Cisco DNA Spaces コンフィギュレーションガイド

初版：2018 年 12 月 18 日

最終更新：2021 年 11 月 29 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

はじめに

ここでは、このマニュアルの対象読者、構成、および使用されている表記法について説明します。

（注） この製品のマニュアルセットは、偏向のない言語を使用するように配慮されています。このドキュメントセットでの偏向のない言語とは、年齢、障害、性別、人種的アイデンティティ、民族的アイデンティティ、性的指向、社会経済的地位、およびインターセクショナリティに基づく差別を意味しない言語として定義されています。製品ソフトウェアのユーザインターフェイスにハードコードされている言語、基準ドキュメントに基づいて使用されている言語、または参照されているサードパーティ製品で使用されている言語によりドキュメントに例外が存在する場合があります。

このマニュアルの構成は、次のとおりです。

対象読者

このガイドは、Cisco Digital Network Architecture（DNA）Spaces のユーザーアカウントを管理し、Cisco DNA Spaces に必要な設定を行うアカウント管理者を対象としています。また、このガイドは、Cisco DNA Spaces を使用してプロキシミティルールを作成し、顧客やビジネスユーザーに通知を送信する事業および店舗の管理者も対象としています。

その他の対象者には、ポータルデザイナーとアクセスコードマネージャが含まれます。

マニュアルの構成

章番号	章タイトル	説明
第 1 章	**Cisco DNA Spaces の前提条件**	Cisco DNA Spaces のさまざまな機能と、Cisco DNA Spaces を展開するための前提条件に関する情報を提供します。
第 2 章	**使用する前に**	Cisco DNA Spaces とその機能の概要を説明します。この章では、プロセスフロー、システム要件、および Cisco DNA Spaces の使用を開始する方法についても説明します。
第 3 章	**Cisco DNA Spaces におけるロケーション階層**	Cisco DNA Spaces のロケーション階層を定義する方法に関する情報を提供します。
第 4 章	**行動メトリクス**	行動メトリクスレポートに関する情報を提供します。
第 5 章	**位置分析**	ロケーション分析レポートの表示方法に関する情報を提供します。
第 6 章	**影響分析**	Impact Analysis アプリの使用に関する情報を提供します。
第 7 章	**Right Now**	Right Now アプリの使用に関する情報を提供します。
第 8 章	**カメラメトリック**	Meraki カメラのレポートに関する情報を提供します。
第 9 章	**Captive Portal アプリの使用**	キャプティブポータルを作成する方法、SMS ゲートウェイなどのサポート機能を構成する方法、およびキャプティブポータルルールを使用してキャプティブポータルを表示する方法について説明します。

章番号	章タイトル	説明
第 10 章	**Engagements** アプリによる通知の送信	顧客およびビジネスユーザーに通知を送信するために定義するエンゲージメントルールについて説明します。
第 11 章	**Location Personas** アプリによるタグの作成	タグの作成または既存タグの修正をするために定義するプロファイルルールについて説明します。
第 12 章	**Cisco DNA Spaces Asset Locator** アプリの使用	Asset Locator アプリの概要を説明します。
第 13 章	モニターリング	[Monitoring] セクションに表示されるアプリの詳細に関する情報を提供します。
第 14 章	**Cisco DNA Spaces** のユーザーとアカウントの管理	Cisco DNA Spaces ユーザー、Cisco DNA Spaces アカウント、および Cisco Connected Mobile Experiences（CMX）アカウントの管理方法に関する情報を提供します。
第 15 章	ワイヤレスネットワークのセットアップ	Cisco DNA Spaces を使用するために必要なセットアップについて説明します。
第 16 章	**Cisco DNA Space** におけるシスコ ワイヤレス コントローラおよび **Cisco Catalyst 9800** シリーズ コントローラの設定	Cisco DNA Spaces を使用するためにシスコ ワイヤレス コントローラおよび Cisco Catalyst 9800 シリーズ コントローラに必要な設定について説明します。
第 17 章	**Cisco DNA Spaces** を使用するための **Cisco Meraki** の設定	Cisco DNA Spaces を使用するために Cisco Meraki に必要な設定について説明します。
第 18 章	統合	Cisco DNA Center と Service Now アプリケーションを統合する方法について説明します。

章番号	章タイトル	説明
第 19 章	**セットアップ**	ワイヤレスネットワークと Meraki カメラのセットアップ方法について説明します。

表記法

このマニュアルでは、以下の表記法を使用しています。

表 *1:* 表記法

表記法	説明
太字	コマンド、コマンドオプションおよびキーワードは太字で示しています。
イタリック体	ユーザーが値を指定する引数は、イタリック体で示しています。
[Option] > [Option]	一連のメニュー オプションを説明するときに使用します。

（注） 「注釈」です。役立つ情報や、このドキュメント以外の参照資料などを紹介しています。

ヒント 読者に提供されるヒントを意味します。ヒントには、問題の解決に役立つ提案が含まれています。

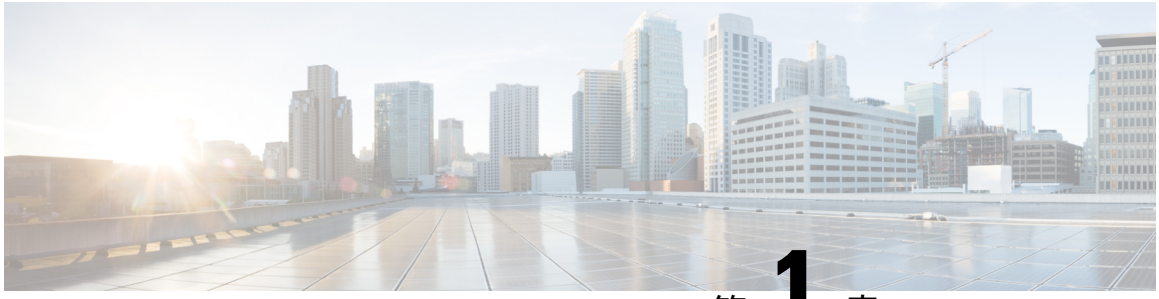
略語の一覧

表 *2:* 略語の一覧

略語	説明
ACL	Access Control List
BLE	Bluetooth Low Energy
CUWN	Cisco Unified Wireless Network
CNA	Captive Network Assistant

略語	説明
RSSI	受信信号強度インジケータ
SSID	Service Set Identifier
UUID	汎用一意識別子

はじめに



第 1 章

Cisco DNA Spaces の前提条件

この章では、Cisco Digital Network Architecture（DNA）Spaces のシステム要件、Cisco DNA Spaces を展開するための帯域幅要件、および Cisco DNA Spaces のポートと IP アドレスについて説明します。この章は、次の項で構成されています。

システム要件

次の表に、Cisco DNA Spaces のシステム要件を示します。

表 *3*:

項目	システム要件
オペレーティング システム	• Microsoft Windows XP 以降 • Mac OS X 10.6 以降
ブラウザ	Windows OS • Firefox バージョン 30 以降 • Chrome バージョン 34 以降 • Safari バージョン 5.1.7 以降 Mac OS • Firefox バージョン 30 以降 • Chrome バージョン 34 以降 • Safari バージョン 5.1.7 以降

項目	システム要件
シスコ ワイヤレス コントローラ	8.3 以降
Cisco Connected Mobile Experiences（CMX）：これは、Cisco CMX と一緒に使用される Cisco AireOS/Catalyst コントローラにのみ必要です。	10.6 以降
Cisco DNA Spaces コネクタ（Cisco AireOS/Catalyst コントローラにのみ適用）	• vCPU：2/4/8 • RAM：4/8/16 GB • ハードディスク：60 GB

Cisco DNA Spaces を展開するための帯域幅要件

次の表は、ロケーション情報の更新を送信するための Cisco DNA Spaces コネクタおよび Cisco Wireless Controller Direct Connect のインターネット帯域幅要件を示しています。

表 *4:* ロケーション情報更新の帯域幅要件

テスト データ	タイプ	必要な帯域幅
5000 台の AP 60000 台のクライアント	Cisco Wireless Controller Direct Connect	250 Kbps
5000 台の AP 60000 台のクライアント	Cisco DNA Spaces コネクタ	4 Mbps

アクセス可能なポートと IP アドレス

Cisco DNA Spaces はクラウドベース ソリューションであり、物理的な設置作業は必要ありません。そのため、Cisco Meraki などのクラウドベースのワイヤレスネットワークに Cisco DNA Spaces を展開するためのポートを開く必要はありません。クラウドベースではない Cisco AireOS や Cisco Catalyst などの一部のネットワークの場合は、ワイヤレスネットワークと Cisco DNA Spaces の間の接続を確立するためのポートを開く必要があります。この接続は、パブリック IP または VPN により確立することができます。加えて、お客様のインフラストラクチャで特定の Cisco DNA Spaces IP アドレスを許可する必要があります。許可される IP アドレスの詳細については、Cisco DNA Spaces IP アドレスの許可 （3 ページ）を参照してください。デフォルトの Cisco Unified Wireless Network インストールでは、ポート 80 とポート 443 が開かれ、パブリックアクセスが可能になっている必要があります。

Cisco DNA Spaces と Cisco CMX との接続を確立する必要がある次のシナリオでは、Cisco CMX へのパブリックアクセスが可能になっている必要があります。

- Cisco CMX への接続
- ロケーションおよびアクセス ポイントのインポート
- Cisco CMX マップの表示
- Cisco DNA Spaces レポートの表示

Cisco DNA Spaces IP アドレスの許可

Cisco DNA Spaces と Cisco AireOS/Cisco Catalyst（シスコ ワイヤレス コントローラ/Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ）間の接続を確立するには、ネットワーク インフラストラクチャで特定の Cisco DNA Spaces IP アドレスを許可する必要があります。許可する必要のある IP アドレスを表示するには、Cisco DNA Spaces ダッシュボードで、キャプティブポータルアプリからアクセスできる SSID ウィンドウの [Configure Manually] リンクをクリックします。

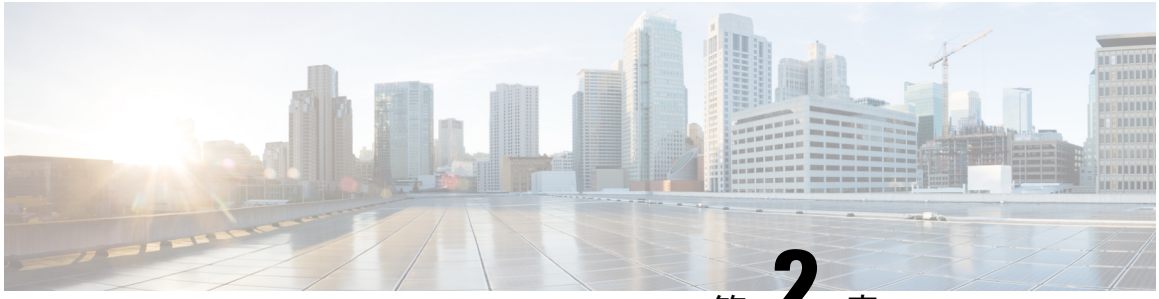
VPN 接続の確立については Cisco DNA Spaces サポートチームにお問い合わせください。

（注） Cisco DNA Spaces に接続するのに、パブリックに解決可能なドメイン名は必要ありません。

お客様のネットワークに展開された Cisco CMX インスタンスが Cisco DNA Spaces の分析および通知サーバーと通信できるようにするには、お客様のインフラストラクチャで特定のドメイン名も許可する必要があります。許可する必要があるドメイン名を確認するには、Cisco DNA Spaces ダッシュボードで、SSID ウィンドウの [Configure Manually] リンクをクリックします。

Cisco DNA Spaces 互換性マトリクス

アプリケーション	AireOS コントローラ	Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	Cisco 組み込みワイヤレスコントローラ（EWC）	3375 アプライアンス	Cisco Prime/Cisco DNA Center
Cisco DNA Spaces（検出と位置特定、キャプティブポータル、エンゲージメント、ロケーションペルソナ、行動メトリクスの各機能を搭載）	• シスコ ワイヤレス コントローラ ネイティブ クラウド コネクタ：8.3 以降（Presence 用の 8.3.102 を除く） • Cisco DNA Spaces コネクタ：8.0.119 以降	16.10 以降	16.11.1s 以降	NA	マップ用は 3.0 以降 （注） シスコ組み込みワイヤレスコントローラのマップに対する Cisco Prime のサポートはありません。



第 2 章

使用する前に

この章では、Cisco Digital Network Architecture（DNA）Spaces の概要、その機能、プロセスフロー、ライセンスパッケージ、およびCisco DNA Spaces のシステム要件について説明します。

この章は、次の項で構成されています。

Cisco DNA Spaces の概要

Cisco DNA Spaces は、物理的なビジネス拠点にいる訪問者を把握し、訪問者に接続し関与することを可能にするマルチチャネルエンゲージメントプラットフォームです。小売、製造、サービス業、医療、教育、金融、エンタープライズワークスペースなど、さまざまな業種のビジネスを対象としています。Cisco DNA Spaces は、施設内の資産を監視および管理するためのソリューションも提供します。

Cisco DNA Spaces の主な機能は次のとおりです。

- 訪問者の関与、資産とリソース、およびビーコンを管理するための共通プラットフォーム。
- 1 つの設定セクションですべてのプラットフォーム設定の完了が可能。
- SSID に接続している顧客へのプロモーションやオファーの表示をサポート。

- ルールを使用した、ロケーション、タグ、訪問頻度、滞在時間などに基づく、顧客に対する個別の、またはグループとしてのターゲティングをサポート。
- 複数のワイヤレスネットワークとの同時連携をサポート。
- ビジネスパフォーマンスの表示に向けたプロビジョニング。
- キャプティブポータルを作成し、ルールに基づいて顧客に表示するためのアプリ。
- 顧客がお客様の事業施設内にいるときに顧客に通知を送信するアプリ。
- 顧客がお客様の事業施設の近くにいるときに従業員に知らせるアプリ。
- 顧客をグループ化し、タグを作成するアプリ。
- サードパーティのパートナーアプリを追加するためのプロビジョニング。
- ワイヤレスネットワークと同じ構造でのロケーション階層のインポートをサポート。
- さまざまな権限とロケーションアクセス権を持つCisco DNA Spacesユーザーを作成するためのプロビジョニング。
- Cisco DNA Spaces とそのアプリおよび遅延のパフォーマンスステータスを監視するためのプロビジョニング。

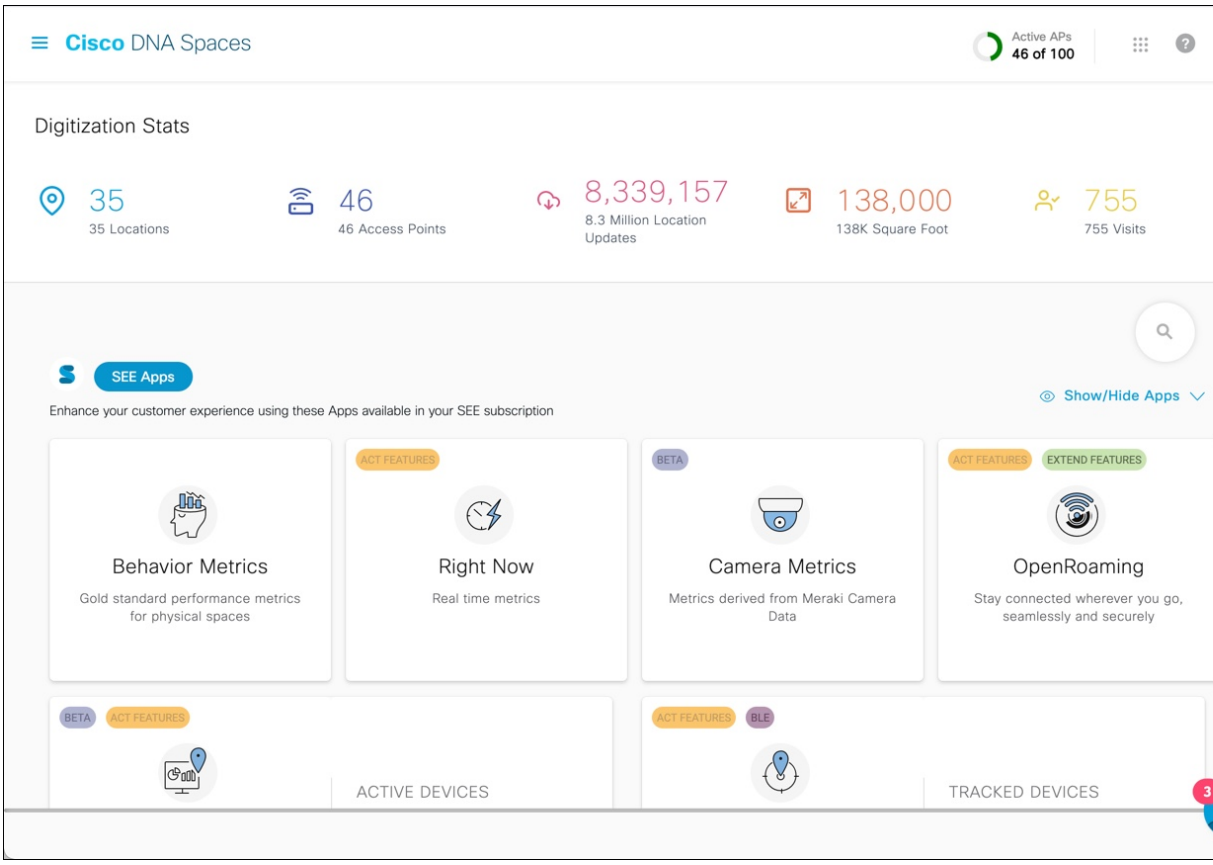
ABC ショッピング モールでは、無料の Wi-Fi を利用するために、顧客はモールに入ってから SSID に接続する必要があります。ABC は、顧客の購入履歴や訪問頻度に基づき、Wi-Fi に接続する各顧客にパーソナライズされたエクスペリエンスを提供したいと考えました。Cisco DNA Spaces をインストールすることで、ABC は、キャプティブポータルを介して Wi-Fi ユーザーに関する詳細を収集し、この詳細を利用して、利用可能なオファーやサービスについての通知を顧客に送信することが可能になりました。Wi-Fi に一度接続された顧客はキャプティブ ポータルに誘導され、ここで、名前、電子メールアドレス、電話番号などの詳細を入力して登録するオプションが示されます。キャプチャされたこの情報は、Cisco DNA Spaces に保存されます。顧客がモールを再び訪問すると、SMS、電子メールを使用して顧客にプロモーションオファーが送信されます。

またCisco DNA Spacesは、顧客のアクティビティについて、従業員などのビジネスユーザーに通知するように設定することもできます。たとえば、Cisco DNA Spaces ダッシュボードで、リピート客をプラチナメンバーとして特定しタグ付けすることができます。プラチナの顧客がレストランに入り、顧客のデバイスがワイヤレスアクセスポイントによって検出されると、レストランの担当者がデバイスでアラートを受信します。これにより、顧客にパーソナライズされたサービスを提供することができます。

Cisco DNA Spaces ダッシュボード

次の図に、Cisco DNA Spaces にログインした後に表示されるダッシュボードの外観を示します。

図 *1 : Cisco DNA Spaces* ダッシュボード



Cisco DNA Spaces の機能

Cisco DNA Spaces の主な機能は次のとおりです。

デジタル化に関する統計情報

Cisco DNA Spaces ダッシュボードのホームページでは、次の累積統計値がページの上部に表示されます。[Digitization Stats] セクションを 1 つの行として表示できます。

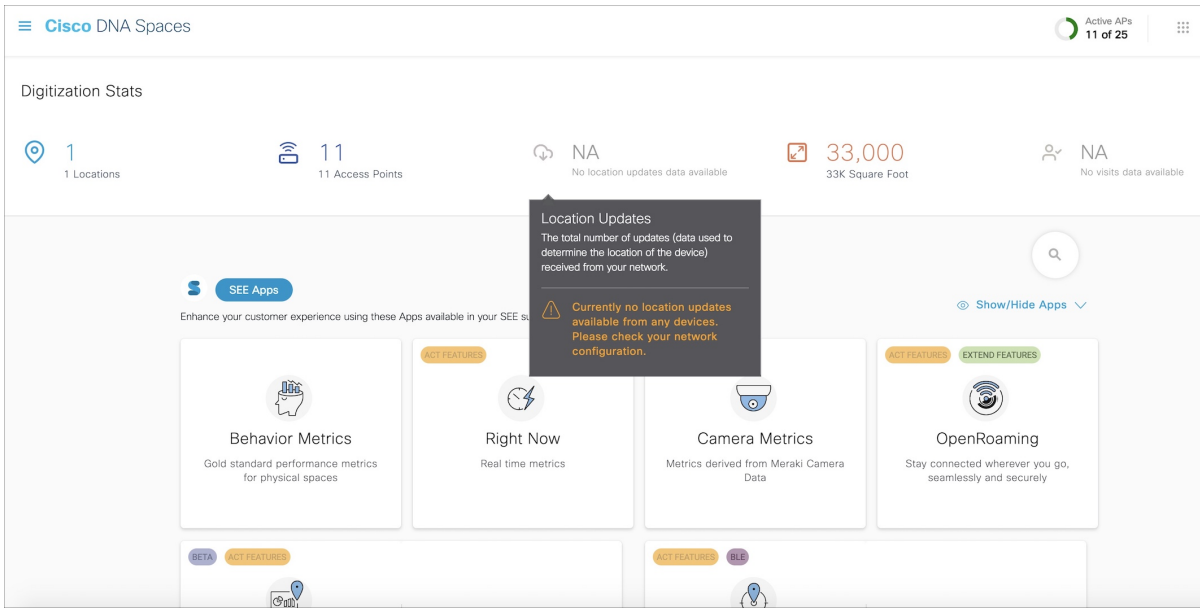
- [Locations]：さまざまなワイヤレスネットワーク用に Cisco DNA Spaces で設定されたネットワークロケーションの合計。
- [Access Points]：Cisco DNA Spaces に追加された AP の総数。
- [Location Updates]：Cisco DNA Spaces の導入日以降にワイヤレスネットワークから受信したロケーションアップデートの総数。
- [Square Foot]：[Location Hierarchy] の [Location Info] オプションでネットワークロケーションに対して設定された総面積。ただし、[Location Hierarchy] でネットワークロケーション

に対して総面積が設定されていない場合、[Square Foot] の値は AP の数に基づいて表示されます。

- [Visits]：Cisco DNA Spaces の導入日以降にビジネス拠点で発生した訪問の総数（ユニークビジターの繰り返しの訪問を含む）。

（注）

- ロケーション階層からロケーションが削除されても、対応する [Location Updates] と [Visits] のカウンター値は引き続き [Digitization Stats] セクションに保持されます。
- カウンターをクリックするか、その上にカーソルを合わせると、対応する情報を含むツールチップが表示されます。
- カウンターのデータが利用できない場合、次の図に示すように、ツールチップに警告メッセージが表示されます。



機能

Cisco DNA Spaces は、さまざまなタスク指向のアプリを提供します。パートナーアプリを Cisco DNA Spaces に追加することもできます。Cisco DNA Spaces は次のアプリを提供します。

キャプティブポータルアプリ

キャプティブポータルアプリを使用すると、キャプティブポータルルールに基づいて、キャプティブポータルを作成して顧客に表示できます。

キャプティブポータル

キャプティブ ポータルとは、特定のロケーションから固有の Wi-Fi ネットワーク ID（SSID）で Wi-Fi にアクセスするユーザに表示されるポータルのことです。このキャプティブポータルの顧客は、お客様のビジネス拠点から Wi-Fi に接続するインターネットユーザーです。

Cisco DNA Spaces で提供されるさまざまなポータルモジュールを使用して、ウェルカムメッセージ、通知、プロモーション、アプリ、ビデオ、ヘルプラインなどのさまざまな機能でポータルを強化できます。ポータルの作成と管理の詳細については、「ポータルの作成と管理」セクションを参照してください。

Captive Portal Rule

Cisco DNA Spaces では、さまざまなパラメータに基づいてキャプティブポータルを表示するキャプティブポータルルールを作成できます。ロケーション、顧客の訪問回数、顧客の種類、顧客のアプリケーションステータスなどに基づいてキャプティブポータルを表示するように設定できます。

このルールを使用して、顧客のインターネット プロビジョニングを管理し、顧客情報を外部 API に送信することもできます。

詳細については、「キャプティブポータルルール」のセクションを参照してください。

エンゲージメントアプリ

Cisco DNA Spaces は Wi-Fi ベースのビーコンとしても機能し、Wi-Fi 対応デバイスを持つ顧客が構内および付近にいるときに、顧客に対して適切な通知を送信することを可能にします。エンゲージメントアプリを使用すると、個々の顧客に異なるプロモーションおよびオファーを提供することができます。顧客が使用可能なオファーやメンバーシップの詳細について顧客に通知することができます。また、特定の店舗でのみオファーを提供するように設定することもできます。

エンゲージメント ルール アプリを使用して通知を送信するように設定できます。Cisco DNA Spaces を使用すると、顧客が Wi-Fi に接続したときに通知を送信できます。

Cisco DNA Spaces を使用すると、次の方法で通知を送信できます。

- SMS
- 電子メール
- API 通知
- Cisco Webex Teams

詳細については、「エンゲージメント ルールの作成」のセクションを参照してください。

ロケーションペルソナアプリ

Cisco DNA Spaces では、顧客をグループ化してタグを作成できます。ロケーションペルソナアプリを使用してタグを作成できます。ロケーションペルソナアプリを使用すると、既存のタグにさらに顧客を追加したり、既存のタグから特定の顧客を削除したりすることもできます。タ

グの作成の詳細については、「ロケーションペルソナアプリを使用したタグの作成または変更」のセクションを参照してください。

行動メトリクス、Right Now、カメラメトリクスアプリ

行動メトリクス

行動メトリックアプリを使用すると、ビジネスのパフォーマンスについての知見を提供するさまざまなレポートを表示できます。自社のパフォーマンスを業界のパフォーマンスと比較できます。デフォルトでは、レポートにはCisco DNA Spacesをインストールした日からのデータが含まれます。レポートは、アクセスできるすべてのロケーションについて表示されます。特定のロケーション、月、またはタグのレポートを表示するようにフィルタリングできます。行動メトリクスレポートの詳細については、このガイドの「行動メトリクス」の章を参照してください。

Right Now

Right Now アプリは、現在あなたのロケーションにいる訪問者の詳細を示す Right Now レポートを提供します。Right Now アプリを使用して、密度ルールを作成し、訪問者の密度やビジネスロケーションのデバイス数に基づいて、従業員などのビジネスユーザーに通知を送信できるすることもできます。Right Now レポートの詳細については、このガイドの「Right Now」の章を参照してください。

カメラメトリック

カメラメトリクスアプリを使用してと、Merakiカメラを使用してキャプチャしたデータに基づくメトリクスレポートを表示できます。このレポートは特定の月に表示されます。カメラメトリクスの詳細については、このガイドの「カメラメトリクス」の章を参照してください。

ロケーション解析アプリと影響分析アプリ

ロケーション解析アプリを使用すると、ロケーション訪問者のレポートを表示できます。影響分析は、行ったアクションの効果を分析の前後に基づいて測定する方法です。これらのアプリの詳細については、それぞれの章を参照してください。

Asset Locator、Detect & Locate、Proximity Reporting の各アプリケーションおよび IoT サービス

資産ロケータ

Asset Locator アプリにより、資産の監視、および資産、センサー、アラートシステム、および運用ワークフローのパフォーマンス最適化が可能になります。このアプリでは、タグとセンサーが一定量提供され、接続運用を継続的に統合、監視、および管理できます。クラウドベースのインターフェースを使用して、各資産のプロファイル、カテゴリ、および所有者を定義できます。ビジネスルールを確立して、資産とセンサーのワークフローおよび求められる動作範囲を定義できます。Asset Locator アプリの詳細については、『Cisco DNA Spaces Asset Locator Configuration Guide』を参照してください。

検出と位置特定

Cisco DNA Spaces の検出と位置特定により、展開内の Wi-Fi デバイスの現在および過去の位置を表示できます。追跡されたデバイスの数は、[Detect and Locate] アプリケーションタイルに表示されます。Detect and Locate アプリの詳細については、『Cisco DNA Spaces Detect and Locate Configuration Guide』を参照してください。

プロキシミティレポート

Proximity Reporting アプリを使用して、プロキシミティレポートを生成できます。

Proximity Reporting アプリは、COVID-19 のパンデミックの最中に職場に戻る従業員のために、職場の管理者が安全な環境を作成することを支援します。レポート対象ユーザー（監視対象の人）のワイヤレスデバイスは、ワイヤレスネットワークに関連付けられ、物理的な場所にマッピングされます。 Proximity Reporting アプリにより、COVID-19 の検査で陽性となった人の動きを追跡できます。作成されたプロキシミティレポートの数が、[Proximity Reporting] アプリケーションタイルに表示されます。Proximity Reporting アプリの詳細については、『Cisco DNA Spaces Proximity Reporting Configuration Guide』を参照してください。

IoT サービス

Cisco DNA Spaces の IoT サービスは、Cisco DNA Spaces 内のプラットフォームサービスであり、シスコのワイヤレスインフラストラクチャを使用して IoT デバイスを要求、管理、および監視できます。IoT サービスは、複数のベンダー、フォームファクタ、テクノロジープロトコルにまたがって IoT デバイスを管理できるように設計されています。Bluetooth Low Energy（BLE）は、IoT サービスを使用した管理に利用できる業界初の技術です。IoT サービスの詳細については、『Cisco DNA Spaces IoT Services Configuration Guide』を参照してください。

パートナーアプリ

Cisco DNA Spaces では、サードパーティのアプリを Cisco DNA Spaces に統合できます。サードパーティアプリは、Cisco DNA Spaces ダッシュボードにパートナーシップアプリとして表示されます。

IoT Device Marketplace アプリケーション

Cisco DNA Spaces ダッシュボードで、新しいアプリ IOT Device Marketplace を利用できるようになりました。このアプリは、ACT ライセンスユーザーのみが利用できます。SEE および EXTEND アカウントの場合、[IOT Device Marketplace] タイルは無効モードで表示されます。

IOT Device Marketplace アプリを使用すると、業界やユースケースに合致したデバイスを調べて、注文することができます。

Cisco DNA Spaces ダッシュボードで [IoT Device Marketplace] タイルをクリックすると、IoT Device Marketplacehttps://dnaspaces.io/devicemarketplace/homeアプリケーションに自動的にリダイレクトされます。この機能強化が行われる前は、IoT Device Marketplace アプリケーションにログインするにはログイン情報を再度入力する必要がありました。

ログイン後は、業界とユースケースを選択し、選択したユースケースで利用可能な IoT デバイスを表示できます。その後、デバイスの詳細を表示し、見積をリクエストできます。見積リクエストが送信されると、お客様の連絡先とともに対応するベンダーにリダイレクトされ、その後の購入手続きは、お客様とベンダーの間で直接行われ、Cisco DNA Spaces は関与しません。

ロケーション階層

ロケーション階層機能を使用して、Cisco DNA Spaces でビジネスロケーションを定義できます。ワイヤレスネットワークでロケーションが定義されている構造と同じ構造でロケーションをインポートできます。エンゲージメント、キャプティブポータル、ロケーションペルソナルールなどのアプリは、定義されたロケーション階層によって異なります。Cisco DNA Spaces はユニバーサルアカウントを提供しており、複数のワイヤレスネットワークのロケーションをロケーション階層に追加できます。

ロケーション階層に追加できる AP は、保有する Cisco DNA Spaces ライセンスのタイプによって異なります。

詳細については、「Cisco DNA Spaces のロケーション階層」セクションを参照してください。

モニター

[Monitor] セクションでは、Cisco DNA Spaces とそのアプリのパフォーマンスステータスを監視できます。また、アプリの遅延と異常も表示されます。詳細については、「モニタリング」のセクションを参照してください。

管理者管理

[Admin Management] 機能を使用すると、Cisco DNA Spaces ユーザーを作成できます。各ユーザーの権限をロールに基づいて制限できます。詳細については、「Cisco DNA Spaces のユーザーとアカウントの管理」のセクションを参照してください。

設定

ワイヤレスネットワークとカメラ

ワイヤレス ネットワーク

さまざまな方法で Cisco DNA Spaces を特定のワイヤレスネットワークに接続するための機能と手順を表示します。詳細については、「さまざまなワイヤレスネットワークで動作する Cisco DNA Spaces の設定」を参照してください。

Camera

Cisco DNA Spaces で動作するように Cisco Meraki カメラを設定するための機能と手順を表示します。

マップサービス

CMX テザリングのロケーションのマップをアップロードできるようにします。

ワイヤレス ネットワーク ステータス

ワイヤレス ネットワーク ステータス オプションを使用すると、ワイヤレスネットワークの同期ステータスを表示できます。最後の同期が実行された時刻を表示できます。

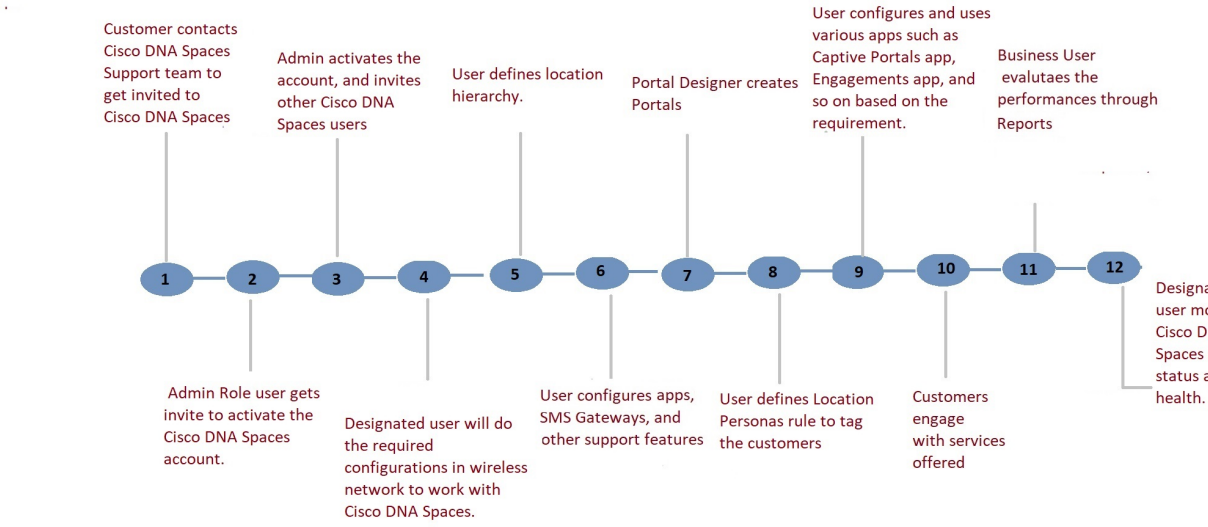
Cisco DNA Spaces ライセンスパッケージ

Cisco DNA Spaces は、**See**（基本）、**Act**（高度）、**Extend** という 3 種類のライセンスパッケージで利用できます。アカウントで使用できる機能は、所有する Cisco DNA Spaces ライセンスパッケージのタイプによって異なります。[Cisco DNA Spaces] ダッシュボードでは、利用可能なライセンスタイプに基づいてアプリが表示されます。

Cisco DNA Spaces のプロセスフロー

Cisco DNA Spaces のプロセスフローを次の図に示します。

図 *2 : Cisco DNA Spaces* のプロセスフロー



Cisco DNA Spaces のシングルサインオン

Cisco DNA Spaces ではシングルサインオン（SSO）がサポートされているため、ユーザーは SSO 資格情報を使用して Cisco DNA Spaces にログインできます。たとえば、シスコのドメインで SSO が有効になっている場合、Cisco DNA Spaces アカウントを持つシスコの従業員は、シスコの電子メールアドレスとパスワードを使用して Cisco DNA Spaces にアクセスできます。さらに、シスコの従業員が他のシスコの Web サイトまたはアプリケーションを介してシスコ

ドメインにすでにログインしている場合、そのシスコの従業員は、シスコの電子メールアドレスを指定するだけで Cisco DNA Spaces にアクセスできます。

[Login] ボタンをクリックすると、[e-mail ID] フィールドのみが [Login] ウィンドウに表示され、あわせて [Continue] ボタンが表示されます。ユーザーがすでに SSO が有効なドメインにログインしている場合、[Continue] ボタンをクリックすると直接 Cisco DNA Spaces ダッシュボードに移動します。Cisco DNA Spaces アカウントが複数の顧客名をサポートしている場合は、[Select Customer] ウィンドウが表示されます。ユーザーがドメインにログインしていない場合、ログイン認証のために IDP ページにリダイレクトされ、SSO 資格情報を指定してログインできます。

Cisco DNA Spaces アカウントで SSO を有効にするには、Cisco DNA Spaces サポートチームに次の情報を提供する必要があります。

- アカウント名
- SSO を有効にする必要があるドメイン名
- Application Name
- SSO のタイプ：現在、SAML のみがサポートされています。
- 認証のみが必要か、または認証と承認の両方を有効にする必要があるか。これは、authenticateOnly フラグを True または False に設定することで指定します。
  - True：ユーザーに対して認証のみが有効になります。
  - False：ユーザーに対して認証と承認の両方が有効になります。

  注 authenticateOnly を False に設定することを選択した場合、ユーザーの詳細を送信するときに IDP から追加情報を渡す必要があります。たとえば、role =dnaspaces:174923535949:Dashboard_Admin などです。

- metadata.xml ファイルからの次の情報：
  - SSO の詳細
  - エンティティ
  - エントリポイント

上記の詳細を提供すると、Cisco DNA Spaces サポートチームから次の情報が送信され、アプリケーションを設定できるようになります。

- Entity ID
- 応答 URL（Assertion Consumer Service の URL とも呼ばれます）

- 次の情報を含むシスコのメタデータファイル：
  - 米国または EU の Cisco DNA Spaces IDP のメタデータ（アプリケーションの場所に応じて）
  - ID：https://dnaspaces.io
  - サインオン URL：https://dnaspaces.io/api/tm/v1/account/login
  - サインアウト URL：https://dnaspaces.io/api/tm/v1/account/login
  - IDP から Cisco DNA Spaces へのコールバック URL：https://dnaspaces.io/api/tm/v1/account/login/callback

IDP メタデータは、次のように [firstName]、[lastName]、および [email] フィールドを返すように設定する必要があります。

```
nameid-format:emailAddress","firstName":"Jane","lastName":"Doe","phone":"9876543210","level":"info","
```

Cisco DNA Spaces の使用を開始する

Cisco DNA Spaces の使用を開始する前に、「Cisco DNA Spaces の前提条件」セクションに記載されている前提条件を満たしていることを確認してください。

（注） 最初に、Cisco DNA Spaces サポートチームに連絡して、Cisco DNA Spaces アカウントを作成する必要があります。電子メールで Cisco DNA Spaces アカウントをアクティブにするための招待状を受け取ります。[Accept Activate] ボタンをクリックし、表示されるウィンドウでログイン情報を構成し、[Activate Account] をクリックします。これで、Cisco DNA Spaces にログインしました。ダッシュボード管理者であれば、他の Cisco DNA Spaces ユーザーを招待できます。

Cisco DNA Spaces の使用を開始するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces にログインします。

（注） Cisco DNA Spaces のシングルサインオンを有効にすることができます。詳細については、Cisco DNA Spaces のシングルサインオン （13 ページ）を参照してください。

ステップ 2 ワイヤレスネットワークに接続し、Cisco DNA Spaces ダッシュボードの [Setup] セクションの手順を参照して、Cisco DNA Spaces のワイヤレスネットワークを設定します。

セットアップ手順は、このガイドの次のセクションでも説明しています。

- Meraki：Cisco Meraki ネットワークの設定については、「Cisco DNA Spaces を使用するための Cisco Meraki の設定」を参照してください。

- Cisco CMX を使用した Cisco Unified Wireless Network：Cisco CMX を介して Cisco DNA Spaces を Cisco AireOS コントローラに接続するには、「Cisco CMX を介して Cisco DNA Spaces をシスコ ワイヤレス コントローラに接続する （248 ページ） 」の項を参照してください。

- Cisco AireOS ワイヤレスコントローラまたは Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ（Cisco CMX なし）。

  （注） シスコ ワイヤレス コントローラの直接接続方式による接続は、小規模な展開でのみ推奨されます。大規模な実稼働展開には、すべて Cisco DNA Spaces コネクタが必要です。

  - Cisco Wireless Controller Direct Connect 使用：Wireless Controller Direct Connectを使用してCisco DNA Spaces とシスコ ワイヤレス コントローラの接続を設定するには、WLC 直接接続または Cisco DNA Spaces コネクタを使用した、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラまたはシスコ ワイヤレス コントローラの Cisco DNA Spaces への接続 （262 ページ） の項を参照してください。

  - Cisco DNA Spaces コネクタの使用：Cisco DNA Spaces コネクタを使用して、Cisco DNA Spaces と Cisco AireOS ワイヤレスコントローラまたは Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの接続を設定する方法については、Cisco DNA Spaces コネクタを使用した、Cisco DNA Spaces の Cisco AireOS ワイヤレスコントローラまたは Cisco Catalyst 9800 シリーズ ワイヤレス コントローラへの接続 （284 ページ） を参照してください。

  - Cisco Embedded Wireless Controller の使用：Cisco Embedded Wireless Controller を使用した Cisco Unified Wireless Network の設定については、「Cisco DNA Spaces と連携するための Mobility Express の設定」の項を参照してください。

（注） Cisco DNA Spaces ではユニバーサルアカウントが提供されるため、Cisco DNA Spaces を複数のワイヤレスネットワークに接続できます。

ステップ 3 チームメンバーを追加し、ロールと権限を割り当てます。Cisco DNA Spaces ユーザーの追加の詳細については、「Cisco DNA Spaces のユーザーとアカウントの管理」を参照してください。

ステップ 4 ワイヤレスネットワークで定義されているロケーション階層を Cisco DNA Spaces にインポートします。ロケーション階層の設定の詳細については、「Cisco DNA Spaces のロケーション階層」のセクションを参照してください。

次の手順はオプションであり、使用するアプリと実行するアクティビティによって異なります。

ステップ 5 Captive Portals アプリを使用するには、SSID を Cisco DNA Spaces にインポートします。SSID のインポートの詳細については、「SSID」の項を参照してください。

ステップ 6 顧客にタグを付けるためのロケーションペルソナルールを定義します。ロケーションペルソナルールの作成の詳細については、「ロケーションペルソナアプリを使用したタグの作成または変更」の項を参照してください。

ステップ 7 SMS ゲートウェイなど、サポートしている機能を設定します。設定方法については、このガイドの該当するトピックを参照してください。

ステップ 8 必要に応じて、キャプティブポータルを作成します。キャプティブポータルの作成の詳細については、「ポータルの作成と管理」を参照してください。

ステップ 9 必要に応じて、キャプティブポータルルールを作成して、さまざまな顧客に適切なキャプティブポータルを表示します。キャプティブポータルルール作成の詳細については、「キャプティブポータルルール」のセクションを参照してください。

ステップ 10 必要に応じて、エンゲージメントルールを作成して、適切な通知を顧客に送信します。エンゲージメントルールの作成の詳細については、「エンゲージメントルールの作成」のセクションを参照してください。

ステップ 11 Behavior Metrics、Location Analytics、Impact Analysis などのアプリを使用して、Cisco DNA Spaces のパフォーマンスおよびビジネスパフォーマンスを分析します。これらのアプリの詳細については、それぞれのセクションを参照してください。

ステップ 12 [Monitor] セクションを使用して、Cisco DNA Spaces ドメインとアプリを監視します。

Profile Information

Cisco DNA Spaces は、Cisco DNA Spaces ダッシュボードユーザーの名、姓、携帯電話番号などのプロファイル情報の追加をサポートしています。

- [Account Preferences] ウィンドウの [My Profile] タブを使用して、プロファイル情報を追加できます。このウィンドウでは、名、姓、および携帯電話番号を指定できます。携帯電話番号とその確認はオプションです。携帯電話番号を指定すると、[Verify Mobile Number] リンクが表示され、ワンタイムパスワードを使用して携帯電話番号を確認できます。携帯電話番号が確認されると、[Verified] ステータスが表示されます。携帯電話番号を変更すると、[Verify Mobile Number] リンクが再び表示されます。
- Cisco DNA Spaces のログインワークフローでは、特定の Cisco DNA Spaces ユーザーのプロファイル情報が存在しない場合、ログインプロセスの一環として [Update Profile Information] ダイアログボックスが表示されます。このステップをスキップして、ログインに進むことができます。その後、いつでも [Account Preferences] ウィンドウからプロファイルの詳細を追加できます。ただし、時間情報が提供されるまで、[Profile Information] ダイアログボックスがログインワークフローの一部として表示されます。

  （注） SSO ユーザーは、プロファイル情報を編集したり、携帯電話番号を確認したりすることはできません。また、ログイン時に SSO ユーザーに [Update Profile Information] ダイアログボックスは表示されません。

有効期限後のパスワード変更のサポート

Cisco DNA Spaces では、パスワードの有効期限が切れた後でもパスワードを変更できます。ログイン情報を入力して [Continue] ボタンをクリックすると、パスワードを変更するためのポップアップウィンドウが表示され。

Cisco DNA Spaces のナビゲーション

Cisco DNA Spaces ダッシュボードにログインすると、Cisco DNA Spaces アプリが Cisco DNA Spaces ホームページに表示されます。アプリは、利用可能なライセンスタイプの下に表示されます。ダッシュボードの左上に表示される 3 本線のメニューアイコンを使用して、[Location

Hierarchy]、[Monitor]、[Admin Management]、[Setup] といった Cisco DNA Spaces の他の機能にもアクセスできます。ダッシュボードの左上に表示される [Cisco DNA Spaces] をクリックするか、3 本線メニューの [Home] オプションを使用して、ホームページに移動できます。

ダッシュボードの右上に表示されるアプリランチャ（グリッド）アイコンを使用すると、あるアプリから別のアプリに簡単に移動できます。アプリランチャアイコンをクリックすると、ユーザーに対してアクティブ化されたすべての Cisco DNA Spaces アプリが一覧表示されます。ダッシュボードの左上に表示される [Cisco DNA Spaces] をクリックして、アプリからホームページに移動できます。

Cisco DNA Spaces のアイドルタイムアウト

Cisco DNA Spaces ダッシュボードにログインしているユーザーは、特定の期間だけアイドル状態を維持できます。20 分間非アクティブな場合、そのユーザーはダッシュボードから自動的にログアウトされます。アイドルタイムアウトの 5 分前に通知が表示され、Cisco DNA Spaces アプリケーションが開いているブラウザウィンドウのタイトルが `INACTIVE: You will be logged out in 5 mins` に変わります。対応するウィンドウで実行されたアクションは、ユーザーのセッションを拡張します。

Cisco Smart License

Cisco Smart License は、ソフトウェアのアクティブ化と管理の方法を合理化する柔軟なライセンスモデルです。このソリューションを使用すると、ライセンスのステータスとソフトウェアの使用傾向を簡単に追跡できます。

Cisco DNA Spaces でスマートライセンスをサポートすると、Cisco スマートアカウントの Cisco DNA Spaces ソフトウェアライセンスを表示および管理できます。Cisco DNA Spaces で Cisco Smart License を有効にするには、Cisco Smart Software Manager（CSSM）を使用して設定されたスマートアカウントが必要です。Cisco DNA Spaces ダッシュボードで、[Profile Icon] > [Activate Smart License] を選択して、Cisco Smart License をアクティブ化します。

[My Accounts] > **[License Information]** タブから Cisco Smart License をアクティブ化することもできます。

（注） Cisco DNA Spaces でスマートライセンスを有効にするには、シスコで設定されたスマートアカウントが必要です。Cisco Smart License の詳細については、『Smart Software Licensing』を参照してください。

スマートライセンスのアクティブ化

ステップ 1 Cisco DNA Spaces ダッシュボードで、**[Profile Icon]** > **[Activate Smart License]** を選択します。

[Terms and Conditions] ウィンドウが表示されます。[Link Cisco Smart Account] ウィンドウが表示されます。

ステップ 2 利用規約を読み、[Accept Terms and Conditions] をクリックします。

[Smart License Configuration] ウィンドウが表示されます。

ステップ 3 Cisco Smart Software Manager（CSSM）ですでにアカウントを持っている場合は、[Yes, I have] オプションボタンをクリックします。

CSSM でアカウントを持っていない場合は、[No, I don't have] オプションボタンをクリックし、CSSM でアカウントを作成する手順を表示します。

ステップ 4 [Next] をクリックします。

ステップ 5 画面の指示に従って、CSSM ツールでトークンを作成します。

（注） 生成されたトークンをコピーして、手順 7 でそれを使用してください。

ステップ 6 トークンを生成したら、[Next] をクリックします。

ステップ 7 [Product Instance Token] フィールドに、生成したトークンを貼り付けます。

ステップ 8 [Register] をクリックして、Cisco DNA Spaces を CSSM アカウントに登録します。

成功通知メッセージが表示されます。[License Information] タブの下の [My Accounts] ウィンドウで、スマートライセンス ソフトウェアの登録の詳細とライセンスのコンプライアンスに関する情報を表示できます。

（注） シスコスマートライセンスをアクティブ化した後、Cisco DNA Spaces サポートチームに連絡して、トライアルサポートを有効にすることができます。トライアルモードが有効になっている場合、スマートエージェントはライセンスの使用状況を Cisco Smart License Management に更新しません。

シスコスマートライセンスをアクティブ化した後、Cisco DNA Spaces ライセンスをアップグレードまたはダウングレードできます。これを行うには、**[Profile] アイコン** > **[License Info]** > **[Select License Level]** を選択します。詳細については、ライセンス情報の更新 （19 ページ）を参照してください。

ライセンス情報の更新

[My Accounts] ウィンドウの [License Information] タブを使用して、Cisco DNA Spaces のライセンスを管理します。使用可能なライセンスは、**Cisco DNA Spaces See**、**Cisco DNA Spaces Act**、**Cisco DNA Spaces Extend** です。

認証と登録の更新、Cisco DNA Spaces のスマートライセンスの再登録と登録解除を行うことができます。

ステップ 1 Cisco DNA Spaces ダッシュボードで、**[Profile Icon]** > **[My Account]** を選択します。

ステップ 2 [License Information] タブをクリックします。

[Your License] エリアには、Cisco DNA Spaces ライセンス、ライセンスがアクティブになるまでの日付、および有効期限までの残り日数が表示されます。

ステップ 3 ライセンスをアップグレードまたはダウングレードするには、[Select License Level] をクリックします。

[Select License Level] ウィンドウが表示されます。現在のプランは緑色のチェックマークで示されます。アップグレードまたはダウングレードの可能性は、[Select License Level] ウィンドウにも表示されます。

a) アップグレードまたはダウングレードするプランを選択します。

ライセンスのアップグレードまたはダウングレード情報を含む警告メッセージが表示されます。

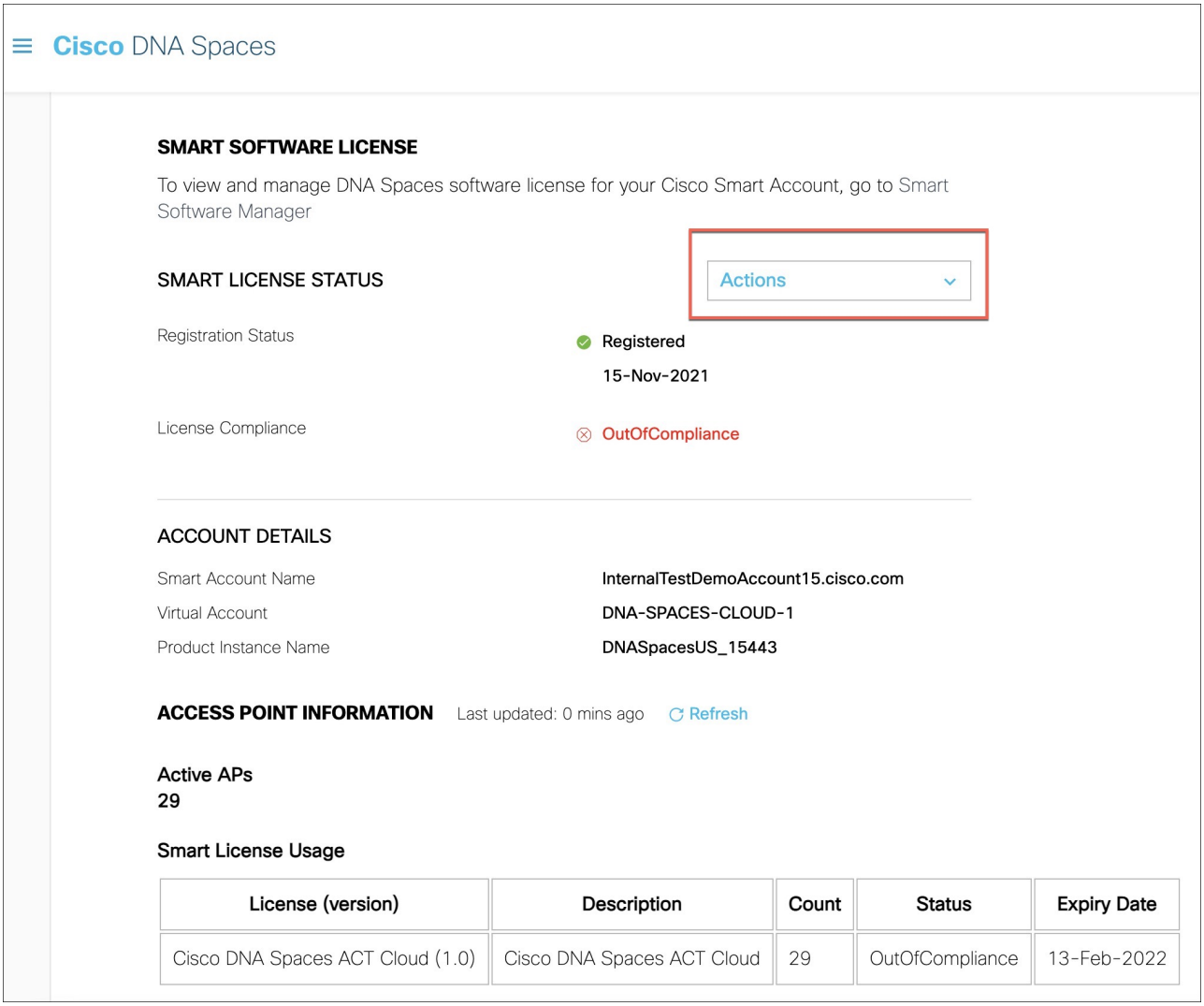
b) [I accept the terms and conditions] チェック ボックスをオンにして続行します。
c) [Change Plan] をクリックします。

成功通知メッセージが表示されます。

d) 最新のライセンスの詳細を表示するには、[Login] をクリックして、Cisco DNA Spaces にログインします。

ステップ 4 [Smart License Status] エリアに、次の情報が表示されます。

図 *3*:スマート ソフトウェア ライセンス



- [Registration Status]：Cisco DNA Spaces スマートライセンスの登録されたステータスを表示します。
- [License Compliance]：Cisco DNA Spaces のスマート ライセンス コンプライアンスの詳細を表示します。

ステップ 5 [Actions] ドロップダウンリストをクリックして、次のオプションを表示します。

- [Renew Authorization]：クリックすると、Cisco DNA Spaces のスマートライセンス認証が更新されます。

（注）
- Cisco DNA Spaces が CSSM と通信するときに認証の更新が自動的に実行されるため、このアクションはオプションです。または、スマートライセンスエージェントが、バックエンドから 30 日ごとに認証の更新を自動的に実行します。
- ステータスが [Out of Compliance] の場合に、トラブルシューティングするか、認証を手動で更新する場合は、このアクションを実行することをお勧めします。また、認証を手動で更新して、最近のスマートアカウントの更新を反映して、Cisco DNA Spaces に反映することもできます。

- [Renew Registration]：クリックすると、Cisco DNA Spaces のスマートライセンス登録が更新されます。

（注）
- 登録の更新は、登録時にバックエンドで Cisco DNA Spaces によって自動的に実行されるため、このアクションはオプションです。
- このアクションにより、CSSM の登録 ID と証明書が更新されます。Cisco DNA Spaces は、バックエンドから 6 ヵ月ごとにこのアクションを自動的に実行します。

- [Re-register]：クリックすると、CSSM の Cisco DNA Spaces のスマートライセンスを再登録します。

（注）
- このアクションにより、スマートライセンスが強制的に再登録され、既存の登録済みインスタンスが上書きされます。このアクションにより、スマートアカウントの特定のインスタンスのデータ損失が報告されます。
- このアクションを実行して、スマートライセンスのトラブルシューティングを行うことをお勧めします。

- [De-register]：クリックすると、CSSM の Cisco DNA Spaces のスマートライセンスを登録解除します。

（注） Cisco DNA Spaces が使用されておらず、CSSM からインスタンスを登録解除する場合は、このアクションを実行することをお勧めします。

ステップ 6 [Account Details] エリアに、次の情報が表示されます。

- [Smart Account Name]：Cisco DNA Spaces のスマート ライセンス アカウント名を表示します。
- [Virtual Account]：isco DNA Spaces のバーチャルアカウント名を表示します。
- [Product Instance Name]：Cisco DNA Spaces の製品インスタンス名を表示します。

ステップ 7 [Access Point Information] エリアには、次の情報が表示されます。

- [Active APs]：アクティブなアクセスポイントの数を表示します。

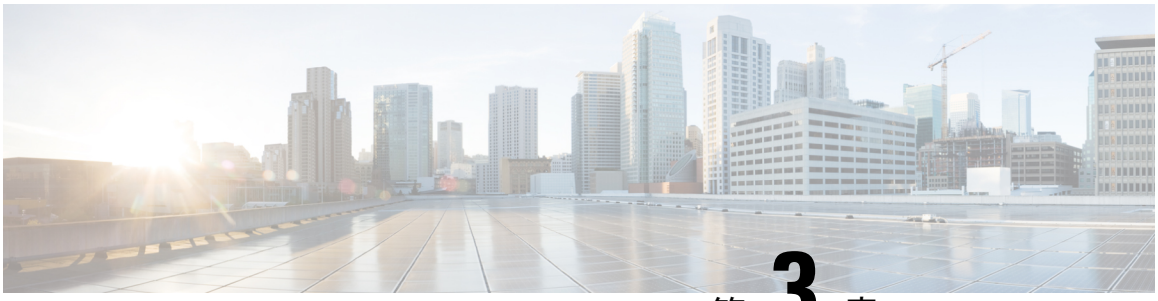
ステップ 8 [Smart License Usage] エリアに、次の情報が表示されます。

- [License]：ライセンスのバージョンを表示します。
- [Description]：ライセンスの説明を表示します。
- [Count]：アクティブなアクセスポイントの数を表示します。

- [Status]：ライセンスのステータスを表示します。
- [Expiry Date]：スマートライセンスの有効期限日を表示します。

Cisco DNA Spaces ドキュメント

Cisco DNA Sapces ダッシュボードの右上に表示される [Cisco DNA Spaces Support] アイコンを使用して、コンフィギュレーション ガイドやリリースノートを含む Cisco DNA Spaces のドキュメントにアクセスできます。



第 3 章

Cisco DNA Spaces におけるロケーション階層

この章では、Cisco Digital Network Architecture（DNA）Spaces におけるロケーション階層の構造と、Cisco DNA Spaces でロケーション階層を定義する方法について説明します。

ロケーション階層の概要

Cisco DNA Spaces では、Cisco AireOS ワイヤレスコントローラ、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ、Cisco Meraki などのワイヤレスネットワークで定義したものと同じ構造のロケーションをインポートできます。

Cisco DNA Spaces のお客様にはそれぞれデフォルトのお客様名（ルート名）が提供され、このお客様名は Cisco DNA Spaces ロケーション階層のルートロケーションとして機能します。

Cisco DNA Spaces はユニバーサルアカウントを提供するため、複数のワイヤレスネットワークのロケーションをインポートして管理できます。プロキシミティルールには、複数のワイヤレスネットワークのロケーションを含めることができます。

キャプティブポータルルール、エンゲージメントルール、ロケーションペルソナルールなどのプロキシミティルールを作成し、ロケーション階層内の任意のロケーションのアクセスポイント、ユーザー、および子ロケーションを表示できます。ロケーション階層の各ロケーションのアクセスポイント、プロキシミティルール、子ロケーション、およびユーザーの数が、その特定のロケーションに対して表示されます。たとえば、あるグループのプロキシミティルール、子ロケーション、およびユーザーの数は、ロケーション階層のそのグループに対して表示されます。これらのロケーションパラメータの数は、累積的に表示されます。

ロケーション階層には、Cisco Prime Infrastructure または Cisco DNA Center からインポートされたマップで定義されている階層構造が自動的に反映されます。

Cisco DNA Spaces ダッシュボードでは、次の方法を使用して、キャンパス、ビルディング、フロアなどのロケーションのみをロケーション階層に選択的にインポートすることを可能にしています。

- AP ゾーンの追加
- ビルディングの追加
- キャンパスの追加
- CMX ゾーンの追加
- フロアの追加

（注）

- キャンパス、ビルディング、フロアなどのロケーションがロケーション階層から削除された場合、以前にアップロードしたマップを [Map Service] > [Maps Upload] を使用してアップロードすることにより、ロケーション階層に追加し直すことができます。
- Cisco DNA Spaces のお客様は、Cisco Prime Infrastructure ベースのマップから Cisco DNA Spaces 内の Cisco DNA Center ベースのマップに移行できます。ロケーション階層と既存の Cisco DNA Spaces データに影響を与えない方法で新しいマップへのシームレスな移行を確実にするために、Cisco DNA Spaces サポートチームに連絡してロケーション階層を検証し、いかなる問題も発生せずに確実にデータが引き継がれるようにすることを推奨します。

ロケーション階層を定義するための前提条件

Cisco DNA Spaces ダッシュボードでロケーション階層を定義するには、最初に Cisco Meraki、Cisco AireOS ワイヤレスコントローラ、または Cisco Catalyst 9800 シリーズ ワイヤレス コントローラなどのワイヤレスネットワークで必要な階層構造を定義する必要があります。さらに、Cisco DNA Spaces とワイヤレスネットワーク間の接続を確立する必要があります。

- Cisco DNA Spaces を使用するための Cisco Meraki の設定 （299 ページ）
- Cisco CMX を介して Cisco DNA Spaces をシスコ ワイヤレス コントローラに接続する （248 ページ）
- Cisco WLC Direct Connect を使用した Cisco DNA Spaces のシスコ ワイヤレス コントローラへの接続 （263 ページ）
- Cisco WLC Direct Connect を使用した Cisco DNA Spaces の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラへの接続 （266 ページ）
- Cisco DNA Spaces コネクタを使用した、Cisco DNA Spaces の Cisco AireOS ワイヤレスコントローラまたは Cisco Catalyst 9800 シリーズ ワイヤレス コントローラへの接続 （284 ページ）

ロケーション階層の定義

Cisco DNA Spaces は、次のワイヤレスネットワークをサポートしています。

- **Cisco Meraki**
- **Cisco CMX を備えた、または備えていないシスコ ワイヤレス コントローラ**
- **Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ**

（注） Cisco CMX を備えていないシスコ ワイヤレス コントローラと、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの場合、Cisco DNA Spaces コネクタを使用して、コントローラと Cisco DNA Spaces の間で適切なデータ転送が行われるようにすることができます。

使用するワイヤレスネットワークに基づいて、次から必要な手順を選択します。

Cisco Meraki のロケーション階層の定義

Cisco Meraki ロケーションをインポートするには、最初にお客様の名前の下に Cisco Meraki 組織を追加する必要があります。その後、Meraki ネットワークをインポートできます。Meraki ネットワークをインポートすると、フロアとアクセスポイントもインポートされます。アクセスポイントをグループ化し、ネットワークまたはフロア レベルでゾーンを作成できます。ロケーションは、お客様名レベルまたは組織レベルでグループ化できます。顧客名を変更することもできます。

Meraki ネットワークロケーションには、Cisco DNA Spaces でサポートされているタグが付いた 1 つ以上の Meraki アクセスポイントが含まれる場合があります。このような Meraki ネットワークロケーションを追加すると、これらのタグ付き AP のみがロケーション階層に追加されます。現在、Cisco DNA Spaces では `Cisco-DNASpaces` タグのみがサポートされています。

Cisco DNA Spaces タグ付き AP が 1 つ以上ある Meraki ネットワークロケーションが Cisco DNA Spaces ロケーション階層にすでに追加されている場合、これらのタグ付き AP のみがバックグラウンドでのネットワークの同期中に追加されます。このネットワークのロケーション階層に存在する Cisco DNA Spaces タグの付いていない AP は、次回のバックグラウンドでのネットワークの同期中に、それぞれのロケーションから削除されます。

ただし、Cisco DNA Spaces でサポートされているタグが Meraki ネットワーク内のどの AP にもない場合、すべてのアクセスポイントがロケーション階層に追加されます。タグ付けされた AP がないそのような Meraki ネットワークロケーションが Cisco DNA Spaces ロケーション階層にすでに追加されている場合、すべての AP がロケーション階層に同期されます。既存のロケーション階層に変更はありません。

ロケーション階層を作成する前に、すべての前提条件が満たされていることを確認してください。ロケーション階層を作成するための前提条件については、ロケーション階層を定義するための前提条件 （26 ページ）を参照してください。

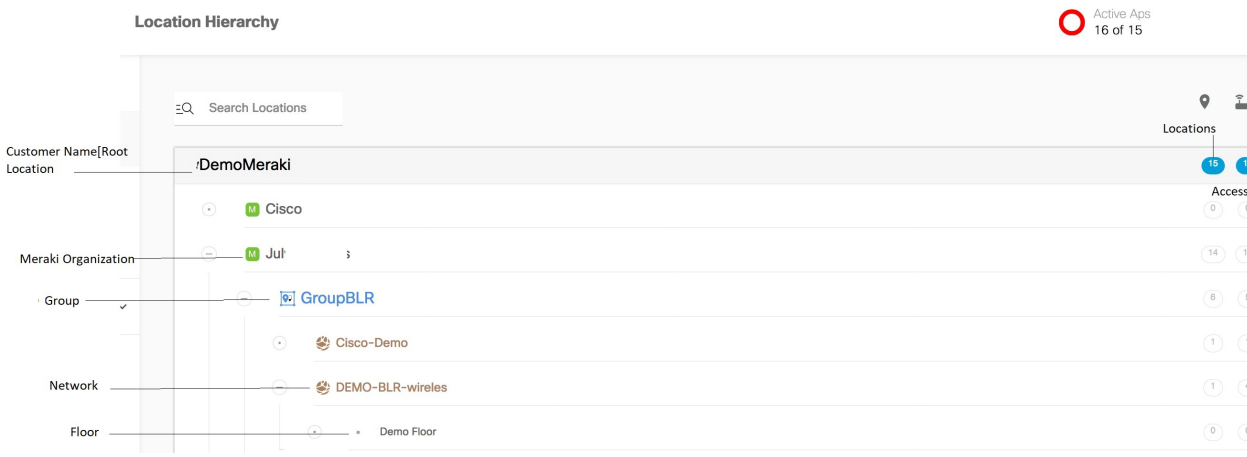
（注） ロケーションをインポートするには、Cisco Meraki のログイン情報が必要です。その後、ロケーション階層は、Meraki サービスアカウントを使用して Cisco Meraki と同期されます。したがって、ロケーション階層を最新の状態に保つには、バックグラウンドでのネットワークの同期用に Cisco Meraki カスタマーアカウントで Cisco Meraki サービスアカウントを設定する必要があります。ただし、Cisco DNA Spaces を Cisco Meraki に接続するには、引き続き Meraki カスタマーアカウントを使用する必要があります。Cisco Meraki サービスアカウントの設定の詳細については、Cisco Meraki サービスアカウントの設定 （299 ページ）を参照してください。

Cisco Meraki ネットワークのロケーション階層は次のとおりです。

Meraki > **組織** > **ネットワーク** > **フロア** > **アクセスポイント**。

Cisco Meraki のロケーション階層を次の図に示します。

図 *4 : Meraki* のロケーション階層



Meraki のログイン情報がない場合は、Meraki API キーを使用してロケーションをインポートできます。API キーを使用して Meraki からロケーションをインポートする方法の詳細については、API キーを使用した Cisco Meraki ロケーションのインポート （30 ページ）を参照してください。

Meraki のログイン情報を持っている場合、Meraki ロケーションを Cisco DNA Spaces にインポートするには、次の手順を実行します。

（注） ロケーション階層を設定した後は、ロケーションのタイムゾーンが定義されていることを確認してください。定義されたタイムゾーンによって、Cisco DNA Spaces のルールとレポートが影響を受けます。

Cisco Meraki 組織の追加

Cisco DNA Spaces でロケーション階層を作成するには、ロケーション階層にロケーションをインポートする Cisco Meraki 組織を最初に追加する必要があります。

（注） Cisco DNA Spaces では、ロケーション階層に複数の Cisco Meraki 組織を追加できるため、複数の Meraki 組織に同時に接続することができます。

Cisco Meraki 組織をロケーション階層に追加するには、次の手順を実行します。

ステップ 1 [Cisco DNA Spaces] ダッシュボードで、[Location Hierarchy] を選択します。

ステップ 2 表示される [Location Hierarchy] ウィンドウで、顧客名（ルート名）の [More Actions] をクリックします。

ステップ 3 [Add a Wireless Network] を選択します。

ステップ 4 表示される [Wireless Network] ドロップダウンリストから、[Cisco Meraki] を選択します。

ステップ 5 Meraki アカウントのユーザー名とパスワードを入力し、[Login] をクリックします。

ステップ 6 [Organization] ドロップダウンリストから、ロケーションのインポート元となる Cisco Meraki 組織を選択します。

ステップ 7 [Add] をクリックします。

追加された組織がロケーション階層のリストに表示されます。

Cisco Meraki 組織へのネットワークの追加

Cisco DNA Spaces では、Cisco Meraki のロケーション階層に従って、ネットワークとフロアの構造を管理できます。Cisco Meraki 組織をロケーション階層に追加した後、そのネットワークおよび関連付けられたフロアをインポートできます。

ネットワークおよび関連付けられたフロアをロケーション階層にインポートするには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Location Hierarchy] をクリックします。

ステップ 2 [Location Hierarchy] ウィンドウで、ネットワークに追加する Cisco Meraki 組織の右端の [More Actions] アイコンをクリックします。

ステップ 3 [Add Network] を選択します。

ステップ 4 [Add Network] ウィンドウで、ロケーション階層に追加するネットワークを選択します。

[Add Network] ウィンドウに、その Cisco Meraki 組織で使用可能なすべてのネットワークが表示されます。

ステップ 5 [Add] をクリックします。

追加されたネットワークは、関連付けられたフロアとともにロケーション階層にリストされます。

（注） Cisco Meraki アプリケーションでは、ネットワーク名が重複しないようにします。

ゾーンの作成とアクセス ポイントの追加

ゾーンを使用して、ネットワークまたはフロアのアクセス ポイントをグループ化することができます。ゾーンは、ネットワークまたはフロア レベルで作成できます。

（注） フロアのアクセス ポイントを変更することはできません。

ネットワークまたはフロアに対してゾーンを作成するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Location Hierarchy] を選択します。

ステップ 2 [Locations] ウィンドウで、ゾーンを作成するネットワークまたはフロアの右端にある [More Actions] をクリックします。

ステップ 3 [Add Zone] を選択します。

ステップ 4 表示される [Add Zone] ウィンドウで、次の手順を実行します。

a) [Name] フィールドに、ゾーンの名前を入力します。
b) [Select Access Points] エリアで、ゾーンに追加するアクセスポイントのチェックボックスをオンにします。
c) [Add] をクリックします。

次のタスク

ヒント ゾーンを作成する前に、Cisco Meraki ダッシュボードでゾーンに含めるアクセスポイントを特定しておきます。

（注） ネットワークまたはフロアのアクセス ポイントをゾーンに追加すると、そのアクセス ポイントはそのネットワークまたはフロアでは使用できなくなります。ゾーンに追加されたアクセスポイントは、別のゾーンでは使用できません。

API キーを使用した Cisco Meraki ロケーションのインポート

API キーを使用して Cisco Meraki ロケーションをインポートするには、次の手順を実行します。

ステップ 1 [Location Hierarchy] ウィンドウで、顧客名（ルート名）の [More Actions] アイコンをクリックし、次に [Add a Wireless Network] をクリックします。

ステップ 2 表示されるウィンドウで、[Add a Wireless Network] ドロップダウンリストから [Cisco Meraki] を選択します。

ステップ 3 [Cisco Meraki] を選択すると表示される [Import Organization using API] リンクをクリックします。

ステップ 4 [API Key] フィールドで、Meraki の API キーを入力して、[Fetch Organizations] をクリックします。

入力した API キーの組織が一覧表示されます。

ステップ 5 インポートする組織を選択して、[Add] をクリックします。

組織が [Locations] ウィンドウのリストに表示されます。

ステップ 6 組織の [More Actions] メニューの [Add Network] を使用して、組織のネットワークを追加します。

ネットワークをインポートすると、そのフロアとアクセスポイントもインポートされます。

ステップ 7 フロアの [More Actions] メニューの [Add Zones] を使用して、フロアにゾーンを作成します。

Cisco AireOS/ Cisco Catalyst のロケーション階層の定義

CiscoAireOS（シスコ ワイヤレス コントローラ）および Cisco Catalyst（Cisco Catalyst 9800 シリーズ ワイヤレスコントローラ）を Cisco DNA Spaces に接続し、Cisco CMX、Cisco WLC Direct Connect、または Cisco DNA Spaces コネクタのいずれかを使用してロケーション階層をインポートできます。

Cisco CMX を使用した Cisco AireOS/シスコ ワイヤレス コントローラのロケーション階層の定義

ロケーション階層を作成する前に、すべての前提条件が満たされていることを確認してください。ロケーション階層を作成するための前提条件については、ロケーション階層を定義するための前提条件 （26 ページ）を参照してください。

Cisco DNA Spaces は、Cisco CMX 10.6 以降のみをサポートします。

（注） [Add a Wireless] ウィンドウの [CMX on Prem] オプションは機能しなくなります。Cisco DNA Spaces を Cisco CMX を使用して Cisco AireOS/Catalyst に接続する場合、ロケーションをロケーション階層にインポートするために、CMX テザリングを使用してロケーションをインポートできます。CMX テザリングは、マップをマップサービスにアップロードするか、Cisco CMX でトークンを設定することで実行できます。マップをインポートすると、マップデータが自動的に [Location Hierarchy] に反映されます。

Cisco CMX がインストールされている Cisco AireOS ワイヤレスコントローラのロケーション階層は次のとおりです。

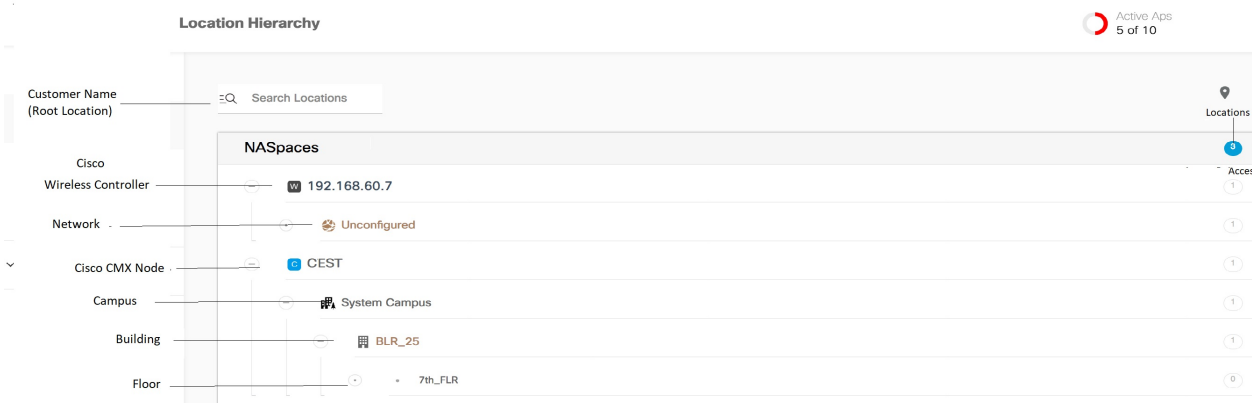
[Cisco CMX Node] > [Campus] > [Building（Network）] > [Floor] > [CMX Zone]（定義されている場合）

（注）

- マップサービスの更新により、2020 年 10 月以降に新しくインポートされたロケーション階層には、[Campus] > [Building] > [Floor] > [CMX Zone]（定義されている場合）のみが含まれるようになります。ただし、マップのアップロードによって既存のロケーション階層に加えられた更新では、[CMX Node] が引き続き含められます。
- 既存のロケーション階層に対して、マップサービスを使用してロケーションを再インポートすると、重複する AP（すでにロケーション階層に存在し、インポートされたマップにも存在する AP）がマップベースの階層に移動されます。したがって、レポートおよびプロキシミティルールが影響を受けます。 また、キャプティブポータルを表示したり、通知を送信したりするには、プロキシミティルールを再構成する必要があります。
- [Cisco DNA Spaces] ダッシュボードでは、 [Location Hierarchy] > [Add Wireless Networks] で、[CMX On-Prem] または [WLC Direct Connect] > [Import from Maps] を使用して、ロケーションのインポートが制限されます。

Cisco CMX を使用した Cisco AireOS/Catalyst ワイヤレスコントローラのロケーション階層を次の図に示します。

図 *5 : Cisco CMX* によるロケーション階層



（注）

ロケーション階層を設定した後、ロケーションのタイムゾーンが定義されていることを確認します。定義されたタイムゾーンによって、Cisco DNA Spaces のルールとレポートが影響を受けます。

CMX テザリングを使用した、Cisco DNA Spaces のシスコ ワイヤレス コントローラまたは Cisco Catalyst 9800 シリーズ ワイヤレス コントローラへの接続

Cisco CMX 10.6 以降を使用している場合、CMX テザリング機能を使用して、Cisco DNA Spaces をコントローラに接続し、ロケーションをインポートし、通知とレポートのロケーション更新を設定できます。

Cisco DNA Spaces ネットワーク同期サーバーは、CMX テザリングの AP 同期をサポートしています。CMX テザリングの場合、Cisco Prime の AP に加えられた変更は、Cisco DNA Spaces のロケーション階層で更新されます。AP の変更を同期するには、次のいずれかを実行します。

- Cisco CMX で、[SYSTEM] をクリックします。表示されるダッシュボードで、**[Settings]** > **[Controllers and Maps Setup]** > **[Import]** を選択します。表示されるウィンドウで、Cisco Prime のユーザー名、パスワード、および IP アドレスを入力します。次に [Import Controllers and Maps] をクリックして、最新のマップ変更を取得します。[**Save**] をクリックします。
- Cisco Prime から更新されたマップをダウンロードし、Cisco CMX にアップロードします。
- Cisco Prime から更新されたマップをダウンロードし、Cisco DNA Spaces のマップサービスにアップロードします。

CMX テザリングを次の方法で実行できます。

Cisco CMX でのトークン設定による *CMX* テザリング

トークンによる CMX テザリングを設定するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、**[Setup]** > **[Wireless Networks]**を選択します。

ステップ 2 [Connect your wireless network] ウィンドウで、[Add New] をクリックします。

ステップ 3 [Cisco AireOS/Catalyst] の [Select] をクリックします。

ステップ 4 [Connect Via CMX Tethering] の [Select] をクリックします。

このオプションを使用するための前提条件が表示されます。

ステップ 5 [Continue Setup] をクリックします。

[Connect your wireless network] ウィンドウに [Connect Via CMX Tethering] ウィジェットが表示されます。

ステップ 6 [Connect Via CMX Tethering] ウィジェットを展開します。

ステップ 7 ステップ 2 で表示された [Create New Token] をクリックします。

ステップ 8 [Create a new token] ウィンドウで、Cisco CMX テザリングの名前と説明を入力します。

ステップ 9 [**Save**] をクリックします。

ステップ 10 ステップ 2 で表示された [View Tokens] をクリックします。

追加された Cisco CMX テザリングインスタンスが一覧表示されます。

ステップ 11 Cisco DNA Spaces を Cisco CMX に接続するためのトークンを生成するには、[CMX Tethering Tokens] ウィンドウで、トークンを生成する Cisco CMX テザリングインスタンスの [Key] アイコンをクリックします。

ステップ 12 [**コピー（Copy）**] をクリックします。

ステップ 13 Cisco CMX にログインします。

ステップ 14 **[Manage]** > **[Cloud Apps]**を選択します。

ステップ 15 表示される [Cloud Applications] ウィンドウで、[Cisco DNA Spaces] の [Actions] 列にある [Enable] をクリックします。

ステップ 16 表示されるウィンドウで、Cisco DNA Spaces ダッシュボードからコピーしたトークンを設定します。

トークンを使用して CMX テザリングを設定すると、特定の CMX ノードのロケーションマップが [Map Service] ウィンドウに表示され、ロケーションが Cisco DNA Spaces ダッシュボードの [Location Hierarchy] に自動的に表示されます。

（注） [Location Hierarchy] からロケーションを削除すると、[Map Service] からも削除されます。

（注）
- Cisco CMX で [Cisco DNA Spaces] サービスを有効にするには、Cisco DNA Spaces アカウントが必要です。
- Cisco CMX の場合、ロケーション階層の [More Actions] を使用してキャンパス、ビルディング、およびその他の子ロケーションを追加することはできません。**[Setup]** > **[Map Service]** でロケーションを更新する必要があります。ただし、ゾーン (AP ゾーン) を追加することはできません。ロケーション階層からロケーションをグループ化または削除できます。ロケーション階層からロケーションを削除すると、そのロケーションは [Map Service] からも削除されます。詳細については、Cisco CMX を使用したシスコ ワイヤレス コントローラのロケーション階層の管理 （52 ページ）を参照してください。
- Cisco Prime でのロケーションの更新を Cisco DNA Spaces で自動的に同期するには、Cisco CMX の [Map Sync] ボタンをクリックする必要があります。

マップサービスにロケーションマップをアップロードすることによる *CMX* テザリング

（注） 設定は Cisco DNA Spaces の一部ではない外部アプリケーションで行うため、このマニュアル内のメニューパス、タブやウィンドウ、オプションなどに指定する名前が変わる場合があります。

（注） マップは、Cisco Prime または Cisco DNA Center からエクスポートできます。Cisco Prime Infrastructure または Cisco DNA Center からエクスポートされ、[Map Service] を使用して Cisco DNA Spaces にインポートされたマップは、[Location Hierarchy] の下に自動的に表示されます。

Cisco Prime からマップをエクスポートして、ロケーションをロケーション階層にインポートするには、次の手順を実行します。

ステップ 1 Cisco Prime Infrastructure にログインします。

ステップ 2 [Settings /Getting Started] ウィンドウで、ウィンドウの左上（Cisco ロゴの近く）にある円形のアイコンをクリックします。

ステップ 3 表示されるウィンドウで、左ペインの [Maps] をクリックします。

ステップ 4 [Wireless Maps] 領域で、[Site Maps (Deprecated)] をクリックします。

（注） [Site Maps (New)] オプションを使用して、新しい場所を追加できます。

ステップ 5 [Go] の近くにあるドロップダウンリストをクリックし、[Export Maps] を選択します。

ステップ 6 [移動（Go）] をクリックします。

ステップ 7 ロケーションマップのツリービューから、エクスポートする親ロケーション（CMX ノード）を選択し、**Export** をクリックします。

（注） [Include Map Information] チェックボックスがオンになっていることを確認します。

ロケーションマップをコンピュータに保存します。

（注） マップは zip 形式でダウンロードし、同じ形式で Cisco DNA Spaces にアップロードする必要があります。

ステップ 8 Cisco DNA Spaces ダッシュボードで、**[Setup]** > **[Map Service]** を選択します。

ステップ 9 ウィンドウの左上にある [Upload] をクリックし、Cisco Prime Infrastructure からダウンロードしたロケーションマップを選択します。

ロケーションマップが [Map Service] にアップロードされます。

（注） マップに表示される正方形のアイコン（展開/折りたたみアイコンの下）を使用して、**[Setup]** > **[Map Service]** で CMX ゾーンを追加できます。

ステップ 10 Cisco DNA Spaces ダッシュボードで、[Location Hierarchy] を選択します。

- [Map Service] にインポートされたロケーションマップで使用可能なキャンパスとそれに関連するビルディングとフロアが表示されます。
- Cisco Prime Infrastructure からエクスポートされ、[Map Service] を使用して Cisco DNA Spaces にインポートされたマップが、[Location Hierarchy] の下に自動的に表示されます。
- [Location Hierarchy] からロケーションを削除すると、[Map Service] からも削除されます。

（注）
- Cisco CMX の場合、ロケーション階層の [More Actions] を使用してキャンパス、ビルディング、およびその他の子ロケーションを追加することはできません。**[Setup]** > **[Map Service]** でロケーションを更新する必要があります。ただし、ゾーン（AP ゾーン）を追加することはできません。ロケーション階層からロケーションをグループ化または削除できます。ロケーション階層からロケーションを削除すると、そのロケーションは [Map Service] からも削除されます。詳細については、Cisco CMX を使用したシスコ ワイヤレス コントローラのロケーション階層の管理 （52 ページ）を参照してください。
- Cisco Prime でのロケーションの更新を Cisco DNA Spaces で同期するには、最新のマップをマップサービスにアップロードする必要があります。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラまたはシスコ ワイヤレス コントローラ（Cisco CMX なし）のロケーション階層の定義

次のいずれかのコネクタを使用して、Cisco AireOS ワイヤレスコントローラ（CMX なし）または Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを Cisco DNA Spaces に接続できます。

- Cisco WLC Direct Connect
- Cisco DNA Spaces コネクタ

これらのコネクタでサポートされる機能の詳細については、各種コネクタがサポートする機能（244 ページ）を参照してください。

Cisco WLC Direct Connect または Cisco DNA Spaces コネクタを使用してコントローラを Cisco DNA Spaces に接続すると、次のいずれかの方法を使用して、ロケーションをロケーション階層にインポートできます。

- [Access Point Prefix]：このオプションを使用している場合は、ロケーション階層にネットワーク、グループ、およびゾーンのみを追加できます。シスコ ワイヤレス コントローラを Cisco DNA Spaces に接続し、ロケーション階層を Cisco DNA Spaces ダッシュボードにインポートする方法の詳細については、アクセス ポイント プレフィックスを使用したロケーションのインポート （37 ページ）を参照してください。または、Cisco DNA Spaces ダッシュボードの [Setup] > [Wireless Networks] で、[Connect WLC/Catalyst 9800 Directly] の設定手順を参照することもできます。
- [Importing from Maps]：このラジオボタンは現在無効になっています。現在、マップを介してロケーションをインポートするには、**[Setup]** > **[Map Service]** を使用する必要があります。マップを使用すると、Cisco Prime、Campus-Building-Floor と同じ階層構造で場所をインポートできます。ロケーション階層のロケーションを表示するには、ロケーションマップを Cisco Prime Infrastructure からエクスポートして、そのマップを Cisco DNA Spaces ダッシュボードの [Map Service] オプションにアップロードする必要があります。マップを Cisco DNA Spaces にインポートすると、マップデータはロケーション階層に自動的に反映されます。マップサービスを使用したロケーションのインポートの詳細については、マッ

プサービスを使用したロケーションのロケーション階層へのインポート （39 ページ）を参照してください。

（注）

- 以前に Cisco DNA Spaces で Cisco CMX を使用していた場合、Cisco DNA Spaces でシスコ ワイヤレス コントローラを直接使用するように移行した場合は、レポートとプロキシミティルールが影響を受けます。レポートは、新しいロケーション構成に基づいて表示されます。また、キャプティブポータルを表示したり、通知を送信したりするには、プロキシミティルールを再構成する必要があります。
- 既存のロケーション階層に対して、マップサービスを使用してロケーションを再インポートすると、重複する AP（すでにロケーション階層に存在し、新しくインポートされたマップにも存在する AP）がマップベースの階層に移動されます。したがって、レポートおよびプロキシミティルールが影響を受けます。また、キャプティブポータルを表示したり、通知を送信したりするには、プロキシミティルールを再構成する必要があります。

.

アクセス ポイント プレフィックスを使用したロケーションのインポート

ステップ 1 ロケーションを Cisco DNA Spaces にインポートするには、Cisco DNA Spaces ダッシュボードの左上にある 3 本線のメニューアイコンをクリックします。

ステップ 2 [Location Hierarchy] を選択します。

ステップ 3 [Location Hierarchy] ウィンドウで、顧客名（ルート名）の右端にある [More Actions] をクリックします。

ステップ 4 [Add a Wireless Network] をクリックします。

ステップ 5 [Network Settings] ドロップダウンリストから、[WLC Direct Connect] を選択します。

ステップ 6 [Access Point Prefix] オプションボタンをクリックします。

インポートされたシスコ ワイヤレス コントローラが一覧表示されます。

（注） シスコ ワイヤレス コントローラは、そのシスコ ワイヤレス コントローラを Cisco DNA Spaces にインポートするように設定した場合にのみリストに表示されます。

ステップ 7 シスコ ワイヤレス コントローラを選択し、[Next] をクリックします。

このシスコ ワイヤレス コントローラは、プライマリ シスコ ワイヤレス コントローラとして機能します。

ステップ 8 セカンダリコントローラとして別のシスコ ワイヤレス コントローラを選択し、[Next] をクリックします。

（注） この機能は、プライマリコントローラがダウンした場合に、同じ AP を含むセカンダリ シスコ ワイヤレス コントローラで Cisco DNA Spaces を管理するのに役立ちます。

セカンダリコントローラはオプションです。[Skip] ボタンをクリックすると、セカンダリコントローラを選択せずに次の画面に移動できます。

ステップ 9 追加するネットワークを選択します。

（注） Cisco DNA Spaces は、AP 名のプレフィックスに基づいて AP を自動的にグループ化し、ネットワークを作成します。ネットワークでグループ化されていない AP は、「Unconfigured」という名前でリストに表示されます。

（注） あるネットワークを選択していない場合、そのネットワーク内の AP は、「Unconfigured」という名前でロケーション階層に追加されます。

ステップ 10 [完了（Done）] をクリックします。

選択したプライマリコントローラとセカンダリコントローラの AP がロケーション階層に一覧表示されます。

ステップ 11 ロケーション階層で、ネットワークの右端にある [More Actions] アイコンをクリックし、次に [Add Zone] をクリックします。

ステップ 12 表示されるウィンドウで、ゾーンの名前を入力し、ゾーンに含める AP を選択します。

ステップ 13 同様に、必要なすべてのゾーンを作成します。

ステップ 14 すでに Cisco CMX を使用してロケーション階層を作成している場合は、そのロケーション階層を削除し、キャプティブポータルルール、エンゲージメントルール、ロケーションペルソナルールなどのルールを再設定します。

（注）
- ロケーション階層を設定した後、ロケーションのタイムゾーンが定義されていることを確認します。定義されたタイムゾーンによって、Cisco DNA Spaces のルールとレポートが影響を受けます。
- シスコ ワイヤレス コントローラに AP を追加するときは、Cisco DNA Spaces での自動ネットワーク作成を容易にするため、適切な命名規則に従います（該当するプレフィックスを使用）。
- シスコ ワイヤレス コントローラで、新しい AP がシスコ ワイヤレス コントローラに追加されると、追加された AP は、次のシスコ ワイヤレス コントローラ同期の際に自動的にインポートされます。インポートされた AP がシスコ ワイヤレス コントローラから削除された場合、この変更は 48 時間経過しないと Cisco DNA Spaces に反映されません。
- シスコ ワイヤレス コントローラでは、Cisco DNA Spaces を使用して、異なるプレフィックスを持つアクセスポイントを 1 つのネットワークでグループ化できます。ネットワークをロケーション階層にインポートした後、ネットワークをクリックして、さまざまなプレフィックスの AP を追加します。ロケーション階層でネットワークロケーションをクリックすると、[Location Info] タブに、そのネットワークにさまざまなプレフィックスの AP を追加するための新しい [Access Points Prefix Used] オプションが表示されます。プレフィックスを追加すると、指定されたプレフィックスを持つ、未構成のネットワークに属する AP がこのネットワークに移動します。[Access Points Prefix Used] オプションは、ネットワークロケーションでのみ使用できます。ただし、[Access Points Prefix Used] オプションを未構成のネットワークに対して使用することはできません。

次のタスク

プライマリコントローラを変更したり、セカンダリコントローラを追加したりすることができます。さまざまなプレフィックスの AP を 1 つのネットワークに追加することもできます。詳細については、シスコ ワイヤレス コントローラまたは Cisco Catalyst 9800 シリーズ コントローラのロケーション階層の管理（WLC Direct Connect または Cisco DNA Spaces コネクタを使用）（56 ページ）を参照してください。

マップサービスを使用したロケーションのロケーション階層へのインポート

シスコ ワイヤレス コントローラまたは Cisco Catalyst 9800 シリーズ ワイヤレスコントローラが WLC Direct Connect または Cisco DNA Spaces コネクタを介して Cisco DNA Spaces に接続されている場合、マップサービスを使用してロケーションをロケーション階層にインポートできます。このオプションを使用している場合は、同じ階層構造（キャンパス - ビルディング - フロア）に場所をインポートできます。

（注） マップは、Cisco Prime または Cisco DNA Center からエクスポートできます。Cisco Prime Infrastructure または Cisco DNA Center からエクスポートされ、[Map Service] を使用して Cisco DNA Spaces にインポートされたマップは、[Location Hierarchy] の下に自動的に表示されます。

Cisco Prime からマップをエクスポートして、ロケーションをロケーション階層にインポートするには、次の手順を実行します。

ステップ 1 Cisco Prime Infrastructure にログインします。

ステップ 2 [Settings /Getting Started] ウィンドウで、ウィンドウの左上（Cisco ロゴの近く）にある円形のアイコンをクリックします。

ステップ 3 表示されるウィンドウで、左ペインの [Maps] をクリックします。

ステップ 4 [Wireless Maps] 領域で、[Site Maps (Deprecated)] をクリックします。

（注） [Site Maps (New)] オプションを使用して、新しい場所を追加できます。

ステップ 5 [Go] の近くにあるドロップダウンリストをクリックし、[Export Maps] を選択します。

ステップ 6 [移動（Go）] をクリックします。

ステップ 7 ロケーションマップのツリービューから、エクスポートする親ロケーション（CMX ノード）を選択し、[Export] をクリックします。

（注） [Include Map Information] チェックボックスがオンになっていることを確認します。

ステップ 8 ロケーションマップをコンピュータに保存します。

（注） マップは gzip 形式でダウンロードし、同じ形式で Cisco DNA Spaces にアップロードする必要があります。

ステップ 9 Cisco DNA Spaces ダッシュボードで、[Setup] > [Map Service] を選択します。

ステップ 10 ウィンドウの左上にある [Upload] をクリックし、Cisco Prime Infrastructure からダウンロードしたロケーションマップを選択します。

ロケーションマップが [Map Service] にアップロードされます。

ステップ 11 Cisco DNA Spaces ダッシュボードで、[Location Hierarchy] を選択します。

- [Map Service] にインポートされたロケーションマップで使用可能なキャンパスとそれに関連するビルディングとフロアが表示されます。
- Cisco Prime Infrastructure からエクスポートされ、[Map Service] を使用して Cisco DNA Spaces にインポートされたマップが、[Location Hierarchy] の下に自動的に表示されます。
- [Location Hierarchy] からロケーションを削除すると、[Map Service] からも削除されます。

（注） ロケーション階層を設定した後は、ロケーションのタイムゾーンが定義されていることを確認してください。定義されたタイムゾーンによって、Cisco DNA Spaces のルールとレポートが影響を受けます。

- ロケーションが [Map Service] を使用してインポートされた場合、ロケーション階層の [More Actions] を使用してキャンパス、ビルディング、およびその他の子ロケーションを追加することはできません。**[Setup]** > **[Map Service]**でロケーションを更新する必要があります。ただし、ゾーン（AP ゾーン）を追加することはできません。ロケーション階層からロケーションをグループ化または削除できます。ロケーション階層からロケーションを削除すると、そのロケーションは [Map Service] からも削除されます。詳細については、Cisco CMX を使用したシスコ ワイヤレス コントローラのロケーション階層の管理 （52 ページ）を参照してください。

ロケーション階層の管理

顧客の名前の変更

顧客の名前を変更するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Location Hierarchy] をクリックします。
ステップ 2 [Location Hierarchy] ウィンドウで、顧客名の右端にある [More Actions] をクリックします。
ステップ 3 [Rename <ルート名>] をクリックします。
ステップ 4 表示される [Rename root] ウィンドウに新しい顧客名を入力します。
ステップ 5 [Rename] をクリックします。

ワイヤレスネットワークの追加

Cisco DNA Spaces は、Cisco AireOS ワイヤレスコントローラ（シスコ ワイヤレス コントローラ）、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ、および Cisco Meraki をサポートしています。[Add a Wireless Network] オプションを使用して、複数のワイヤレスネットワークをロケーション階層に追加できます。

[Add a Wireless Network] ウィンドウの [Add a Wireless Network] ドロップダウンリストには、次の 3 つのオプションがあります。

- [Meraki]：Meraki ネットワークのロケーション階層を定義します。
- [CMX On Prem]：このオプションは機能しなくなります。ロケーション階層へのロケーションのインポートは、**[Setup]** > **[Map Service]** で管理されます。
- [WLC Direct Connect]：Cisco Catalyst 9800 シリーズ ワイヤレス コントローラまたはシスコ ワイヤレス コントローラ（Cisco CMX なし）のロケーション階層を定義します。

[Add a Wireless Network] オプションを使用した Cisco CMX ノード、Cisco Meraki 組織、またはシスコ ワイヤレス コントローラ アクセス ポイントの追加に関する詳細については、ロケーション階層の定義 （27 ページ）を参照してください。

ロケーションのメタデータの追加

メタデータを使用してロケーションをグループ化できます。プロキシミティルールを定義するときに、このメタデータを使用できます。このメタデータを使用して、Behavior Metrics アプリのブランドを定義することもできます。

ロケーションのメタデータを追加するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Location Hierarchy] を選択します。

ステップ 2 [Location Hierarchy] ウィンドウで、メタデータを追加するロケーションの [More Actions] をクリックします。

ステップ 3 [Add/Edit Metadata] をクリックします。

ステップ 4 表示される [Add Metadata for <location>] ウィンドウで、次の手順を実行します。

a) [Key] フィールドに、メタデータキーを入力します。
b) 値のフィールドにキーの値を入力します。
c) [**保存（Save）**] をクリックします。

次のタスク

（注） 同様に、このメタデータが必要な他のロケーションにメタデータを追加します。

ロケーションのメタデータの更新

ロケーションのメタデータを更新するには、次の手順を実行します。

ステップ 1 [Location Hierarchy] ウィンドウで、ロケーションのメタデータを更新するロケーションの右端にある [More Actions] をクリックします。

ステップ 2 [Add/Edit Metadata] をクリックします。

ステップ 3 [Add Metadat for <location>] ウィンドウが表示されたら、更新するメタデータをクリックします。

ステップ 4 必要な変更を行って、[Update] をクリックします。

次のタスク

（注） そのメタデータの [Delete] ボタンをクリックすると、ロケーション メタデータを削除できます。

ロケーションのタイム ゾーンの定義または変更

ロケーション階層内のさまざまなロケーションにタイムゾーンを定義できます。ロケーションのタイム ゾーンを定義するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Location Hierarchy] を選択します。

ステップ 2 [Location Hierarchy] ウィンドウで、タイムゾーンを定義するロケーションをクリックします。

ステップ 3 [Location Info] タブで、[Location Data] の [Edit] をクリックします。

[Location Information] ポップアップウィンドウが表示されます。

ステップ 4 [Select Time Zone] ドロップダウンリストから、このロケーションに設定するタイムゾーンを選択します。

ステップ 5 [更新（Update）] をクリックします。

タイム ゾーンがロケーションに定義されます。

次のタスク

（注） ロケーションでは設定されたタイム ゾーンに基づいて通知が送信されます。

ロケーションの情報の追加

ロケーション階層では各ロケーションのアドレスなどの情報を指定できます。

ロケーションのロケーション情報を追加するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードの左上にある 3 本線のメニューアイコンをクリックします。

ステップ 2 [Location Hierarchy] を選択します。

ステップ 3 [Location Hierarchy] ウィンドウで、情報を追加するロケーションをクリックします。

ステップ 4 [Location Info] タブで、[Location Data] の [Edit] をクリックします。

ステップ 5 表示される [Location Information] ウィンドウで、特定のロケーションの情報を入力します。

ロケーションに関する次の情報を追加できます。

- ブランド
- 国
- 都道府県
- 市区町村郡
- 郵便番号
- 住所
- タイム ゾーン
- 面積（平方フィートまたは平方メートル）
- 収容人数制限（最大キャパシティ）

ステップ 6 [更新（Update）] をクリックします。

追加されたロケーション情報は、[Location Info] タブの [Location Data] エリアに表示されます。

（注） ロケーション情報を指定しない場合、そのロケーションは親ロケーションの情報を継承します。親ロケーションから継承されたロケーション情報はオレンジ色で表示されます。ただし、ロケーションごとにロケーション情報を更新することをお勧めします。

ロケーションの検索

名前を使用してロケーション階層内のロケーションを検索できます。ロケーション階層のロケーションを検索するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Location Hierarchy] を選択します。

[Location Hierarchy] ウィンドウが表示されます。

ステップ 2 [Search] フィールドに、検索するロケーションの名前を入力します。

ロケーションがロケーション階層で強調表示されます。

アクセス ポイントの検索

名前または MAC アドレスを使用してアクセス ポイントを検索できます。

ロケーション階層のアクセス ポイントを検索するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Location Hierarchy] を選択します。

[Location Hierarchy] ウィンドウが表示されます。

ステップ 2 [Search] フィールドに、検索するアクセスポイントの名前または MAC アドレスを入力します。

アクセス ポイントが強調表示されます。

ロケーションのマップの管理

マップはデフォルトでワイヤレスネットワークのマップ設定に基づいて表示されます。

ロケーションのマップを表示するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Location Hierarchy] を選択します。

ロケーション階層を示す [Location Hierarchy] ウィンドウが表示されます。

ステップ 2 ロケーション階層で、マップを表示するロケーションをクリックします。

ステップ 3 [Maps] タブをクリックします。

マップが [Maps] タブに表示されます。

アクセス ポイントの管理

ゾーンへのアクセス ポイントを追加または削除できます。

ゾーンへのアクセス ポイントの追加

ゾーンにアクセス ポイントを追加するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Location Hierarchy] を選択します。

ロケーション階層を示す [Location Hierarchy] ウィンドウが表示されます。

ステップ 2 ロケーション階層で、アクセス ポイントを追加するゾーンをクリックします。

ステップ 3 [Modify Access Points] をクリックします。

ステップ 4 追加するアクセス ポイントのチェックボックスをオンにします。

ステップ 5 [Add] をクリックします。

アクセス ポイントが、ゾーンに追加されます。

次のタスク

（注） そのゾーンにアクセスポイントがない場合、ボタンの名前は [Add Access Points] になります。

（注） Cisco Unified Wireless Network の場合、アクセスポイントをインポートするには、Cisco CMX にパブリックにアクセスできる必要があります。デフォルトの Cisco Unified Wireless Network インストールでは、ポート 80 とポート 443 が開いている必要があります。詳細については、「Cisco DNA Spaces を展開するための帯域幅要件」のセクションを参照してください。

ゾーンからのアクセス ポイントの削除

ゾーンからアクセス ポイントを削除するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Location Hierarchy] を選択します。

ロケーション階層を示す [Location Hierarchy] ウィンドウが表示されます。

ステップ 2 ロケーション階層で、アクセス ポイントを削除するゾーンをクリックします。

ステップ 3 [Modify Access Points] をクリックします。

ステップ 4 削除するアクセスポイントのチェックボックスをオフにします。

ステップ 5 [Add] をクリックします。

アクセス ポイントが、ゾーンから削除されます。

ロケーションのアクセスポイントの表示

各ロケーションにあるアクセスポイントを表示できます。理想的には、アクセスポイントはフロアまたはゾーンに属しています。

ロケーションのアクセスポイントを表示するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Location Hierarchy] を選択します。

ロケーション階層を示す [Location Hierarchy] ウィンドウが表示されます。

ステップ 2 ロケーション階層で、アクセスポイントを表示するロケーションをクリックします。

ステップ 3 [Access Points] タブをクリックします。

そのロケーションに関連付けられているアクセスポイントが表示されます。

次のタスク

（注） ロケーションの [Access Points] リンクは、そのロケーションに少なくとも 1 つのアクセスポイントが存在する場合にのみ有効になります。

グループの管理

Cisco DNA Spaces では、グループ名の名前変更、グループの編集、および個別のグループの削除を行うことができます。

グループの作成

グループ化を使用して、ロケーションのセットに固有のプロキシミティルールを作成することができます。ロケーション階層の上位レベルにグループを作成できます。

Cisco Unified Wireless Network の場合、ロケーション階層内の CMX ノードまたはキャンパスをグループ化できます。たとえば、あるグループの下で Campus 1 と Campus 2 をグループ化し、別のグループの下で Campus 3 と Campus 4 をグループ化することができます。また、これらのグループの下にサブグループを作成することもできます。Meraki の場合、ロケーション階層の Cisco Meraki 組織またはネットワークをグループ化できます。たとえば、あるグループの下で Network 1 と Network 2 をグループ化し、別のグループの下で Network 3 と Network 4 をグループ化することができます。また、これらのグループの下にサブグループを作成することもできます。

Cisco Unified Wireless Network と Meraki の両方のワイヤレス ネットワーク ノードを含むグループを作成することもできます。ただし、Cisco Unified Wireless Network と Meraki の下位レベルのロケーションをグループ化することはできません。たとえば、キャンパスと Meraki ネットワークをグループ化することはできません。

ロケーションに対してグループを作成するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Location Hierarchy] をクリックします。

ステップ 2 [Location Hierarchy] ウィンドウで、グループを追加するロケーションの右端にある [More Actions] をクリックします。

ステップ 3 [Create Group] をクリックします。

ステップ 4 表示されるウィンドウで、次の手順を実行します。

a) グループの名前を入力します。

b) グループの下に追加するロケーションを選択します。

（注） 選択可能なロケーションは、ロケーション階層においてグループを追加するロケーションによって異なります。たとえば、（ルートレベルではなく）顧客名の下にグループを追加する場合、第一レベルのロケーション（CMX ノード、Cisco Meraki 組織など）を選択することができます。CMX ノードの下にグループを追加すると、その CMX ノードの下のキャンパスのみ選択できます。

c) [Add] をクリックします。

次のタスク

ヒント ロケーションのない親グループと、ロケーションのあるサブグループが必要な場合は、まず、サブグループの一部になる必要があるロケーションすべてを含む親グループを作成します。それから親グループの下にサブグループを作成します。親グループに追加されたロケーションを選択することができます。サブグループの下に追加するロケーションを選択します。同様に、親グループの下にさらにサブグループを作成することができます。

（注） ロケーションはいつでもグループに追加できます。

グループの名前変更

グループの名前を変更するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Location Hierarchy] を選択します。

ロケーション階層を示す [Location Hierarchy] ウィンドウが表示されます。

ステップ 2 ロケーション階層で、名前を変更するグループの [More Actions] をクリックします。

ステップ 3 [Rename "group name"] をクリックします。

ステップ 4 表示される [Rename group] ウィンドウに、グループの新しい名前を入力します。

ステップ 5 [Rename] をクリックします。

グループの編集

ロケーションをグループに追加またはグループから削除できます。

グループを編集するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Location Hierarchy] を選択します。

ロケーション階層を示す [Location Hierarchy] ウィンドウが表示されます。

ステップ 2 ロケーション階層で、編集したいグループの [More Actions] をクリックします。

ステップ 3 [Edit group] をクリックします。

ステップ 4 表示される [Edit Group] ウィンドウで、グループの一部にするロケーションのチェックボックスをオンにします。

ステップ 5 [更新（Update）] をクリックします。

グループの削除

グループを削除するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Location Hierarchy] を選択します。

ロケーション階層を示す [Location Hierarchy] ウィンドウが表示されます。

ステップ 2 ロケーション階層で、削除するグループの右端の [More Actions] をクリックします。

ステップ 3 [Delete group] ボタンをクリックします。

次のタスク

（注） グループを削除するには、そのグループのロケーションとサブグループを（存在する場合）先に削除する必要があります。

（注） プロキシミティルールに関連付けられたゾーンは削除できません。

ゾーンの管理

Cisco Unified Wireless Network または Meraki 用に作成されたゾーンの名前を変更、削除できます。

ゾーンの名前変更

ゾーンの名前を変更するには、次の手順を実行します

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Location Hierarchy] を選択します。

[Location Hierarchy] ウィンドウが表示されます。

ステップ 2 ロケーション階層で、名前を変更するゾーンの [More Actions] をクリックします。

ステップ 3 [Rename "zone name"] をクリックします。

ステップ 4 表示される [Rename-zone] ウィンドウに、ゾーンの新しい名前を入力します。

ステップ 5 [Rename] をクリックします。

ゾーンの削除

ゾーンを削除するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Location Hierarchy] を選択します。

[Location Hierarchy] ウィンドウが表示されます。

ステップ 2 ロケーション階層で、削除するフロアの [More Actions] をクリックします。

ステップ 3 [Delete zone] をクリックします。

次のタスク

（注） プロキシミティルールに関連付けられたゾーンは削除できません。

Meraki のロケーション階層の管理

Meraki に属するロケーションの名前を変更したり、ロケーションを削除したりできます。

ネットワークにフロアを追加する

ネットワークにフロアを追加するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Location Hierarchy] を選択します。

ステップ 2 [Location Hierarchy] ウィンドウで、フロアを作成するネットワークの右端にある [More Actions] をクリックします。

ステップ 3 表示される [Add Floor] ウィンドウで、ネットワークに追加するフロアを選択します。

ステップ 4 [Add] をクリックします。

フロアがネットワークに追加されます。

Cisco Meraki 組織の名前変更

Cisco Meraki 組織の名前を変更するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Location Hierarchy] を選択します。

ロケーション階層を示す [Location Hierarchy] ウィンドウが表示されます。

ステップ 2 ロケーション階層で、名前を変更する組織の [More Actions] をクリックします。

ステップ 3 [Rename "Organization Name"] をクリックします。

ステップ 4 表示される [Rename-Meraki] ウィンドウに、Cisco Meraki 組織の新しい名前を入力します。

ステップ 5 [Rename] をクリックします。

Cisco Meraki 組織の削除

Cisco Meraki 組織を削除するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Location Hierarchy] を選択します。

ロケーション階層を示す [Location Hierarchy] ウィンドウが表示されます。

ステップ 2 ロケーション階層で、削除する Cisco Meraki 組織の [More Actions] をクリックします。

ステップ 3 [Delete Organization] をクリックします。

次のタスク

（注） 組織を削除するには、その組織のロケーションとグループを（存在する場合）先に削除する必要があります。

- プロキシミティルールに関連付けられた組織は削除できません。

ネットワークの名前変更

ネットワークの名前を変更するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Location Hierarchy] を選択します。

ロケーション階層を示す [Location Hierarchy] ウィンドウが表示されます。

ステップ 2 ロケーション階層で、名前を変更するネットワークの [More Actions] をクリックします。

ステップ 3 [network name] をクリックします。

ステップ 4 表示される [Rename-location] ウィンドウに、ロケーションの新しい名前を入力します。

ステップ 5 [Rename] をクリックします。

ネットワークの削除

ネットワークを削除するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Location Hierarchy] を選択します。

ロケーション階層を示す [Location Hierarchy] ウィンドウが表示されます。

ステップ 2 ロケーション階層で、削除するネットワークの [More Actions] をクリックします。

ステップ 3 [Delete network] をクリックします。

次のタスク

（注） ネットワークを削除するには、そのネットワーク内のアクセスポイントを（存在する場合）先に削除する必要があります。

- プロキシミティルールに関連付けられたネットワークは削除できません。

フロアの名前変更

フロアの名前を変更するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Location Hierarchy] を選択します。

ロケーション階層を示す [Location Hierarchy] ウィンドウが表示されます。

ステップ 2 ロケーション階層で、名前を変更する組織の [More Actions] をクリックします。

ステップ 3 [Rename "floor name"] をクリックします。

ステップ 4 表示される [Rename-floor] ウィンドウに、フロアの新しい名前を入力します。
ステップ 5 [Rename] をクリックします。

フロアの削除

フロアを削除するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Location Hierarchy] を選択します。

ロケーション階層を示す [Location Hierarchy] ウィンドウが表示されます。

ステップ 2 ロケーション階層で、削除したいフロアの [More Actions] をクリックします。
ステップ 3 [Delete floor] をクリックします。

次のタスク

（注） 削除するフロアの下にゾーンがある場合、そのゾーンは、フロアの削除の後、ネットワークの下に移動します。

（注） プロキシミティルールに関連付けられたフロアは削除できません。

Cisco CMX を使用したシスコ ワイヤレス コントローラのロケーション階層の管理

Cisco CMX を使用しているシスコ ワイヤレス コントローラの場合、ロケーション階層の [More Actions] を使用してキャンパス、ビルディング、およびその他の子ロケーションを追加することはできません。**[Setup]** > **[Map Service]** でロケーションを更新する必要があります。一方、ロケーション階層からロケーションをグループ化または削除することは可能です。

ロケーション階層からロケーションを削除すると、そのロケーションは [Map Service] からも削除されます。[Map Service] からロケーションを削除すると、AP のみがロケーション階層から削除され、階層構造はそのまま残ります。

CMX ノードの名前の変更

CMX ノードの名前を変更するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Location Hierarchy] を選択します。

ロケーション階層を示す [Location Hierarchy] ウィンドウが表示されます。

ステップ 2 ロケーション階層で、名前を変更する CMX ノードの [More Actions] をクリックします。

ステップ 3 [Rename <Cisco CMX Node>] をクリックします。

ステップ 4 表示されるウィンドウに、CMX ノードの新しい名前を入力します。

ステップ 5 [Rename] をクリックします。

次のタスク

（注） 名前の変更は Cisco CMX に反映されません。

CMX ノードの削除

ロケーション階層から CMX ノードを削除するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Location Hierarchy] を選択します。

ロケーション階層を示す [Location Hierarchy] ウィンドウが表示されます。

ステップ 2 ロケーション階層で、ロケーション階層から削除する CMX ノードの [More Actions] をクリックします。

ステップ 3 オプションをクリックして、CMX ノードを削除します。

次のタスク

（注） CMX ノードを削除するには、その CMX ノードのロケーションとグループを（存在する場合）先に削除する必要があります。

（注） プロキシミティルールに関連付けられた CMX ノードは削除できません。

キャンパスの名前変更

キャンパスの名前を変更するには、次の手順を実行します

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Location Hierarchy] を選択します。

ロケーション階層を示す [Location Hierarchy] ウィンドウが表示されます。

ステップ 2 ロケーション階層で、名前を変更するキャンパスの [More Actions] をクリックします。
ステップ 3 [Rename <campus name>] をクリックします。
ステップ 4 表示される [Rename-campus] ウィンドウに、キャンパスの新しい名前を入力します。
ステップ 5 [Rename] をクリックします。

キャンパスの削除

キャンパスを削除するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Location Hierarchy] を選択します。

ロケーション階層を示す [Location Hierarchy] ウィンドウが表示されます。

ステップ 2 ロケーション階層で、削除したいキャンパスの [More Actions] をクリックします。
ステップ 3 [Delete campus] をクリックします。

次のタスク

（注） キャンパスを削除するには、そのキャンパスの下のロケーションを（存在する場合）、先に削除する必要があります。

（注） プロキシミティルールに関連付けられたキャンパスは削除できません。

ビルディング名の変更

ビルディング名を変更するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Location Hierarchy] を選択します。

ロケーション階層を示す [Location Hierarchy] ウィンドウが表示されます。

ステップ 2 ロケーション階層で、名前を変更するビルディングの [Location Hierarchy] をクリックします。
ステップ 3 [Rename <ビルディング名>] をクリックします。
ステップ 4 表示される [Rename -network] ウィンドウに、ビルディングの新しい名前を入力します。
ステップ 5 [Rename] をクリックします。

ビルディングの削除

ビルディングを削除するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Location Hierarchy] を選択します。

ロケーション階層を示す [Location Hierarchy] ウィンドウが表示されます。

ステップ 2 ロケーション階層で、削除したいビルディングの [More Actions] をクリックします。

ステップ 3 [Delete building] をクリックします。

次のタスク

（注） ビルディングを削除するには、先にそのビルディングの下のフロアまたはゾーン（ある場合）を削除する必要があります。

（注） プロキシミティルールに関連付けられたビルディングは削除できません。

フロアの名前変更

フロアの名前を変更するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Location Hierarchy] を選択します。

ロケーション階層を示す [Location Hierarchy] ウィンドウが表示されます。

ステップ 2 ロケーション階層で、名前を変更する組織の [More Actions] をクリックします。

ステップ 3 [Rename "floor name"] をクリックします。

ステップ 4 表示される [Rename-floor] ウィンドウに、フロアの新しい名前を入力します。

ステップ 5 [Rename] をクリックします。

フロアの削除

フロアを削除するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Location Hierarchy] を選択します。

ロケーション階層を示す [Location Hierarchy] ウィンドウが表示されます。

ステップ 2 ロケーション階層で、削除するフロアの [More Actions] をクリックします。

ステップ 3 [Delete floor] をクリックします。

次のタスク

（注） 削除するフロアの下にゾーンがある場合、そのゾーンは、フロアの削除の後、ビルディングの下に移動します。

シスコ ワイヤレス コントローラまたは Cisco Catalyst 9800 シリーズ コントローラのロケーション階層の管理（WLCDirectConnectまたはCisco DNA Spaces コネクタを使用）

プライマリコントローラのネットワークの自動追加

シスコ ワイヤレス コントローラのインポート時にネットワークの選択をスキップした場合、後でいつでもネットワークを自動で追加できます。

シスコ ワイヤレス コントローラまたは Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのネットワークを自動で追加するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Location Hierarchy] を選択します。

ステップ 2 [Location Hierarchy] ウィンドウで、ネットワークを追加するワイヤレスコントローラの [More Actions] アイコンをクリックします。

ステップ 3 [Edit] をクリックします。

ステップ 4 表示される [Edit Controller] ウィンドウで、[Auto Network Creation] チェック ボックスをオンにします。

ステップ 5 [完了（Done）] をクリックします。

同じプレフィックスを持つ AP がグループ化され、ネットワークが自動的に形成されます。自動作成されたネットワークに追加されていない AP は、ネットワーク名「未設定」の下にリストされます。

次のタスク

（注） 自動ネットワークの設定後にワイヤレスコントローラに追加された AP のみがグループ化されます。「未設定」のネットワーク名の下にある既存の AP は、この設定に基づいて自動的にグループ化されません。ただし、「未設定」ネットワーク内の既存の AP と同じプレフィックスを持つ新しい AP がワイヤレスコントローラに追加された場合、既存の AP は、追加された新しい AP とグループ化されます。

プライマリコントローラのネットワークの手動追加

シスコ ワイヤレス コントローラまたは Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのネットワークを手動で追加するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Location Hierarchy] を選択します。

ステップ 2 [Location Hierarchy] ウィンドウで、ネットワークを定義するシスコ ワイヤレス コントローラの [More Actions] アイコンをクリックします。

ステップ 3 [Add Network] をクリックします。

[Add Nework] ウィンドウが表示されます。

ステップ 4 表示される [Name] フィールドに、ネットワークの名前を入力します。

ステップ 5 表示される [Access Point Prefix] フィールドに、AP がネットワークの下でグループ化するために必要なプレフィックスを入力し、[Fetch] をクリックします。

ネットワークがロケーション階層にリストされます。

（注） ワイヤレスネットワークでは複数のプレフィックスがサポートされています。ただし、ネットワークを追加する場合は、1 つのプレフィックスの AP のみを追加できます。このネットワークに別のプレフィックスを持つアクセスポイントを追加する場合は、追加後にネットワークを編集する必要があります。複数のプレフィックスを持つ AP の追加の詳細については、複数のプレフィックスを持つ AP のネットワークへの追加 （57 ページ） を参照してください。

ステップ 6 [完了（Done）] をクリックします。

ネットワークは、前述のプレフィックスを持つ AP と共に作成されます。

複数のプレフィックスを持つ AP のネットワークへの追加

複数のプレフィックスを持つ AP をネットワークに追加できます。たとえば、プレフィックスが AB、BC、および CA の AP があり、AB および BC の AP を 1 つのワイヤレスネットワークにグループ化する場合、それが可能です。

複数のプレフィックスを持つ AP を、シスコ ワイヤレス コントローラまたは Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのネットワークに追加するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、ウィンドウの左上にある 3 本線のメニューアイコンをクリックします。

ステップ 2 [Location Hierarchy] を選択します。

ステップ 3 [Location Hierarchy] ウィンドウで、複数のプレフィックスを持つ AP を追加するネットワークをクリックします。

ステップ 4 [Location Info] タブで、[Access Points Prefix Used] の [Edit] をクリックします。

ステップ 5 表示される [Edit Prefix] ウィンドウの [Prefix] フィールドに、プレフィックスを入力します。

入力されたプレフィックスを持つ AP が一覧表示されます。

ステップ 6 [**プレフィックスの追加（Add Prefix**）] をクリックします。

これで、新しく追加されたプレフィックスが、ウィンドウの右側のペインの [Added Prefixes] の下にリストされます。[Add Prefix] は、入力されたプレフィックスを持つ AP がある場合にのみ有効になります。

ステップ 7 [**保存（Save**）] をクリックします。

プレフィックスを追加した後、このプレフィックスを持つ [unconfigured] のネットワークの下にある AP がこのネットワークに移動します。

プレフィックスを削除するには、[Added Prefixes] の下にあるプレフィックスにカーソルを合わせ、表示される [Delete] アイコンをクリックします。

（注） [Access Points Prefix Used] オプションは、ネットワークロケーションでのみ、[Location Info] タブで使用できます。ただし、[Access Points Prefix Used]オプションを [Unconfigured] のネットワークに使用することはできません。

追加のセカンダリコントローラの追加

シスコ ワイヤレス コントローラのインポート時にセカンダリコントローラの追加をスキップした場合、後でいつでも追加できます。セカンダリコントローラを設定した場合でも、複数のセカンダリコントローラを追加できます。

シスコ ワイヤレス コントローラのセカンダリコントローラを追加するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Location Hierarchy] を選択します。

ステップ 2 [Location Hierarchy] ウィンドウで、セカンダリコントローラを追加するシスコ ワイヤレス コントローラの [More Actions] アイコンをクリックします。

ステップ 3 [Edit] をクリックします。

ステップ 4 表示される [Edit Controller] ウィンドウで、追加するコントローラの [Add More] をクリックします。

ステップ 5 表示される [Add additional controller] ウィンドウで、セカンダリコントローラとして設定するシスコ ワイヤレス コントローラを選択します。

（注） プライマリコントローラに類似したシスコ ワイヤレス コントローラ（同じ AP を持っている）がリストの一番上に表示されます。

ステップ 6 [Add] をクリックします。

これで、新しく設定したシスコ ワイヤレス コントローラがセカンダリ コントローラになりました。

（注） 複数のシスコ ワイヤレス コントローラをセカンダリコントローラとして追加できます。ただし、一度に追加できるコントローラは 1 つだけです。

セカンダリコントローラの削除

セカンダリコントローラを削除するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードの左上に表示される 3 本線のメニューアイコンをクリックします。

ステップ 2 [Location Hierarchy] を選択します。

ステップ 3 ロケーション階層で、セカンダリ シスコ ワイヤレス コントローラを削除するプライマリコントローラで [More Actions] アイコンをクリックします。

ステップ 4 [Edit] をクリックします。

表示された [Edit Controller] ウィンドウで、その PrimaryController に追加されたセカンダリコントローラが [Additional Controllers] の下に一覧表示されます。

ステップ 5 削除するセカンダリコントローラで [Delete] アイコンをクリックします。

ステップ 6 表示されるウィンドウで、削除を確定します。

これで、セカンダリコントローラが削除されました。

次のタスク

（注） セカンダリコントローラを削除すると、このセカンダリコントローラ固有の AP（プライマリコントローラまたは他のセカンダリコントローラにない AP）も削除されます。

プライマリコントローラの名前変更

プライマリコントローラの名前を変更するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Location Hierarchy] を選択します。

ステップ 2 [Location Hierarchy] で、名前を変更するシスコ ワイヤレス コントローラの [More Actions] アイコンをクリックします。

ステップ 3 [Rename <cisco wireless controller>] をクリックします。

ステップ 4 表示される [Rename WLC] ウィンドウで、必要な名前を入力し、[Rename] をクリックします。

これで、シスコ ワイヤレス コントローラの名前が、指定された新しい名前に変更されました。

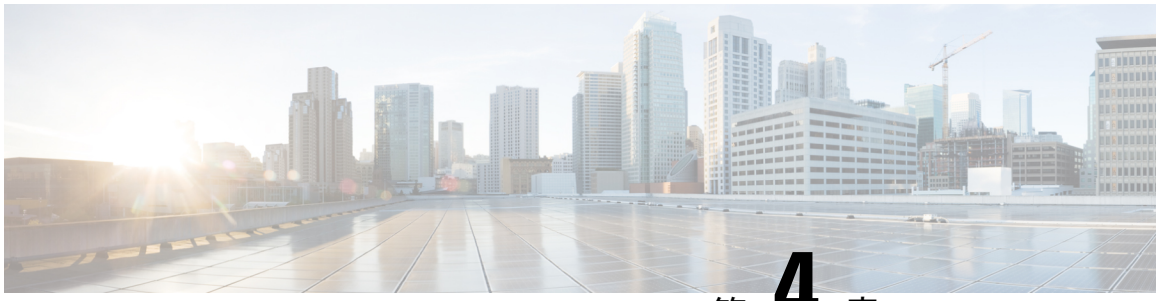
（注） 名前の変更は、シスコ ワイヤレス コントローラには反映されません。

ロケーション階層での累積数の表示

ロケーション階層では、AP、近接ルール、およびロケーションの子ロケーションの数が累積値として表示されます。ロケーションの数は、ロケーションとそのすべての子ロケーションの数の合計になります。たとえば、あるフロアの AP の総数は、フロアの AP とそのフロアの下の各ゾーンの AP の合計になります。

数がゼロのロケーションには、詳細を表示するためのリンクがありません。ロケーションをクリックすると、そのロケーションの AP、近接ルール、ロケーション、およびユーザーを表示できます。ロケーションパラメータの詳細は、関連付けられたロケーションからのみ表示できます。

近接ルールの場合、一意のルールのみがカウントされます。たとえば、フロアの2つのゾーンがあるエンゲージメントルールに含まれている場合、フロアのルールをカウントするとき、そのエンゲージメントルールは 1 回だけカウントされます。



第 4 章

行動メトリクス

この章では、行動メトリクスレポートについて説明します。

行動メトリクスの概要

[Behavior Metrics] アプリを使用すると、ビジネスのパフォーマンスについての知見を提供するさまざまなレポートを表示できます。デフォルトでは、レポートには前月のデータが含まれます。特定のロケーションと月のレポートを表示するようにフィルタ処理できます。タグに基づいてレポートをフィルタ処理することもできます。

Cisco Digital Network Architecture（DNA）Spaces のインストール後、最初のレポートが表示されるまでに 1 か月かかります。この期間中、サンプルレポートを表示できます。この期間中に [My Data] オプションに切り替えることで、レポートがどのように構成されているかを確認することもできます。レポートの準備ができたら、通知が送信されます。

行動メトリクスアプリは、次のタイプのレポートを表示します。

- 行動メトリクス（ビジネスメトリクス） （65 ページ）

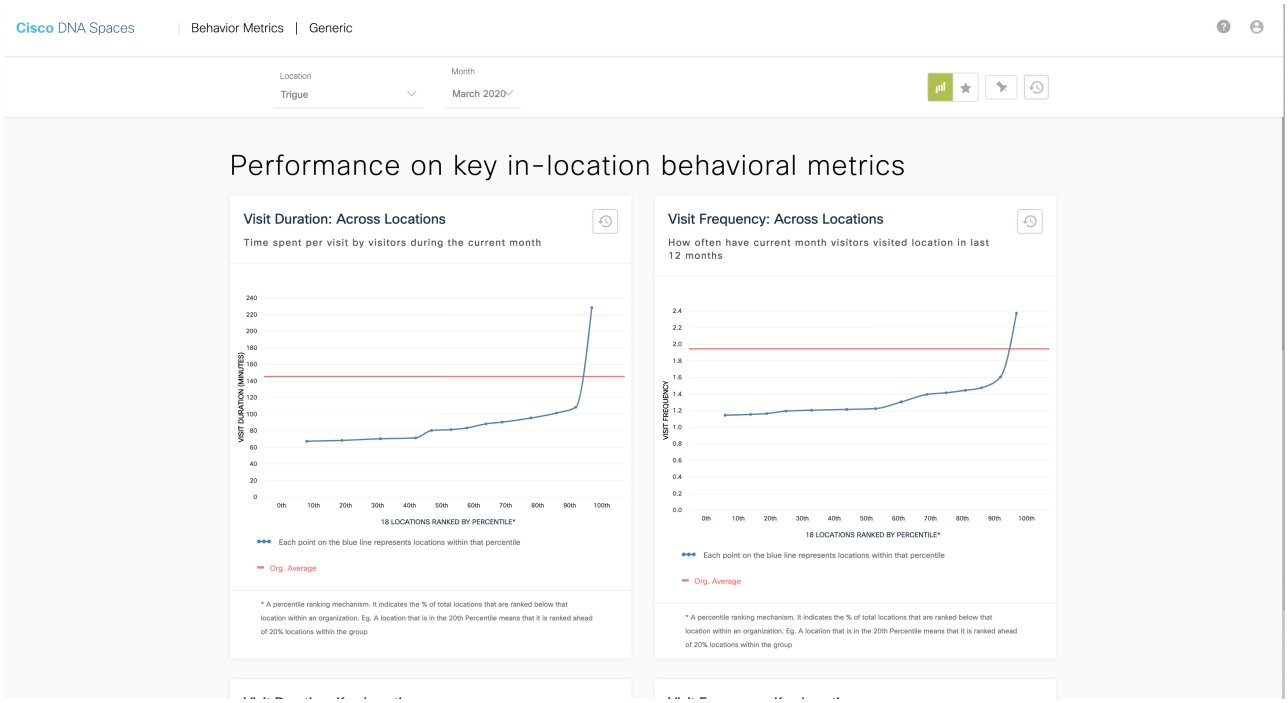
行動メトリクスレポートの表示

行動メトリクスアプリが提供するさまざまなレポートを表示するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Behavior Metrics] をクリックします。

行動メトリクスレポートが表示されます。

図 *6:* 行動メトリクスレポート



ステップ 2 ページ上部の対応するドロップダウンリストで、レポートを表示するロケーション、タグ、および月を指定します。

次のタスク

（注）

- デフォルトでは、組織全体のレポートが表示されます。組織レベルでのアクセス権がない場合、アクセス権のある最上位のロケーションのレポートが表示されます。ネットワークレベルまでのロケーションをフィルタ処理できます。
- フィルタ処理されたロケーションのレポートに記載されているパーセンテージまたはカウントは、すべての子ロケーションの合計値または平均値になります。たとえば、フィルタ処理されたロケーションがネットワークの場合、ネットワークに表示される訪問数は、そのネットワークの全フロアにおける訪問数の合計になります。
- 顧客が小売業を営んでいる場合、[Behavior Metrics] ウィンドウの上部に、[Retail] というタイトルが [Behavior Metrics] とともに表示されます。[Workspaces] 分野の場合、[Workspaces] というタイトルが [Behavior Metrics] とともに表示されます。他のビジネスの場合は、[Generic] になります。

ベンチマーク

[Organization Benchmark]：組織全体の平均値を表示します。たとえば、組織がシスコの場合、「Average Visit Duration」の [Organization Benchmark] は、シスコの「平均訪問時間」を示します。

[Industry Benchmark]：企業が属する業界の平均値を表示します。たとえば、小売業の場合、訪問時間の分布グラフには、小売業の平均訪問時間が表示されます。業界ベンチマークの平均値は、Cisco DNA Spaces をインストールした他のクライアントから取得したデータに限定されています。

[Country Benchmark]：特定の国でタグ付けされたロケーションの平均値を表示します。たとえば、タグとして「米国」を選択すると、平均訪問時間グラフには米国に対応するバーが表示されます。これは、米国でタグ付けされたすべてのロケーションの平均訪問時間です。国タグに関連付けられたロケーションの総数も表示されます。特定の国のタグの下にあるロケーションが他のタグに関連付けられている場合、平均訪問時間などの一部のグラフでは、そのタグの平均値も表示されます。

[State Benchmark]：特定の州でタグ付けされたロケーションの平均値を表示します。[state] タグを選択すると、一部のレポートでは 2 つのバーが追加でグラフに表示されます。1 つは州名と共に平均値を表示し、もう 1 つは州内のロケーションの総数と平均値を表示します。たとえば、平均訪問時間のグラフなどです。

[Brand Benchmark]：ブランド名の平均値を表示します。ブランド名は、特定の州のロケーションのメタデータとしてのみ使用できます。ブランドを選択すると、平均訪問時間などの一部のグラフでは、ブランドがタグ付けされている州の平均値も表示されます。

[Filtered Location Benchmark]：フィルタリングされたロケーションの平均値を表示します。特定のロケーションをフィルタリングした場合にのみ表示されます。たとえば、ロケーション階

層で「Cisco San Fransisco」がフィルタリングされている場合、Cisco San Fransisco の「平均訪問時間」が組織の平均とともに表示されます。フィルタリングされたロケーションの下にあるロケーションの総数も表示されます。

[Top and Bottom 3 locations]： ツリーの上位および下位 3 つのロケーションを表示します。

[Important Locations]：インテント率、獲得率、訪問分布、訪問頻度など、さまざまなパラメータの総合ランキングで上位にある子ロケーションを表示します。上位5つの重要なロケーションがグラフに表示されます。

（注）

- 国、州、ブランドのベンチマークは、特定の顧客のデータに基づいて表示されます。
- ブランドのレポートをフィルタリングする場合、そのブランドに関連付けられていない州名をフィルタリングしないでください。
- 2 つのブランドのレポートを同時にフィルタリングしないでください。
- デフォルトでは、上位 3 つと下位 3 つのロケーションのレポートが表示されます。ページの右上にあるトグルスイッチをクリックすると、重要なロケーションのレポートを表示できます。
- ロケーションのメタデータを定義することにより、国、州、およびブランドのベンチマークの下のロケーションにタグ付けできます。

.

[Report] タブ

行動メトリクスレポートには次のタブがあります。

[Groups] タブ

デフォルトでは、レポートは[Group] ビューで表示され、組織全体のレポートが表示されます。

[Historical] タブ

過去 12 か月の平均値を示すレポートが表示されます。ほとんどのレポートでは、過去 12 か月の平均が各月の平均とともに表示されます。レポートに基づいた業界と組織の平均も表示されます。[Behavior Metrics] ウィンドウの右端にある [Toggle Historical View] ボタンをクリックすると、[Historical] ビューにアクセスできます。

[Comparative] タブ

ロケーションをフィルタ処理すると、[Comparative] タブが表示され、その特定のロケーションに関するレポートが組織のベンチマークとともに表示されます。

.

行動メトリクス（ビジネスメトリクス）

パフォーマンスベンチマーク：ピアに関連するコアメトリクスのパフォーマンス

（注） [Workspaces] 分野の行動メトリクスレポートは、以下のものとは異なります。[Workspaces] 分野の行動メトリクスレポートについては、[Workspaces] 分野（行動メトリクス） （68 ページ）を参照してください。

Visit Duration

[Visit Duration: Across Locations]

すべてのビジネス拠点の平均滞在時間を折れ線グラフで表示します。このレポートにより、訪問者がさまざまなロケーションで過ごした時間を特定できます。業界や組織の平均滞在時間もグラフに表示されます。

[Visit Duration: Key Locations]

主要なロケーションでの平均滞在時間を表す棒グラフが表示されます。このレポートには、業界および組織のベンチマークとともに、上位および下位 3 つのロケーションまたは重要なロケーションが示されます。ロケーションをフィルタリングしている場合、フィルタリングされたロケーションの平均値もレポートに表示されます。

[Visit Duration: By Sub-brand]

ビジネスのさまざまなブランドの平均滞在時間を示す棒グラフが表示されます。業界と組織のベンチマークもグラフに表示されます。

Visit Duration: Distribution

さまざまな滞在期間の範囲の訪問の合計数を示す棒グラフが表示されます。組織と業界の平均がレポートに表示されます。

Visit Frequency

[Visit Frequency] は、「訪問者による訪問回数」を「訪問者数」で割った訪問頻度を表します。

Visit Frequency: Across Locations

すべてのビジネス拠点の平均訪問頻度を折れ線グラフで表示します。このレポートにより、訪問者があなたのロケーションを訪れる頻度を特定できます。業界や団体の平均訪問頻度もグラフに表示されます。

Visit Frequency: Key Locations

主要なロケーションでの平均訪問頻度を表す棒グラフが表示されます。このレポートには、訪問頻度の上位および下位3つのロケーション、または訪問頻度が最も高い重要なロケーションが、業界および組織のベンチマークとともに表示されます。ロケーションをフィルタリングしている場合、フィルタリングされたロケーションの平均値もレポートに表示されます。

Visit Frequency: By Sub-brand

ビジネスにおけるさまざまなブランドの平均訪問頻度を示す棒グラフが表示されます。このレポートにより、より頻繁にアクセスされるブランドを特定できます。業界と組織のベンチマークもグラフに表示されます。

Visit Frequency: Distribution

さまざまな訪問頻度の範囲の訪問の合計数を示す棒グラフが表示されます。組織と業界の平均がレポートに表示されます。

診断：コアメトリクスに影響を与える要因、またはコアメトリクスの影響を受ける要因

Visit Duration by Visit Number

さまざまな訪問回数について、訪問者がそのロケーションで過ごした時間を示す棒グラフが表示されます。このレポートは、訪問回数に基づいて、滞在期間に生じた変化を特定するのに役立ちます。

各棒は、さまざまな訪問回数に対する訪問者の平均滞在時間を表します。たとえば、7の棒は、指定された月にそのロケーションを 7 回訪問した訪問者の平均滞在時間を表します。

Repeat Visitors: Across Locations

すべてのロケーションのリピート訪問者の割合を示す折れ線グラフが表示されます。リピート訪問者の組織と業界のベンチマークもレポートに表示されます。

Repeat Visitors :Key Locations

主要なロケーションのリピート訪問者の割合を示す棒グラフが表示されます。このレポートには、リピート訪問者の上位および下位3つのロケーション、またはリピート訪問者が最も多い重要なロケーションが、リピート訪問者の業界および組織のベンチマークとともに表示されます。ロケーションをフィルタリングしている場合、フィルタリングされたロケーションの平均値もレポートに表示されます。

Visit Recency : Across Locations

このレポートには、さまざまなロケーションのリピート訪問者の訪問間隔を示す折れ線グラフが表示されます。訪問の新しさは日数で表示されます。訪問の新しさに関する業界および組織のベンチマークもレポートに表示されます。

Visit Recency : Key Locations

このレポートには、主要なロケーションへのリピート訪問者の訪問間隔を日数で示す棒グラフが表示されます。このレポートには、訪問の新しさの上位 3 か所と下位 3 か所、または重要なロケーションが、業界および組織のベンチマークとともに表示されます。

Repeat Visitors: By Sub-brand

ビジネスにおけるさまざまなブランドのリピート訪問者の割合を示す棒グラフが表示されます。このレポートを使用すると、ブランドのリピート訪問が最も多いロケーションを特定できます。リピート訪問者の業界や組織のベンチマークもグラフに表示されます。

Visit Recency- By Sub-Brand

ビジネスのさまざまなブランドについて、訪問の新しさ（リピート訪問者による2回の訪問の間の日数）を示す棒グラフが表示されます。訪問の新しさに関する業界および組織のベンチマークもグラフに表示されます。

Visit Distribution: Hour of the Day

1日のさまざまな時間帯における、組織内の日次訪問数（組織のすべてのロケーションの平均）を表す棒グラフが表示されます。このレポートを使用すると、そのロケーションでより多く訪問される時間帯を特定できます。

グラフの各棒は、「1日の合計訪問数」のうち、「その日の特定の時間に発生した訪問の割合」を表します。たとえば、午後 2 時の棒は、1 日の平均合計訪問数のうち、午後 2 時に発生した訪問の割合を表します。

Visit Distribution: Day of the Week

週のさまざまな曜日における、組織内の平均日次訪問数を表す棒グラフが表示されます。このレポートにより、訪問者が多い曜日を特定できます。

グラフの各棒は、「1 週間の平均合計訪問数」のうち、「その特定の曜日に発生した訪問の割合」を表します。たとえば、「THU」の棒は、「1 週間の合計訪問数」に対する「木曜日に発生した訪問の割合」を表します。

Size of the Store and Visit Duration

ロケーションの面積（平方フィート）に基づいた滞在時間を示すグラフが表示されます。このレポートを使用すると、ロケーションの規模がそのロケーションで訪問者が過ごす時間に与える影響を特定できます。

青いドットは、滞在時間が最も長い3つの子ロケーションと、滞在時間が最も短い3つの子ロケーションを示しています。グラフの灰色のドットは、他の子ロケーションを表します。各ドットは、その特定の子ロケーションの合計面積（平方フィート）とその平均滞在時間を表します。

Size of the Store and No. of Visits

ロケーションの面積（平方フィート）に基づいた訪問回数を示すグラフが表示されます。このレポートを使用すると、ロケーションの規模がそのロケーションのリピート訪問数に与える影響を特定できます。

青いドットは、訪問回数が最も多い3つの子ロケーションと、訪問回数が最も少ない3つの子ロケーションを示しています。グラフの灰色のドットは、他の子ロケーションを表します。各ドットは、その特定の子ロケーションの合計面積（平方フィート）とその平均訪問回数を表します。

Retail Experience Grid

すべてのロケーションからの月全体の滞在時間と訪問頻度を統合したレポートを示すグラフが表示されます。グラフは、ルートロケーションとグループロケーションについてのみ表示されます。滞在時間は X 軸に表示され、訪問頻度は Y 軸に表示されます。[Retail Experience Grid] は、[Retail] 分野でのみ使用できます。

[Workspaces] 分野（行動メトリクス）

[Workspaces] 分野ではキャンパスレベルの計算が実装されています。以前は、ロケーション階層のネットワークノードを使用してメトリクスを取得していました。[Workspaces] 分野について報告されるデータの品質を向上させるために、キャンパスノードを使用して訪問を追跡し、知見を得ることができます。企業や大学のほとんどのリアルタイム環境では、人々はキャンパス内にある近接する建物間を往来します。ネットワーク間を移動する人々のこのような行動から、訪問を追跡して知見を得るための単一の連続したスペースであるキャンパスノードに移行する必要性が高まっています。

（注）

- [Location] オプションからキャンパスノードを選択すると、キャンパスの平均が、[Workday Duration]、[Employee Frequency]、[Density Index]、[Entry Time]、[Exit Time] チャートに表示されます。
- デフォルトでは、キャンパスとグループのロケーションデータはルートレベルのビューに表示されます。ロケーション階層でキャンパスロケーションが定義されていない場合は、ネットワークのロケーションデータが表示されます。

[Workspaces] 分野の [Behavior Metrics] ウィンドウには、次の情報が表示されます。

コアメトリクス：個々のワークスペースのロケーションが主要なメトリクスに従ってどの程度機能しているか

Workday Duration

- [Workday Duration]：このレポートには、従業員が職場で過ごした平均時間数が表示されます。
- [Workday Duration: Distribution]：このレポートには、従業員が職場で過ごした時間が滞在時間の割合として表示されます。この情報はグループビューとロケーションビューの両方で表示されます。

Employee Frequency

- [Employee Frequency]：このレポートには、従業員が職場に滞在した平均頻度が表示されます。
- [Employee Frequency: Distribution]：このレポートには、従業員ごとの職場での滞在回数が示されています。この情報はグループビューとロケーションビューの両方で表示されます。

Employees

- [Employees: %Share By floor]：このレポートには、特定のフロアでの従業員の滞在回数がパーセンテージで表示されます。この情報はグループビューとロケーションビューの両方で表示されます。
- [Employees: %Share By zone]：このレポートには、さまざまなゾーンでの従業員の滞在回数がパーセンテージで表示されます。この情報はグループビューとロケーションビューの両方で表示されます。

Presence

- [Presence: By floor]：このレポートには、フロア別の従業員のプレゼンス（在席情報）が工数で表示されます。この情報はグループビューとロケーションビューの両方で表示されます。
- [Presence: By zone]：このレポートには、ゾーン別の従業員のプレゼンス（在席情報）が工数で表示されます。この情報はグループビューとロケーションビューの両方で表示されます。

Visit Duration

- [Visit Duration: By floor]：このレポートには、従業員が就業日に各フロアで過ごした時間が表示されます。この情報はグループビューとロケーションビューの両方で表示されます。
- [Visit Duration: By zone]：このレポートには、従業員が就業日に各ゾーンで過ごした時間が表示されます。この情報はグループビューとロケーションビューの両方で表示されます。

密度

- [Density: By floor]：このレポートには、職場の各フロアの 1000 平方フィートあたりの従業員のプレゼンスが示されます。この情報はグループビューとロケーションビューの両方で表示されます。
- [Density: By zone]：このレポートには、職場の各ゾーンの 1000 平方フィートあたりの従業員のプレゼンスが示されます。この情報はグループビューとロケーションビューの両方で表示されます。
- [Density Index]：このレポートには、職場での 1000 平方フィートあたりの毎月の従業員のプレゼンス（工数）が示されます。この情報はグループビューとロケーションビューの両方で表示されます。

診断：コアメトリクスに影響を与える要因、またはコアメトリクスの影響を受ける要因の分析

Entry Time

- [Entry Time]：このレポートには、従業員の職場への平均入室時間が表示されます。
- [Entry Time: Distribution]：このレポートには、1 日のさまざまな時間帯にそのロケーションに入室した従業員の割合と、1 日の各時間の業界および組織の平均割合が表示されます。

Exit Time

- [Exit Time]：このレポートには、従業員の職場からの平均退出時間が表示されます。
- [Exit Time: Distribution]：このレポートには、1 日のさまざまな時間帯にそのロケーションから退出した従業員の割合と、1 日の各時間の業界および組織の平均割合が表示されます。

Employee Presence

- [Employees Presence: Hour of Day]：このレポートには、1 日のさまざまな時間帯に職場にいる従業員の割合が、1 日の各時間の業界および組織の平均割合とともに表示されます。
- [Employees Presence: Day of the Week]：このレポートには、各曜日に職場にいた従業員の割合が、各曜日の業界および組織の平均割合とともに表示されます。

Guest Presence

- [Guest Presence: Hour of Day]：このレポートには、1 日のさまざまな時間帯に職場にいるゲストの割合が、1 日の各時間の業界および組織の平均割合とともに表示されます。
- [Guest Presence: Day of the Week]：このレポートには、各曜日に職場にいたゲストの割合が、各曜日の業界および組織の平均割合とともに表示されます。

[Education]分野（行動メトリクス）

Cisco DNA Spaces では、**行動メトリクス**アプリの [Education] という新しい分野をサポートします。すべての主要なチャートは、学生のメトリクスに基づいた情報を反映しています。[Education] 分野のチャートで使用されるすべてのメトリクスは、[Workspaces] 分野のチャートと同様です。

[Education] 分野の [Behavior Metrics] ウィンドウには、次の情報が表示されます。

コアメトリクス：個々のロケーションが主要なメトリクスに従ってどの程度機能しているか

Visit Duration

- [Visit Duration: Across Locations]：このレポートには、1 か月の間に学生が大学に登校した際に過ごした平均時間が表示されます。
- [Visit Duration: Distribution]：このレポートには、学生が大学で過ごした時間が滞在時間の割合として表示されます。

Student Frequency: Across Locations

- [Student Frequency: Across Locations]：このレポートには、1 か月の間に学生が大学に登校した平均回数が表示されます。
- [Student Frequency: Distribution]：このレポートには、学生が大学に登校した回数が登校回数の割合として表示されます。

Density Index

- [Density Index: Across Locations]：このレポートには、大学の敷地 1000 平方フィートあたりの大学での月間工数が示されています。

診断：コアメトリクスに影響を与える要因、またはコアメトリクスの影響を受ける要因の分析

Entry Time

- [Entry Time: Across Locations]：このレポートには、ロケーション全体の学生の平均登校時間が表示されます。
- [Entry Time : Distribution]：このレポートには、特定の登校時間（時間帯）における大学の学生数が割合で表示されます。

Exit Time

- [Exit Time: Across Locations]：このレポートには、ロケーション全体の学生の平均下校時間が表示されます。
- [Exit Time : Distribution]：このレポートには、特定の下校時間（時間帯）における大学の学生数が割合で表示されます。

Student Presence

- [Student Presence: Hour of Day]：このレポートには、1 日の時間帯ごとに出席している学生の数が割合で表示されます。
- [Student Presence: Day of the Week]：このレポートには、曜日ごとに出席している学生の数が割合で表示されます。

Guest Presence

- [Guest Presence: Hour of Day]：このレポートには、1 日の時間帯ごとに存在しているゲストの数が割合で表示されます。
- [Guest Presence: Day of the Week]：このレポートには、曜日ごとに存在しているゲストの数が割合で表示されます。

ロケーションのピン留め

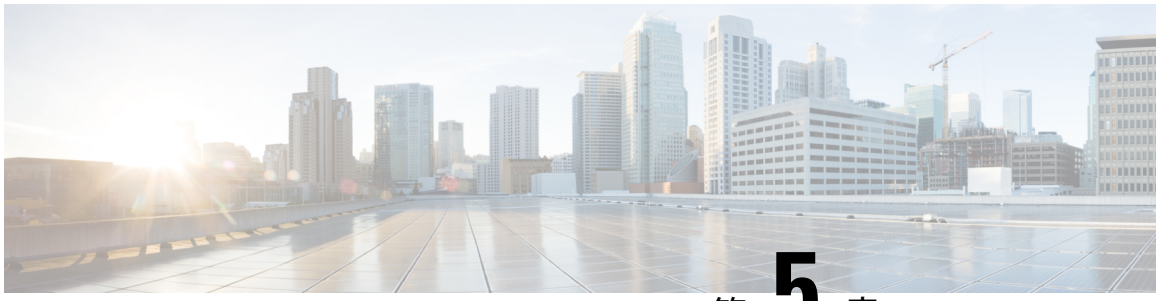
特定のロケーションをお気に入りとして追加する場合、それらのロケーションをピン留めできます。一度に3つまでのロケーションをピン留めできます。ピン留めされたロケーションを追加すると、ピン留めされたロケーションの値がすべてのグラフにデフォルトで表示されます。棒グラフには、ピン留めされたロケーションごとに 1 本の棒が表示されます。

ロケーションをピン留めするには、次の手順を実行します。

ステップ 1 [Behavior Metrics] ウィンドウで、ウィンドウの右端にある [Pin Locations] ボタンをクリックします。

ステップ 2 [Pin Locations] ウィンドウで、ピン留めするロケーションを選択できます。

ステップ 3 [Apply] をクリックします。



第 5 章

ロケーション分析レポート

この章では、ロケーション分析レポートについて説明します。

概要

ロケーション解析アプリを使用すると、ロケーション訪問者のレポートを表示できます。このレポートでは、従業員の訪問もカウントされます。

ロケーション分析レポートの表示

ロケーション分析レポートを表示するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Home] を選択します。

ステップ 2 表示されるウィンドウで、[Location Analytics] をクリックします。

[Location Analytics] レポートが表示されます。

デフォルトでは、2019 年 1 月 1 日から現在までのルートロケーションのレポートが表示されます。ロケーション、日付、SSID でレポートをフィルタリングできます。データが存在しない場合、レポートは表示されません。

ステップ 3 [Filter by Location] ドロップダウンリストから、レポートを表示する親ロケーションを選択します。

（注） ACT および EXTEND ライセンスの場合、フロアとゾーンのレポートを表示できます。ただし、SEE ライセンスの場合、フィルタリングできるのはネットワーク ロケーションのみです。

ステップ 4 [Filter by date] ドロップダウンリストから、レポートを表示する日付の範囲を選択します。

[Choose date range] ウィンドウで、用意されている期間を指定するか、開始日と終了日を指定してカスタムの日付範囲を指定できます。[Apply] をクリックします。

デフォルトでは、次の期間を選択できます。

- [Today]：レポートには、特定の日の各時間の合計訪問数が表示されます。
- [Yesterday]：レポートには、前日の各時間の合計訪問数が表示されます。
- [Current Week]：レポートには、現在の週の各曜日の合計訪問数が表示されます。
- [Previous Week]：レポートには、前の週の各曜日の合計訪問数が表示されます。
- [Current Month]：レポートには当月の各日の合計訪問数が表示されます。
- [Previous Month]：レポートには、前月の各日の合計訪問数が表示されます。
- [Last 15 days]：レポートには、過去 15 日間の各日の合計訪問数が表示されます。
- [Last 30 days]：レポートには、過去 30 日間の各日の合計訪問数が表示されます。
- [Last 3 Months]：レポートには、過去 3 ヵ月の各日の合計訪問数が表示されます。
- [Last 6 Months]：レポートには、過去 6 ヵ月の各日の合計訪問数が表示されます。
- [Custom]：レポートには指定した期間の各日の合計訪問数が表示されます。

特定の日の訪問の詳細を表示するには、グラフの該当する日にカーソルを合わせます。

ステップ 5 [Filter by SSID] ドロップダウンリストから、レポートを表示する SSID を選択します。

次の SSID オプションを選択できます。

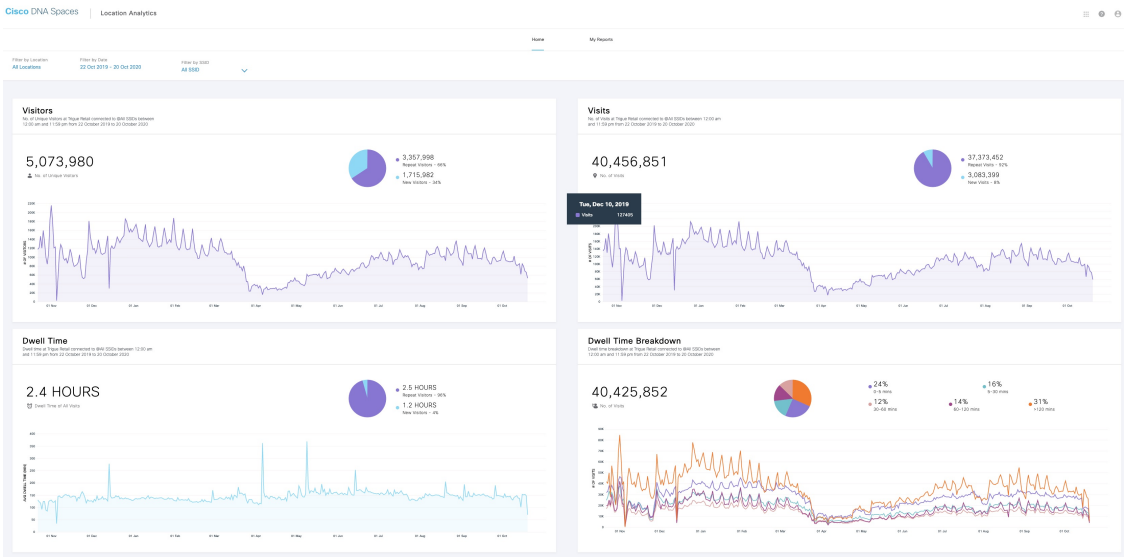
- [All SSIDs]：フィルタリングされたロケーションで SSID を使用してキャプチャされた、指定された期間の訪問データを表示します。
- [Custom SSID configured in Cisco DNA Spaces]：特定の SSID を使用してキャプチャされた、フィルタリングされたロケーションの指定された期間の訪問データを表示します。

（注） 適用されたフィルタに応じてレポートが表示されます。フィルタを適用できるのは、ACT ライセンスユーザーのみです。SEE ライセンスのユーザーは、SSID フィルタを使用できません。ただし SEE ライセンスのユーザーは、日付範囲フィルタを使用できます。また、ネットワーク、フロア、ゾーン以外のロケーションをフィルタリングできます。

ロケーション分析レポート

ロケーション分析レポート

図 7: ロケーション分析レポート



ロケーション分析レポートでは、次の情報を表示できます。

- [Visitors]：指定の期間におけるフィルタ処理されたロケーションへのユニークビジターの総数を表示します。[New Unique Visitors] と [Repeat Unique Visitors] の数とパーセンテージが別個に表示されます。また、指定の期間における各日のユニークビジター数を示すグラフも表示されます。
  - [New Visitors]：フィルタ処理されたロケーションを初めて訪問したユニークビジターの総数。
  - [Repeat Visitors]：フィルタ処理されたロケーションを 2 回以上訪問したユニークビジターの総数。
- [Visits]：指定の期間におけるフィルタ処理されたロケーションへの訪問の総数を表示します。[New Visits] と [Repeat Visits] の数とパーセンテージが別個に表示されます。また、指定の期間における各日の訪問数を示すグラフも表示されます。
  - [New Visits]：フィルタ処理されたロケーションへの初回訪問の総数。
  - [Repeat Visits]：フィルタ処理されたロケーションで複数回発生した個別の訪問の総数。

注
- 滞在時間が 5 分未満の訪問は除外されます。この設定は、訪問者数と訪問数の水増しにつながる短時間の一時的な訪問者を除外するのに役立ちます。
- 滞在時間が 1440 分を超える訪問は除外されます。この設定は、常にオンになっているデバイスを除外して、平均滞在時間の水増しを防ぐのに役立ちます。

- [Dwell Time Distribution]：指定された期間中にフィルタ処理されたロケーションで発生した全 SSID への訪問の滞在時間内訳を表示します。すべての訪問の滞在時間と訪問の総数も表示されます。0 ～ 5 分のカウントは、フィルタ処理された場所で 0 ～ 5 分間継続した訪問の合計数を表します。

- [Path widget]：訪問者のロケーション間での移動パターンと、同じ [Network] 内のさまざまなフロアまたはゾーンへの訪問の割合を表示します。カスタムレポートで、[Path widget] の任意のフロアまたはゾーンにカーソルを合わせると、正確な訪問数が表示されます。[Network] の下の利用可能なロケーションのみを使用してフィルタ処理することで、パス分析を表示できます。[Path widget] は、Cisco DNA Spaces ACT ライセンスアカウントのみで使用できます。

さまざまなフィルタを備えたウィジェットを使用して、カスタムレポートを作成できます。

カスタム レポートの作成

ロケーション分析用に表示されるデフォルトのレポートに加えて、ウィジェットフィルタを適用してカスタムレポートを作成することができます。各カスタムレポートには、複数のウィジェットを含めることができます。レポートタイプ、ロケーション、期間、SSID、訪問範囲、および表示オプションをさまざまに組み合わせたウィジェットを作成できます。カスタムレポートには同じレポートタイプのウィジェットを複数追加できます。

カスタムレポートを作成するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Home] を選択します。
ステップ 2 表示されるウィンドウで、[Location Analytics] をクリックします。
ステップ 3 ウィンドウの左上に表示されている 3 本の平行線のアイコンをクリックします。
ステップ 4 表示されるウィンドウで、[My Reports] をクリックします。
ステップ 5 [Create New Report] をクリックします。
ステップ 6 [Create New Report）] ウィンドウが表示されたら、レポートの名前と説明を入力します。
ステップ 7 [作成（Create）] をクリックします。

ステップ 8 [Add New Widgets] をクリックします。

ステップ 9 [Add a Widget] ウィザードで、次の手順を実行します。

a) [Name of the widget] フィールドに、ウィジェットの名前を入力します。

b) カスタムレポートに追加する必要があるレポートのタイプをクリックします。

選択できるレポートタイプは、デフォルトレポートで使用できるものとなります。

ウィジェットに対して選択できるレポートタイプは 1 つだけです。

c) [Next] をクリックします。

d) [Choose Locations] ウィンドウで、レポートを表示するロケーションにチェックを入れます。

（注）
- 「Visitors」のレポートタイプを選択している場合、選択できるロケーションは 1 つだけです。他のレポートタイプでは、複数のロケーションをフィルタ処理できます。
- フィルタ処理にはネットワークのロケーションのみを選択できます。フィルタ処理用にフロアとゾーンを選択することはできません。

e) [Next] をクリックします。

f) [Filter by] ウィンドウで、[From] および [To] フィールドの値を指定して、レポートを表示する期間を指定します。

g) [SSID] ドロップダウンリストから、レポートを表示する SSID を選択します。

次の SSID オプションを選択できます。

- [All SSIDs]：フィルタリングされたロケーションで SSID を使用してキャプチャされた、指定された期間の訪問データを表示します。
- [Without SSIDs]：SSID を介してキャプチャされていない、フィルタリングされたロケーションでの指定された期間の訪問データを表示します。たとえば、フィルタリングされたロケーションを訪問したが、指定された期間中にフィルタリングされたロケーションのいずれの SSID にも接続しなかった訪問者などです。ただし、以前にいずれかの SSID に少なくとも 1 回接続したことがある訪問者の訪問はカウントされます。
- [Custom SSID configured in Cisco DNA Spaces]：特定の SSID を使用してキャプチャされた、フィルタリングされたロケーションの指定された期間の訪問データを表示します。

（注） フィルタを適用できるのは、ACT ライセンスユーザーのみです。SEE ライセンスのユーザーは、SSID フィルタを使用できません。ただし SEE ライセンスのユーザーは、日付範囲フィルタを使用できます。また、ネットワーク、フロア、ゾーン以外のロケーションをフィルタリングできます。

h) [Visit Range] ドロップダウンリストから、レポートを表示する時間を選択します。たとえば、[Mid Night] を選択した場合、レポートには、指定された期間中に選択したロケーションで深夜に発生した訪問の詳細が表示されます。

次のオプションを選択できます。

- [All Day]：終日（午前 0 時から午後 11 時 59 分）に発生した訪問がレポートに含まれます。

- [Mid Night]：深夜（午前 0 時から午前 2 時 59 分）の訪問のみがレポートに含まれます。
- [Early Morning]：早朝（午前 3 時から午前 4 時 59 分）の訪問のみがレポートに含まれます。
- [Morning]：朝（午前 5 時から午前 8 時 59 分）の訪問のみがレポートに含まれます。
- [Business Hours]：営業時間内（午前 9 時から午後 4 時 59 分まで）の訪問のみがレポートに含まれます。
- [Evening]：夕方から夜（午後 5 時から午後 8 時 59 分）の訪問のみがレポートに含まれます。
- [Late Evening]：夜遅く（午後 9 時から午後 11 時 59 分）の訪問のみがレポートに含まれます。
- [AM]：午前（午前 0 時から午前 11 時 59 分）の訪問のみがレポートに含まれます。
- [PM]：午後（午後 0 時から午後 11 時 59 分）の訪問のみがレポートに含まれます。

i) [View By] ドロップダウンリストから、レポートにデータを表示する順序を選択します。

- [by day]：指定された期間の各日の訪問データが表示されます。
- [by Hour of Day]：時間ごとの訪問データが表示されます。特定の時間の訪問数は、指定された期間中にその特定の時間で発生した訪問の合計になります。たとえば、2019 年 11 月の「by Hour of Day」レポートで、午後 2 時に表示される訪問数は、2019 年 11 月全体の午後 2 時から午後 2 時 59 分までに発生した訪問数の合計になります。
- [by Week]：指定された期間の各週の訪問データが表示されます。
- [by Day of Week]：指定された期間の各週の訪問データと、その特定の週の各日の訪問数が表示されます。
- [by Month]：指定された期間の各月の訪問データが表示されます。

j) [Add] をクリックします。

新しいウィジェットがカスタムレポートに追加されます。

ステップ 10 同様に、[Add New Widget] アイコンを使用して、複数のウィジェットをカスタムレポートに追加できます。

作成されたカスタムレポートは、[My Reports] ウィンドウにリストされます。

（注） ACT（高度）サブスクリプションのお客様は、ウィジェットですべてのフィルタ（ロケーション、SSID、時間範囲、および訪問範囲）を適用できます。SEE（基本）サブスクリプションのお客様が適用できるのは SSID および訪問範囲フィルタに制限されており、ネットワークロケーションをフィルタ処理することはできません。

カスタムレポートの共有

Location Analytics アプリのカスタムレポートの共有機能を使用すると、Cisco DNA Spaces ユーザーと Cisco DNA Spaces 以外のユーザーのどちらともレポートを共有できます。Cisco DNA Spaces 以外のユーザーは、レポートにアクセスするために 1 回限りの登録を実行する必要があります。レポートにアクセスするために必要な権限がない場合は、管理者またはレポートを開始したユーザーにアクセス権をリクエストしてください。

削除または取り消されたレポートにはアクセスできません。レポートを取り消すことができるのは、管理者または送信者のみです。

カスタムレポートを共有するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Home] を選択します。

ステップ 2 表示されるウィンドウで、[Location Analytics] をクリックします。

ステップ 3 表示されるウィンドウで、[My Reports] をクリックします。

ステップ 4 使用可能なカスタムレポートリストからレポートをクリックします。

ステップ 5 ウィンドウの右上に表示される共有アイコンをクリックします。

[Share Report] ウィンドウが表示されます。

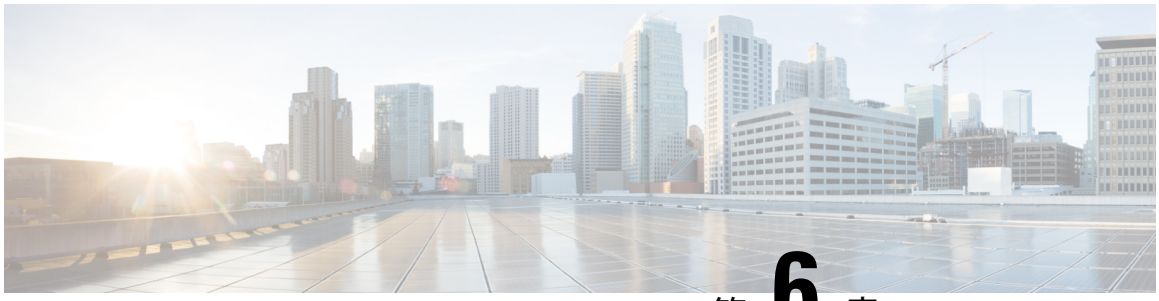
ステップ 6 次の情報を入力します。

- [Add Email]：レポートの受信者の電子メールアドレスを入力します。これは必須フィールドです。
- [Add Message]：電子メールのメッセージを入力します。

（注）
- [Preview] オプションを使用して、レポートが受信者とどのように共有されるかを表示します。
- レポート名の横にある編集アイコンをクリックして、カスタムレポートの名前を編集します。

ステップ 7 [共有（Share）] をクリックします。

ウィンドウに成功通知メッセージが表示されます。



第 6 章

影響分析

この章では、影響分析アプリの使用方法について説明します。

影響分析の概要

影響分析は、ビフォー/アフター分析に基づいて、行ったアクションの効果を測定する方法です。Impact Analysis アプリを使用して、影響分析を行うことができます。たとえば、2019 年 11 月にあなたのロケーション A を訪れたすべての訪問者に割引オファーを提供したとします。オファー期間中の指標を過去 365 日間の指標と比較することで、この割引オファーの影響を測定できるようになりました。

このアプリは、SEE、ACT、および Extend ライセンスタイプで利用できます。

特定の期間のイベントを作成して、次のいずれかを実行できます。

- イベント期間の指標を、過去 365 日間の日次平均の指標と比較します（イベント中の期間）。
- 指定されたイベント期間の前後の同じ期間のメトリックを比較します。（イベント後の期間）

次の指標を比較できます。

- 滞在時間
- 訪問回数

インパクトキャンペーン（イベント）の追加

（注）
- Cisco DNA Spaces の新規顧客であり、Cisco DNA Spaces アカウントのデータがない場合、キャンペーンを追加、編集、または変更することはできません。
- 訪問データが 30 日未満の場合、新しいキャンペーンを作成することはできません。
- Cisco DNA Spaces アカウントへの読み取り専用アクセス権のみがあるユーザーは、そのアカウントの既存のキャンペーンの影響分析レポートを表示できますが、キャンペーンを追加、変更、または削除することはできません。

インパクトキャンペーン（イベント）を追加するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Impact Analysis] を選択します。

ステップ 2 表示される [Impact Analysis] ウィンドウで、[Add Impact Campaign] をクリックします。

[Add Impact Campaign] ウィンドウが表示されます。

ステップ 3 [Event Name] フィールドに、イベントの名前を入力します。

ステップ 4 [Business Location] ドロップダウンリストから、イベントを作成するロケーションを選択します。

ネットワークのロケーションのみを選択できます。

ステップ 5 [Choose the event period that you like to measure] 領域（[Edit] ウィンドウの [Compared To] ドロップダウンリスト）で、イベント期間を選択します。

次のオプションを選択できます。

- [Period DURING Event]：このオプションを使用すると、「指定されたイベント期間のデータ」と「過去 365 日間の日次平均データ」を比較できます。たとえば、イベント期間を 2019 年 12 月 10 日から 2019 年 12 月 20 日として選択している場合、影響分析レポートのグラフには 2 つの棒グラフが表示され、1 つは「2019 年 12 月 10 日から 2019 年 12 月 20 日までのデータ」を含み、もう 1 つは「2018 年 12 月 21 日から 2019 年 12 月 20 日までの日次平均データ」を含みます。
- [Period AFTER Event]：このオプションを使用すると、「指定した日付範囲の前の同じ期間のデータ」と「指定した日付範囲の後の同じ期間のデータ」を比較できます。たとえば、イベント期間を「2020 年 1 月 1 日から 2020 年 1 月 10 日」（10 日間）として指定している場合、影響分析レポートのグラフには 2 つの棒グラフが表示され、1 つは「2019 年 12 月 22 日から 2019 年 12 月 31 日までの期間（10 日間）のデータ」を含み、もう 1 つは「2020 年 1 月 10 日から 2020 年 1 月 19 日までの期間（10 日間）のデータ」を含みます。

（注） 訪問時間と訪問回数のグラフは別々に表示されます。[Visit Duration] グラフでは、2 つの棒グラフ間の訪問時間の差が分単位で表示されます。[Visit Count] グラフでは、2 つの棒グラフ間の訪問回数の差がパーセンテージで表示されます。

ステップ 6 [EVENT DURATION] 領域で、[From] フィールドと [To] フィールドにそれぞれイベントの開始日と終了日を指定します。

ステップ 7 [See Impact] をクリックします。

これでキャンペーンが追加されました。

- キャンペーンを編集するには、[Impact Analysis] ウィンドウにリストされているキャンペーンから、編集するキャンペーンをクリックします。ウィンドウの右上にある [Edit Campaign] をクリックし、必要な変更を加えます。[更新（Update）] をクリックして変更を保存します。
- キャンペーンを削除するには、[Impact Analysis] ウィンドウにリストされているキャンペーンから、削除するキャンペーンをクリックします。ウィンドウの右上に表示される [Delete] をクリックします。[Delete Impact Compaign] ウィンドウで、[Delete] をクリックして削除を確定します。一度に複数のキャンペーン（イベント）を削除するには、[Impact Analysis] ウィンドウで、削除するキャンペーンに対応するチェックボックスをオンにして、ウィンドウの下部に表示される [Delete] をクリックします。

影響分析レポートの表示

影響分析レポートを表示するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Impact Analysis] を選択します。

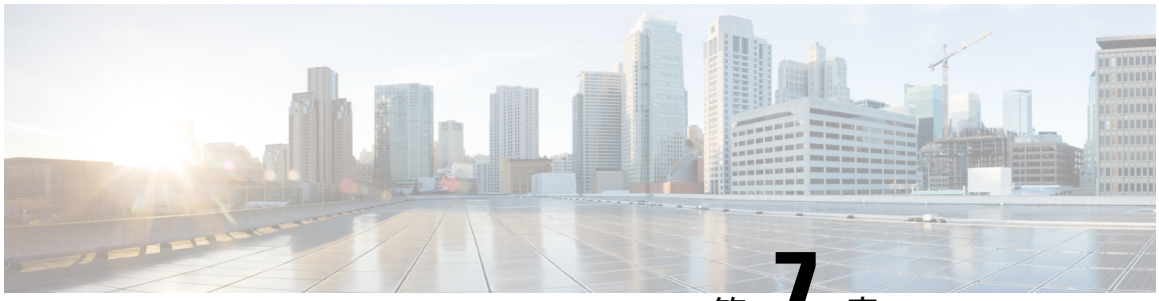
[Impact Analysis] ウィンドウが表示されます。作成されたすべてのキャンペーンがこのウィンドウにリストされます。

ステップ 2 レポートを表示するキャンペーン/イベントをクリックします。

選択したキャンペーンの影響分析レポートが表示されます。レポートには次のグラフが含まれます。

- **訪問時間への影響**：イベントの平均訪問時間と、選択した時間枠の平均訪問時間を分単位で示す棒グラフを表示します。
- **訪問回数への影響**：イベントの平均訪問回数と、選択した時間枠の平均訪問回数をパーセンテージで示す棒グラフを表示します。

（注） 当月または将来の期間でイベントを作成した場合、レポートは表示されません。



第 7 章

Right Now

この章では、**Right Now** アプリについて説明します。

Right Now の概要

Right Now アプリは、現在あなたのロケーションにいる訪問者の詳細を示す Right Now レポートを提供します。**Right Now** アプリを使用して、**密度ルール**を作成し、訪問者の密度やビジネスロケーションのデバイス数に基づいて、従業員などのビジネスユーザーに通知を送信できるすることもできます。

Right Now on WiFi

Right Now on WiFi レポートには、現在あなたのロケーションにいる訪問者の詳細が表示されます。

デフォルトでは、レポートには、現在すべてのロケーションにいる訪問者の詳細が表示されます。最大でフロアレベルまでフィルタリングできます。

Right Now アプリは、SEE、ACT、および EXTEND ライセンスタイプで使用できます。

（注）

- ロケーション階層からロケーションが削除または変更された場合、そのロケーションの名前と数は Right Now レポートでは更新されません。

Right Now レポートの表示

Right Now レポートを表示するには、次の手順を実行します。

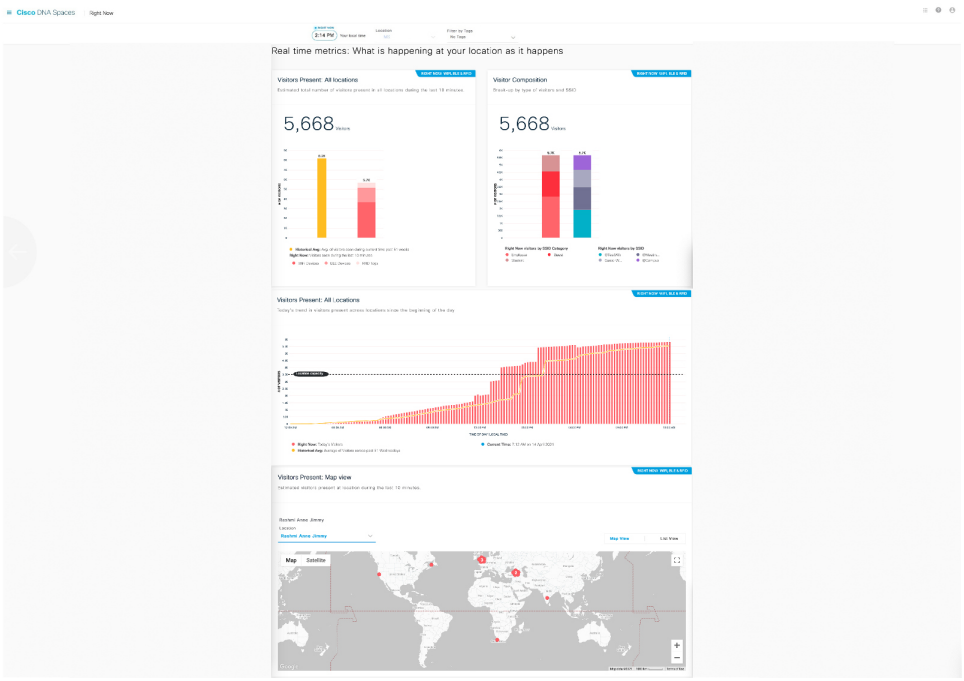
ステップ 1 Cisco DNA Spaces ダッシュボードで、[Right Now] を選択します。

[Right Now] ウィンドウが表示されます。

ステップ 2 [Location] ドロップダウンリストから、目的のネットワークロケーションを選択します。

選択したネットワークロケーションの Right Now レポートが表示されます。

図 8 : Right Now on Wi-Fi



レポート上部の [Right Now] セクションに、システムの現地時間が表示されます。

Right Now レポートには、次のチャートが表示されます。

- [Visitors Present: All locations]：子ロケーションを含むフィルタリングされたロケーションでの、過去 10 分間の推定合計訪問者数を表示します。
- [Visitor Composition]：アクティブな訪問者の構成を、SSID カテゴリ（従業員、ゲストなど）および SSID（上位 5 つの SSID） ごとにパーセンテージで表示します。
- [Visitors Present: All Locations]：フィルタリングされたロケーションでの、過去 10 分間の合計訪問者数の傾向を表示します。
- [Visitors Present: Map View]：フィルタリングされたロケーションの子ロケーションでの、アクティブな訪問者のロケーション別カウントを表示します。

- [Map View]：フィルタリングされたロケーションの子ロケーションが、それらの各子ロケーションの合計訪問者数とともに世界地図に表示されます。
  - [Floor map view]：特定のフロアを選択すると、選択したフロアマップビューも表示されます。

    選択したロケーションに、Cisco CMX からインポートされて Cisco DNA Spaces にアップロードされたマップがある場合、そのフロアと、表示されたフロアの合計訪問者数を表示できます。

- [List View]：フィルタリングされたロケーションの子ロケーションが一覧表示され、各子ロケーションの現在の訪問者数がそのロケーションに対して表示されます。

（注）
- 「アクティブな訪問者」とは、過去10分間にそのロケーションにいて、ネットワーク（WLANまたは SSID）に接続している訪問者です。
- 10 分間の中でデバイスの滞留時間が 1 分未満の場合、そのデバイスは Right Now レポートから除外されます。
- 過去 51 週間の平均値が、レポートの各チャートの履歴データとして表示されます。

Right Now on Camera

[Right Now on Camera] オプションでは、ロケーションに設置されている Meraki カメラでキャプチャされたデータに基づいて、ロケーションの Right Now レポートが表示されます。このレポートは、[Setup] の [Camera] オプションを使用して Cisco DNA Spaces 用に Meraki カメラを設定した場合にのみ利用できます。 Meraki カメラの設定の詳細については、#unique_148を参照してください。

Meraki カメラの Right Now レポートの表示

Meraki カメラのRight Now レポートを表示するには、次の手順を実行します。

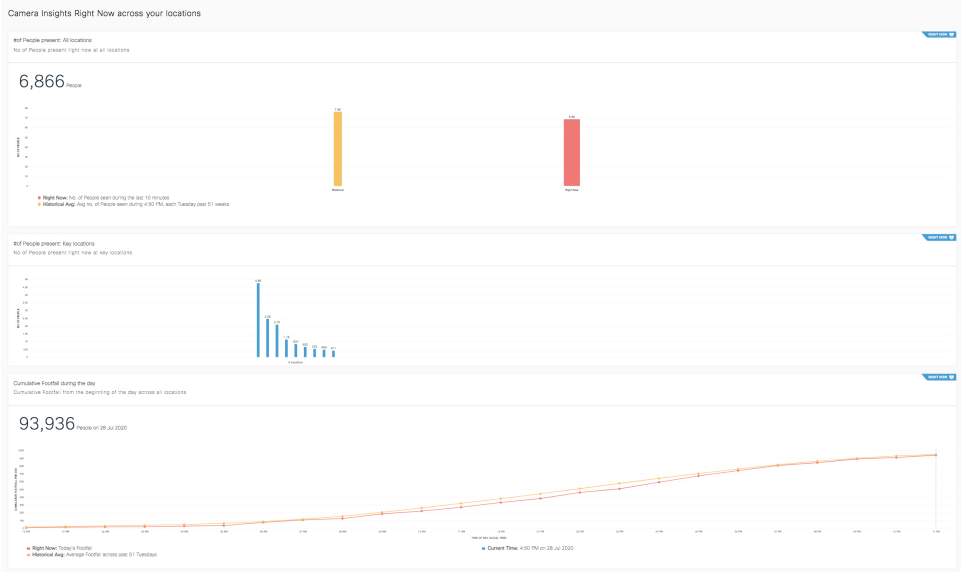
ステップ 1 Cisco DNA Spaces ダッシュボードで、[Right Now] を選択します。

[Right Now] ウィンドウが表示されます。

ステップ 2 ウィンドウの左上に表示される 3 本線のメニューアイコンをクリックし、[Right Now on Camera] を選択します。

[Right Now on Camera] ウィンドウに、Meraki カメラの Right Now レポートが表示されます。

図 *9 : Right Now on Camera* レポート



ステップ 3 必要に応じて、[Location] ドロップダウンリストから、レポート表示の対象となるロケーションを選択します。

（注） デフォルトでは、ルートロケーションのレポートが表示されます。

レポートには次の詳細が含まれます。

- ウィンドウの上部に現地時間が表示され、この時間のレポートのデータが表示されます。
- [# of people present]：選択したロケーションとその子ロケーションに現在滞在している人の合計数を示す棒グラフを表示します。過去 51 週間のこの時間に、選択したロケーションとその子ロケーションに滞在していた人の平均数を、[Historical Average] として表示します。現在滞在している人の合計数は、「過去 15 分間にそのロケーションのカメラのトリップワイヤ入り口から入場した人の合計数」 -「過去 15 分間にそのロケーションのカメラのトリップワイヤ出口から退出した人の合計数」になります。
- [#of people presents: Key Locations]：それぞれの子ロケーションに現在滞在している人の合計数を示す棒グラフを表示します。ロケーションの合計数が 15 以上の場合、上位および下位の 3 つのロケーションのカウントが表示されます。このような場合、最大 3 つの場所をピン留めして、選択した場所の現在の滞在人数を表示できます。このグラフは、ネットワーク、フロア、ゾーン以外の場所にのみ表示されます。現在滞在している人の合計数は、「過去 15 分間にその子ロケーションのカメラのトリップワイヤ入り口から入場した人の合計数」 -「過去 15 分間にその子ロケーションのカメラのトリップワイヤ出口から退出した人の合計数」になります。

  （注） ロケーションをピン留めするオプションは、ロケーションの数が 15 以上の場合にのみ使用できます。

- [# of the people present: Key Cameras]：フィルタリングされたロケーションの各カメラに対して滞在している人の合計数を示す棒グラフを表示します。カメラの総数が 6 台を超える場合は、上位および下位の 3 つのカメラのカウントが表示されます。このような場合、最大 3 台のカメラをピン留めして、

選択したカメラの現在の滞在人数を表示できます。このグラフは、ネットワーク、フロア、およびゾーンレベルのロケーションについてのみ表示されます。

（注） カメラをピン留めするオプションは、カメラの数が 7 台以上の場合にのみ使用できます。

- [# of the people present: Key Cameras Zones]：フィルタリングされたロケーション内のカメラに定義されている各カメラゾーンに滞在している人の合計数を示す棒グラフを表示します。カメラゾーンの総数が 6 を超える場合は、上位および下位の 3 つのカメラゾーンのカウントが表示されます。このような場合、最大 3 つのカメラゾーンをピン留めして、選択したカメラゾーンの現在の滞在人数を表示できます。このグラフは、ネットワーク、フロア、およびゾーンレベルのロケーションについてのみ表示されます。

  （注） カメラゾーンをピン留めするオプションは、カメラゾーンの数が 7 以上の場合にのみ使用できます。

- [Cumulative Footfall during the day]：Right Now レポートで表示されている 1 日の各時間における合計訪問者数を累積的に示す折れ線グラフを表示します。たとえば、午前 3 時の合計訪問者数は、午前 0 時から午前 3 時までの訪問者の合計になります。

  （注） グラフは、ネットワーク、フロア、およびゾーンレベルのロケーションのタイムゾーンに基づいて表示されます。たとえば、ルートロケーション XYZ にカリフォルニア、東京、バンガロールのネットワークロケーションがある場合、レポートには、現在の時間に基づいてこれらのネットワークのデータが表示されます。インドが午前 8 時である場合、日本は同じ日の午前 11 時 30 分で、カリフォルニアは前日の午後 7 時 30 分です。したがって、午前 8 時（IST）に Right Now on Camera レポートを表示している場合、[Cumulative Footfall during the day] セクションに 2 つのグラフが表示されます。1 つは午前 8 時のバンガロールと午前 11 時 30 分の東京（両方とも同じ日）の累積訪問者数、もう 1 つは 2020 年 7 月 19 日の午後 7 時 30 分のカリフォルニアの累積訪問者数です。

- [Presence: By Location]：レポート用に選択されたロケーションとその子ロケーションがグローバルマップに表示され、これらのロケーションに現在滞在している訪問者数が [Map View] に表示されます。[List View] を使用して、現在の訪問者数を階層として知ることもできます。

（注） [# of the people present: Key Cameras Zones] グラフは、カメラの近くにいる人々に基づいており、残りのすべてのグラフは、カメラに対して描かれたトリップワイヤラインを超える人々の出入りに基づいています。

ロケーション、カメラ、またはカメラゾーンのピン留めについては、ロケーション、カメラ、またはカメラゾーンのピン留め （90 ページ）を参照してください。

次のタスク

ウィンドウの左上に表示される 3 本線メニューの [Right Now on WiFi] オプションを使用して、Right Now レポートに戻ることができます。

ロケーション、カメラ、またはカメラゾーンのピン留め

ロケーション、カメラ、またはカメラ ゾーンをピン留めするには、次の手順を実行します。

ステップ 1 [Right Now on Camera] ウィンドウで、ウィンドウの右上にある [Pin] アイコンをクリックします。

[Pin] ウィンドウが表示されます。

ステップ 2 必要に応じて、次の操作を実行します。

- ロケーションをピン留めするには、[Pin Location] 領域でピン留めするロケーションのチェックボックスをオンにして、[Apply] をクリックします。選択した場所は、[Pinned Locations] 領域に表示されます。最大 3 つのロケーションをピン留めできます。
- カメラをピン留めするには、[Pin Cameras] 領域で [Cameras] タブをクリックし、ピン留めするカメラのチェックボックスをオンにして、[Apply] をクリックします。選択したカメラは、[Pinned Cameras] 領域に表示されます。最大 3 台のカメラをピン留めできます。
- カメラゾーンをピン留めするには、[Pin Cameras] 領域で [Camera Zones] タブをクリックし、ピン留めするカメラゾーンのチェックボックスをオンにして、[Apply] をクリックします。選択したカメラゾーンは、[Pinned Camera Zones] 領域に表示されます。最大 3 つのカメラゾーンをピン留めできます。

（注） それぞれの領域に表示される [Search] オプションを使用して、特定のロケーション、カメラ、またはカメラゾーンを検索できます。

密度ルール

密度ルールを使用すると、ビジネスロケーション内の一意のデバイスまたは訪問者の密度を追跡できます。このオプションは、ACT ライセンスでのみ使用できます。

[Density Rule]（密度ルール）オプションを使用すると、訪問者の密度、一意デバイスの数、またはビジネスロケーションの占有率に基づいて、ビルディング管理者などのビジネスユーザーへの通知をトリガーするルールを作成できます。SMS、電子メール、Cisco Webex Teams を介して、またはトリガー API を使用して通知を送信するように設定できます。

このルールを使用してロケーション内の訪問者を監視して、COVID 19 への対応状況を維持できます。また、ロケーションでの COVID 19 の影響を測定するためにも使用できます。

[Density Rule] オプションでは、ビジネスロケーションに設置された Meraki カメラでキャプチャされた人数に基づいて、ビジネスユーザーへの通知をトリガーするルールを作成することもできます。

密度ルールを作成するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Right Now] を選択します。

[Right Now] ウィンドウが表示されます。

ステップ 2 ウィンドウの左上に表示される 3 本線のメニューアイコンをクリックし、[Density Rules] を選択します。

ステップ 3 表示される [Density Rule] ウィンドウで、ウィンドウの右上に表示される [Create New Rule] をクリックします。

[Create Density Rule] ウィンドウが開きます。

ステップ 4 [Rule Name] フィールドに、密度ルールの名前を入力します。

ステップ 5 [Sense] 領域で、[When a user is connect to WiFi and] ドロップダウンリストから必要なフィルタ条件を選択します。

- [density]：特定のエリア内の訪問者密度に基づいて通知を送信する場合は、このオプションを選択します。エリアは平方フィートまたは平方メートルで設定できます。このオプションを選択した場合は、次の設定を行います。
  - 隣接するドロップダウンリストを使用して密度制限を設定します。密度制限は、特定の値を「超える」または「未満」として設定するか、「間」を使用して値の範囲として構成できます。最初のドロップダウンリストから [more than]、[less than]、または [between] を選択し、手動で値を入力するか、2 番目のフィールドのドロップダウンリストから値を選択できます。
  - [per] フィールドで、値を手動で入力するかドロップダウンリストを使用して、密度制限の基準となる面積を指定します。次に、隣接するドロップダウンリストから測定尺度を選択します。平方フィートまたは平方メートルで測定値を指定できます。

- [count]：キャンパス、ビルディング（ネットワーク）、フロア、ゾーンなどの特定のロケーションタイプ内の一意のデバイス数に基づいて通知を送信する場合は、このオプションを選択します。このオプションを選択した場合は、次の設定を行います。
  - 隣接するドロップダウンリストを使用してデバイス数制限を設定します。デバイス数制限は、特定の値を「超える」または「未満」として設定するか、「間」を使用して値の範囲として構成できます。最初のドロップダウンリストから [more than]、[less than]、または [between] を選択し、手動で値を入力するか、2 番目のフィールドのドロップダウンリストから値を選択できます。
  - [at any] ドロップダウンリストから、デバイス数制限の基準となるロケーションタイプを選択します。

    （注） Cisco DNA Spaces コネクタまたは WLC Direct Connectを介して接続された Cisco Meraki ネットワークと Cisco AireOS/Cisco Catalyst には、ロケーションタイプとして [Campus] がありません。したがって、これらのネットワークでは、ロケーションタイプとして [Campus] を選択している場合、ルールは実行されません。

- [occupancy]：特定のロケーションの占有率に基づいて通知を送信する場合は、このオプションを選択します。[Location Hierarchy] の [Location Information]ロケーションの情報の追加 （43 ページ）ウィンドウで、ロケーションごとの占有制限を定義できます。ロケーションの占有率が、そのロケーションに定義された特定の占有率上限のパーセンテージに達したときに通知をトリガーするように設定できます。このオプションを選択した場合は、次の設定を行います。

- 隣接するドロップダウンリストを使用して、通知がトリガーされる占有率制限のパーセンテージを設定します。占有制限のパーセンテージは、特定の値を「超える」または「未満」として設定するか、「間」を使用してパーセンテージの範囲として構成できます。最初のドロップダウンリストから [more than]、[less than]、または [between] を選択し、手動でパーセンテージを入力するか、[percent] ドロップダウンリストからパーセンテージを選択できます。

ステップ 6 [Location] 領域で、ルールを適用するロケーションを指定します。

ロケーション階層全体、グループ、ロケーション、フロア、ゾーンなどの 1 つまたは複数のロケーションにルールを適用するように設定できます。密度ルールには、Cisco Meraki、Cisco AireOS、Cisco Catalyst などの複数のネットワークタイプの場所を追加できます。ロケーション階層の作成に関する詳細については、「ロケーション階層の定義」のセクションを参照してください。

選択したロケーション、またはその親や子のロケーションに定義されているメタデータに基づき、ロケーションを再度フィルタリングできます。ロケーションのメタデータ設定の詳細については、「ロケーションのメタデータの追加」のセクションを参照してください。特定のメタデータのロケーションにルールを適用するか、または特定のメタデータのロケーションを除外することができます。ロケーションのフィルタリングの詳細については、「ロケーションによるフィルタリング」を参照してください。

ステップ 7 [Schedule] 領域で、ルールを適用する期間を指定します。

a) [Set a date range for the rule] チェックボックスをオンにし、表示されるフィールドで、密度ルールを適用する期間の開始日と終了日を指定します。

b) [Set a time range for the rule] チェックボックスをオンにし、表示されるフィールドに、密度ルールを適用する時間範囲を指定します。

c) 特定の日にのみルールを適用する場合、[Filter by days of the week] チェックボックスをオンにし、表示される曜日のリストから密度ルールを適用する曜日をクリックします。

ステップ 8 [Actions] 領域で、通知の頻度と通知モードを指定します。

a) [Notify] ドロップダウンリストから、次のいずれかのオプションを選択します。

- [Only Once]：通知は一度だけビジネスユーザーに送信されます。
- [Once In]：通知は、指定された間隔に基づいて複数回送信されます。このオプションを選択する場合は、[every] ドロップダウンリストから間隔の値を選択し、隣接するドロップダウンリストから次のいずれかの間隔期間を選択します。
  - [Hour(s)]：指定した時間数に一度通知を送信します。
  - [Day(s)]：指定した日数に一度通知を送信します。
  - [Week(s)]：指定した週数に一度通知を送信します。
  - [Month(s)]：指定された月数に一度通知を送信します。

b) 送信する通知のモードを指定します。

通知は、Cisco Webex Teams、電子メール、SMS通じて顧客へ、または外部 API へ送信できます。通知タイプの詳細については、ビジネスユーザーの通知タイプ （212 ページ）を参照してください。

ルールの概要がウィンドウの右側に表示されます。

（注）
- [Via Email] オプションを使用している場合、電子メール ID の許可リストの [From] フィールドに電子メール ID が入力されていることを確認する必要があります。電子メール ID を許可リストに含める方法については、Cisco DNA Spaces サポートチームにお問い合わせください。特定の電子メール ID を使用しない場合は、デフォルトで許可されている電子メール ID である **no-reply@dnaspaces.io** を使用できます。ただし、このデフォルト ID が自動的にダッシュボードに表示されることはありません。そのため、手動で入力する必要があります。

ステップ 9 [Save and Publish] をクリックします。

ルールがパブリッシュされ、[Density Rules] ウィンドウにリストされます。

ルールを今すぐパブリッシュしたくない場合、[Save] ボタンをクリックします。ルールを開いて [Save and Publish] ボタンをクリックすることで、後でいつでもルールをパブリッシュできます。また、[Density Rules] ウィンドウの右側にある [Make Rule Live] アイコンをクリックして、ルールをパブリッシュすることもできます。

次のタスク

ウィンドウの左上に表示される 3 本線のメニューの [Right Now on WiFi] オプションを使用して、[Right Now] レポートに戻ることができます。

密度ルールレポートの表示

密度ルールレポートを使用して、各密度ルールのレポートを表示できます。

密度ルールレポートを表示するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Right Now] をクリックします。

[Right Now] ウィンドウが表示されます。

ステップ 2 ウィンドウの左上に表示される 3 本線のメニューアイコンをクリックします。

ステップ 3 [Density Rules] を選択します。

既存のすべての密度ルールが一覧表示された [Density Rules] ウィンドウが表示されます。

ステップ 4 レポートを表示する [Density Rule] をクリックします。

該当するルールの密度ルールレポートが表示されます。

密度ルールレポートには、次の詳細が含まれます。

- **ルールのサマリー**
  - [# of times triggered]：特定のルールに関する通知がトリガーされた合計回数を表示します。
  - [Top 3 locations]：通知数の多いロケーション上位 3 か所の詳細を表示します。

- [Location]：ロケーション名とそのロケーション階層。
- [# of times triggered]：特定の密度ルールに関して、このロケーションで通知がトリガーされた合計回数。
- [most recent]：特定の密度ルールに関して、このロケーションで通知がトリガーされた最新の日時。

- [Recent Activity]：特定のルールに関して、発生したすべてのアクティビティを一覧表示します。最近のアクティビティは上に表示されます。
  - [Location]：アクティビティが発生したロケーションの名前とロケーション階層。
  - [time]：アクティビティが発生した日時。
  - [count of people]：アクティビティが発生した時点でそのロケーションにいた人の総数。
  - [result]：アクティビティの結果。たとえば、あるロケーションで人数が 10 を超えた場合に 1 時間ごとに通知をトリガーするように密度ルールが設定されているときに、特定の時間に人数が 10 未満であるため通知がスキップされた場合、アクティビティの結果は「Skipped notification due to the interval set」になります。
- [Trigger History]：特定の歴月の各日における通知の詳細を表示します。
  - [Location]：レポートは [All Locations] を対象とします。
  - [Month]：矢印キーを使用して、レポートを表示する月を選択します。デフォルトでは、通知が最近トリガーされた月と累積通知数が表示されます。
  - [Calendar]：各日のさまざまなロケーションタイプ（キャンパス、ビルディング、フロア、ゾーン）に関する通知がカレンダーに表示されます。カレンダーの日付をクリックすると、その日のロケーション、時間、人数、結果といった通知の詳細が表示されます。

密度ルールのテスト

密度ルールをテストするには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Right Now] をクリックします。

[Right Now] ウィンドウが表示されます。

ステップ 2 ウィンドウの左上に表示される 3 本線のメニューアイコンをクリックします。

ステップ 3 [Density Rules] を選択します。

既存のすべての密度ルールが一覧表示された [Density Rules] ウィンドウが表示されます。

ステップ 4 テストする密度ルールの右端に表示される [Test Rule] アイコンをクリックします。

[Test the Rule] ウィンドウが表示されます。

ステップ 5 選択したチャネルで通知をトリガーするには [Yes] をクリックします。

通知がトリガーされ、成功メッセージが表示されます。

ステップ 6 [Continue] をクリックします。

密度ルールの変更

密度ルールを変更するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Right Now] をクリックします。

[Right Now] ウィンドウが表示されます。

ステップ 2 ウィンドウの左上に表示される 3 本線のメニューアイコンをクリックします。

ステップ 3 [Density Rules] を選択します。

既存のすべての密度ルールが一覧表示された [Density Rules] ウィンドウが表示されます。

ステップ 4 変更する密度ルールの右端に表示される [Edit Rule] アイコンをクリックします。

ステップ 5 必要な変更を加えます。

ステップ 6 変更を保存するには、[Save] をクリックします。または変更をパブリッシュするには、[Save and Publish] をクリックします。

（注） ライブ ルールに表示されるのは [Save and Publish] ボタンのみです。[Save and Publish] ボタンをクリックすると、変更を反映したルールがパブリッシュされます。

密度ルールの一時停止

密度ルールを一時停止するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Right Now] をクリックします。

[Right Now] ウィンドウが表示されます。

ステップ 2 ウィンドウの左上に表示される 3 本線のメニューアイコンをクリックします。

ステップ 3 [Density Rules] を選択します。

既存のすべての密度ルールが一覧表示された [Density Rules] ウィンドウが表示されます。

ステップ 4 一時停止する密度ルールの右端に表示される [Pause Rule] アイコンをクリックします。

ステップ 5 表示されるウィンドウで、一時停止を確定します。

密度ルールが一時停止されました。

次のタスク

（注） 複数の密度ルールを一時停止するには、一時停止する密度ルールのチェックボックスをオンにし、ページの下部に表示される [Pause] ボタンをクリックします。

密度ルールの再開

密度ルールを再開するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Right Now] をクリックします。

[Right Now] ウィンドウが表示されます。

ステップ 2 ウィンドウの左上に表示される 3 本線のメニューアイコンをクリックします。

ステップ 3 [Density Rule] を選択します。

[Density Rules] ウィンドウが表示され、既存のすべての密度ルールがリストされます。

ステップ 4 再開する密度ルールの右端に表示される [Make Rule Live] アイコンをクリックします。

（注） デフォルトでは、すべてのルールのアイコン名が [Pause Rule] となります。一時停止しているルールについてのみ、アイコン名が [Make Rule Live] に変わります。

密度ルールが再開します。

次のタスク

（注） 複数の密度ルールを再開するには、再開する密度ルールのチェックボックスをオンにし、ウィンドウの下部に表示される [Make Live] ボタンをクリックします。

密度ルールの削除

密度ルールを削除するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Right Now] をクリックします。

[Right Now] ウィンドウが表示されます。

ステップ 2 ウィンドウの左上に表示される 3 本線のメニューアイコンをクリックします。

ステップ 3 [Density Rule] を選択します。

[Density Rules] ウィンドウが表示され、既存のすべての密度ルールがリストされます。

ステップ 4 削除する密度ルールの右端に表示される [Delete Rule] アイコンをクリックします。

ステップ 5 表示されるダイアログボックスで [Delete Rule] をクリックします。

密度ルールが削除されます。

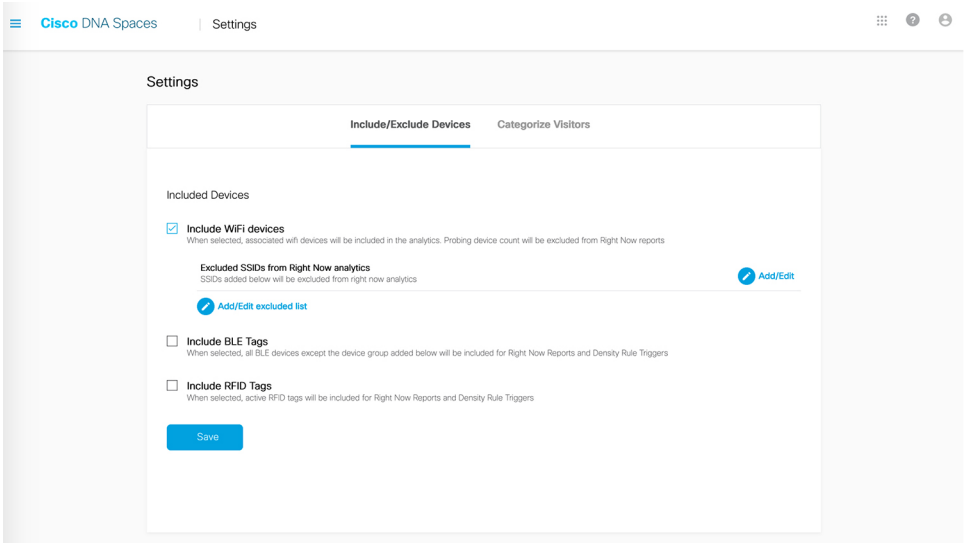
次のタスク

（注） 複数の密度ルールを削除するには、削除する密度ルールのチェックボックスをオンにし、ページの下部に表示される [Delete] ボタンをクリックします。

設定

[Settings] メニューは、[Right Now] アプリレポート内のデバイス、SSID、および訪問者を管理するのに役立ちます。[Settings] メニューには、[Include/Exclude Devices] タブと [Categorize Visitors] タブが含まれています。

図 10 : [Right Now] - [Settings]



デバイスを含めるまたは除外する

[Include/Exclude Devices] タブを使用して、Right Now レポートの Wi-Fi、BLE、および RFID の各デバイスについて次のオプションから選択します。

- Wi-Fi デバイス：分析に Wi-Fi デバイスを含めるには、[Include WiFi Devices] を選択します。

  特定の SSID に接続されているデバイスを Right Now 分析から除外するには、[Add/Edit] または [Add/Edit excluded list] をクリックし、[Exclude SSIDs] リストから目的の SSID を選択します。

- BLE タグ：Right Now レポートに BLE タグを含めるには、[Include BLE Tags] を選択します。

  Right Now 分析から特定のデバイス グループを除外するには、[Add/Edit] または [Add/Edit excluded list] をクリックし、[Exclude BLE devices] リストから目的の BLE デバイスを選択します。

- RFID タグ：Right Now レポートに RFID タグを含めるには、[Include RFID Tags] を選択します。

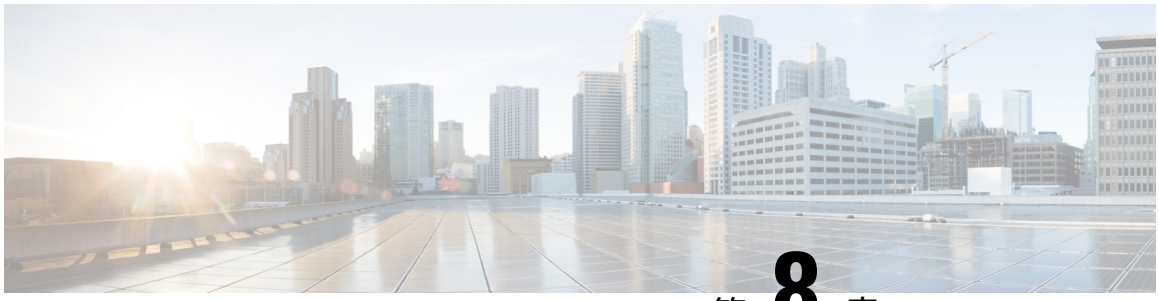
- 有線デバイス：有線デバイスを Right Now レポートのアクティブな訪問者の一部として含めるには、[Include Wired Devices] を選択します。デフォルトでは、有線デバイスは除外されます。

（注） RFID タグと BLE タグを選択すると、対応するデバイス数も Right Now レポートに表示されます。

訪問者の分類

[Categorize Visitors] タブを使用して、SSID に参加した訪問者を訪問者タイプに基づいて自動または手動で分類します。次のオプションを使用できます。

- Auto
- ゲスト
- Employee
- Custom



第 8 章

カメラメトリック

この章では、Camera Metrics アプリについて説明します。

カメラメトリック

[Camera Metrics] アプリを使用すると、Meraki カメラを使用してキャプチャしたデータに基づくメトリクスレポートを表示できます。このレポートは特定の月に表示されます。

（注）

- [Camera Metrics] アプリは、[Setup] の [Camera] オプションを使用して Cisco DNA Spaces で Meraki カメラを設定した場合にのみ、レポートを表示します。Meraki カメラの設定に関する詳細については、Cisco Meraki カメラと連動するように Cisco DNA Spaces を設定する （327 ページ）を参照してください。
- まだ Meraki カメラを設定していないか、Meraki カメラのデータがない Cisco DNA Spaces ユーザーアカウントの場合、サンプルレポートが表示されます。
- まだ Meraki カメラを設定していない Cisco DNA Spaces ユーザーアカウントの場合、「Looks like you haven't setup your Meraki Camera（Meraki カメラが設定されていないようです）」という通知が、Meraki カメラの設定ウィンドウに移動するためのセットアップガイドリンクとともに表示されます。

カメラメトリックレポートの表示

カメラメトリックレポートを表示するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Camera Metrics] をクリックします。

今月のカメラメトリックレポートが表示されます。

図 *11* : カメラメトリックレポート

ステップ 2 必要に応じて、[Location] ドロップダウンリストから、レポート表示の対象となるロケーションを選択します。

（注） デフォルトでは、ルートロケーションのレポートが表示されます。

ステップ 3 [Month] ドロップダウンリストから、レポートを表示する年と月を選択します。

レポートは、選択したロケーションと月でフィルタ処理されます。

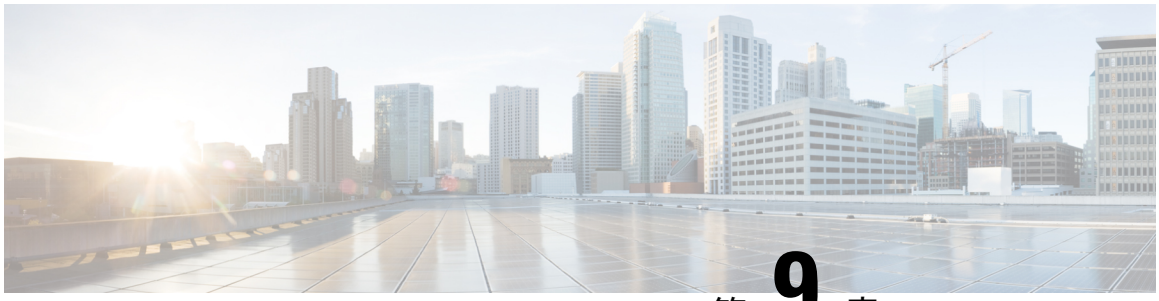
（注） 2020 年に [Camera] オプションが Cisco DNA Spaces に導入されたため、2020 年以降の年のみを選択できます。

現在、レポートには次のグラフが表示されます。

- [Monthly Footfall: All Locations]：選択した月間の、フィルタ処理されたロケーションとその子ロケーションへの総来訪者数を表示します。選択したロケーションとその子ロケーションへの過去 12 か月間の平均来訪者数が過去の平均として表示されます。
- [Daily Footfall]：選択した月の各日の、フィルタ処理されたロケーションとその子ロケーションへの総来訪者数を表示します。選択した月のすべての日における、選択したロケーションとその子ロケーションへの平均日次エントリは、平均日次来訪者数として表示されます。
- [Footfall Distribution : By hour of day]：フィルタ処理されたロケーションとその子ロケーションへの選択した月の各時間における平均来訪者数を「総来訪者数のパーセンテージ」として表示します。グラフの右上にある [Toggle Historical View] アイコンをクリックすると、1 日の各時間の過去における平均を表示できます。1 日の各時間の過去における平均（フィルタ処理されたロケーションとその子ロケーションに該当する日時に滞在した人の過去 12 か月間の平均数）が、過去の平均の合計（フィルタ処理されたロケーションとその子ロケーションに滞在した人の過去 12 か月間の平均数）に対するパーセンテージとして表示されます。
- [Presence by hour of day]：選択した月間の 1 日の各時間における、フィルタ処理されたロケーションとその子ロケーションに滞在した人の平均数を表示します。過去 12 か月間の 1 日の各時間における、フィルタ処理されたロケーションとその子ロケーションに滞在した人の平均数を表示します。
- [Peak Presence : By hour of day]：このグラフは、ネットワークロケーション用にのみ使用できます。このグラフは、選択した月の 1 日の各時間における平均滞在者数を累積して表示し、特定の日時におけるピーク数を示します。

（注） 理想的には、過去 12 か月間のチャートの過去における平均が表示されます。とはいえ、過去 12 か月以内にカメラを設置した場合は、カメラを設置した月のデータが過去の平均と見なされます。

すべてのチャートは、カメラ用に描画されたトリップワイヤラインを経た訪問者の出入りに基づいています。



第 9 章

キャプティブポータルアプリの使用

この章では、Cisco DNA Spaces を使用してキャプティブポータルを作成する方法について説明します。

ポータルの作成と管理

ポータルは、Wi-Fi ユーザーが SSID に接続したときに表示されるユーザーインターフェイスです。Cisco DNA Spaces を使用してキャプティブポータルを作成し、Cisco DNA Spaces により提供されるさまざまなポータルモジュールを使用して、ポータルを強化できます。

Cisco DNA Spaces では、独自のポータル（エンタープライズ キャプティブ ポータル）を使用して、Wi-Fi に接続するエンドユーザーをオンボードすることもできます。エンタープライズ キャプティブ ポータルの詳細については、エンタープライズ キャプティブ ポータルを参照してください。

ポータル作成の前提条件I

- ポータルを適用可能なロケーションを指定するには、ロケーション階層を定義する必要があります。ロケーション階層の定義の詳細については、ロケーション階層の定義 （27ページ）のセクションを参照してください。
- ポータルのソーシャル認証を設定する場合は、ソーシャルアプリで特定の設定を行い、そのソーシャルアプリをCisco DNA Spacesに追加する必要があります。ソーシャル認証の設定の詳細については、「ポータルへのソーシャル認証」のセクションを参照してください。
- ポータルにSMSベースの認証を設定する場合は、SMSゲートウェイを設定する必要があります。SMSゲートウェイ設定の詳細については、Cisco DNA Spaces でのSMSゲートウェイの設定 （168ページ）のセクションを参照してください。

帯域幅の要件

キャプティブポータルの場合、優れたエンドユーザーエクスペリエンスのために、最低30 Mbpsの帯域幅をお勧めします。

次の表は、帯域幅に基づきキャプティブポータルをロードするための応答時間を示しています。

表 *5:*

帯域幅	ユーザ数	応答（秒）
1 Mbps	1	5.86
	2	5.49
	3	5.40
	4	5.63
	5	5.92

帯域幅	ユーザ数	応答（秒）
2 Mbps	1	5.09
	2	5.10
	3	5.04
	4	5.25
	5	5.16
	6	5.23
	7	5.26
	8	5.30
	9	5.34
	10	5.40
	11	5.49
5 Mbps	5	4.92
	10	4.98
	11	5.05
	12	5.08
	13	5.11
	14	5.13
	15	5.17
	16	5.18
	20	5.25
7 Mbps	25	5.13
	30	5.20
	31	5.23
	32	5.26
	33	5.29
	34	5.33

帯域幅	ユーザ数	応答（秒）
9 Mbps	30	4.93
	35	4.98
	40	5.05
	41	5.07
	42	5.10
	43	5.13
	44	5.15
	45	5.17
	46	5.19
	47	5.15
11 Mbps	35	4.68
	40	4.91
	50	5.05
	55	5.16
	56	5.18
	57	5.20
	58	5.24
	59	5.28
	60	5.25
	61	5.30

サンプルのポータル

Cisco DNA Spaces は、さまざまな認証タイプのサンプルポータルを提供しています。

- データキャプチャによる電子メール認証
- パスワードの確認とデータのキャプチャを含むインライン SMS
- インラインソーシャル認証
- パスワードの確認とデータのキャプチャを含む SMS
- リンクの確認を含む SMS

- 電子メール認証
- ユーザー契約

さらに、COVID-19 の要件を満たすためのサンプルポータルが提供されています。

サンプルポータルを確認してコピーを作成するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Home] を選択します。
ステップ 2 表示されるウィンドウで、[Captive Portal] を選択します。
ステップ 3 表示される [Captive Portal] ウィンドウで、左ペインの **Portal** を選択します。

ポータルリストの下部に、さまざまな認証タイプのサンプルポータルが表示されます。

ステップ 4 目的のサンプルポータルの右端にある [Make a Copy] アイコンをクリックします。
ステップ 5 表示されるポータルウィザード画面で、キャプティブポータルの名前を指定します。
ステップ 6 必要に応じて、ポータル設定に必要なカスタマイズを行います。
ステップ 7 ポータルを保存します。

ポータルの作成

ポータルを定義するときに、ポータルを利用可能にする必要があるロケーションを設定することもできます。

ポータルを作成するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Home] を選択します。
ステップ 2 表示されるウィンドウで、[Captive Portal] を選択します。
ステップ 3 表示される [Captive Portal] ウィンドウで、左ペインの [Portal] を選択します。
ステップ 4 [Create New] をクリックします。

ポータルウィザードが表示されます。

ステップ 5 [Portal Name] フィールドに、ポータルの名前を入力します。
ステップ 6 このポータルを特定のロケーションでのみ使用できるようにする場合は、[Enable this portal forall locations] チェックボックスをオフにします。

（注） デフォルトでは、[Enable this portal forall locations] チェックボックスがオンになっており、ロケーション階層内のすべてのロケーションでポータルを使用できるようになっています。

ステップ 7 [Next] をクリックします。

[Authentication] ウィンドウが表示されます。

ステップ 8 [Authentication Type] ドロップダウンリストから、ポータルに適用する認証タイプを選択します。

選択した認証タイプに基づいて、追加のフィールドが表示されます。各種認証タイプの認証手順の詳細については、ポータルへの認証の設定 （113 ページ）を参照してください。

ステップ 9 認証タイプの詳細を指定したら、[Next] をクリックします。

[Data Capture] ウィンドウが表示されます。

（注） [Social Sign In] 認証の場合、ソーシャルサインインではデータキャプチャがないため、[User Agreements] 画面に移動します。ソーシャルサインインでは手順 10 から手順 12 をスキップします。

ステップ 10 このポータルにデータキャプチャフォームを追加する場合は、[Enable Data Capture] チェックボックスをオンにします。

ステップ 11 データキャプチャフォームを設定します。[+ Add Field Element] ボタンを使用して、データキャプチャフォームに必要なフィールドを追加します。データキャプチャフォームへのフィールドの追加の詳細については、ポータルへのデータキャプチャフォームの追加 （122 ページ）を参照してください。

ステップ 12 [Next] をクリックします。

[User Agreements] ウィンドウが表示されます。

ステップ 13 [Terms & Condition Message] フィールドに、ポータルの「利用規約」を入力します。

（注） デフォルトでは、[Enable Terms & Conditions] チェックボックスはオンになっています。「利用規約」を指定しない場合は、[Enable Terms & Conditions] チェックボックスをオフにします。

ステップ 14 利用規約とともにプライバシーポリシーを表示する場合は、[Enable Privacy Policy] チェックボックスをオンにして、表示される [Privacy Policy] フィールドにプライバシーポリシーを入力します。

プライバシーポリシーを指定すると、顧客獲得時に「利用規約」とともにプライバシーポリシーも表示されます。

ステップ 15 [How frequently do you want users to accept agreements] ドロップダウンリストから、顧客がインターネットにアクセスするために「利用規約」に同意する必要がある頻度を選択します。

ステップ 16 [User Accepts Terms In] 領域で、顧客獲得時に「利用規約」をどのように表示するかを選択します。

- [1-Click]：[Terms & Conditions] リンクのみを表示する場合は、このオプションを選択します。このオプションを選択すると、顧客獲得時に、顧客は [Accept Terms and Continue] ボタンをクリックして先に進むことができます。
- [2-Click]：[Terms & Conditions] リンクとともにチェックボックスを表示する場合は、このオプションを選択します。このオプションを選択した場合、顧客獲得時に、顧客はチェックボックスを選択し、[Accept Terms and Continue] ボタンをクリックして先に進む必要があります。

（注） [2-Click] オプションは、特定の国の法的要件を満たすために Cisco DNA Spaces で提供されています。

ステップ 17 特定の年齢未満の顧客によるインターネットアクセスを制限する場合は、[Enable Age gating] チェックボックスをオンにして、必要な年齢制限の方法を以下から選択します。

- [Moderate]：このオプションを選択した場合、顧客獲得時に、顧客は年齢が 16 歳以上であることを確認する必要があります。

- [Strict]：このオプションを選択すると、顧客獲得時に、顧客は生年月日を指定してインターネットにアクセスする必要があります。顧客が16歳未満の年齢を指定した場合、警告メッセージが表示され、顧客はそれ以上インターネットにアクセスできなくなります。ただし、必要に応じて、年齢を変更するオプションが顧客に提供されます。

ステップ 18 [Save and Configure Portal] をクリックします。

[Portal saved successfully] メッセージが表示されて [Portal] ウィンドウが開き、左側にポータルモジュールが、右側にポータルのプレビューが表示されます。

ステップ 19 ポータル モジュール （109 ページ）を使用してポータルに機能を追加します。

ステップ 20 [Save] をクリックして、各モジュールに加えた変更を保存します。

（注） ポータルの作成時に、ポータルの名前と場所を指定した後で、ポータルを保存できます。新しいポータルが [Portal] ウィンドウにリストされます。そのポータルの [Edit Portal] ボタンを使用して、認証タイプ、利用規約、データキャプチャフォームなどを後でいつでも構成できます。

（注） キャプティブポータルを使用してSSIDに接続する顧客の名前や電話番号などの詳細情報をキャプチャするには、「データキャプチャフォーム」をキャプティブポータルに追加していることを確認してください。顧客獲得時（ランタイム）に、インターネットをプロビジョニングする前に、データキャプチャフォームが顧客に表示されます。キャプチャされた顧客の詳細情報は、Cisco DNA Spaces に保存されます。

（注） ポータルをキャプティブポータルルールに関連付けると、ポータルが稼働を開始し、そのルールが公開されます。

ポータル モジュール

Cisco DNA Spaces のポータルモジュールは次のとおりです。

- **Brand Name**：このモジュールを使用してポータルのブランド名を定義します。ブランド名をテキストやロゴのイメージで追加できます。
- **Welcome Message**：このモジュールを使用してポータルにウェルカム メッセージを追加します。初回ユーザーとリピートユーザーに異なるウェルカムメッセージを表示するように構成できます。
- **Notice**：このモジュールを使用してポータルに通知を追加します。これにより、必要に応じてポータルユーザに通知を表示できます。太字テキスト、テキスト、またはイメージ形式のテキストで通知するように設定できます。
- **Authentication**：ポータルの作成時に選択した認証タイプに基づいて、ポータルに認証モジュールが表示されます。モジュールの名前は、認証タイプに基づきます。たとえば、ポータルの認証タイプとして [SMS with link verification] を選択した場合、そのポータルの認証モジュールの名前は「SMS Authentication」になります。認証モジュールには、ポータルのランディングページ URL を構成するためのプロビジョニングが含まれます。[Data

Capture] と [User Agreements] の両方が有効になっていない場合、認証タイプ [No Authentication] の認証モジュールは使用できません。

- **Venue Map**：このモジュールを使用して、施設マップのラベルとアイコンを追加します。施設マップは、ロケーションに基づいてワイヤレスネットワークからポータルにアップロードされます。
- **Videos**：このモジュールを使用してポータルに YouTube ビデオを追加します。また、ポータルのビデオ セクションに適したキャプションとアイコンも追加できます。またアップロードすると、ビデオのプレビューを表示できます。
- **Feedback**：このモジュールを使用してポータルのフィードバックの質問を追加します。複数の選択肢と評価の質問を追加できます。このモジュールでは、[Submit] ボタン、[Thank You] メッセージ、および [Post Submission] ボタンのラベルもカスタマイズできます。コメントを追加するためのテキストボックスをユーザーに表示するかどうかを設定することができます。また、フィードバック用の電子メールアドレスおよび件名を指定することもできます。
- **Help**：このモジュールを使用して、顧客がサポートを求める際に連絡するヘルプの電話番号を追加します。ヘルプのキャプションおよびアイコンをカスタマイズできます。
- **Get Apps**：このモジュールを使用してポータルにアプリケーションを追加します。このモジュールを使用して、各アプリケーションに適したキャプションとアイコンを追加できます。
- **Get Internet**：顧客がポータルの [Get Internet] セクションから移動できる外部 URL を追加します。この URL にアクセスするには、指定された利用規約を顧客が承認する必要があります。
- **Promos & Offers**：このモジュールを使用して、ポータルで表示するプロモーションおよび特典を追加します。プロモーションのタイトルを変更できます。プロモーションごとに適したキャプションとイメージを追加し、プロモーションの詳細の URL を指定できます。プロモーションは回転式で表示されます。
- **Add Module**：このモジュールを使用して、ポータルにカスタマイズしたコンテンツおよびメニューアイテムを追加します。前述のすべてのモジュールは、Cisco DNA Spaces によって提供されるデフォルトのモジュールです。[Add Module] ボタンを使用すると、要件に応じてポータルに別のアイテムを追加できます。

ポータルの言語の設定

Cisco DNA Spaces では、ポータル内のモジュールのキャプションや静的コンテンツを表示する言語を設定できます。英語以外の言語で静的コンテンツを表示するには、対応するテキストを Cisco DNA Spaces にアップロードする必要があります。Cisco DNA Spaces は、英語以外の言語でのコンテンツの入力をサポートしていません。デフォルトの言語は英語に設定されています。デフォルトの言語は変更できます。

（注） Cisco DNA Spaces を使用して、ある言語で作成されたコンテンツを他の言語に翻訳することはできません。

ポータルのコンテンツを表示する言語を設定するには、次の手順を実行します。

ステップ 1 メッセージ、国名などの静的コンテンツを英語ではない言語で表示するには、その言語のキー値をアップロードします。任意の言語のキー値をアップロードする操作の詳細については、任意の言語の静的コンテンツのキー値のアップロード （112 ページ）を参照してください。

ステップ 2 言語を設定するポータルを開きます。

ステップ 3 [Portal] ウィンドウの上部にある [Languages]（地球）アイコンをクリックします。

[Add Language] ウィンドウが表示されます。

ステップ 4 [Add Language] をクリックします。

ステップ 5 表示される検索フィールドに、言語を入力します。

その言語が Cisco DNA Spaces でサポートされている場合、言語名がドロップダウンリストに表示されます。

ステップ 6 言語名の隣に表示される [Add] ボタンをクリックします。

言語が [Added Languages] リストに追加されます。

ステップ 7 [Add] をクリックします。

ポータルで、[Languages] アイコンの隣にドロップダウンリストが表示され、新しく追加された言語がそのドロップダウンリストに表示されます。

ステップ 8 [Languages] アイコンの隣のドロップダウンリストから、ポータルの静的コンテンツを表示する言語を選択します。

各モジュールのキャプションは、選択された言語で表示されます。

デフォルト言語の設定

デフォルト言語を設定するには、次の手順を実行します。

ステップ 1 ポータルで、ウィンドウ右上の [Languages] アイコンをクリックします。

ステップ 2 [Add Language] ウィンドウで、[Default Language] ドロップダウンリストからデフォルト言語を選択します。

ステップ 3 [Add] をクリックします。

任意の言語の静的コンテンツのキー値のアップロード

静的コンテンツを英語以外の言語で表示するように設定するには、次の手順を実行します。

ステップ 1 ポータルで、ウィンドウ右上の [Languages] アイコンをクリックします。

ステップ 2 [Add Language] ウィンドウで [Download] をクリックしてテンプレートをダウンロードし、保存します。

ステップ 3 テンプレートを開きます。

テンプレートには、さまざまな静的メッセージのキー値と、言語が英語である場合に表示されるメッセージが含まれています。英語の列には、1 行目に「en」と表示されています。

ステップ 4 英語の列の隣に、静的コンテンツを表示する言語の言語識別子を入力します。

たとえば、コンテンツをアラビア語で表示する場合は、1 行目に「AR」と入力します。

ステップ 5 残りの行には、対応するキーに対して表示する必要があるテキストを入力します。

ステップ 6 ファイルを保存します。

ステップ 7 [Add Language] ウィンドウで、[Upload] ボタンを使用してウィンドウをアップロードします。

ステップ 8 [Add] をクリックします。

次のタスク

静的コンテンツを任意の言語で表示する方法については、ポータルの言語の設定 （110ページ）を参照してください。

さまざまな言語の言語コードを次の図に示します。

図 *12 : [*言語コード（*Language Code***）*]***

[{"Abkhaz":"ab"},{"Afar":"aa"},{"Afrikaans":"af"},{"Akan":"ak"},{"Albanian":"sq"},{"Amharic":"am"},{"Arabic":"ar"},{"Aragonese":"an"},
{"Armenian":"hy"},{"Assamese":"as"},{"Avaric":"av"},{"Avestan":"ae"},{"Aymara":"ay"},{"Azerbaijani":"az"},{"Bambara":"bm"},
{"Bashkir":"ba"},{"Basque":"eu"},{"Belarusian":"be"},{"Bengali":"bn"},{"Bihari":"bh"},{"Bislama":"bi"},{"Bosnian":"bs"},{"Breton":"br"},
{"Bulgarian":"bg"},{"Catalan":"ca"},{"Chamorro":"ch"},{"Chechen":"ce"},{"Chichewa":"ny"},{"Chinese":"zh"},{"Chuvash":"cv"},
{"Cornish":"kw"},{"Corsican":"co"},{"Cree":"cr"},{"Croatian":"hr"},{"Czech":"cs"},{"Danish":"da"},{"Divehi":"dv"},{"Dutch":"nl"},
{"Dzongkha":"dz"},{"English":"en"},{"Esperanto":"eo"},{"Estonian":"et"},{"Ewe":"ee"},{"Faroese":"fo"},{"Fijian":"fj"},{"Finnish":"fi"},
{"French":"fr"},{"Fula":"ff"},{"Galician":"gl"},{"Georgian":"ka"},{"German":"de"},{"Greek":"el"},{"GuaranÃ":"gn"},{"Gujarati":"gu"},
{"Haitian":"ht"},{"Hausa":"ha"},{"Hebrew":"he"},{"Herero":"hz"},{"Hindi":"hi"},{"Hungarian":"hu"},{"Interlingua":"ia"},{"Indonesian":"id
{"Interlingue":"ie"},{"Irish":"ga"},{"Igbo":"ig"},{"Inupiaq":"ik"},{"Ido":"io"},{"Icelandic":"is"},{"Italian":"it"},{"Inuktitut":"iu"},
{"Japanese":"ja"},{"Javanese":"jv"},{"Kalaallisut":"kl"},{"Kannada":"kn"},{"Kanuri":"kr"},{"Kashmiri":"ks"},{"Kazakh":"kk"},{"Khmer":"km
{"Kikuyu":"ki"},{"Kinyarwanda":"rw"},{"Kyrgyz":"ky"},{"Komi":"kv"},{"Kongo":"kg"},{"Korean":"ko"},{"Kurdish":"ku"},{"Kwanyama":"kj"},
{"Latin":"la"},{"Luxembourgish":"lb"},{"Ganda":"lg"},{"Limburgish":"li"},{"Lingala":"ln"},{"Lao":"lo"},{"Lithuanian":"lt"},
{"Latvian":"lv"},{"Manx":"gv"},{"Macedonian":"mk"},{"Malagasy":"mg"},{"Malay":"ms"},{"Malayalam":"ml"},{"Maltese":"mt"},{"Marathi":"mr"}
{"Marshallese":"mh"},{"Mongolian":"mn"},{"Nauru":"na"},{"Navajo":"nv"},{"Nepali":"ne"},{"Ndonga":"ng"},{"Norwegian Nynorsk":"nn"},
{"Norwegian":"no"},{"Nuosu":"ii"},{"Southern Ndebele":"nr"},{"Occitan":"oc"},{"Ojibwe":"oj"},{"Old Church Slavonic":"cu"},{"Oromo":"om"}
{"Oriya":"or"},{"Ossetian":"os"},{"Panjabi":"pa"},{"Persian":"fa"},{"Polish":"pl"},{"Pashto":"ps"},{"Portuguese":"pt"},{"Quechua":"qu"},
{"Romansh":"rm"},{"Kirundi":"rn"},{"Romanian":"ro"},{"Russian":"ru"},{"Sanskrit":"sa"},{"Sardinian":"sc"},{"Sindhi":"sd"},{"Northern
Sami":"se"},{"Samoan":"sm"},{"Sango":"sg"},{"Serbian":"sr"},{"Scottish Gaelic":"gd"},{"Shona":"sn"},{"Sinhala":"si"},{"Slovak":"sk"},
{"Slovene":"sl"},{"Somali":"so"},{"Southern Sotho":"st"},{"Spanish":"es"},{"Sundanese":"su"},{"Swahili":"sw"},{"Swati":"ss"},
{"Swedish":"sv"},{"Tamil":"ta"},{"Telugu":"te"},{"Tajik":"tg"},{"Thai":"th"},{"Tigrinya":"ti"},{"Tibetan Standard":"bo"},{"Turkmen":"tk"
{"Tagalog":"tl"},{"Tswana":"tn"},{"Tonga":"to"},{"Turkish":"tr"},{"Tsonga":"ts"},{"Tatar":"tt"},{"Twi":"tw"},{"Tahitian":"ty"},
{"Uyghur":"ug"},{"Ukrainian":"uk"},{"Urdu":"ur"},{"Uzbek":"uz"},{"Venda":"ve"},{"Vietnamese":"vi"},{"Walloon":"wa"},{"Welsh":"cy"},
{"Wolof":"wo"},{"Western Frisian":"fy"},{"Xhosa":"xh"},{"Yiddish":"yi"},{"Yoruba":"yo"},{"Zhuang":"za"},{"Zulu":"Zulu"}]

ポータルへの認証の設定

ハッキングや悪用からポータルを保護するため、ポータルには、さまざまな認証オプションを設定することができます。顧客は、認証が成功した場合にのみアクセスできます。

インターネットプロビジョニングのための認証は、SMS、電子メール、アクセスコード、または Facebook、Twitter、 LinkedIn などのソーシャルネットワークを介して実行できます。Cisco DNA Spaces は、SMS 認証用としてサードパーティベンダーの SMS ゲートウェイをサポートしています。「パスワードを含む SMS による確認」または「リンクを含む SMS による確認」を使用して SMS 認証を実行するように設定できます。「パスワードを含む SMS による確認」の場合、ポータル用のカスタム認証コードを定義するか、認証コードの自動生成を設定できます。

顧客の獲得中に、顧客がポータルのメニュー項目をクリックすると、認証プロセスが開始されます。ただし、認証モジュールがキャプティブポータルに表示されるようにインライン認証を設定することもできます。インライン認証の詳細については、インライン認証 （121 ページ）を参照してください。

Cisco DNA Spaces は、次の認証タイプをサポートしています。

- **パスワードを含む SMS による確認**：この認証タイプでは、携帯電話番号の確認が必須です。顧客が有効な携帯電話番号を入力すると、リンクと認証コードを含む SMS が携帯電話番号に送信されます。顧客は、SMS 内の認証コードを入力することで、インターネットにアクセスできます。認証コードが入力されるまで、顧客は操作を進めることができません。この認証タイプの使用例には、SMS ベースのエンゲージメントキャンペーン、インターネットに接続するユーザーを確認するための国固有の要件などがあります。顧客獲得時の認証手順については、SMS with Password Verification 認証の手順 （183 ページ）を参照してください。「パスワードを含む SMS による確認」の詳細については、ポータルでのパスワード検証付き SMS の設定 （115 ページ）のセクションを参照してください。

  リンクを含む SMS による確認：この認証タイプでは、携帯電話番号の確認はオプションです。顧客が有効な携帯電話番号を入力すると、認証リンクを含む SMS が携帯電話番号に送信されます。顧客は、SMS の認証リンクをクリックして確認を完了することができます。ただし、顧客は確認プロセスをスキップして先に進むことができます。この認証タイプは、携帯電話番号の確認が必須でない場合に使用できます。顧客獲得時の認証手順については、リンク検証付き SMS による認証の手順 （181 ページ）を参照してください。詳細については、ポータルでのリンク検証付き SMS の設定 （114 ページ）を参照してください。

  電子メール：顧客がインターネットにアクセスするには、有効な電子メール ID を入力する必要があります。顧客獲得時の認証手順については、電子メール認証の手順 （185 ページ）を参照してください。電子メール認証の設定に関する詳細については、Email 認証のためのポータルの設定 （119 ページ）を参照してください。

  ソーシャルサインイン：認証のために設定されているソーシャルサイトに顧客がログインしている場合にのみ、インターネットへのアクセスが提供されます。このオプションを使用するには、少なくとも 1 つのソーシャル サイトを設定する必要があります。顧客獲得時の認証手順については、ソーシャル認証の手順 （189 ページ）を参照してください。ソー

シャルサインイン認証の設定に関する詳細については、「Social Sign In 認証のためのポータル設定」のセクションを参照してください。

アクセスコード：顧客がインターネットにアクセスするには、有効なアクセスコードを入力する必要があります。顧客獲得時の認証手順については、アクセスコード認証の手順（187ページ）を参照してください。アクセスコード認証の設定に関する詳細については、アクセスコード認証用ポータルの設定（120 ページ）を参照してください。

認証なし：認証プロセスなしでインターネットへのアクセスが提供されます。顧客獲得時の認証手順については、利用規約による認証省略の手順（188 ページ）を参照してください。ポータルを認証なしに設定する手順の詳細については、認証なしでのポータルの設定（121 ページ）を参照してください。

（注） [Opt In] オプションは、「ソーシャルサインイン」認証タイプでは使用できません。「ソーシャルサインイン」を除くすべての認証タイプ用にデータキャプチャフォームを設定できます。データキャプチャフォーム設定の詳細については、ポータルへのデータキャプチャフォームの追加（122ページ）を参照してください。オプトイン機能の詳細については、「ユーザーのオプトインオプション」のセクションを参照してください。

（注） **リンクを含む SMS による確認**または**パスワードを含む SMS による確認**の場合、SMS ゲートウェイに渡す必要のある追加情報を含めることができます。たとえば、英語以外の言語でSMSを顧客に送信する場合、SMS ゲートウェイに送信される SMS にその情報を含めることができるようになりました。

ポータルでのリンク検証付き SMS の設定

ポータルで「リンク検証付き SMS」を設定するには、次の手順を実行します。

ステップ 1 ポータルを作成するときに、[Active Access Codes] ドロップダウンリストから [SMS with Link verification] を選択します。

ステップ 2 このポータルでインライン認証を構成し、ホームページに「データキャプチャフォーム」と「ユーザーの同意」を表示する場合は、[Display Authentication, Data Capture, and User Agreements on portal home page] チェックボックスをオンにします。インライン認証の詳細については、インライン認証 （121 ページ）を参照してください。

ステップ 3 通知を受け取るかどうか選択するオプションを顧客に提供する場合は、[Allow users to Opt in to receive message] チェックボックスをオンにします。

ステップ 4 [Allow users to Opt in to receive message] チェックボックスがオンになっている場合、次のフィールドが表示されます。

- [Opt in Message]：オプトインメッセージを入力します。
- [Default Opt-In Check Box Behavior]

- [Checked]：顧客獲得時に [**Opt In**] チェックボックスがデフォルトでオンの状態で表示されるようにする場合は、このオプションをクリックしま
- [Unchecked]：顧客獲得時に [**Opt In**] チェックボックスがデフォルトでオフの状態で表示されるようにする場合は、このオプションをクリックします。

ステップ 5 [SMS Text] フィールドに、ユーザーに送信する SMS に表示されるテキストメッセージを入力します。

（注） 顧客がキャプティブ ポータルにアクセスできるリンクを表示する際は、テキストメッセージを編集する際に「{Link}」が削除されていないことを確認します。

ステップ 6 [Default Country] ドロップダウンリストから、この設定が適用される国を選択します。

ステップ 7 [SMS Gateway] ドロップダウンリストから、SMS ゲートウェイを選択します。

[Settings] オプションで設定された SMS ゲートウェイが選択可能になっています。シスコが提供する有料の [Demo Gateway] も使用できます。

（注） SMS ゲートウェイを設定するときの詳細については、Cisco DNA Spaces での SMS ゲートウェイの設定 （168 ページ）を参照してください。

ステップ 8 変更内容を保存します。

次のタスク

（注） 認証タイプが [SMS with link verification] のポータルには、[SMS Authentication] という名前の認証モジュールがあります。この認証モジュールの詳細については、認証モジュール （122 ページ）を参照してください。

（注） ポータルの作成時に認証タイプを構成していない場合は、[Portals] ウィンドウでそのポータルの [Edit Portal] ボタンを使用していつでも指定できます。

ポータルでのパスワード検証付き SMS の設定

ポータルを「パスワード検証付き SMS」に設定するには、次の手順を実行します。

ステップ 1 ポータルを作成するときに、[Authentication Type] ドロップダウンリストから [SMS with password verification] を選択します。

ステップ 2 このポータルでのインライン認証を設定し、ポータルホームページにユーザーの同意を表示する場合は、[Display Authentication and User Agreements on portal home page] チェックボックスをオンにします。インライン認証の詳細については、インライン認証 （121 ページ）を参照してください。

ステップ 3 通知を受け取るかどうか選択するオプションを顧客に提供する場合は、[Allow users to Opt in to receive message] チェックボックスをオンにします。

ステップ 4 [Allow users to Opt in to receive message] チェックボックスがオンになっている場合、次のフィールドが表示されます。

- [Opt in Message]：オプトインメッセージを入力します。
- [Default Opt-In Check Box Behavior]
  - [Checked]：顧客獲得時に [**Opt In**] チェックボックスがデフォルトでオンの状態で表示されるようにする場合は、このオプションをクリックしま
  - [Unchecked]：顧客獲得時に [**Opt In**] チェックボックスがデフォルトでオフの状態で表示されるようにする場合は、このオプションをクリックします。

ステップ 5 [Password Type] で必要なオプションをクリックします。

- [Auto Generated password}：認証要求ごとに、パスワードを自動的に生成します。自動生成されたパスワードが顧客に送信されます。
- [Fixed Password]：認証用のパスワードを定義します。このパスワードは、すべての顧客に対して、認証要求があるたびに送信されます。[Fixed Password] オプションをクリックすると表示される [Password] フィールドに、顧客に送信するパスワードを入力します。

ステップ 6 [SMS field] フィールドに、ユーザーに送信する SMS に表示されるテキストを入力します。

（注） 顧客がキャプティブ ポータルにアクセスできるリンクを表示する際は、テキストメッセージを編集する際に「{Link}」が削除されていないことを確認します。同様に、メッセージ内にパスワードを表示する際は、「{Password}」が削除されていないことを確認します。

ステップ 7 [Default Country] ドロップダウンリストから、この設定が適用される国を選択します。

ステップ 8 [SMS Gateway] ドロップダウンリストから、SMS ゲートウェイを選択します。

[Settings] オプションで設定された SMS ゲートウェイが選択可能になっています。シスコが提供する有料の [Demo Gateway] も使用できます。

（注） [SMS Gateway] ウィンドウが表示され、必要な SMS ゲートウェイ を設定できます。SMS ゲートウェイを設定するときの詳細については、Cisco DNA Spaces での SMS ゲートウェイの設定 （168 ページ）を参照してください。

ステップ 9 変更内容を保存します。

次のタスク

（注） 認証タイプが [SMS with password verification] のポータルには、[SMS Authentication] という名前の認証モジュールがあります。この認証モジュールの詳細については、認証モジュール （122 ページ）を参照してください。

（注） ポータルの作成時に認証タイプを構成していない場合は、[Portals] ウィンドウでそのポータルの [Edit Portal] ボタンを使用していつでも指定できます。

Social Sign In 認証のためのポータル設定

Cisco DNA Spaces は、次のソーシャルネットワークを介した認証をサポートしています。

- Facebook
- Twitter
- LinkedIn
- Instagram

（注）
- 現在、Instagram 認証はダッシュボードでサポートされません。Instagram 認証の設定に関する詳細については、Instagram の認証の設定 （118 ページ）を参照してください。
- ソーシャルネットワークを介してインターネットへのアクセスを認証するには、Cisco DNA Spaces でそのソーシャルネットワークのアプリケーションを設定する必要があります。[Settings] オプションを使用して、Cisco DNA Spaces でソーシャルアプリケーションを設定できます。詳細については、ソーシャル認証のためのソーシャルアプリケーションの追加（167 ページ）を参照してください。

ポータルへのアクセスを Social Sign In で認証するには、次の手順を実行します。

ステップ 1 ポータルを作成する際、[Authentication Type] ドロップダウンリストから [Social Sign In] を選択します。

Cisco DNA Spaces での認証用にサポートされているソーシャルネットワークが、設定済みのソーシャルアプリケーションと一緒に表示されます。

ステップ 2 このポータルでのインライン認証を設定し、ポータルホームページにユーザー契約を表示する場合は、[Display Authentication and Users Agreements on portal home page] チェックボックスをオンにします。インライン認証の詳細については、インライン認証 （121 ページ）を参照してください。

ステップ 3 インターネットへのアクセスの認証に使用するソーシャルネットワークの隣にあるチェックボックスをオンにします。

[Settings] セクションの [Social Apps] オプションで設定されたソーシャルネットワークを選択できます。ソーシャルアプリケーションの設定の詳細については、ソーシャル認証のためのソーシャルアプリケーションの追加 （167 ページ）を参照してください。

ステップ 4 変更内容を保存します。

次のタスク

（注） 認証タイプが [Social Sign In] のポータルには、[Social Authentication] という名前の認証モジュールがあります。この認証モジュールの詳細については、認証モジュール （122 ページ）を参照してください。

（注） [+Add] ボタンをクリックすると [Social Apps] ウィンドウが表示されます。このウィンドウで、カスタマイズされたアプリケーションを設定できます。

（注） ポータルの作成時に認証タイプを設定していない場合は、[Portals] ウィンドウでそのポータルの [Edit Portal] ボタンを使用していつでも指定できます。

Instagram の認証の設定

Cisco DNA Spaces を使用すると、Instagram のログイン情報を介して、キャプティブポータルにインターネット認証を提供できます。現在、Cisco DNA Spaces ダッシュボードには、キャプティブポータルで Instagram 認証を設定するプロビジョニングがありません。そのため、Instagram アプリを作成した後、Instagram 認証用のキャプティブポータルを設定するために Cisco DNA Spaces サポートチームに連絡する必要があります。

（注） Facebook デベロッパーアカウントが必要です。

ポータルの Instagram 認証を設定するには、次の手順を実行します。

ステップ 1 developers.facebook.com に移動します。

ステップ 2 **[Products]** > **[Add Instagram]** > **[Setup]** > **[Basic Display]** を選択します。

ステップ 3 [Create New App] をクリックします。

ステップ 4 [Display name] として Facebook アカウント名を入力し、[Valid OAuth Redirect URIs] フィールドで有効な Web サイトの URL を設定します。EU リージョンの例：**https://splash.dnaspaces.eu/p/instagram_auth**、米国およびその他のリージョンの例：**https://splash.dnaspaces.io/p/instagram_auth**。

[Products] > **[Instagram]**の [Basic Display] ウィンドウで、Instagram のアプリ ID と秘密鍵を表示できるようになりました。

ステップ 5 Facebook アプリが開発モードのときに、Facebook アプリから Instagram アプリにアクセスするようにできます。そのためには、次の手順を実行します。

これは、すでにアクティブ化された Instagram アプリには適用されません。

a) Facebook デベロッパーアプリで、**[Roles]** > **[Roles]**を選択します。
b) 表示されるウィンドウで、[Instagram Testers] セクションまで下にスクロールします。
c) [Add Instagram Testers] をクリックします。
d) Instagram アカウントのユーザー名を入力し、招待状を送信します。
e) 新しい Web ブラウザを開き、www.instagram.com にアクセスします。
f) 招待された Instagram アカウントにサインインします。
g) Instagram ホームページで、[Profile] アイコンをクリックします。
h) **[Edit Profile]** > **[Apps and Websites]** > **[Tester Invites]** を選択します。
i) 招待を承諾します。

または、手順 e から i まで、https://www.instagram.com/accounts/manage_access/ をクリックしてサインインし、[Tester Invites] タブで、招待に対して [Accept] をクリックします。

ステップ 6 Cisco DNA Spaces サポートチームに連絡し、ポータルで Instagram 認証を設定するための Instagram アプリ ID と秘密鍵を共有します。

Cisco DNA Spaces サポートチームは、バックエンドから必要な設定を行い、キャプティブポータルで Instagram ログイン情報を入力するためのテキストフィールドを作成します。

ステップ 7 ワイヤレスネットワークで、次の instagram ドメインを許可するように設定します。

- instagram.com
- *.instagram.com
- api.instagram.com
- d36xtkk24g8jdx.cloudfront.net
- www.facebook.com
- connect.facebook.net
- *.akamaihd.net

instagram 認証用のワイヤレスネットワークの設定の詳細については、ソーシャル認証に向けたワイヤレスネットワークの設定 （165 ページ） を参照してください。

Email 認証のためのポータルの設定

ポータルを Email 認証に設定するには、次の手順を実行します。

ステップ 1 ポータルを作成する際、[Authentication Type] ドロップダウンリストから [Email] を選択します。

ステップ 2 このポータルでのインライン認証を設定する場合は、[Display Authentication and User Agreements on portal home page] チェックボックスをオンにします。インライン認証の詳細については、インライン認証 （121 ページ）を参照してください。

ステップ 3 通知を受け取るかどうか選択するオプションを顧客に提供する場合は、[Allow users to Opt in to receive message] チェックボックスをオンにします。

ステップ 4 [Allow users to Opt in to receive message] チェックボックスがオンになっている場合、次のフィールドが表示されます。

- [Opt in Message]：オプトインメッセージを入力します。
- [Default Opt-In Check Box Behavior]
  - [Checked]：顧客獲得時に [Opt In] チェックボックスがデフォルトでオンの状態で表示されるようにする場合は、このオプションをクリックします。
  - [Unchecked]：顧客獲得時に [Opt In] チェックボックスがデフォルトでオフの状態で表示されるようにする場合は、このオプションをクリックします。

ステップ 5 変更内容を保存します。

次のタスク

（注） 認証タイプが [Email] のポータルには、[Email] という名前の認証モジュールがあります。この認証モジュールの詳細については、認証モジュール （122 ページ）を参照してください。

アクセスコード認証用ポータルの設定

アクセスコード認証用のポータルを設定するには、次の手順を実行します。

ステップ 1 ポータルを作成する際、[Authentication Type] ドロップダウンリストから [Access Code] を選択します。

ステップ 2 このポータルでのインライン認証を設定し、ポータルホームページにユーザー契約を表示する場合は、[Display Authentication and User Agreements on portal home page] チェックボックスをオンにします。インライン認証の詳細については、インライン認証 （121 ページ）を参照してください。

ステップ 3 通知を受け取るかどうか選択するオプションを顧客に提供する場合は、[Allow users to Opt in to receive message] チェックボックスをオンにします。

ステップ 4 [Allow users to Opt in to receive message] チェックボックスがオンになっている場合、次のフィールドが表示されます。

- [Opt in Message]：オプトインメッセージを入力します。
- [Default Opt-In Check Box Behavior]
  - [Checked]：顧客獲得時に [Opt In] チェックボックスがデフォルトでオンの状態で表示されるようにする場合は、このオプションをクリックします。
  - [Unchecked]：顧客獲得時に [Opt In] チェックボックスがデフォルトでオフの状態で表示されるようにする場合は、このオプションをクリックします。

ステップ 5 変更内容を保存します。

キャプティブポータルアプリの左ペインに表示される [Access Code] オプションを使用して、アクセスコードを作成し、顧客と共有することができます。アクセスコードの作成と共有の詳細については、アクセスコード （156 ページ）を参照してください。

次のタスク

（注） [Data Capture] または [User Agreements] が有効になっている場合の [Access Code] 認証タイプのポータル。この認証モジュールの詳細については、認証モジュール （122 ページ）を参照してください。

認証なしでのポータルの設定

ポータルを認証なしで設定するには、次の手順を実行します。

ステップ 1 ポータルを作成するときに、[Authentication Type] ドロップダウンリストから [No Authentication] を選択します。

ステップ 2 ポータルホームページにデータキャプチャとユーザーの同意を表示する場合は、[Display Data Capture and User Agreements on portal home page] チェックボックスをオンにします。

ステップ 3 通知を受け取るかどうか選択するオプションを顧客に提供する場合は、[Allow users to Opt in to receive message] チェックボックスをオンにします。

ステップ 4 [Allow users to Opt in to receive message] チェックボックスがオンになっている場合、次のフィールドが表示されます。

- [Opt in Message]：オプトインメッセージを入力します。
- [Default Opt-In Check Box Behavior]
  - [Checked]：顧客獲得時に [Opt In] チェックボックスがデフォルトでオンの状態で表示されるようにする場合は、このオプションをクリックします。
  - [Unchecked]：顧客獲得時に [Opt In] チェックボックスがデフォルトでオフの状態で表示されるようにする場合は、このオプションをクリックします。

ステップ 5 変更内容を保存します。

インライン認証

キャプティブポータルでは、認証を他のモジュールとともにインラインモジュールとして追加できます。つまり、顧客がキャプティブポータル内のリンクをクリックする前に認証オプションが表示されるため、認証プロセスを開始するために必要なクリック数が削減されます。

インライン認証を設定するには、[Authentication] 画面で、インライン認証を設定するためのチェックボックスをオンにします。

[SMS with Link verification] 認証タイプと [SMS with password verification] 認証タイプの場合、認証セクションには、携帯電話番号を入力するフィールドと [Connect] ボタンがあります。電子メール認証の場合、認証セクションには電子メールIDを入力するフィールドがあります。ソーシャル認証の場合、認証セクションには、ポータル用に設定されたソーシャルネットワークごとに関連するボタンがあり、顧客はこのボタンを使用してソーシャルネットワーク経由で認証を完了することができます。

認証モジュール

ポータルの認証タイプを選択すると、選択した認証タイプに基づいて、ポータルの認証モジュールが作成されます。

ポータルの認証タイプとして [No Authentication] または [Access Code] を選択したときに、[Data Capture] または [User Agreements] のいずれかが有効になっていない場合、そのポータルの認証モジュールは作成されません。

認証モジュールには、ポータルの代替ランディングページを指定するフィールドがあります。

ポータルへのデータキャプチャフォームの追加

ポータルで [Social Sign In] 以外の認証タイプを選択した場合、キャプティブポータルにデータキャプチャフォームを追加できます。ポータルの作成時に、データキャプチャフォームにフィールドを追加できます。顧客の名、姓、携帯電話番号などの詳細をキャプチャするように、フィールドを設定できます。顧客のフィルタリング基準となるビジネス タグの追加もできます。

（注） データキャプチャフォームで定義されたビジネスタグは、キャプティブポータルルール、エンゲージメントルール、プロファイルルールなどのルールで使用可能な [Add Tags] オプションで使用できます。

キャプティブポータルでデータキャプチャフォームを設定するには、次の手順を実行します。

ステップ 1 ポータルを作成する場合は、利用規約を指定した後、[Next] をクリックします。

データキャプチャの画面が表示されます。

ステップ 2 [Data Capture] チェックボックスを有効にします。

ステップ 3 [Add Field Element] をクリックします。

データキャプチャフォームには、次のフィールド要素を追加できます。

- [Title]：顧客の敬称を指定します。たとえば、Mr、Ms などです。このフィールドを設定すると、顧客獲得（ランタイム）中に、この Title、Mr および Ms が顧客のデータキャプチャフォームで選択できるようになります。

- [Email]：顧客の電子メール ID を指定します。
- [Mobile Number]：顧客の携帯電話の番号を指定します。携帯電話の番号のデフォルトの国を指定すると、顧客獲得の際にデフォルトの国のコードがデータ キャプチャ フォームに表示されるようにできます。
- [First Name]：顧客の名を指定します。
- [Last Name]：顧客の姓を指定します。
- [Gender]：顧客の性別を指定します。
- [Date of Birth]：顧客の生年月日を指定します。[Date of Birth] フィールドを追加すると、[User Agreements] ウィンドウの [Enable Age Gating] エリアで [Moderate] オプションを選択できなくなります。
- [Business Tags]：ビジネスタグ質問に対して顧客が選択する回答を提供します。このビジネスタグは、顧客の分類に役立ちます。
- **国固有のフィールド**
  - 郵便番号：住所の郵便番号を提供します。
  - CPF：CPF を提供します（これはブラジルにのみ適用されます）。

（注） [Email] フィールド要素は、**Email**認証の場合、電子メール情報は認証時にすでに収集されているため、使用できません。[Mobile Number] フィールド要素は、顧客が認証時に携帯電話番号を入力する必要があるため、**SMS with password verification** 認証では使用できません。

ステップ 4 対応するオプションをクリックして、フィールドを追加します。

一般のフィールド

- [Place Holder] フィールドには、フィールドのプレースホルダとして表示する必要があるテキストを入力します。
- フィールドを必須にするには、[Make this field mandatory] チェックボックスをオンにします。

要素固有のフィールド

- [Mobile Number] フィールド要素では、デフォルトの国を選択し、顧客獲得時にその国の国コードがデータキャプチャフォームに表示されるようにします。
- [Zip/Postal Code] フィールド要素では、[Country] ドロップダウンリストから国を選択します。これにより、顧客はデータキャプチャフォームで特定の国の郵便番号を追加できます。複数の国の郵便番号をサポートするには、[Add Country] をクリックして、別の国を追加します。
- [Business Tag] フィールド要素には、次の追加フィールドを設定する必要があります。
  - [Name] フィールドには、ビジネスタグの名前を入力します。
  - [Field Label] フィールドには、顧客に尋ねる質問を入力します。
  - [+Add Option] をクリックします。

- 表示されるフィールドに、顧客が選択するために提供する回答を入力します。
- その他の回答用選択肢も、同様に、[+ Add Option] を使用して追加します。

（注） 追加した選択肢を削除するには、対応する [Delete] アイコンを使用します。

（注） 顧客が認証プロセス中に [Data Capture] フォームにアクセスすると、指定した回答がドロップダウンリストで使用できるようになります。顧客は必要な値を選択できます。この値は、プロキシミティルールで顧客をフィルタリングするのに使用できます。

ステップ 5 変更内容を保存します。

（注） 顧客獲得時に、**データキャプチャ**フォームの [CPF] フィールドに入力された値は、「000.000.000-00」形式に変換されます。ユーザーが CPF の数値を入力すると、数値は自動的にフォーマットされます。したがって、キャプティブポータルのユーザーは、必要な形式を維持するためにドットやハイフンを手動で追加する必要はありません。

ポータルのブランド名の定義

Cisco DNA Spaces では、[Brand Name] モジュールを使用して、ポータルにブランド名を追加することができます。ブランド名は、テキストまたはイメージとして追加できます。たとえば、会社ロゴをブランド名として使用することができます。

ポータルのブランド名を定義するには、次の手順を実行します。

ステップ 1 ブランド名を定義するポータルを開きます。

ステップ 2 [Brand Name] モジュールをクリックします。

[Brand Name] ウィンドウが表示されます。

ステップ 3 ブランドのタイプを選択します。

a) [Text only] を選択する場合は、表示される [Brand Name] フィールドにブランド名を入力します。
b) [Logo] を選択する場合は、表示される [Upload] ボタンをクリックし、ロゴイメージをアップロードします。

ステップ 4 [Save] をクリックします。

ポータルにブランド名が定義されます。

次のタスク

（注） パブリッシュされているキャプティブポータルにすでに関連付けられているポータルを変更する場合、[Save & Publish] ボタンをクリックして、変更を速やかにパブリッシュします。[Save and Publish] ボタンは、ポータルがキャプティブポータルルールに関連付けられている場合のみ表示されます。キャプティブ ポータルルールを作成するときの詳細については、キャプティブポータルを表示するためのキャプティブポータルルールの作成（144 ページ）を参照してください。

ポータルへのウェルカム メッセージの追加

[Welcome] モジュールを使用すると、ポータルにウェルカム メッセージを追加することができます。追加されたウェルカムメッセージは、顧客がポータルにアクセスした際に表示されます。初回ユーザーとリピートユーザーに異なるウェルカムメッセージを表示するように設定できます。

ポータルにウェルカム メッセージを追加するには、次の手順を実行します。

ステップ 1 ウェルカム メッセージの追加が必要なポータルを開きます。

ステップ 2 [Welcome Message] モジュールをクリックします。

[Welcome Message] ウィンドウが表示されます。

ステップ 3 [First time visitor welcome text] フィールドで、顧客が初めてポータルにアクセスした際に表示する必要があるウェルカムメッセージを入力します。Smart Link 変数を使用して、ロケーションの詳細を含めることができます。Smart Link の詳細については、キャプティブポータルのスマートリンクとテキスト変数（190 ページ）を参照してください。

ステップ 4 リピートユーザーには別のウェルカムメッセージを表示する場合は、[Add a custom message for Repeat Visitors] チェックボックスがオンになっていることを確認し、その隣のテキストボックスに、再訪ユーザーのためのウェルカムメッセージを入力します。Smart Link 変数を使用して、名前とロケーションの詳細を含めることができます。変数「firstName」および「lastName」は、ポータルで [Data Capture] モジュールを [First Name] および [Last Name] フィールドを使用して構成した場合にのみ選択できます。変数「firstName」および「lastName」は、「Social Sign In」以外の認証タイプで使用できます。Smart Link の詳細については、キャプティブポータルのスマートリンクとテキスト変数（190 ページ）を参照してください。

ステップ 5 [Save] をクリックします。

ポータルにウェルカム メッセージが定義されます。

次のタスク

（注） パブリッシュされているキャプティブポータルにすでに関連付けられているポータルを変更する場合、[Save and Publish] ボタンをクリックして、変更を速やかにパブリッシュします。[Save and Publish] ボタンは、ポータルがキャプティブポータルルールに関連付けられている場合のみ表示されます。キャプティブポータルルールを作成するときの詳細については、キャプティブポータルを表示するためのキャプティブポータルルールの作成（144ページ）を参照してください。

ポータルへの通知の追加

[Notice] モジュールでは、ポータル内に通知を表示することができます。このモジュールは、顧客に重要な情報を伝える際に便利です。ティッカーおよびテキストの通知を追加できます。テキストの通知とともにイメージを追加することもできます。

通知をいつまでポータル内に表示するかの日付を設定できます。

ポータル内の通知をダッシュボードから追加するには、次の手順を実行します。

ステップ 1 通知を追加するポータルを開きます。

ステップ 2 [Notice] モジュールをクリックします。

[Notice] ウィンドウが表示されます。

ステップ 3 必要な通知の種類をクリックします。次のオプションを使用できます。

- [Ticker Text Only]：通知は、動くテキストの形式で表示されます。[Ticker Text Only] の場合、表示される [Notice] フィールドに通知のテキストを入力します。
- **[Text Only]**：通知は、テキスト形式で表示されます。[Text Only] の場合、表示される [Notice] フィールドに通知のテキストを入力します。
- [Text with Image]：通知は、アップロードされたイメージを伴うテキストとして表示されます。[Text with Image] の場合、以下の手順を実行します。
  - [Notice] フィールドに、通知のテキストを入力します。
  - [Notice image] エリアで、[Upload] ボタンをクリックし、通知と一緒に表示する必要があるイメージをアップロードします。

ステップ 4 [Hide After] フィールドで、通知をいつまでポータル内に表示するかの日付を選択します。

ステップ 5 [Save] をクリックします。

ポータルに通知が追加されます。

次のタスク

（注） パブリッシュされているキャプティブポータルにすでに関連付けられているポータルを変更する場合、[Save and Publish] ボタンをクリックして、変更を速やかにパブリッシュします。[Save and Publish] ボタンは、ポータルがキャプティブポータルルールに関連付けられている場合のみ表示されます。キャプティブポータルルール作成の詳細については、キャプティブポータルを表示するためのキャプティブポータルルールの作成 （144 ページ）を参照してください。

ポータルでの施設詳細の表示

[Venue Map] モジュールを使用すると、ポータル内に施設の詳細を表示することができます。このモジュールを使用すると、施設に対し、ラベル名の定義、アイコンイメージのアップロード、およびマップの表示をすることができます。

このモジュールのデフォルト名は、[Venue Map] です。モジュール名は、[Label] フィールドで加える変更に応じて変更されます。

ポータルに施設の詳細を追加するには、次の手順を実行します。

ステップ 1 施設の詳細を追加するポータルを開きます。

ステップ 2 [Venue Map] モジュールをクリックします。

[VENUE MAP] ウィンドウが表示されます。

ステップ 3 [Label] フィールドに、ポータルに表示される施設マップのラベル名を入力します。

（注） [Venue Map] モジュールの名前が、[Label] フィールドで指定した名前に変更されます。

ステップ 4 [Icon] 領域で、マップラベルの隣に表示されるマップアイコンを、[Upload] ボタンを使用してアップロードします。

（注） アイコンを削除するには、[Delete] アイコンを使用します。

ステップ 5 [Store Map] 領域に、この施設のマップが、ワイヤレスネットワークと同様に表示されます。

（注） マップは、ワイヤレスネットワーク（CUWN、Meraki）でマップが定義されているロケーションにポータルが関連付けられている場合のみ、表示されます。顧客が現在いるロケーションのマップが表示されます。

ステップ 6 [Save] をクリックします。

ポータルに施設マップが設定されます。

次のタスク

（注） パブリッシュされているキャプティブポータルにすでに関連付けられているポータルを変更する場合、[Save and Publish] ボタンをクリックして、変更を速やかにパブリッシュします。[Save and Publish] ボタンは、ポータルがキャプティブポータルルールに関連付けられている場合のみ表示されます。キャプティブポータルルールを作成するときの詳細については、キャプティブポータルを表示するためのキャプティブポータルルールの作成（144ページ）を参照してください。

ポータルへのビデオのアップロード

[Videos] モジュールを使用して、 Cisco DNA Spaces のポータルにビデオをアップロードできます。このモジュールでは、ポータル内のビデオが表示される領域にラベルとイメージを追加することと、ビデオの YouTube URL を指定することができます。

このモジュールのデフォルト名は、[Videos] です。モジュール名は、[Label] フィールドで加える変更に応じて変更されます。

（注） ポータルに表示できるのは、YouTube のビデオのみです。

ポータルにビデオをアップロードするには、次の手順を実行します。

ステップ 1 ビデオをアップロードするポータルを開きます。

ステップ 2 [Videos] モジュールをクリックします。

[VIDEOS] ウィンドウが表示されます。

ステップ 3 [Label] フィールドに、ポータル内のビデオが表示される領域のために表示が必要なラベルを入力します。

（注） [Videos] モジュールの名前が、[Label] フィールドで指定した名前に変更されます。

ステップ 4 [Icon] 領域で、ビデオラベルの隣に表示が必要なビデオアイコンを、[Upload] ボタンを使用してアップロードします。

（注） アイコンを削除するには、[Delete] アイコンを使用します。

ステップ 5 [Add a Video] をクリックします。

ステップ 6 表示される [YouTube URL] フィールドに、ポータルに表示するビデオの YouTube URL を入力します。

ステップ 7 [Save] をクリックします。

ポータルにビデオがアップロードされます。

次のタスク

（注） パブリッシュされているキャプティブポータルにすでに関連付けられているポータルを変更する場合、[Save and Publish] ボタンをクリックして、変更を速やかにパブリッシュします。[Save and Publish] ボタンは、ポータルがキャプティブポータルルールに関連付けられている場合のみ表示されます。キャプティブ ポータルルールを作成するときの詳細については、キャプティブポータルを表示するためのキャプティブポータルルールの作成（144 ページ）を参照してください。

ポータルでの [Feedback] セクションの提供

Cisco DNA Spaces の [Feedback] モジュールを使用すると、ポータルの顧客からフィードバックを収集することができます。このモジュールでは、[Feedback] セクションに複数の質問を追加することができます。これらの質問には、選択肢による回答または評価による回答を付加できます。顧客がコメントを追加できるテキストボックスを提供することもできます。

ポータルに [Feedback] セクションを追加するには、次の手順を実行します。

ステップ 1 フィードバックセクションを追加する必要があるポータルを開きます。

ステップ 2 [Feedback] モジュールをクリックします。

[FEEDBACK] ウィンドウが表示されます。

ステップ 3 [Label] フィールドに、[Feedback] セクションに表示する必要がある名前を入力します。

ステップ 4 [Icon] エリアで、フィードバックラベルの隣に表示する必要があるアイコンイメージを、[Upload] ボタンを使用してアップロードします。

ステップ 5 [Question] フィールドに、顧客に回答してほしい質問を入力します。

ステップ 6 [Image] エリアで、質問の隣に表示する必要があるイメージを、[Upload] ボタンを使用してアップロードします。

ステップ 7 [Question Type] エリアで、次のいずれかを選択します。

- [Rating]：顧客は、評価で質問に回答できます。
- [Multiple Choice]：顧客は、提供される複数の選択肢から回答できます。このオプションを選択した場合、[Option 1] および [Option 2] フィールドに回答の選択肢を入力します。提供する選択肢の数を増やす場合は、[Add option] ボタンを使って選択肢を追加します。

（注） [feedback] セクションに質問を追加するには、[Add question] ボタンを使用します。

ステップ 8 [Submit Button Label] フィールドに、顧客が回答の提出に使用する送信ボタンの名前を入力します。

ステップ 9 [Thank You/Success message] フィールドに、顧客が回答を提出した後に顧客に表示されるメッセージを入力します。

ステップ 10 [Post Submission button label] フィールドに、顧客の回答が提出された後に表示されるボタンの名前を入力します。顧客がこのボタンをクリックすると、Cisco DNA Spaces ダッシュボードが表示されます。

ステップ 11 顧客がコメントを入力するためのテキストボックスを提供するには、[Add a text box for additional comments from end user?] チェックボックスをオンにします。

ステップ 12 [Email to] フィールドに、フィードバックを送信する宛先の電子メールアドレスを入力します。

ステップ 13 [Email from] フィールドに、フィードバックメールの受信者に表示する [From] 電子メール アドレスを入力します。

ステップ 14 [Email Subject] フィールドに、フィードバックを含む電子メールの件名を入力します。

ステップ 15 [Save] をクリックします。

ポータルに [Feedback] セクションが作成されます。

次のタスク

（注） パブリッシュされているキャプティブポータルにすでに関連付けられているポータルを変更する場合、[Save and Publish] ボタンをクリックして、変更を速やかにパブリッシュします。[Save and Publish] ボタンは、ポータルがキャプティブポータルルールに関連付けられている場合のみ表示されます。キャプティブ ポータル ルールを作成するときの詳細については、キャプティブポータルを表示するためのキャプティブポータルルールの作成（144 ページ）を参照してください。

ポータルへのヘルプ オプションの追加

[Help] モジュールを使用すると、Cisco DNA Spaces のポータルにヘルプラインを追加することができます。顧客は、サポートが必要な際に、このヘルプラインを使用して連絡することができます。このモジュールでは、ポータル内のヘルプラインが表示される領域にラベルとイメージを追加することと、顧客がサポートが必要な際に連絡する番号を指定することができます。

このモジュールのデフォルト名は、[Help] です。モジュール名は、[Label] フィールドで加える変更に応じて変更されます。

ポータルにヘルプ オプションを追加するには、次の手順を実行します。

ステップ 1 ヘルプ オプションの追加が必要なポータルを開きます。

ステップ 2 [Help] モジュールをクリックします。

[HELP] ウィンドウが表示されます。

ステップ 3 [Label] フィールドに、ポータル内のヘルプラインが表示される領域に表示されるラベルを入力します。

（注） [Help] モジュールの名前が、[Label] フィールドで指定した名前に変更されます。

ステップ 4 [Icon] 領域で、ヘルプラベルの隣に表示されるヘルプアイコンを、[Upload] ボタンを使用してアップロードします。

（注） アイコンを削除するには、[Delete] アイコンを使用します。

ステップ 5 [Contact] フィールドに、ヘルプラインの番号を入力します。

ステップ 6 **Save** をクリックします。

ポータルにヘルプ オプションが定義されます。

次のタスク

（注） パブリッシュされているキャプティブポータルにすでに関連付けられているポータルを変更する場合、[Save and Publish] ボタンをクリックして、変更を速やかにパブリッシュします。[Save and Publish] ボタンは、ポータルがキャプティブポータルルールに関連付けられている場合のみ表示されます。キャプティブ ポータル ルールを作成するときの詳細については、キャプティブポータルを表示するためのキャプティブポータルルールの作成（144 ページ）を参照してください。

ポータルへのアプリケーションの追加

アプリケーションモジュールを使用すると、Cisco DNA Spaces ポータルにアプリケーションを追加することができます。アプリケーションは、iOS アプリストアと Play Store の両方から追加できます。このモジュールでは、ポータル内のアプリケーションが表示される領域にラベルとイメージを追加することができます。

このモジュールのデフォルト名は、[Get Apps] です。モジュール名は、[**Button Label**] フィールドで加える変更に応じて変更されます。

ポータルにアプリケーションを追加するには、次の手順を実行します。

ステップ 1 アプリケーションの追加が必要なポータルを開きます。

ステップ 2 [Get Apps] モジュールをクリックします。

[GET APPS] ウィンドウが表示されます。

ステップ 3 [Label] フィールドに、ポータル内のアプリケーションが表示される領域に表示されるラベルを入力します。

（注） [Get Apps] モジュール名が、[Label] フィールドで指定した名前に変更されます。

ステップ 4 [**Icon**] 領域で、アプリケーションラベルの隣に表示が必要なアプリケーションアイコンを、[**Upload**] ボタンを使用してアップロードします。

（注） アイコンを削除するには、[Delete] アイコンを使用します。

ステップ 5 [Add an App] をクリックします。

ステップ 6 [Add App] 領域で、次の手順を実行します。

a) [Platform] ドロップダウンリストから、アプリケーション プラットフォームを選択します。

b) [App Store URL] フィールドに、そこからアプリケーションを追加するアプリケーションストアの URL を入力します。

c) [App URL Scheme] フィールドに、デバイスにアプリケーションをインストールする際に受け取るアプリケーションの URL スキームを入力します。

d) デスクトップおよびラップトップに別の URL を提供する場合は、[Show this URL for Desktops and Laptops] チェックボックスをオンにします。

e) [Show this URL for Desktops and Laptops] チェックボックスをオンにしたら、デスクトップおよびラップトップのための URL を入力します。

（注） アプリケーションをさらに追加するには、[Add an App] ボタンを使用します。

ステップ 7 [Save] をクリックします。

ポータルにアプリケーションが追加されます。

次のタスク

（注） パブリッシュされているキャプティブポータルにすでに関連付けられているポータルを変更する場合、[Save and Publish] ボタンをクリックして、変更を速やかにパブリッシュします。[Save and Publish] ボタンは、ポータルがキャプティブポータルルールに関連付けられている場合のみ表示されます。キャプティブ ポータル ルールを作成するときの詳細については、キャプティブポータルを表示するためのキャプティブポータルルールの作成（144 ページ）を参照してください。

ポータルからのインターネットへのアクセスの提供

[Get Internet] モジュールを使用すると、ポータルからインターネットへのアクセスを提供することができます。[Get Internet] モジュールを使用すると、外部 URL をポータルに追加することができます。このモジュールでは、ポータル内のインターネット リンクが表示される領域にラベルとイメージを追加することができます。

このモジュールのデフォルト名は、[Get Internet] です。モジュール名は、[Button Label] フィールドで加える変更に応じて変更されます。

（注） キャプティブポータルにインライン認証が設定されている場合、[Get Internet] モジュールは、設定されていても、顧客の獲得中に表示されません。インライン認証の詳細については、インライン認証 （121 ページ）を参照してください。

ポータルからインターネットへのアクセスを提供するには、次の手順を実行します。

ステップ 1 インターネットへのリンクの提供が必要なポータルを開きます。

ステップ 2 [Get Internet] モジュールをクリックします。

[GET INTERNET] ウィンドウが表示されます。

ステップ 3 [Label] フィールドに、ポータル内のインターネットリンクが表示されるエリアに表示されるラベルを入力します。

（注） [Get Internet] モジュールの名前が、[Label] フィールドで指定した名前に変更されます。

ステップ 4 インターネットリンクの隣に表示が必要なアイコンを、[Upload] ボタンを使用してアップロードします。

（注） [Delete] アイコンを使用して、画像を削除できます。

ステップ 5 ランディングページを変更するには、[Change Landing page URL] チェックボックスがオンになっていることを確認します。

ステップ 6 [Launch Page] フィールドに、ポータルからインターネットに接続するための URL を入力します。

ステップ 7 [Save] をクリックします。

ポータルにインターネットにアクセスするためのオプションが設定されます。

次のタスク

（注） パブリッシュされているキャプティブポータルにすでに関連付けられているポータルを変更する場合、[Save and Publish] ボタンをクリックして、変更を速やかにパブリッシュします。[Save and Publish] ボタンは、ポータルがキャプティブポータルルールに関連付けられている場合のみ表示されます。キャプティブポータルルールを作成するときの詳細については、キャプティブポータルを表示するためのキャプティブポータルルールの作成（144 ページ）を参照してください。

ポータルへのプロモーションとオファーの追加

[Promos & Offers] モジュールでは、顧客に提供するプロモーションおよびオファーをポータルに追加することができます。さまざまなプロモーション URL にリンクできるさまざまなプロモーションアイテムをポータルに追加できます。このモジュールでは、各プロモーションにラベル、アイコン、および Web URL を追加することができます。

（注） プロモーションは回転式で表示されます。

ポータルにプロモーションとオファーを追加するには、次の手順を実行します。

ステップ 1 [Promos & Offers] モジュールを追加するポータルを開きます。

ステップ 2 [Promos & Offers] モジュールをクリックします。

[Promos & Offers] ウィンドウが表示されます。

ステップ 3 [Label] フィールドに、プロモーションとオファーが表示されるエリアに表示されるラベルを入力します。

ステップ 4 [Add a Promotion] をクリックします。

ステップ 5 [Promo Name] フィールドに、プロモーションリンクの名前を入力します。

ステップ 6 [Promo Image] エリアで、プロモーションリンクの隣に表示する必要があるアイコンを、[Upload] ボタンを使用してアップロードします。

ステップ 7 [Link Promo to URL] フィールドに、プロモーション Web ページにリンクする URL を入力します。

ステップ 8 [Save] をクリックします。

ポータルにプロモーションおよびオファーが追加されます。

次のタスク

（注） [Add a Promotion] ボタンを使用すると、ポータルに複数のプロモーションを追加できます。

（注） パブリッシュされているキャプティブポータルにすでに関連付けられているポータルを変更する場合、[Save and Publish] ボタンをクリックして、変更を速やかにパブリッシュします。[Save and Publish] ボタンは、ポータルがキャプティブポータルルールに関連付けられている場合のみ表示されます。キャプティブポータルルールを作成するときの詳細については、キャプティブポータルを表示するためのキャプティブポータルルールの作成（144 ページ）を参照してください。

ポータルからのプロモーションおよびオファーの削除

Cisco DNA Spaces では、必要な期間の後、ポータルからプロモーションを削除することができます。

ポータルからプロモーションを削除するには、次の手順を実行します。

ステップ 1 プロモーションを削除するポータルを開きます。

ステップ 2 [Promos & Offers] モジュールをクリックします。

[PROMOS and OFFERS] ウィンドウが表示され、そのポータルに追加されているプロモーションが示されます。

ステップ 3 削除するプロモーションの右上に表示されている [Delete] アイコンをクリックします。

カスタムのコンテンツとメニューアイテムのポータルへの追加

[Add Module] モジュールでは、要件に応じてポータルにカスタムのコンテンツやメニューアイテムを追加することができます。さまざまな Web ページにリンクできるさまざまなメニューアイテムをポータルに追加できます。このモジュールでは、各メニューアイテムにラベル、アイコン、および Web URL を追加することができます。リンク先の Web ページに互換性がある場合、「戻る」ボタンを有効にすることもできます。

カスタマイズしたメニューアイテムをポータルに追加するには、次の手順を実行します。

ステップ 1 カスタム メニュー アイテムの追加が必要なポータルを開きます。

ステップ 2 [Add Module] をクリックします。

ステップ 3 次のいずれかを選択します。

- [Custom Content]：カスタマイズした追加テキストをポータルに含めます。
- [Menu Item]：Web ページにリンクするメニューアイテムをポータルに含めます。

カスタムモジュールがポータルモジュールリストに追加され、そのページが開きます。カスタムモジュールに表示されるフィールドは、カスタムモジュールのタイプによって異なります。

ステップ 4 [Custom Content] の場合、カスタムモジュールに関する以下の詳細を入力します。

- [HTML Module Name] フィールドに、モジュールの名前を入力します。
- [Rich] フィールドにコンテンツを追加します。

ステップ 5 [Menu Item] フィールドの場合、カスタムモジュールの次の詳細を入力します。

a) [Label] フィールドに、カスタムメニューアイテムに表示されるラベルを入力します。

（注） [Menu Item] モジュールの名前が、[Label] フィールドで指定した名前に変更されます。

b) [Icon] 領域で、メニュー アイテムの隣に表示が必要なアイコンを、[Upload] ボタンを使用してアップロードします。

（注） アイコンを削除するには、[Delete] アイコンを使用します。

c) [Link to URL] フィールドに、メニューアイテムのリンク先 URL を入力します。

（注） Smart Link オプションを使用すると、URL を強化することができます。[Add Variable] ドロップダウンリストをクリックして追加できる変数を表示します。スマートリンクの作成についての詳細は、キャプティブポータルのスマートリンクとテキスト変数（190ページ）を参照してください。

ステップ 6 リンク先 Web ページの「戻る」ボタンを有効にするには、[Enable Back button] チェックボックスをオンにします。

ステップ 7 [保存（**Save**）] をクリックします。

カスタマイズされたコンテンツまたはメニューアイテムがポータルに正常に追加されます。

次のタスク

（注） 追加されたメニューアイテムは、ポータルのプレビューではテキストとして表示されますが、実行時にはリンクとして表示されます。

（注） パブリッシュされているキャプティブポータルにすでに関連付けられているポータルを変更する場合、[Save and Publish] ボタンをクリックして、変更を速やかにパブリッシュします。[Save and Publish] ボタンは、ポータルがキャプティブポータルルールに関連付けられている場合のみ表示されます。キャプティブポータルルールの作成の詳細については、キャプティブポータルを表示するためのキャプティブポータルルールの作成（144 ページ）を参照してください。

ポータルのエクスポート

Cisco DNA Spaces では、各種ポータルモジュールを使用して作成したポータルをエクスポートすることができます。

ポータルをエクスポートするには、次の手順を実行します。

ステップ 1 エクスポートするポータルを開きます。

ステップ 2 [Portal] ウィンドウの上部にある [Export Portal] アイコンをクリックします。

[Export Portal] ダイアログボックスが表示されます。

ステップ 3 [Download] をクリックします。

ステップ 4 表示されるウィンドウで、次のいずれかを実行します。

a) エクスポートされたファイルを直接開くには、[Open] を選択します。

b) ポータルファイルをコンピュータに保存するには、[Save File] を選択します。

ポータルの zip ファイルがコンピュータの [ダウンロード] フォルダに保存されます。

（注） ポータルは、zip 形式でエクスポートされます。

ポータルのスタイル シートの編集

Cisco DNA Spaces の [Style Sheet Editor] オプションでは、ポータルのスタイルシートを更新することができます。これは、ポータルのフォント プロパティや外観を変更するのに役立ちます。

ポータルのスタイル シートを編集するには、次の手順を実行します。

ステップ 1 スタイル シートを編集するポータルを開きます。
ステップ 2 [Portal] ウィンドウの上部にある [Stylesheet Editor] をクリックします。
ステップ 3 [CSS Editor] タブで、スタイルシートに必要な変更を加えます。
ステップ 4 [Save] をクリックします。

次のタスク

スタイルシートを外部ソースからアップロードすることができます。たとえば、別のポータルのためにデザインされた CSS などです。

また、スタイルシートをダウンロードして必要な更新を行い、編集したスタイルシートをアップロードすることもできます。たとえば、CSS デザイナーにポータルの編集を依頼する場合、[Download CSS] ボタンを使用してスタイルシートをダウンロードすることができます。スタイルシートに必要な変更を加えた後、[Upload CSS] ボタンを使用して Cisco DNA Spaces にアップロードすることができます。

スタイル シートへのアセットの追加

ポータルの外観を強化するため、イメージやフォントなどのアセットをポータルの [Style Sheet Editor] に追加することができます。jpeg、png、tif などのイメージ ファイルが追加できます。スタイル シートを編集し、これらのアセットをポータルに組み込みます。

ポータルのスタイル シートにアセットを追加するには、次の手順を実行します。

ステップ 1 スタイル シートを編集するポータルを開きます。
ステップ 2 [Stylesheet Editor] をクリックします。
ステップ 3 [Asset Library] タブをクリックします。
ステップ 4 アセットファイルをドラッグアンドドロップするか、[Choose File] ボタンを使用してアップロードします。

（注） キャプティブポータルのアセットライブラリに新しいアセットをアップロードする場合、添付ファイルごとにサポートされる最大ファイル サイズは 15 MB です。

ファイルがアセット リストに追加されます。

次のタスク

アセット下部のアセットで表示される [Copy Asset url] ボタンを使用して、アセットの URL をコピーすることができます。このアセットをポータルに追加するには、スタイルシートの適切な場所に URL を追加します。

アセットを削除するには、アセットリスト内のそのアセットに表示された [Delete] アイコンを使用します。

ポータルのインポート

Cisco DNA Spaces では、外部パスからポータルをインポートすることができます。たとえば、外部アプリケーションを使用してポータルを強化する場合、[Export Portal] アイコンを使用してポータルをエクスポートし、必要な強化を加え、[Import Portal] オプションを使用してポータルファイルを Cisco DNA Spaces にインポートすることができます。

ポータルをインポートするには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Home] を選択します。

ステップ 2 表示されるウィンドウで、[Captive Portal] をクリックします。

ステップ 3 [Captive Portal] ウィンドウで、左ペインの [Portal] を選択します。

[Captive Portal] ウィンドウが表示されます。

ステップ 4 ウィンドウの右上にある [Import Portal] をクリックします。

ステップ 5 表示される [Import Portal] ウィンドウで、次の手順を実行します。

a) [Portal Name] フィールドに、ポータルのファイル名を入力します。

b) ウィンドウにポータルをドラッグアンドドロップし、[Choose File] ボタンをクリックして、インポートするファイルを選択します。

c) このポータルをすべてのロケーションで使用できるようにする場合は、[Add all locations to this portal] チェックボックスがオンになっていることを確認します。選択したロケーションでのみポータルを使用できるようにする場合は、[Add all locations to this portal] チェックボックスをオフにして、ポータルを使用できるようにする必要があるロケーションを選択します。

ウィンドウの右側に選択したロケーションが表示されます。

ステップ 6 [Import] をクリックします。

次のタスク

（注） ポータルは、zip 形式でアップロードされます。

ポータルの削除

ポータルを削除するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Home] を選択します。

ステップ 2 表示されるウィンドウで、[Captive Portal] をクリックします。

ステップ 3 [Captive Portal] ウィンドウで、左ペインの [Portal] を選択します。

[Captive Portal] ウィンドウが表示され、Cisco DNA Spaces 内で使用可能なポータルのリストが表示されます。

ステップ 4 削除するポータルの右端に表示される [Delete] アイコンをクリックします。

ステップ 5 表示される [Delete Portals] ウィンドウで、[Yes] をクリックします。

ポータルが Cisco DNA Spaces から削除されます。

（注） 削除するポータルの隣のチェックボックスを複数選択し、ウィンドウの下部に表示される [Delete] ボタンをクリックすると、複数のポータルを同時に削除できます。

（注） キャプティブポータルルールに関連付けられているポータルは、削除できません。

ポータルの編集

ポータルを編集するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Home] を選択します。

ステップ 2 表示されるウィンドウで、[Captive Portal] をクリックします。

ステップ 3 [Captive Portal] ウィンドウで、左ペインの [Portal] を選択します。

[Captive Portal] ウィンドウが表示され、Cisco DNA Spaces 内で使用可能なポータルのリストが表示されます。

ステップ 4 編集するポータルの右端に表示される [Edit] アイコンをクリックします。

ステップ 5 必要な変更を行い、各モジュールに加えた変更を保存します。

ステップ 6 変更をパブリッシュするには、そのポータルの [Save and Publish] ボタンをクリックします。

ポータルのロケーションの編集

ポータルのロケーションを編集するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Home] を選択します。

ステップ 2 表示されるウィンドウで、[Captive Portal] をクリックします。

ステップ 3 [Captive Portal] ウィンドウで、左ペインの [Portal] を選択します。

ステップ 4 [Captive Portal] ウィンドウが表示されたら、ロケーションを編集するポータルのチェックボックスをオンにします。

ステップ 5 ウィンドウの下部に表示される [Add to Locations] をクリックします。

ステップ 6 表示される [Add Locations to Portals] ウィンドウで、ポータルのロケーションを選択し、[Save Changes] をクリックします。

ステップ 7 変更をパブリッシュするには、そのポータルの [Save and Publish] ボタンをクリックします。

ポータルプレビュー URL の電子メールでの送信

ポータルのプレビュー URL を電子メールで送信し、受信者がその URL を使用してポータルをプレビューできるようにすることが可能です。

ポータルのプレビュー URL を電子メールで送信するには、次の手順を実行します。

ステップ 1 プレビュー URL を電子メールで送信するポータルを開きます。

ポータルが表示されます。

ステップ 2 ウィンドウの右端にある [Portal Preview] エリアの [Link] アイコンをクリックします。

ステップ 3 [Email Portal URL] フィールドに、ポータルプレビュー URL を電子メールで送信する宛先電子メール ID を入力します。

ステップ 4 [Send] をクリックします。

URL が指定された電子メール アドレスに送信されたことを知らせるメッセージが表示されます。

QR コードを使用したポータルのプレビュー

Cisco DNA Spaces では、ポータルの QR コードを使用してポータルをプレビューできます。この機能を使用するには、使用するモバイルに QR コードリーダーアプリをインストールする必要があります。

ポータルの QR コードをスキャンするには、次の手順を実行します。

ステップ 1 QR コードをスキャンするポータルを開きます。

ステップ 2 ウィンドウの右端にある [Portal Preview] エリアの [Link] アイコンをクリックします。

ステップ 3 モバイル デバイスで QR コード リーダー アプリケーションを開きます。

ステップ 4 ポータルで、[Scan with QR code reader on your mobile device] というラベルのエリアに、モバイルデバイスでフォーカスします。

モバイル デバイスは QR コードをスキャンして、URL を開くかどうか質問するメッセージを表示します。

ステップ 5 [OK] をクリックします。

モバイル デバイスの画面にポータルが開きます。

ポータルのプレビュー

Cisco DNA Spaces では、キャプティブポータルの外観を表示することができます。Cisco DNA Spaces を使用すると、キャプティブポータルで各モジュールを個別にプレビューできます。デフォルトのプレビューは、キャプティブポータルのホーム画面です。認証モジュールのプレビューは、顧客獲得（ランタイム）フローをシミュレートします。モジュールのプレビューは回転式で表示されます。

キャプティブポータルをプレビューするには、次の手順を実行します。

ステップ 1 プレビューを表示するポータルを開きます。

ポータルのホーム画面のプレビューは、[Portal Preview] エリアに表示されます。

ステップ 2 右向き矢印をクリックし、次の画面に移動します。

さまざまなデバイスでのポータルのプレビュー

Cisco DNA Spaces では、さまざまなデバイスでキャプティブポータルの外観を表示することができます。モバイルデバイス、タブレット、およびラップトップでのポータルをプレビューすることができます。Cisco DNA Spaces を使用すると、キャプティブポータルで各モジュールを個別にプレビューできます。デフォルトのプレビューは、キャプティブポータルのホーム画面です。

デバイスのキャプティブポータルをプレビューするには、次の手順を実行します。

ステップ 1 さまざまなデバイスでプレビューを表示するポータルを開きます。

デバイスで表示されるポータルのホーム画面のプレビューは、ポータルの右側に表示されます。

CSS エディターウィンドウが表示され、右側のペインにデバイスのプレビューが表示されます。

ステップ 2 次のいずれかを実行します。

a) モバイルデバイスでのポータルのプレビューを表示するには、モバイルデバイスのタブをクリックします。
b) タブレットでのポータルのプレビューを表示するには、タブレットタブをクリックします。
c) ラップトップでのポータルのプレビューを表示するには、ラップトップのタブをクリックします。

選択したデバイスでのキャプティブ ポータル ホーム ページのプレビューが表示されます。

ステップ 3 キャプティブポータルで特定のモジュールをプレビューするには、隣にあるドロップダウンリストからモジュールを選択します。

（注） [Preview] ウィンドウでその他のデバイスでのプレビューを表示するには、対応するタブをクリックします。[Preview] ウィンドウでは、QR コードのスキャン、ポータルの URL の電子メールでの送信、および向きの変更もできます。

キャプティブポータル内のモジュールの表示、非表示、順序変更

ポータル管理者は、モジュールの左上にあるオン/オフのトグルスイッチを切り替えることで、ポータルに追加されたモジュールを表示または非表示にすることができます。モジュールを並び替えるには、必要な位置にモジュールをドラッグ アンド ドロップします。プレビュー セクションに変更が反映されます。

キャプティブポータルルール

キャプティブ ポータル ルールにより、キャプティブ ポータルの表示および SSID に接続している顧客のインターネット プロビジョニングを管理できます。

キャプティブ ポータル ルールを使用して、次の方法で、キャプティブ ポータルの表示およびインターネット プロビジョニングを管理できます。

- **キャプティブポータルの表示**：ルールに応じてフィルタリングされた顧客が、そのルールで設定された SSID に接続すると、キャプティブポータルが表示されます。必要な認証手順が完了したら、ポータルのメニュー項目をクリックしてインターネットにアクセスできます。顧客のロケーション、アクセス数、顧客が属するタグ、ロケーションへのアクセス数、アクセス期間などに基づき、顧客に合ったさまざまなキャプティブポータルを表示するように設定できます。セッションごとに、インターネットを提供する必要がある期間を制限することができます。また、このキャプティブポータルルールでインターネットに必要な帯域幅を定義できます。
- **直接インターネットアクセス**：ルールに応じてフィルタリングされた顧客が、ルールで設定された SSID に接続すると、認証プロセスなしで、インターネットが即座に提供されます。この場合、キャプティブ ポータルは表示されません。
- **インターネットアクセスの拒否**：ルールに応じてフィルタリングされた顧客が SSID に接続しようとすると、インターネットが拒否されて接続を確立できません。

また、キャプティブ ポータル ルールにより、次の操作を行うことができます。

- ルールのフィルタリングに基づいてタグを作成するか、または既存のタグを変更します。
- 外部 API へのキャプティブ ポータルにサインインする顧客の詳細を送信します。

キャプティブ ポータル ルールでは、定義された条件が満たされているときに実行するアクションを設定できます。ロケーション、タグ、顧客のアクセスの数や時間、アプリケーションのステータスなど、さまざまなパラメータに基づいて、ルールに応じて顧客をフィルタリングできます。

この章では、キャプティブ ポータル ルールを作成する方法について説明します。

キャプティブポータルルール作成の前提条件

- キャプティブポータルルールを適用可能なロケーションを指定するには、ロケーション階層を定義する必要があります。ロケーション階層の定義の詳細については、「ロケーション階層の概要」セクションを参照してください。
- [CMX On Prem] オプションの場合、必要なすべての AP が Cisco CMX に追加されていることを確認します。
- キャプティブポータルを表示する SSID を指定するには、ワイヤレス ネットワーク システムで作成された SSID を Cisco DNA Spaces にインポートする必要があります。SSID のインポートの詳細については、ワイヤレスネットワークからの SSID のインポート （154 ページ）を参照してください。
- キャプティブポータルルールに基づいてキャプティブポータルを表示するには、ポータルを作成する必要があります。キャプティブポータルの作成の詳細については、ポータルの作成と管理 （103 ページ）を参照してください。
- ルールを適用可能なタグを指定するには、タグを定義する必要があります。タグの作成の詳細については、「ロケーションペルソナアプリを使用したタグの作成または変更」のセクションを参照してください。
- キャプティブポータルにサインインした顧客の姓名などの詳細を外部 API に送信するには、キャプティブポータルでデータキャプチャフォームを設定する必要があります。Data Capture フォームがないと、デバイスの MAC アドレスなどの情報のみが外部 API に送信されます。データキャプチャフォーム設定の詳細については、ポータルへのデータキャプチャフォームの追加 （122 ページ）を参照してください。
- キャプティブポータルには RADIUS 認証を強くお勧めします。RADIUS 認証は、[Seamlessly Provision Internet]、[Deny Internet]、およびセッション期間と帯域幅の拡張に必須です。インターネット プロビジョニングと RADIUS 認証を管理するには、ワイヤレスネットワークで必要な設定を行います。
  - 使用するワイヤレスネットワークが Meraki の場合は、RADIUS 認証用の Cisco Meraki の設定 （301 ページ）で説明されている設定を行います。
  - 使用するワイヤレスネットワークが CUWN（Cisco AireOS）の場合は、インターネット プロビジョニングおよび RADIUS 認証のためのシスコ ワイヤレス コントローラの設定 （258 ページ）で説明されている設定を行います。

キャプティブポータルを表示するためのキャプティブポータルルールの作成

キャプティブポータルルールを作成する前に、すべての前提条件が満たされていることを確認してください。キャプティブポータルルールを作成するための前提条件については、キャプティブポータルルール作成の前提条件 （143 ページ）を参照してください。

顧客のロケーション、顧客がオプトインユーザーかどうか、顧客が属するタグ、初回ユーザーかリピートユーザーか、顧客のアクセス回数などに基づいて、ルールを適用する顧客をフィルタリングできます。ロケーションまたはそのロケーションに関連付けられているメタデータに基づいて、ルールが適用されるロケーションをフィルタリングできます。指定された時間内に指定したロケーションに顧客がアクセスした回数に基づいて、ルールを適用することもできます。また、特定の期間内の特定の時間だけ、および特定の曜日だけにルールを適用するように設定することもできます。

キャプティブ ポータル ルールにより、ルールに応じてフィルタリングされた顧客が SSID に接続する際に、直接インターネット接続を提供するように設定することもできます。この場合、キャプティブ ポータルは表示されませんが、顧客はインターネットへアクセスできるようになります。また、キャプティブポータルルールに応じてフィルタリングされた顧客にインターネットアクセスを拒否するようにも設定できます。

キャプティブ ポータル ルールを使用して、新しいタグを作成、またはルールに応じてフィルタリングされた顧客の既存のタグを変更できます。キャプティブポータルルールはまた、ルールで設定されている SSID に接続されている顧客の詳細を外部 API へ送信します。

（注） シスコ ワイヤレス コントローラが Cisco CMX を介して接続されている場合は、キャプティブポータルルールが機能するために必要なすべての AP が Cisco CMX に追加されていることを確認してください。ロケーション階層を定義した後、新しい AP を Cisco CMX に追加すると、新しく追加された AP はロケーション階層に自動的に表示されます。

ポータルを表示するキャプティブ ポータル ルールを作成するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、Captive Portal アプリをクリックします。

ステップ 2 表示される [Captive Portal] ウィンドウで、ダッシュボードの左ペインにある [Captive Portal Rule] をクリックします。

ステップ 3 ウィンドウの右端にある [Create New Rule] をクリックします。

ステップ 4 [Rule Name] フィールドに、キャプティブポータルルールの名前を入力します。

ステップ 5 [Sense] 領域で、次の手順を実行します。

a) [When a user is on WiFi] の後のドロップダウンリストから、[WiFi] を選択します。

b) [and connected to] の後のドロップダウンリストから、ルールを適用する SSID を選択します。

（注） SSIDは、SSIDをインポート/設定した場合にのみ選択することができます。必要なSSIDがインポート/設定されていない場合は、ドロップダウンリストに表示されている[Configure SSID]ボタンを使用してインポート/設定できます。[Configure SSID]ボタンを選択すると、[Import/Configure SSID]ウィンドウにリダイレクトされます。SSIDのインポート/設定の詳細については、ワイヤレスネットワークからのSSIDのインポート（154ページ）を参照してください。

ステップ6 [Location]領域で、ルールを適用するロケーションを指定します。

ロケーション階層全体、グループ、ロケーション、フロア、ゾーンなどの1つまたは複数のロケーションにルールを適用するように設定できます。キャプティブポータルルールにはMerakiとCUWNの両方のロケーションを追加できます。ロケーション階層の作成に関する詳細については、「ロケーション階層の定義」のセクションを参照してください。

選択したロケーション、またはその親や子のロケーションに定義されているメタデータに基づき、ロケーションを再度フィルタリングできます。ロケーションのメタデータ設定の詳細については、「ロケーションのメタデータの定義または編集」のセクションを参照してください。特定のメタデータのロケーションにルールを適用するか、または特定のメタデータのロケーションを除外することができます。ロケーションのフィルタリングの詳細については、ロケーションによるフィルタリング（171ページ）を参照してください。

ステップ7 [IDENTIFY]領域で、ルールを適用する顧客のタイプを指定します。

（注） 顧客のオンボーディングステータス、顧客がオプトインユーザーかどうか、顧客が属するタグ、顧客の訪問回数などに基づいてルールを適用する顧客をフィルタリングできます。これらのフィルタをすべて適用することも、要件に応じて一部を適用することもできます。

キャプティブポータルルールを適用する顧客を指定するには、次の手順を実行します。

a) 顧客のオンボーディングステータスに基づいて顧客をフィルタリングするには、[Filter by Onboarding Status]チェックボックスをオンにします。オンボーディング済みの顧客（認証プロセスを完了した顧客）をルールでフィルタリングする場合は、[Onboarded Visitor]ラジオボタンをクリックします。オンボーディング済みでない顧客（認証プロセスを完了していない顧客）をルールでフィルタリングする場合は、[Not Onboarded Visitor]ラジオボタンをクリックします。

b) オプトインステータスにより顧客をフィルタリングする場合、[Filter by Opt-In Status]チェックボックスをオンにして、オプトインユーザーまたは非オプトインユーザーのどちらをフィルタリングするかを指定します。オプトインユーザーの詳細については、ページ6～5の「ユーザーのオプトインオプション」を参照してください。

c) タグに基づいて顧客をフィルタリングするには、[Filter by Tags]チェックボックスをオンにします。

（注） 2つの異なる方法でタグをフィルタリングできます。ルールを適用する必要のあるタグを指定することも、ルールを適用しないタグを指定することもできます。要件に基づいて、最適なフィルタリング方法を選択できます。たとえば、1つのタグを除くすべてのタグの顧客にルールを適用する場合、除外オプションを選択し、ルールを適用しない特定のタグを指定する方法が簡単です。

- 選択したタグの顧客にルールが適用されるようにタグを含めるには、[Include]の[Add Tags]ボタンを使用します。

- 除外したタグの顧客にルールを適用しないようにするには、[Exclude] の [Add Tags] ボタンを使用します。

タグフィルタの使用の詳細については、「タグによるフィルタリング」を参照してください。

d) 選択したロケーションにおける顧客の訪問数に基づいて顧客をフィルタリングするには、[Filter by Previous Visits] チェックボックスをオンにします。

[Add Locations] ボタンをクリックします。[Choose Locations] ウィンドウで、顧客の訪問をフィルタリングの条件にする必要があるロケーションを指定します。次のフィールドで、フィルタリング対象のアクセス数と時間を指定します。自分で設定できる訪問回数と継続時間の詳細については、「以前の訪問の条件」のセクションを参照してください。

ステップ 8 [Schedule] 領域で、ルールを適用する期間を指定します。

a) [Set a date range for the rule] チェックボックスをオンにし、表示されるフィールドで、キャプティブポータルルールを適用する期間の開始日と終了日を指定します。

b) [Set a time range for the rule] チェックボックスをオンにし、表示されるフィールドに、キャプティブポータルルールを適用する時間範囲を指定します。

c) 特定の曜日にのみルールを適用する場合、[Filter by days of the week] チェックボックスをオンにし、表示される曜日のリストからルールを適用する曜日をクリックします。

ステップ 9 [Actions] 領域で、前述の条件が満たされたときに実行する操作を設定します。

a) ルールに応じてフィルタリングされた顧客のインターネットのプロビジョニングを管理するには、次から必要なオプションを選択してください。

- [Show Captive Portal]：キャプティブポータルルールに応じてフィルタリングされた顧客が、そのルールで設定された SSID に接続するとキャプティブポータルが表示されるようにするには、このオプションを選択します。[Select Captive Portal] ドロップダウンリストから、このルールで定義された条件を満たすときに表示するキャプティブポータルを選択します。

（注） 選択したロケーションに作成したポータルを選択することができます。必要なポータルを作成していない場合は、[Select Captive Portal] ドロップダウンリストにある [Create Portal] ボタンを使用して作成できます。[Create Portal] ボタンを選択すると、[Create Portal] ウィンドウにリダイレクトされます。ポータルの作成の詳細については、ポータルの作成（107 ページ）を参照してください。

- あるセッションに対してインターネットが提供される期間を制限する場合は、[Session Duration] チェックボックスをオンにして、表示されるフィールドにセッション期間を入力します。セッション期間は分、時間、または日数で指定できます。

- このキャプティブポータルルールに基づいて顧客に提供されるインターネットの帯域幅を制限する場合は、[Bandwidth] チェックボックスをオンにして、表示される帯域幅バーで帯域幅を指定します。帯域幅は、1 kbps から 1 tbps の範囲で定義できます。

（注） ここで定義されたセッション期間は、シスコ ワイヤレス コントローラや Meraki などのワイヤレスネットワークのセッション有効期限の設定を上書きします。そのため、このオプションを使用すると、ワイヤレスネットワークで設定されているものより長いセッション期間をキャプティブポータルで定義できます。

- [Seamlessly Provision Internet]：顧客が SSID に接続してすぐにインターネットを提供するには、このオプションを選択します。 この場合、顧客は認証の手順を実行する必要がありません。このオプションを使用するには、キャプティブポータルルール作成の前提条件 （143 ページ）で説明されているように、シスコ ワイヤレス コントローラや Meraki などのワイヤレスネットワークで特定の設定を行う必要があります。このオプションに入力するデータは、ワイヤレスネットワークによって異なります。
  - [Rule/Policy Name] フィールドに、ポリシーの名前を入力します。ワイヤレスネットワークで定義したものと同じ名前を指定する必要があります。

（注） このフィールドは、シスコ ワイヤレス コントローラまたは Cisco 9800 シリーズ ワイヤレス コントローラでは必須ではありません。

- セッション期間を指定するには、[Session Duration] チェックボックスをオンにして、[Enter Session Duration] フィールドに、接続ごとにインターネットアクセスを提供する期間を指定します。
- 帯域幅を指定するには、[Bandwidth the Limit] チェックボックスをオンにし、表示される帯域幅バーを使用して帯域幅を指定します。最大で 1 tbps の帯域幅を指定できます。

  [Show Manual Configuration] オプションを使用して、キャプティブポータルルールで許可される帯域幅を手動で入力することもできます。このオプションを使用すると、事前定義された値ではなく、設定したい正確な帯域幅を指定できます。帯域幅は、KBPS、MBPS、GBPS、または TBPS で指定できます。

（注） Meraki の場合、Cisco Meraki で設定された帯域幅が考慮されるため、帯域幅フィールドは必須ではありません。

- [Deny Internet]：顧客が SSID に接続しようとしたときに、ルールに応じてフィルタリングされた顧客に対してインターネットを拒否するには、このオプションを選択します。この場合、顧客は SSID への接続が許可されません。

b) このキャプティブ ポータル ルールに基づいてフィルタリングされた顧客にタグを作成する、または、フィルタリングされた顧客を既存のルールに追加または削除するには、[Add Tags] ボタンをクリックします。タグフィルタの使用の詳細については、「タグによるフィルタリング」セクションを参照してください。

c) このルール向けに設定されたキャプティブポータルにサインアップした顧客の名、姓、携帯電話番号などの詳細情報を外部 API に送信する場合は、[Trigger API] チェックボックスをオンにして、必要な API 設定を行います。API 設定の詳細については、「通知のためのトリガー API の設定」を参照してください。

（注） ルールの概要がウィンドウの右側に表示されます。

ステップ 10 [Save and Publish] をクリックします。

ルールがパブリッシュされ、[Captive Portal Rules] ウィンドウにリストされます。

（注） ルールを今すぐパブリッシュしたくない場合、[Save] ボタンをクリックします。ルールを開いて [Save and Publish] ボタンをクリックすることで、後でいつでもルールをパブリッシュできます。また、[Captive Portal Rules] ウィンドウの右側にある [Make Rule Live] アイコンをクリックして、ルールをパブリッシュすることもできます。

使用例：キャプティブポータルルール

XYZ は、モバイル ストアからスーパーマーケットまで、さまざまな事業のストリームラインに関わっているビジネス グループです。XYZ はニューヨークの各地に 5 軒のモバイルストアと 4 軒のスーパーマーケットを展開しています。ニューヨークの XYZ の SSID 名は XYZID です。XYZ は顧客が XYZ のスーパーマーケットから XYZID に接続すると、スーパーマーケットのさまざまな品目が利用可能なオファーを表示する、キャプティブ ポータル C1 を表示したいと考えています。同様に、キャプティブ ポータル C2 は、XYZ のモバイル ストアから XYZID に接続する顧客に表示される必要があります。キャプティブ ポータルは、オプトインではないユーザに表示される必要があります。

スーパー マーケットのロケーション：L1、L2、L3、L4、L5

モバイル ストアのロケーション：L7、L8、L9、L10

前述のシナリオを実現するには、次の手順を実行します。

ステップ 1 シスコ ワイヤレス コントローラで、アクセスポイントのモードを定義し、ACL を作成し、SSID「XYZID」を作成します。シスコ ワイヤレス コントローラの設定に関する詳細については、Cisco Meraki 用の SSID のインポート （155 ページ）を参照してください。

ステップ 2 Cisco DNA Spaces にログインします。

ステップ 3 [Import SSID] オプションを使用して、Cisco DNA Spaces に XYZID を追加します。

ステップ 4 XYZ のロケーション階層を作成します。ロケーション階層では、ニューヨークの XYZ のすべてのスーパーマーケットとモバイルストアが、ロケーション [New York] に属するロケーションとして定義される必要があります。ロケーション L1、L2、L3、L4、L5 のロケーションメタデータとしてキー [StoreType]、値 [SM] を追加します。ロケーション L7、L8、L9、L10 のロケーションメタデータとしてキー [StoreType]、値 [MS] を追加します。ロケーションメタデータの定義の詳細については、「ロケーションのメタデータの定義または編集」のセクションを参照してください。

ステップ 5 スーパーマーケットのポータル **C1** と、モバイルストアのポータル **C2** を作成します。ポータルの作成の詳細については、ポータルの作成 （107 ページ）を参照してください。

ステップ 6 Cisco DNA Spaces ダッシュボードで、[Home] を選択します。

ステップ 7 表示されるウィンドウで、[Captive Portal] を選択します。

ステップ 8 [Captive Portal] ウィンドウで、左ペインの [Captive Portal Rule] を選択します。

ステップ 9 [Create New Rule] をクリックします。

ステップ 10 [RULE NAME] フィールドに、キャプティブポータルルールの名前「**R1**」を入力します。

ステップ 11 [When a user is on] ドロップダウンリストから [Wi-Fi] を、[add Connected to] ドロップダウンリストから [XYZID] を選択します。

ステップ 12 [Locations] 領域で、次の手順を実行します。

a) [Add Locations] ボタンをクリックし、表示される [Choose Locations] ウィンドウで、ニューヨークのロケーションを選択し、[OK] をクリックします。

b) [Filter by metadata] チェックボックスをオンにし、フィルタの [Add Metadata] ボタンをクリックします。

c) [Choose Location Metadata] ウィンドウで、キー [StoreType] を選択し、値 [SM] を選択します。

（注） ロケーションメタデータ [StoreType] は、ロケーション [New York] に属するロケーションに対して定義されているため、[Choose Location Metadata] ウィンドウで選択することができます。

ステップ 13 [Identify] エリアで、[Filter by Opt-In Status] チェックボックスをオンにし、[Only for not opted-in Visitor] を選択します。

ステップ 14 [Schedule] エリアで、[Set a date range for the rule] チェックボックスをオンにし、開始日に現在の日付を、終了日に今年の最終日を指定します。

ステップ 15 [Actions] エリアで、[Show Captive Portal] を選択し、[Select Captive Portal] ドロップダウンリストから [C1] を選択します。

ステップ 16 [Save and Publish] をクリックします。

ルールがパブリッシュされます。

ステップ 17 同様に、ロケーション メタデータ キーが [StoreType]、値が [MS]、キャプティブ ポータルが [C2] の、別のルール **R2** を、モバイル グループ用に作成します。

これで、顧客が XYZ のスーパーマーケットにアクセスして XYZID に接続すると、**C1** が表示されます。同じ顧客が XYZ のモバイル ストアから XYZID に接続すると、**C2** が表示されます。

レポート

Cisco DNA Spaces では、次のキャプティブ ポータル レポートが提供されます。

デフォルトでは、過去 1 年間におけるすべてのロケーションのレポートが提供されます。レポートのロケーションと期間をフィルタ処理できます。

レポートを表示するには、[Captive Portal] ウィンドウの左ペインで [Reports] をクリックします。

デバイスのオンボーディング

デバイスのオンボーディングレポートは、SSID に接続されたデバイスに関する情報を提供します。顧客が複数のデバイスから SSID に接続している場合、該当するデバイスごとにカウントされてデバイス数が算出されます。

Onboarding Journey

このセクションには、選択したロケーションと期間における一意のデバイスの数が表示されます。

- [Connected to SSID]：指定された期間に選択されたロケーションから SSID に接続した一意のデバイスの総数。
- [Shown Captive Portal]：指定された期間に選択されたロケーションから SSID に接続し、キャプティブポータルが正常にロードされた一意のデバイスの総数。
- [Provisioned Internet]：指定された期間中に、選択したロケーションからインターネットがプロビジョニングされた一意のデバイスの総数。Cisco DNA Spaces の導入日以降の全ロケーションにおけるこのメトリクスが、[Total Unique Devices Provisioned Internet] のレポートの上部に表示されます。

日次トレンド：SSID に接続した新規デバイスと復帰デバイス

このセクションには、指定された期間にそのロケーションから SSID に接続した、新規および復帰した一意のデバイスの日次の傾向が表示されます。

- [New Devices]：指定された期間に選択されたロケーションから SSID に接続した一意の新規デバイスの総数。デバイスの総数に対する一意の新規デバイスの割合も表示されます。
- [Returning Devices]：指定された期間中に、選択したロケーションから SSID に複数回接続した一意のデバイスの総数。接続されている一意のデバイスの総数に対する一意の復帰デバイスの割合も表示されます。

グラフは、指定された期間の各日に選択したロケーションから接続された一意の新規デバイスと復帰デバイスの対比を表します。グラフのX軸は選択した期間の日数を表し、Y軸は一意のデバイスの数を表します。新規および復帰した一意のデバイスのカラーインジケーターは、グラフの上部に表示されます。

Menu Button Clicks in Captive Portal

このセクションには、プロモーションやオファーによる顧客のエンゲージメント詳細が日次で表示されます。プロモーションやオファーによる毎日のエンゲージメントは、指定された期間中に顧客がクリックしたメニューボタンに基づいて計算されます。

- [Menu buttons]：指定した期間中に選択したロケーションから少なくとも1回クリックされたメニューボタンの総数。
- [Clicks]：指定した期間中に選択したロケーションからキャプティブポータルで行われたクリックの合計数。

顧客獲得

このレポートは、指定の期間中に選択したロケーションから新たに獲得された個々の顧客と、獲得された顧客から収集されたデータ（個人データおよびデモグラフィックデータ）に関する知見を提供します。

（注） 新しい顧客が複数のデバイスを使用してお客様のロケーションに接続し、同じ個人 ID（携帯電話番号、電子メール、またはソーシャル ID）を使用した場合、顧客は 1 回だけカウントされます。

顧客獲得

（注） このレポートでは、認証タイプ [No Authentication] および [Access Code] で獲得された顧客はカウントされません。

- [New Devices Connected to SSID]：指定された期間に選択されたロケーションから SSID に接続した一意の新規デバイスの総数。デバイスの総数に対する一意の新規デバイスの割合も表示されます。
- [News Customers Identified]：指定された期間に、選択した場所から携帯電話番号、電子メール、ソーシャル ID などの個人識別情報を介して獲得した、一意の新規顧客の合計数。接続された一意の新規デバイスの合計のうち、獲得した一意の新規顧客の割合も表示されます。Cisco DNA Spaces のインストール日以降のすべてのロケーションにおけるこのメトリックが、このレポートの上部にある [Customers Identified] に表示されます。
- [Customers Opted In]：指定されて期間に、選択したロケーションからサブスクリプションにオプトインした、一意の新規獲得顧客の総数。一意の新規顧客獲得の総数のうち、オプトインした一意の新規獲得顧客の割合も表示されます。オプトインユーザーの詳細については、「ユーザーのオプトインオプション」を参照してください。
- [Completed Data Capture]：携帯電話番号、電子メール、ソーシャル ID などの個人識別情報を通じて獲得され、指定された期間中に、指定されたロケーションからデータキャプチャフォームを完了した一意の新規獲得顧客の総数。一意の新規獲得顧客の総数のうち、データキャプチャを完了した一意の新規獲得顧客の割合も表示されます。

日次顧客獲得

このセクションには、指定された期間における選択したロケーションの、「SSID に接続された一意の新規デバイス」と「携帯電話番号、電子メール、ソーシャル ID などの個人識別情報を通じて獲得された一意の新規顧客」の数を示す棒グラフが表示されます。また、サブスクリプションにオプトインしてデータキャプチャを完了した、「一意の新規顧客獲得」の数も日次で示しています。X 軸は、選択した期間の日を表します。Y 軸はカウントを表します。カラー

インジケータが、グラフの上部に表示されます。グラフにカーソルを合わせると、特定の日のカウントが表示されます。

（注） このレポートでは、認証タイプ「認証なし」および「アクセスコード」で獲得された顧客はカウントされません。

キャプチャされたデータ

このセクションには、指定した期間に選択したロケーションからキャプチャされた電子メールアドレス、電話番号、名前、性別の詳細などが表示されます。

- 電話番号：指定した期間に指定したロケーションからキャプチャされた、一意の電話番号の総数。
- 電子メール：指定した期間に指定したロケーションからキャプチャされた、一意の電子メールアドレスの総数。
- ソーシャルID： ソーシャル認証を介して、指定した期間に指定したロケーションからキャプチャされた、一意のソーシャル IDの総数。
- 名前：指定した期間に指定したロケーションから名前（姓/名）がキャプチャされた、顧客/デバイスの総数。
- 性別：指定した期間に指定したロケーションから性別が収集された顧客/デバイスの総数。

顧客分布

このセクションには、指定された期間に選択したロケーションから新たにキャプチャされた国、性別、言語などのプロファイルの詳細が表示されます。

[Countries]：国データが収集された顧客の総数のうち、さまざまな国からの顧客の割合を円グラフで表示します。国の総数が円グラフの中央に表示されます。顧客数が最も多い国は、顧客数とともに円グラフの下に表示されます。[Show All] ボタンをクリックすると、少なくとも 1 人の顧客がいるすべての国を表示できます。国名は、認証プロセス中に指定された電話番号の国コードに基づいて導出されます。

[Languages]：言語データが収集された顧客の総数のうち、さまざまな言語を使用する顧客の割合を円グラフで表示します。最も多くの顧客が使用する言語は、顧客数とともに円グラフの下に表示されます。[Show All] ボタンをクリックすると、少なくとも 1 人の顧客が使用するすべての言語を表示できます。言語数は、キャプティブポータルで顧客が選択した言語に基づいて算出されます。

[Gender]：顧客総数に対する男性、女性、「性別指定なし」の顧客の割合を円グラフで表示します。性別の詳細を入力した顧客の割合の合計が円グラフの中央に表示されます。男性、女性、および性別不明の顧客の数は、円グラフの下部に表示されます。

SSID

SSID とは、お客様がインターネットにアクセスするために接続するワイヤレスネットワーク ID を指します。ビジネス拠点に複数の SSID がある場合があります。Cisco DNA Spaces では、要件に応じて、ビジネス拠点の同じ SSID またはさまざまな SSID に対して、異なるキャプティブポータルを表示できます。

SSID は、ワイヤレス ネットワーク システムで定義されます。たとえば、Cisco Unified Wireless Network の Cisco Wireless Controller です。SSID に対して表示されるキャプティブポータルを定義するには、SSID を Cisco DNA Spaces にインポートする必要があります。

インポートされた SSID はグリッドビューに表示されます。各 Meraki SSID には、Meraki で SSID を設定できる「Details」リンクがあります。必要に応じて、グリッドからワイヤレスネットワーク用にインポートされた SSID を削除できます。

SSID の [Configure Manually] リンクをクリックすると、対応するワイヤレスネットワークの手動設定手順が表示されます。たとえば、Meraki SSID の [Configure Manually] リンクは、Cisco Meraki の設定手順につながります。

Cisco DNA Spaces では、SSID が Cisco Meraki などのワイヤレスネットワークから削除されていない場合でも、SSID を削除できます。これにより、ネットワーク同期の遅延中に不要な SSID を削除できます。

SSID のインポートまたは設定の前提条件

SSID を Cisco DNA Spaces にインポートまたは設定するには、次の手順を実行する必要があります。

- ロケーション階層を作成します。ロケーション階層の作成に関する詳細については、「ロケーション階層の概要」のセクションを参照してください。
- ワイヤレス ネットワーク システムで SSID を作成します。
  - CUWN 用の SSID の作成については、Cisco DNA Space におけるシスコ ワイヤレス コントローラおよび Cisco Catalyst 9800 シリーズ コントローラの設定 （243 ページ）の章を参照してください。
  - Meraki 用の SSID の作成については、Cisco Meraki での SSID の有効化 （300 ページ）のセクションを参照してください。
- Meraki の場合、SSID をインポートするには、Cisco DNA Spaces と Meraki が接続されている必要があります。通常、この接続は、ロケーション階層を定義するときに確立されます。Cisco DNA Spaces ダッシュボードの右上にある [Wi-Fi] アイコンを使用して Meraki に接続することもできます。

ワイヤレスネットワークからの SSID のインポート

SSID をインポートする前に、前提条件が満たされていることを確認してください。SSID をインポートするための前提条件の詳細については、SSID のインポートまたは設定の前提条件（153 ページ）を参照してください。

（注） SSID のキャプティブポータルルールを作成するには、その SSID を CUWN または Meraki からインポートする必要があります。

シスコ ワイヤレス コントローラまたは Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの SSID のインポート

（注）
- Cisco AireOS シリーズ ワイヤレス コントローラまたは Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの場合、Cisco DNA Spaces に SSID を手動で追加する必要があります。
- CMX を備えた Cisco AireOS シリーズ ワイヤレス コントローラまたは Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの場合、SSID は Cisco CMX ではなく、シスコ ワイヤレス コントローラで設定します。
- Cisco DNA Spaces で指定した SSID 名は、コントローラで設定されている SSID 名と一致する必要があります。コントローラダッシュボードで SSID 名を確認できます。
- Cisco DNA Spaces クラウド RADIUS サーバーは、Web RADIUS 認証用の PAP のみをサポートします。CHAP はサポートされていません。クライアント認証の失敗を回避するには、シスコ ワイヤレス コントローラで Web RADIUS 認証方式として PAP を設定する必要があります。

SSID をシスコ Cisco DNA Spaces に手動でインポートするには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Home] を選択します。

ステップ 2 [My Apps] エリアで、[Captive Portal] を選択します。

ステップ 3 表示される [Captive Portal] ウィンドウで、左ペインの [SSIDs] を選択します。.

ステップ 4 [Import/Configure SSID] をクリックします。

ステップ 5 表示される [Import/Configure SSID] ウィンドウで、[Wireless Network] ドロップダウンリストから [CUWN (CMX/WLC)] を選択します。

ステップ 6 [SSID] フィールドに、インポートする SSID の名前を入力し、[Add] をクリックします。

インポートされた SSID が [SSIDs] ウィンドウに表示されます。

次のタスク

（注） Cisco DNA Spaces は、インポートされた SSID をロードするにはコントローラと同期させる必要があるため、インポートされた SSID を表示するためにウィンドウを更新する必要があります。

Cisco Meraki 用の SSID のインポート

Meraki の SSID のキャプティブポータルルールを作成するには、Meraki ネットワークからその SSID をインポートする必要があります。SSID をインポートした後、Meraki ダッシュボードで、Cisco DNA Spaces と連携できるように SSID を設定する必要があります。

（注） ロケーション階層にインポートされるロケーションの SSID のみをインポートできます。

SSID をインポートするには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Home] を選択します。

ステップ 2 [My Apps] エリアで、[Captive Portal] を選択します。

ステップ 3 表示される [Captive Portal] ウィンドウで、左ペインの [SSIDs] を選択します。

ステップ 4 [Import/Configure SSID] をクリックします。

ステップ 5 表示される [Import/Configure] ウィンドウで、[Wireless Network] ドロップダウンリストから [Meraki] を選択します。

ステップ 6 [Organization] ドロップダウンリストから、SSID を追加する組織を選択します。

選択した組織の Meraki で有効になっている SSID を選択できます。

ステップ 7 インポートする SSID のチェックボックスをオンにして、[Import] をクリックします。

インポートされた SSID が [SSIDs] ウィンドウに表示されます。

ステップ 8 その SSID のグリッドで、[Detail] リンクをクリックします。

ステップ 9 表示されるウィンドウで、SSID の [Activate] ボタンをクリックし、Meraki の SSID に関する Cisco DNA Spaces の設定を更新します。

[SSID Configuration Sync] ウィンドウに、Meraki で設定する必要のある SSID の更新が表示されます。

ステップ 10 [更新（Update）] をクリックします。

（注） Meraki で SSID を手動設定することもできます。Meraki で SSID を手動設定する方法については、「Cisco Meraki 用 SSID の手動設定」のセクションを参照してください。

次のタスク

（注） インポートされた SSID をロードするために Cisco DNA Spaces を Meraki ネットワークと同期させる必要があるので、SSID を表示するには、ウィンドウの更新が必要になる場合があります。

アクセスコード

Cisco DNA Spaces では、アクセスコードを使用してビジネス構内のインターネットプロビジョニングを制御できます。さまざまなロケーション用のアクセスコードを作成し、そのアクセスコードを使用してこれらのロケーションのインターネットアクセスを制限できます。つまり、顧客は、そのロケーション用に設定されたアクセスコードを入力した後でのみインターネットにアクセスできます。このセクションでは、Cisco DNA Spaces を使用してアクセスコードを作成および管理する方法について説明します。

この機能を使用するには、キャプティブポータルのアクセスコード認証を設定する必要があります。キャプティブポータルのアクセスコード認証の設定に関する詳細は、「アクセスコード認証用ポータルの設定 （120 ページ）」を参照してください。

Cisco DNA Spaces では、作成したアクセスコードを顧客と共有することができます。アクセスコードの有効期間を指定できます。アクセス コードに単一のコード値を持たせる、またはコード値を毎週や毎月変更するように設定できます。アクセスコードに手動でコード値を指定するか、または自動生成することができます。アクセスコードを使用して、顧客がインターネットにアクセスできる時間を定義できます。Cisco DNA Spaces では、特定のアクセスコードを使用してインターネットにアクセスするときに、アクセスコードのダウンロードおよびアップロードの帯域幅制限を設定することもできます。

1 つのロケーションに複数のアクセスコードを定義できます。たとえば、プラチナメンバーにのみ高速インターネットを提供する場合、最大帯域幅を持つアクセスコードを作成し、限られた帯域幅を持つアクセスコードを別に作成できます。その後、顧客のタイプに基づいてアクセス コードを共有できます。

アクセスコード認証の認証手順については、「アクセスコード認証の手順 （187ページ）」をご覧ください。

（注）

- アクセスコードを作成または管理できるのは、管理者またはアクセスコードマネージャの権限を持つ Cisco DNA Spaces ユーザーのみです。
- アクセスコードマネージャとしてユーザーを招待できるのは Cisco DNA Spaces 管理者ユーザーのみです。アクセスコードオプションは、アカウント管理者またはアクセス コード マネージャ アカウントのみが、Cisco DNA Spaces ダッシュボードで使用できます。

アクセス コードの作成

アクセス コードを作成するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Captive Portals] をクリックします。

ステップ 2 表示されたウィンドウの左側ペインで、[Access Code] をクリックします。

（注） [Access Code] オプションは、Cisco DNA Spaces アカウント管理者またはアクセス コード マネージャ ユーザーのみ、Cisco DNA Spaces ダッシュボードで使用できます。Cisco DNA Spaces ユーザーの作成の詳細については、Cisco DNA Spaces ユーザーの招待 （237 ページ）を参照してください。

ステップ 3 [Location] ドロップダウンリストから、アクセスコードを定義するロケーションを選択します。

ステップ 4 [Create Access Code] をクリックします。

ステップ 5 [Create Access Code] ウィンドウで、作成するアクセスコードのタイプを選択します。

- [Fixed]：コード値はアクセスコードが有効である限り変わりません。
- [Weekly]：アクセスコードのコード値は毎週変更されます。
- [Monthly]：アクセスコードのコード値は毎月変更されます。

表示される残りのフィールドは、選択したアクセス コード タイプによって異なります。

アクセス コード タイプに [Fixed] を選択したら、次の詳細を入力します。

a) [Access Code Name] フィールドにアクセスコードの名前を入力します。
b) アクセスコードに独自コード値を定義するには、[Set your own access code?] チェックボックスをオンにします。
c) 表示される [Access Code] フィールドに、コード値を入力します。
d) [Limit session by time] バーを調整して、アクセスコードを使用して顧客がインターネットにアクセスできる時間を指定します。この時間は、1 回のセッションの値です。
e) アクセスコードの有効期間を定義するには、[Define a validity period for this access code] チェックボックスをオンにします。それぞれのボタンをクリックして、開始日と終了日を指定します。
f) 顧客がこのアクセスコードを使用してインターネットにアクセスするときに帯域幅を制限する場合、[Limit bandwidth] チェックボックスをオンにします。
g) [Bandwidth Limit] バーを調整して、このアクセスコードを使用してインターネットにアクセスするときに、顧客に提供する必要がある最大帯域幅を指定します。
h) [Show More] リンクをクリックして、アップロードおよびダウンロードの制限を指定します。
i) [Number of times access code can be used] ドロップダウンリストから、顧客がこのアクセスコードを使用してインターネットにアクセスできる最大回数を選択します。

アクセス コード タイプに [Weekly] を選択したら、次の詳細を入力します。

a) [Access Code Name] フィールドにアクセスコードの名前を入力します。
b) アクセス コードを生成する方法を指定します。

- すべての週に独自のコード値を指定する場合は、[Upload access codes from the csv file] チェック ボックスをオンにします。メッセージボックス内のリンクをクリックすると、アクセスコードのテンプレートをダウンロードできます。テンプレートで必要なすべての週にすべてのコード値を入力した後、[Upload] ボタンを使用してテンプレートを CSV ファイルとしてアップロードできます。
- すべての週のコード値を自動的に生成するには、[Access Code Validity time period] バーを調整して、このアクセスコードが有効な期間を週単位で指定します。

（注） [Access Code Validity time period] バーは [Upload access codes from the csv file] チェックボックスを選択しなかった場合のみ使用できます。[Upload access codes from csv File] チェックボックスを選択した場合、有効期間は CSV ファイルに入力したコード値の数に基づいて判断されます。たとえば、CSV ファイルに 3 つのコード値を定義した場合、アクセス コードは 3 週間有効です。CSV ファイルに指定されたコード値は、それぞれの週に順次対応していると見なされます。

c) [Limit session by time] バーを調整して、アクセスコードを使用して顧客がインターネットにアクセスできる時間を指定します。この時間は、1 回のセッションの値です。
d) [Start Date] ボタンをクリックして、アクセスコードが有効になる開始日を指定します。
e) 顧客がこのアクセスコードを使用してインターネットにアクセスするときに帯域幅を制限する場合、[Limit bandwidth] チェックボックスをオンにします。
f) 表示される [Bandwidth limit] バーで、このアクセスコードを使用してインターネットにアクセスするときに、顧客に提供する必要がある最大帯域幅を、バーを調節して指定します。
g) [Show More] リンクをクリックして、アップロードおよびダウンロードの制限を指定します。
h) [Number of times access code can be used] ドロップダウンリストから、顧客がこのアクセスコードを使用してインターネットにアクセスできる最大回数を選択します。

[Monthly] を選択した場合、次の詳細を入力します。

a) [Access Code Name] フィールドにアクセスコードの名前を入力します。
b) アクセス コードを生成する方法を指定します。

- すべての月に独自のコード値を指定する場合、[Upload access codes from the csv file] チェックボックスをオンにします。メッセージボックスのリンクをクリックすると、アクセスコードのテンプレートをダウンロードできます。テンプレートで必要なすべての月のすべてのコード値を入力した後、[Upload] ボタンを使用してテンプレートを CSV ファイルとしてアップロードできます。
- すべての月のコード値を自動的に生成するには、[Access Code Validity time period] バーを調整して、このアクセスコードが有効な期間を月単位で指定します。

（注） [Access Code Validity time period] バーは [Upload access codes from the csv file] チェックボックスをオンにしなかった場合のみ使用できます。[Upload access codes from the csv file] チェックボックスをオンにした場合、有効期間は CSV ファイルに入力したコード値の数に基づいて判断されます。たとえば、CSV ファイルに 3 つのコード値を定義した場合、アクセス コードは 3 か月間有効です。CSV ファイルに指定されたコード値は、それぞれの月に順次対応していると見なされます。

c) [Limit session by time] バーを調整して、アクセスコードを使用して顧客がインターネットにアクセスできる時間を指定します。この時間は、1 回のセッションの値です。
d) [Start Date] ボタンをクリックして、アクセスコードが有効になる開始日を指定します。
e) 顧客がこのアクセスコードを使用してインターネットにアクセスするときに帯域幅を制限する場合、[Limit bandwidth] チェックボックスをオンにします。
f) 表示される [Bandwidth limit] バーで、このアクセスコードを使用してインターネットにアクセスするときに、顧客に提供する必要がある最大帯域幅を、バーを調節して指定します。
g) [Show More] リンクをクリックして、アップロードおよびダウンロードの制限を指定します。
h) [Number of times access code can be used] ドロップダウンリストから、顧客がこのアクセスコードを使用してインターネットにアクセスできる最大回数を選択します。

ステップ 6 [作成（Create）] をクリックします。

アクセス コードの表示

有効期間がまだ切れていないロケーションのすべてのアクセスコードを表示できます。

ロケーションに定義されているアクセスコードを Cisco DNA Spaces で表示するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Captive Portals] をクリックします。
ステップ 2 表示されたウィンドウの左側ペインで、[Access Code] をクリックします。

（注） [Access Code] オプションは、Cisco DNA Spaces アカウント管理者またはアクセス コード マネージャ ユーザーのみ、Cisco DNA Spaces ダッシュボードで使用できます。Cisco DNA Spaces ユーザーの作成の詳細については、Cisco DNA Spaces ユーザーの招待 （237 ページ）を参照してください。

ステップ 3 表示された [Access Code] ウィンドウのドロップダウンリストから、アクセスコードを表示するロケーションを選択します。

ロケーションに対して定義されたアクセスコードが表示されます。

選択したロケーションについて、利用可能なアクセスコードの総数、期限切れのアクセスコードの総数、およびそれらのうちのアクティブおよび非アクティブなアクセスコードの数が表示されます。

さらに、ロケーションに対して定義されたアクセスコードの次のような詳細が表示されます。

- [Status]：アクセスコード名がアクティブであるかどうか。
- [Name]：アクセスコードの名前。
- [Code]：アクセスコードを表示した時点のアクセスコード名のコード値。コードの値は毎週または毎月変更するように設定した場合、変更されます。
- [Type]：アクセスコードのタイプ。アクセス コード タイプは固定するこも、毎週または毎月変更することもできます。

- [Expiry Date]：アクセスコードが有効である期間。
- [Actions]：編集、共有、削除など、アクセスコードに対して実行できる操作。

アクセス コードの編集

アクセス コードを編集するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Captive Portals] をクリックします。
ステップ 2 表示されたウィンドウの左側ペインで、[Access Code] をクリックします。

（注） [Access Code] オプションは、Cisco DNA Spaces アカウント管理者またはアクセス コード マネージャ ユーザーのみ、Cisco DNA Spaces ダッシュボードで使用できます。Cisco DNA Spaces ユーザーの作成の詳細については、Cisco DNA Spaces ユーザーの招待 （237 ページ）を参照してください。

ステップ 3 表示される [Access Code] ウィンドウで、アクセスコードを編集するロケーションを選択します。

そのロケーションに対して定義されたアクセスコードが表示されます。

ステップ 4 編集するアクセスコードの [Active Access Codes] 領域で、[Edit] ボタンをクリックします。
ステップ 5 必要な変更を行って、[Update] をクリックします。

アクセスコードの共有

Cisco DNA Spaces では、顧客とアクセスコードを共有できます。

アクセス コードを共有するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Captive Portals] をクリックします。
ステップ 2 表示されたウィンドウの左側ペインで、[Access Code] をクリックします。

（注） [Access Code] オプションは、Cisco DNA Spaces アカウント管理者またはアクセス コード マネージャ ユーザーのみ、Cisco DNA Spaces ダッシュボードで使用できます。Cisco DNA Spaces ユーザーの作成の詳細については、Cisco DNA Spaces ユーザーの招待 （237 ページ）を参照してください。

ステップ 3 表示される [Access Code] ウィンドウで、アクセスコードを共有するロケーションを選択します。

そのロケーションに対して定義されたアクセスコードが表示されます。

ステップ 4 共有するアクセス コードの [Active Access Codes] 領域で、[Share] ボタンをクリックします。

ステップ 5 表示される [Share Access Code] ウィンドウに、アクセスコードを共有する人の電子メール ID を入力し、[Invite] をクリックします。

アクセス コードの削除

アクセス コードを削除するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Captive Portals] をクリックします。

ステップ 2 表示されたウィンドウの左側ペインで、[Access Code] をクリックします。

（注） [Access Code] オプションは、Cisco DNA Spaces アカウント管理者またはアクセス コード マネージャ ユーザーのみ、Cisco DNA Spaces ダッシュボードで使用できます。Cisco DNA Spaces ユーザーの作成の詳細については、Cisco DNA Spaces ユーザーの招待 （237 ページ）を参照してください。

ステップ 3 表示される [Access Code] ウィンドウで、アクセスコードを削除するロケーションを選択します。

そのロケーションに対して定義されたアクセスコードが表示されます。

ステップ 4 [Active Access Codes] エリアで、削除するアクセスコードの [Delete] ボタンをクリックします。

ステップ 5 表示される [Delete] ウィンドウで [Yes] をクリックし、削除を確定します。

（注） 複数のアクセスコードを同時に削除できます。アクセスコードごとにチェックボックスが表示され、一度に複数のアクセスコードを選択して同時に削除することができます。また、期限切れのアクセスコードを削除することもできます。

アクセス コードの非アクティブ化

アクセス コードを非アクティブ化するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Captive Portals] をクリックします。

ステップ 2 表示されたウィンドウの左側ペインで、[Access Code] をクリックします。

（注） [Access Code] オプションは、Cisco DNA Spaces アカウント管理者またはアクセス コード マネージャ ユーザーのみが、Cisco DNA Spaces ダッシュボードで使用できます。Cisco DNA Spaces ユーザーの作成の詳細については、Cisco DNA Spaces ユーザーの招待 （237 ページ）を参照してください。

ステップ 3 表示される [Access Code] ウィンドウで、アクセスコードを非アクティブ化するロケーションを選択します。

そのロケーションに対して定義されたアクセスコードが表示されます。

ステップ 4 非アクティブ化するアクセスコードの [Status] トグルスイッチを切り替えます。

非アクティブ化すると、ステータス ボタンはグレーに変わります。

アクセスコードの再アクティブ化

デフォルトでは、アクセス コードは作成されたときはアクティブ モードになっています。これを非アクティブ化した後は、アクセス コードの有効期限内であれば、必要に応じてアクティブ化できます。

アクセスコードを再アクティブ化するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Captive Portals] をクリックします。

ステップ 2 表示されたウィンドウの左側ペインで、[Access Code] をクリックします。

（注） [Access Code] オプションは、Cisco DNA Spaces アカウント管理者またはアクセス コード マネージャ ユーザーのみが、Cisco DNA Spaces ダッシュボードで使用できます。Cisco DNA Spaces ユーザーの作成の詳細については、Cisco DNA Spaces ユーザーの招待 （237 ページ）を参照してください。

ステップ 3 表示される [Access Code] ウィンドウで、アクセスコードをアクティブ化するロケーションを選択します。

そのロケーションに対して定義されたアクセスコードが表示されます。

ステップ 4 アクティブ化するアクセスコードの [Status] トグルスイッチを切り替えます。

アクティブ化すると、ステータス ボタンは緑に変わります。

アクセスコードのエクスポート

Cisco DNA Spaces では、ロケーション用に作成したアクセスコードを .csv ファイルまたは PDF としてエクスポートできます。

Cisco DNA Spaces でロケーション用に定義されているアクセスコードを表示するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Captive Portals] をクリックします。

ステップ 2 表示されたウィンドウの左側ペインで、[Access Code] をクリックします。

（注） [Access Code] オプションは、Cisco DNA Spaces アカウント管理者またはアクセス コード マネージャ ユーザーのみ、Cisco DNA Spaces ダッシュボードで使用できます。Cisco DNA Spaces ユーザーの作成の詳細については、Cisco DNA Spaces ユーザーの招待 （237 ページ）を参照してください。

ステップ 3 表示された [Access Code] ウィンドウのドロップダウンリストから、アクセスコードをエクスポートするロケーションを選択します。

選択したロケーションについて、利用可能なアクセスコードの総数、期限切れのアクセスコードの総数、およびそれらのうちのアクティブおよび非アクティブなアクセスコードの数が表示されます。

ステップ 4 必要な形式に基づいて、次のいずれかを実行します。

- アクセスコードを PDF ファイルとしてエクスポートするには、**[Export]** > **[Export as PDF]** を選択します。
- アクセスコードを .csv ファイルとしてエクスポートするには、**[Export]** > **[Export as CSV]** を選択します。

ステップ 5 表示されるウィンドウで、[OK] をクリックしてファイルを保存します。

アクセスコードは、指定された形式でコンピュータの [ダウンロード] フォルダにダウンロードされます。

（注） アクティブなアクセスコードのみがエクスポートされます。

次のタスク

期限切れのアクセスコードをエクスポートする場合、または特定の期間内に有効なアクセスコードをエクスポートする場合は、[Filter] オプションを使用して実行できます。

エクスポートするアクセスコードのフィルタリング

エクスポートするアクセスコードをフィルタリングするには、次の手順を実行します。

ステップ 1 [Access Code] ウィンドウのドロップダウンリストから、アクセスコードをエクスポートするロケーションを選択します。

ステップ 2 [Filter] をクリックします。

- [All Access Codes]：選択した場所に対して作成されたすべてのアクセス コードをエクスポートします。アクティブなアクセスコードと期限切れのアクセスコードが含まれます。
- [Filter by]：適用されたフィルタに基づいてアクセスコードをエクスポートします。今週、今月、または特定の日付範囲で期限切れになるアクセスコードをフィルタリングするように選択できます。同様に、今週、今月、または特定の日付範囲に期限切れになったアクセスコードをフィルタリングすることもできます。[Expires in] および [Expired] オプションを使用して、期限切れのアクセスコードとアクティブなアクセスコードの両方を同時に含めることができます。

ステップ 3 [Apply] をクリックします。

フィルタリングされたアクセスコードは、[Filtered Access Codes] ウィンドウに表示されます。

ステップ 4 必要な形式に基づいて、次のいずれかを実行します。

- アクセスコードを PDF ファイルとしてエクスポートするには、**[Export]** > **[Export as PDF]** を選択します。
- アクセスコードを .csv ファイルとしてエクスポートするには、**[Export]** > **[Export as CSV]** を選択します。

ステップ 5 表示されるウィンドウで、[OK] をクリックしてファイルを保存します。

アクセスコードは、指定された形式でコンピュータの [ダウンロード] フォルダにダウンロードされます。

ユーザー 管理

[User Management] オプションを使用して、ユーザーロール、[Creative User] または [AccessCodeManager] を持つキャプティブ ポータル ユーザーを招待できます。キャプティブポータルアプリで「読み取り」および「書き込み」権限を持つユーザーのみが、[User Management] オプションを使用して他のユーザーを招待できます。

- [Creative User]：このユーザーは、アクセス権が提供されているロケーションでキャプティブポータルを作成、表示、および編集できます。このユーザーは、Cisco DNA Spaces の他の機能にはアクセスできません。このロールは、基本的にキャプティブ ポータル デザイナー向けです。
- [AccessCodeManager]：このユーザーは、アクセス権が提供されているロケーションのアクセスコードを作成し、管理できます。このユーザーは、**キャプティブポータル**アプリにのみアクセスできます。このロールは、基本的にアクセスコードマネージャ向けです。

このロールは [Roles] タブに一覧表示されます。[Roles] タブからロールを編集することはできません。

[Access Code Manager] または [Creative User] を定義するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Home] を選択します。

ステップ 2 [Captive Portals] をクリックします。

ステップ 3 表示されるウィンドウで、左ペインの [User Management] をクリックします。

（注） [User Management] オプションは、キャプティブポータルアプリで「読み取り」および「書き込み」権限を持つユーザーのみが Cisco DNA Spaces ダッシュボードで使用できます。詳細については、Cisco DNA Spaces ユーザーの招待 （237 ページ）を参照してください。

ステップ 4 [Invite User] をクリックします。

ステップ 5 [Invite User] ウィンドウで、招待するユーザーの電子メールアドレスを入力し、[Next] をクリックします。

ステップ 6 [Role] ドロップダウンリストから、[Creative User] または [AccessCodeManager] を選択します。

ステップ 7 [Location] をクリックします。

ステップ 8 [Location Hierarchy] エリアで、このユーザーにアクセスを許可するロケーションのチェックボックスをオンにします。

ステップ 9 [完了（Done）] をクリックします。

ステップ 10 [Send Invitation] をクリックします。

ユーザーに招待状が送信されます。[Users] タブにこのユーザー名が表示されます。[Find Users] フィールドを使用して、ユーザーを検索できます。

ポータルへのソーシャル認証

ポータルへのソーシャル認証を有効にするには、次の手順を実行します。

- Social Sign In 認証のためのポータル設定 （117 ページ）

ソーシャル認証に向けたワイヤレスネットワークの設定

ソーシャル認証の場合、Meraki や CUWN などのワイヤレスネットワークでいくつかの設定を行う必要があります。詳細については、次のリンクを参照してください。

- ソーシャル認証のための Cisco Meraki の設定 （304 ページ）
- ソーシャル認証のためのシスコ ワイヤレス コントローラの設定 （260 ページ）

ソーシャル認証のためのアプリケーションの設定

このセクションでは、さまざまなネットワーキングサイトを介したソーシャル認証のためのアプリケーションに必要な設定について説明します。

Facebook

ソーシャル認証のために Facebook アプリケーションを設定するには、次の手順を実行します。

ステップ 1 developers.facebook.com に移動します。

ステップ 2 [My Apps] ドロップダウンリストから、ソーシャル認証のために Cisco DNA Spaces で設定するアプリケーションを選択します。

ステップ 3 [設定（Settings）] をクリックします。

ステップ 4 [App Domains] フィールドに、リージョンに基づいて、以下のリストから適切な値を入力します。

- 米国の場合、**splash.dnaspaces.io** と入力します。
- EU の場合、**splash.dnaspaces.eu** と入力します。

ステップ 5 [User Data Deletion] フィールドに、リージョンに基づいて、以下のリストから適切な**データ削除コールバック URL** を入力します。

- 米国の場合、**`https://splash.dnaspaces.io/p/<CustomerAccountName>/fb_revoke`** と入力します。
- EU の場合、**`https://splash.dnaspaces.eu/p/<CustomerAccountName>/fb_revoke`** と入力します。

ステップ 6 [Facebook Login Settings] タブの [Valid OAuth Redirect URIs] フィールドに、リージョンに基づいて、以下のリストから適切な値を入力します。

- 米国の場合、https://splash.dnaspaces.io/p/facebook_auth と入力します。
- EU の場合、https://splash.dnaspaces.eu/p/facebook_auth と入力します。

Twitter

ソーシャル認証のために Twitter アプリケーションを設定するには、次の手順を実行します。

ステップ 1 **https://developer.twitter.com/en/apps** にログインします。
ステップ 2 ソーシャル認証のために Cisco DNA Spaces で設定するアプリケーションをクリックします。
ステップ 3 [Settings] タブをクリックします。
ステップ 4 [Callback URL] フィールドに、コールバック URL を入力します。

- グローバルリダイレクト URL：**https://splash.dnaspaces.io/p/twitter_auth**
- EU のリダイレクト URL：**https: //splash.dnaspaces.eu/p/twitter_auth**

ステップ 5 [Enable Callback Locking] チェックボックスをオフにします。
ステップ 6 [Allow this application to be used to Sign in with Twitter] チェックボックスをオンにします。
ステップ 7 Twitter から情報を取得するには、[Permissions] タブで次の操作を行います。

- [Access Permissions] エリアで、[Read and write] オプションボタンを選択します。
- [Additional Permissions] エリアで、[Request email address from users] をオンにします。

LinkedIn アプリケーション

ステップ 1 https://www.linkedin.com/developers/ にログインします。
ステップ 2 [My Apps] をクリックします。
ステップ 3 ソーシャル認証のために設定するアプリケーションをクリックします。

ステップ 4 [Authentication] をクリックします。

ステップ 5 [Default Application Permissions] エリアで、[r_basicprofile] および [r-emailaddress] チェックボックスをオンにします。

ステップ 6 [Authorized Redirect URLs] フィールドにリダイレクト URL を入力し、[Add] をクリックします。

- グローバルリダイレクト URL：**https://splash.dnaspaces.io/p/linkedin_auth**
- EU のリダイレクト URL：**https: // splash.dnaspaces.eu/p/linkedin_auth**

ステップ 7 [Settings] タブで、ドメインの **splash.dnaspaces.io** を設定します。

EU リージョンの場合、ドメインは **splash.dnaspaces.eu** です。

ソーシャル認証のためのソーシャル アプリケーションの追加

ソーシャル ネットワーク サイトを介したポータルへの認証を管理するには、対応するソーシャルアプリを Cisco DNA Spaces で設定する必要があります。たとえば、Facebook にサインイン中の顧客に対してポータルへのアクセスを認証する必要がある場合、Cisco DNA Spaces で Facebook アプリを設定する必要があります。Cisco DNA Spaces に追加できるソーシャル ネットワーク サイトのアプリは次のとおりです。

- Facebook
- Twitter
- LinkedIn

Cisco DNA Spaces でソーシャルアプリを設定するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Home] を選択します。

ステップ 2 表示されるウィンドウで、[Captive Portal] をクリックします。

ステップ 3 表示される [Captive Portal] ウィンドウの左ペインで [Settings] をクリックします。

ステップ 4 [Settings] ウィンドウで [Social Apps] を選択します

ステップ 5 アプリを設定するソーシャル ネットワーク サイトに対応する [Add] ボタンをクリックします。

アプリケーションを設定するためのフィールドが表示されます。

ステップ 6 アプリケーションの名前、アプリケーションID、およびアプリケーションの秘密鍵を、それぞれのフィールドに入力します。

ステップ 7 [Save] をクリックします。

Cisco DNA Spaces での SMS ゲートウェイの設定

SMS 通知を送信し、SMS を介してポータル認証を管理するには、SMS ゲートウェイを設定する必要があります。Cisco DNA Spaces では、サードパーティベンダーの SMS ゲートウェイを使用できます。Cisco DNA Spaces で SMS ゲートウェイを設定するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[**Home**] を選択します。

ステップ 2 表示されるウィンドウで、[Captive Portal] をクリックします。

ステップ 3 表示される [Captive Portal] ウィンドウの左ペインで [Settings] をクリックします。

ステップ 4 [Settings] ウィンドウで、[SMS] を選択します。

ステップ 5 [Add SMS gateway] をクリックします。

ステップ 6 [SMS Gateway Type] ドロップダウンリストから、使用する SMS ゲートウェイタイプを選択します。選択した SMS ゲートウェイタイプに基づいて、追加のフィールドが表示されます。

Cisco DNA Spaces では、次の SMS ゲートウェイタイプがサポートされます。

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

ステップ 7 選択した SMS ゲートウェイタイプに基づいて表示される追加フィールドで、必要な値を指定します。

ステップ 8 [**保存（Save）**] をクリックします。

（注） 作成された SMS ゲートウェイは、ポータルの [SMS with password verification] および [SMS with link verification] 認証オプションの [SMS Gateway] ドロップダウンリストで選択肢として表示されます。これらの SMS ゲートウェイは、エンゲージメントルールで SMS 通知を構成するときにも選択できます。

キャプティブポータルルールの管理

要求されるたびに、キャプティブ ポータル ルールを一時停止したり、再度有効にしたりできます。必要に応じて、キャプティブ ポータル ルールを変更したり、削除したりできます。ロケーションに設定されているキャプティブポータルルールを表示することもできます。

キャプティブ ポータル ルールの一時停止

キャプティブ ポータル ルールを一時停止するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Home] を選択します。

ステップ 2 [My Apps] エリアで、[Captive Portal] を選択します。

ステップ 3 [Captive Portal] ウィンドウで、[Captive Portal Rule] を選択します。

作成されたキャプティブ ポータル ルールがリストされます。

ステップ 4 一時停止するキャプティブポータルルールのチェックボックスをオンにします。

ステップ 5 ウィンドウ下部に表示される [Pause] ボタンをクリックします。

ステップ 6 表示されるウィンドウで [Pause Rule] をクリックし、一時停止することを確認します。

キャプティブ ポータル ルールが一時停止します。

次のタスク

（注） 複数のキャプティブポータルルールを一時停止するには、一時停止するキャプティブポータルルールのチェックボックスをオンにし、ページの下部に表示される [Pause] ボタンをクリックします。

キャプティブ ポータル ルールの再起動

一次停止中のキャプティブポータルルールを再起動するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、**Home** を選択します。

ステップ 2 [My Apps] エリアで、[Captive Portal] を選択します。

ステップ 3 [Captive Portal] ウィンドウで、[Captive Portal Rule] を選択します。

作成されたキャプティブ ポータル ルールがリストされます。

ステップ 4 再起動するキャプティブポータルルールのチェックボックスをオンにします。

ウィンドウ下部に表示される [Make Live] ボタンをクリックします。

次のタスク

（注） 複数のキャプティブポータルルールを再起動するには、再起動するキャプティブポータルルールのチェックボックスをオンにして、ウィンドウの下部に表示される [Make Live] ボタンをクリックします。

キャプティブ ポータル ルールの変更

キャプティブ ポータル ルールを変更するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Home] を選択します。

ステップ 2 [My Apps] エリアで、[Captive Portal] を選択します。

ステップ 3 [Captive Portal] ウィンドウで、[Captive Portal Rule] を選択します。

作成されたキャプティブ ポータル ルールがリストされます。

ステップ 4 変更するキャプティブポータルルールの [Edit Rule] アイコンをクリックします。

ステップ 5 必要な変更を加えます。

ステップ 6 変更を保存するには、[Save] をクリックします。または変更をパブリッシュするには、[Save and Publish] をクリックします。

（注） ライブルールに表示されるのは [Save and Publish] オプションのみです。[Save and Publish] ボタンをクリックすると、変更を反映したルールがパブリッシュされます。

キャプティブ ポータル ルールの削除

キャプティブ ポータル ルールを削除するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Home] を選択します。

ステップ 2 [My Apps] エリアで、[Captive Portal] を選択します。

ステップ 3 [Captive Portal] ウィンドウで、[Captive Portal Rule] を選択します。

作成されたキャプティブ ポータル ルールがリストされます。

ステップ 4 削除するキャプティブポータルルールの右端に表示される [Delete Rule] アイコンをクリックします。

次のタスク

（注） 複数のキャプティブポータルルールを削除するには、削除するキャプティブポータルルールのチェックボックスをオンにし、ウィンドウの下部に表示される [Delete] ボタンをクリックします。

ロケーションのキャプティブポータルルールの表示

グループ、ビルディング、フロアなどのロケーションのキャプティブポータルルールを表示するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Location Hierarchy] を選択します。

ロケーション階層を示す [Location Hierarchy] ウィンドウが表示されます。

ステップ 2 キャプティブポータルルールを表示するロケーションをクリックします。

ステップ 3 [Proximity Rules] タブをクリックします。

ステップ 4 [Captive Portal Rule] タブをクリックします。

ロケーションのキャプティブポータルルールがリストされます。

次のタスク

（注） ロケーションの [Proximity Rules] リンクは、そのロケーションに少なくとも 1 つのプロキシミティルールが存在する場合にのみ有効になります。

ロケーションによるフィルタリング

キャプティブポータルルール、エンゲージメントルール、ロケーションペルソナルール、密度ルールなどの Cisco DNA Spaces ルールでは、ルールを適用するロケーションをフィルタリングできます。ロケーションに定義されているメタデータにより、ロケーションをフィルタリングすることも可能です。

ルールを適用するロケーションを指定するには、次の手順を実行します。

ステップ 1 [Add Locations] ボタンをクリックします。

ステップ 2 表示される [Choose Locations] ウィンドウで、ルールを適用するロケーションを選択します。

ステップ 3 [完了（Done）] をクリックします。

ロケーションに定義されているメタデータを使用して、ロケーションを再度フィルタリングできます。選択したロケーション、その親および子のロケーションに定義されているメタデータのみを選択できます。

特定のメタデータのロケーションにルールを適用する

特定のメタデータのロケーションにルールを適用するには、次の手順を実行します。

ステップ 1 [Filter by Metadata] チェックボックスをオンにします。

ステップ 2 [Filter] 領域で、[Add Metadata] ボタンをクリックします。
[Choose Location Metadata] ウィンドウが表示されます。

ステップ 3 ドロップダウン リストから、メタデータの変数を選択し、隣接フィールドに変数の値を選択します。

ステップ 4 [完了（Done）] をクリックします。

特定のメタデータのロケーションを除外する

特定のメタデータのロケーションを除外するには、次の手順を実行します。

ステップ 1 [Filter by Metadata] チェックボックスをオンにします。

ステップ 2 [Exclude] 領域で、[Add Metadata] ボタンをクリックします。
[Choose Location Metadata] ウィンドウが表示されます。

ステップ 3 ドロップダウン リストから、メタデータの変数を選択し、隣接フィールドに変数の値を選択します。

ステップ 4 [Done] をクリックします。

トリガー API の設定

Cisco DNA Spaces ルールを使用して通知または顧客の詳細を外部 API に送信するように設定するには、次の手順を実行します。

- [Method] ドロップダウン リストから、API をトリガーするメソッドを選択します。

（注） API URI にスマートリンク変数を追加するか、メソッドパラメータに変数を追加することにより、API に送信される通知メッセージまたは顧客の詳細に顧客の姓名などのデータを含めることができます。

- GET：GET メソッドを使用して API に通知または顧客の詳細を送信します。このメソッドを選択すると、要求パラメータを指定できる追加のフィールドが表示され、顧客の名、

姓、携帯番号などの追加情報を含めることができます。API で定義された要求パラメータのキーを追加し、変数を使用してこれらの値を指定できます。値はハードコード値または変数のどちらでもかまいません。[Value] フィールドをクリックすると、追加できる変数が一覧表示されます。変数の詳細については、キャプティブポータルのスマートリンクとテキスト変数（190 ページ）を参照してください。[**Add**] ボタンを使用して、さらに「get パラメータ」を追加できます。

- POST FORM：POST FORM メソッドを使用して API に通知または顧客の詳細を送信します。このメソッドを選択すると、フォームパラメータを指定できる追加のフィールドが表示され、顧客の名、姓、携帯番号などの追加情報を含めることができます。API で定義されたフォームパラメータのキーを追加して、これらの値を指定できます。値はハードコード値または変数のどちらでもかまいません。[Value] フィールドをクリックすると、追加できる変数が一覧表示されます。変数の詳細については、キャプティブポータルのスマートリンクとテキスト変数（190 ページ）を参照してください。[**Add**] ボタンを使用して、さらに「フォームパラメータ」を追加できます。

- POST JSON：POST JSON メソッドを使用して API に通知または顧客の詳細を送信します。このメソッドを選択すると、API に送信する JSON データを指定できるテキストボックスが表示されます。API で定義されるさまざまな JSON フィールドの JSON 値を指定できます。値はハードコード値または変数のどちらでもかまいません。変数を JSON として追加するには、[JSON Data] テキストボックスをクリックします。変数がリストされます。追加する変数を選択します。変数の詳細については、キャプティブポータルのスマートリンクとテキスト変数（190 ページ）を参照してください。

- POST BODY：POST BODY メソッドを使用して API に通知または顧客の詳細を送信します。このメソッドを選択すると、API に送信する内容を指定できる追加のフィールドが表示されます。内容には変数を追加できます。変数を BODY として追加するには、[Post Body Data] テキストボックスをクリックします。変数がリストされます。

  - [URI] フィールドに、API の URI を入力します。スマートリンクを使用して、API に送信する通知または顧客データに追加の顧客情報を含めることができます。[URI] フィールドをクリックして追加できる変数を表示します。変数についての詳細は、キャプティブポータルのスマートリンクとテキスト変数（190 ページ）を参照してください。

注　GET、POST FORM、POST BODY、および POST JSON の各メソッドのカスタム変数を定義できます。メソッドの変数フィールドをクリックすると、事前定義された変数とともに [Add Custom Variable] ボタンが表示されます。POST BODY メソッドの場合、現在、POST BODY DATA フィールドに対するカスタム変数のサポートはありません。一方、URI フィールドにはカスタム変数のサポートがありません。

（注） ポータルの [Data Capture] モジュールを使用してキャプチャするように設定されたこれらのデータだけが通知に含まれます。

ポータルの認定デバイス リスト

ポータルのためにテストされ、認定されているデバイスおよびオペレーティング システムは、次の表のとおりです。

表 *6:*

デバイス	**OS** バージョン	ブラウザ/キャプティブ ネットワーク アシスタント（**CNA**）（サイトが正常に読み込まれ、動作する）
モバイル デバイス		
Moto G2	6.0	CNA、Google Chrome
Sony Experia SP	4.3	Google Chrome
Samsung S2	4.1.2	Google Chrome
Samsung Galaxy S5	6.0.1	Google Chrome
Samsung S6	6.0.1	Google Chrome
Micromax	5.0 および 4.4.4	Google Chrome
Google Nexus 6	6.0.1	CNA、Google Chrome
Moto X Play	6.0.1	Google Chrome
iPhone 4s	7.1.2	CNA Safari
iPhone 5s	9.3.5 および 9.3.4	CNA、Safari
iPhone 6	9.3.4	CNA、Safari
iPhone 6s	9.3.4	CNA、Safari
iPhone 6 Plus	9.3.2	CNA、Safari
Huwaei Honur	6.0.1 および 6.0	Google Chrome
Huwaei P8	5.0.1	Google Chrome

デバイス	OS バージョン	ブラウザ/キャプティブネットワーク アシスタント（CNA）（サイトが正常に読み込まれ、動作する）
Microsoft Lumia 950	Windows 10	CNA およびネイティブ ブラウザ
Nokia Lumia 1320	Windiows 8.1	CNA およびネイティブ ブラウザ
iPad またはタブレット		
Samsung Galaxy Tab 2	4.1.2	Google Chrome
Samsung Galaxy Tab 3 Neo	4.2.2	Google Chrome
iPad mini	8.3	CNA、Safari
iPad 2	9.3.2	CNA、Safari
ラップトップまたはデスクトップ		
Windows Lap HP ProBook	Windows 7	Chrome/Firefox/IE
Windows Lap Lenovo	Windows 10	Chrome/Firefox/IE
Macbook Pro 13-inch	Mac OS X EI Capitan 10.11.6	CNA
Macbook Pro 13-inch Retina display	Mac OS X EI Capitan 10.11.6	CNA

Cisco DNA Spaces キャプティブポータルの動作

さまざまなデバイスでのキャプティブ ポータルの動作は、次のとおりです。

Apple iOS 7.x ～ 11.x

顧客がキャプティブポータル URL で設定されている SSID に接続すると、Captive Network Assistant（CNA）ウィンドウが表示されます。CNA によってポータルのコンテンツがロードされ、表示されます。

顧客がポータル内のいずれかのメニューまたはリンクをクリックすると、ポータルで設定された認証タイプに応じた内容のログイン画面が表示されます。ポータルへの認証を設定するときの詳細については、ポータルへの認証の設定（113 ページ）を参照してください。顧客は、認証手順を実行する必要があります。認証手順は、利用規約の承認のみ、SMS 認証、Email 認証、またはソーシャル認証のいずれかです。各種認証タイプの認証手順の詳細については、顧

客の認証手順 （181 ページ）を参照してください。必要な認証手順が完了すると、Cisco DNA Spaces が、当該のデバイスにインターネット プロビジョニングをするよう、ワイヤレスネットワーク（CUWN、Meraki）に要求を送信します。インターネットプロビジョニングが正常に行われると、CNA ウィンドウは破棄され、Mobile Safari が開きます。Mobile Safari では、顧客が先にクリックしていたメニューまたはリンクの Web ページが開きます。

（注） iOS11.0 ～ 11.3 の場合、インターネット プロビジョニング後、CNA ウィンドウは自動的に閉じられません。[Complete] ボタンをクリックして CNA ウィンドウを閉じるよう顧客に求めるメッセージが表示されます。

あるいは、CNA が無視され、顧客が Mobile Safari または Chrome ブラウザを使用して許可リストにない（アクセス制御リストまたはウォールドガーデン範囲にない）URL にアクセスした場合、顧客は、設定されているキャプティブポータルの URL にリダイレクトされます。ブラウザによってキャプティブ ポータルのコンテンツがロードされ、表示されます。顧客がポータル内のいずれかのメニューまたはリンクをクリックすると、ログイン画面が表示されます。インターネットを利用するには、顧客はここで、前述した認証手順を完了する必要があります。

（注） インターネットプロビジョニングの後は、顧客は、それ以上の認証なしでポータル内のメニューやリンクに移動できます。

（注） インターネット プロビジョニング中にエラーが生じると、キャプティブ ポータルが再表示されます。

（注） キャプティブポータルで認証モジュールをインラインモジュールとして設定すると、ポータルのリンクをクリックせずに、認証プロセスを開始できます。認証モジュールをインラインモジュールとして設定する方法の詳細については、インライン認証 （121 ページ）を参照してください。

Android 5.x 以降（CNA を使用）

顧客がキャプティブ ポータル URL で設定されている SSID に接続すると、[Sign in to {SSID name}] オプションが通知領域に表示されます。通知をクリックすると、Android 5.x 以降を搭載したデバイスでは、CNA ウィンドウが立ち上がります。CNA によってポータル URL からコンテンツがロードされ、ポータルが表示されます。顧客がポータル内のいずれかのメニューまたはリンクをクリックすると、ポータルで設定された認証タイプに応じた内容のログイン画面が表示されます。ポータルへの認証を設定するときの詳細については、ポータルへの認証の設定 （113 ページ）を参照してください。顧客は、認証手順を実行する必要があります。認証手

順は、利用規約の承認のみ、SMS 認証、Email 認証、またはソーシャル認証のいずれかです。各種認証タイプの認証手順の詳細については、顧客の認証手順（181 ページ）を参照してください。必要な認証手順が完了すると、Cisco DNA Spaces が、当該のデバイスにインターネットプロビジョニングをするよう、ワイヤレスネットワーク（CUWN, Meraki）に要求を送信します。インターネットプロビジョニングが正常に行われると、CNA ウィンドウは破棄されます。

あるいは、顧客は通知を無視してネイティブ ブラウザまたは Chrome ブラウザの使用に進むこともできます。顧客が、許可リストにない（アクセス制御リストやウォールドガーデンの範囲にない）URL にアクセスした場合、顧客は、設定済みのキャプティブポータル URL にリダイレクトされます。ブラウザによってキャプティブ ポータルのコンテンツがロードされ、表示されます。顧客がポータル内のいずれかのメニューまたはリンクをクリックすると、ログイン画面が表示されます。インターネットを利用するには、顧客はここで、前述した認証手順を完了する必要があります。インターネット プロビジョニングが正常に行われると、顧客が先にクリックしていたメニューまたはリンクの Web ページが表示されます。

（注） インターネットプロビジョニングの後は、顧客は、それ以上の認証なしでポータル内のメニューやリンクに移動できます。

（注） インターネット プロビジョニング中にエラーが生じると、キャプティブ ポータルが再表示されます。

（注） キャプティブポータルで認証モジュールをインラインモジュールとして設定すると、ポータルのリンクをクリックせずに、認証プロセスを開始できます。認証モジュールをインラインモジュールとして設定する方法の詳細については、インライン認証 （121 ページ）を参照してください。

Android 4.x 以前

顧客がキャプティブ ポータル URL で設定されている SSID に接続すると、[Sign in to {SSID name}] オプションが通知領域に表示されます。通知をクリックすると、Android 4.x 以前を搭載したデバイスでは、デフォルトのブラウザが立ち上がります。ブラウザは、デバイスによって生成される URL をロードしようとします。この URL は許可リストにない（アクセス制御リストまたはウォールドガーデンの範囲にない）ため、顧客はキャプティブポータルにリダイレクトされます。顧客がポータル内のいずれかのメニューまたはリンクをクリックすると、ポータルで設定された認証タイプに応じた内容のログイン画面が表示されます。ポータルへの認証を設定するときの詳細については、ポータルへの認証の設定 （113 ページ）を参照してください。顧客は、認証手順を実行する必要があります。認証手順は、利用規約の承認のみ、SMS 認証、Email 認証、またはソーシャル認証のいずれかです。各種認証タイプの認証手順の詳細については、顧客の認証手順（181 ページ）を参照してください。必要な認証手順が完了すると、

Cisco DNA Spaces が、当該のデバイスにインターネットプロビジョニングをするよう、ワイヤレスネットワーク（CUWN、Meraki）に要求を送信します。インターネットプロビジョニングが正常に行われると、同じブラウザに、顧客が先にクリックしていたメニューまたはリンクの Web ページが表示されます。

（注） インターネットプロビジョニングの後は、顧客は、それ以上の認証なしでポータル内のメニューやリンクに移動できます。

（注） インターネット プロビジョニング中にエラーが生じると、キャプティブ ポータルが再表示されます。

（注） キャプティブポータルで認証モジュールをインラインモジュールとして設定すると、ポータルのリンクをクリックせずに、認証プロセスを開始できます。認証モジュールをインラインモジュールとして設定する方法の詳細については、インライン認証 （121 ページ）を参照してください。

Windows Phone

顧客がキャプティブ ポータル URL で設定されている SSID に接続すると、Captive Network Assistant（CNA）が表示されます。CNA によってキャプティブ ポータル URL のコンテンツがロードされ、表示されます。顧客がポータル内のいずれかのメニューまたはリンクをクリックすると、ポータルで設定された認証タイプに応じた内容のログイン画面が表示されます。ポータルへの認証を設定するときの詳細については、ポータルへの認証の設定 （113 ページ）を参照してください。顧客は、認証手順を実行する必要があります。認証手順は、利用規約の承認のみ、SMS 認証、Email 認証、またはソーシャル認証のいずれかです。各種認証タイプの認証手順の詳細については、顧客の認証手順 （181 ページ）を参照してください。必要な認証手順が完了すると、Cisco DNA Spaces が、当該のデバイスにインターネットプロビジョニングをするよう、ワイヤレスネットワーク（CUWN、Meraki）に要求を送信します。インターネットプロビジョニングが正常に行われると、CNA ウィンドウは破棄されます。

（注） インターネット プロビジョニング中にエラーが生じると、キャプティブ ポータルが再表示されます。

（注） キャプティブポータルで認証モジュールをインラインモジュールとして設定すると、ポータルのリンクをクリックせずに、認証プロセスを開始できます。認証モジュールをインラインモジュールとして設定する方法の詳細については、インライン認証 （121 ページ）を参照してください。

Windows PC とラップトップ

顧客が、キャプティブポータル URL で設定されている SSID に正常に接続した後で、許可リストにない（アクセス制御リストやウォールドガーデンの範囲にない）URL を参照した場合、顧客は、その SSID のために設定されているキャプティブポータルページにリダイレクトされます。顧客がポータル内のいずれかのメニューまたはリンクをクリックすると、ポータルで設定された認証タイプに応じた内容のログイン画面が表示されます。ポータルへの認証を設定するときの詳細については、ポータルへの認証の設定 （113 ページ）を参照してください。顧客は、認証手順を実行する必要があります。認証手順は、利用規約の承認のみ、SMS 認証、Email 認証、またはソーシャル認証のいずれかです。各種認証タイプの認証手順の詳細については、顧客の認証手順 （181 ページ）を参照してください。必要な認証手順が完了すると、Cisco DNA Spaces が、当該のデバイスにインターネット プロビジョニングをするよう、ワイヤレスネットワーク（CUWN、Meraki）に要求を送信します。インターネット プロビジョニングが正常に行われると、同じブラウザに、顧客が先にクリックしていたメニューまたはリンクの Web ページが表示されます。

Windows 10 の場合、顧客がキャプティブ ポータル URL で設定されている SSID に接続すると、Captive Network Assistant（CNA）が表示されます。CNA によってキャプティブ ポータル URL のコンテンツがロードされ、表示されます。顧客がポータル内のいずれかのメニューまたはリンクをクリックすると、ポータルで設定された認証タイプに応じた内容のログイン画面が表示されます。ポータルへの認証を設定するときの詳細については、ポータルへの認証の設定 （113 ページ）を参照してください。顧客は、認証手順を実行する必要があります。認証手順は、利用規約の承認のみ、SMS 認証、Email 認証、またはソーシャル認証のいずれかです。各種認証タイプの認証手順の詳細については、顧客の認証手順 （181 ページ）を参照してください。必要な認証手順が完了すると、Cisco DNA Spaces が、当該のデバイスにインターネット プロビジョニングをするよう、ワイヤレスネットワーク（CUWN、Meraki）に要求を送信します。インターネット プロビジョニングが正常に行われると、CNA ウィンドウは破棄されます。

（注） インターネットプロビジョニングの後は、顧客は、それ以上の認証なしでポータル内のメニューやリンクに移動できます。

（注） インターネット プロビジョニング中にエラーが生じると、キャプティブ ポータルが再表示されます。

（注） キャプティブポータルで認証モジュールをインラインモジュールとして設定すると、ポータルのリンクをクリックせずに、認証プロセスを開始できます。認証モジュールをインラインモジュールとして設定する方法の詳細については、インライン認証 （121 ページ）を参照してください。

Macbook

顧客がキャプティブ ポータル URL で設定されている SSID に接続すると、Captive Network Assistant（CNA）ウィンドウが表示されます。CNA によってキャプティブポータルのコンテンツがロードされ、表示されます。顧客がポータル内のメニューまたはリンクをクリックすると、ポータルに設定された認証タイプに基づくログイン画面が表示されます。ポータルへの認証を設定するときの詳細については、ポータルへの認証の設定 （113 ページ）を参照してください。顧客は、認証手順を実行する必要があります。認証手順は、利用規約の承認のみ、SMS 認証、Email 認証、またはソーシャル認証のいずれかです。各種認証タイプの認証手順の詳細については、顧客の認証手順 （181 ページ）を参照してください。必要な認証手順が完了すると、Cisco DNA Spaces が、当該デバイスにインターネットをプロビジョニングをするよう、ワイヤレスネットワーク（CUWN、Meraki）にリクエストを送信します。インターネットプロビジョニングが正常に行われると、顧客のデフォルトのブラウザに、顧客が先にクリックしていたメニューまたはリンクの Web ページが表示されます。ブラウザは、顧客がクリックしていたリンクに加え、CNA 内のホーム ページを別のタブで開きます。

あるいは、顧客は、キャプティブ ポータルのウィンドウを破棄してブラウザの使用に進むこともできます。顧客が、許可リストにない（アクセス制御リストやウォールドガーデンの範囲にない）URL にアクセスした場合、顧客は設定済みのキャプティブポータル URL にリダイレクトされます。ブラウザによってキャプティブ ポータル URL のコンテンツがロードされ、表示されます。顧客がポータル内のいずれかのメニューまたはリンクをクリックすると、ログイン画面が表示されます。インターネットを利用するには、顧客はここで、前述した認証手順を完了する必要があります。インターネットプロビジョニングが正常に行われると、同じブラウザに、顧客が先にクリックしていたメニューまたはリンクの Web ページが表示されます。

（注） インターネットプロビジョニングの後は、顧客は、それ以上の認証なしでポータル内のメニューやリンクに移動できます。

（注） インターネット プロビジョニング中にエラーが生じると、キャプティブ ポータルが再表示されます。

（注） キャプティブポータルで認証モジュールをインラインモジュールとして設定すると、ポータルのリンクをクリックせずに、認証プロセスを開始できます。認証モジュールをインラインモジュールとして設定する方法の詳細については、「インライン認証 （121 ページ）」を参照してください。

顧客の認証手順

さまざまな認証タイプで、インターネットを利用できるようにするために顧客が完了する必要がある認証手順は、次のとおりです。

リンク検証付き SMS による認証の手順

「リンク検証付き SMS」による認証を完了するには、次の手順を実行します。

ステップ 1 キャプティブ ポータルで、いずれかのメニュー アイテムをクリックまたはタップします。

ステップ 2 表示されるログイン画面で、携帯電話の番号を入力します。

（注） [Data Capture] モジュールが設定されている場合、帯電話番号フィールドを含むデータキャプチャフォームが表示されます。

ステップ 3 データキャプチャフォームに携帯電話番号とすべての必須フィールドを入力し、[Accept Terms and Continue] を押します。

インターネット接続が提供され、ポータルにアクセスするためのリンクが含まれた SMS が、入力した携帯電話の番号に送信されます。

ステップ 4 SMS 内のリンクをクリックして、フィンガープリント検証を行います。

フィンガープリント検証の詳細については、フィンガープリントの検証 （183 ページ）を参照してください。

（注） 顧客が一定時間内に SMS 内のリンクをクリックしなかった場合、[Skip] ボタンが表示されます。顧客は、フィンガープリント検証を行わずに [Skip] ボタンをクリックして先に進むことができます。顧客が次回インターネットにアクセスしようとすると、空白の携帯電話番号フィールドが表示され、携帯電話番号の再入力が求められます。これは、顧客がフィンガープリント検証を完了するまで、すべてのインターネットアクセスに対して発生します。

リンク検証付き SMS でのリピートユーザーの認証手順

さまざまなシナリオでのリピート ユーザの認証手順は、次のとおりです。

- **指紋認証を完了している（[Data Capture] モジュールが設定されていない）**：顧客がメニュー項目をクリック/タップすると、インターネットが提供されます。
- **指紋認証を完了している（[Data Capture] モジュールが設定され、[Data Capture] フォームに入力されている）**：顧客がメニュー項目をクリック/タップすると、インターネットが提供されます。
- **指紋認証を完了しているが、[Data Capture] フォームに入力されてない、または一部が入力されている（必須フィールド以外）**：顧客がメニュー項目をクリック/タップすると、インターネットが提供されます。ただし、[Data Capture] フォームに変更がある場合は、[Data Capture] フォームが表示されます。
- **指紋認証は完了していないが [Data Capture] フォームに入力されている**：顧客がメニュー項目をクリックまたはタップすると、事前に入力された [Data Capture] フォームとともに携帯電話番号フィールドが表示されます。インターネットにアクセスするには携帯電話番号を再度入力する必要があります。これは、顧客が指紋認証を完了するまで、すべてのインターネットアクセス試行に対して継続されます。
- **前回のインターネットアクセス中に携帯電話番号の検証プロセスが完了していなかった**：所定の時間内に検証プロセスが完了しなかった場合、無効な携帯電話番号に対してもインターネットが提供されます。このようなリピートユーザーの場合、キャプティブポータルが読み込まれ、顧客がポータル内のメニュー項目またはリンクをクリックすると、ログイン画面に携帯電話番号フィールドが表示されます。有効な携帯電話番号を入力する必要があります。
- **[Data Capture] モジュールが設定されており、登録情報が無効化している**：キャプティブポータルがロードされ、顧客がポータル内のいずれかのメニューアイテムまたはリンクをクリックすると、以前に入力されたデータを含む登録フォームが表示されます。顧客は、フォームを更新して [Connect] を押すと、インターネットにアクセスできます。

  以下は、登録情報が無効化するシナリオの一部です。

  - **新規必須フィールドを追加**：[Data Capture] モジュールに新規必須フィールドを追加した場合。たとえば、次のような場合です。[Gender] フィールドなしで [Data Capture] モジュールを設定。顧客が登録を完了。その後、[Data Capture] モジュールに [Gender] フィールドを必須フィールドとして追加。
  - **オプションのフィールドが必須になった場合**：[Data Capture] モジュールが変更され、顧客が登録時に入力しなかった任意フィールドを必須フィールドとした場合。たとえば、次のような場合です。[Last Name] を任意にして [Data Capture] モジュールを設定。顧客は SSID に接続し、姓を入力せずに登録を完了。その後、[Data Capture] モジュールを変更し、[Last Name] を登録のために必須とする。
  - **選択肢を変更した場合**：選択可能だった選択肢が削除または置き換えられた場合。たとえば、次のような場合です。「Child」および「Adult」という選択肢を伴う必須のビジネス タグ、「Age Criteria」を設定。顧客は「Age Criteria」に「Child」を選択して登録を完了。その後、選択肢の表示を「Kids」と「Adult」に変更。

（注） 上記のすべてのシナリオで、定義済みの利用規約が変更された場合は、[Accept Terms and Continue]ボタンが表示されます。インターネットにアクセスしたり、次の認証手順に進んだりするには、顧客は [Accept Terms and Continue] ボタンを押す必要があります。

フィンガープリントの検証

顧客が「リンク検証付き SMS」認証用の携帯電話番号を提供すると、提供された携帯電話番号にリンク付きのメッセージが送信され、インターネットのプロビジョニングが行われます。フィンガープリント検証は、顧客がメッセージ内のリンクをクリックすると実行されます。事前に定義された時間内に顧客がリンクをクリックしない場合、[SKIP] オプションを含む一時ページが顧客に表示されます。顧客が [Skip] オプションをクリックすると、フィンガープリント検証なしでインターネットにアクセスできます。

さまざまなシナリオのフィンガープリント検証ステータスを次に示します。

- 顧客がメッセージ内のリンクをクリックすると、フィンガープリントが一致した場合は顧客獲得が行われ、顧客はポータルページにリダイレクトされます。顧客は、次回の訪問時にはリピートユーザーと見なされます。
- 顧客がメッセージ内のリンクをクリックしたときにフィンガープリント検証に失敗すると（たとえば、顧客が SMS 認証の開始に使用したものとは別のブラウザでリンクを開いた場合、フィンガープリント検証は失敗します）、確認ページが顧客に表示されます。顧客が [Confirm] をクリックすると、顧客獲得が行われ、顧客はポータル ページにリダイレクトされます。顧客は、次回の訪問時にはリピートユーザーと見なされます。
- 顧客がメッセージ内のリンクをクリックしたときにフィンガープリント検証に失敗すると、顧客に確認ページが表示されます。顧客が [Cancel] をクリックすると、顧客は次回の訪問時に初回ユーザーと見なされ、ログイン画面に空白の携帯電話番号フィールドが表示されます。
- 表示された一時ページで顧客が [Skip] をクリックすると、顧客は次回の訪問時に初回ユーザーと見なされ、ログイン画面に空白の携帯電話番号フィールドが表示されます。

SMS with Password Verification 認証の手順

SMS with password verification 認証を完了するには、次の手順を実行します。

ステップ 1 キャプティブ ポータルで、いずれかのメニュー アイテムをクリックまたはタップします。

ステップ 2 表示されるログイン画面で、携帯電話の番号を入力します。

ステップ 3 顧客が通知の受け取りを停止するには、[Opt In to Receive notification] チェックボックスをオフにします。

（注） [Opt In to receive notification] チェックボックスがログイン画面に表示されるのは、ポータルの認証の詳細を設定する際、[Authentication] 画面で [Allow users to Opt in to receive message] チェックボックスをオンにしていた場合のみです。

ステップ 4 [Accept Terms and Continue] を押します。

ステップ 5 表示される画面で、SMS を通じて受け取った認証コードを入力します。

ステップ 6 [Verify] を押します。

データキャプチャフォームが設定されている場合、認証コードの検証が成功すると、データキャプチャフォームが表示されます。

ステップ 7 データキャプチャフォームのすべての必須フィールドに入力し、[Connect] を押します。

（注） すべてのフィールドが任意である場合、[Skip] と [Connect] という 2 つのボタンが表示されます。[Skip] ボタンをクリックすると、顧客はデータを入力せずに続行することができます。フォームに変更がある場合のみ、顧客が [Skip] をクリックした際、顧客に対してデータキャプチャフォームが表示されます。

登録が成功すると、インターネットプロビジョニングのプロセスが開始し、インターネットが利用できるようになります。

（注） [Data Capture] モジュールが有効でない場合、認証コードの検証後、インターネットはすぐにプロビジョニングされます。

パスワード検証付き SMS によるリピートユーザーの認証手順

さまざまなシナリオでのリピート ユーザの認証手順は、次のとおりです。

- [Data Capture is not configured]：キャプティブポータルをロードし、顧客がポータル内のいずれかのメニューアイテムまたはリンクをクリックすると、インターネットがプロビジョニングされます。
- **データキャプチャが設定されており、顧客が登録を完了している**：キャプティブポータルがロードされ、顧客がポータル内のいずれかのメニューアイテムまたはリンクをクリックすると、インターネットがプロビジョニングされます。
- **データキャプチャが設定されていない、登録詳細が古い**：キャプティブポータルをロードし、顧客がポータル内のいずれかのメニューアイテムまたはリンクをクリックすると、以前入力したデータが入ったデータキャプチャフォームが表示されます。顧客はフォームを更新して [Connect] ボタンを押すと、インターネットにアクセスできます。

  以下は、登録情報が無効化するシナリオの一部です。

  - **新規必須フィールドを追加**：データキャプチャフォームに新規必須フィールドを追加した場合。たとえば、[Gender] フィールドのないデータキャプチャフォームを設定したような場合です。顧客が登録を完了。その後、データキャプチャフォームに [Gender] フィールドを必須フィールドとして追加したような場合です。
  - **オプションのフィールドが必須になった場合**：データキャプチャフォームが変更され、顧客が登録時に入力しなかった任意フィールドが必須フィールドになっています。たとえば、次のような場合です。[LastName] を任意にしてデータキャプチャフォームを設定。顧客は SSID に接続し、姓を入力せずに登録を完了。その後、データキャプチャフォームを変更し、[Last Name] を登録のために必須とする。

- **選択肢を変更した場合**：選択可能だった選択肢が削除または置き換えられています。たとえば、次のような場合です。「Child」および「Adult」という選択肢を伴う必須のビジネス タグ、「Age Criteria」を設定。顧客は「Age Criteria」に「Child」を選択して登録を完了。その後、選択肢の表示を「Kids」と「Adult」に変更。
- **前回のログイン時に無効な電子メール ID を入力した場合**：キャプティブポータルをロードし、顧客がポータル内のいずれかのメニューアイテムまたはリンクをクリックすると、前回ログイン時に入力された無効な電子メール ID を含むデータキャプチャフォームが表示されます。続行するには、顧客は有効な電子メール ID を入力する必要があります。

（注） 上記のすべてのシナリオで、定義済みの利用規約が変更された場合は、[Accept Terms and Continue]ボタンが表示されます。顧客がインターネットにアクセス、または次の認証手順に進むには、 [Accept Terms and Continue] ボタンを押す必要があります。

電子メール認証の手順

Email 認証を完了するには、次の手順を実行します。

ステップ 1 キャプティブ ポータルで、いずれかのメニュー アイテムをクリックまたはタップします。

ステップ 2 表示されるログイン画面で、電子メール ID を入力します。

ステップ 3 顧客が通知の受け取りを停止するには、[Opt In to Receive notification] チェックボックスをオフにします。

（注） [Opt In to Receive notification] チェックボックスがログイン画面に表示されるのは、ポータルの認証の詳細を設定する際に、認証タイプ [Email] について [Allowed users to Opt in to receive message] チェックボックスをオンにしていた場合のみです。

ステップ 4 [Accept Terms and Continue] を押します。

入力された電子メール ID が有効であれば、インターネットが利用できるようになります。

ステップ 5 キャプティブポータルの認証画面でデータキャプチャが有効になっている場合、顧客が [Accept Terms and Continue] を押すと、データキャプチャフォームが表示されます。

ステップ 6 データキャプチャフォームのすべての必須フィールドに入力し、[Connect] を押します。

（注） すべてのフィールドが任意である場合、[Skip] と [Connect] という 2 つのボタンが表示されます。[Skip] ボタンをクリックすると、顧客はデータを入力せずに続行することができます。顧客が [Skip]をクリックした際、フォームに変更がある場合のみ、リピートユーザーに対してデータキャプチャフォームが表示されます。

インターネット プロビジョニングのプロセスが開始し、インターネットが利用できるようになります。

Email 認証によるリピート ユーザの認証手順

さまざまなシナリオでのリピート ユーザの認証手順は、次のとおりです。

- [Entered invalid e-mail ID during previous log in]：キャプティブポータルがロードされ、顧客がポータル内のいずれかのメニューアイテムまたはリンクをクリックすると、前回ログイン時に入力された無効な電子メール ID を含むログイン画面が表示されます。続行するには、顧客は有効な電子メール ID を入力する必要があります。
- [Data Capture is not enabled]：キャプティブポータルがロードされ、顧客がポータル内のいずれかのメニューアイテムまたはリンクをクリックすると、インターネットが利用できるようになります。
- [Data Capture is enabled, and the customer completed the registration]：キャプティブポータルがロードされ、顧客がポータル内のいずれかのメニューアイテムまたはリンクをクリックすると、インターネットが利用できるようになります。
- [Data Capture is enabled, and the registration details are outdated]：キャプティブポータルがロードされ、顧客がポータル内のいずれかのメニュー アイテムまたはリンクをクリックすると、以前に入力されたデータを含むデータキャプチャフォームが表示されます。顧客は、フォームを更新して [Connect] を押すと、インターネットにアクセスできます。

  以下は、登録情報が無効化するシナリオの一部です。

  - [Added new mandatory fields]：データキャプチャフォームに新しい必須フィールドが追加されています。たとえば、次のような場合です。[Gender] フィールドなしでデータキャプチャフォームを設定。顧客が登録を完了。その後、データキャプチャフォームに [Gender] フィールドを必須フィールドとして追加。
  - [Optional field becomes mandatory]：データキャプチャフォームが変更され、顧客が登録時に入力しなかった任意フィールドが必須フィールドになっています。たとえば、次のような場合です。[Last Name] を任意にしてデータキャプチャフォームを設定。顧客は SSID に接続し、姓を入力せずに登録を完了。その後、データキャプチャフォームを変更し、[Last Name] を登録のために必須とする。
  - **選択肢の変更**：選択可能だった選択肢が、削除または置き換えされています。たとえば、次のような場合です。「Child」および「Adult」という選択肢を伴う必須のビジネス タグ、「Age Criteria」を設定。顧客は「Age Criteria」に「Child」を選択して登録を完了。その後、選択肢の表示を「Kids」と「Adult」に変更。

（注） 上記のすべてのシナリオで、定義済みの利用規約が変更された場合は、[Accept Terms and Continue] ボタンが表示されます。インターネットにアクセスしたり、次の認証手順に進んだりするには、顧客は [Accept Terms and Continue] ボタンを押す必要があります。

アクセスコード認証の手順

「アクセスコード」認証を完了するには、次の手順を実行します。

ステップ 1 キャプティブ ポータルで、いずれかのメニュー アイテムをクリックまたはタップします。

ステップ 2 表示されるログイン画面で、アクセスコードを入力します。

ステップ 3 顧客が通知の受け取りを停止するには、[Opt In to Receive notification] チェックボックスをオフにします。

（注） [Opt In to receive notification] チェックボックスがログイン画面に表示されるのは、ポータルの認証の詳細を設定する際、[Authentication] 画面で [Allow users to Opt in to receive message] チェックボックスをオンにしていた場合のみです。

ステップ 4 [Accept Terms and Continue] を押します。

ステップ 5 [Verify] を押します。

[Data Capture] が有効である場合、アクセスコードの検証が成功すると、データキャプチャフォームが表示されます。

ステップ 6 登録のためのすべての必須フィールドに入力し、[Connect] を押します。

（注） すべてのフィールドが任意である場合、[Skip] と [Connect] という 2 つのボタンが表示されます。[Skip] ボタンをクリックすると、顧客はデータを入力せずに続行することができます。フォームに変更がある場合のみ、顧客が [Skip] をクリックした際に、顧客に対して登録フォームが表示されます。

登録が成功すると、インターネット プロビジョニングのプロセスが開始し、インターネットが利用できるようになります。

（注） [Data Capture] モジュールが有効でない場合、認証コードが検証されると、すぐにインターネット接続が提供されます。

アクセスコード認証によるリピートユーザーの認証手順

さまざまなシナリオでのリピート ユーザの認証手順は、次のとおりです。

- **データキャプチャが設定されていない**：キャプティブポータルをロードし、顧客がポータル内のいずれかのメニューアイテムまたはリンクをクリックすると、インターネットがプロビジョニングされます。
- **データキャプチャが設定されていない、顧客が登録を完了している**：キャプティブポータルをロードし、顧客がポータル内のいずれかのメニューアイテムまたはリンクをクリックすると、インターネットがプロビジョニングされます。
- **データキャプチャが設定されていない、登録詳細が古い**：キャプティブポータルをロードし、顧客がポータル内のいずれかのメニューアイテムまたはリンクをクリックすると、以前入力したデータが入ったデータキャプチャフォームが表示されます。顧客はフォームを更新して [Connect] ボタンを押すと、インターネットにアクセスできます。

以下は、登録情報が無効化するシナリオの一部です。

- **新規必須フィールドを追加**：データキャプチャフォームに新規必須フィールドを追加した場合。たとえば、[Gender] フィールドのないデータキャプチャフォームを設定し、顧客が登録を完了。その後、データキャプチャフォームに [Gender] フィールドを必須フィールドとして追加した場合などです。
- **オプションのフィールドが必須になった場合**：データキャプチャフォームが変更され、顧客が登録時に入力しなかった任意フィールドが必須フィールドになっています。たとえば、次のような場合です。[LastName] を任意にしてデータキャプチャフォームを設定。顧客は SSID に接続し、姓を入力せずに登録を完了。その後、データキャプチャフォームを変更し、フォームの [Last Name] を必須とした場合などです。
- **選択肢を変更した場合**：選択可能だった選択肢が削除または置き換えられています。たとえば、次のような場合です。「Child」および「Adult」という選択肢を伴う必須のビジネス タグ、「Age Criteria」を設定。顧客は「Age Criteria」に「Child」を選択して登録を完了。その後、選択肢の表示を「Kids」と「Adult」に変更。
- **前回のログイン時に無効な電子メール ID を入力した場合**：キャプティブポータルをロードし、顧客がポータル内のいずれかのメニューアイテムまたはリンクをクリックすると、前回ログイン時に入力された無効な電子メール ID を含むデータキャプチャフォームが表示されます。続行するには、顧客は有効な電子メール ID を入力する必要があります。

（注） 上記のすべてのシナリオで、定義済みの利用規約が変更された場合は、[Accept Terms and Continue] ボタンが表示されます。顧客がインターネットにアクセス、または次の認証手順に進むには、 [Accept Terms and Continue] ボタンを押す必要があります。

利用規約による認証省略の手順

顧客へのインターネットプロビジョニングを、顧客が利用規約を承認することのみを条件として行うように設定することができます。

利用規約の承認のみが必要な認証を完了するには、次の手順を実行します。

ステップ 1 キャプティブ ポータルで、いずれかのメニュー アイテムをクリックまたはタップします。

ステップ 2 表示されるログイン画面で、[Accept Terms and Continue] を押します。

インターネット プロビジョニングのプロセスが開始し、インターネットが利用できるようになります。

利用規約の承認によるリピート ユーザの認証手順

キャプティブ ポータルがロードされ、顧客がポータル内のいずれかのメニュー アイテムまたはリンクをクリックすると、インターネットが利用できるようになります。

（注） 定義済みの利用規約が変更された場合は、[Accept Terms and Continue] ボタンが表示されます。インターネットにアクセスしたり、次の認証手順に進んだりするには、顧客は [Accept Terms and Continue] ボタンを押す必要があります。

ソーシャル認証の手順

ポータルへのソーシャル認証を完了するには、次の手順を実行します。

ステップ 1 顧客がキャプティブ ポータル内のいずれかのメニューアイテムまたはリンクをクリックすると、ポータルへのすべての Social Sign In オプションが使用できる画面が表示されます。

（注） サインイン オプションは、ポータルに設定されているソーシャル ネットワークのみに表示されます。ポータルに対してソーシャルネットワークを設定する方法の詳細については、Social Sign In 認証のためのポータル設定 （117 ページ）を参照してください。

ステップ 2 認証を完了するために使用するソーシャル ネットワークのサインイン オプションをクリックします。ソーシャル ネットワークのログイン ページが表示されます。

たとえば、LinkedIn のサインインオプションをクリックすると、LinkedIn のログイン画面が表示されます。

ステップ 3 ソーシャル ネットワークのログイン クレデンシャルを入力して、ログイン ボタンを押します。

ステップ 4 表示される画面で、[Allow] を押します。

リダイレクト URI がロードされ、[Terms and Conditions] 画面が表示されます。

ステップ 5 [Accept Terms and Continue] を押します。

（注） Facebook および Twitter には、リダイレクト URI の設定は不要です。リダイレクト URI は、Linked In の場合に設定が必要です。Linked In のリダイレクト URI を設定するときの詳細については、ソーシャル認証のためのアプリケーションの設定 （165 ページ）を参照してください。

ステップ 6 インターネット プロビジョニングが行われると、[Continue] ウィンドウが表示されます。

ステップ 7 先にクリックしていたリンクのページを表示するには、[Continue] を押します。

ソーシャル認証によるリピート ユーザの認証手順

キャプティブ ポータルがロードされ、顧客がポータル内のいずれかのメニュー アイテムまたはリンクをクリックすると、設定されているすべてのソーシャル ネットワークについて、接続のためのオプションが表示されます。顧客が以前に認証のために使用したソーシャル ネット

ワークは、「Continue with [social network]」というラベルで表示されます。たとえば、顧客が以前、キャプティブ ポータルを通じたインターネットへのアクセスに Facebook 認証を使用していた場合、Facebook のオプションが、[Continue with Facebook] というラベルで表示されます。これまで認証に使用されていないソーシャル ネットワークについては、サインイン オプションが表示されます。たとえば、[Signin with Linkedin] です。

- 顧客が以前に認証のために使用したソーシャルネットワークを継続して使用する場合、インターネットは、認証プロセスなしで利用できます。ただし、利用規約に変更がある場合は、[Terms and Conditions] 画面が表示されます。このとき、インターネットにアクセスするには、顧客は [Accept Terms and Continue] ボタンを押す必要があります。
- 顧客がこれまで認証に使用されていないソーシャルネットワークを使用してサインインする場合、顧客は、そのソーシャルネットワークの認証プロセスの全体を完了する必要があります。顧客がいずれかのソーシャルネットワークを介したソーシャル認証を使用してインターネットにアクセスした場合、認証プロセス中に [Terms and Conditions] 画面は表示されません。ただし、利用規約に変更がある場合は、認証プロセス中に [Terms and Conditions] 画面が表示されます。このとき、インターネットにアクセスするには、顧客は [Accept Terms and Continue] ボタンを押す必要があります。

キャプティブポータルのスマートリンクとテキスト変数

スマートリンク

[Smart Link] オプションにより、パーソナライズされた Web ページやメッセージを顧客に提供することができます。[Smart Link] オプションを使用して、キャプティブポータル内のカスタムメニューリンクへの URL をカスタマイズし、パーソナライズされたビューを提供することができます。サイトのページをユーザ別またはユーザのグループ別にパーソナライズすることができます。

たとえば、ポータル内のカスタム メニュー アイテムに「optedinstatus」パラメータを設定することができます。これにより、このカスタムメニューアイテムの Web ページで「オプトイン」ユーザーと「非オプトイン」ユーザーに対して異なるコンテンツを表示するよう設定することができます。オプトイン ユーザがキャプティブ ポータルでカスタム メニュー リンクをクリックすると、オプトインユーザ用のコンテンツが表示されます。非オプトインユーザーが同じカスタムメニューリンクをクリックすると、非オプトインユーザー用のコンテンツが表示されます。

（注） これらのパラメータを使用して顧客にパーソナライズされたビューを表示するためには、Web ページをそれに応じて設定する必要があります。

キャプティブポータルアプリで、スマートリンクを以下のオプションに含めることができます。

- ポータルに追加されたカスタム メニュー アイテムに追加されたリンク

- トリガー API の **URI** フィールドに追加された URL。

テキスト変数

テキスト変数を使用することで、**Trigger API** を使用して API エンドポイントに送信されるメッセージに、名前、携帯電話番号、性別などの顧客の個人情報を追加できます。デフォルトでは、メッセージには顧客の姓名が記載されます。この変数を使用して、さらに顧客の詳細を追加できます。

たとえば、Trigger API 通知を作成し、SMS 通知の [message] テキストボックスに変数「mobile」および「gender」を設定していたとします。この場合、顧客がこのエンゲージメントルールに基づく SMS メッセージを受信すると、メッセージには、顧客の携帯電話の番号と性別の詳細も表示されます。

次のオプションで変数を追加できます。

- **Trigger API** を使用して API エンドポイントに送信されるメッセージ。
- 初めてのユーザーとリピーターのユーザーへのウェルカムメッセージ。
- ポータルに追加された通知（バックエンドサポートのみ）。

Cisco DNA Spaces は、データキャプチャフォームを使用して顧客の個人情報をキャプチャします。つまり、スマートリンクまたはテキスト変数に名、姓、性別などの個人に関する詳細を含めるためには、ポータルにデータキャプチャフォームを設定する必要があります。キャプティブポータルへのデータキャプチャフォームの追加の詳細については、「ポータルへのデータキャプチャフォームの追加」セクションを参照してください。

（注） 「SMS with link verification」と「SMS with password verification」メッセージに含まれるキャプティブポータルの URL は、スマートリンク機能ではサポートされません。

Cisco DNA Spaces は、特定の定義済み変数を提供します。Web ページのパーソナライズされたビューの提供と、通知メッセージへの顧客の詳細の追加には、これらの変数を使用する必要があります。

スマートリンクには、静的変数と動的変数を含めることができます。

スマートリンクまたはテキストに含めることができる静的パラメータは、次のとおりです。

表 7: 静的変数一覧

静的変数名	説明
$location または **$locationName**	ルールがトリガーされるロケーションの名前。
$Address	[Location Hierarchy] の [Location Info] ウィンドウでロケーションに設定されたアドレス。
$State	[Location Hierarchy] の [Location Info] ウィンドウでロケーションに設定されたステート。

静的変数名	説明
$Country	[Location Hierarchy] の [Location Info] ウィンドウでロケーションに設定された国。
$City	[Location Hierarchy] の [Location Info] ウィンドウでロケーションに設定された市区町村。
$TotalAreaValue	[Location Hierarchy] の [Location Info] ウィンドウのロケーションに設定されたエリア合計。
$firstName（ウェルカムモジュールの初回訪問者には適用されません）。	顧客の名前。
$lastName（ウェルカムモジュールの初回訪問者には適用されません）。	顧客の姓。
次の変数は [Welcome] モジュールには適用されませんが、[Custom] モジュールとトリガー API にのみ適用されます。	
$email	顧客の電子メールアドレス。
$mobile	顧客の携帯電話番号。
$gender	顧客の性別。
$URL	URL リンク値。
$macaddress	デバイスの MAC アドレス。
$encryptedMacAddress	暗号化された、デバイスの MAC アドレス。
$deviceSubscriberId	データベース内のデバイスのサブスクライバ ID。
$optinStatus	顧客のオプトインステータス。

さらに、スマートリンクまたはテキストには、次の動的変数を含めることができます。

表 *8*: 動的変数一覧

動的変数名	説明
Business Tags	顧客が属するビジネスタグ。データキャプチャフォームで設定されるビジネスタグは、変数としてリストされます。ビジネスタグの作成の詳細については、「ポータルへのデータキャプチャフォームの追加」セクションを参照してください。

動的変数名	説明
Location Metadata	顧客のロケーションのロケーションメタデータ。ロケーション階層で定義されたロケーションメタデータのキーは、変数としてリストされます。ロケーションメタデータの定義の詳細については、「ロケーションのメタデータの追加のセクションを参照してください。

URL にスマートリンクを、またはテキストに変数を挿入するには、次の手順を実行します。

ステップ 1 URL フィールドまたはテキストボックスの任意の場所をクリックするか、対応する [Add Variable] ドロップダウンリストをクリックします。

追加できる変数がリストされています。

ステップ 2 追加する変数を選択します。

第 10 章

Engagements アプリによる通知の送信

Cisco DNA Spaces は、Cisco DNA Spaces に対応した施設内にいる顧客を識別する WiFi ビーコンとして機能し、定義されたエンゲージメントルールに基づいて顧客とビジネスユーザーに通知を送信します。

この章では、ビジネスの構内に近い顧客に通知を送信できるようにするエンゲージメントルールを作成する方法について説明します。顧客は、ビジネスの構内から以前購入したことがあるユーザ、潜在的な購入者、訪問者のいずれかにすることができます。また、従業員などのビジネス ユーザまたは API エンド ポイントに対して通知を送信するようにエンゲージメント ルールを設定することもできます。たとえば、カスタマーケア担当者が顧客に付加価値サービスを提供できるように、権限のある顧客が構内に入るとカスタマーケア担当者に通知するエンゲージメント ルールを設定できます。

顧客の WiFi への接続状況に基づいて通知を送信するように設定できます。

（注） エンゲージメントルールは、ルールで指定したロケーションに定義されているすべての SSID に対して適用されます。

エンゲージメントルール作成の前提条件

- 通知を送信するには、ワイヤレス ネットワーク システムで一定の設定を行う必要があります。
  - 使用するワイヤレスネットワークが Cisco Meraki の場合は、通知およびレポート用 Cisco Meraki の設定 （303 ページ）で説明されている設定を行います。
  - 使用するワイヤレスネットワークが Cisco AireOS または Cisco Catalyst の場合は、通知およびレポート用のシスコ ワイヤレス コントローラ（Cisco CMX なし）の設定（266 ページ）で説明されている設定を行います。
  - 使用するワイヤレスネットワークが Cisco Catalyst の場合は、モードおよびコネクタに応じて、次のいずれかの設定を行います。
    - CLI を使用したキャプティブポータルおよびエンゲージメントアプリ用の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ（ローカルモード）の設定 （268 ページ）
    - キャプティブポータルおよびエンゲージメントアプリ用の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ GUI（ローカルモード） （272 ページ）
    - キャプティブポータルおよびエンゲージメントアプリ用の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ GUI（フレックスモードまたは Mobility Express）（278 ページ）
- エンゲージメントルールを適用可能なロケーションを指定するには、ロケーション階層を定義する必要があります。ロケーション階層の定義の詳細については、ロケーション階層の概要 （25 ページ）を参照してください。
- ルールを適用可能なタグを指定するには、タグを定義する必要があります。タグの作成の詳細については、ロケーションペルソナアプリを使用したタグの作成または変更 （219 ページ）を参照してください。
- キャプティブポータルにサインインした顧客の姓名などの詳細を外部 API に送信するには、キャプティブポータルでデータキャプチャフォームを設定する必要があります。データキャプチャフォームがない場合、デバイスの MAC アドレスなどの情報のみが外部 API に送信されます。データキャプチャフォームの設定の詳細については、ポータルへのデータキャプチャフォームの追加 （122 ページ）を参照してください。

エンゲージメント ルールの作成

エンゲージメントルールとは、対象ユーザに送信される通知に基づく条件のことです。顧客および従業員などのビジネスユーザ、またはAPIエンドポイントに対してエンゲージメントルールを作成できます。

通知を送信する頻度を設定できます。また、通知を送信するための必要条件を定義できます。通知は単一ユーザまたは複数のロケーションのユーザ グループに送信するように設定できます。

顧客の場合、SMS または電子メールを通じて通知を送信できます。ビジネスユーザーの場合、Cisco Webex Teams、SMS、電子メールを通じて、または外部 API に対して通知を送信できます。顧客とビジネスユーザーの場合、SSID に対する顧客の接続に基づいて通知を送信するように設定することができます。ユーザが複数の形式の通知を取得できるように、エンゲージメントルールには複数の通知タイプを設定できます。これにより、通知がユーザに通知される確率が向上します。

顧客に対するエンゲージメント ルールの作成

SMS または電子メールを通じて、顧客に通知を送信できます。

顧客に通知を送信するエンゲージメント ルールを定義するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Engagements] を選択します。

ステップ 2 表示される [Engagements] ウィンドウで、[Create New Rule] をクリックします。

ステップ 3 [Rule Name] フィールドに、新しいエンゲージメントルールの名前を入力します。

ステップ 4 [When a user is on WiFi and] ドロップダウンリストから、次のいずれかを選択します。

- [Entering Location]：Wi-Fi に接続されている訪問者がロケーションに入ると通知が送信されるようにするには、このオプションを選択します。
- [Away from the Location]：Wi-Fi に接続されている訪問者が指定された時間ロケーションを離れると通知が送信されるようにするには、このオプションを選択します。このオプションを選択している場合、[For] スクロールリストから、通知を送信するために訪問者がロケーションから離れている必要がある分数を選択します。

  （注）
  - [Exiting Location] オプションは使用できなくなりました。[Exiting Location] が設定されている既存のエンゲージメントルールを編集している場合は、[Choose User Activity] ドロップダウンリストが、オプションが選択されていない状態で表示されます。ルールを正常に保存するには、[Choose User Activity] ドロップダウンリストから必要なオプションを選択する必要があります。
  - 訪問者がロケーションに物理的に存在していても、[For] スクロールリストで指定された分数の間 Wi-Fi から切断されていれば、訪問者は通知の送信対象と見なされます。

- [Present at location]：訪問者が Wi-Fi に接続され、指定された期間または特定の時刻にロケーションにいると通知が送信されるようにするには、このオプションを選択します。このオプションを選択すると、追加のフィールドが表示されて、顧客がこのルールの対象としてフィルタリングされるための期間または時刻を指定できます。

ステップ 5 [Locations] 領域で、通知を送信するロケーションを指定します。

お客様名全体または単一または複数のロケーション（グループ、フロア、グループ、ゾーンなど）に対して通知の送信を設定できます。エンゲージメントルールに、Cisco Meraki、シスコ ワイヤレス コントローラなどの異なるワイヤレスネットワークのロケーションを追加できます。

選択したロケーションまたはその親あるいは子のロケーションに対して定義されているメタデータに基づいて、通知を送信するロケーションを再度フィルタリングすることもできます。特定のメタデータを持つロケーションに対して通知を送信することも、特定のメタデータを持つロケーションを除外することもできます。エンゲージメントルールのロケーションを定義する方法の詳細については、エンゲージメントルールのロケーションフィルタ （210 ページ）を参照してください。

ステップ 6 [IDENTIFY] 領域で、通知を送信する顧客のタイプを指定します。

（注） 通知を送信する顧客は、顧客がオプトインユーザーかどうか、顧客が属するタグ、顧客の訪問回数に基づいてフィルタリングすることができます。これらのフィルタをすべて適用することも、要件に応じて一部を適用することもできます。

通知を送信する顧客を指定するには、次の手順を実行します。

a) オプトインステータスにより顧客をフィルタリングする場合、[Filter by Opt-In Status] チェックボックスをオンにして、オプトインユーザーまたは非オプトインユーザーのどちらに通知を送信するかを選択します。
b) タグに基づいて顧客をフィルタリングするには、[Filter by Tags] チェックボックスをオンにします。

（注） 2つの異なる方法でタグをフィルタリングできます。通知を送信するタグを指定するか、通知を送信してはならないタグを指定することができます。要件に基づいて、最適なフィルタリング方法を選択できます。たとえば、1つのタグを除いてすべてのタグに対して通知を送信する場合、除外項目を選択するのは簡単です。

c) 選択したロケーションにおける顧客の訪問数に基づいて顧客をフィルタリングするには、[Filter by Previous Visits] チェックボックスをオンにします。[Add Locations] ボタンをクリックします。[Choose Locations] ウィンドウで、顧客の訪問をフィルタリングの条件にする必要があるロケーションを指定します。次のフィールドで、通知を送信するために必要な訪問回数および継続時間を指定します。

ステップ 7 [Schedule] 領域で、ルールを適用する期間を指定します。

a) [Set a date range for the rule] チェックボックスをオンにし、表示されるフィールドで、エンゲージメントルールを適用する期間の開始日と終了日を指定します。
b) [Set a time range for the rule] チェックボックスをオンにし、表示されるフィールドで、指定した日付範囲内でのエンゲージメントルールを適用する時間範囲を指定します。
c) 特定の日にのみエンゲージメントルールを適用する場合、[Filter by days of the week] チェックボックスをオンにし、表示される曜日のリストから通知を送信する曜日をクリックします。

ステップ 8 [Actions] 領域で、次の手順を実行します。

a) [Notify] ドロップダウンリストから [Consumer] を選択し、隣のドロップダウンリストから次のいずれかを選択します。

- [Only Once]：通知は一度だけ顧客に送信されます。
- [Once In]：通知は指定した通知頻度に基づいて複数回顧客に送信されます。このオプションを選択すると表示される追加のフィールドで、通知頻度を指定します。

b) 通知のモードを指定します。電子メールまたはSMSを通じて、顧客に通知を送信できます。通知タイプの詳細については、消費者用の通知タイプ （211 ページ）を参照してください。

（注） [Via Email] の場合、[From] フィールドに入力する電子メール ID は、電子メール ID の許可リストに含まれている必要があります。電子メール ID を許可リストに含める方法については、Cisco DNA Spaces サポートチームにお問い合わせください。特定の電子メール ID を使用しない場合は、デフォルトで許可されている電子メール ID である **no-reply@dnaspaces.io** を使用できます。ただし、このデフォルト ID が自動的にダッシュボードに表示されることはありません。そのため、手動で入力する必要があります。

ルールの概要がウィンドウの右側に表示されます。

ステップ 9 **[Save and Publish]** をクリックします。

ルールが [Engagement Rules] ページのリストにパブリッシュされます。

（注） ルールを今すぐパブリッシュしたくない場合、[Save] ボタンをクリックします。[Save and Publish] ボタンをクリックすることで、後でいつでもルールをパブリッシュできます。また、[Engagement Rules] ページの右端にある [Make Rule Live] アイコンをクリックして、ルールをパブリッシュすることもできます。

使用例：顧客用のエンゲージメントルール

小売店 ABC は欧州全域に店舗があります。サマーセールの一環として、ABC は顧客に対してオファーを提供することを決めました。オファーは、ロケーション A の ABC 店舗とロケーション B のフロア 1 を訪れる顧客のみが対象です。今年 5 回以上 ABC のいずれかの店舗を訪問したすべての顧客がオファーの対象者です。ABC は、今年 5 回以上 ABC のいずれかの店舗を訪問した顧客に対してオファーに関する通知を送信します。通知は、顧客が Wi-Fi に接続してロケーション A またはロケーション B のフロア 1 に入るときに送信する必要があります。オファーは週末の間だけなので、通知は週末にのみ送信します。通知はオプトインユーザーに 2 週間だけ送信されます。ABC は、訪問時に毎回、電子メールで通知を送信します。

上記のシナリオの条件を満たすには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces にログインします。

ステップ 2 ABC のすべてのロケーションを含むロケーション階層を作成します。

ステップ 3 Cisco DNA Spaces ダッシュボードで、[Engagements] をクリックします。

ステップ 4 表示される [Engagements] ページで、[Create New Rule] をクリックします。

ステップ 5 [Rule Name] フィールドに、新しいエンゲージメントルールの名前を入力します。

ステップ 6 [When a user is on Wi-Fi and] ドロップダウンリストから、[Entering Location] を選択します。

ステップ 7 [Locations] 領域で、ロケーションを選択するために [Add Locations] ボタンをクリックし、ロケーション A およびロケーション B のフロア 1 を選択します。

ステップ 8 [Identify] エリアで、以下を実行します。

a) [Filter by Opt-In Status] チェックボックスをオンにし、[Only for opted-in Visitor] を選択します。
b) [Filter by Previous Visits] チェックボックスをオンにし、[Add Locations] ボタンをクリックします。顧客名（ルート名）のチェックボックスをオンにし、ABC の全ロケーションへの訪問を考慮して、[Done] をクリックします。
c) 次のドロップダウンリストから、[At least, 5 Times in This Year] を選択します。

ステップ 9 [Schedule] エリアで、以下を実行します。

a) [Set a date range for the rule] チェックボックスをオンにし、オファーを提供する 2 週間の日付範囲を指定します。必要に応じて、時間も設定します。
b) [Filter by days of the week] チェックボックスをオンにし、[Sat] および [Sun] をクリックします。

ステップ 10 [Actions] 領域で、以下を実行します。

a) [Notify] ドロップダウンリストから、[Consumer] を選択します。
b) 隣接する 3 つのドロップダウンリストから、[Once in, 1]、および [Visits] をそれぞれ選択します。
c) [Via Email] チェックボックスをオンにします。
d) [From Name] フィールドに、顧客に表示する必要がある電子メール名を入力し、[From Email] フィールドに、顧客に表示する必要がある電子メール ID を入力します。
e) [Subject] フィールドに、電子メールの件名を入力します。必要に応じて、次のテキスト ボックスのメッセージを編集します。
f) [Via SMS] チェックボックスをオンにして、SMS ゲートウェイを指定します。必要に応じて、次のテキスト ボックスの内容を編集します。

（注） この設定の目的は、アプリケーションの通知が失敗した場合にも通知を送信することです。また、アプリケーション ユーザではない顧客は SMS によって通知を取得します。

ステップ 11 [Save and Publish] をクリックします。

ルールがパブリッシュされます。

ビジネス ユーザに対するエンゲージメント ルールの作成

エンゲージメントルールを作成する前に、前提条件が満たされていることを確認してください。エンゲージメントルールを作成するための前提条件の詳細については、「エンゲージメントルール作成の前提条件」のセクションを参照してください。

Cisco Webex Teams、SMS または電子メールを使用して、従業員などのビジネスユーザーに通知を送信できます。外部 API に通知を送信することもできます。

ビジネス ユーザまたは外部 API に通知を送信するエンゲージメント ルールを定義するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Engagements] をクリックします。
ステップ 2 表示される [Engagements] ウィンドウで、[Create New Rule] をクリックします。
ステップ 3 [Rule Name] フィールドに、新しいエンゲージメントルールの名前を入力します。

ステップ 4 [When a user is on WiFi and] ドロップダウンリストから、次のいずれかを選択します。

- [Entering Location]：Wi-Fi に接続されている訪問者がロケーションに入るとビジネスユーザーに通知が送信されるようにするには、このオプションを選択します。
- [Away from the Location]：Wi-Fi に接続されている訪問者が指定された時間ロケーションを離れるとビジネスユーザーに通知が送信されるようにするには、このオプションを選択します。このオプションを選択している場合、[For] スクロールリストから、通知を送信するために訪問者がロケーションから離れている必要がある分数を選択します。

（注）
- [Exiting Location] オプションは使用できなくなりました。[Exiting Location] が設定されている既存のエンゲージメントルールを編集している場合は、[Choose User Activity] ドロップダウンリストが、オプションが選択されていない状態で表示されます。ルールを正常に保存するには、[Choose User Activity] ドロップダウンリストから必要なオプションを選択する必要があります。
- 訪問者がロケーションに物理的に存在していても、[For] スクロールリストで指定された分数の間 Wi-Fi から切断されていれば、訪問者は通知の送信対象と見なされます。

- [Present at location]：訪問者が Wi-Fi に接続され、指定された期間または特定の時刻にロケーションにいるとビジネスユーザーに通知が送信されるようにするには、このオプションを選択します。このオプションを選択すると、追加のフィールドが表示されて、顧客がこのルールの対象としてフィルタリングされるための期間または時刻を指定できます。

ステップ 5 [Locations] エリアで、通知を送信するロケーションを指定します。

すべての顧客名または単一のロケーションや複数のロケーション（グループ、フロア、グループ、ゾーンなど）に対して通知の送信を設定できます。エンゲージメントルールに、Cisco Meraki、シスコ ワイヤレス コントローラなどの異なるワイヤレスネットワークのロケーションを追加できます。

また、選択したロケーションまたはその親あるいは子ロケーションに対して定義されているメタデータに基づいて通知を送信するロケーションをフィルタリングすることもできます。特定のメタデータを持つロケーションに対して通知を送信することも、特定のメタデータを持つロケーションを除外することもできます。エンゲージメントルールのロケーションを定義する方法の詳細については、エンゲージメントルールのロケーションフィルタ （210 ページ）を参照してください。

ステップ 6 [Identify] エリアで、ビジネスユーザーに通知を送信する顧客のタイプを指定します。

（注） 通知を送信する顧客は、顧客がオプトインユーザーかどうか、顧客が属するタグ、顧客の訪問回数に基づいてフィルタリングすることができます。これらのフィルタをすべて適用することも、要件に応じて一部を適用することもできます。

ビジネス ユーザに通知を送信する顧客を指定するには、次の手順を実行します。

a) オプトインステータスにより顧客をフィルタリングする場合、[Filter by Opt-In Status] チェックボックスをオンにして、オプトインユーザーまたは非オプトインユーザーのどちらに通知を送信するかを選択します。
b) タグに基づいて顧客をフィルタリングするには、[Filter by Tags] チェックボックスをオンにします。

2つの異なる方法でタグをフィルタリングできます。通知を送信するタグを指定するか、通知を送信してはならないタグを指定することができます。要件に基づいて、最適なフィルタリング方法を選択できます。たとえば、1 つのタグを除くすべてのタグに対してビジネス ユーザに通知を送信する場合、除外オプションを選択し、通知を送信しない特定のタグを指定する方法が簡単です。

c) 選択したロケーションにおける顧客の訪問数に基づいて顧客をフィルタリングするには、[Filter by Previous Visits] チェックボックスをオンにします。

[Add Locations] ボタンをクリックします。[Choose Locations] ウィンドウで、顧客の訪問をフィルタリングの条件にする必要があるロケーションを指定します。次のフィールドで、通知を送信するために必要な訪問回数および継続時間を指定します。自分で設定できる訪問回数と継続時間の詳細については、「以前の訪問の条件」のセクションを参照してください。

ステップ 7 [Schedule] エリアで、エンゲージメントルールを適用する期間を指定します。

a) [Set a date range for the rule] チェックボックスをオンにし、表示されるフィールドで、エンゲージメントルールを適用する期間の開始日と終了日を指定します。

b) [Set a time range for the rule] チェックボックスをオンにし、表示されるフィールドで、指定した日付範囲内でのエンゲージメントルールを適用する時間範囲を指定します。

c) 特定の日にのみルールを適用する場合、[Filter by days of the week] チェックボックスをオンにし、表示される曜日のリストからエンゲージメントルールを適用する曜日をクリックします。

ステップ 8 [Actions] エリアで、次の手順を実行します。

a) [Notify] ドロップダウンリストから [Business] を選択し、隣のドロップダウンリストから次のいずれかを選択します。

- [Only Once]：通知は一度だけビジネスユーザーに送信されます。
- [Once In]：通知は指定した通知頻度に基づいて複数回ビジネスユーザーに送信されます。このオプションを選択すると表示される追加のフィールドで、通知頻度を指定します。通知頻度の詳細については、「通知の頻度」のセクションを参照してください。
- 通知のモードを指定します。Cisco Webex Teams、電子メール、SMS を使用して、顧客に通知を送信できます。外部 API に通知を送信することもできます。通知タイプの詳細については、ビジネスユーザーの通知タイプ （212 ページ）を参照してください。

（注） 名、姓、携帯電話の番号などの変数を通知メッセージに表示するには、ポータルでデータキャプチャフォームを設定する必要があります。ポータルでのデータキャプチャフォームの設定に関する詳細については、「ポータルへのデータキャプチャフォームの追加」のセクションを参照してください。

（注） ルールの概要がページの右側に表示されます。

ステップ 9 [Save and Publish] をクリックします。

ルールが [Engagement Rules] ページのリストにパブリッシュされます。

（注） ルールを今すぐパブリッシュしない場合は、[Save] ボタンをクリックします。ルールを開いて [Save and Publish] ボタンをクリックすることで、後でいつでもルールをパブリッシュできます。また、[Engagement Rules] ページでルールの右端にある [Make Rule Live] アイコンをクリックして、ルールをパブリッシュすることもできます。

使用例：ビジネスユーザーに対するエンゲージメントルール

ABC は、世界中にホテルを持つホテル グループです。ABC には特権のある多数の顧客がいて、主にホテルを利用するビジネス ユーザです。25 周年記念の一環として、ABC はロケーション A の最初のホテルを訪問するプラチナ ロイヤルティ メンバーに特別なギフトを提供します。ABC は、ロケーション A またはロケーション C にあるホテルを過去 2 年間に 10 回以上訪問したことがあるすべての顧客をプラチナ ロイヤルティ メンバーとみなしています。ABC は、カスタマー ケア担当者が顧客に直接会って顧客にギフトを渡すことを考えています。ABC は、SMS によってプラチナ ロイヤルティ メンバーの到着についてカスタマー ケア担当者に通知を送信します。通知は、顧客がロケーションに入るときにオプトインユーザに対して送信する必要があります。通知は今月の間だけ送信します。ABC は顧客について 1 回だけ通知を送信します。

上記のシナリオの条件を満たすには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces にログインします。

ステップ 2 ABC のすべてのロケーションを含むロケーション階層を作成します。

ステップ 3 [Profile Rule] を使用して、プラチナ ロイヤルティ メンバーに対するタグ **Platinum** を作成します。ルールでは、ロケーション A またはロケーション C を過去 2 年間に 10 回以上訪問した顧客をフィルタリングする必要があります。

ステップ 4 Cisco DNA Spaces ダッシュボードで、[Engagements] をクリックします。

ステップ 5 表示される [Engagements] ウィンドウで、[Create New Rule] をクリックします。

ステップ 6 [RULE NAME] フィールドに、新しいエンゲージメントルールの名前を入力します。

ステップ 7 [When a user is on Wi-Fi and] ドロップダウンリストから、[Entering Location] を選択します 。

ステップ 8 [Locations] 領域で、[Add Locations] ボタンをクリックし、ロケーション A を選択します。ABC が顧客にギフトを提供するロケーションです。

ステップ 9 [Identify] エリアで、以下を実行します。

a) [Filter by Opt-In Status] チェックボックスをオンにし、[Only for opted-in Visitor] を選択します。

b) [Filter by Tags] チェックボックスをオンにし、[Include] の [Add Tags] ボタンをクリックします。

c) [Choose Tags] ウィンドウで、ステップ 3 で作成した [Platinum1] の [Include] オプションボタンをクリックして、[Done] をクリックします。

ステップ 10 [Schedule] 領域で、以下を実行します。

a) [Set a date range for the rule] チェックボックスをオンにし、ABC がオファーを提供する今月の開始日と終了日を指定します。

ステップ 11 [Actions] 領域で、以下を実行します。

a) [Notify] ドロップダウンリストから、[Business] を選択します。
b) 隣のドロップダウン リストから、[Only Once] を選択します。
c) [Via Email] チェックボックスをオンにします。[From] フィールドで電子メールに表示する差出人の電子メール ID を指定し、[To] フィールドで通知を送信するビジネスユーザーの電子メール ID を入力し、[Subject] フィールドで通知の電子メールの件名を入力します。必要に応じて、次に表示されるテキストエディタで通知メッセージを編集します。

   [From] フィールドに入力する電子メール ID は、電子メール ID の許可リストに含まれている必要があります。電子メール ID を許可リストに含める方法については、Cisco DNA Spaces サポートチームにお問い合わせください。

ステップ 12 **[Save and Publish]** をクリックします。

エンゲージメント ルールがパブリッシュされます。

次のタスク

これで、オプトイン プラチナ ロイヤルティ メンバーがロケーション A の構内に入ると、ロケーション A のカスタマーケア担当者に通知が送信されるようになりました。

エンゲージメントルールの管理

エンゲージメント ルールの一時停止

エンゲージメント ルールを一時停止するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Engagements] をクリックします。

すべてのエンゲージメントルールがリストされた [Engagements] ウィンドウが表示されます。

ステップ 2 一時停止するエンゲージメントルールの右端に表示される [Pause Rule] アイコンをクリックします。

ステップ 3 表示されるウィンドウで、一時停止を確定します。

エンゲージメント ルールが一時停止します。

次のタスク

（注） 複数のエンゲージメントルールを一時停止するには、一時停止するエンゲージメントルールのチェックボックスをオンにし、ページの下部に表示される [Pause] ボタンをクリックします。

エンゲージメント ルールの再起動

エンゲージメント ルールを再起動するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Engagements] をクリックします。

すべてのエンゲージメントルールがリストされた [Engagements] ウィンドウが表示されます。

ステップ 2 再起動するエンゲージメントルールの右端に表示される [Make Rule Live] アイコンをクリックします。

エンゲージメント ルールが再起動します。

次のタスク

（注） 複数のエンゲージメントルールを再起動するには、再起動するエンゲージメントルールのチェックボックスをオンにし、ウィンドウの下部に表示される [Make Live] ボタンをクリックします。

エンゲージメント ルールの変更

エンゲージメント ルールを変更するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Engagements] をクリックします。

すべてのエンゲージメントルールがリストされた [Engagements] ウィンドウが表示されます。

ステップ 2 変更するエンゲージメントルールの右端に表示される [Edit Rule] アイコンをクリックします。

ステップ 3 必要な変更を加えます。

ステップ 4 変更を保存するには、[Save] をクリックします。または変更をパブリッシュするには、[Save and Publish] をクリックします。

（注） ライブルールに表示されるのは [Save and Publish] ボタンのみです。[Save and Publish] ボタンをクリックすると、変更を反映したルールがパブリッシュされます。

エンゲージメント ルールの削除

エンゲージメント ルールを削除するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Engagements] をクリックします。

すべてのエンゲージメントルールがリストされた [Engagements] ウィンドウが表示されます。

ステップ 2 削除するエンゲージメントルールの右端に表示される [Delete Rule] アイコンをクリックします。

ステップ 3 表示されるウィンドウで、削除を確定します。

次のタスク

（注） 複数のエンゲージメントルールを削除するには、削除するエンゲージメントルールのチェックボックスをオンにし、ページの下部に表示される [Delete] ボタンをクリックします。

ロケーションのエンゲージメントルールの表示

グループ、ビルディング、フロアなどのロケーションのエンゲージメントルールを表示するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードの左上にある 3 本線のメニューアイコンをクリックします。

ステップ 2 [Location Hierarchy] を選択します。

ロケーション階層を示す [Location Hierarchy] ウィンドウが表示されます。

ステップ 3 エンゲージメントルールを表示するロケーションをクリックします。

ステップ 4 [Rules] タブをクリックします。

ステップ 5 [Engagement Rule] タブをクリックします。

ロケーションのエンゲージメントルールがリストされます。

次のタスク

（注） ロケーション階層の各ロケーションに表示される [Rules] リンクをクリックして、[Rules] タブにアクセスすることもできます。ロケーションの [Rules] リンクは、そのロケーションに少なくとも 1 つのプロキシミティルールが存在する場合にのみ有効になります。

エンゲージメント ルール レポート

Cisco DNA Spaces では、各エンゲージメントルールに固有のレポートを表示することができます。このレポートは、特定のルールに関するルール アクティビティおよびユーザ エンゲージメントの詳細を表示します。

エンゲージメント ルールのエンゲージメント ルール レポートを表示するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Home] を選択します。

ステップ 2 [My Apps]エリアで、[Engagements] を選択します。

エンゲージメント ルール レポートを表示するルールをクリックします。

ステップ 3 [Filter] 領域で、レポートを表示する期間を選択します。

レポートは指定された期間に対してフィルタリングされます。

エンゲージメント ルール レポートには次のセクションがあります。

ルールアクティビティ

このセクションには、特定のエンゲージメントルールに基づいて送信された通知の詳細が表示されます。

- [Daily Engagements]：特定のエンゲージメントルールに基づく日ごとの“通知の送信先の一意ユーザー" に対する“送信された通知数" の比率を表示します。X 軸は、フィルタが適用された期間の日数を表します。Y 軸は、送信された通知の数を表します。グラフ内の特定の日の領域にマウスを合わせると、その日のデータを表示できます。
- [Engagements]：このセクションには、対象の各ロケーションについて、送信された通知の総数が表示されます。
- [Engagement by Time of Day]：この棒グラフは、1 日の各時間に顧客に送信された通知の数を表示します。これにより、ルールでフィルタリングされた顧客がビジネスの施設内にいる時間を特定し、それに応じてターゲットにすることができます。

訪問者エンゲージメント

訪問者エンゲージメントレポートには、設定したエンゲージメントルールに基づいて、訪問者とのエンゲージメントの詳細が表示されます。訪問者エンゲージメントレポートにアクセスするには、[Engagements] ウィンドウで、ウィンドウの左上にある 3 本線のメニューアイコンをクリックしてから、[Visitor Engagement] をクリックします。

エンゲージメント

[Total Engagements]：指定された期間中に、選択したロケーションを訪れた訪問者との（SMS または電子メール通知による）エンゲージメントの合計数。Cisco DNA Spaces インストール日以降の全ロケーションにおけるこのメトリックが、[Total Engagements with Visitors] のレポートの上部に表示されます。

[Via SMS]：指定された期間中に、選択したロケーションを訪れた訪問者への SMS によるエンゲージメントの合計数。エンゲージメント合計数のうち、SMS によるエンゲージメントの割合も表示されます。

[Via Email]：指定された期間中に、選択したロケーションを訪れた訪問者への電子メールによるエンゲージメントの合計数。エンゲージメント全体のうち、電子メールによるエンゲージメントの割合も表示されます。

エンゲージメントの日次トレンド

このセクションには、SMS、電子メールなどのさまざまな通知タイプによる、指定された期間の各日におけるロケーションからのエンゲージメント数を示す折れ線グラフが表示されます。グラフの上部には、さまざまな通知タイプのカラーインジケータが表示されます。グラフにカーソルを合わせると、特定の日におけるエンゲージメントの詳細が表示されます。

エンゲージメント ルール レポート

このセクションでは、さまざまなエンゲージメントルールのレポートが一覧表示されます。ルールがパブリッシュされた日付が、そのルールに基づいて行われたエンゲージメントの合計数とともに表示されます。対応するルールをクリックすると、特定のエンゲージメントルールの詳細レポートを表示できます。エンゲージメント ルール レポートの詳細については、エンゲージメント ルール レポート （206 ページ）を参照してください。

エンゲージメント URL

エンゲージメント URL とは、SMS およびユーザーに送信される通知メッセージで提供される URL のことです。ビジネスユーザーの場合、SMS 通知にエンゲージメント URL を追加できます。ユーザがこの URL をクリックすると、通知に関連するサイト ページを表示することができます。たとえば、顧客が使用可能なディスカウントおよびオファーの詳細情報をサイト ページで提供することができます。このサイトページは、サイト作成アプリケーションを使用して作成できます。

以前の訪問の条件

以前の訪問に基づいて顧客をフィルタリングするためのさまざまな条件を定義できます。

- **Atleast ..Times**：顧客の訪問回数が指定した数になるとルールが適用されます。
  - [Last 1 day]：過去 1 日間の顧客の訪問回数が指定した数になるとルールが適用されます。
  - [Last 7 days]：過去 7 日間の顧客の訪問回数が指定した数になるとルールが適用されます。
  - [Last 15 days]：過去 15 日間の顧客の訪問回数が指定した数になるとルールが適用されます。

- [Last 30 days]：過去 30 日間の顧客の訪問回数が指定した数になるとルールが適用されます。
- [Last 90 days]：過去 90 日間の顧客の訪問回数が指定した数になるとルールが適用されます。
- [This Weekend]今週の顧客の訪問回数が指定した数になるとルールが適用されます。
- [This Month]：今月の顧客の訪問回数が指定した数になるとルールが適用されます。
- [This Year]：今年の顧客の訪問回数が指定した数になるとルールが適用されます。
- [Date Range]特定の期間の顧客の訪問回数が指定した数になるとルールが適用されます。このオプションを選択すると、追加のフィールドが表示され、期間の開始日と終了日を指定できます。

- [Between, ..Times]：顧客の訪問回数が指定した数の範囲内になるとルールが適用されます。
  - [Last 1 day]：過去 1 日間の顧客の訪問回数が指定した数の範囲になるとルールが適用されます。
  - [Last 7 days]：過去 7 日間の顧客の訪問回数が指定した数の範囲になるとルールが適用されます。
  - [Last 15 days]：過去 15 日間の顧客の訪問回数が指定した数の範囲になるとルールが適用されます。
  - [Last 30 days]：過去 30 日間の顧客の訪問回数が指定した数の範囲になるとルールが適用されます。
  - [Last 90 days]：過去 90 日間の顧客の訪問回数が指定した数の範囲になるとルールが適用されます。
  - [This Week]：今週の顧客の訪問回数が指定した数の範囲になるとルールが適用されます。
  - [This Month]：今月の顧客の訪問回数が指定した数の範囲になるとルールが適用されます。
  - [This Year]：今年の顧客の訪問回数が指定した数の範囲になるとルールが適用されます。
  - [Date Range]：特定の期間の顧客の訪問回数が指定した数の範囲になるとルールが適用されます。このオプションを選択すると、追加のフィールドが表示され、期間の開始日と終了日を指定できます。

通知タイプ

Cisco DNA Spaces では、次の形式で通知を送信できます。

- SMS：SMS として通知を送信します。ビジネスユーザーの場合、通知の送信先とする携帯電話番号を定義できます。
- Email：電子メールとして通知を送信します。ビジネスユーザーの場合、通知の送信先とする電子メールアドレスを定義できます。
- API Notifications：外部アプリケーションに API 通知を送信します。Cisco DNA Spaces では、サードパーティアプリケーションに通知を送信することができます。この通知タイプは顧客には適用されません。
- Cisco Webex Teams：ビジネスユーザーの Webex Team アカウントに通知を送信します。この通知タイプは顧客には適用されません。この通知タイプを使用するには、Cisco Webex アカウントが必要です。

通知の頻度

エンゲージメント ルールで通知を送信する頻度です。エンゲージメント ルールには次の通知頻度を設定できます。

- Only Once：ユーザに一度だけ通知を送信します。
- Once in：指定された期間に一度通知を送信します。
  - Visits：顧客の訪問回数が指定した数になると通知を送信します。
  - Hours：指定した時間数に一度通知を送信します。
  - Days：指定した日数に一度通知を送信します。
  - Weeks：指定した週数に一度通知を送信します。
  - Months：指定された月数に一度通知を送信します。

エンゲージメントルールのロケーションフィルタ

通知を送信するロケーションを指定するには、次の手順を実行します。

1. [Add Locations] ボタンをクリックします。
2. [Choose Locations] ウィンドウが表示されたら、通知を送信するロケーションのチェックボックスをオンにします。
3. [完了（Done）] をクリックします。

ロケーションに定義されているメタデータを使用して、ロケーションを再度フィルタリングできます。選択したロケーション、その親および子のロケーションに定義されているメタデータのみを選択できます。

特定のロケーションメタデータを持つロケーションに対してのみ通知を送信するには、次の手順を実行します。

1. [Filter by Metadata] チェックボックスをオンにします。
2. [Filter] 領域で、[Add Metadata] ボタンをクリックします。

   [Choose Location Metadata] ウィンドウが表示されます。
3. ドロップダウンリストから、メタデータの変数を選択し、隣接フィールドに変数の値を選択します。
4. [完了（Done）] をクリックします。

特定のメタデータを持つロケーションに対する通知の送信を除外するには、次の手順を実行します。

1. [Filter by Metadata] チェックボックスをオンにします。
2. [Exclude] 領域で、[Add Metadata] ボタンをクリックします。

   [Choose Location Metadata] ウィンドウが表示されます。
3. ドロップダウンリストから、メタデータの変数を選択し、隣接フィールドに変数の値を選択します。
4. [Done] をクリックします。

消費者用の通知タイプ

エンゲージメントルールの [Actions] エリアで、顧客に通知を送信する際に使用するモードを指定します。

- SMS で通知を送信する場合、[Via SMS] チェックボックスをオンにします。[SMS Gateway] ドロップダウンリストから、SMS 通知を送信する SMS ゲートウェイを選択します。シスコが提供する有料の [Demo Gateway] も使用できます。SMS ゲートウェイの追加に関する情報については、続いて表示されるテキストボックスで、顧客に送信されるメッセージの内容を参照してください。変数を使用してメッセージの内容を強化することができます。デフォルトでは、顧客の名および姓、およびエンゲージメント URL が変数として追加されます。テキストボックスをクリックするとテキストボックスの下に一覧表示される変数を使用して、メッセージにテキスト変数をさらに追加できます。テキスト変数の追加に関する詳細については、「エンゲージメントルールと密度ルールのための Smark Link とテキスト変数」のセクションを参照してください。

  必要に応じて、[Link] フィールドで、通知に表示する必要があるエンゲージメント URL を入力します。エンゲージメント URL の作成の詳細については、エンゲージメント URL（208 ページ）のセクションを参照してください。
- 電子メールで通知を送信する場合、[Via Email] チェックボックスをオンにします。[From Name] フィールドで顧客が電子メールを受信する名前を指定し、[From Email] フィールド

で顧客が電子メールを受信する電子メール ID を指定し、[Subject] フィールドで通知メールの件名を入力します。顧客に送信されるメッセージの内容は、次のテキストボックスに表示されます。テキスト変数を使用してメッセージの内容を強化することができます。デフォルトでは、顧客の名および姓、およびエンゲージメント URL が変数として追加されます。テキストボックスをクリックするとテキストボックスの下に一覧表示される変数を使用して、メッセージにテキスト変数をさらに追加できます。テキスト変数の追加に関する詳細については、「エンゲージメントルールと密度ルールのための Smark Link とテキスト変数」の項を参照してください。

必要に応じて、[Link] フィールドで、通知に表示する必要があるエンゲージメント URL を入力します。エンゲージメント URL の作成の詳細については、エンゲージメント URL（208 ページ）のセクションを参照してください。

（注）

- [Via Email] オプションを使用している場合、電子メール ID の許可リストの [From] フィールドに電子メール ID が入力されていることを確認する必要があります。電子メール ID を許可リストに含める方法については、Cisco DNA Spaces サポートチームにお問い合わせください。特定の電子メール ID を使用しない場合は、デフォルトで許可されている電子メール ID である **no-reply@dnaspaces.io** を使用できます。ただし、このデフォルト ID が自動的にダッシュボードに表示されることはありません。そのため、手動で入力する必要があります。
- 変数「$firstName」は顧客の名前を表示し、「$lastName」は顧客の姓を表示し、「$email」は顧客の電子メールアドレスを表示し、「$mobile」は顧客の携帯電話の番号を表示し、「$URL」はエンゲージメント URL を表示し、「$gender」は顧客の性別を表示し、「locationName」はメッセージが送信されるロケーションを表示します。
- 名、姓、携帯電話の番号などの変数を通知メッセージに表示するには、ポータルでデータキャプチャフォームを設定する必要があります。ポータルでのデータキャプチャフォームの設定に関する詳細については、「ポータルへのデータキャプチャフォームの追加」のセクションを参照してください。

ビジネスユーザーの通知タイプ

Cisco Webex Teams、SMS、電子メール経由で、ビジネスユーザーに通知を送信できます。API エンドポイントに通知を送信することもできます。

- Cisco Webex Teams 経由で通知を送信する場合は、[Via Cisco Webex Teams] チェックボックスをオンにします。[Webex Accounts] ドロップダウンリストから、通知を送信する Webex アカウントを選択します。[Add Webex Account] オプションを使用して、Webex アカウントを追加できます。Webex アカウントを追加するには、webex デベロッパーアカウントを指定する必要があり、Webex デベロッパーサイトを使用してそのアカウントのトークンを生成する必要があります。次に、デベロッパーサイトでトークンに表示されるタイムアウト期間内に、[Add Webex Account] ウィンドウでトークンを設定する必要があります。デ

フォルトのトークンの代わりに、デベロッパーサイトでボットを作成し、タイムアウト制限なしでトークンを生成できます。

ビジネスユーザーに送信されるメッセージの内容は、[Notification Message] テキストボックスに表示されます。テキスト変数を使用して、このメッセージを強化することができます。 デフォルトでは、顧客の名および姓、およびエンゲージメント URL が変数として追加されます。テキストボックスをクリックするとテキストボックスの下に一覧表示される変数を使用して、メッセージにテキスト変数をさらに追加できます。テキスト変数の追加に関する詳細については、「エンゲージメントルールと密度ルールのための Smark Link とテキスト変数」のセクションを参照してください。

- SMS 経由で通知を送信する場合、[Via SMS] チェックボックスをオンにします。[SMS Gateway] ドロップダウンリストから、SMS 通知を送信する SMS ゲートウェイを選択します。シスコが提供する有料の [Demo Gateway] も使用できます。表示される [To] フィールドで、通知を送信するビジネスユーザーの携帯電話の番号（国番号を付加）を入力します。必要に応じて、[Link] フィールドで、通知に表示する必要があるエンゲージメント URL を入力します。エンゲージメント URL の設定の詳細については、エンゲージメント URL （208 ページ）を参照してください。

  ビジネスユーザーに送信されるメッセージの内容は、次のテキストボックスに表示されます。テキスト変数を使用して、このメッセージを強化することができます。デフォルトでは、顧客の名および姓、およびエンゲージメント URL が変数として追加されます。テキストボックスをクリックするとテキストボックスの下に一覧表示される変数を使用して、メッセージにテキスト変数をさらに追加できます。テキスト変数の追加に関する詳細については、「エンゲージメントルールと密度ルールのための Smark Link とテキスト変数」のセクションを参照してください。
- 電子メール経由で通知を送信する場合、[Via Email] チェックボックスをオンにします。[From]フィールドで電子メールに表示する「差出人の電子メールID」を指定し、[To]フィールドで通知を送信するビジネスユーザーの電子メール ID を入力し、[Subject] フィールドで通知の電子メールの件名を入力します。

  [From] フィールドに入力する電子メール ID は、電子メール ID の許可リストに含まれている必要があります。電子メールIDを許可リストに含める方法については、Cisco DNA Spaces サポートチームにお問い合わせください。特定の電子メールIDを使用しない場合は、デフォルトで許可されている電子メール ID である **no-reply@dnaspaces.io** を使用できます。ただし、このデフォルトIDが自動的にダッシュボードに表示されることはありません。そのため、手動で入力する必要があります。

  ビジネスユーザーに送信されるメッセージの内容は、次のテキストボックスに表示されます。デフォルトでは、顧客の名および姓、およびエンゲージメント URL が変数として追加されます。テキストボックスをクリックするとテキストボックスの下に一覧表示される変数を使用して、メッセージにテキスト変数をさらに追加できます。テキスト変数の追加

に関する詳細については、「エンゲージメントルールと密度ルールのための Smark Link とテキスト変数」のセクションを参照してください。必要に応じて、[Link] フィールドで、通知に表示する必要があるエンゲージメント URL を入力します。エンゲージメント URL の設定の詳細については、エンゲージメント URL （208 ページ）を参照してください。

- 外部 API に通知を送信するには、[Trigger API] チェックボックスをオンにします。トリガー API の設定の詳細については、「通知のためのトリガー API の設定」のセクションを参照してください。

エンゲージメントルールと密度ルールのための Smark Link とテキスト変数

エンゲージメントルールと密度ルールでは、すべての通知タイプ（[Via Cisco Webex Teams]、[Via SMS]、[Via Email]、および [Trigger API]）で送信される通知メッセージにテキスト変数を追加でき、**トリガー API** URI のスマートリンクを作成できます。この変数により、通知メッセージまたはトリガー API URI に、顧客、ロケーション、デバイスの詳細を表示できます。デフォルトでは、通知メッセージには顧客の姓名が記載されます。この変数を使用して、さらに詳細を追加できます。

たとえば、顧客に SMS 通知を送信するエンゲージメントルールを作成し、SMS 通知の [message] テキストボックスに変数「mobile」および「gender」を設定していたとします。この場合、顧客がこのエンゲージメントルールに基づく SMS メッセージを受信すると、メッセージには、顧客の携帯電話の番号と性別の詳細も表示されます。

（注） Cisco DNA Spaces は、データキャプチャフォームを使用して顧客の個人情報をキャプチャします。つまり、スマートリンクまたはテキスト変数に名、姓、性別などの個人に関する詳細を含めるためには、ポータルにデータキャプチャフォームを設定する必要があります。キャプティブポータルへのデータキャプチャフォームの追加の詳細については、「ポータルへのデータキャプチャフォームの追加」セクションを参照してください。

通知メッセージと URL には、静的変数と動的変数を含めることができます。

通知メッセージに含めることができる静的変数は次のとおりです。

表 *9*: 静的変数一覧

静的変数名	説明
$firstName	顧客の名前。
$lastName	顧客の姓。
$email	顧客の電子メールアドレス。
$mobile	顧客の携帯電話番号。

静的変数名	説明
$gender	顧客の性別。
$URL	URL リンク値。
$TotalAreaValue	[Location Hierarchy] の [Location Info] ウィンドウのロケーションに設定されたエリア合計。
$TotalAreaUnit	[Location Hierarchy] の [Location Info] ウィンドウのロケーションに設定されたエリアユニット合計。
$TotalCapacity	[Location Hierarchy] の [Location Info] ウィンドウのロケーションに設定されたキャパシティ合計。
$locationName	ルールがトリガーされるロケーションの名前。
$buildingName（密度ルールのみ）	通知がトリガーされるロケーションのビルディング名。
$floorName（密度ルールのみ）	通知がトリガーされるロケーションのフロア名。
$zoneName（密度ルールのみ）	通知がトリガーされるロケーションのゾーン名。
$deviceCount（密度ルールのみ）	通知がトリガーされるロケーションのデバイス数。
$locationPath（密度ルールのみ）	ルールがトリガーされるロケーションのロケーションパス（親階層）。階層内のロケーションは「>」で区切られます（サンプル形式：アカウント>CMXNode>キャンパス>ビルディング>フロア>ゾーン）。
トリガー API の通知タイプには、エンゲージメントルールと密度ルールの両方に次の追加変数があります。	
$macaddress	デバイスの MAC アドレス。
$encryptedMacAddress	暗号化された、デバイスの MAC アドレス。
$deviceSubscriberId	データベース内のデバイスのサブスクライバ ID。
$optinStatus-	顧客のオプトインステータス。

通知メッセージに含めることができる動的変数、およびエンゲージメントルールと密度ルールの URL は次のとおりです。

表 *10*：動的変数一覧

動的変数名	説明
Business Tags	顧客が属するビジネスタグ。データキャプチャフォームで設定されるビジネスタグは、変数としてリストされます。ビジネスタグの作成の詳細については、「ポータルへのデータキャプチャフォームの追加」セクションを参照してください。
Location Metadata	顧客のロケーションのロケーションメタデータ。ロケーション階層で定義されたロケーションメタデータのキーは、変数としてリストされます。ロケーションメタデータの定義の詳細については、「ロケーションのメタデータの追加のセクションを参照してください。

通知メッセージの URL またはテキスト変数にスマートリンクを含めるには、次の手順を実行します。

ステップ 1 スマートリンクを含めるには、[URI] フィールド内の任意の場所をクリックします。テキスト変数を含めるには、通知メッセージテキストボックス内の任意の場所をクリックします。[Via Email] にテキスト変数を含めるには、リッチテキストエディタの [Smartlinks] ドロップダウンリストをクリックします。

追加できる変数がリストされています。

ステップ 2 追加する変数を選択します。

通知のためのトリガー API の設定

ルールを介して外部 API に通知を送信するには、[Create [Rule Name]] ウィンドウの [Actions] 領域で、次の手順を実行します。

1. [Trigger API] チェックボックスをオンにします。
2. [Method] ドロップダウンリストから、API をトリガーするメソッドを選択します。

注 API URI にリンク変数を追加するか、メソッドパラメータにテキスト変数を追加することで、通知メッセージに顧客の詳細を追加できます。

- [Get]：“GET” メソッドを使用して API に通知または顧客の詳細を送信します。このメソッドを選択すると、GET 要求ヘッダーおよびパラメータを指定できる追加のフィールドが表示され、顧客の名、姓、携帯番号などの追加情報を通知に含めることができます。API で定義された要求パラメータのキーを追加し、テキスト変数を使用してこれらの値を指定できます。値はハードコード値または変数のどちらでもかまいません。[Value] フィールドをクリックすると、追加できる変数が表示されます。対応する [Add] ボタンを使用して、[GET] ヘッダーをさらに追加できます。
- [Post Form]：”POST FORM” メソッドを使用して API に通知または顧客の詳細を送信します。このメソッドを選択すると、要求ヘッダーおよびパラメータを指定できる追加のフィールドが表示され、顧客の名、姓、携帯番号などの追加情報を含めることができます。API に定義されている form パラメータのキーを追加し、それらの値を指定できます。値は、ハードコード値または変数のどちらでもかまいません。[Value] フィールドをクリックすると、追加できる変数が表示されます。[Add] ボタンを使用して、さらに「フォームパラメータ」を追加できます。
- [Post JSON]：”POST JSON” メソッドを使用して API に通知または顧客の詳細を送信します。このメソッドを選択すると、要求ヘッダーフィールドが、API に通知メッセージとして送信する JSON データを指定できるテキストボックスとともに表示されます。API で定義されるさまざまな JSON 要求ヘッダーフィールドの値を指定できます。値はハードコード値または変数のどちらでもかまいません。[Value] フィールドをクリックすると、追加できる変数が表示されます。テキストボックスをクリックして、JSON データに追加できる変数を表示できます。
- [Post Body]：”POST BODY” メソッドを使用して API に通知または顧客の詳細を送信します。このメソッドを選択すると、API に送信する通知に含める必要がある内容を指定できる要求ヘッダーフィールドが、[Post Body Data] フィールドとともに表示されます。API で定義されるさまざまな Body 要求ヘッダーフィールドの値を指定できます。値はハードコード値または変数のどちらでもかまいません。[Value] フィールドをクリックすると、追加できる変数が表示されます。フィールドをクリックすると、[Post Body Data] フィールドに追加できる変数を表示できます。

注　ポータルの [Data Capture] フォームを使用してキャプチャするように設定されたこれらのデータだけが通知に含まれます。

3. [URI] フィールドに、API の URI を入力します。スマート リンクを使用して通知メッセージに顧客の詳細を含めることができます。URI に含めることができる変数を表示するには、[URI] フィールドをクリックします。

- キャプティブポータルルールに追加できる変数については、キャプティブポータルのスマートリンクとテキスト変数 （190 ページ）を参照してください。
- エンゲージメントルールまたは密度ルールに追加できる変数については、エンゲージメントルールと密度ルールのための Smark Link とテキスト変数 （214 ページ）を参照してください。

第 11 章

Location Personas アプリによるタグの作成

Cisco Digital Network Architecture（DNA）Spaces では、タグを使用して顧客をグループ化できます。その後、エンゲージメントルールなどの Cisco DNA Spaces ルールでこれらのタグを使用できます。Cisco DNA Spaces では、Location Personas アプリを使用してタグを作成できます。また、Location Personas アプリを使用して、既存のタグに顧客を追加したり、既存のタグから特定の顧客を削除したりすることもできます。複数のタグの下に顧客をグループ化できます。

タグを作成するときに、既存のタグを使用して、選択したロケーションの顧客をフィルタリングできます。たとえば、ロケーション A とロケーション B のタグを作成するときに Android ユーザに限定したい場合、iOS のタグを削除するタグ フィルタを使用できます。

ロケーションペルソナアプリを使用したタグの作成または変更

タグを作成、または顧客を既存のタグに含めるか除外するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Location Personas] をクリックします。

ステップ 2 表示される [Location Personas] ウィンドウで、[Create New Rule] をクリックします。

ステップ 3 [Rule Name] フィールドに、ロケーションペルソナ/プロファイルルールの名前を入力します。

ステップ 4 [When a user is on WiFi and] ドロップダウンリストから、次のいずれかを選択します。

- [Entering Location]：Wi-Fi に接続されている訪問者がロケーションに入ったときにタグを付けるには、このオプションを選択します。
- [Away from the Location]：Wi-Fi に接続されている訪問者が、指定された時間ロケーションを離れた場合にタグを付けるには、このオプションを選択します。このオプションを選択している場合、[For] ス

クロールリストから、このルールに基づきタグ付けするために、訪問者がロケーションから離れている必要がある時間（分）を選択します。

（注）
- [Exiting Location] オプションは使用できなくなりました。[Exiting Location] が設定されている既存の [Location Personas] を編集している場合、[Choose User Activity] ドロップダウンリストが、オプションが選択されていない状態で表示されます。ルールを正常に保存するには、[Choose User Activity] ドロップダウンリストから必要なオプションを選択する必要があります。
- 訪問者がロケーションに物理的に存在していても、[For] スクロールリストで指定された分数の間 Wi-Fi から切断されていれば、訪問者はタグ付けの対象と見なされます。

- [Present at location]： Wi-Fi に接続されている訪問者が、指定した期間、または特定の時間に、ロケーションにいるとタグ付けされるようにするには、このオプションを選択します。このオプションを選択すると、追加のフィールドが表示され、顧客がフィルタ対象となるために満たすべき期間または時間を指定できます。

ステップ 5 [Location] 領域で、ルールに応じて顧客をフィルタリングするロケーションを指定します。

すべての顧客名、あるいは 1 つまたは複数の ロケーション（グループ、キャンパス、ビルディング、フロア、ゾーンなど）を選択できます。CUWN と Cisco Meraki の両方のロケーションを追加できます。

選択したロケーション、またはその親や子のロケーションに定義されているメタデータに基づき、ロケーションを再度フィルタリングできます。特定のメタデータのロケーションを選択するか、または特定のメタデータのロケーションを除外することができます。プロファイルルールのロケーションの設定の詳細については、ロケーションペルソナルールのロケーションフィルタ （224 ページ）を参照してください。

ステップ 6 [Identify] エリアで、ルールでフィルタリングする顧客のタイプを指定します。

（注） 顧客がオプトインユーザかどうか、顧客が属するタグ、顧客のアクセス回数、顧客のデバイスのアプリケーションの状態などに基づいて顧客をフィルタリングできます。これらのフィルタをすべて適用することも、要件に応じて一部を適用することもできます。

ルールに応じてフィルタリングする顧客を指定するには、次の手順を実行します。

a) オプトインステータスにより顧客をフィルタリングする場合、[Filter by Opt-In Status] チェックボックスをオンにして、ルールでオプトインユーザーまたは非オプトインユーザーのどちらをフィルタリングするかを選択します。

（注） オプトイン ユーザの詳細については、ユーザーのオプトインオプション （224 ページ）を参照してください。

b) タグに基づいて顧客をフィルタリングするには、[Filter by Tags] チェックボックスをオンにします。

（注） 既存のタグを含む、または除外することによって、顧客をフィルタリングできます。2つの異なる方法でタグをフィルタリングできます。ルールに応じて含める顧客の既存のタグ、またはルールに応じて除外する顧客の既存のタグを指定できます。要件に基づいて、最適なフィルタリング方法を選択できます。たとえば、1つのタグを除くすべての既存のタグの顧客を追加する場合、除外オプションを選択し、顧客を除外する特定のタグを指定する方法が簡単です。

タグ フィルタの使用の詳細については、タグによるフィルタリング （223 ページ）を参照してください。

c) 選択したロケーションにおける顧客の訪問数に基づいて顧客をフィルタリングするには、[Filter by Previous Visits] チェックボックスをオンにします。

[Add Locations] ボタンをクリックします。[Choose Locations] ウィンドウで、顧客の訪問をフィルタリングの条件にする必要があるロケーションを指定します。次のフィールドで、ルールに応じてフィルタ対象となる顧客のアクセス数および時間を指定します。

d) 顧客のアプリステータスに基づいて顧客をフィルタリングする場合は、[Filter by App Status] チェックボックスをオンにして、ルールでアプリユーザーまたは非アプリユーザーのどちらをフィルタリングするかを選択します。

ステップ 7 [Schedule] 領域で、顧客をフィルタリングするルールを適用する期間を指定します。

（注） 指定した期間で前述の条件を満たす顧客のみがルールに応じてフィルタリングされます。

a) [Set a date range for the rule] チェックボックスをオンにし、表示されるフィールドで、プロファイルルールを適用する期間の開始日と終了日を指定します。

b) [Set a time range for the rule] チェックボックスをオンにし、表示されるフィールドに、プロファイルルールを適用する時間範囲を指定します。

c) 特定の曜日にだけルールを実行するには、[Filter by days of the week] チェックボックスをオンにし、表示される曜日のリストから、ルールを適用する曜日を選択します。

ステップ 8 [Action] 領域で、前述の条件に基づきフィルタリングされた顧客を含めるまたは除外することで新しいタグを作成するかどうかを指定します。

a) [Add Tags] ボタンをクリックします。

- 既存のタグからフィルタリングされた顧客を追加または削除するには、フィルタリングされた顧客を含めるタグ、およびフィルタリングされた顧客を除外するタグを指定します。
  - 既存のタグにこのプロファイル ルールに基づいてフィルタリングされた顧客を追加するには、顧客を追加するタグの [Add] ラジオ ボタンを選択します。
  - 既存のタグからこのプロファイル ルールに基づいてフィルタリングされた顧客を削除するには、顧客を削除するタグの [Remove] ラジオ ボタンを選択します。

（注） [Choose Tags] ウィンドウで、[Search] オプションを使用してタグを検索できます。選択したタグはウィンドウの右側に表示されます。

- ルールの新しいタグを作成する場合は、[Create New Tag] ボタンをクリックします。表示された [Enter the tag name] フィールドにタグの名前を入力し、[Add] をクリックします。新しく作成されたタグがタグリストに表示されます。タグからフィルタリングされた顧客を含めるか除外するかを選択します。

b) [完了（Done）] をクリックします。

（注） プロファイル ルールを使用して、フィルタリングされた顧客を含む、または除外するタグを作成する、または同様に、フィルタリングされた顧客を含む、または除外することで既存のタグを変更できます。ルールに対して複数のタグを作成することもできます。

（注） ルールの概要がページの右側に表示されます。

ステップ 9 [Save and Publish] をクリックします。

ルールは [Profile Rules] ページにパブリッシュされ、リストされます。

（注） ルールを今すぐパブリッシュしたくない場合、[Save] ボタンをクリックします。[Save and Publish] ボタンをクリックすることで、後でいつでもルールをパブリッシュできます。また、[Location Personas] ウィンドウの右側にある [Make Rule Live] アイコンをクリックして、プロファイルルールをパブリッシュすることもできます。

使用例：ロケーションペルソナルール（プロファイルルール）

ABC ホテル グループは 25 周年記念の一環として、プラチナメンバーに特別なギフトを提供したいと考えています。ABC はロケーション A またはロケーション C のホテルを過去 2 年間で少なくとも 10 回訪れた顧客をプラチナ メンバーと見なします。WiFi に少なくとも 45 分間接続したすべての訪問者を顧客とみなします。ABC はプラチナ メンバー用のタグを作成する必要があります。現在の月末までに前述の条件を満たすオプトイン顧客がタグに追加されます。

上記のシナリオの条件を満たすには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces にログインします。

ステップ 2 ABC のすべてのロケーションを含むロケーション階層を作成します。

ステップ 3 Cisco DNA Spaces ダッシュボードで、[Location Personas] をクリックします。

ステップ 4 表示される [Location Personas] ウィンドウで、[Create New Rule] をクリックします。

ステップ 5 [Rule Name] フィールドに、プロファイルルールの名前を入力します。.

ステップ 6 [When a user is on WiFi and] ドロップダウンリストから、[Present at Location] を選択し、表示されるドロップダウンリストから、[45 Minutes] を選択します。

ステップ 7 [Locations] エリアで、[Add Locations] ボタンをクリックし、[Location A]、[Location C] を選択します。

ステップ 8 [Identify] エリアで、以下を実行します。

a) [Filter by Opt-In Status] チェックボックスをオンにし、[Only for opted-in Visitor] を選択します。
b) [Filter by Previous Visits] チェックボックスをオンにし、[Add Locations] ボタンをクリックして、[Location A]、[Location C] を追加します。
c) 次のフィールドで、[At least]、[10 回]、[Date Range] をそれぞれ選択します。
d) 日付範囲のフィールドに、過去 2 年間の開始日と終了日を入力します。

ステップ 9 [Schedule] エリアで、[Set a date range for the rule] チェックボックスをオンにし、開始日に現在の日付を、終了日に今月の最終日を指定します。

ステップ 10 [Actions] 領域で、以下を実行します。

a) [Add Tags] ボタンをクリックします。
b) [Create Tags] ウィンドウで、[Create New Tag] をクリックします。
c) [Enter the tag name] フィールドに「Platinum1」と入力し、[Add] をクリックします。タグリストで「Platinum1」の [Include] ラジオボタンをクリックし、[Done] をクリックします。

ステップ 11 [Save and Publish] をクリックします。

プロファイル ルールがパブリッシュされます。

タグによるフィルタリング

フィルタリング用にタグを含む、または除外することを選択できます。

タグを含める

タグを含めるには、次の手順を実行します。

ステップ 1 プロキシミティルール（キャプティブポータルルール、エンゲージメントルール、プロファイルルール）の [Filter by Tags] エリアで、[Include] の [Add Tags] ボタンをクリックします。
ステップ 2 [Choose Tags] ウィンドウで、追加するタグの [Include] オプションボタンをクリックします。
ステップ 3 [Done] をクリックします。

タグの除外

タグを除外するには、次の手順を実行します。

ステップ 1 プロキシミティルール（キャプティブポータルルール、エンゲージメントルール、プロファイルルール）の [Filter by Tags] エリアで、[Exclude] の [Add Tags] ボタンをクリックします。
ステップ 2 [Choose Tags] ウィンドウで、除外するタグの [Exclude] オプションボタンをクリックします。
ステップ 3 [Done] をクリックします。

タグの検索

タグを検索するには、次の手順を実行します。

ステップ 1 新しいルールを作成するウィンドウの [Filter by Tags] エリアで、含める、または除外するために [Add Tags] ボタンをクリックします。
ステップ 2 [Choose Tags] ウィンドウに、検索するタグの名前を入力します。

タグのリストが検索結果でフィルタリングされます。

タグのクリア

タグの [Include] または [Exclude] オプションボタンを選択した場合、そのタグの **Clear Selection** オプションを使用して、選択内容をクリアすることができます。

ユーザーのオプトインオプション

Cisco DNA Spaces では、顧客が通知サブスクリプションからオプトアウトできるオプションをキャプティブ ポータルで提供できます。

ポータルで、[Allow users to opt in to receive message] チェックボックスをオンにして、サブスクリプションに登録するかどうかを選択するオプションを顧客に提供します。[Allow users to opt in to receive message] オプションは、認証タイプ [SMS with password verification] または [Email] で使用できます。

デフォルトでは、顧客はサブスクリプションにオプトインされています。顧客はキャプティブポータルにアクセスするときに、サブスクリプションからオプトアウトできます。顧客がSSIDに接続することでキャプティブポータルにアクセスすると、オプトインのチェックボックスが顧客に表示されます。

ロケーションペルソナルールのロケーションフィルタ

ロケーションを指定するには、次の手順を実行します。

1. [Add Locations] ボタンをクリックします。
2. 表示される [Choose Location] ウィンドウで、プロファイルルールのロケーションを選択します。
3. [OK] をクリックします。

ロケーションに定義されているメタデータを使用して、ロケーションを再度フィルタリングできます。選択したロケーション、その親および子のロケーションに定義されているメタデータのみを選択できます。

特定のメタデータのロケーションを含めるには、次の手順を実行します。

ステップ 1 [Filter by Metadata] チェックボックスをオンにします。

ステップ 2 [Filter] 領域で、[Add Metadata] ボタンをクリックします。

[Choose Location Metadata] ウィンドウが表示されます。

ステップ 3 ドロップダウン リストから、メタデータの変数を選択し、隣接フィールドに変数の値を選択します。

ステップ 4 [完了（Done）] をクリックします。

特定のメタデータのロケーションを除外するには、次の手順を実行します。

ステップ 1 [Filter by Metadata] チェックボックスをオンにします。

ステップ 2 [Exclude] 領域で、[Add Metadata] ボタンをクリックします。

[Choose Location Metadata] ウィンドウが表示されます。

ステップ 3 ドロップダウン リストから、メタデータの変数を選択し、隣接フィールドに変数の値を選択します。

ステップ 4 [OK] をクリックします。

ロケーションペルソナルールの管理

必要な場合はいつでも、ロケーションペルソナ（プロファイル）ルールを一時停止したり、再度有効にしたりできます。必要に応じてロケーションペルソナルールを変更し、削除することができます。ロケーション要素に固有のロケーションペルソナルールを作成し、ロケーション階層から表示できます。

ロケーションペルソナルールの一時停止

ロケーションペルソナルールを一時停止するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Location Personas] をクリックします。

表示される [Location Personas] ウィンドウに、既存のすべてのロケーションペルソナルールが示されます。

ステップ 2 一時停止するロケーションペルソナルールの右端に表示される [Pause Rule] アイコンをクリックします。

ロケーションペルソナルールが一時停止されます。

次のタスク

（注） 複数のロケーションペルソナルールを一時停止するには、一時停止するロケーションペルソナルールのチェックボックスをオンにし、ウィンドウの下部に表示される [Pause] ボタンをクリックします。

ロケーションペルソナルールの再開

ロケーションペルソナルールを再開するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Location Personas] をクリックします。

表示される [Location Personas] ウィンドウに、既存のすべてのロケーションペルソナルールが示されます。

ステップ 2 再開するロケーションペルソナルールの右端に表示される [Make Rule Live] アイコンをクリックします。

ロケーションペルソナルールが再開されます。

次のタスク

（注） 複数のロケーションペルソナルールを再開するには、再開するロケーションペルソナルールのチェックボックスをオンにし、ウィンドウの下部に表示される [Make Live] ボタンをクリックします。

ロケーションペルソナルールの変更

ロケーションペルソナルールを変更するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Location Personas] をクリックします。

表示される [Location Personas] ウィンドウに、既存のすべてのロケーションペルソナルールが示されます。

ステップ 2 変更するロケーションペルソナルールの [Edit Rule] アイコンをクリックします。

ステップ 3 必要な変更を加えます。

ステップ 4 変更を保存するには、[Save] をクリックします。または変更をパブリッシュするには、[Save and Publish] をクリックします。

（注） ライブルールに表示されるのは [Save and Publish] オプションのみです。[Save and Publish] ボタンをクリックすると、変更を反映したルールがパブリッシュされます。

ロケーションペルソナルールの削除

ロケーションペルソナルールを削除するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Location Personas] をクリックします。

表示される [Location Personas] ウィンドウに、既存のすべてのロケーションペルソナルールが示されます。

ステップ 2 削除するロケーションペルソナルールの右端に表示される [Delete Rule] アイコンをクリックします。

次のタスク

（注） 複数のロケーションペルソナルールを削除するには、削除するロケーションペルソナルールのチェックボックスをオンにし、ウィンドウの下部に表示される [Delete] ボタンをクリックします。

ロケーションに対するロケーションペルソナルールの表示

グループ、ビルディング、フロアなどのロケーションのロケーションペルソナルールを表示するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードの左上にある 3 本線のメニューアイコンをクリックします。

ステップ 2 [Location Hierarchy] を選択します。

[Location] ウィンドウがロケーション階層とともに表示されます。

ステップ 3 ロケーションペルソナルールを表示するロケーションをクリックします。

ステップ 4 [Rules] タブをクリックします。

ステップ 5 [Profile Rule] タブをクリックします。

ロケーションのロケーションペルソナルールが一覧表示されます。

次のタスク

（注） ロケーション階層の各ロケーションに表示される [Rules] リンクをクリックして、[Rules] タブにアクセスすることもできます。ロケーションの [Rules] リンクは、そのロケーションに少なくとも 1 つのプロキシミティルールが存在する場合にのみ有効になります。

ロケーション ペルソナ ルール レポート

ロケーション ペルソナ ルール レポートには、ロケーションペルソナルールのパフォーマンスが表示されます。これはロケーションペルソナルールに固有です。

ロケーションペルソナルールのロケーションペルソナ（プロファイル）ルールレポートを表示するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Location Personas] をクリックします。

表示される [Location Personas] ウィンドウに、既存のすべてのロケーションペルソナルールが示されます。

ステップ 2 ロケーション ペルソナ ルール レポートを作成するルールをクリックします。

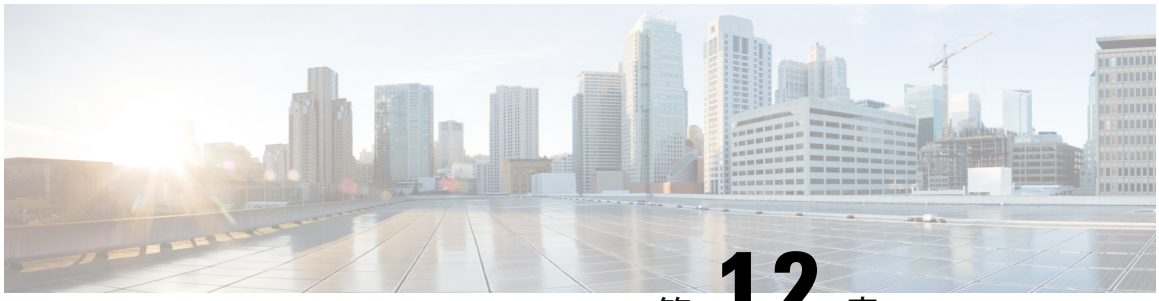
ステップ 3 [Filter] 領域で、レポートを表示する期間を選択します。

- [Total Devices Tagged]：ロケーションペルソナルールが作成された日以降の、ロケーションペルソナルールにタグ付けされたデバイスの総数。
- [Total Users Tagged]：ロケーションペルソナルールが作成された日以降の、ロケーションペルソナルールにタグ付けされた訪問者の総数。
- [Total Tags Removed]：ロケーションペルソナルールが作成された日以降の、ロケーションペルソナルールで指定したタグから削除された訪問者の総数。

ルールアクティビティ

このセクションには、指定した期間中に特定のロケーションペルソナルールに基づいてタグ付けされた顧客とデバイスの数が表示されます。

- [Tagging Trends]：指定した期間中に特定のルールでタグ付けされたデバイスと顧客の総数を表示します。特定のロケーションペルソナルールに基づいて、顧客がタグから削除した数も表示されます。折れ線グラフは、指定した期間の各日に追加または削除されたタグの総数を表します。指定した期間が 1 週間未満の場合、データは棒グラフで表示されます。指定した期間が 2 日以内の場合、グラフには、毎日のさまざまなタイミングでタグ付けされた顧客の数が表示されます。
- [Tags Added]：ルールで作成されたタグの総数を表示します。
- [Device Tags added by Location]：指定した期間中に各ロケーションからタグ付けされたデバイスの数を表示します。
- [Tags Removed by Location]：このセクションは、特定のタグからフィルタリングされたデバイスを削除するようにロケーションペルソナルールで指定されている場合にのみ表示されます。特定の期間中に特定のロケーションペルソナルールに基づいて、各ロケーションからタグ付けされていないデバイスの総数が表示されます。
- [Tagging by Time of Day]：この棒グラフには、指定した期間中の 1 日のさまざまなタイミングで、ロケーションペルソナルールに基づいてさまざまなタグに追加された顧客の数が表示されます。これは、このルールの対象となる顧客が対象のロケーションを最も多く訪問した時間を特定するのに役立ちます。



第 12 章

Cisco DNA Spaces Asset Locator アプリ

Cisco DNA Spaces Asset Locator アプリにより、アセットの監視、およびアセット、センサー、アラートシステム、および運用ワークフローのパフォーマンス最適化が可能になります。

• Cisco DNA Spaces 資産ロケータアプリの使用 （229 ページ）

Cisco DNA Spaces 資産ロケータアプリの使用

Cisco DNA Spaces 資産ロケータアプリでは、さまざまなタグとセンサーが提供され、接続運用を継続的に統合、監視、および管理できます。クラウドベースのインターフェイスを使用して、各資産のプロファイル、カテゴリ、および所有者を定義できます。ビジネスルールを確立して、資産とセンサーのワークフローおよび求められる動作範囲を定義できます。

Cisco DNA Spaces 資産ロケータの詳細については、「資産ロケータ」を参照してください。

第 13 章

モニタリング

この章では、Cisco DNA Spaces に表示されるモニタリングの詳細について説明します。

[Monitor] ウィンドウにアクセスするには、[Cisco DNA Spaces] ダッシュボードで、左上の 3 本線のメニューアイコンをクリックし、[Monitor] を選択します。

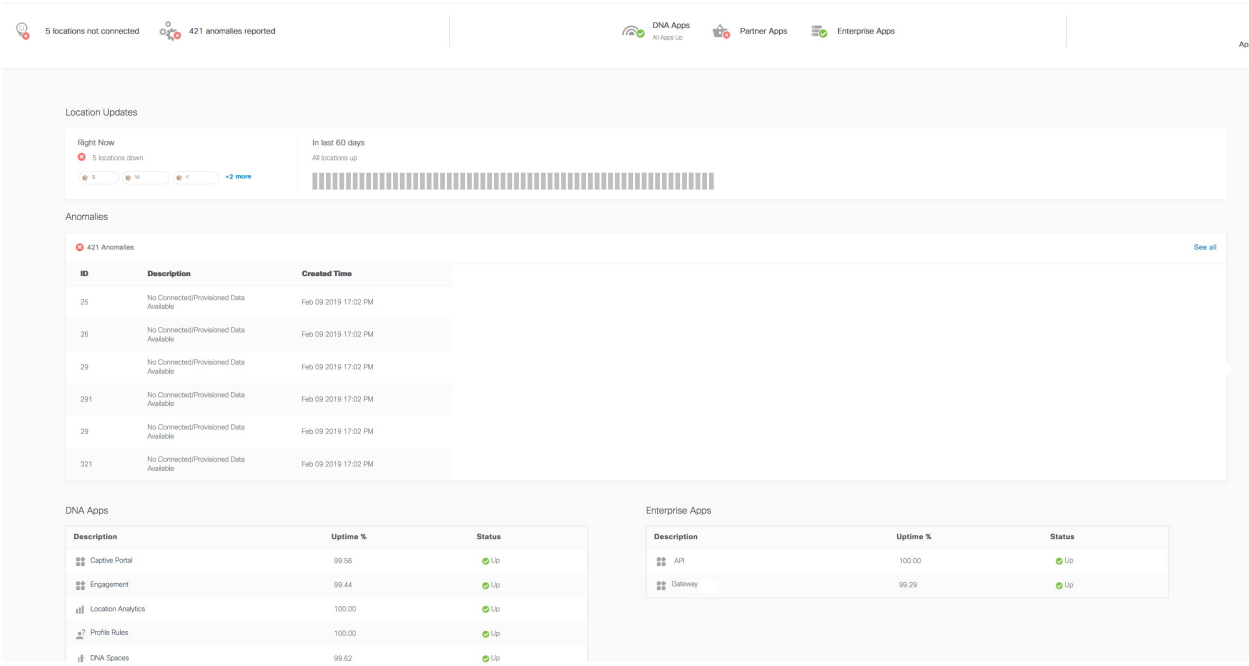
モニタリング

このセクションでは、[Monitor] セクションに表示される Cisco DNA Spaces の正常性の詳細について説明します。

Cisco DNA Spaces の [Monitor] セクションを以下の図に示します。

モニタリング

図 *13* : モニター



モニタリングセクションのヘッダーには、次の詳細が含まれます。

- **接続されているすべてのロケーション**：アクセスできるロケーションの現在のロケーション更新ステータスを表示します。すべてのロケーションからロケーションの更新を受信した場合、このセクションは「up」とマークされ、ステータスは **All Locations Connected** になります。ロケーションの更新に問題がある場合、このセクションは「donw」とマークされ、ロケーションの更新に問題があるロケーションの総数が表示されます。
- **異常の報告なし**：ロケーションの更新とロケーションのインターネットプロビジョニングの現在のステータスを表示します（これは、キャプティブポータルを介した顧客獲得を設定した場合にのみ該当します）。ロケーションの更新とインターネットプロビジョニングがすべてのロケーションで問題なく行われている場合、このセクションは「up」とマークされます。いずれかのロケーションでこのどれも発生していない場合、ステータスは「down」になります。ロケーションの更新とインターネット プロビジョニングの両方がロケーションで行われていない場合、そのロケーションがリストに表示されます。
- **DNA アプリ**：Cisco DNA Spaces アプリの現在のステータスを表示します。すべての Cisco DNA Spaces アプリが現在アクティブな場合、このセクションは「up」とマークされます。
- **パートナーアプリ**：Cisco DNA Spaces と統合されたパートナーアプリの現在のステータスを表示します。このセクションは、Cisco DNA Spaces と統合されているパートナーアプリが期待どおりに機能している場合、「up」とマークされます。パートナーアプリを Cisco DN Spaces と統合していない場合、またはパートナーアプリが期待どおりに機能していない場合、このセクションは「down」とマークされます。

- **エンタープライズアプリ**：Cisco DNA Spaces と統合されたエンタープライズアプリの現在のステータスを表示します。このセクションは、Cisco DNA Spaces と統合されているエンタープライズアプリが期待どおりに機能している場合、「up」とマークされます。エンタープライズアプリを Cisco DNA Spaces と統合していない場合、またはエンタープライズアプリが期待どおりに機能していない場合、このセクションは「down」とマークされます。
- **アプリ遅延**：このエリアには、アプリの現在の遅延ステータスが表示されます。

ロケーション情報更新

ロケーション情報の更新が行われていないロケーションが、この領域に表示されます。この領域には、過去 30 日間のロケーション情報の更新ステータスを示すバーも表示されます。バーの線は、それぞれ過去 30 日間の 1 日を表します。ロケーション情報の更新に問題がある日は、バーの対応する線が赤で表示されます。

異常

このエリアには、ロケーションで現在発生しているロケーション更新の問題とインターネットプロビジョニングの問題が表示されます（これはキャプティブポータルを介した顧客獲得を設定した場合にのみ該当します）。Cisco DNA Spaces アカウントにおける異常の合計数が一覧表示されます。

異常ごとに次の詳細が表示されます。

- [ID]：異常の ID。
- [Description]：ロケーション更新の問題か、それともインターネット プロビジョニングの問題かを説明します。
- [Created Time]：異常が記録された日時。

DNA アプリ

このエリアには、Cisco DNA Spaces によって提供されたアプリの過去 30 日間のステータスが表示されます。各 Cisco DNA Spaces アプリに関する次の詳細が表示されます。

次のアプリのステータスが表示されます。

- [Captive Portal]：キャプティブポータルアプリのステータスが表示されます。
- [Engagement]：エンゲージメントアプリのステータスが表示されます。
- [Location Analytics]：全ロケーションのロケーション更新のステータスが表示されます。
- [Location Personas]：ロケーションペルソナアプリのステータスが表示されます。

- [Cisco DNA Spaces] ：Cisco DNA Spaces ドメインのステータスが表示されます。Cisco DNA Spaces ドメインのステータスは、関連付けられているすべてのアプリがアクティブな場合にのみアクティブになります。

（注） Cisco DNA Spaces ドメインは、ドメインがすべての Cisco DNA Spaces の顧客に対して機能している場合にのみ、アップとマークされます。

アプリごとに次の詳細が表示されます。

- [Description]：アプリの名前。
- [Uptime %]：過去 30 日間のうち、アプリが稼働していた期間の割合。たとえば、過去 30 日の間、アプリが正常性の問題なしでずっとアクティブだった場合、[Uptime %] の値は 100 % になります。
- [Status]：アプリの現在のステータスが表示されます。

アプリのステータスを判定する際、次の正常性プロパティが考慮されます。

- [Captive Portal]：ポータルの正常性、ルールエンジンの正常性、サブスクライバの正常性、電子メール検証の正常性、SMS の正常性、データベースの正常性。
- Cisco DNA Spaces：Vault の正常性、ダッシュボードの正常性、DMS の正常性、TMS の正常性。
- [Engagement]：ダッシュボードの正常性、サブスクライバの正常性、サーバーの正常性、ロケーション受信者の正常性、DMS の正常性、電子メール検証の正常性、SMS の正常性、データベースの正常性。
- [Location Analytics]：ダッシュボードの正常性、サブスクライバの正常性、サーバーの正常性、ロケーション受信者の正常性、データベースの正常性。
- [Location Personas]：ダッシュボードの正常性、サブスクライバの正常性、サーバーの正常性、ロケーション受信者の正常性、データベースの正常性。

アプリ遅延

この領域には、アプリに関連する遅延のステータスが過去 30 日間に渡って表示されます。

アプリ遅延の次の詳細が表示されます。

- [Description]：アプリの名前（例：Kafka サーバー）。
- [Latency]：過去 30 日間の、アプリ遅延ステータスが [Up] であった期間の割合。 たとえば、過去 30 日間の1 日で Kaftka サーバーのアプリ遅延が 発生した場合、遅延の値は 96.6 % になります。
- [Status]：アプリ遅延の現在のステータス。

エンタープライズアプリ

この領域には、エンタープライズアプリのステータスが過去 30 日間に渡って表示されます。

次のエンタープライズアプリの詳細が表示されます。

- [Description]：エンタープライズアプリの名前。
- [Uptime Percentage]：過去 30 日間の、エンタープライズアプリが稼働していた期間の割合。
- [Status]：エンタープライズアプリの現在のステータス。

パートナーアプリ

この領域には、アクティブ化したすべてのアプリの稼働時間と正常性ステータスが表示されます。パートナーアプリのステータス概要は、[Summary] セクションに表示されます。

パートナー アプリの次の詳細が表示されます。

- [Partner Name]：パートナーの名前。
- [AppName]：パートナーアプリの名前。
- [Uptime %]：パートナーアプリが稼働していた期間の割合。
- [Status]：パートナーアプリの現在のステータス。

第 14 章

Cisco DNA Spaces のユーザーとアカウントの管理

この章では、Cisco DNA Spaces ユーザーを招待および管理する方法について説明します。

Cisco DNA Spaces ユーザーの管理

Cisco DNA Spaces では、ユーザーが実行するロールに基づいて、ユーザーにさまざまな権限が付与されます。

Cisco DNA Spaces ユーザーの招待

Cisco DNA Spaces アカウントが作成されると、提供された電子メール ID を持つアカウントに対して Dashboard Admin Role ユーザーが作成されます。このダッシュボード管理者は、他のユーザーを Cisco DNA Spaces に招待できます。

Cisco DNA Spaces は、デフォルトのユーザーロールである Dashboard Admin Role のみを提供します。デフォルトでは、Dashboard Admin Role には、DNASpaces（ダッシュボードの左ペインのメニュー項目、および Behavior Metrics、OpenRoaming、Location Analytics、Location Analytics、Location Personas の各アプリを含む）、CaptivePortalsおよび OperationsInsights の各ロールタイプに対してのみ読み取りおよび書き込みアクセス権が付与されます。

（注）

- Dashboard Admin Role が BLEManager などの他のロールタイプ（アプリ）へのアクセス権を必要とする場合は、Cisco DNA Spaces サポートチームに連絡する必要があります。
- デフォルトでは、SEE（Base）ライセンスの Dashboard Admin Role では、DNASpaces にのみアクセスできます。

Cisco DNA Spaces では、さまざまなアプリへのさまざまなアクセス権を持つユーザーロールを定義できます。たとえば、Captive Portals アプリでは読み取りと書き込みのパーミッションを持ち、Operational Insights アプリでは読み取り専用のパーミッションを持つユーザーロールを作成できます。

アカウントで特定のサービスが有効になっている場合は、ユーザーロールに次のロールタイプ（アプリ）を含めることができます。

- [DNASpaces]：このロールタイプは、[Location Hierarchy]、[Admin Management]、[Monitoring and Support]、[Setup] など、Cisco DNA Spaces ダッシュボードの左ペインにあるすべてのメニュー項目へのアクセスを提供します。さらに、このロールタイプは、Behavior Metrics、OpenRoaming、Behavior Metrics、Engagements、Location Personas などのアプリへのアクセスを提供します。

  [Asset Locator]：このロールタイプは、Asset Locator アプリへのアクセス権を提供します。

- [Detect and Locate]：このロールタイプは、Captive Detect and Locate アプリへのアクセス権を提供します。
- [CaptivePortals]：このロールタイプは、Captive Portals アプリへのアクセス権を提供します。
- [MapService]：このロールタイプは、[Map Service] へのアクセス権を提供します。
- [IoT Services]：のロールタイプは、[IoT Services] へのアクセス権を提供します。
- [Location Analytics]：このロールタイプは、Location Analytics アプリへのアクセス権を提供します。

（注） Map Services へのアクセスは、DNASpaces の一部としては提供されなくなりました。ただし、MapServices のロールへの割り当ては、DNASpaces の割り当てと同時に行う必要があります。たとえば、MapServices への読み取りおよび書き込みアクセスと、DNASpaces への読み取り専用アクセスを持つロールを作成できます。

Dashboard Admin ロールの場合、Location Analytics へのアクセスはデフォルトで提供されます。他のロールについては、アクセスを個別に割り当てる必要があります。ただし、Location Analytics のロールへの割り当ては、DNASpaces サービスの割り当てと同時に行う必要があります。たとえば、Location Analytics への読み取りおよび書き込みアクセスと、DNASpaces への読み取り専用アクセスを持つロールを作成できます。[Location Analytics] タイルは、Location Analytics へのアクセス権のない Cisco DNA Spaces ユーザーアカウントでは無効になります。

Cisco DNA Spaces ユーザーを招待するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、[Admin Management] を選択します。

ステップ 2 [Invite Admin] をクリックします。

ステップ 3 [Invite Admin] ウィンドウで、次の詳細を入力します。

a) [Email] フィールドで、追加するユーザーの電子メールアドレスを入力します。
b) [Role Name] ドロップダウンリストから、このユーザーに提供するユーザーロールを選択します。

デフォルトのユーザーロール、および以前に定義したユーザーロールが、選択用のドロップダウンリストに表示されます。必要なユーザーロールがない場合は、[Create New Role] を使用してユーザーロールを定義できます。新規ユーザーロールの作成の詳細については、「ユーザーロールの作成」を参照してください。定義されているすべてのユーザーロールが [Roles] タブに一覧表示されます。

c) [Invite] をクリックします。

（注）
- [Invite Admin] ボタンは、読み取りおよび書き込み権限を持つ Cisco DNA Spaces 管理者のみが使用できます。
- Captive Portals などの一部のアプリには、その特定のアプリのユーザーを管理するためのプロビジョニングが含まれます。たとえば、読み取り/書き込み権限を持つ Captive Portals アプリユーザーは、 Captive Portals アプリの [User Management] オプションから、ユーザーロール Creative User または AccessCodeManger を持つユーザーを招待できます。Admin Management ユーザーが [User Management] ウィンドウに表示されますが、Captive Portals アプリの [User Management] オプションからは、[Admin Management] で作成されたユーザーアカウントを変更することはできません。

ユーザー ロールの作成

Cisco DNA Spaces ユーザーロールを作成するには、次の手順を実行します。

ステップ 1 [Cisco DNA Spaces] ダッシュボードで、[Admin Management] をクリックします。

ステップ 2 [Roles] タブをクリックし、[Create Role] をクリックします。

（注） [Invite Admin] ウィンドウの [Role Name] ドロップダウンリストで [Create New Role] をクリックする方法もあります。

ステップ 3 [Create New Role] ウィンドウで、次の詳細を入力します。

a) [ROLE NAME] フィールドに、ユーザーロールの名前を入力します。
b) [APPS] エリアで、このユーザーロールに提供するロールタイプのチェックボックスをオンにします。

ロールタイプ（アプリ）の詳細については、Cisco DNA Spaces ユーザーの招待 （237 ページ）で説明されているロールタイプを参照してください。

c) 各ロールタイプに表示されるドロップダウンリストから、特定のユーザーロールに付与するアクセス権を選択します。

アクセス権を [Read Only] または [Read/Write] に設定することができます。

たとえば、ダッシュボードのメニュー項目への完全なアクセス権と、キャプティブポータルアプリへの読み取り専用アクセス権を持つユーザーロールを作成する場合は、[DNA Spaces] チェックボックス

をオンにして、対応するドロップダウンリストから [Read/Write] を選択します。次に、[Captive Portal] チェックボックスをオンにし、対応するドロップダウンリストから [Read only] を選択します。

d) [作成（Create）] をクリックします。

[Invite Admin] ウィンドウの [Role Name] ドロップダウンリストにユーザーロールが表示されるようになります。

Cisco DNA Spaces ユーザーの編集

「読み取り」および「書き込み」権限を持つダッシュボード管理ユーザーは、ユーザーのユーザーロールを変更できます。たとえば、ダッシュボード管理者の「読み取り」は、ダッシュボード管理者の「読み取り」および「書き込み」ユーザーに昇格できます。

Cisco DNA Spaces ユーザーのユーザー権限を変更するには、次の手順を実行します。

ステップ 1 **Cisco DNA Spaces** ダッシュボードで、[Admin Management] を選択します。

Cisco DNA Spaces ユーザーの電子メール ID のリストを含む [Admin] ページが表示されます。

ステップ 2 編集するユーザーの電子メール ID の右端にある [Edit] アイコンをクリックします。

[Invite Admin] ウィンドウが表示されます。

ステップ 3 [Role Name] ドロップダウンリストから、ユーザーに付与するアクセスのタイプを選択します。

デフォルトのユーザーロール、および以前に定義したユーザーロールが、選択用のドロップダウンリストに表示されます。必要なユーザーロールがない場合は、[Create New Role] を使用してユーザーロールを定義できます。新規ユーザーロールの作成の詳細については、「**ユーザーロールの作成**」を参照してください。

ステップ 4 [更新（Update）] をクリックします。

Cisco DNA Spaces ユーザーの削除

あるユーザーが Cisco DNA Spaces にアクセスする必要がなくなった場合は、そのようなユーザーを Cisco DNA Spaces のユーザーリストから削除することを推奨します。[Dashboard Admin Role] のユーザーは、他のユーザーを削除できます。

既存の Cisco DNA Spaces ユーザーを削除するには、次の手順を実行します。

ステップ 1 [Cisco DNA Spaces] ダッシュボードで、[Admin Management] を選択します。

[Admins] ページに、Cisco DNA Spaces ユーザーのリストが表示されます。

ステップ 2 削除するユーザーの電子メール ID の右端にある [Delete] アイコンをクリックします。

複数のユーザーを削除する場合は、対応する電子メール ID のチェックボックスをオンにして、ウィンドウの右上に表示される [Delete Admins] をクリックします。

God Admin

Cisco DNA Spaces は、シスコ社内ユーザーのみが使用できる God Admin ダッシュボードにアクセスするための God Admin ユーザーロールを提供します。現在、一度に利用できる God Admin アカウントの数に制限を設けています。[チーム] オプションでは、God Admin ユーザーロールの作成をサポートしていません。このユーザーロールは、Cisco DNA Spaces チームによって内部的に作成されています。God Admin ダッシュボードは、すべての Cisco DNA Spaces のお客様のデータに基づいて生成されたレポートを提供し、シスコが Cisco DNA Spaces の全体的なパフォーマンスを分析するのに役立ちます。

God Admin ダッシュボードに表示されるデータは次のとおりです。

- ロケーションの総数
- AP の総数
- ロケーション情報更新の総数
- Cisco DNA Spaces がカバーする総平方フィート面積
- 訪問および訪問者の総数
- マップビューおよびリストビューでのロケーション別の訪問者数
- 上位 5 つのロケーション
- さまざまな訪問時間範囲における滞在時間
- さまざまな訪問時間範囲における訪問回数
- 時間ごとの訪問数のグラフ
- キャプチャされた携帯電話番号の件数、電子メール ID の数、名前の数と、性別がキャプチャされた訪問者の数。
- オプトインユーザーの数

Cisco DNA Spaces のアカウントの管理

この項では、Cisco DNA Spaces アカウントを管理する方法について説明します。

Cisco DNA Spaces パスワードの変更

アプリケーションのセキュリティ向上のため、Cisco DNA Spaces のパスワードを頻繁に変更することをお勧めします。

Cisco DNA Spaces アカウントのパスワードを変更するには、以下の手順に従います。

ステップ 1 Cisco DNA Spaces ダッシュボードで、ダッシュボードの右端に表示される [User Account] アイコンをクリックします。

ステップ 2 [Change Password] をクリックします。

ステップ 3 表示されるウィンドウで、次の手順を実行します。

a) [Current Password] フィールドに、Cisco DNA Spaces アカウントの現在のパスワードを入力します。
b) [New Password] フィールドに、Cisco DNA Spaces アカウントの新しいパスワードを入力します。
c) [Confirm Password] フィールドに、確認のために新しいパスワードを再入力します。
d) [Change Password] をクリックします。

パスワードの強度（Password Strength）

Cisco DNA Spaces パスワードには、次のパラメータが必要です。

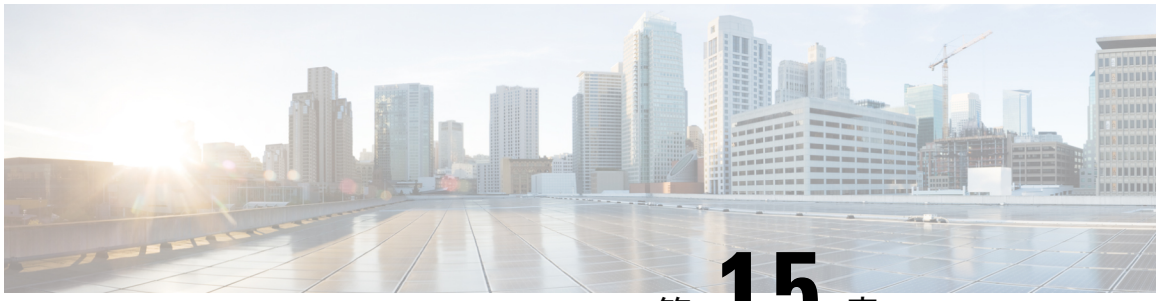
- 8 文字以上。
- 1 つ以上の大文字（A-Z）
- 1 つ以上の小文字（A-Z）
- 1 つ以上の特殊文字
- 1 つ以上の数字（0-9）

Cisco DNA Spaces からのサインアウト

Cisco DNA Spaces からサインアウトするには、次の手順を実行します。

ステップ 1 **Cisco DNA Spaces** ダッシュボードで、ダッシュボードの右端に表示される [User Account] アイコンをクリックします。

ステップ 2 **[Logout]** をクリックします。



第 15 章

Cisco DNA Space におけるシスコ ワイヤレス コントローラおよび Cisco Catalyst 9800 シリーズ コントローラの設定

この章では、Cisco DNA Spaces で動作するシスコ ワイヤレス コントローラ（Cisco AireOS）または Cisco Catalyst 9800 シリーズ コントローラで行う設定について説明します。必要な設定は、使用するワイヤレスコントローラのタイプとコネクタによって異なります。

（注）

- ハイパーロケーションを備えたシスコ ワイヤレス コントローラを Cisco DNA Spaces と Cisco CMX に同時に接続することはできません。
- シスコ ワイヤレス コントローラを Cisco CMX と Cisco DNA Spaces の両方に同時に接続する場合は、 Cisco DNA Spaces コネクタを使用する必要があります。シスコ ワイヤレス コントローラがサポートできる NMSP 接続数の制限を確認し、シスコ ワイヤレス コントローラが Cisco DNA Spaces コネクタへの新しい接続の追加をサポートできることを確認します（特に、複数の Cisco CMX サーバーへの既存の接続がある場合）。
- シスコ ワイヤレス コントローラを Cisco WLC Direct Connect と Cisco DNA Spaces コネクタの両方に同時に接続することはできません。Cisco DNA Spaces コネクタを使用する前に、Cisco WLC Direct Connect を無効にします。
- 特に古いバージョンのシスコ ワイヤレス コントローラを使用している場合は、Cisco WLC Direct Connect ではなく Cisco DNA Spaces コネクタを使用することをお勧めします。また、Operation Insights、Detect and Locate などの特定のアプリは、Cisco DNA Spaces コネクタによってのみサポートされます。
- ワイヤレスネットワークに表示されるデータを Cisco DNA Spaces レポートに表示されるデータと比較することは推奨されません。これは設計上、遅延することが予想されるためです。

（注） 設定はCisco DNA Spacesの一部ではない外部アプリケーションで行うため、このマニュアル内のメニューパス、タブやウィンドウ、オプションなどに指定する名前が変わる場合があります。

さまざまなコネクタタイプでサポートされる機能、およびワイヤレスコントローラとコネクタのさまざまな組み合わせの設定は次のとおりです。

- 各種コネクタがサポートする機能 （244 ページ）
- Cisco CMX を介して Cisco DNA Spaces をシスコ ワイヤレス コントローラに接続する （248 ページ）
- WLC 直接接続または Cisco DNA Spaces コネクタを使用した、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラまたはシスコ ワイヤレス コントローラの Cisco DNA Spaces への接続 （262 ページ）
- Cisco DNA Spaces 拡張ベンチマーク （296 ページ）

各種コネクタがサポートする機能

次の表に、各タイプのコネクタでサポートされている機能を示します。使用する機能またはアプリに基づいてコネクタを選択できます。Operational Insights や Open Roaming などのアプリを使用する場合は、Cisco DNA Spaces コネクタをお勧めします。

表 *11* : コネクタ：機能サポート

機能/アプリ	Cisco DNA Spaces コネクタ	**Cisco WLC Direct Connect**（小規模な展開でのみ推奨）[1] Cisco WLC Direct Connect を使用した Cisco DNA Spaces のシスコ ワイヤレス コントローラへの接続 Cisco WLC Direct Connect を使用した Cisco DNA Spaces の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラへの接続	Cisco CMX を使用した Cisco AireOS/ シスコ ワイヤレス コントローラのロケーション階層の定義	Cisco DNA Spaces を使用するための Cisco Meraki の設定
Cisco DNA Spaces ダッシュボード	Cisco DNA Spaces ダッシュボード	Cisco DNA Spaces ダッシュボード	Cisco DNA Spaces ダッシュボード	Cisco DNA Spaces ダッシュボード
キャプティブポータル	キャプティブポータルアプリの使用	キャプティブポータルアプリの使用	キャプティブポータルアプリの使用	キャプティブポータルアプリの使用
エンゲージメント	Engagements アプリによる通知の送信	Engagements アプリによる通知の送信	Engagements アプリによる通知の送信	Engagements アプリによる通知の送信
ロケーションペルソナ	Location Personas アプリによるタグの作成	Location Personas アプリによるタグの作成	Location Personas アプリによるタグの作成	Location Personas アプリによるタグの作成
位置分析	ロケーション分析レポート	ロケーション分析レポート	ロケーション分析レポート	ロケーション分析レポート
影響分析	影響分析	影響分析	影響分析	影響分析
カメラメトリック	カメラメトリック	カメラメトリック	カメラメトリック	カメラメトリック
行動メトリクス	行動メトリクス	行動メトリクス	行動メトリクス	行動メトリクス
RightNow WiFi	Right Now	Right Now	Right Now	Right Now
RightNow Video	Right Now	Right Now	Right Now	Right Now
Open Roaming[2]	サポート対象	未サポート	未サポート	サポート対象

機能/アプリ	Cisco DNA Spaces コネクタ	**Cisco WLC Direct Connect**（小規模な展開でのみ推奨）[1] Cisco WLC Direct Connect を使用した Cisco DNA Spaces のシスコ ワイヤレス コントローラへの接続 Cisco WLC Direct Connect を使用した Cisco DNA Spaces の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラへの接続	Cisco CMX を使用した Cisco AireOS/シスコ ワイヤレス コントローラのロケーション階層の定義	Cisco DNA Spaces を使用するための Cisco Meraki の設定
IoT サービス	サポート対象[3]	未サポート	未サポート	—
検出と位置特定	サポートあり	限定サポート（関連クライアントのみ）	サポートあり	—
HyperLocation	サポートあり	未サポート	サポートあり	未サポート
FastLocate	サポートあり	未サポート	サポートあり	未サポート
スケールのサポート 詳細については、Cisco DNA Spaces 拡張ベンチマーク（296 ページ）のスケールの概要を参照してください。	スケーリングに最適	AireOS コントローラ 8.8 MR2 および Cisco Catalyst 9800 シリーズ 16.12.1 ではスケールがサポートされます。最大 50 クライアント。	Cisco CMX が処理できるスケールをサポートします。	スケーリングに最適
AireOS コントローラ プラットフォームのサポート	サポート対象	サポート対象	サポート対象	N/A

機能/アプリ	Cisco DNA Spaces コネクタ	**Cisco WLC Direct Connect**（小規模な展開でのみ推奨）[1] Cisco WLC Direct Connect を使用した Cisco DNA Spaces のシスコ ワイヤレス コントローラへの接続 Cisco WLC Direct Connect を使用した Cisco DNA Spaces の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラへの接続	Cisco CMX を使用した Cisco AireOS/ シスコ ワイヤレス コントローラのロケーション階層の定義	Cisco DNA Spaces を使用するための Cisco Meraki の設定
Cisco Catalyst 9800 プラットフォームのサポート	サポート対象	サポート対象	サポート対象	N/A

[1] シスコ ワイヤレス コントローラの直接接続方式による接続は、小規模な展開でのみ推奨されます。大規模な実稼働展開には、すべて Cisco DNA Spaces コネクタが必要です。
[2] **Open Roaming** アプリはベータ版であるため、現在、このアプリのドキュメントは利用できません。**Open Roaming** に関連する情報については、Cisco DNA Spaces サポートチームにお問い合わせください。
[3] 現在、IoT サービスのサポートは Cisco Catalyst 9800 コントローラでのみ利用可能です。

（注）

- シスコ ワイヤレス コントローラの直接接続方式による接続は、小規模な展開でのみ推奨されます。大規模な実稼働展開には、すべて Cisco DNA Spaces コネクタが必要です。
- **Open Roaming** アプリはベータ版であるため、現在、このアプリのドキュメントは利用できません。**Open Roaming** に関連する情報については、Cisco DNA Spaces サポートチームにお問い合わせください。

Cisco CMX を介して Cisco DNA Spaces をシスコ ワイヤレス コントローラに接続する

Cisco CMX を介して Cisco DNA Spaces をシスコ ワイヤレス コントローラに接続するには、Cisco CMX 10.6 以降が必要です。

Cisco CMX を使用している Cisco Unified Wireless Network の場合、Cisco DNA Spaces と連携するには、次の構成が必要です。

（注）
- インターネット プロビジョニングと RADIUS 認証の構成は、RADIUS 認証が必要な場合にのみ必要です。この構成は、ポータルにソーシャル認証が必要な場合にのみ必要です。

WLC でのアクセスポイントモード、SSID、ACL、スプラッシュ URL、および仮想インターフェイスの設定

キャプティブポータルルールを作成するには、まずアクセスポイントのモードを定義し、シスコ ワイヤレス コントローラで SSID と ACL を作成します。また、SSID のスプラッシュ URL がシスコ ワイヤレス コントローラで設定されていることを確認する必要があります。

（注） SSID と ACL は、Cisco CMX ではなく、シスコ ワイヤレス コントローラで作成されます。

ローカルモードと flexconnect モードでシスコ ワイヤレス コントローラの設定は異なります。

（注） 設定は Cisco DNA Spaces の一部ではないシスコ ワイヤレス コントローラで行うため、このマニュアル内のメニューパス、タブやウィンドウ、オプションなどに指定する名前が変わる場合があります。

Cisco DNA Spaces を使用したローカルモードの設定

シスコ ワイヤレス コントローラ を、ローカルモードの Cisco DNA Spaces を使用するように設定するには、次の手順を実行します。

アクセス ポイントのローカル モードを設定する

アクセス ポイントのローカル モードを設定するには、次の手順を実行します。

ステップ 1 シスコ ワイヤレス コントローラのログイン情報を使用して、ワイヤレスコントローラにログインします。

ステップ 2 シスコ ワイヤレス コントローラのメインウィンドウで、[Wireless] タブをクリックします。

すべてのアクセス ポイントが一覧表示されます。

ステップ 3 モードをローカルに設定するアクセス ポイントをクリックします。

ステップ 4 [General] タブをクリックします。

ステップ 5 [AP Mode] ドロップダウンリストから、[Local] を選択して、[Apply] をクリックします。

シスコ ワイヤレス コントローラでの SSID の作成

（注） SSID は、Cisco CMX ではなく、シスコ ワイヤレス コントローラで作成されます。

シスコ ワイヤレス コントローラで SSID を作成するには、次の手順を実行します。

ステップ 1 シスコ ワイヤレス コントローラのメインウィンドウで、[WLANs] タブをクリックします。

ステップ 2 WLAN を作成するには、ウィンドウの右側にあるドロップダウンリストで [Create New] を選択し、[Go] をクリックします。

ステップ 3 表示される [New] ウィンドウで、[Type]、[Profile Name]、[SSID] などの WLAN の詳細を入力します。

ステップ 4 [Apply] をクリックします。

[Edit <SSID Name>] ウィンドウが表示されます。

ステップ 5 SSID を Cisco DNA Spaces ダッシュボードに追加します。

ステップ 6 シスコ ワイヤレス コントローラ メインウィンドウの [General] タブで、[Broadcast SSID] チェックボックスをオフにします。

（注） SSID ブロードキャストが中断され、設定を完了する前に顧客が SSID にアクセスすることが回避されます。

ステップ 7 **[Security]** > **[Layer 2]** を選択して、[MAC Filtering] チェックボックスをオンにします。

ステップ 8 [Layer 3] タブで、次を設定します。

a) [Layer 3 security] ドロップダウンリストから、[Web Policy] を選択します。

（注） [Web Policy] は、シスコ ワイヤレス コントローラでキャプティブポータルを設定できるようにする Layer 3 セキュリティのオプションです。

b) [On Mac Filter Failure] ラジオボタンを選択します。

c) [Preauthentication ACL] 領域で、[IPv4] ドロップダウンリストから、先に定義した ACL を選択します。

d) スリープ状態のクライアントの [Enable] チェックボックスをオンにします。

（注） スリープ状態のクライアントを有効にすることは必須ではありません。ただし有効にすると、認証後にスリープモードになっている顧客が指定された時間内にスリープ状態から復帰した場合、認証なしで接続されます。Web 認証に成功したゲストアクセスを持つクライアントは、ログインページから別の認証プロセスを実行せずにスリープおよび復帰することを許可されています。再認証が必要になるまでスリープ状態にあるクライアントが記録される期間を設定できます。有効な範囲は 1 時間から 720 時間（30 日）で、デフォルトは 12 時間です。これがセッション タイムアウトと同じになるのが理想的です。

e) [Over-ride Global Config] の [Enable] チェックボックスをオンにします。

（注） [Override global config] を有効にすると、顧客を外部 URL である Cisco DNA Spaces URL にリダイレクトできます。

f) [Web Auth Type] ドロップダウンリストから [External (Redirect to External Server)] を選択します。

（注） Cisco DNA Spaces ページはコントローラではなく外部サーバーでホストされるため、[Web Auth Type] は [External] である必要があります。

g) 表示される [URL] フィールドに、Cisco DNA Spaces のスプラッシュ URL を入力します。

CUWN または AireOS アカウントのスプラッシュ URL を表示するには、Cisco DNA Spaces ダッシュボードの [SSIDs] ウィンドウで AireOS SSID の [Configure Manually] リンクをクリックします。[Configure Manually] リンクは、Cisco AireOS SSID を追加した後にのみ表示されます。

（注） オンボーディング中に顧客が Cisco DNA Spaces Web ページにリダイレクトされるようにスプラッシュページを設定する必要があります。

h) [Apply] をクリックします。

ステップ 9 [Advanced] タブをクリックします。

ステップ 10 [Enable Session Timeout] フィールドに、必要なセッションタイムアウト値を秒単位で入力します。たとえば、セッションタイムアウトが 30 分の場合は、1800 と入力します。

ステップ 11 [Apply] をクリックします。

ステップ 12 [General] タブで、[Status] および [Broadcast SSID] オプションの [Enabled] チェックボックスをオンにして、SSID を有効にします。

ステップ 13 コマンドプロンプトで次のコマンドを実行して、キャプティブバイパスを無効にします。次に、ワイヤレスコントローラを再起動します。

config network web-auth captive-bypass disable Management > HTTP-HTTPS

（注） キャプティブバイパスが有効になっている場合、CNA は iOS デバイスに対してポップアップしません。

ステップ 14 表示される [HTTP-HTTPS configuration] ウィンドウで、次を実行します。

a) [HTTP Access] ドロップダウンリストから、[Disabled] を選択します。
b) [HTTPS Access] ドロップダウンリストから、[Enabled] を選択します。
c) [WebAuth SecureWeb] ドロップダウンリストから、[Disabled] を選択します。
d) [Apply] をクリックします。

ステップ 15 **[Security]** > **[Web Auth]** > **[Web Login Page]** の順に選択し、[Redirect URL after login] フィールドが空白であることを確認します。

（注） リダイレクト URL フィールドは、[Layer 3] で設定された Cisco DNA Spaces のスプラッシュ URL を上書きしないように空白にする必要があります。

次のタスク

（注） [Management] タブに変更を加えた場合は、変更を反映するためにシスコ ワイヤレス コントローラを再起動します。

アクセス コントロール リストを作成する

顧客のインターネットアクセスを制限し、SSID に接続したときに Cisco DNA Spaces スプラッシュページ URL へのアクセスのみを許可するには、ACL で Cisco DNA Spaces の IP（ウォールガーデン範囲）を設定する必要があります。これで、顧客が SSID に接続すると、スプラッシュページが顧客に表示されます。

ACL で一部の必要な IP が設定されていない場合、Cisco DNA Spaces が外部 URL と見なされ、顧客に対して複数回のリダイレクトが発生します。

アクセス コントロール リストを作成するには、次の手順を行います。

ステップ 1 シスコ ワイヤレス コントローラのログイン情報を使用して、ワイヤレスコントローラにログインします。

ステップ 2 **[Security]** > **[Access Control Lists]** > **[Access Control Lists]** を選択します。

ステップ 3 ACL を追加するには、[New] をクリックします。

ステップ 4 表示される [New] ウィンドウに、次のように入力します。

a) [Access Control List Name] フィールドに新しい ACL の名前を入力します。

（注） 最大 32 文字の英数字を入力できます。

b) ACL タイプとして [IPv4] を選択します。

c) [Apply] をクリックします。

ステップ 5 [Access Control Lists] ウィンドウが再度表示されたら、新しい ACL の名前をクリックします。

ステップ 6 表示される [Edit] ウィンドウで、[Add New Rule] をクリックします。

[Rules] > **[New]** ウィンドウが表示されます。

ステップ 7 必要なウォールガーデンの範囲にこの ACL のルールを設定します。

ウォールガーデンの範囲を表示するには、[Cisco DNA Spaces] ダッシュボードの [SSIDs] ウィンドウで、Cisco Unified Wireless Network SSID の [Configure Manually] リンクをクリックします。ウォールガーデンの範囲は、キャプション [Creating the Access Control List] の下に一覧表示されています。[Configure Manually] リンクは、Cisco AireOS SSID を追加した後にのみ表示されます。

ACL ルールを定義するときには、次のように値を設定します。

- **Direction**：Any
- **Protocol**：Any
- **Source Port Range**：0-65535
- **Destination Port Range**：0-65535
- **DSCP**：Any
- **Action**：Permit

ステップ 8 ポータルにソーシャル認証を装備する場合は、ソーシャル認証用にウォールガーデン範囲も構成する必要があります。

（注） ソーシャル認証用に設定されたこのウォールガーデン範囲により、顧客は SSID に接続した後、キャプティブポータルを使用せずに、すべての HTTPS Web サイトに直接アクセスできます。

仮想インターフェイスの設定

仮想インターフェイスを設定するには、次の手順を実行します。

ステップ 1 **[Controller]** > **[Interfaces]** を選択します。

ステップ 2 [Virtual] リンクをクリックします。

ステップ 3 表示される **[Interfaces]** > **[Edit]** ページで、次のパラメータを入力します。

a) [IP address] フィールドに、未割り当ておよび未使用のゲートウェイ IP アドレス（存在する場合）を入力します。

b) [DNS Host Name] フィールドに、DNS ホスト名（存在する場合）を入力します。

（注） 理想的には、このフィールドは空白になります。

（注） 接続して Web 認証を確立するには、DNS サーバは常に仮想インターフェイスをポイントしている必要があります。仮想インターフェイスに DNS ホスト名が設定されている場合は、クライアントが使用する DNS サーバ上で同じ DNS ホスト名が設定されている必要があります。

c) [Apply] をクリックします。

（注） 仮想インターフェイスに変更を加えた場合は、変更を反映するためにシスコ ワイヤレス コントローラを再起動します。

Cisco DNA Spaces を使用するための FlexConnect モードの設定

中央スイッチまたはローカル スイッチのモードに FlexConnect を設定できます。

FlexConnect 中央スイッチ モード

FlexConnect 中央スイッチモードで Cisco DNA Spaces を使用するようにシスコ ワイヤレス コントローラを設定するには、次の手順を実行します。

アクセス ポイントの *FlexConnect* モードを設定する

この設定は、FlexConnect の中央スイッチおよびローカルスイッチモードに適用されます。アクセスポイントに FlexConnect 中央スイッチモードを設定するには、次の手順を実行します。

ステップ 1 シスコ ワイヤレス コントローラのメインウィンドウで、[Wireless] タブをクリックします。

すべてのアクセス ポイントが一覧表示されます。

（注） アクセスポイントの詳細については、シスコ ワイヤレス コントローラのユーザーガイドを参照してください。

ステップ 2 モードを FlexConnect に設定するアクセス ポイントをクリックします。

ステップ 3 [General] タブをクリックします。

ステップ 4 [AP Mode] ドロップダウンリストから [FlexConnect] を選択します。

ステップ 5 [Apply] をクリックして変更を適用し、アクセス ポイントをリブートします。

シスコ ワイヤレス コントローラでの *FlexConnect* 中央スイッチモード用の *SSID* の作成

ローカルモードの場合と同じ手順で SSID を作成します。詳細については、シスコ ワイヤレス コントローラでの SSID の作成 （249 ページ）を参照してください。

FlexConnect 中央スイッチ モードのアクセス制御リストの作成

ローカル モードの場合と同じ手順を使用して、アクセス コントロール リストを作成します。詳細については、アクセス コントロール リストを作成する （251 ページ）を参照してください。

仮想インターフェイスの設定

仮想インターフェイスを設定するには、次の手順を実行します。

ステップ 1 **[Controller]** > **[Interfaces]** を選択します。

ステップ 2 [Virtual] リンクをクリックします。

ステップ 3 表示される **[Interfaces]** > **[Edit]** ページで、次のパラメータを入力します。

a) [IP address] フィールドに、未割り当ておよび未使用のゲートウェイ IP アドレス（存在する場合）を入力します。

b) [DNS Host Name] フィールドに、DNS ホスト名（存在する場合）を入力します。

（注） 理想的には、このフィールドは空白になります。

（注） 接続して Web 認証を確立するには、DNS サーバは常に仮想インターフェイスをポイントしている必要があります。仮想インターフェイスに DNS ホスト名が設定されている場合は、クライアントが使用する DNS サーバ上で同じ DNS ホスト名が設定されている必要があります。

c) [Apply] をクリックします。

（注） 仮想インターフェイスに変更を加えた場合は、変更を反映するためにシスコ ワイヤレス コントローラを再起動します。

FlexConnect ローカル スイッチ モード

FlexConnect ローカルスイッチモードで Cisco DNA Spaces を使用するようにシスコ ワイヤレス コントローラ を設定するには、次の手順を実行します。

• アクセス ポイントの FlexConnect モードを設定する （253 ページ）

アクセス ポイントの *FlexConnect* モードを設定する

この設定は、FlexConnect の中央スイッチおよびローカルスイッチモードに適用されます。アクセスポイントに FlexConnect 中央スイッチモードを設定するには、次の手順を実行します。

ステップ 1 シスコ ワイヤレス コントローラのメインウィンドウで、[Wireless] タブをクリックします。

すべてのアクセス ポイントが一覧表示されます。

（注） アクセスポイントの詳細については、シスコ ワイヤレス コントローラのユーザーガイドを参照してください。

ステップ 2 モードを FlexConnect に設定するアクセス ポイントをクリックします。

ステップ 3 [General] タブをクリックします。

ステップ 4 [AP Mode] ドロップダウンリストから [FlexConnect] を選択します。

ステップ 5 [Apply] をクリックして変更を適用し、アクセス ポイントをリブートします。

シスコ ワイヤレス コントローラでの *FlexConnect* ローカルスイッチモード用 *SSID* の作成

（注） SSID は、Cisco CMX ではなく、シスコ ワイヤレス コントローラで作成されます。

FlexConnect のローカル スイッチ モードの CUWN で SSID を作成するには、次の手順を実行します。

ステップ 1 シスコ ワイヤレス コントローラのメインウィンドウで、[WLANs] タブをクリックします。

ステップ 2 WLAN を作成するには、ウィンドウの右側にあるドロップダウンリストで [Create New] を選択し、[Go] をクリックします。

ステップ 3 表示される [New] ウィンドウで、[Type]、[Profile Name]、[SSID] などの WLAN の詳細を入力します。

ステップ 4 [Apply] をクリックします。

[Edit <SSID Name>] ウィンドウが表示されます。

ステップ 5 SSID を Cisco DNA Spaces ダッシュボードに追加します。

ステップ 6 シスコ ワイヤレス コントローラ メインウィンドウの [General] タブで、[Broadcast SSID] チェックボックスをオフにします。

（注） SSID ブロードキャストが中断され、設定を完了する前に顧客が SSID にアクセスすることが回避されます。

ステップ 7 **[Security]** > **[Layer 2]** を選択して、[MAC Filtering] チェックボックスをオンにします。

ステップ 8 [Layer 3] タブで、次を設定します。

a) [Layer 3 security] ドロップダウン リストから、[Web Policy] を選択します。

（注） [Web Policy] は、シスコ ワイヤレス コントローラでキャプティブポータルを設定できるようにする [Layer 3] のセキュリティオプションです。

b) [On Mac Filter Failure] ラジオボタンを選択します。

c) [Preauthentication ACL] 領域で、[WebAuth FlexACL] ドロップダウンリストから、事前に定義されている ACL を選択します。

d) スリープ状態のクライアントの [Enable] チェックボックスをオンにします。

（注） スリープ状態のクライアントを有効にすることは必須ではありません。ただし有効にすると、認証後にスリープモードになっている顧客が指定された時間内にスリープ状態から復帰した場合、認証なしで接続されます。Web 認証に成功したゲストアクセスを持つクライアントは、ログインウィンドウから別の認証プロセスを実行せずにスリープおよび復帰することを許可されています。再認証が必要になるまでスリープ状態にあるクライアントが記録される期間を設定できます。有効な範囲は 1 時間から 720 時間（30 日）で、デフォルトは 12 時間です。これがセッション タイムアウトと同じになるのが理想的です。

e) [Over-ride Global Config] の [Enable] チェックボックスをオンにします。

（注） [Override Global Config] を有効にすると、顧客を外部 URL である Cisco DNA Spaces URL にリダイレクトできます。

f) [Web Auth Type] ドロップダウンリストから、[External] を選択します。

（注） Cisco DNA Spaces ページはコントローラではなく外部サーバーでホストされるため、[Web Auth Type] は [External] である必要があります。

g) 表示される [URL] フィールドに、Cisco DNA Spaces のスプラッシュ URL を入力します。

CUWN アカウントのスプラッシュ URL を表示するには、Cisco DNA Spaces ダッシュボードの [SSIDs] ウィンドウで CUWN SSID の [Configure Manually] リンクをクリックします。[Configure Manually] リンクは、Cisco AireOS SSID を追加した後にのみ表示されます。

（注） オンボーディング中に顧客が Cisco DNA Spaces Web ページにリダイレクトされるようにスプラッシュページを設定する必要があります。

h) [Apply] をクリックします。

ステップ 9 [Advanced] タブをクリックします。

ステップ 10 [Enable Session Timeout] フィールドに、必要なセッションタイムアウト値を秒単位で入力します。たとえば、セッションタイムアウトが 30 分の場合は、1800 と入力します。

ステップ 11 [FlexConnect] 領域で、FlexConnect ローカルスイッチングの [Enabled] チェックボックスをオンにして、[Apply] をクリックします。

ステップ 12 [General] タブで、[Status] および [Broadcast SSID] オプションの [Enabled] チェックボックスをオンにして、SSID を有効にします。

ステップ 13 コマンドプロンプトで次のコマンドを実行して、キャプティブバイパスを無効にします。次に、ワイヤレスコントローラを再起動します。

config network web-auth captive-bypass disable

（注） キャプティブバイパスが有効になっている場合、CNA は iOS デバイスに対してポップアップしません。

ステップ 14 **[Management]** > **[HTTP-HTTPS]** を選択します。

ステップ 15 表示される [HTTP-HTTPS Configuration] ウィンドウで、次を実行します。

a) [HTTP Access] ドロップダウンリストから、[Disabled] を選択します。
b) [HTTPS Access] ドロップダウンリストから、[Enabled] を選択します。
c) [WebAuth SecureWeb] ドロップダウンリストから、[Disabled] を選択します。
d) [Apply] をクリックします。

ステップ 16 **[Security]** > **[Web Auth]** > **[Web Login Page]** の順に選択し、[Redirect URL after login] フィールドが空白であることを確認します。

（注） リダイレクト URL フィールドは、[Layer 3] で設定された Cisco DNA Spaces のスプラッシュ URL を上書きしないように空白にする必要があります。

FlexConnect ローカルスイッチモードのアクセス制御リストの作成

顧客のインターネットアクセスを制限し、SSID に接続したときに Cisco DNA Spaces スプラッシュページ URL へのアクセスのみを許可するには、ACL で Cisco DNA Spaces の IP（ウォールガーデン範囲）を設定する必要があります。これで、顧客が SSID に接続すると、スプラッシュページが顧客に表示されます。

ACL で一部の必要な IP が設定されていない場合、Cisco DNA Spaces が外部 URL と見なされ、顧客に対して複数回のリダイレクトが発生します。

FlexConnect のローカル スイッチ モードでのアクセス コントロール リストを作成するには、次の手順を実行します。

ステップ 1 シスコ ワイヤレス コントローラのログイン情報を使用して、ワイヤレスコントローラにログインします。

ステップ 2 **[Security]** > **[Access Control Lists]** > **[FlexConnect ACLs]** の順に選択します。

ステップ 3 ACL を追加するには、[New] をクリックします。

ステップ 4 表示された [New] ウィンドウに、次のように入力します。

a) [Access Control List Name] フィールドに新しい ACL の名前を入力します。

（注） 最大 32 文字の英数字を入力できます。

b) [Apply] をクリックします。

ステップ 5 [Access Control Lists] ウィンドウが再度表示されたら、新しい ACL の名前をクリックします。

ステップ 6 表示される [Edit] ウィンドウで、[Add New Rule] をクリックします。

[Rules] > **[New]** ウィンドウが表示されます。

ステップ 7 必要なウォールガーデンの範囲にこの ACL のルールを設定します。

ウォールガーデンの範囲を表示するには、Cisco DNA Spaces ダッシュボードの [SSIDs] ウィンドウで CUWN SSID の [Configure Manually] リンクをクリックします。

ACL ルールを定義するときには、次のように値を設定します。

- **Direction**：Any
- **Protocol**：Any
- **Source Port Range**：0-65535
- **Destination Port Range**：0-65535
- **DSCP**：Any
- **Action**：Permit

ステップ 8 ポータルにソーシャル認証を装備する場合は、ソーシャル認証用にウォールガーデン範囲も構成する必要があります。ソーシャル認証用に設定する必要があるウォールガーデンの範囲については、「ソーシャル認証に向けたワイヤレスネットワークの設定」のセクションを参照してください。

（注） ソーシャル認証用に設定されたこのウォールガーデン範囲により、顧客は SSID に接続した後、キャプティブポータルを使用せずに、すべての HTTPS Web サイトに直接アクセスできます。

仮想インターフェイスの設定

仮想インターフェイスを設定するには、次の手順を実行します。

ステップ 1 **[Controller]** > **[Interfaces]** を選択します。

ステップ 2 [Virtual] リンクをクリックします。

ステップ 3 表示される **[Interfaces]** > **[Edit]** ページで、次のパラメータを入力します。

a) [IP address] フィールドに、未割り当ておよび未使用のゲートウェイ IP アドレス（存在する場合）を入力します。

b) [DNS Host Name] フィールドに、DNS ホスト名（存在する場合）を入力します。

（注） 理想的には、このフィールドは空白になります。

（注） 接続して Web 認証を確立するには、DNS サーバは常に仮想インターフェイスをポイントしている必要があります。仮想インターフェイスに DNS ホスト名が設定されている場合は、クライアントが使用する DNS サーバ上で同じ DNS ホスト名が設定されている必要があります。

c) [Apply] をクリックします。

（注） 仮想インターフェイスに変更を加えた場合は、変更を反映するためにシスコ ワイヤレス コントローラを再起動します。

インターネット プロビジョニングおよび RADIUS 認証のためのシスコ ワイヤレス コントローラの設定

キャプティブポータルには RADIUS 認証を使用することを強くお勧めします。

（注） Cisco DNA Spaces クラウド RADIUS サーバーは、Web RADIUS 認証用の PAP のみをサポートします。CHAPはサポートされていません。クライアント認証の失敗を回避するには、シスコ ワイヤレス コントローラで Web RADIUS 認証方式として PAP を設定する必要があります。

次の機能は、RADIUS 認証を設定した場合にのみ機能します。

- シームレスなインターネット プロビジョニング。
- 拡張されたセッション期間とインターネット帯域幅。
- インターネットの拒否

また、キャプティブポータルによる顧客オンボーディングには、インターネットプロビジョニング設定が必要です。

RADIUS認証とシームレスなインターネットプロビジョニングを設定するには、次の手順に従います。

ステップ 1 シスコ ワイヤレス コントローラのログイン情報を使用して、シスコ ワイヤレス コントローラにログインします。

ステップ 2 [Cisco Wireless Controller] のメインウィンドウで、 **Security** タブをクリックします。

ステップ 3 **[Radius]** > **[Authentication]** の順に選択します。

[Radius Authentication Servers] ウィンドウが表示されます。

ステップ 4 [Auth Called Station ID Type] ドロップダウンリストから、[AP MAC Address:SSID] を選択します。

ステップ 5 [MAC-Delimiter] ドロップダウンリストから、[Hyphen] を選択します。

ステップ 6 [New] をクリックします。

ステップ 7 表示された [New]] ウィンドウで、サーバーの IP アドレス、ポート番号、秘密鍵など、認証用の RADIUS サーバーの詳細を入力し、[Server Status] で [Enabled] を選択し、[Apply] をクリックします。

ポート番号：1812

（注） Cisco DNA Spaces RADIUS サーバーのみを設定できます。RADIUS サーバーの IP アドレスと秘密鍵を表示するには、Cisco DNA Spaces ダッシュボードで、[SSIDs] ウィンドウの CUWN SSID の [Configure Manually] リンクをクリックします。 [Configure Manually] リンクは、Cisco AireOS SSID を追加した後にのみ表示されます。プライマリとセカンダリの両方の Radius サーバー IP を設定します。Cisco DNA Spaces サポートチームに連絡することもできます。

ステップ 8 **[Radius]** > **[Accounting]** の順に選択します。

[Radius Accounting Servers] ウィンドウが表示されます。

ステップ 9 [Acct Called Station ID] タイプから、[AP MAC Address:SSID] を選択します。

ステップ 10 [MAC-Delimiter] ドロップダウンリストから、[Hyphen] を選択します。

ステップ 11 [New] をクリックします。

ステップ 12 表示された [New] ウィンドウで、サーバーの IP アドレス、ポート番号、秘密鍵など、アカウンティング用の RADIUS サーバーの詳細を入力し、[Server Status] で [Enabled] を選択し、[Apply] をクリックします。

Port Number: 1813

（注） Cisco DNA Spaces の Radius サーバーのみを設定できます。Cisco DNA Spaces の Radius サーバーのみを設定できます。RADIUS サーバーの IP アドレスと秘密鍵を表示するには、Cisco DNA Spaces ダッシュボードで、[SSIDs] ウィンドウの CUWN SSID の [Configure Manually] リンクをクリックします。

ステップ 13 シスコ ワイヤレス コントローラのメインウィンドウで、[WLANs] タブをクリックします。

ステップ 14 キャプティブポータルルールの SSID の [WLAN] をクリックします。

ステップ 15 [Security] を選択します。

ステップ 16 [Layer 2] タブで、[MAC Filtering] チェックボックスをオンにします。

ステップ 17 [Layer 3] タブで、次が設定されていることを確認します。

[Layer 3 security] ドロップダウンリストで、[Web Policy] が選択されていること、また [Mac Filter Failure] ラジオボタンが選択されていること。

（注） SSID を作成するときに、[Layer 3] でこれらの設定が実行されます。

ステップ 18 [AAA Servers] タブの、[Radius Servers] 領域で、次の手順を実行します。

a) [Authentication Servers] の [Enabled] チェックボックスをオンにします。

a) [Server 1] ドロップダウンリストで、先に定義した RADIUS サーバーを選択します。

ステップ 19 [web-auth user] 領域の認証の優先順位に、[Order Used for Authentication] ボックスで、[Radius] を順序の先頭に設定します。

（注） [Up] および [Down] ボタンを使用し、順序を並び替えます。

ステップ 20 [Advanced] タブをクリックし、[Allow AAA Override] の [Enabled] チェックボックスをオンにします。

ステップ 21 [Apply] をクリックします。

ステップ 22 [Cisco Wireless Controller] のメインウィンドウで、[Security] タブをクリックします。

ステップ 23 **[AAA]** > **[MAC Filtering]** の順に選択します。

ステップ 24 表示される [MAC Filtering] ウィンドウで、次の手順を実行します。

a) [RADIUS Compatibility Mode] ドロップダウンリストから、[Cisco ACS] を選択します。
b) [MAC-Delimiter] ドロップダウンリストから、[Hyphen] を選択します。
c) [Apply] をクリックします。

ステップ 25 ウォールガーデンが ACL に応じて設定されていることを確認します。ウォールガーデンの範囲を表示するには、Cisco DNA Spaces ダッシュボードで、[SSID] ウィンドウの CUWN SSID の [Configure Manually] リンクをクリックします。[Configure Manually] リンクは、Cisco AireOS SSID を追加した後にのみ表示されます。

ソーシャル認証のためのシスコ ワイヤレス コントローラの設定

Cisco Unified Wireless Network へのソーシャル認証のためには、シスコ ワイヤレス コントローラに設定を行う必要があります。

ソーシャル認証のために Cisco Unified Wireless Network を設定するには、次の手順を実行します。

ステップ 1 ログイン情報を使用して、シスコ ワイヤレス コントローラにログインします。

ステップ 2 **[Security]** > **[Access Control Lists]** > **[Access Control Lists]** を選択します。

ステップ 3 表示される [Access Control List] ウィンドウで、Cisco DNA Spaces のために設定されたアクセス制御リストをクリックします。

[Add New Rule] をクリックし、次の情報を持つ 2 つの追加ルールを追加します。.

いいえ	アクション	送信元 IP アドレス/ネットマスク	宛先 IP アドレス/ネットマスク	プロトコル	送信元ポート範囲	宛先ポート範囲	DSCP	方向
1	Permit	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	TCP	HTTPS	いずれか（Any）	いずれか（Any）	いずれか（Any）
2	Permit	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	TCP	いずれか（Any）	HTTPS	いずれか（Any）	いずれか（Any）

（注） ソーシャル認証用に設定構成されたこのウォールガーデン範囲により、顧客は SSID に接続した後、キャプティブポータルを使用せずに、すべての HTTPS Web サイトに直接アクセスできます。

ステップ 4 認証に使用するソーシャルネットワークに基づき、ソーシャルプラットフォーム固有のドメインを ACL として追加します。ソーシャルドメインを ACL として追加するには、次の手順を実行します。

a) シスコ ワイヤレス コントローラ ダッシュボードで、**[Security]** > **[Access Control Lists]** を選択します。
b) Cisco DNA Spaces 用に設定されたアクセス制御リストの [More Actions] をクリックします。
c) [Add Remove URL] をクリックします。
d) ソーシャル URL 名を入力し、[Add] をクリックします。
e) ドメインごとに、手順 **c** と **d** を繰り返します。

（注） これらのドメイン名はソーシャルネットワークによって管理され、いつでも変更できます。また、これらのドメイン名は、国/地域によって変更される可能性があります。問題が発生した場合は、Cisco DNA Spaces サポートチームにお問い合わせください。

さまざまなソーシャルプラットフォームで一般的に使用されるドメイン名は次のとおりです。

表 12：

ソーシャルドメイン
Facebook
facebook.com
static.xx.fbcdn.net
www.gstatic.com
m.facebook.com
fbcdn.net
fbsbx.com
LinkedIn
www.linkedin.com
static-exp1.licdn.com
Twitter
abs.twimg.com
syndication.twitter.com
twitter.com
analytics.twitter.com
Instagram
instagram.com

ソーシャルドメイン
*.instagram.com
api.instagram.com
d36xtkk24g8jdx.cloudfront.net
www.facebook.com
connect.facebook.net
*.akamaihd.net

WLC 直接接続または Cisco DNA Spaces コネクタを使用した、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラまたはシスコ ワイヤレス コントローラの Cisco DNA Spaces への接続

Cisco 9800 シリーズ ワイヤレス コントローラまたはシスコ ワイヤレス コントローラ（CMX なし）から Cisco DNA スペースにロケーションをインポートするには、最初にいずれかのコネクタを介してコントローラを Cisco DNA Spaces に接続する必要があります。

[Cisco WLC Direct Connect] と [Cisco DNA Spaces Connector] の両コネクタは、シスコ ワイヤレス コントローラと Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの両方に使用できます。

（注）

- シスコ ワイヤレス コントローラを Cisco CMX と Cisco DNA Spaces の両方に同時に接続する場合は、Cisco DNA Spaces コネクタを使用する必要があります。ただし、1 つのコントローラを Cisco DNA Spaces と Cisco CMX の両方に同時に接続することは推奨しません。
- 行動メトリクスなどの Cisco DNA Spaces レポートに表示されるデータを、シスコ ワイヤレス コントローラまたは Cisco CMX に表示されるデータと比較しないようにお勧めします。設計によって表示されるデータが異なることが予想されるためです。
- コントローラを Cisco DNA Spaces にインポートするには、少なくとも 1 つの AP がその特定のコントローラに接続されていることを確認してください。
- コントローラで、新しい AP がコントローラに追加されると、追加された AP は次のコントローラ同期の際に自動的にインポートされます。インポートされた AP がコントローラから削除された場合、この変更は 48 時間経過しないと Cisco DNA Spaces に反映されません。ただし、更新されない AP は、更新が他の AP から送信されている場合にのみ 48 時間後に削除されます。たとえば、10 の AP が設定されていて、2 つの AP がコントローラから削除された場合、削除された 2 つの AP は、他の 8 つの AP から更新が受信された場合にのみ Cisco DNA Spaces から削除されます。
- AP がコントローラとの関連付けを解除された場合、Cisco DNA Spaces からすぐに削除されて AP 数に反映されることありません。その AP は、48 時間経過しないと Cisco DNA Spaces から削除されません。

ワイヤレスコントローラとコネクタのさまざまな組み合わせに必要な設定は次のとおりです。

Cisco WLC Direct Connect を使用した Cisco DNA Spaces のシスコ ワイヤレス コントローラへの接続

シスコ ワイヤレス コントローラ バージョン 8.3 以降（Cisco CMX のインストールなし）を Cisco DNA Spaces に接続し、シスコ ワイヤレス コントローラとそのアクセスポイントを Cisco DNA Spaces にインポートするには、次の手順を実行します。

始める前に

- シスコ ワイヤレス コントローラ バージョン 8.3 以降が必要です。
- シスコ ワイヤレス コントローラを Cisco DNA Spaces にインポートするには、少なくとも 1 つの AP がその特定のシスコ ワイヤレス コントローラに接続されていることを確認してください。
- シスコ ワイヤレス コントローラは、HTTPS 経由で Cisco DNA Spaces クラウドに到達できる必要があります。
- シスコ ワイヤレス コントローラはインターネットに接続できる必要があります。

- Cisco DNA Spaces をアンカーモードで使用するには、アンカーコントローラモードと外部コントローラモードの両方でシスコ ワイヤレス コントローラをネットワーク展開する必要があります。ネットワーク展開にアンカーコントローラモードと外部コントローラモードのシスコ ワイヤレス コントローラが含まれている場合、このセクションで説明するコマンドを使用して、両方のコントローラで Cisco WLC Direct Connect を有効にする必要があります。さらに、どちらのモードのシスコ ワイヤレス コントローラも、HTTPS 経由で Cisco DNA Spaces クラウドに到達できる必要があります。ただし、Cisco DNA Spaces は、アンカーモードのシスコ ワイヤレス コントローラ バージョン 8.3.102 をサポートしていません。
- Cisco WLC Direct Connect を使用して Cisco AirOS ワイヤレス コントローラ バージョン 8.3 以降を Cisco DNA Spaces に正常に接続するには、DigiCert CA が発行するルート証明書が必要です。ネットワーク展開にアンカーコントローラモードと外部コントローラモードのシスコ ワイヤレス コントローラが含まれている場合、両方のモードのシスコ ワイヤレス コントローラに証明書をインポートする必要があります。

ステップ 1 DigiCert CA ルート証明書をインポートします。

a) 次のリンクからルート証明書をダウンロードします。
'

https://global-root-ca.chain-demos.digicert.com/info/index.html

b) ルート証明書の内容を .cer 拡張子のファイルにコピーし、ファイルを {your_filename}.cer として保存します。

c) **{your_filename}.cer** ファイルを TFTP サーバー上のデフォルトディレクトリにコピーします。

d) シスコ ワイヤレス コントローラの CLI にログインし、次のコマンドを実行します。

```
transfer download datatype cmx-serv-ca-cert
transfer download mode tftp
transfer download filename {your_filename}.cer
transfer download serverip {your_tftp_server_ip}
transfer download start
```

e) **Y** を入力してアップロードを開始します。

f) 新しいルート証明書が正常にアップロードされたら、次のコマンドを実行して Cisco CMX クラウドサービスを無効にし、その後で有効にします。

```
config cloud-services cmx disable
config cloud-services cmx enable
```

（注） ルート証明書をアップロードした後、シスコ ワイヤレス コントローラの再起動が求められます。再起動をお勧めしますが、必須ではありません。いずれの場合も証明書がインストールされます。

DigiCert CA が発行したものではないルート証明書を使用してワイヤレスコントローラを Cisco DNA Spaces に接続しようとすると、次のエラーが発生します。

```
https:SSL certificate problem: unable to get local issuer certificate
```

ステップ 2 シスコ ワイヤレス コントローラの CLI モードで、次のコマンドを実行します。

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

（注） {Customer Path Key}、{LB Domain}、{LB IP Address}、および {Customer JWT Token} を表示するには、Cisco DNA Spaces ダッシュボードにログインし、ダッシュボードの左上に表示される 3 本線のメニューアイコンをクリックします。[Setup] > [Wireless Networks] の順に選択します。次に、[Connect WLC / Catalyst 9800 Directly] を展開し、[View Token] をクリックします。[WLC] タブをクリックすると、ステップ 1b で {Customer Path Key}、{LB Domain}、および {LB IP Address} を、ステップ 1c で {Customer JWT Token} を表示できます。

ステップ 3 次のコマンドを使用して、概要を確認します。

```
show cloud-services cmx summary
```

結果が表示されます。

Cisco DNA Spaces ダッシュボードで、[Add a Wireless Network] ウィンドウの [CUWN-WLC] を選択すると、WLC が一覧表示されます。これにより、その WLC の AP を Cisco DNA Spaces にインポートできます。

例：

結果サンプル

(Cisco Controller) >show cloud-services cmx summary

CMX Service

Server ..... https://$customerpathkey.dnaspaces.io

IP Address..... <Local System IP Address>

Connectivity..... https: UP

Service Status ..... アクティブ

Last Request Status..... HTTP/1.1 200 OK

Heartbeat Status ..... OK

これで、シスコ ワイヤレス コントローラを Cisco DNA Spaces ロケーション階層にインポートできるようになりました。マップサービスまたはアクセス ポイント プレフィックスを使用してロケーションをインポートできます。

- アクセスポイントのプレフィックスに基づいてロケーションをインポートするには、アクセス ポイント プレフィックスを使用したロケーションのインポート （37 ページ）を参照してください。
- マップサービスを使用してロケーションをインポートするには、マップサービスを使用したロケーションのロケーション階層へのインポート （39 ページ）を参照してください。

次のタスク

ソーシャル認証、RADIUS認証、およびインターネットプロビジョニングについては、次のセクションを参照してください。

- インターネット プロビジョニングおよびRADIUS 認証のためのシスコ ワイヤレス コントローラの設定
- インターネット プロビジョニングおよびRADIUS 認証のためのシスコ ワイヤレス コントローラの設定

通知およびレポート用のシスコ ワイヤレス コントローラ（Cisco CMX なし）の設定

Cisco CMX を使用しない場合、WLC Direct Connectおよび Cisco DNA Spaces コネクタといったコネクタを使用して、シスコ ワイヤレス コントローラを Cisco DNA Spaces に接続できます。このような場合、通知とレポートに必要な設定は、シスコ ワイヤレス コントローラをインポートするときに自動的に行われます。

（注） Cisco DNA Spaces で WLC Direct Connect または Cisco DNA Spaces コネクタを使用している場合、コントローラは「フォーリンコントローラ」モードである必要があります。

Cisco WLC Direct Connect を使用した Cisco DNA Spaces の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラへの接続

始める前に

- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを Cisco DNA Spaces にインポートする場合、少なくとも 1 つの AP がその特定の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラに接続されていることを確認してください。
- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラは、HTTPS 経由で Cisco DNA Spaces クラウドに到達できる必要があります。
- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラは、インターネットに接続できる必要があります。
- Cisco WLC Direct Connect を使用して Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを Cisco DNA Spaces に正常に接続するには、シスコが信頼するルート証明書が必要です。

Cisco Catalyst 9800 シリーズ コントローラを Cisco DNA Spaces に接続し、そのコントローラとそのアクセスポイントを Cisco DNA Spaces にインポートするには、次の手順を実行します。

ステップ 1 シスコ社外の信頼できるルートストアをインポートして、コントローラに DigiCert グローバルルート CA をインストールします。

a) 次のコマンドを使用してルート証明書をダウンロードします。

```
(config)#crypto pki trustpool import url http://www.cisco.com/security/pki/trs/ios.p7b
```

b) 次のコマンドを使用して証明書のインストールを検証します。

```
#show crypto pki trustpool | section DigiCert Global Root CA
cn=DigiCert Global Root CA
cn=DigiCert Global Root CA
```

（注） 出力をチェックして、トラストプールが正しくインストールされていることを確認する必要があります。

ステップ 2 Cisco Catalyst 9800 シリーズ コントローラで、次のコマンドを使用して、DNS が Cisco DNA Spaces URL を解決できるようにします。

```
a. (config)#ip name-server <Primary IP> <Secondary IP>
b. (config)#ip domain lookup
c. (config)#ip route 0.0.0.0 0.0.0.0 <default_gw_ip_addr>
```

ステップ 3 HTTPS 経由で Cisco DNA Spaces Cloud と通信するため、Cisco Catalyst 9800 シリーズ コントローラで nmsp cloud-services を有効にします。

```
a. (config)#nmsp cloud-services server url <URL>
b. (config)#nmsp cloud-services server token <Customer JWT TOKEN>
c. (config)#nmsp cloud-services http-proxy <proxy ip_addr> <proxy port> -This command is optional,
 and must be used only if the proxy server needs to reach the internet.
d. (config)#nmsp cloud-services enable
```

（注） サーバーの URL とトークンを表示するには、Cisco DNA Spaces ダッシュボードにログインし、ダッシュボードの左上に表示される 3 本線のメニューアイコンをクリックします。[Setup]>[Wireless Networks] の順に選択します。次に、[Connect WLC / Catalyst 9800 Directly] を展開し、[View Token] をクリックします。[Cisco Catalyst 9800] タブをクリックすると、ステップ 2b で URL が表示され、ステップ 2c でトークンが表示されます。

ステップ 4 次のコマンドを実行して、Cisco Catalyst 9800 シリーズ コントローラと Cisco DNA Spaces Cloud 間の接続を確認します。

```
#show nmsp cloud-services summary
```

結果は次のようになります。

例：

結果サンプル

サーバー：https://abc.dnaspaces.io

CMX サービス：Enabled

接続：https: UP

サービスステータス：Active

最後の IP アドレス：<ローカルシステム IP アドレス>

最後のリクエストステータス：HTTP/1.1 200 OK

ハートビートステータス：OK

これで、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを Cisco DNA Spaces のロケーション階層にインポートできるようになります。

ステップ 5 アクティブ/非アクティブな Cisco CMX クラウド接続の概要を表示するには、次のコマンドを実行します。

```
#show nmsp status
```

（注） Cisco DNA Spaces Cloud 接続への接続状態を確認できます。

ステップ 6 すべてのアクティブな Cisco DNA Spaces クラウド接続の集約されたサブスクリプションの概要を表示するには、次のコマンドを実行します。

```
# show nmsp subscription summary
```

（注） 接続が確立されると、Cisco DNA Spaces Cloud が登録しているサービスを表示できます。

ステップ 7 ロケーションを Cisco DNA Spaces ダッシュボードにインポートします。ロケーションのインポートの詳細については、「Cisco Catalyst 9800 シリーズ ワイヤレス コントローラまたはシスコ ワイヤレス コントローラ（Cisco CMX なし）のロケーション階層の定義 （36 ページ）」を参照してください。

ステップ 8 **キャプティブポータル**および **Engagements** アプリを使用する場合は、以下のうち必要な設定を実行します。

CLI を使用したキャプティブポータルおよびエンゲージメントアプリ用の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ（ローカルモード）の設定

（注） サポートされる Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの最小バージョンは、16.10.20181030 です。

キャプティブポータルおよびエンゲージメントアプリ用に Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを設定するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、Cisco Catalyst SSID を設定します。SSID の設定の詳細については、「シスコ ワイヤレス コントローラまたは Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの SSID のインポート」セクションを参照してください。

（注） SSID には任意の名前を定義できます。Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを設定したときと同じ SSID 名を使用する必要があります。

ステップ 2 Cisco Catalyst 9800 シリーズ ワイヤレス コントローラで、次のように HTTP と HTTPS を有効にします。

ip http server

ip http secure-server

ステップ 3 クライアントのリダイレクト用のパラメータマップを設定します。

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

（注） スプラッシュ URL と IP アドレスについては、Cisco DNA Spaces ダッシュボードで、Captive Portal アプリをクリックします。[SSIDs] をクリックし、ステップ 1 で作成した Cisco Catalyst SSID の [Configure Manually] リンクをクリックします。CUWN アカウントのスプラッシュ URL は、[Creating the SSIDs in CUWN-WLC] セクションにリストされます。IP アドレスは、[Creating the Access Control List] セクションに一覧表示されます。リストにある IP アドレスのいずれか 1 つのみを使用する必要があります。Cisco DNA Spaces サポートチームに連絡することもできます。

ステップ 4 クライアントリダイレクト用の仮想 IP アドレスを設定します。

parameter-map type webauth global

virtual-ip ipv4 192.0.2.0

intercept-https-enable

（注）
- **ipV4** *192.0.2.0* の代わりに、任意の仮想 IP を構成できます。virtual-ip は、ルーティング不可能な未使用の IP アドレスである必要があります。
- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラに仮想 IP/ドメインの有効な SSL 証明書をインストールする必要があります。

ステップ 5 FQDN URL フィルタリングを設定します。

中央スイッチの WLAN の場合、URL フィルタリストはポリシープロファイルに添付されます。

urlfilter list social_login_fqdn_central

action permit

url <splash page domain>

（注） 手順 3 で設定したドメインを「redirect for-login」用に設定します。

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

フレックス WLAN の場合、URL フィルタリストはフレックスプロファイルに添付されます。

urlfilter list social_login_fqdn_flex
action permit
url <splash page domain>

（注） 手順 3 で設定したドメインを「redirect for-login」用に設定します。

url *.fbcdn.net
url *.licdn.com
url *.licdn.net
url *.twimg.com
url *.gstatic.com
url *.twitter.com
url *.akamaihd.net
url *.facebook.com
url *.facebook.net
url *.linkedin.com
url ssl.gstatic.com
url *.googleapis.com

```
url static.licdn.com
url *.accounts.google.com
url *.connect.facebook.net
url oauth.googleusercontent.com
urlfilter list social_login_fqdn_central
wireless profile flex default-flex-profile
acl-policy <WA-sec-<ip>>
urlfilter list social_login_fqdn_flex
description "default flex profile"
```

ステップ 6 RADIUS サーバーを設定します。

```
aaa new-model
aaa group server radius <group name>
server name <radius server name>
subscriber mac-filtering security-mode mac
mac-delimiter hyphen
aaa accounting login <authentication> group <group name>
aaa authorization network <Authorization> group <Group Name>
aaa accounting identity <Accounting> start-stop group <Group Name>
aaa server radius dynamic-author
client <Radius Server IP> server-key <Radius Secret>
aaa session-id common
radius-server attribute wireless accounting call-station-id ap-macaddress-ssid
radius server <Radius Name>
address ipv4 <Radius Server IP> auth-port 1812 acct-port 1813
key <Radius Secret>
```

（注） Cisco DNA Spaces の Radius サーバーのみを設定できます。Radius サーバー設定用の ipV4 IP アドレス、秘密鍵およびポートを表示するには、Cisco DNA Spaces ダッシュボードで、[Captive Portal] アプリをクリックします。[SSIDs] をクリックし、ステップ 1 で作成した Cisco Catalyst SSID の [Configure Manually] リンクをクリックします。Radius サーバーの詳細は、[Radius Server Configuration] セクションのリストに表示されます。プライマリとセカンダリの両方の Radius サーバー IP を設定します。Cisco DNA Spaces サポートチームに連絡することもできます。

ステップ 7 ポリシープロファイルを設定します。

```
wireless profile policy default-policy-profile
aaa-override
accounting-list <Accounting Server>
```

autoqos mode voice

description "default policy profile"

service-policy input platinum-up

service-policy output platinum

urlfilter list pre-auth-filter <url filter>

vlan <id>

no shutdown

ステップ 8 WLAN を設定します。

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

（注） ここで指定する WLAN 名が、ステップ 1 で Cisco DNA Spaces で設定した SSID 名と一致することを確認してください。

ステップ 9 DNS 解決を有効にして、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラにデフォルトゲートウェイが設定されていることを確認します。

ip name-server <dns_ip_address>

ip domain-lookup

ip route 0.0.0.0 0.0.0.0 <default_gw_ip_addr>

その後、SSID を Cisco DNA Spaces にインポートし、キャプティブポータルルールを使用して SSID のキャプティブポータルを設定します。

キャプティブポータルおよびエンゲージメントアプリ用の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ GUI（ローカルモード）

（注） サポートされる Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの最小バージョンは、16.10.1E および 16.10.11 です。

キャプティブポータルおよびエンゲージメントアプリ用に Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを設定するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、Cisco Catalyst SSID を設定します。SSID の設定の詳細については、「シスコ ワイヤレス コントローラまたは Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの SSID のインポート」セクションを参照してください。

ステップ 2 パラメータマップを作成します。

a) Cisco Catalyst 9800 シリーズ ワイヤレス コントローラにログインします。

b) **[Configuration]** > **[Security]** > **[Web Auth]** の順に選択します。

c) [Web Auth Parameter Map] タブで、[Add] をクリックします。

d) [Parameter-map name] フィールドに、パラメータマップ名を入力します。

e) [Type] ドロップダウンリストから [Consent] を選択し、[Apply to Device] をクリックします。
新しく作成されたパラメータマップが [Web Auth Parameter Map] タブのリストに表示されます。

f) 新しく作成された [Parameter Map] をクリックします。

g) [General] タブで、[Disable Success Window] チェックボックスと [Disable Logout Window] チェックボックスをオンにします。

h) [Advanced] タブで、次の操作を実行します。

- [Redirect for log-in] フィールドに、スプラッシュページの URL（https://<domain>/p2/<customerPathKey>）を入力します。
- [Redirect Append for AP MAC Address] フィールドに、「ap_mac」を入力します。
- [Redirect Append for Client MAC Address] フィールドに、「client_mac」を入力します。
- [Redirect Append for WLAN SSID] フィールドに、wlan を入力します。
- [Portal IPV4 Address] フィールドに、許可される Cisco DNA Spaces IP を入力します。

（注） 許可される IP アドレスを表示するには、Cisco DNA Spaces ダッシュボードで、[Captive Portals] アプリをクリックします。[SSIDs] をクリックしてから、Cisco Catalyst SSID の [Configure Manually] リンクをクリックします。IP アドレスは、[Creating the Access Control List] セクションに一覧表示されます。リストにある IP アドレスのいずれか 1 つのみを使用する必要があります。残りの IP は、ACL の作成時に指定されます。[Configure Manually] リンクは、Cisco Catalyst SSID を追加するまで表示されません。

i) [Update and Apply] をクリックします。

ステップ 3 Web 認証証明書をインストールし、グローバルパラメータマップを設定します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラに仮想 IP/ドメインの有効な SSL 証明書をインストールする必要があります。任意のワイルドカード証明書を購入できます。

a) Cisco Catalyst 9800 シリーズ ワイヤレス コントローラにログインします。

b) Cisco Catalyst 9800 Series Wireless Controller ダッシュボードで、**[Configuration]** > **[Security]** > **[Web Auth]** を選択します。

c) パラメータマップ名 [global] をクリックします。

d) [Maximum Http connections] を [100] に設定します。
e) [Init-State Timeout(Secs)] を [120] に設定します。
f) [General] タブの [Type] ドロップダウンリストから、[Webauth] を選択します。
g) それぞれのフィールドで仮想 IPv4 アドレス（仮想 IP）または仮想 IPv4 ホスト名（ドメイン）を指定します。
h) [Watch List Expiry Timeout(Secs)] を [600] に設定します。
i) [Web Auth intercept HTTPS] チェックボックスをオンにします。
j) [Update & Apply] をクリックします。
k) 証明書を pkcs12 に変換します。

ファイル形式は .p12 になります。

l) ファイルを TFTP サーバーにコピーします。
m) 次の手順を使用して、TFTP サーバーにコピーされた証明書をダウンロードします。

- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの CLI で、次のコマンドを入力します。

```
crypto pki import <name> pkcs12 tftp://<tftp server ip>:/ password <certificate password>
```

- **tftp** サーバーの IP を確認するには、「**yes**」と入力します。
- 証明書ファイル名を入力します。たとえば「wildcard.wifi-mx.com.p12」のように入力します。

  証明書がダウンロードされます。

n) インストールされている証明書を確認するには、Cisco Catalyst 9800 Series Wireless Controller ダッシュボードで、**[Configuration]** > **[Web Auth]** > **[Certificate]** を選択します。

ダウンロードされた証明書は、リスト末尾の証明書として表示されます。

o) インストールされた証明書をウェブ認証パラメータマップにマッピングするには、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの CLI で、次のコマンドを実行します。

- `Conf t`
- `parameter-map type webauth global`
- `trustpoint <installed trustpool name > ex: trustpool name`
- `end`
- `wr (to save the configuration)`

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラをリロードします。

ステップ 4 URL フィルタを追加して ACL を作成します。

a) **[Configuration]** > **[Security]** > **[URL Filter]** を選択します。
b) [URL Filters] ウィンドウで、[Add] をクリックします。
c) [List Name] フィールドに、リストの名前を入力します。
d) [Action] のステータスを [Permit] に変更します。
e) [URLs] フィールドに、ステップ 2h（パラメータマップ）で設定したスプラッシュページドメインを入力します。

ソーシャル認証を有効にする場合は、次のドメインを追加します。

- *.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) **[Configuration]** > **[Tags and Profiles]** > **[Policy]** を選択します。
g) [Policy Profile] ウィンドウで、[default-policy-profile] をクリックします。
h) [Edit Policy Profile] ウィンドウで、[Access Policies] タブをクリックします。
i) [URL Filters] エリアの [Pre Auth] ドロップダウンリストから、以前に作成した ACL を選択します。
j) [Update & Apply to Device] をクリックします。

ステップ 5 SSID を作成します。

a) **[Configuration]** > **[Tags and Profiles]** > **[WLANs]** を選択します。
b) [Add] をクリックします。
a) [General] タブで、[Profile Name] フィールドにプロファイル名を入力します。
b) [SSID] フィールドに、ステップ 1 で定義した SSID 名を入力します。
c) ステータスを [Enabled] に設定します。
d) [Security] タブをクリックしてから、[Layer2] タブをクリックします。
e) [Layer 2 Security Mode] ドロップダウンリストから、[None] を選択します。
f) [Layer3] タブをクリックします。
g) [Web Policy] チェックボックスをオンにします。
h) [Web Auth Parameter Map] ドロップダウンリストから、ステップ 2 で作成した Web 認証パラメータマップを選択します。
i) [Save & Apply to Device] をクリックします。

ステップ 6 RADIUS サーバを設定します。

（注） キャプティブポータルにはRADIUS認証を使用することを強く推奨します。次の機能は、RADIUS認証を設定した場合にのみ使用できます。

- シームレスなインターネット プロビジョニング
- セッション持続時間の延長
- インターネットの拒否

a) **[Configuration]** > **[Security]** > **[AAA]** の順に選択します。
b) [Authentication Authorization and Accounting] ウィンドウで、[Servers/Groups] タブをクリックします。
c) **[Radius]** > **[Servers]** を選択して、[Add] をクリックします。
d) [Name] フィールドに、Radius サーバーの名前を入力します。
e) [IPv4/IPv6 Server Address] フィールドに、Radius サーバーのアドレスを入力します。

（注） Cisco DNA Spaces の Radius サーバーのみを設定できます。Radius サーバーの IP アドレスと秘密鍵を表示するには、Cisco DNA Spaces ダッシュボードで、[Captive Portal] アプリをクリックします。[SSIDs] をクリックしてから、ステップ 1 で作成した Cisco Catalyst SSID の [Configure Manually] リンクをクリックします。表示されるウィンドウで、Radius サーバーの詳細が [Radius Server Configuration] セクションのリストに表示されます。プライマリおよびセカンダリ Radius サーバの両方の IP を設定します。Cisco DNA Spaces サポート チームに連絡することもできます。

f) [Key] フィールドにキーを入力し、[Confirm Key] フィールドでキーを確認します。
g) [Auth Port] フィールドに「1812」と入力します。
h) [Acct Port] フィールドに「1813」と入力します。
i) [Save & Apply to Device] をクリックします。
追加されたサーバーは、[Servers] リストに表示されます。
j) **[Radius]** > **[Server Groups]** を選択して、[Add] をクリックします。
k) [Name] フィールドに、名前を入力します。
l) [MAC-Delimiter] ドロップダウンリストから、[hyphen] を選択します。
m) [MAC-Filtering] ドロップダウンリストから、[mac] を選択します。
n) 矢印ボタンを使用して、以前に作成した Radius サーバーを [Available Servers] から [Assigned Servers] に移動します。
o) [Save & Apply to Device] をクリックします。
p) [Authentication Authorization and Accounting] ウィンドウで、[AAA Method List] タブをクリックします。
q) [Authentication] をクリックし、[Add] をクリックして、次の詳細を指定します。

1. [Method List Name] フィールドに、メソッドリストの名前を入力します。
2. [Type] ドロップダウンリストから、[Login] を選択します。
3. [Group Type] ドロップダウンリストから、[Group] を選択します。

4. 以前に作成したサーバーグループ（ステップ j からステップ o）を [Available Server Groups] から [Assigned Servers Groups] に移動し、[Save & Apply to Device] をクリックします。

r) [AAA Method List] タブで、[Authorization] をクリックし、[Add] をクリックして、次の詳細を指定します。

1. [Method List Name] フィールドに、メソッドリストの名前を入力します。
2. [Type] ドロップダウンリストから、[Network] を選択します。
3. [Group Type] ドロップダウンリストから、[Group] を選択します。
4. 矢印ボタンを使用して、以前に作成したサーバーグループ（ステップ j からステップ o）を [Available Servers] から [Assigned Servers] に移動し、[Save & Apply to Device] をクリックします。

s) [AAA Method List] タブで、[Accounting] をクリックし、[Add] をクリックして、次の詳細を指定します。

1. [Method List Name] フィールドに、メソッドリストの名前を入力します。
2. [Type] ドロップダウンリストから、[Identity] を選択します。
3. [Group Type] ドロップダウンリストから、[Group] を選択します。
4. 矢印ボタンを使用して、以前に作成したサーバーグループ（ステップ j からステップ o）を [Available Servers] から [Assigned Servers] に移動し、[Save & Apply to Device] をクリックします。

ステップ 7 L3 および L2 認証（MAC フィルタリング）を有効にします。

Radius 認証のパラメータマップで、[Type] として [webauth] が選択されていることを確認します。

（注） L3 および L2 認証を設定するには、SSID を作成し、ステップ 5 のすべての設定を完了していることを確認してください。その後、SSID を Cisco DNA Spaces にインポートし、キャプティブポータルルールを使用して SSID のキャプティブポータルを設定します。

a) **[Configuration]** > **[Tags and Profiles]** > **[WLANs]** を選択します。
b) L2 および L3 認証を設定する SSID をクリックします。
c) [Edit WLAN] ウィンドウで [Security] タブをクリックします。
d) [Layer3] タブで、[Authentication] ドロップダウンリストから、以前に（ステップ 6q で）設定した Radius 認証を選択します。
e) [Layer2] タブで、[MAC Filtering] チェックボックスをオンにして、MAC フィルタリングを有効にします。
f) 表示される [Authorization List] ドロップダウンリストから、以前に（ステップ 6r で）作成した許可サーバーを選択します。
g) [Show Advanced Settings] をクリックします。
h) [On Mac Filter Failure] チェックボックスをオンにします。
i) [Update & Apply to Device] をクリックします。
j) **[Configuration]** > **[Tags and Profiles]** > **[Policy]** を選択します。
k) [default-policy-profile] をクリックします。

l) [Advanced] タブの [AAA Policy] エリアで、[Allow AAA Override] チェックボックスをオンにします。
m) [Policy Name] ドロップダウンリストから、デフォルトの [aaa] ポリシーが選択されていることを確認します。
n) [Update & Apply to Device] をクリックします。

キャプティブポータルおよびエンゲージメントアプリ用の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ GUI（フレックスモードまたは Mobility Express）

（注） サポートされる Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの最小バージョンは、16.10.1E および 16.10.11 です。

キャプティブポータルおよびエンゲージメントアプリ用に「フレックスモードの Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ」または「Mobility Express を備えた Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ」を設定するには、次の手順を実行します。

ステップ 1 フレックスモードの Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを設定するには、次の設定が完了していることを確認します。

この設定は、Mobility Express には必要ありません。

a) Cisco Catalyst 9800 シリーズ ワイヤレス コントローラにログインします。
b) **[Configuration]** > **[Tags]** > **[Site]** を選択します。
c) 必要なサイト名を選択します。
d) [Enabled Local Site] チェックボックスをオフにします。
e) [Update & Apply to Device] をクリックします。
f) **[Configuration]** > **[Policy]** を選択します。
g) 必要なポリシー名を選択します。
h) [Central Switching] を無効にします。
i) [Update & Apply to Device] をクリックします。

（注） [Local Mode] から [Flex Mode] に変更すると、AP が再起動してワイヤレスコントローラに再参加する場合があります。

ステップ 2 Cisco DNA Spaces ダッシュボードで、Cisco Catalyst SSID を設定します。SSID の設定の詳細については、「シスコ ワイヤレス コントローラまたは Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの SSID のインポート」セクションを参照してください。

ステップ 3 パラメータマップを作成します。

a) Cisco Catalyst 9800 シリーズ ワイヤレス コントローラにログインします。
b) **[Configuration]** > **[Security]** > **[Web Auth]** の順に選択します。
c) [Web Auth Parameter Map] タブで、[Add] をクリックします。
d) [Parameter-map name] フィールドに、パラメータマップ名を入力します。

e) [Type] ドロップダウンリストから [Consent] を選択し、[Apply to Device] をクリックします。
新しく作成されたパラメータマップが [Web Auth Parameter Map] タブのリストに表示されます。

f) 新しく作成された [Parameter Map] をクリックします。

g) [General] タブで、[Disable Success Window] チェックボックスと [Disable Logout Window] チェックボックスをオンにします。

h) [Advanced] タブで、次の操作を実行します。

- [Redirect for log-in] フィールドに、スプラッシュページの URL（https://<domain>/p2/<customerPathKey>）を入力します。
- [Redirect Append for AP MAC Address] フィールドに、ap_mac を入力します。
- [Redirect Append for Client MAC Address] フィールドに、client_mac を入力します。
- [Redirect Append for WLAN SSID] フィールドに、wlan を入力します。
- [Portal IPV4 Address] フィールドに、許可される Cisco DNA Spaces IP を入力します。

（注） 許可される IP アドレスを表示するには、Cisco DNA Spaces ダッシュボードで、[Captive Portals] アプリをクリックします。[SSIDs] をクリックしてから、CUWN/Catalyst SSID の [Configure Manually] リンクをクリックします。IP アドレスは、[Creating the Access Control List] セクションに一覧表示されます。リストにある IP アドレスのいずれか 1 つのみを使用する必要があります。残りの IP は、ACL の作成時に指定されます。[Configure Manually] リンクは、Cisco Catalyst SSID を追加するまで表示されません。

i) [Update and Apply] をクリックします。

ステップ 4 Web 認証証明書をインストールし、グローバルパラメータマップを設定します。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラに仮想 IP/ドメインの有効な SSL 証明書をインストールする必要があります。任意のワイルドカード証明書を購入できます。

a) Cisco Catalyst 9800 シリーズ ワイヤレス コントローラにログインします。

b) Cisco Catalyst 9800 Series Wireless Controller ダッシュボードで、**[Configuration]** > **[Security]** > **[Web Auth]** を選択します。

c) パラメータマップ名 [global] をクリックします。

d) [Maximum Http connections] を [100] に設定します。

e) [Init-State Timeout(Secs)] を [120] に設定します。

f) [General] タブの [Type] ドロップダウンリストから、[Webauth] を選択します。

g) それぞれのフィールドで仮想 IPv4 アドレス（仮想 IP）または仮想 IPv4 ホスト名（ドメイン）を指定します。

h) [Watch List Expiry Timeout(Secs)] を [600] に設定します。

i) [Web Auth intercept HTTPS] チェックボックスをオンにします。

j) [Update & Apply] をクリックします。

k) 証明書を pkcs12 に変換します。
ファイル形式は .p12 になります。

l) ファイルを TFTP サーバーにコピーします。

m) 次の手順を使用して、TFTP サーバーから証明書をダウンロードします。

- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの CLI で、次のコマンドを入力します。

```
crypto pki import <name> pkcs12 tftp://<tftp server ip>:/ password <certificate password>
```

- **tftp** サーバーの IP を確認するには、「**yes**」と入力します。
- 証明書ファイル名を入力します。たとえば「wildcard.wifi-mx.com.p12」のように入力します。

  証明書がダウンロードされます。

n) インストールされている証明書を確認するには、Cisco Catalyst 9800 Series Wireless Controller ダッシュボードで、**[Configuration]** > **[Web Auth]** > **[Certificate]** を選択します。
ダウンロードされた証明書は、リスト末尾の証明書として表示されます。

o) インストールされた証明書をウェブ認証パラメータマップにマッピングするには、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの CLI で、次のコマンドを実行します。

- `Conf t`
- `parameter-map type webauth global`
- `trustpoint <installed trustpool name > ex: trustpool name`
- `end`
- `wr (to save the configuration)`

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラをリロードします。

ステップ 5 URL フィルタを追加して ACL を作成します。

a) **[Configuration]** > **[Security]** > **[URL Filter]** を選択します。
b) [URL Filters] ウィンドウで、[Add] をクリックします。
c) [List Name] フィールドに、リストの名前を入力します。
d) [Action] のステータスを [Permit] に変更します。
e) [URLs] フィールドに、ステップ 3h（パラメータマップ）で設定したスプラッシュページドメインを入力します。

ソーシャル認証を有効にする場合は、次のドメインを追加します。

- *.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) **[Configuration]** > **[Tags and Profiles]** > **[Policy]** を選択します。
g) [Policy Profile] ウィンドウで、[default-policy-profile] をクリックします。
h) [Edit Policy Profile] ウィンドウで、[Access Policies] タブをクリックします。
i) [URL Filters] エリアの [Pre Auth] ドロップダウンリストから、以前に作成した ACL を選択します。
j) [Update & Apply to Device] をクリックします。
k) **[Configuration]** > **[Tags and Profiles]** > **[Flex]** を選択します。
l) 使用中のプロファイルをクリックします。
m) 表示される [Edit Flex Profile] ウィンドウで、[Policy ACL] タブをクリックします。
n) [Add] をクリックします。
o) [ACL Name] ドロップダウンリストから、[WA-sec-<ip>] を選択します。
p) [Pre Auth URL Filter] ドロップダウンリストから、以前に作成した URL フィルタ ACL を選択します（ステップ 5a から 5e）。
q) [Save] をクリックします。
r) [Update & Apply to Device] をクリックします。

ステップ 6 SSID を作成します。

a) **[Configuration]** > **[Tags and Profiles]** > **[WLANs]** を選択します。
b) [Add] をクリックします。
a) [General] タブで、[Profile Name] フィールドにプロファイル名を入力します。
b) [SSID] フィールドに、ステップ 2 で定義した SSID 名を入力します。
c) ステータスを [Enabled] に設定します。
d) [Security] タブをクリックしてから、[Layer2] タブをクリックします。
e) [Layer 2 Security Mode] ドロップダウンリストから、[None] を選択します。
f) [Layer3] タブをクリックします。
g) [Web Policy] チェックボックスをオンにします。
h) [Web Auth Parameter Map] ドロップダウンリストから、ステップ 3 で作成した Web 認証パラメータマップを選択します。
i) [Save & Apply to Device] をクリックします。

ステップ 7 RADIUS サーバを設定します。

（注） キャプティブポータルには Radius 認証を使用することを強く推奨します。次の機能は、Radius 認証を設定した場合にのみ使用できます。

- シームレスなインターネット プロビジョニング
- セッション持続時間の延長
- インターネットの拒否

a) **[Configuration]** > **[Security]** > **[AAA]** の順に選択します。
b) [Authentication Authorization and Accounting] ウィンドウで、[Servers/Groups] タブをクリックします。
c) **[Radius]** > **[Servers]** を選択して、[Add] をクリックします。
d) [Name] フィールドに、Radius サーバーの名前を入力します。
e) [IPv4/IPv6 Server Address] フィールドに、Radius サーバーのアドレスを入力します。

（注） Cisco DNA Spaces の Radius サーバーのみを設定できます。Radius サーバーの IP アドレスと秘密鍵を表示するには、Cisco DNA Spaces ダッシュボードで、[Captive Portal] アプリをクリックします。[SSIDs] をクリックし、ステップ 2 で作成した Cisco Catalyst SSID の [Configure Manually] リンクをクリックします。表示されるウィンドウで、Radius サーバーの詳細が [Radius Server Configuration] セクションのリストに表示されます。プライマリおよびセカンダリ Radius サーバの両方の IP を設定します。Cisco DNA Spaces サポート チームに連絡することもできます。

f) [Key] フィールドにキーを入力し、[Confirm Key] フィールドでキーを確認します。
g) [Auth Port] フィールドに「1812」と入力します。
h) [Acct Port] フィールドに「1813」と入力します。
i) [Save & Apply to Device] をクリックします。
追加されたサーバーは、[Servers] リストに表示されます。
j) **[Radius]** > **[Server Groups]** を選択して、[Add] をクリックします。
k) [Name] フィールドに、名前を入力します。
l) [MAC-Delimiter] ドロップダウンリストから、[hyphen] を選択します。
m) [MAC-Filtering] ドロップダウンリストから、[mac] を選択します。
n) 矢印ボタンを使用して、以前に作成した Radius サーバーを [Available Servers] から [Assigned Servers] に移動します。
o) [Save & Apply to Device] をクリックします。
p) [Authentication Authorization and Accounting] ウィンドウで、[AAA Method List] タブをクリックします。
q) [Authentication] をクリックし、[Add] をクリックして、次の詳細を指定します。

1. [Method List Name] フィールドに、メソッドリストの名前を入力します。
2. [Type] ドロップダウンリストから、[Login] を選択します。
3. [Group Type] ドロップダウンリストから、[Group] を選択します。
4. 以前に作成したサーバーグループ（ステップ j からステップ o）を [Available Server Groups] から [Assigned Servers Groups] に移動し、[Save & Apply to Device] をクリックします。

r) [AAA Method List] タブで、[Authorization] をクリックし、[Add] をクリックして、次の詳細を指定します。

1. [Method List Name] フィールドに、メソッドリストの名前を入力します。
2. [Type] ドロップダウンリストから、[Network] を選択します。
3. [Group Type] ドロップダウンリストから、[Group] を選択します。
4. 矢印ボタンを使用して、以前に作成したサーバーグループ（ステップ j からステップ o）を [Available Servers] から [Assigned Servers] に移動し、[Save & Apply to Device] をクリックします。

s) [AAA Method List] タブで、[Accounting] をクリックし、[Add] をクリックして、次の詳細を指定します。

1. [Method List Name] フィールドに、メソッドリストの名前を入力します。
2. [Type] ドロップダウンリストから、[Identity] を選択します。
3. [Group Type] ドロップダウンリストから、[Group] を選択します。
4. 矢印ボタンを使用して、以前に作成したサーバーグループ（ステップ j からステップ o）を [Available Servers] から [Assigned Servers] に移動し、[Save & Apply to Device] をクリックします。

ステップ 8 L3 および L2 認証（MAC フィルタリング）を有効にします。

Radius 認証のパラメータマップで、[Type] として [webauth] が選択されていることを確認します。

（注） L3 および L2 認証を設定するには、SSID を作成し、ステップ 6 のすべての設定を完了していることを確認してください。その後、SSID を Cisco DNA Spaces にインポートし、キャプティブポータルルールを使用して SSID のキャプティブポータルを設定します。

a) **[Configuration]** > **[Tags and Profiles]** > **[WLANs]** を選択します。
b) L2 および L3 認証を設定する SSID をクリックします。
c) [Edit WLAN] ウィンドウで [Security] タブをクリックします。
d) [Layer3] タブで、[Authentication] ドロップダウンリストから、以前に（ステップ 7q で）設定した Radius 認証を選択します。
e) [Layer2] タブで、[MAC Filtering] チェックボックスをオンにして、MAC フィルタリングを有効にします。
f) 表示される [Authorization List] ドロップダウンリストから、以前に（ステップ 7r で）作成した許可サーバーを選択します。
g) [Show Advanced Settings] をクリックします。
h) [On Mac Filter Failure] チェックボックスをオンにします。
i) [Update & Apply to Device] をクリックします。
j) **[Configuration]** > **[Tags and Profiles]** > **[Policy]** を選択します。
k) [default-policy-profile] をクリックします。
l) [Advanced] タブの [AAA Policy] エリアで、[Allow AAA Override] チェックボックスをオンにします。
m) [Policy Name] ドロップダウンリストから、デフォルトの [aaa] ポリシーが選択されていることを確認します。

n) [Update & Apply to Device] をクリックします。

Cisco DNA Spaces コネクタを使用した、Cisco DNA Spaces の Cisco AireOS ワイヤレスコントローラまたは Cisco Catalyst 9800 シリーズ ワイヤレス コントローラへの接続

Cisco DNA Spaces コネクタを備えた シスコ ワイヤレス コントローラ

Cisco DNA Spaces コネクタを使用して Cisco AireOS ワイヤレスコントローラを Cisco DNA Spaces に接続し、キャプティブポータルの認証または通知を設定するには、次の手順を実行します。

- 『Cisco DNA Spaces：コネクタ コンフィギュレーション ガイド』に記載されている手順を参照しながら、Cisco DNA Spaces コネクタを使用して Cisco AireOS ワイヤレスコントローラを Cisco DNA Spaces に接続します。
- Cisco AireOS コントローラを Cisco DNA Spaces に接続した後、インターネット プロビジョニングおよびRADIUS認証のためのシスコ ワイヤレス コントローラの設定の説明に従い、RADIUS 認証とインターネット プロビジョニングを設定します。
- キャプティブポータル認証が必要な場合は、SSID をインポートし、必要な認証タイプでキャプティブポータルを作成し、「キャプティブポータルアプリの使用 （103 ページ）」の章で説明されている手順に基づき、キャプティブポータルルールを設定します。
- キャプティブポータルにソーシャル認証が必要な場合は、「ソーシャル認証のためのシスコ ワイヤレス コントローラの設定 （260 ページ）」の説明に従って、ソーシャル認証を設定します。
- Cisco DNA Spaces を使用して通知を送信する場合は、「Engagements アプリによる通知の送信 （195 ページ）」の章で説明されている手順に基づき、エンゲージメントルールを設定します。

Cisco DNA Spaces コネクタを備えた Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ

Cisco DNA Spaces コネクタを使用して Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを Cisco DNA Spaces に接続し、キャプティブポータルの認証または通知を設定するには、次の手順を実行します。

- Cisco DNA Spaces コネクタを使用して Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを Cisco DNA Spaces に接続するには、『Cisco DNA Spaces：コネクタ コンフィギュレーション ガイド』に記載されている手順を参照してください。
- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを Cisco DNA Spaces に接続した後、ソーシャル認証、RADIUS認証、および（**キャプティブポータル**アプリと**エンゲージメント**アプリ使用のための）インターネットプロビジョニングについては、次の該当するセクションを参照してください。

- CLI を使用したキャプティブポータルおよびエンゲージメントアプリ用の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ（ローカルモード）の設定 （268 ページ）
- キャプティブポータルおよびエンゲージメントアプリ用の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ GUI（ローカルモード） （272 ページ）
- キャプティブポータルおよびエンゲージメントアプリ用の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ GUI（フレックスモードまたは Mobility Express） （278 ページ）。

- キャプティブポータル認証を設定するには、SSID をインポートし、必要な認証タイプでキャプティブポータルを作成し、「キャプティブポータルアプリの使用 （103 ページ）」の章で説明されている手順に基づき、キャプティブポータルルールを設定します。
- Cisco DNA Spaces を使用して通知を送信する場合は、「Engagements アプリによる通知の送信 （195 ページ）」の章で説明されている手順に基づき、エンゲージメントルールを設定します。

Cisco DNA Spaces と連携するための Mobility Express の設定

この項では、Cisco DNA Spaces を使用するために Mobility Express コントローラで行う設定について説明します。

必要な設定は、Mobility Express のバージョンによって異なります。Mobility Express バージョン別の設定方法を次に示します。

Cisco DNA Spaces 用の Mobility Express 8.7 以降の設定

Cisco DNA スペース用に Mobility Express 8.7 以降を設定するには、次の手順を実行します。

Mobility Express での SSID の作成

Mobility Express で SSID を作成するには、次の手順を実行します。

ステップ 1 ログイン情報を使用して [Mobility Express] にログインします。

ステップ 2 メインウィンドウで、左ペインの [Wireless Settings] をクリックします。

ステップ 3 [WLAN（WLANs）] をクリックします。

ステップ 4 WLAN を作成するには、[Add New WLAN] をクリックします。

ステップ 5 表示されるウィンドウの [General] タブで、[Type]、[Profile Name]、[SSID] などの WLAN の詳細を入力します。

ステップ 6 [Apply] をクリックします。

[Add New WLAN/RLAN] ウィンドウが表示されます。

ステップ 7 [WLAN Security] をクリックします。

ステップ 8 [Guest Network] トグルスイッチを有効にします。

ステップ 9 [Captive Network Assistant] トグルスイッチを有効にします。

ステップ 10 [Captive Portal] ドロップダウンリストから、[External Splash Page] を選択します。

ステップ 11 [Access Type] ドロップダウンリストから、[Web Consent] を選択します。

ステップ 12 表示される [Captive Portal URL] フィールドに、Cisco DNA Spaces のスプラッシュ URL を入力します。

ME アカウントのスプラッシュ URL を表示するには、Cisco DNA Spaces ダッシュボードの [SSIDs] ウィンドウで CUWN SSID の [Configure Manually] リンクをクリックします。

ステップ 13 [Apply] をクリックします。

ステップ 14 SSID を有効にしてブロードキャストするには、[General] タブの [Admin] ドロップダウンリストから [Enabled] を選択し、[Broadcast SSID] トグルスイッチを有効にします。

ステップ 15 コマンドプロンプトで次のコマンドを実行して、secure webauth モードを無効にします。その後、ME を再起動します。

```
config network web-auth secureweb disable
```

ステップ 16 コマンド プロンプトで次のコマンドを実行して、webauth login success page を [Default] から [None] に変更します。

config custom-web webauth-login-success-page none

Mobility Express 8.7 以後での Radius 認証の設定

Mobility Express 8.7 以後で Radius 認証を設定するには、次の手順を実行します。

ステップ 1 ログイン情報を使用して [Mobility Express] にログインします。

ステップ 2 ME のメインウィンドウで、ウィンドウ右上の [Switch to Expert View] をクリックします。

ステップ 3 表示されるポップアップウィンドウで、[OK] を選択します。

ステップ 4 左ペインで、[Management] > [Admin Accounts] をクリックします。

ステップ 5 表示されるウィンドウで、[Radius] タブをクリックします。

ステップ 6 [Add RADIUS Authentication Server] をクリックします。

[Add/ Edit Radius Authentication Server] ウィンドウが表示されたら、Radius サーバーに関する次の詳細を入力します。

a) [Server IP Address] フィールドに、Radius サーバーの IP アドレスを入力します。
b) [Shared Secret] フィールドに、Radius 秘密鍵を入力します。
c) [Confirm Shared Secret] フィールドに、Radius 秘密鍵を再入力します。

（注） Cisco DNA Spaces の Radius サーバーのみを設定できます。Radius サーバー設定用の IP アドレスと秘密鍵を表示するには、Cisco DNA Spaces ダッシュボードで、[Captive Portal] アプリをクリックします。[SSIDs] をクリックし、次に Cisco Unified Wireless Network（Cisco AireOS）SSID の [Configure Manually] リンクをクリックします。[Configure SSID in CUWN-WLC] タブをクリックします。Radius サーバーの詳細は、[Radius Server Configuration] セクションのリストに表示されます。プライマリおよびセカンダリ Radius サーバーの両方の IP を設定します。Cisco DNA Spaces サポートチームに連絡することもできます。

ステップ 7 [Apply] をクリックします。

ステップ 8 [Mobility Express] メインウィンドウで、左側のペインの [Wireless Settings] をクリックします。

ステップ 9 [WLANs] をクリックします。

[WLAN/RLAN Configuration] ウィンドウに SSID リストが表示されます。

ステップ 10 以前に作成した SSID の [Edit] アイコンをクリックします。

ステップ 11 表示される [Edit WLAN] ウィンドウで [WLAN Security] タブをクリックします。

ステップ 12 [Access Type] ドロップダウンリストから、[Radius] を選択します。

ステップ 13 [Radius Server] タブをクリックし、[Add Radius Authentication Server] をクリックします。

ステップ 14 [Server IP Address] ドロップダウンリストから Radius サーバーを選択し、[Apply] をクリックします。

ステップ 15 [Edit WLAN] ウィンドウで、[Apply] をクリックします。

これで、Mobility Express 8.7 以降が Radius サーバー認証用に設定されました。

Mobility Express 8.7 以降でのアクセス制御リストの作成

Mobility Express 8.7 以降でアクセス制御リストを作成するには、次の手順を行います。

ステップ 1 ログイン情報を使用して Mobility Express にログインします。

ステップ 2 Mobility Express のメインウィンドウで、左側のペインの [Wireless Settings] をクリックします。

ステップ 3 [WLAN（WLANs）] をクリックします。

[WLAN/RLAN Configuration] ウィンドウに SSID リストが表示されます。

ステップ 4 以前に作成した SSID の [Edit] アイコンをクリックします。

表示される [Edit WLAN] ウィンドウで [WLAN Security] タブをクリックします。

ステップ 5 [Pre Auth ACLs] タブをクリックします。

ステップ 6 [Add IP Rules] をクリックします。

ステップ 7 [Add/Edit IP ACLs] で、次の構成のルールを作成します。

アクション	送信元 IP アドレス/ネットマスク	宛先 IP アドレス/ネットマスク	プロトコル	送信元ポート範囲	宛先ポート範囲	DSCP
許可	34.235.248.212/255.255.255.255	0.0.0.0/0.0.0.0	いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）
許可	0.0.0.0/0.0.0.0	34.235.248.212/255.255.255.255	いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）
許可	52.55.235.39/255.255.255.255	0.0.0.0/0.0.0.0	いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）
許可	0.0.0.0/0.0.0.0	52.55.235.39/255.255.255.255	いずれか（Any）	いずれか（Any）	いずれか（Any）	いずれか（Any）

（注） EU リージョンの場合、34.235.248.212、52.55.235.39を 54.77.207.183、34.252.175.120 に置き換える必要があります。

ACL ルールを定義するときには、次のように値を設定します。

- **Protocol**：Any
- **DSCP**：Any
- **Action**：Permit

ステップ 8 [Apply] をクリックします。

ソーシャル認証のための Mobility Express 8.7 以降の設定

キャプティブポータルのソーシャルサイン認証用に Mobility Express を設定するには、次の手順を実行します。

ステップ 1 ログイン情報を使用して Mobility Express にログインします。

ステップ 2 Mobility Express のメインウィンドウで、左側のペインの [Wireless Settings] をクリックします。

ステップ 3 [WLAN（WLANs）] をクリックします。

[WLAN/RLAN Configuration] ウィンドウに SSID リストが表示されます。

ステップ 4 以前に作成した SSID の [Edit] アイコンをクリックします。

表示される [Edit WLAN] ウィンドウで [WLAN Security] タブをクリックします。

ステップ 5 [Pre Auth ACLs] タブをクリックします。

ステップ 6 [Add IP Rules] をクリックします。

ステップ 7 [Add/Edit IP ACLs] で、既存の ACL ルールに加えて、次の 2 つのルールを設定します。

アクション	送信元 IP アドレス/ネットマスク	宛先 IP アドレス/ネットマスク	プロトコル	送信元ポート範囲	宛先ポート範囲	DSCP
許可	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	TCP	HTTPS	いずれか（Any）	いずれか（Any）
許可	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	TCP	いずれか（Any）	HTTPS	いずれか（Any）

Mobility Express 8.7 以降での URL の許可

Mobility Express 8.7 以降で URL を許可するには、次の手順を行います。

ステップ 1 ログイン情報を使用して Mobility Express にログインします。

ステップ 2 Mobility Express のメインウィンドウで、左ペインの [Wireless Settings] をクリックします。

ステップ 3 [WLAN（WLANs）] をクリックします。

[WLAN/RLAN Configuration] ウィンドウに SSID リストが表示されます。

ステップ 4 以前に作成した SSID の [Edit] アイコンをクリックします。

ステップ 5 表示される [Edit WLAN] ウィンドウで [WLAN Security] タブをクリックします。

ステップ 6 [Pre Auth ACLs] タブをクリックします。

ステップ 7 [Add URL Rules] をクリックします。

ステップ 8 表示される [Add/Edit URL ACLs] ウィンドウで、許可リストに含める URL を設定します。

URL ルールを定義するときには、次のように値を設定します。

- [URL]：domain
- **Action**：Permit

ステップ 9 [更新（Update）] をクリックします。

通知およびレポート用 Mobility Express の設定

WLC 接続で Mobility Express を使用している場合、ロケーションの更新を設定するには、次の手順を実行します。

ステップ 1 シスコ ワイヤレス コントローラの **CLI** で、次のコマンドを実行します。

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

（注） Customer Path Key}、{LB Domain}、{LB IP Address}、{Customer JWT Token} を表示するには、Cisco DNA Spaces ダッシュボードの [SSID] ウィンドウで、CUWN SSID の [Configure Manually] リンクをクリックします。Cisco DNA Spaces サポートチームに連絡することもできます。末尾または先頭にスペースがないことを確認します。

ステップ 2 次のコマンドを使用して、概要を確認します。

show cloud-services cmx summary

結果が表示されます。

Cisco DNA Spaces ダッシュボードで、[Add a Wireless Network] ウィンドウの [CUWN-WLC] を選択すると、WLC が一覧表示されます。これにより、その WLC の AP を Cisco DNA Spaces にインポートできます。

結果サンプル

(Cisco Controller) >show cloud-services cmx summary

CMX Service

Server ..... https://$customerpathkey.dnaspaces.io

IP Address..... 50.16.12.224

Connectivity..... https: UP

Service Status ..... アクティブ

Last Request Status..... HTTP/1.1 200 OK

Heartbeat Status ..... OK

次のタスク

これで、シスコ ワイヤレス コントローラを Cisco DNA Spaces のロケーション階層にインポートできるようになります。シスコワイヤレスコントローラとそのアクセスポイントのインポートの詳細については、「Cisco WLC Direct Connect を使用した Cisco DNA Spaces のシスコ ワイヤレス コントローラへの接続 （263 ページ）」で説明されている手順のステップ 4 から実行してください。

Cisco DNA Spaces 用の Mobility Express 8.6 以前の設定

Cisco DNA Spaces 用に Mobility Express 8.6 以前を設定するには、次の手順を実行します。

Mobility Express 8.6 以前での SSID の作成

Mobility Express 8.6 以前で SSID を作成する手順は、Mobility Express 8.7 以降の場合と同じです。設定手順については、Mobility Express での SSID の作成 （285 ページ）を参照してください。

Mobility Express 8.6 以前での Radius 認証の設定

Mobility Express 8.6 以前の場合、Radius サーバーを個別に設定することはできません。

Mobility Express 8.6 以前で Radius 認証を設定するには、次の手順を実行します。

ステップ 1 ログイン情報を使用して [Mobility Express] にログインします。

ステップ 2 [Mobility Express] メインウィンドウで、左側のペインの [Wireless Settings] をクリックします。

ステップ 3 [WLAN（WLANs）] をクリックします。

[WLAN/RLAN Configuration] ウィンドウに SSID リストが表示されます。

ステップ 4 以前に作成した SSID の [Edit] アイコンをクリックします。

ステップ 5 表示される [Edit WLAN] ウィンドウで [WLAN Security] タブをクリックします。

ステップ 6 [Access Type] ドロップダウンリストから、[Radius] を選択します。

ステップ 7 Radius サーバーを追加するには、[Add] をクリックします。

ステップ 8 表示されるウィンドウで、次の Radius サーバーの詳細を入力します。

1. [Server IP Address] フィールドに、Radius サーバーの IP アドレスを入力します。
2. [Shared Secret] フィールドに、Radius 秘密鍵を入力します。
3. [Confirm Shared Secret] フィールドに、Radius 秘密鍵を再入力します。
4. [Apply] をクリックします。

（注） Cisco DNA Spaces の Radius サーバーのみを設定できます。Radius サーバー設定用の IP アドレスと秘密鍵を表示するには、Cisco DNA Spaces ダッシュボードで、[Captive Portal] アプリをクリックします。[SSIDs] をクリックし、次に Cisco Unified Wireless Network（Cisco AireOS）SSID の [Configure Manually] リンクをクリックします。[Configure SSID in CUWN-WLC] タブをクリックします。Radius サーバーの詳細は、[Radius Server Configuration] セクションのリストに表示されます。プライマリおよびセカンダリ Radius サーバーの両方の IP を設定します。Cisco DNA Spaces サポートチームに連絡することもできます。

ステップ 9 [Edit WLAN] ウィンドウで、[Apply] をクリックします。

これで、Cisco DNA Spaces キャプティブポータルの Radius サーバー認証が Mobility Express に設定されました。

Mobility Express 8.6 以前での ACL の作成

Mobility Express 8.6 以前には、アクセス制御リストを設定するためのユーザーインターフェイスがありません。そのため、ACL を作成し、ソーシャル認証を設定するには、コマンドプロンプトを使用する必要があります。これらの ACL の設定に使用するコマンドについては、『Mobility Express コマンドリファレンスガイド』を参照してください。

これで、シスコ ワイヤレス コントローラを Cisco DNA Spaces のロケーション階層にインポートできるようになります。シスコ ワイヤレス コントローラと、シスコ ワイヤレス コントロー

ラへのアクセスポイントのインポートの詳細については、「Cisco WLC Direct Connect を使用した Cisco DNA Spaces のシスコ ワイヤレス コントローラへの接続 （263 ページ）」で説明されている手順のステップ 3 から実行してください。

通知およびレポート用 Mobility Express の設定

WLC 接続で Mobility Express を使用している場合、ロケーションの更新を設定するには、次の手順を実行します。

ステップ 1 シスコ ワイヤレス コントローラの **CLI** で、次のコマンドを実行します。

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

（注） Customer Path Key}、{LB Domain}、{LB IP Address}、{Customer JWT Token} を表示するには、Cisco DNA Spaces ダッシュボードの [SSID] ウィンドウで、CUWN SSID の [Configure Manually] リンクをクリックします。Cisco DNA Spaces サポートチームに連絡することもできます。末尾または先頭にスペースがないことを確認します。

ステップ 2 次のコマンドを使用して、概要を確認します。

show cloud-services cmx summary

結果が表示されます。

Cisco DNA Spaces ダッシュボードで、[Add a Wireless Network] ウィンドウの [CUWN-WLC] を選択すると、WLC が一覧表示されます。これにより、その WLC の AP を Cisco DNA Spaces にインポートできます。

結果サンプル

(Cisco Controller) >show cloud-services cmx summary

CMX Service

Server ..... https://$customerpathkey.dnaspaces.io

IP Address..... 50.16.12.224

Connectivity..... https: UP

Service Status ..... アクティブ

Last Request Status..... HTTP/1.1 200 OK

Heartbeat Status ..... OK

次のタスク

これで、シスコ ワイヤレス コントローラを Cisco DNA Spaces のロケーション階層にインポートできるようになります。シスコ ワイヤレス コントローラとそのアクセスポイントのインポートの詳細については、「Cisco WLC Direct Connect を使用した Cisco DNA Spaces のシスコ ワイヤレス コントローラへの接続 （263 ページ）」で説明されている手順のステップ 4 から実行してください。

Cisco DNA Spaces 用 Aironet 4800 シリーズ Mobility Express コントローラ 8.10.150.0 の設定

Cisco DNA Spaces 用 AireOS 4800 シリーズ Mobility Express コントローラ 8.10.150.0 を設定するには、次の手順を実行します。

Mobility Express 8.10.150.0 の設定

Cisco DNA Spaces 用に Mobility Express 8.10.105.0 を設定するには、次の手順を実行します。

ステップ 1 ログイン情報を使用して Mobility Express にログインします。

ステップ 2 **[Advanced]** > **[Security Settings]** に移動します。

ステップ 3 [Add New ACL] をクリックします。

ステップ 4 [Add ACL Rule] ウィンドウで、ACL の詳細を入力します。

a) [ACL Type] ドロップダウンリストから、[IPv4] を選択します。

b) [ACL Name] フィールドに、新しい ACL の名前を入力します。

c) [Add URL Rules] をクリックします。

[Add /Edit URL ACLs] ウィンドウが表示されます。

d) [URL] フィールドに、スプラッシュページの URL ドメインを入力します。

e) [Action] ドロップダウンリストで、[Permit] を選択します。

f) ソーシャル認証を有効にするには、ACL に次のドメインを追加します。

- *.facebook.com
- *.facebook.com
- ssl.gstatic.com
- static.licdn.com
- *.fbcdn.net
- *.akamaihd.net
- *.twitter.com
- *.twimg.com
- oauth.googleusercontent.com
- *.googleapis.com
- *.accounts.google.com

- *.gstatic.com
- *.linkedin.com
- *.licdn.net
- *.licdn.com

この手順は、ソーシャル認証を有効にする場合にのみ必要です。

g) [更新（Update）] をクリックします。

ステップ 5 RADIUS サーバーを設定する手順は、次のとおりです。

a) ACL を作成します。
b) [Expert View] を有効にします。
c) **[Managenent]** > **[Admin Accounts]** > **[Radius]** に移動します。
d) [Authentication Call Station ID Type] ドロップダウンリストから、[AP MAC Address:SSID] を選択します。
e) [Authentication MAC Delimiter] ドロップダウンリストから、[Hyphen] を選択します。
f) [Accounting Call Station ID Type] ドロップダウンリストから、[AP MAC Address:SSID] を選択します。
g) [Accounting MAC Delimiter] ドロップダウンリストから、[Hyphen] を選択します。
h) [Fallback Mode] ドロップダウンリストから、[Off] を選択します。
i) [Apply] をクリックします。

ステップ 6 [Add Radius Authentication Server] をクリックし、表示される [Add/Edit Radius Authentication Server] で、次の詳細を入力します。

a) [CoA] を無効にします。
b) [Server Ip Address] フィールドに RADIUS サーバーの IP アドレスを入力します。
c) [Shared Secret] フィールドに、秘密鍵を入力します。
d) [Confirm Shared Secret] フィールドに、確認のための秘密鍵を入力します。
e) [Apply] をクリックします。

追加された Radius サーバーは、Radius サーバーリストの下に表示されます。

（注） Cisco DNA Spaces の Radius サーバーのみを設定できます。Radius サーバー設定の IP アドレスと秘密鍵を表示するには、Cisco DNA Spaces ダッシュボードで、[Captive Portals] アプリをクリックします。[SSIDs] をクリックし、次に Cisco Unified Wireless Network（Cisco AireOS）SSID の [Configure Manually] リンクをクリックします。Radius サーバーの詳細は、[Radius Server Configuration] セクションに表示されます。プライマリとセカンダリの両方の Radius サーバー IP を設定します。Cisco DNA Spaces サポートチームに連絡することもできます。

ステップ 7 Radius サーバーの [WLAN] を設定するには、次の手順を実行します。

a) [Cisco Aironet ME] ダッシュボードで、**[Wireless Settings]** > **[WLAN]** を選択します。
b) [General] タブをクリックします。
c) [Profile Name] フィールドに、SSID の名前を入力します。
d) [Admin State] ドロップダウンリストから、[Enabled] を選択します。
e) [Radio Policy] ドロップダウンリストから、[ALL] を選択します。
f) [WLAN Security] タブをクリックします。

g) [Guest Network] を有効にします。
h) [Captive Network Assistant] を有効にします。
i) [Captive Portal URL] フィールドに、キャプティブポータルの URL を入力します。

（注） キャプティブポータルの URL を表示するには、Cisco DNA Spaces ダッシュボードで、[Captive Portals] アプリをクリックします。[SSIDs] をクリックし、次に Cisco Unified Wireless Network（Cisco AireOS）SSID の [Configure Manually] リンクをクリックします。**WLC Direct Connect の SSID の作成**セクションに移動します。手順 7g で URL が表示されます。

j) [Access Type] から、[RADIUS] を選択します。
k) [ACL Name (IPV4)] で、手順 4b で設定した ACL の名前を選択します。
l) Radius サーバーの場合、[Add Radius Authentication Server] をクリックします。
m) リストから、手順 6b で追加した Radius サーバーの IP を選択します。

ステップ 8 Radius L2 認証の場合、[MAC Filtering] と [ON MAC Filter failure] を有効にします。

ステップ 9 [Apply] をクリックします。

通知およびレポート用 Mobility Express の設定

WLC 接続で Mobility Express を使用している場合、ロケーションの更新を設定するには、次の手順を実行します。

ステップ 1 **シスコ ワイヤレス コントローラの CLI** で、次のコマンドを実行します。

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

（注） Customer Path Key}、{LB Domain}、{LB IP Address}、{Customer JWT Token} を表示するには、Cisco DNA Spaces ダッシュボードの [SSID] ウィンドウで、CUWN SSID の [Configure Manually] リンクをクリックします。Cisco DNA Spaces サポートチームに連絡することもできます。末尾または先頭にスペースがないことを確認します。

ステップ 2 次のコマンドを使用して、概要を確認します。

show cloud-services cmx summary

結果が表示されます。

Cisco DNA Spaces ダッシュボードで、[Add a Wireless Network] ウィンドウの [CUWN-WLC] を選択すると、WLC が一覧表示されます。これにより、その WLC の AP を Cisco DNA Spaces にインポートできます。

結果サンプル

(Cisco Controller) >show cloud-services cmx summary

CMX Service

Server ..... https://$customerpathkey.dnaspaces.io

IP Address..... 50.16.12.224

Connectivity..... https: UP

Service Status ..... アクティブ

Last Request Status..... HTTP/1.1 200 OK

Heartbeat Status ..... OK

次のタスク

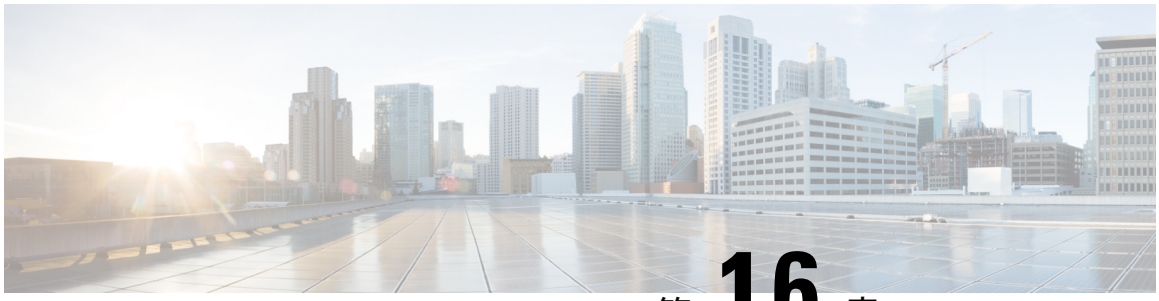
これで、シスコ ワイヤレス コントローラを Cisco DNA Spaces のロケーション階層にインポートできるようになります。シスコ ワイヤレス コントローラとそのアクセスポイントのインポートの詳細については、「Cisco WLC Direct Connect を使用した Cisco DNA Spaces のシスコ ワイヤレス コントローラへの接続 （263 ページ）」で説明されている手順のステップ 4 から実行してください。

Cisco DNA Spaces 拡張ベンチマーク

表 *13 :* 拡張の概要

SNO	Cisco DNA Spaces コネクタ	Cisco WLC Direct Connect		CMX テザリング コネクタ
プラットフォーム	Cisco AireOS	Cisco AireOS	Cisco Catalyst 9800 シリーズ	Cisco AireOS
サポートされているアプライアンスでの最大拡張	12500 台の AP、250000 台のクライアント 着信 NMSP は、10500 メッセージ/秒を超えることはできません。	50 台の AP と 50 台のクライアント	50 台の AP と 50 台のクライアント	60000 台のクライアント、5000 台の AP、50000 個の RFID タグ 1 ビルディング - 100 フロアと各フロアに 50 台の AP のマップ
拡張がサポートされているリリース	コネクタバージョン 2.1.1 と docker v2.0.204	8.8MR2	16.12、17.1	8.8MR2 と CMX 10.6（ハイエンド）

（注） 現在、Mobility Express は拡張に対応していません。



第 16 章

Cisco DNA Spaces を使用するための Cisco Meraki の設定

この章では、Cisco DNA Spaces を使用するために Cisco Meraki に必要な設定について説明します。

Cisco Meraki サービスアカウントの設定

組織、ネットワーク、AP などの Meraki ネットワークの詳細は、Meraki サービスアカウントを使用して取得し、Cisco DNA Spaces に提供できます。

このサポートを利用するには、Meraki カスタマーアカウントから Meraki サービスアカウントを招待する必要があります。Meraki サービスアカウントの電子メール ID については、Cisco DNA Spaces サポートチームにお問い合わせください。

（注）

- ただし、Cisco DNA Spaces を Cisco Meraki に接続するには、引き続き Meraki カスタマーアカウントを使用する必要があります。お客様の Meraki アカウントは、ユーザーがアクセス可能なロケーション階層にネットワークをインポートするために使用されます。サービスアカウントは、ロケーション階層を最新の状態に保つためのバックグラウンドネットワーク同期に使用されます。
- Cisco Meraki は Cisco DNA Spaces に含まれていないため、メニューパスおよびメニュー名は変更される場合があります。

Cisco Meraki で Cisco Meraki サービスアカウントを設定するには、次の手順を実行します。

ステップ 1 https://meraki.cisco.com に移動します。

ステップ 2 Cisco Meraki アカウントのログイン情報を使用してアプリケーションにログインします。

ステップ 3 [Cisco Meraki Organization] ドロップダウンリストから、Meraki サービスアカウントを設定する組織を選択します。

ステップ 4 **[Organization]** > **[Administrators]** > **[Add Admin]** を選択します。

ステップ 5 Cisco Meraki サービスアカウントの名前と電子メール ID を入力します。

ステップ 6 [Organization Access] ドロップダウンリストから [Full] を選択します。

ステップ 7 [Create Admin] をクリックします。

これで、フィルタリングされた組織に対して Cisco Meraki サービスアカウントが設定されました。

Cisco Meraki での SSID の有効化

SSID をキャプティブポータルルール用に設定するために Cisco DNA Spaces にインポートするには、それらの SSID を Cisco Meraki で有効にする必要があります。

（注） Cisco Meraki は Cisco DNA Spaces に含まれていないため、メニューパスおよびメニュー名は変更される場合があります。

Cisco Meraki で SSID を有効にするには、次の手順を実行します。

ステップ 1 https://meraki.cisco.com に移動します。

ステップ 2 Cisco Meraki アカウントのログイン情報を使用してアプリケーションにログインします。

ステップ 3 SSID を有効にする必要のある [Cisco Meraki Organization] をクリックし、必要なネットワークを選択します。

ステップ 4 **[Wireless]** > **[Configure]** > **[SSIDs]** の順に選択します。

ネットワークで使用可能な SSID が表示されます。

ステップ 5 SSID の名前を変更して有効にします。

ステップ 6 [Edit Settings] をクリックし、[Splash] ページオプションで [Click-Through] オプションボタンをクリックします。

ステップ 7 [Save Changes] をクリックします。

SSID が Cisco Meraki で正常に有効化されました。

RADIUS 認証用の Cisco Meraki の設定

ポータルにより多くのセキュリティを提供するために、Cisco DNA Spaces はポータルに RADIUS 認証を提供します。また、キャプティブポータルルールを使用して設定できるシームレスなインターネット プロビジョニングを管理するには、Cisco Meraki で特定の設定が必要です。

シームレスなインターネット プロビジョニングを設定するときに必要な Radius サーバー設定は、標準の Radius サーバー設定とは異なります。

RADIUS 認証用の Cisco Meraki の設定（シームレスなインターネット設定なし）

RADIUS 認証用に Cisco Meraki を設定するには、次の手順を実行します。

ステップ 1 Meraki のログイン情報で Cisco Meraki にログインします。

ステップ 2 [Wireless Access Control] を選択します。

ステップ 3 キャプティブ ポータル ルールの SSID を選択します。

ステップ 4 [Association requirements] エリアで、[Open] を選択します。

ステップ 5 [Splash page] エリアで [Sign-on with] を選択し、ドロップダウンリストから [my RADIUS server] を選択します。

ステップ 6 [Radius servers] エリアで [Add a server] をクリックし、表示されたフィールドに認証のための RADIUS サーバーの詳細を指定します。

- ポート：1812

（注） Cisco DNA Spaces RADIUS サーバーのみを設定できます。RADIUS サーバーの IP アドレスと秘密鍵を表示するには、Cisco DNA Spaces ダッシュボードで、[SSIDs] ページの Meraki SSID の [Configure Manually] リンクをクリックします。

ステップ 7 [Radius accounting] ドロップダウンリストから、[Radius Accounting is enabled] を選択します。

ステップ 8 [Radius accounting servers] エリアで、[Add a server] をクリックし、表示されたフィールドにアカウンティングのための RADIUS サーバーの詳細を指定します。

- ポート：1813

（注） Cisco DNA Spaces の Radius サーバーのみを設定できます。Cisco DNA Spaces RADIUS サーバーのみを設定できます。RADIUS サーバーの IP アドレスと秘密鍵を表示するには、Cisco DNA Spaces ダッシュボードで、[SSIDs] ページの Meraki SSID の [Configure Manually] リンクをクリックします。

ステップ 9 ウォールド ガーデンの範囲を設定します。ウォールガーデンの範囲を表示するには、Cisco DNA Spaces ダッシュボードで、SSID ページの Meraki SSID の [Configure Manually] リンクをクリックします。

ステップ 10 変更内容を保存します。

RADIUS 認証およびシームレスなインターネット プロビジョニングのための Cisco Meraki の設定

Radius 認証およびシームレスなインターネット プロビジョニング向けに Cisco Meraki を設定するには、Cisco Meraki で次の設定を行います。

ステップ 1 Meraki のログイン情報で Cisco Meraki にログインします。

ステップ 2 **[Wireless]** > **[Access]** > **[Control]** の順に選択します。

ステップ 3 キャプティブ ポータル ルールの SSID を選択します。

ステップ 4 [Association requirements] 領域で、[Mac-based access control (no encryption)] を選択します。

ステップ 5 [Splash] ページ領域で、[Click-through] を選択します。

ステップ 6 [Radius servers] エリアで [Add a server] をクリックし、表示されたフィールドに認証のための RADIUS サーバーの詳細を指定します。

- ポート：1812

（注） Cisco DNA Spaces の Radius サーバーのみを設定できます。RADIUS サーバーの IP アドレスと秘密鍵を表示するには、Cisco DNA Spaces ダッシュボードで、[SSIDs] ページの Meraki SSID の [Configure Manually] リンクをクリックします。

ステップ 7 [Radius accounting] ドロップダウンリストから、[Radius Accounting is enabled] を選択します。

ステップ 8 [Radius accounting servers] エリアで、[Add a server] をクリックし、表示されたフィールドにアカウンティングのための RADIUS サーバーの詳細を指定します。

- ポート：1813

（注） Cisco DNA Spaces RADIUS サーバーのみを設定できます。RADIUS サーバーの IP アドレスと秘密鍵を表示するには、Cisco DNA Spaces ダッシュボードで、[SSIDs] ページの Meraki SSID の [Configure Manually] リンクをクリックします。

ステップ 9 [Radius attribute specifying group policy name] ドロップダウンリストから、[Filter-Id] を選択します。

ステップ 10 変更内容を保存します。

ステップ 11 Cisco Meraki ダッシュボードで、[Network-wide Group Policies] をクリックします。

ステップ 12 [Add a Group] をクリックします。

ステップ 13 表示される [New group] ウィンドウに、グループの名前を入力します。

（注） Cisco DNA Spaces ダッシュボードで、この名前をポリシー名として設定する必要があります。グループ名を「CaptiveBypass」と指定する場合、このポリシー名はすべてのキャプティブポータルルールのデフォルトのポリシー名として機能します。つまり、[Seamlessly Internet Provision] が選択されるキャプティブポータルルールに対してポリシー名を指定しない場合、ポリシー名「CaptiveBypass」がこのルールに対して適用されます。

ステップ 14 [Bandwidth] ドロップダウンリストから必要なオプションを選択し、顧客にプロビジョニングするインターネットの帯域幅を指定します。

ステップ 15 [Splash] ドロップダウン リストから [Bypass] を選択します。

ステップ 16 [Apply] をクリックします。

ステップ 17 ウォールド ガーデンの範囲を設定します。ウォール ガーデンの範囲を表示するには、Cisco DNA Spaces ダッシュボードで、SSID ページの Meraki SSID の [Configure Manually] リンクをクリックします。

通知およびレポート用 Cisco Meraki の設定

Cisco DNA Spaces を使用して通知を送信し、Cisco DNA Spaces レポートを表示するには、Cisco Meraki で特定の設定を行う必要があります。

（注） Meraki ネットワークロケーションをロケーション階層にインポートすると、通知 URL が Cisco Meraki で自動的に設定されます。このサポートは、Meraki API キーを使用して追加された Meraki ネットワークには適用されません。

Cisco DNA Spaces を使用して通知を送信する、または Cisco DNA Spaces のレポートを表示するために Cisco Meraki を手動で設定するには、次の手順を実行します。

ステップ 1 Cisco Meraki アカウントのログイン情報を使用して Meraki にログインします。

ステップ 2 SSID を有効にする必要のある組織をクリックし、必要なネットワークを選択します。

ステップ 3 **[Network-wide]** > **[Configure]** > **[General]** の順に選択します。

ステップ 4 [CMX] 領域で、次の手順を実行します。

a) [Analytics] ドロップダウンリストから、[Analytics is enabled] を選択します。
b) [Scanning API] ドロップダウンリストから、[Scanning API enabled] を選択します。
c) [Add a Post URL] をクリックし、それぞれのフィールドに POST URL の詳細を入力します。

投稿 URL の詳細を表示するには、Cisco DNA Spaces ダッシュボードで、[SSIDs] ウィンドウの Meraki SSID の [Configure Manually] リンクをクリックします。

ステップ 5 [Save Changes] をクリックします。

ソーシャル認証のための Cisco Meraki の設定

Cisco Meraki でソーシャル認証を行うには、meraki.cisco.com に一定の設定をする必要があります。

ソーシャル認証のために Cisco Meraki を設定するには、次の手順を実行します。

ステップ 1 Cisco Meraki ダッシュボードで、**[Wireless]** > **[Configure]** > **[Access Control]** の順に選択します。

[Access Control] ウィンドウが表示されます。

ステップ 2 [SSID] ドロップダウンリストから、ソーシャル認証を設定する SSID を選択します。

ステップ 3 [Wall Garden Ranges] フィールドに、次の表にリストされているソーシャルネットワークのドメイン名を入力し、[Save Changes] をクリックします。

表 *14*: ソーシャル ネットワークのドメイン名

Facebook	Twitter	LinkedIn	Instagram
*.facebook.com	*.twitter.com	*.linkedin.com	instagram.com
*.fbcdn.net	*.twimg.com	*.licdn.net	*.instagram.com
*.akamaihd.net		*.licdn.com	api.instagram.com
*.connect.facebook.net			d36xtkk24g8jdx.cloudfront.net
			www.facebook.com
			connect.facebook.net
			*.akamaihd.net

Cisco Meraki のソーシャル認証が正常に設定されます。

Cisco Meraki の SSID の手動設定

Meraki で SSID を手動設定するには、まずその SSID を Cisco DNA Spaces にインポートする必要があります。詳細については、「Cisco Meraki の SSID のインポート」のセクションを参照してください。

Meraki で SSID を手動設定するには、次の手順を実行します。

ステップ 1 Cisco Meraki アカウントのログイン情報を使用して Meraki にログインします。

ステップ 2 それぞれのドロップダウンリストから必要な Meraki 組織およびネットワークを選択します。

ステップ 3 **[Wireless]** > **[Access Control]** の順に選択します。

ステップ 4 [SSID] ドロップダウンリストから、Cisco DNA Spaces に設定する SSID を選択します。

ステップ 5 [splash] ページ領域で、[Click-through] を選択します。

ステップ 6 [Wall garden] ドロップダウンリストから、[Wall garden is enabled] を選択します。

ステップ 7 [Wall garden ranges] テキストフィールドに、必要なウォールドガーデンの範囲を入力します。

ウォールドガーデンの範囲を表示するには、Cisco DNA Spaces ダッシュボードで、[SSIDs] ウィンドウにある Meraki SSID の [Configure Manually] リンクをクリックします。

ステップ 8 [Save Changes] をクリックします。

ステップ 9 **[Wireless]** > **[Splash page]** を選択します。

ステップ 10 以前に指定された SSID に対しては、[Custom Splash URL] エリアで、[Or provide a URL where customers will be redirected] を選択するか、隣接するフィールドにスプラッシュ URL を入力します。

Meraki SSID のスプラッシュページ URL を生成して表示するには、次の手順に従います。

a) **[Home]** > **[Captive Portals]** > **[SSIDs]** をクリックして、Meraki SSID を Cisco DNA Spaces にインポートします。
Cisco DNA Spaces ダッシュボードにスプラッシュページの URL が生成されます。

b) [SSIDs] ページで、目的の Meraki SSID の [Configure Manually] リンクをクリックします。
選択した Meraki SSID のスプラッシュページ URL が表示されます。

ステップ 11 [Splash Behavior] エリアで、[Where should users go after the splash page] にある [The URL they were trying to fetch] オプションボタンをクリックします。

ステップ 12 [Save Changes] をクリックします。

ステップ 13 Cisco DNA Spaces で使用するすべての SSID について、ステップ 3 ～ 12 を繰り返します。

次のタスク

Cisco Meraki でのスキャン API の設定

Meraki カメラを使用するには、Cisco Meraki でスキャン API を設定する必要があります。

Cisco Meraki でスキャン API を設定するには、次の手順を実行します。

ステップ 1 Cisco Meraki アカウントのログイン情報を使用して https://meraki.cisco.com にログインします。

ステップ 2 **[Networkwide]** > **[General]** の順に選択します。

ステップ 3 [Location and Scanning] エリアで、次の手順を実行します。

a) [Analytics] ドロップダウンリストから、[Analytics enabled] を選択します。

b) [Scanning API] ドロップダウンリストから、[Scanning API enabled] を選択します。

c) ポスト URL を追加します。

- [Post URL] フィールドに、ポスト URL を入力します。

- [Secret Key] フィールドに、Cisco Meraki クラウドからの JSON ポストを検証するために HTTP サーバーが使用する秘密鍵を入力します。

  （注） Cisco DNA Spaces ダッシュボードの **[Setup]** > **[Camera]** の [Connect your Meraki Camera] ウィンドウから、ポスト URL と秘密鍵をコピーできます。

- [API Version] ドロップダウンリストから、HTTP サーバーが受信して処理できるロケーション API バージョンを選択します。

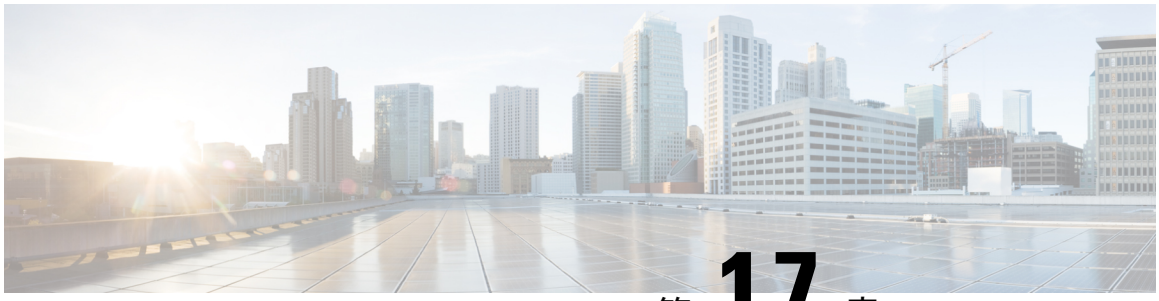
ステップ 4 JSON オブジェクトを受信するように HTTP サーバーを設定し、ホストします。

ステップ 5 最初の接続時に、Cisco Meraki クラウドは、組織の ID が Cisco Meraki の顧客であることを確認します。

次に、Cisco Meraki クラウドが JSON の送信を開始します。

第 部

統合



第 17 章

Cisco DNA Spaces SDK の統合

この章では、Cisco DNA Spaces ソフトウェア開発キット（SDK）の統合に関する情報を提供します。

Cisco DNA Spaces SDK の統合

Cisco DNA Spaces ソフトウェア開発キット（SDK）は、OpenRoaming テクノロジーを活用して、ユーザーによる操作を必要とせずに、シームレスかつ安全にユーザーを Wi-Fi ネットワークに接続します。Cisco DNA Spaces SDK により、iOS または Android アプリケーションのデベロッパーは、バックエンドシステムで検証できる任意の ID を使用して iOS および Android デバイスを設定できます。また、Cisco DNA Spaces SDK を使用すると、デベロッパーは、iOS および Android の通知フレームワーク経由で、ユーザーに関する詳細情報を追加し、デバイス上でユーザーと直接関わり合うことができます。

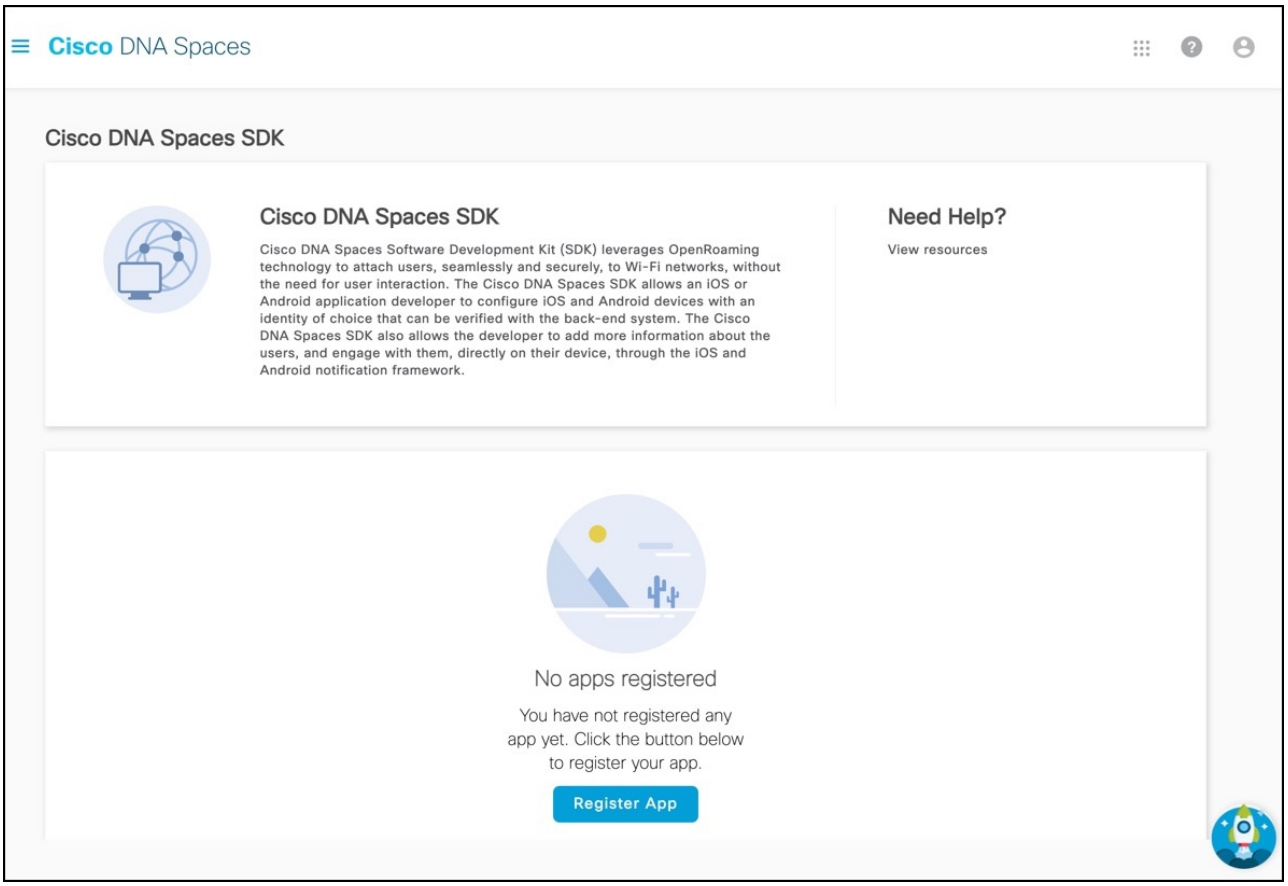
SDK 設定セクションには、[Hamburger] メニューアイコン > [Integrations] > [Cisco DNA Spaces SDK] からアクセスできます。これにより、顧客はネイティブアプリ（iOS および/または Android）を Cisco DNA Spaces に登録できます。

Cisco DNA Spaces SDK の統合

ステップ 1 Cisco DNA Spaces ダッシュボードの左上に表示される 3 本線のメニューアイコンを選択します。

ステップ 2 **[Integrations]** > **[Cisco DNA Spaces SDK]** を選択します。

図 *14* : アプリの登録



ステップ 3 [Register App] をクリックします。

[Register App] ウィンドウが表示されます。

ステップ 4 新しいアプリを登録するプラットフォームを選択するには、[iOS]、[Android] チェックボックスのいずれか、あるいはその両方をオンにします。

両方のプラットフォームを選択すると、後続のウィンドウに両方のプラットフォームのパラメータが表示されます。

ステップ 5 [Next] をクリックします。

ステップ 6 次を入力します。

- [App Name]：アプリケーションの名前を入力します。
- [Bundle Identifier]：iOS プラットフォームでアプリを識別するバンドル ID またはバンドル識別文字列を入力します。

（注） すべての iOS アプリケーションが機能するにはバンドル ID が必要であり、開発者が App Store で公開する場合は一意である必要があります。バンドル ID の形式は、`domain.your-company.app-name` です。

- [Package Name]：Android アプリを識別するための一意のパッケージ名を入力します。

（注） アプリのパッケージ名の形式は、`domain.your-company.app-name` です。ただし、任意の名前を入力することを選択できます。

ステップ 7 [Next] をクリックします。

ステップ 8 プッシュ通知を有効にするには、 [Enable Push Notification for iOS] チェックボックスをオンにします。

a) iOS アプリ ID を入力します。
b) [Upload をクリックして、APNS P12 と証明書を検索、アップロードします。
c) APNS 証明書のパスワードを入力します。

ステップ 9 Android のプッシュ通知を有効にするには、 [Enable Push Notification for Android] チェックボックスをオンにします。

a) Android アプリ ID を入力します。
b) API キーを入力します。

ステップ 10 [Next] をクリックします。

ステップ 11 新しいモバイルアプリのユーザー識別として Apple サインインをサポートするには、[Authentication] セクションの [Enable Apple Sign In] にチェックを付けます。

a) [Enter Client ID] フィールドに、Apple アカウントのサインインクライアント ID を入力します。
b) [Enter Secret Key] フィールドに、Apple アカウントの秘密鍵を入力します。

ステップ 12 新しいモバイルアプリのユーザー識別として Google サインインをサポートするには、[Authentication] セクションの [Enable Google Sign In] にチェックを付けます。

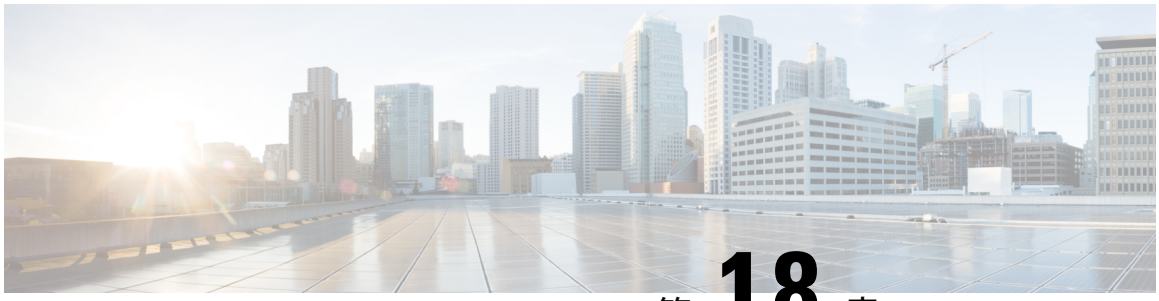
a) [Enter Client ID] フィールドに、Google アカウントのサインインクライアント ID を入力します。
b) [Enter Secret Key] フィールドに、Google アカウントの秘密鍵を入力します。

ステップ 13 [Register App] をクリックして、アプリの登録を完了します。

[View Configurations] をクリックして、アプリケーションの設定の詳細を表示できます。必要に応じて、[Delete] アイコンをクリックして、登録済みのアプリケーションを削除できます。

ステップ 14 （任意）[Edit] をクリックして、iOS および Android プラットフォームのプッシュ通知を更新します。

ステップ 15 （任意）[Update] をクリックします。



第 18 章

Cisco DNA Center の統合

この章では、Cisco DNA Spaces と Cisco DNA Center の統合について説明します。

概要

Cisco DNA Spaces と Cisco DNA Center の統合が可能なので、Cisco DNA Spaces を使用して Cisco DNA Center サイトを監視できます。

（注） 現在、Cisco DNA Center と Cisco DNA Spaces の統合は、自動マップエクスポートとロケーション階層の同期のみに制限されています。この統合では、キャプティブポータルベースの認証機能はサポートされません。

前提条件

- Cisco DNA Center リリース **2.1.2.3 以上**。Cisco DNA Center リリース 2.1.2.3 を使用している場合は、次の情報を dnaspaces-dnac-integration@external.cisco.com に送信する必要があります。
  - Cisco DNA Center クラスタのメンバー ID。この ID は、Cisco DNA Center コンソールで次のコマンドを入力して取得できます。

    ```
    magctl service exec telemetry-agent 'curl
    http://127.0.0.1:8011/api/telemetry-agent/v1/membership/info'
    ```

  - Cisco DNA Center がライセンス供与または登録されている顧客企業の名前。たとえば「Cisco Systems」のように入力します。
- Cisco DNA Spaces Enabler パッケージ。ライセンスの取得については、dnaspaces-dnac-integration@external.cisco.com までご連絡ください。

（注）
- Cisco DNA Center リリース 2.2.1.0 以降、この統合に Cisco DNA Spaces Enabler パッケージは必要ありません。
- Cisco DNA Center を以前のリリースからリリース 2.2.1.0 にアップグレードする場合は、Cisco DNA Spaces Enabler パッケージをアンインストールする必要があります。イネーブラをアンインストールしないと、Cisco DNA Center のバックアップおよび復元操作は失敗します。

Cisco DNA Spaces と Cisco DNA Center の統合

Cisco DNA Spaces を Cisco DNA Center と統合するには、次の手順を実行します。

ステップ 1 Cisco DNA Center に Cisco DNA Spaces Enabler パッケージを展開します。Cisco DNA Center リリース 2.2.1.0 を使用している場合は、このステップをスキップしてステップ 2 から始めてください。ステップ 2 （315 ページ）

a) [Cisco DNA Center] にログインします。
b) Cisco DNA Center ダッシュボードの左上に表示される 3 本線のメニューアイコンをクリックします。
c) **[System]** > **[Settings]** > **[DNA Spaces/CMX Servers]**を選択します。

表示される DNA Spaces/CMX Servers ウィンドウに、「DNA Spaces integration can be enabled using optional package」というメッセージが表示されます。

d) **[System]** > **[Software Updates]** を選択します。

ライセンスが利用可能な場合、表示される [System Update] ウィンドウの [Application Updates] 領域で、[Outdated Applications] の下に DNA Spaces Enabler パッケージがリストされます。

（注） DNA Spaces Enabler の [Outdated Applications] ラベルは、将来のリリースで削除される予定です。

e) [Install All] をクリックします。
f) 表示されるダイアログボックスで、[DNA Spaces Enabler Package] にチェックを入れ、[Continue] をクリックします。
g) 表示される [System Readiness Check] ダイアログボックスで、[Continue] をクリックします。

「Package will soon install」というメッセージを示す [System Update] ウィンドウが表示されます。

h) ウィンドウの左側のペインで、[Installed Apps] をクリックします。

パッケージがインストールされている場合、DNA Spaces Enabler パッケージは、[Installed Applications] ウィンドウの [Outdated Applications] の下にリストされます。

i) ウィンドウ左上の 3 本線のメニューアイコンをクリックして、**[System]** > **[Settings]** > **[DNA Spaces/CMX Servers]**を選択します。

[DNA Spaces/CMX Servers] ウィンドウで、[DNA Spaces] エリアの [Activate] をクリックします。

ステップ 2 Cisco DNA Spaces の顧客のオンボーディング。

a) Cisco DNA Spaces のログインウィンドウで、ログインクレデンシャルを入力し、[Continue] をクリックします。

b) [Select Customer] ドロップダウンリストから、Cisco DNA Center インスタンスの Cisco DNA Spaces の顧客名（テナント）を選択し、[Proceed] をクリックします。

c) ダッシュボードの左上に表示される 3 本線のメニューアイコンをクリックします。

d) **[Setup]** > **[Wireless Networks]** の順に選択します。

e) 表示される [Connect your wireless network] ウィンドウで、[Connect via Spaces Connector] ウィジェットを展開します。

[Connect via Spaces Connector] がウィンドウに表示されない場合は、ワイヤレスネットワークのセットアップ （321 ページ）の指示に従ってウィジェットを表示します。

f) このウィジェットで説明されている手順を使用して、ワイヤレスネットワークを Cisco DNA Spaces に接続します。

Cisco DNA Spaces コネクタを使用してワイヤレスネットワークを Cisco DNA Spaces に接続する方法の詳細については、『Cisco DNA Spaces Connector Configuration Guide』を参照してください。

ステップ 3 Cisco DNA Spaces クラスタを Cisco DNA Spaces に登録します。

a) ダッシュボードの左上に表示される 3 本線のメニューアイコンをクリックします。

b) **[Integrations]** > **[DNA Center]**を選択します。

c) 表示される [DNAC Integration] ウィンドウで、[Create Token] をクリックします。

d) [Instance Name] フィールドの [Create new token] ダイアログボックスで、Cisco DNA Center のインスタンス名を入力し、[Create Token] をクリックします。

トークンが表示されます。

e) [Copy Token] をクリックして、トークンをコピーします。

f) [Cisco DNA Center] にログインします。

g) ウィンドウ左上の 3 本線のメニューアイコンをクリックして、**[System]** > **[Settings]** > **[DNA Spaces/CMX Servers]**を選択します。

h) 表示される [DNA Spaces/CMX Servers] ウィンドウで、[DNA Spaces] エリアの [Activate] をクリックします。

i) [Integrate DNA Spaces] ダイアログボックスで、トークンを貼り付けて、[Connect] をクリックします。

[DNA Spaces/CMX Servers] ウィンドウの [DNA Spaces] エリアに、顧客名（テナント）とともにステータスが [Activated] として表示されます。

（注） 一部のブラウザでは、トークンを貼り付けた後でも、[OK] ボタンが無効のままになる場合があります。**Tab** キーを押して [OK] ボタンに移動するか、別のブラウザをお試しください。

j) ウィンドウ右上の [Account] アイコンをクリックし、アカウント名が [DNA Spaces] エリアに表示されているテナント名と同じであることを確認します。

ステップ 4 Cisco DNA Spaces を Cisco DNA Center サイトに割り当てます。

a) [Cisco DNA Center] ダッシュボードの左上にある 3 本線のメニューアイコンをクリックします。
b) **[System]** > **[Settings]** > **[DNA Spaces/CMX Servers]**を選択します。
c) 表示される [DNA Spaces/CMX Servers] ウィンドウで、CMX サーバーが使用可能であり、Cisco DNA Spaces の顧客名がアクティブ化されていることを確認します。
d) **[Design]** > **[Network Settings]**を選択します。
e) [Cisco DNA Spaces] を使用して監視するロケーションをクリックします。
f) [Wireless] タブをクリックします。
g) [DNA Spaces/CMX Servers] エリアで、[Location Services] ドロップダウンリストから、Cisco DNA Spaces の顧客名を選択し、[Save] をクリックします。
h) [Cisco DNA Center] ダッシュボードの左上にある 3 本線のメニューアイコンをクリックします。
i) **[Design]** > **[Network Hierarchy]**を選択します。
j) 監視するロケーションをクリックします。

このロケーションのサイトマップが AP とともに表示されます。

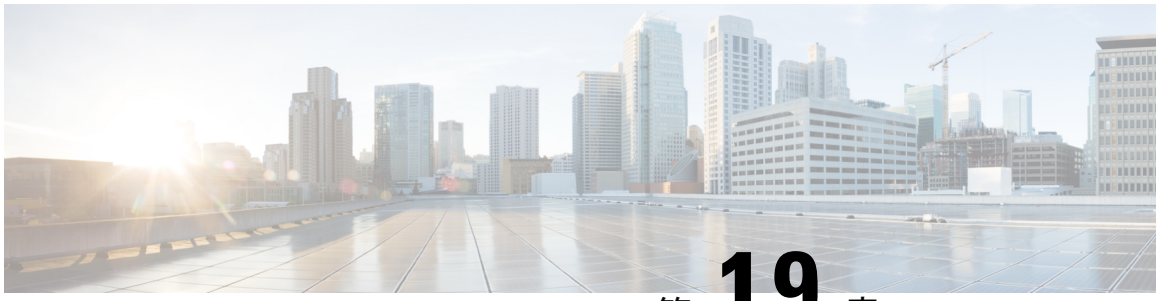
k) カラーバーで、サイトに適用する色をクリックします。
l) ロケーションに表示されるサイトマップをクリックします。

選択した色がサイトマップに適用されます。

m) ステップ 4d からステップ 4l を使用して、監視するその他のサイトを設定します。

サイトを監視できるようになりました。

Cisco DNA Spaces コネクタが接続するシスコ ワイヤレス コントローラのインターフェイス（IP アドレス）が、Cisco DNA Center が接続するシスコ ワイヤレス コントローラのインターフェイスと異なる場合、フロアマップの上部に「Unable to determine connector status」というエラーメッセージが表示されます。これは無視できます。この問題は今後のリリースで修正される予定です。



第 19 章

Cisco DNA Spaces と ServiceNow アプリケーションの統合

この章では、Cisco DNA Spaces を [ServiceNow] アプリケーションと統合する方法について説明します。

Cisco DNA Spaces と ServiceNow アプリケーションの統合

この章では、Cisco DNA Spaces を [ServiceNow] アプリケーションと統合する方法について説明します。

ServiceNow

Cisco DNA Spaces は **ServiceNow** アプリケーションと統合できるため、Cisco DNA Spaces アプリから **ServiceNow** にデータを自動転送して、そのサービスを利用できます。

（注）　現在、**ServiceNow** 統合サポートは、プロキシミティレポートでのみ利用できます。

Cisco DNA Spaces と ServiceNow の統合

Cisco DNA Spaces を ServiceNow アプリケーションと統合するには、次の手順を実行します。

（注）　ServiceNow アカウントがあり、必要なタスク ID を作成していることを確認してください。

ステップ 1　Cisco DNA Spaces ダッシュボードの左上に表示される 3 本線のメニューアイコンを選択します。

ステップ 2　**[Integration]** > **[ServiceNow]** の順に選択します。

ステップ 3 表示される [ServiceNow Integration] ウィンドウで、ServiceNow アカウントの ServiceNow URL、クライアント ID、および秘密鍵を入力します。

ステップ 4 [Register] をクリックします。

ステップ 5 手順 2 で表示される [Authentication] をクリックします。

ServiceNow ログインウィンドウにリダイレクトされます。

ステップ 6 ログイン情報を入力し、[Login] をクリックします。

Cisco DNA Spaces が ServiceNow との接続を確立しようとしていることを示すメッセージが表示されます。

ステップ 7 [Allow] をクリックして統合を認証します。

接続に成功すると、[ServiceNow Integration] ウィンドウに [Active] ステータスが表示されます。[Disconnect] リンクを使用していつでも切断できます。

ステップ 8 次に、ServiceNow アプリケーションを使用する Cisco DNA Spaces アプリで、タスク ID を設定します。たとえば、Proximity Reporting アプリで、レポートを ServiceNow アプリケーションに自動転送するには、次の手順を実行します。

a) **プロキシミティレポート**を開きます。

b) [Create Report] をクリックします。

c) [Look Up Summary] ウィンドウで、レポートを生成するユーザー名または MAC アドレスを検索します。たとえば、00: で始まるすべての MAC アドレスを表示するには、[Search] フィールドに 00: と入力します。

見つかったすべてのデバイスの MAC アドレスが一覧表示されます。

d) レポートを生成する MAC アドレスを確認します。

e) [Time Range] 領域で、レポートを生成する期間の開始日と終了日を入力します。

f) [Auto-submit report data to ServiceNow task] をオンにします。

（注） [Auto-submit report data to ServiceNow task] チェックボックスは、ステップ 1 からステップ 7 で説明した、ServiceNow と Cisco DNA Spaces との統合を認証した場合にのみ表示されます。

g) [DiagnosticTask ID] フィールドに、ServiceNow アプリケーションで作成されたタスク ID を入力します。

（注） [DiagnosticTask ID] フィールドは、[Auto-submit report data to ServiceNow task] をオンにした場合にのみ表示されます。

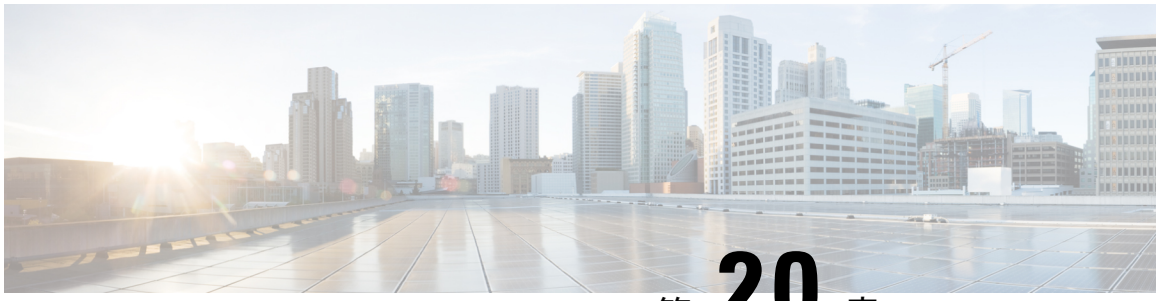
h) [Report Name] フィールドに、レポートの名前を入力します。

i) [Generate Report] をクリックします。

レポートが生成されると、このレポートは ServiceNow アプリケーションに自動的に転送されます。ServiceNow アプリケーションはこのレポートを使用して、設定されたタスク ID に関連するタスクを実行します。

第 II 部

設定



第 20 章

ワイヤレスネットワークのセットアップ

この章では、さまざまなワイヤレスネットワークの設定手順を表示する方法と、さまざまなメソッドを使用してワイヤレスネットワークを設定する方法の概要を示します。

• さまざまなワイヤレスネットワークで動作する Cisco DNA Spaces の設定 （321 ページ）

さまざまなワイヤレスネットワークで動作するCiscoDNA Spaces の設定

Cisco DNA Spaces が動作するためには、ワイヤレスネットワークに接続する必要があります。Cisco DNA Spaces は、Cisco AireOS、Cisco Catalyst、または Cisco Meraki で使用できます。Cisco DNA Spaces は、さまざまなネットワークに接続するために必要な機能と手順を提供します。

Cisco DNA Spaces をワイヤレスネットワークに接続するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、**[Setup]** > **[Wireless Networks]**を選択します。

ステップ 2 [Connect your wireless Network] ウィンドウで、[Add New] をクリックします。

オプション [Cisco AireOS/Catalyst] および [Cisco Meraki] を含むウィンドウが表示されます。

（注） 新しい Cisco DNA Spaces アカウントの場合、ボタン名は [Get Started] になります。

ステップ 3 ワイヤレスネットワークの [Select] をクリックします。

ワイヤレスネットワークに接続できるさまざまなメソッドが表示されます。

- [Cisco AireOS/Catalyst] の場合、次のメソッドの設定が可能です。
  - [Via Spaces Connector]：Cisco DNA Spaces コネクタを使用して Cisco DNA Spaces を シスコ ワイヤレス コントローラに接続します。
  - [Connect WLC directly]：シスコ ワイヤレス コントローラ ダイレクト コネクトを使用して、Cisco DNA Spaces を シスコ ワイヤレス コントローラに接続します。
  - [Connect via CMX Tethering]：Cisco CMX を使用して Cisco DNA Spaces をシスコ ワイヤレス コントローラに接続します。

- [Cisco Meraki] の場合、次のメソッドの設定が可能です。
  - [Connect via Meraki Login]：Cisco Meraki アカウントを使用して Cisco DNA Spaces を Cisco Meraki に接続します。
  - [Connect via API Key]：Cisco Meraki API キーを使用して Cisco DNA Spaces を Cisco Meraki に接続します。

ステップ 4 Cisco DNA Spaces に接続するメソッドの [Select] をクリックします。

選択したメソッド方法でワイヤレスネットワークに接続するための前提条件が表示されます。前提条件を満たしていることを確認します。

ステップ 5 [Customize Setup] をクリックします。

「設定が正常に保存されました」というメッセージが表示されます。

ステップ 6 選択したワイヤレスネットワークの設定メソッド法に対応するバーが、[Connect your wireless network] ウィンドウに表示されます。たとえば、[Via Spaces Connector] を選択すると、[Connect via Spaces Connector] バーが表示されます。

ステップ 7 手順を表示し、ワイヤレスネットワークを設定するには、バーの右端にあるドロップダウンボタンをクリックします。

対応するメソッドを使用して対応するネットワークに接続するための手順と機能が表示されます。

ステップ 8 指示に従って、ワイヤレスネットワークに追加します。

ワイヤレスネットワークバー

選択した接続方法に基づいて、Cisco AireOS に対して次のいずれかのバーが表示されます。

- [Connect via Spaces Connector]：Cisco DNA Spaces コネクタを使用して Cisco DNA Spaces をシスコ ワイヤレス コントローラに接続するための詳細な手順を表示します。ステップ 2 で提供される [Create a new token] オプションを使用して、コネクタを追加できます。ステップ 3 で提供される [Add Controllers] オプションを使用して、シスコ ワイヤレス コントローラを追加できます。次に、ステップ 4 の [Import Controllers] オプションを使用して、追加したシスコ ワイヤレス コントローラを Cisco DNA Spaces のロケーション階層にインポートできます。追加した Cisco DNA Spaces コネクタおよびシスコ ワイヤレス コントローラは、それぞれ [View Connectors] および [View Controllers] オプションを使用して表示できます。[View Location Hierarchy] オプションを使用して、ロケーション階層を表示できます。OpenRoaming アプリの場合、手順 2 で提供される [Add OpenRoaming Hotspot] オプションを使用してホットスポットを設定できます。また、手順 2 で提供される [OpenRoaming Controller Configuration] オプションを使用して、さまざまなコントローラの OpenRoaming アプリの設定を個別に表示することもできます。
- [Connect WLC/ Catalyst 9800 Directly]：Cisco Wireless Controller Direct Connect を使用して、Cisco DNA Spaces を Cisco AireOS ワイヤレスコントローラまたは Cisco Catalyst 9800 シリー

ズワイヤレスコントローラに接続するための詳細な手順を表示します。コントローラGUIからルート証明書をインストールできます。ステップ2で提供される[View Token]および[View Controllers]オプションを使用して、トークンとコントローラを表示できます。ステップ2を使用して、コントローラでトークンを設定することもできます。[Connect WLC/Catalyst 9800 Directly]と[Connect Via Spaces Connector]の下の[Setup]ウィンドウからマップを管理できるようになりました。次の新しいリンクを使用できます。

- [Import/Sync Maps]：Detect & Locate、Asset Tracker、およびIoTサービスとシームレスに連携するために、Cisco Prime InfrastructureまたはCisco DNA Centerマップをアップロードします。
- [Map Upload History]：アップロードされたマップのリストを表示します。ファイル名、ソースタイプ、ステータス、およびその他の関連情報を表示できます。
- [Manage Map]：[Map Service]アプリケーションに移動して、マップを管理します。

- [Connect via CMX Tethering]：トークンによるCMXテザリングを使用してCisco CMXノードのロケーションアップデートを設定するための詳細な手順を表示します。ステップ2で[Create New Token]オプションを使用してトークンを作成し、Cisco CMXで設定できます。

選択内容に応じて、Cisco Merakiの次のいずれかのタブが表示されます。

- [Connect via Meraki Login]：Merakiアカウントを使用してCisco DNA SpacesをCisco Merakiネットワークに接続する手順を表示します。.ステップ1で提供される[Connect]オプションを使用してCisco Merakiに接続できます。ステップ3の[Import Networks]オプションを使用して、Meraki組織とその子ロケーションをロケーション階層にインポートできます。
- [Connect via Meraki API Key]：Meraki APIキーを使用してCisco DNA SpacesをCisco Merakiネットワークに接続する手順を表示します。ステップ3の[Import Networks]オプションを使用して、Meraki組織とその子ロケーションをロケーション階層にインポートできます。

（注）

- [Connect via Meraki Login]または[Connect via Meraki API]を使用してMerakiに接続すると、[Enable Service Account]ウィンドウが表示され、[Continue with Service Account]オプションと[Continue without Service Account]オプションが表示されます。[Continue with Service Account]を選択すると、サービスアカウントに関する手順がMerakiの設定手順の一部として含まれます。
- Merakiと現在同期されているユーザー数が、[Connect your Meraki]オプション（[Connect via Meraki Login]および[Connect via Meraki API Key]）の下に表示されます。

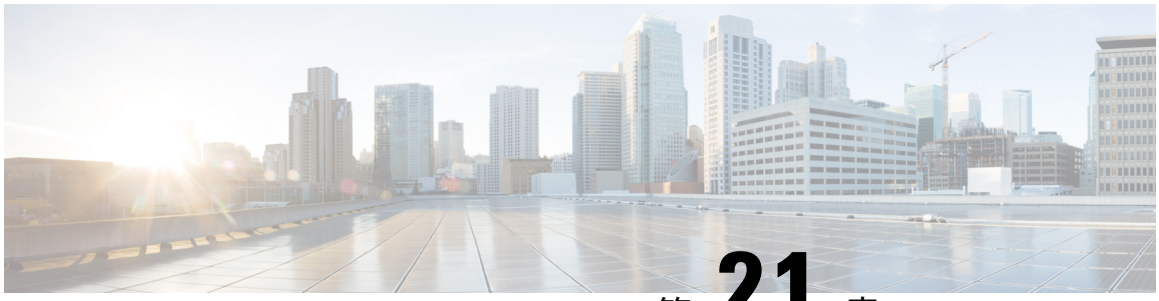
[View Configuration Steps]：特定のワイヤレスネットワークの資料にリダイレクトします。

[System Requirements]：Cisco DNA Spacesのシステム要件を提供します。

[Frequently asked questions]：Cisco DNA Spacesに関するよくある質問へのリンクを提供します。

[Cisco AireOS/Catalyst]：CMX ノード（CMX オンプレミス）を [Location Hierarchy] ウィンドウにインポートする手順を表示します。

[Cisco Meraki]：Meraki 組織を [Location Hierarchy] ウィンドウにインポートする手順を表示します。



第 21 章

マップサービスの設定

この章では、**マップサービス**で使用できる機能について説明します。

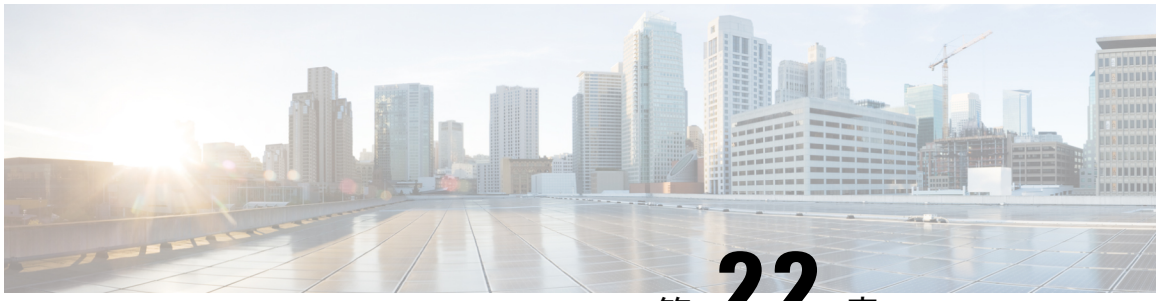
[Map Service] の設定

Cisco DNA Spaces の [Map Service] には、インポートされたマップデータと [Location Hierarchy] の同期を維持するための次の機能が含まれています。

- Cisco Prime Infrastructure または Cisco DNA Center からエクスポートされ、[Map Service] を使用して Cisco DNA Spaces にインポートされたマップは、[Location Hierarchy] に自動的に表示されます。
- [Location Hierarchy] からロケーションを削除すると、[Map Service] からも削除されます。
- AP インポート制限は、Cisco DNA Spaces アカウントの AP ライセンス制限に基づいて導入されています。

（注）

- ロケーションにマップがある場合は、マップベースのロケーション階層を作成します。ただし、[WLC Direct] > [AP prefix]、[CMX On-Prem Auto-Sync]、または [CMX Manual Upload] を使用してロケーション階層をすでに作成しており、重複する AP を含むマップをインポートしている場合、AP はマップベースの階層に移動されます。
- [Map Service] からロケーションを削除すると、対応するアクセスポイントのみが [Location Hierarchy] から削除されます。



第 22 章

Meraki カメラのセットアップ

この章では、Meraki カメラに関して Cisco DNA Spaces で必要な設定について説明します。

• Cisco Meraki カメラと連動するように Cisco DNA Spaces を設定する （327 ページ）

Cisco Meraki カメラと連動するように Cisco DNA Spaces を設定する

Cisco DNA Spaces を使用すると、Cisco Meraki カメラを使用してロケーションを訪れた訪問者の数を確認できます。この機能を利用するには、Meraki にログインできるようにし、ロケーションに Cisco Meraki カメラを設置しておく必要があります。Meraki カメラは、カメラが Meraki クラウドサーバーに到達可能であれば、既存の Cisco AireOS または Cisco Catalyst ネットワークに接続できます。さらに、有効な Meraki MV Sense ライセンスも必要です。

[Camera] 機能を使用して、次の詳細情報をキャプチャできます。

- ロケーションに入場した訪問者の総数。
- ロケーションを退場した訪問者の総数。
- ロケーションに現在滞在している訪問者の総数。

（注） 訪問者がトリップワイヤラインから出た後に再びトリップワイヤラインに入った場合、新たな入場は別の訪問としてカウントされます。

Cisco DNA Spaces ダッシュボードで利用可能な [Camera Metrics] アプリと [Right Now] アプリを使用して、訪問者数を表示できます。

Meraki カメラの設定

Meraki カメラを設定するには、次の手順を実行します。

ステップ 1 Cisco Meraki ダッシュボードで、必要な Meraki ネットワーク上のカメラを設定します。Meraki ネットワークでのカメラの設定に関する詳細については、「カメラの設定」を参照してください。

ステップ 2 Cisco Meraki サービスアカウントを設定します。Cisco Meraki サービスアカウントの設定に関する詳細については、Cisco Meraki サービスアカウントの設定 （299 ページ）を参照してください。

ステップ 3 Cisco DNA Spaces ダッシュボードで、ダッシュボードの左上に表示される 3 本線のメニューアイコンをクリックします。

ステップ 4 **[Setup]** > **[Camera]** を選択します。

[Connect your Camera] ウィンドウが表示されます。

ステップ 5 [Get Started] をクリックします。

（注） 以前に Cisco Meraki に接続したことがある場合は、使用した接続方法に対応するウィジェットが [Connect your Camera] ウィンドウに自動的に表示されます。このような場合、[Get Started] は表示されません。Meraki カメラの設定と同じ接続方法（ログイン、API キー）を使用して Cisco Meraki に接続する場合は、ステップ 4 からステップ 6 までをスキップできます。別の接続方法で接続する場合は、[Add New] を使用して対応するウィジェットを追加できます。両方の接続方法（ログインおよび API キー経由）にウィジェットを追加した場合、[Add New] は無効になります。

ステップ 6 [Select] をクリックして、Cisco Meraki を Cisco DNA Spaces に接続する方法を指定します。

選択した方法の前提条件がウィンドウに表示されます。接続方法の詳細については、さまざまなワイヤレスネットワークで動作する Cisco DNA Spaces の設定 （321 ページ）を参照してください。

ステップ 7 [Continue Setup] をクリックします。

[Connect your wireless network] ウィンドウに、カメラの接続を可能にするウィジェットが表示されます。

表示されるウィジェットは、ステップ 6 で選択した方法によって異なります。[Connect Via Meraki Login] メソッドの場合、表示されるウィジェットは [Meraki Camera for analytics via Meraki Login] になります。[Connect via API Key] メソッドの場合、表示されるウィジェットは [Meraki Camera for analytics via Meraki API Key] になります。

ステップ 8 展開されたウィジェットで、ステップ 1 で表示された [Connect] をクリックします。

同じ接続方法を使用して Cisco Meraki ネットワークにすでに接続している場合、ステップ 1 の指示は接続済みのメッセージに置き換えられ、[Connect] リンクは表示されません。そのような場合は、この手順をスキップできます。

a) [Meraki Camera for analytics via Meraki Login] ウィジェットの場合、ログイン用の電子メールとパスワードを入力するフィールドを含むウィンドウが表示されます。ログイン情報を入力して、[Submit] をクリックします。接続に成功すると、ステップ 1 の内容が「Connected as [接続に使用した電子メール]」というメッセージに置き換えられます。

b) [Meraki Camera for analytics via Meraki API Key] ウィジェットの場合、ウィンドウに [API Key] フィールドが表示されます。API キーを入力して、[Submit] をクリックします。接続に成功すると、ステップ 1 の内容が「Connected with [マスクされた API キー]」というメッセージに置き換えられます。

ステップ 9 [Connect your Meraki Camera] ウィンドウで、ステップ 2 で表示された [Import Networks] をクリックします。

カメラネットワークがすでにロケーション階層セクションにインポートされている場合は、ステップ 9 からステップ 13 までをスキップできます。

ステップ 10 [Import Networks] ウィンドウで、インポートする Meraki 組織（Meraki カメラネットワークが設定される組織）を選択します。

ステップ 11 [Choose Networks] エリアで、インポートする Meraki ネットワークのチェックボックスをオンにします。

ステップ 12 [Import] をクリックします。

インポートされた Meraki ネットワークとカメラの総数が表示されます。

ステップ 13 [Finish] をクリックします。

Cisco Meraki の Meraki カメラ設定が Cisco DNA Spaces と自動的に同期されるようになりました。通常、48 時間以内に自動設定されます。遅延が発生した場合は、次のステップで説明されているとおり、Cisco Meraki で MQTT サーバーの詳細を手動で設定します。

ステップ 14 Cisco Meraki で MQTT サーバーの詳細を手動で設定する場合は、次の手順を実行します。

MQTT サーバーのホストとポートはアカウント固有のもので、ステップ 3 で Cisco DNA Spaces の [Connect your Meraki Camera] ウィンドウに表示されます。こうした MQTT サーバーの詳細を Cisco Meraki で設定する必要があります。

a) Cisco Meraki ダッシュボードにログインします。
b) ダッシュボードの左ペインのメニューから、**[Cameras]** > **[Cameras]** を選択します。
c) [Name] フィールドで、MQTT サーバーを設定するカメラのリンクをクリックします。

選択したカメラの詳細が表示されます。カメラの [Video] タブがデフォルトで表示されます。

d) [Settings] タブをクリックし、[Sense] をクリックします。
e) [Sense API] の右側にある [Enabled] をクリックします。
f) [Add or Edit MQTT Brokers] リンクをクリックします。
g) [Edit MQTT Brokers] ウィンドウで、[New MQTT Broker] をクリックします。
h) 表示される [Edit MQTT Broker] ウィンドウで、MQTT サーバーの詳細を入力します。

ホストとポートは、ステップ 3 で [Connect your Meraki Camera] ウィンドウに表示されます。

i) [**保存（Save**）] をクリックします。

ステップ 15 カメラの入口/出口ラインを設定するには、ステップ 4 で [Connect your Meraki Camera] ウィンドウの [Draw Trip Wire] をクリックします。

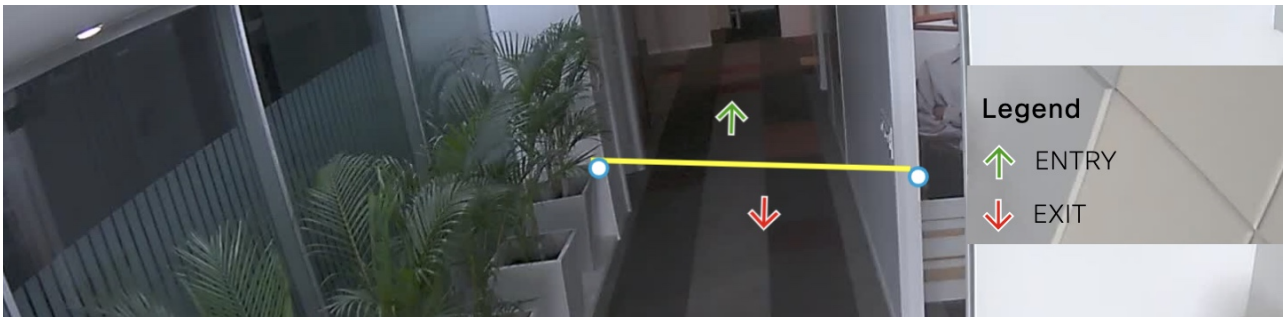
（注） 現在、カメラメトリックはロケーションレベルでのみ計算されます。メトリックが必要なロケーションへのすべての入口にカメラがあり、カメラごとにトリップワイヤが引かれていることを確認してください。正確さを確保するため、カメラは入口/出口ポイント全体がはっきりと見えるように入口の近くに配置する必要があります。トリップワイヤは、入口/出口ポイントで床から数フィート離れた位置に引く必要があります。ロケーションレベルの入口/出口ポイントではないロケーションにカメラのトリップワイヤを引かないでください。

ステップ 16 表示される [Draw Trip-Wire] ウィンドウで、[Select Locations] をクリックし、カメラが設定されているロケーションを選択して、[Done] をクリックします。

ステップ 17 [Select a camera you wish to draw the trip-wire] エリアで、トリップワイヤを設定するカメラのオプションボタンを選択し、[Next] をクリックします。

ステップ 18 カメラのプレビュー画像に [+] を使用して線を引き、トリップワイヤを作成します。

デフォルトでは、入口と出口の矢印はトリップワイヤの中央に表示されます。緑の矢印は入口を表し、赤い矢印は出口を表します。入口と出口の矢印が次の図に示す方向を指していることを確認します。矢印が適切に配置されていない場合は、トリップワイヤラインの端にある青い輪郭のドットをクリックしたままマウスをドラッグして、ラインと矢印を回転させます。



（注） トリップワイヤは、Meraki サービスアカウントが設定されている場合にのみ機能します。

ステップ 19 必ずライン両端のポイントをクリックして、XY 座標を設定するようにしてください。ライン両端のポイントをクリックすると、入り口と出口の矢印の XY 座標が [Trip-wire status] エリアに自動的に表示され、ステータスが [Set] に変更されます。デフォルトでは、ステータスは [Not Set] になります。

（注） ライン両端のポイントをクリックした場合にのみ、ステータスが [Set] に変更されます。

ステップ 20 [Finish] をクリックします。

Cisco DNA Spaces で使用できるようにカメラが設定されました。

次のタスク

Cisco DNA Spaces [Right Now] アプリは、Cisco Meraki でカメラゾーンを設定している場合、ゾーンレベルの滞在データもレポートします。各カメラのゾーンを定義するには、Cisco Meraki のドキュメントを参照してください。

カメラのトリップワイヤの編集

カメラのトリップワイヤの XY 座標を編集するには、次の手順を実行します。

ステップ 1 Cisco DNA Spaces ダッシュボードで、ダッシュボードの左上に表示される 3 本線のメニューアイコンをクリックします。

ステップ 2 **[Settings]** > **[Camera]** を選択します。

[Connect your Meraki Camera] ウィンドウが表示されます。

ステップ 3 [Connect your Meraki Camera] ウィンドウで、手順 4 で表示された [View Cameras] をクリックします。

Cisco DNA Spaces にインポートされたカメラが表示されます。フィルタリングして、特定のロケーションのカメラを表示できます。

ステップ 4 トリップワイヤを編集するカメラの右側に表示されている [Edit] アイコンをクリックします。

ステップ 5 表示される [Edit Trip Wire] ウィンドウで、トリップワイヤの詳細を編集し、[Done] をクリックします。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。