CMX by following the instructions in the Cisco CMX Configuration Guide.
Step 2  In the Cisco DNA Spaces dashboard, choose Location Hierarchy.
Step 3  Click the More Actions menu at the far right of the root location.
Step 4  Click Add a Wireless Network.
Step 5  From the Wireless Network drop-down list, choose CMX On Prem.
Step 6  In the Add a Wireless Network window, under the Add Network by area, click the CMX Tethering radio button.
Step 7  In the Display Name field, enter a name for the CMX node.
Step 8  Click Add.

The locations for the CMX node tethered gets displayed in the location hierarchy.

Note  When you configure CMX tethering using token, the location map for the particular CMX node appears in the Map Services window of the Cisco DNA Spaces dashboard.
Configuring the Cisco Unified Wireless Network 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>HTTP</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</td>
<td>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 range 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.

Configurations for the WLC Direct Connect Option to work with Cisco DNA Spaces

This configuration is not required if you are using a Cisco CMX installation.

To work with Cisco Unified Wireless Network with Cisco WLC option, you must do certain configurations in the Cisco Wireless Controller so that the Cisco Wireless Controller access points will be imported to the Cisco DNA Spaces. The configurations required to import a Cisco Wireless Controller and its access points varies based on the methods you use. The configurations for various methods are as follows:

- Connecting Cisco Wireless Controller to Cisco DNA Spaces Using Wireless Controller Cloud Connect, page 11-18
- Connecting the WLC to the Cisco DNA Spaces using Cisco DNA Spaces Connector
- Configuring Mobility Express to work with Cisco DNA Spaces, page 11-20
- Configuring eWLC to work with Cisco DNA Spaces, page 11-26
Configurations for the WLC Direct Connect Option to work with Cisco DNA Spaces

Note

If you are using WLC Direct Connect option and if you want to connect 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 Wireless Controller to both Cisco DNA Spaces and Cisco CMX simultaneously.

Note

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.

Connecting Cisco Wireless Controller to Cisco DNA Spaces Using Wireless Controller Cloud Connect

Prerequisites

- You must need Cisco Wireless Controller Version 8.3 or later
- The Cisco Wireless Controller must be able to reach Cisco DNA Spaces cloud over HTTPS.
- To connect the Cisco Wireless Controller to the Cisco DNA Spaces, the internet must be available.
- 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 Wireless Controller Cloud 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 Wireless Controller Version 8.3 or later successfully to the Cisco DNA Spaces using Cisco Wireless Controller Connect, you must have a root certificate issued by DigiCert CA. For more information on importing the DigiCert CA root certificate, see the “Importing the DigiCert CA Root Certificate” section on page 11-19. 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”.

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:

Step 1

In the Cisco Wireless Controller CLI mode, execute the following commands:

1. config cloud-services cmx disable
2. config cloud-services server url https://{Customer Path Key}.{LB Domain} {LB IP Address}
3. config cloud-services server id-token <Customer JWT Token>
4. config network dns serverip <dns server ip>
5. config cloud-services cmx enable
Chapter 11  Configuring Cisco Unified Wireless Network (Cisco AireOS) for Cisco DNA Spaces

Configurations for the WLC Direct Connect Option to work with Cisco DNA Spaces

Note
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 the SSIDs window. You can also contact the Cisco DNA Spaces support team. Ensure that there are no trailing/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.proximitymx.io

IP Address............................. 50.16.12.224

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. For more information on importing the Cisco Wireless Controller and access points to the Cisco Wireless Controller, see the Defining the Location Hierarchy for Cisco Unified Wireless Network with Wireless Controller (without Cisco CMX Installation), page 3-9.

Importing the DigiCert CA Root Certificate

If you try to connect the WLC 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
```

To import the DigiCert CA root certificate to connect the WLC successfully to Cisco DNA Spaces, perform the following steps:

Step 1
Download your root certificate from the following link:


Step 2
Copy the root certificate content to a file with .cer extension, and save the file as {your_filename}.cer.

Step 3
Copy the {your_filename}.cer file to the default directory on your TFTP.

Step 4
Log in to the Cisco Wireless Controller CLI, and execute the following commands:

```
transfer download datatype cmx-serv-ca-cert
```
Chapter 11 Configuring Cisco Unified Wireless Network (Cisco AireOS) for Cisco DNA Spaces

Configuring Mobility Express to work with Cisco DNA Spaces

Step 5
Type Y to start the upload.

Step 6
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
```

Note
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.

You can now configure the Cisco Wireless Controller to connect to Cisco DNA Spaces. For more information on connecting the Cisco Wireless Controller to the Cisco DNA Spaces, see the “Connecting Cisco Wireless Controller to Cisco DNA Spaces Using Wireless Controller Cloud Connect” section on page 11-18.

Configuring Cisco Unified Wireless Network with Cisco Wireless Controller for Notifications and Reports (Without a Cisco CMX Installation)

Note
If you are using Cisco DNA Spaces with the WLC Direct Connect option, the Cisco Wireless Controller must be in “Foreign controller” mode.

For the wireless network option, WLC Direct Connect, the configurations required for notifications and reports will be done automatically when you import the Cisco Wireless Controller.

For more information about how to import the Cisco Wireless Controller and its access points, see the “Configurations for the WLC Direct Connect Option to work with Cisco DNA Spaces” section on page 11-17.

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 (ME) versions are different. The configurations for various ME versions are as follows:

- Configuring Mobility Express 8.7 or Later for Cisco DNA Spaces, page 11-21
- Configuring Mobility Express 8.6 orEarlier for Cisco DNA Spaces, page 11-25
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:

1. Creating SSIDs in the Mobility Express, page 11-21
2. Configuring RADIUS Authentication in Mobility Express 8.7 or Later, page 11-22
3. Creating Access Control Lists in Mobility Express 8.7 or Later, page 11-22
4. Configuring Mobility Express 8.7 or Later for Social Authentication, page 11-23
5. Allowing the URLs in the Mobility Express 8.7 or Later, page 11-24
6. Configuring Mobility Express for Notifications and Reports, page 11-24

Creating SSIDs in the Mobility Express

To create SSIDs in the Mobility Express, perform the following steps:

Step 1 Log in to ME 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
Chapter 11 Configuring Cisco Unified Wireless Network (Cisco AireOS) for Cisco DNA Spaces

Configuring Mobility Express to work with Cisco DNA Spaces

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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Log in to ME with your credentials.</td>
</tr>
<tr>
<td>2</td>
<td>In the ME main window, click <strong>Switch to Expert View</strong> in the top right of the window.</td>
</tr>
<tr>
<td>3</td>
<td>In the pop up window that appears, select <strong>OK</strong>.</td>
</tr>
<tr>
<td>4</td>
<td>In the left pane, click <strong>Management &gt; Admin Accounts</strong>.</td>
</tr>
<tr>
<td>5</td>
<td>In the window that appears, click the <strong>Radius</strong> tab.</td>
</tr>
<tr>
<td>6</td>
<td>Click <strong>Add RADIUS Authentication Server</strong>. In the <strong>Add/ Edit Radius Authentication Server</strong> window appears, enter the following radius server details:</td>
</tr>
<tr>
<td></td>
<td>a. In the <strong>Server IP Address</strong> field, enter the IP address of the radius server.</td>
</tr>
<tr>
<td></td>
<td>b. In the <strong>Shared Secret</strong> field, enter your radius secret key.</td>
</tr>
<tr>
<td></td>
<td>c. In the <strong>Confirm Shared Secret</strong> field, re-enter the radius secret key.</td>
</tr>
<tr>
<td>7</td>
<td>Click <strong>Apply</strong>.</td>
</tr>
<tr>
<td>8</td>
<td>In the ME main window, click <strong>Wireless Settings</strong> in the left pane.</td>
</tr>
<tr>
<td>9</td>
<td>Click <strong>WLANs</strong>. The <strong>WLAN/RLAN Configuration</strong> window appears with the SSIDs list.</td>
</tr>
<tr>
<td>10</td>
<td>Click the <strong>Edit</strong> icon for the SSID created previously.</td>
</tr>
<tr>
<td>11</td>
<td>In the <strong>Edit WLAN</strong> window that appears, click the <strong>WLAN Security</strong> tab.</td>
</tr>
<tr>
<td>12</td>
<td>From the <strong>Access Type</strong> drop-down list, choose <strong>Radius</strong>.</td>
</tr>
<tr>
<td>13</td>
<td>Click the Radius Server tab, and click <strong>Add RADIUS Authentication Server</strong>.</td>
</tr>
<tr>
<td>14</td>
<td>From the <strong>Server IP Address</strong> drop-down list, select your Radius Server, and click <strong>Apply</strong>.</td>
</tr>
<tr>
<td>15</td>
<td>In the <strong>Edit WLAN</strong> window, click <strong>Apply</strong>. Now the Mobility Express 8.7 or later is configured for radius server authentication.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Log in to ME with your credentials.</td>
</tr>
<tr>
<td>2</td>
<td>In the ME main window, click the Wireless Settings in the left pane.</td>
</tr>
<tr>
<td>3</td>
<td>Click <strong>WLANs</strong>. The <strong>WLAN/RLAN Configuration</strong> window appears with the SSIDs list.</td>
</tr>
<tr>
<td>4</td>
<td>Click the <strong>Edit</strong> icon for the SSID created previously. In the <strong>Edit WLAN</strong> window that appears, click the <strong>WLAN Security</strong> tab.</td>
</tr>
<tr>
<td>5</td>
<td>Click the <strong>Pre Auth ACLs</strong> tab.</td>
</tr>
</tbody>
</table>
**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>Destination Port Range</th>
<th>DSCP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permit</td>
<td>34.235.248.212/255.255.255.2/255.255.255.255</td>
<td>0.0.0.0/0.0.0.0</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>34.235.248.212/255.255.255.255</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
</tr>
<tr>
<td>Permit</td>
<td>52.55.235.39/255.255.255.255</td>
<td>0.0.0.0/0.0.0.0</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>52.55.235.39/255.255.255.255</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 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.

In the Edit WLAN window that appears, click the WLAN Security tab.

**Step 5** Click the Pre Auth ACLs tab.
Chapter 11 Configuring Cisco Unified Wireless Network (Cisco AireOS) for Cisco DNA Spaces

Configuring Mobility Express to work with Cisco DNA Spaces

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>
<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>

**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:

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:
   1. `config cloud-services cmx disable`
   2. `config cloud-services server url https://{Customer Path Key}.{LB Domain} {LB IP Address}`
   3. `config cloud-services server id-token {Customer JWT Token}`
4. config network dns serverip <dns server ip>
5. config cloud-services cmx enable

---

**Note**

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:

```shell
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.proximitymx.io
IP Address.................................... 50.16.12.224
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 importing to the Cisco DNA Spaces location hierarchy. For more information on importing the Cisco Wireless Controller and its access points, see the Defining the Location Hierarchy for Cisco Unified Wireless Network with Wireless Controller (without Cisco CMX Installation), page 3-9

**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, page 11-25
- Configuring RADIUS Authentication for Mobility Express 8.6 or Earlier, page 11-26
- Creating ACLs for Mobility Express 8.6 or Earlier, page 11-26
- Configuring Mobility Express for Notifications and Reports, page 11-24

**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 ME 8.7 or later. To know the configuration steps, see the Creating SSIDs in the Mobility Express, page 11-21.
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 ME with your credentials.
Step 2 In the ME 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:
   d. In the Server IP Address field, enter the IP address of the radius server.
   e. In the Shared Secret field, enter your radius secret key.
   f. In the Confirm Shared Secret field, re-enter the radius secret key.
   g. Click Apply.
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 “Cisco 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, see the Defining the Location Hierarchy for Cisco Unified Wireless Network with Wireless Controller (without Cisco CMX Installation), page 3-9.

Configuring eWLC to work with Cisco DNA Spaces

Note

The certified eWLC Version is 16.10.20181030.

To configure eWLC to work with Cisco DNA Spaces, perform the following steps:
Step 1  In the Cisco DNA Spaces dashboard, configure a Cisco Unified Wireless Network (Cisco AireOS) SSID. For more information on configuring the SSIDs, see the “Importing the SSIDs for Cisco Unified Wireless Network” section on page 4-42.

Note  You can define any name for the SSID. You must use the same SSID name when configuring the eWLC.

Step 2  On eWLC, 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, choose Home, and click the Captive Portal app. Click SSIDs, and then click the Configure Manually link for the CUWN/AireOS 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 eWLC controller.

Step 5  Configure ACL to allow traffic in webauth state.
```
ip access-list extended <ACL Name>
  permit ip any host <IP address>
  permit ip host <IP address> any
  permit ip any host <IP address>
  permit ip host <IP address> any
  permit udp any eq bootps any
```
permit udp any any eq bootpc
permit udp any eq bootpc any
permit udp any eq domain any
permit udp any any eq domain

Note To view the IP address, in the Cisco DNA Spaces dashboard, choose Home, and click the Captive Portal app. Click SSIDs, and then click the Configure Manually link for the Cisco Unified Wireless Network (Cisco AireOS) SSID created in Step 1. Click the Configure SSID in CUWN-WLC tab. The IP address will be listed in the Creating the Access Control List section. You can also contact the Cisco DNA Spaces support team.

Step 6 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 *.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
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 *.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 <ACL Name>
urlfilter list social_login_fqdn_flex
description "default flex profile"

Step 7 Configure Accounting.

aaa new-model
aaa group server radius ISE
    server name ISE
    subscriber mac-filtering security-mode mac
    mac-delimiter colon
aaa accounting identity default start-stop group radius
radius server ISE
    address ipv4 <IP address> auth-port <port> acct-port <port>
    key secret-key
aaa session-id common
radius-server attribute wireless accounting call-station-id ap-macaddress-ssid
wireless profile policy default-policy-profile
accounting-list default

Note To view the IPv4 IP address and port for radius server configuration, in the Cisco DNA Spaces dashboard, choose Home, and click the Captive Portal app. Click SSIDs, and then click the Configure Manually link for the Cisco Unified Wireless Network (Cisco AireOS) SSID created in Step 1. Click the Configure SSID in CUWN-WLC tab. The radius server details will be listed in the Radius Server Configuration section. You can also contact the Cisco DNA Spaces support team.

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 eWLC.

ip name-server <dns_ip_address>
ip domain-lookup
ip route 0.0.0.0 0.0.0.0 <default_gw_ip_addr>

Step 10 Execute the following command to download trusted root CAs including the root CA from Cisco DNA Spaces.


Step 11 Configure Cisco CMX Cloud on eWLC for sending location updates to Cisco DNA Spaces.
Chapter 11 Configuring Cisco Unified Wireless Network (Cisco AireOS) for Cisco DNA Spaces

Configuring Mobility Express to work with Cisco DNA Spaces

```
nmsp cloud-services server url
nmsp cloud-services server token
nmsp cloud-services enable
```

**Note**  To view the NMSP server token and server URL, in the Cisco DNA Spaces dashboard, choose Home, and click the Captive Portal app. click SSIDs, and then click the Configure Manually link for the Cisco Unified Wireless Network (Cisco AireOS) SSID created in Step 1. You can find the NMSP server token and server URL in the Configure SSID in CUWN-WLC tab. Ensure to copy URL alone as eWLC won’t accept IP address.

**Step 12**  To know the status, execute the following command:
```
show nmsp cloud-services summary
```

**Sample Summary**
```
veWLC_A#show nmsp cloud-services summary
CMX Cloud-Services Status
-----------------------------
Server : https://polarisred.ciscospaces.io
IP Address : 64.103.36.133
CMX Service : Enabled
Connectivity : https: UP
Service Status : Active
Last Request Status : HTTP/1.1 200 OK
Heartbeat Status : OK
```

You can now import the Cisco Wireless Controller and APs to the location hierarchy, using the CUWN-WLC option. For more information, see the “Defining the Location Hierarchy for Cisco Unified Wireless Network with Wireless Controller (without Cisco CMX Installation)” section on page 3-9.

You can then import the SSIDs to Cisco DNA Spaces, and configure captive portals for SSIDs using the Captive Portal Rule.

---

**Configuring eWLC(GUI) to work with Cisco DNA Spaces**

**Note**  The certified eWLC Version is 16.10.1E and 16.10.11.

To configure eWLC to work with Cisco DNA Spaces, perform the following steps:

**Step 1**  In the Cisco DNA Spaces dashboard, configure a Cisco Unified Wireless Network (Cisco AireOS) SSID. For more information on configuring the SSIDs, see the “Importing the SSIDs for Cisco Unified Wireless Network” section on page 4-42.

**Step 2**  Create the Parameter Map.

  a. Log into eWLC.

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 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, choose Home, and click the Captive Portal app. Click SSIDs, and then click the Configure Manually link for the CUWN/AireOS 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 AireOS SSID.

i. Click Update and Apply.

---

**Step 3** Install the web-auth certificate and configure the global parameter map.

**Note** You must have a valid SSL certificate for the virtual IP/Domain installed in eWLC controller. You can purchase any wild card certificate.

a. Convert the certificate into pkcs12.

   The file format will be .p12.

b. Copy the file into the tftp server.

c. In the eWLC dashboard, choose Configuration > Security > Web Auth.

d. Click the parameter map name, global.

e. On the General tab, from the Type drop-down list, choose webauth.

f. Specify virtual IPv4 address (virtual IP) or virtual IPv4 Host name (domain) in the respective field.

g. Click Update & Apply.

h. Download the certificate using the following steps:

   - In the eWLC CLI, enter the following command:

```bash
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.

i. To verify the installed certificate, in the eWLC dashboard, choose `Configuration > Web Auth > Certificate`.

The downloaded certificate appears as the last certificate in the list.

j. To map the installed certificate with `webauth` parameter map, in the eWLC 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).

k. Reload eWLC.

Step 4 Create the ACL.

a. Choose `Configuration > Security > ACL`.

b. In the `Access Control List` window that appears, click `Add`.

c. In the `ACL Name` field, enter a name for the ACL.

d. From the `ACL Type` drop-down list, choose `IPv4 Extended`.

e. In the `Sequence` field, enter the required sequence.

f. From the `Source Type` drop-down list, choose `Host`.

g. In the `Host Name` field that appears, enter an Cisco DNA Spaces IP address to be allowed.

h. From the `Destination Type` drop-down list, choose `any`.

i. From the `Protocol` drop-down list, choose `ip`.

j. Click `Add`.

k. Enter a Sequence.

Note You can specify any number in the sequence field.

l. Select `Source Type` as `any`.

m. Select `Destination Type` as `Host`.

n. In the `Host Name` field that appears, enter an Cisco DNA Spaces IP address to be allowed.

o. Select `Protocol` as `ip`.

p. Click `Add`.

The added ACL rules appear as rows in the grid at the bottom of the window.

Note For more information on the IPs to be allowed, in the Cisco DNA Spaces dashboard, click the `Configure Manually` link for a CUWN SSID in the `SSIDs` window.

q. Repeat the steps for all the Cisco DNA Spaces IPs that need to be allowed.
r. Configure an ACL rule. Each row in the following table represents the values for an ACL rule.
s. After adding the values for a rule, click Add.
The added rule gets displayed in the grid,
t. Similarly, create the remaining ACL rules.

Table 2  

<table>
<thead>
<tr>
<th>Sequence</th>
<th>Action</th>
<th>Source Type</th>
<th>Destination Type</th>
<th>Protocol</th>
<th>Source Port</th>
<th>Select Port</th>
<th>Dest Port</th>
<th>Select Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Permit</td>
<td>any</td>
<td>any</td>
<td>udp</td>
<td>eq</td>
<td>bootps</td>
<td>None</td>
<td>NA</td>
</tr>
<tr>
<td>2</td>
<td>Permit</td>
<td>any</td>
<td>any</td>
<td>udp</td>
<td>None</td>
<td>NA</td>
<td>eq</td>
<td>bootps</td>
</tr>
<tr>
<td>3</td>
<td>Permit</td>
<td>any</td>
<td>any</td>
<td>udp</td>
<td>eq</td>
<td>bootpc</td>
<td>None</td>
<td>NA</td>
</tr>
<tr>
<td>4</td>
<td>Permit</td>
<td>any</td>
<td>any</td>
<td>udp</td>
<td>None</td>
<td>NA</td>
<td>eq</td>
<td>bootpc</td>
</tr>
<tr>
<td>5</td>
<td>Permit</td>
<td>any</td>
<td>any</td>
<td>udp</td>
<td>eq</td>
<td>domain</td>
<td>None</td>
<td>NA</td>
</tr>
</tbody>
</table>

Note  The Select Port drop-down list appears for Source Port or Destination Port when you select the value eq. If Port is None, Select Port is not applicable.

u. Click Update & Apply to Device.
v. Add splash page domain in URL filters.
   1. Choose Configuration > Security > URL Filters.
   2. In the URL Filters window, click Add.
   3. In the List Name field, enter the list name.
   4. Change the status of Action to Permit.
   5. In the URLs field, enter the splash page domain.
   6. Choose Configuration > Tags & Profiles > Policy.
   7. In the Policy Profile window, click default-policy-profile.
   8. In the Edit Policy Profile window, click the Access Policies tab.
   9. In the URL Filters area, from the Pre Auth drop-down list, choose the previously created ACL.
   10. Click Update & Apply to Device.

Step 5  Create the SSID.

a. Choose Configuration > Tags & Profiles > WLANs.
b. Click Add.
c. On the General tab, in the Profile Name field, enter the profile name.
d. In the SSID field, enter the SSID name defined at Step 1.
e. Set the status as Enabled.
f. Click the Security tab, and then click the Layer2 tab.
g. From the **Layer 2 Security Mode** drop-down list, choose **None**.

h. Click the **Layer3** tab.

i. Check the **Web Policy** check box.

j. From the **WebAuth Parameter Map** drop-down list, choose the Web Auth Parameter Map created at step 1.

k. Click **Show Advanced Settings**.

l. In the “**Preauthentication ACL**" area, from the **IPv4** drop-down list, choose the ACL created at step 2.

m. Click **Save & Apply to Device**.

---

**Note**
The above is the basic eWLC configuration. You have to do the following configurations for radius server or social authentication only if there are required.

**Step 6** Configure the Radius Server.

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.

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**.

---

**Note**
The server added will be available in **Available Server** 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**.

r. In the **Method List Name** field, enter the method list name.

s. From the **Type** drop-down list, choose **Login**.

t. From the **Group Type** drop-down list, choose **Group**.

u. Move the server group created earlier (**steps j to Step o**) from **Available Server Groups** to **Assigned Servers Groups**.
v. the AAA Method List tab, click Authorization, and click Add.
w. In the Method List Name field, enter the method list name.
x. From the Type drop-down list, choose Network.
y. From the Group Type drop-down list, choose group.
z. Move the server group previously created from Available Servers to Assigned Servers using the arrow button, and click Save & Apply to Device.

Step 7 Configure Social Authentication.

Note This configuration is required only if you want to manage customer authentication through the social sites Facebook, Twitter, or LinkedIn.

a. Choose Configuration > Security > URL Filters.
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 following URLs.
   • *.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 & 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 8 Enable L2 authentication (Mac Filtering).
Note Make sure **Type** is selected as **webauth** in parameter-map for Radius Authentication.

a. Choose **Configuration > Tags & Profiles > WLANs.**
b. Click the SSID for which you want to configure L2 Authentication.
c. In the **Edit WLAN** window, click the **Security** tab.
d. On the **Layer2** tab, to enable Mac Filtering, check the **MAC Filtering** check box.
e. From the **Authorization List** drop-down list that appears, choose the authorization server created previously.
f. In the **Layer3** tab, from the **Authorization List** drop-down list that appears, choose the authorization server created previously.
g. Click **Show Advanced Settings.**
h. Check the **On Mac Filter Failure** check box.
i. Click **Update & Apply to Device.**
j. Choose **Configuration > Tags & 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.**

Note To configure L2 authentication, ensure that you have created the SSIDs and have done all the configurations in step 3.

You can now import the Cisco Wireless Controller and APs to the location hierarchy, using the CUWN-WLC option. For more information, see the “Defining the Location Hierarchy for Cisco Unified Wireless Network with Wireless Controller (without Cisco CMX Installation)” section on page 3-9.

You can then import the SSIDs to Cisco DNA Spaces, and configure captive portals for SSIDs using the Captive Portal Rule.
Configuring Cisco Meraki for Cisco DNA Spaces

This chapter describes the configurations required in Cisco Meraki for using Cisco DNA Spaces.

- Enabling SSIDs in Cisco Meraki, page 12-1
- Configuring Cisco Meraki for RADIUS Authentication, page 12-2
- Configuring Cisco Meraki for Notifications and Reports, page 12-4
- Configurations Required in Cisco Meraki for Location Manager, page 12-4
- Configuring Cisco Meraki for Social Authentication, page 12-5
- Manually Configuring SSIDs for Cisco Meraki, page 12-6

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), page 12-2
- Configuring Cisco Meraki for RADIUS Authentication and Seamless Internet Provisioning, page 12-3

Configuring Cisco Meraki for RADIUS Authentication (Without Seamless Internet Configurations)

To configure Cisco Meraki for radius authentication, perform the following steps:

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 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 **Mac-based access control (no encryption)**.

**Step 5** In the Splash page area, choose **Click-through**.

**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. 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 CMS 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.

Configurations Required in Cisco Meraki for Location Manager

Before using the Cisco DNA Spaces dashboard for managing locations, the location Manager must do certain configurations in the Cisco Meraki dashboard.

To work as a location manager, in the Cisco Meraki dashboard, perform the following steps:
**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 configure the social authentication.

**Step 3** In the Walled 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>
</tr>
</thead>
<tbody>
<tr>
<td>Facebook</td>
</tr>
<tr>
<td>*facebook.com</td>
</tr>
<tr>
<td>*.fbcdn.net</td>
</tr>
<tr>
<td>*.akamaihd.net</td>
</tr>
<tr>
<td>*.connect.facebook.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 on page 4-42.

To configure the SSID manually in Cisco Meraki, perform the following steps:

Step 1 Log in to Cisco Meraki using the credentials for your Meraki account.

Step 2 Choose the required Cisco Meraki organization and network from the respective drop-down list.

Step 3 Choose Wireless > Access Control.

Step 4 From the SSID drop-down list, choose the SSID that you want to configure for the Cisco DNA Spaces.

Step 5 In the splash page area, choose Click-through.

Step 6 From the Wall garden drop-down list, choose Wall garden is enabled.

Step 7 In the Wall garden ranges field, enter the required 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 window.

Step 8 Click Save Changes.

Step 9 Go to 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.