



Cisco Spaces コンフィギュレーション ガイド

最終更新：2026 年 5 月 28 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/>

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

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

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

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

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

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

© 2026 Cisco Systems, Inc. All rights reserved.



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。

このマニュアルの構成は、次のとおりです。

- [対象読者](#) (iii ページ)
- [表記法](#) (iii ページ)
- [略語の一覧](#) (iv ページ)
- [通信、サービス、およびその他の情報](#) (iv ページ)

対象読者

このガイドは、Cisco Spaces のユーザーアカウントを管理し、Cisco 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 Spaces を使用してプロキシミティールールを作成し、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を対象としています。

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。

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。

表記法	説明
[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
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

通信、サービス、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、[Cisco Profile Manager](#) でサインアップしてください。
- 重要な技術によりビジネスに必要な影響を与えるには、[Cisco Services](#) [英語] にアクセスしてください。
- サービスリクエストを送信するには、[Cisco Support](#) [英語] にアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、[Cisco DevNet](#) [英語] にアクセスしてください。

- 一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、[Cisco Press](#) [英語] にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、[Cisco Warranty Finder](#) にアクセスしてください。

シスコのバグ検索ツール

[シスコのバグ検索ツール](#) (BST) は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理するシスコバグ追跡システムへのゲートウェイです。BSTは、製品とソフトウェアに関する詳細な障害情報を提供します。

マニュアルに関するフィードバック

シスコの技術マニュアルに関するフィードバックを提供するには、それぞれのオンラインドキュメントの右側のペインにあるフィードバックフォームを使用してください。



第 Ⅰ 部

前提条件

- [Cisco DNA Spaces の前提条件](#) (1 ページ)



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 \(1 ページ\)](#)
- [Cisco DNA Spaces を展開するための帯域幅要件 \(2 ページ\)](#)
- [アクセス可能なポートと IP アドレス \(3 ページ\)](#)
- [Cisco Spaces IP アドレス \(3 ページ\)](#)

システム要件

Cisco Spaces のシステム要件を次の表に示します。

表 3: システム要件

項目	システム要件
オペレーティング システム	• Microsoft Windows XP またはそれ以降のバージョン • macOS X 10.6 以降のバージョン

項目	システム要件
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 macOS • 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
Cisco AireOS ワイヤレスコントローラ	8.3 以降のバージョン (注) 8.3はサポート終了（EOL）です。次の場所にある Cisco Wireless Software Release Product Bulletin のガイドラインに従って、推奨リリースのいずれかに移行することをお勧めします。 https://www.cisco.com/c/en/us/products/collateral/wireless/wireless-controllers/bulletin-c25-738147.html
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 以降のバージョン
Cisco 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:帯域幅の要件

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 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 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、顧客のインフラストラクチャでいくつかの Cisco 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 Spaces IP アドレス \(3 ページ\)](#) を参照してください。



(注) デフォルトの Cisco Unified Wireless Network インストールでは、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 Spaces と Cisco CMX へ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 Spaces レポートの表示

Cisco Spaces IP アドレス

Cisco AireOS または Cisco Catalyst 9800 シリーズ ワイヤレス コントローラと Cisco Spaces 間の接続を確立するには、使用するネットワークインフラストラクチャで一定の Cisco Spaces IP アドレスを許可する必要があります。



(注) Cisco 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。

顧客のネットワークに展開された Cisco CMX インスタンスが Cisco 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、顧客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 Spaces ダッシュボードで、[SSIDs] ウィンドウの [手動設定 (Configure Manually)] リンクをクリックします。

承認された IP アドレス

Cisco Spaces ドメインを変更または移行する際は、新しく提供された IP アドレスが承認済み IP アドレスリストに追加されていることを確認してください。これにより、これらの IP に関連付けられているすべてのシステム、ユーザー、およびサービスの Cisco Spaces サービスに中断なくアクセスできます。

オファァ/接続タイプ	追加			既存		
	ドメイン	IPv4	IPv6	ドメイン	IPv4	IPv6
CMXテザリング経由で接続	cmx.ciscospaces.io	75.2.50.127	~~2001:461:5a:403:2001:461:5a:403~~	cmx.dnaspaces.io	52.20.144.155	-
	cmx.ciscospaces.io	99.83.199.229	~~2001:461:5a:403:2001:461:5a:403~~	cmx.dnaspaces.io	34.231.154.95	-
Spaces コネクタ経由で接続	cmx.ciscospaces.io	75.2.50.127	~~2001:461:5a:403:2001:461:5a:403~~	cmx.dnaspaces.io	34.231.154.95	~~2001:461:5a:403:2001:461:5a:403~~
	cmx.ciscospaces.io	99.83.199.229	~~2001:461:5a:403:2001:461:5a:403~~	cmx.dnaspaces.io	52.20.144.155	~~2001:461:5a:403:2001:461:5a:403~~
AireOS コントローラ/Catalyst 9800 ワイヤレスコントローラを直接接続	data.ciscospaces.io	52.1.37.236	-	data.dnaspaces.io	34.231.154.95	-
	-	-	-	-	52.20.144.155	-
Partner Firehose	partner.ciscospaces.io	75.2.96.93	~~2001:461:5a:403:2001:461:5a:403~~	partner.dnaspaces.io	44.199.137.87	-
	partner.ciscospaces.io	99.83.155.204	~~2001:461:5a:403:2001:461:5a:403~~	partner.dnaspaces.io	3.90.124.39	-
キャプティブポータル	splash.ciscospaces.io	15.197.234.109	~~2001:461:5a:403:2001:461:5a:403~~	splash.dnaspaces.io	52.55.235.39	-
	splash.ciscospaces.io	3.33.232.255	~~2001:461:5a:403:2001:461:5a:403~~	splash.dnaspaces.io	34.235.248.212	-

Cisco Spaces コンフィギュレーションガイド



第 II 部

使用する前に

- [Cisco DNA Spaces を試してみる](#) (9 ページ)



第 2 章

Cisco DNA Spaces を試してみる

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 Spaces の概要 \(9 ページ\)](#)
- [シスコ フェデレーション プロセス, on page 10](#)
- [Cisco Customer Identity を使用した SSO のセットアップ, on page 13](#)
- [Cisco Spaces 用シングルサインオン \(15 ページ\)](#)
- [Cisco Spaces のアイドル タイムアウト \(17 ページ\)](#)
- [Cisco DNA Spaces ドキュメント \(17 ページ\)](#)

Cisco Spaces の概要

Cisco Spaces は、物理的なビジネス拠点にいる訪問者を把握し、訪問者とつながり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。

Cisco Spaces は、顧客が大規模なビジネス成果を達成できるようにする、業界で最も拡張性のあるエンドツーエンドの屋内ロケーション サービス クラウド プラットフォームです。包括的なサービススイートにより、すべてのロケーションベースのニーズに向けた強力なソリューションを提供します。

Cisco Spaces また、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。

次のようなさまざまな業種（分野）が対象です。

- 小売
- manufacturing
- サービス業
- ヘルスケア
- 教育 (Education)
- 金融サービス

- 企業ワークスペースなど。

Cisco Spacesを使用すると、ユーザーは、統合されたダッシュボードインターフェイスを介して、すべてのロケーションテクノロジーとインテリジェンスに一元からアクセスできます。既存の Cisco Aironet、Cisco Catalyst、および Cisco Meraki インフラストラクチャとの互換性を考慮して設計された Cisco Spaces は、ロケーションベースのサービスニーズに合わせた汎用性の高いソリューションとして優れています。

シスコ フェデレーション プロセス

シスコフェデレーションプロセスにより、外部パートナー組織とのシングルサインオン（SSO）統合が可能になります。これにより、セキュリティ境界を維持しながら、シームレスな認証が可能になります。このシステムでは、シスコの CCI-Okta インフラストラクチャを使用して、外部のアイデンティティ プロバイダー（IdP）とフェデレーションします。

主な利点

- **セキュリティの強化**：パスワードはパートナードメインから出ることではなく、シスコがパスワードにアクセスすることも、保存することはありません。
- **シームレスなユーザー体験**：シスコアプリケーション間でのシングルサインオン
- **ジャストインタイムプロビジョニング**：最小限の必要属性による自動ユーザープロビジョニング
- **フレキシブル認証フロー**：ユーザー認証のための複数のエントリポイント

Cisco Customer Identity の統合

Cisco Customer Identity（CCI）は、Cisco Spaces アプリケーション全体でユーザーのセキュリティとアクセス性を向上させる統合認証プラットフォームです。これは、個々のアプリケーション固有のアイデンティティ プロバイダー（IdP）を置き換える共通の認証レイヤとして機能し、ユーザーアクセスを合理化して、セキュリティ管理を向上させます。

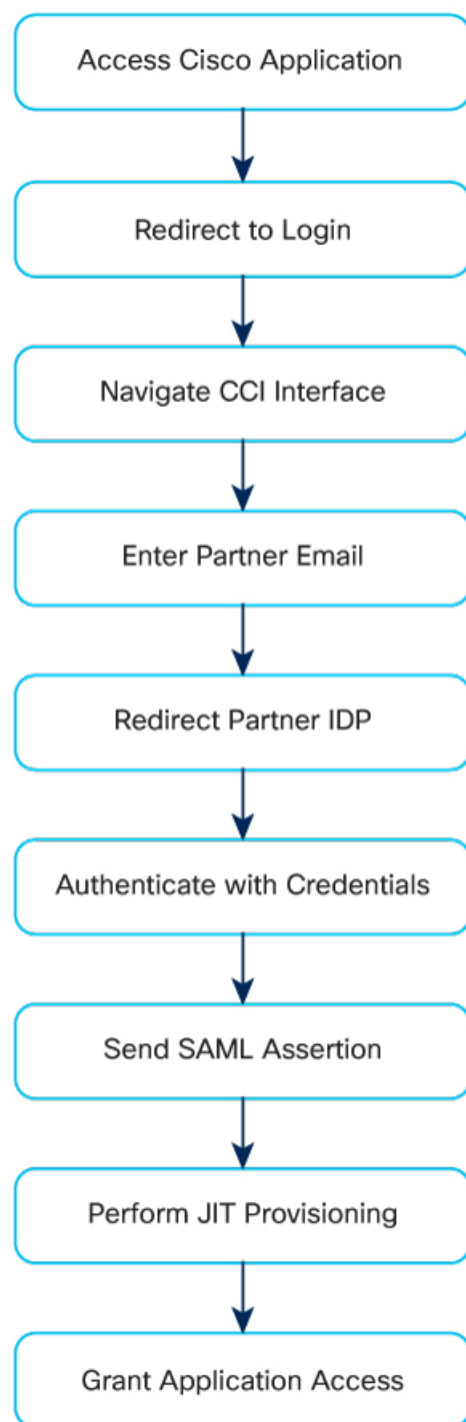
従来のオンボーディングでは、Cisco Spaces にさまざまな IdP が使用されていたため、他のアプリケーションを有効にするときに課題がありました。Cisco Customer Identity（CCI）には、CCI以外の顧客に対する将来の統合課題を回避するための共通の認証インターフェイスが用意されています。進化するシスコ製品エコシステムとの互換性を確保するには、ユーザーはCCI 統合への移行が求められます。

CCIの統合により、すべてのシスコアプリケーションのユーザー認証が一元化されるため、一貫したセキュリティポリシーが保証され、ユーザーの管理が簡素化されます。このアプローチは将来の拡張性をサポートし、認証を CCI に依存する追加のシスコ製品のシームレスなアクティビティ化を可能にします。

主要な属性：

- 承認された電子メールアドレスドメイン（@abc.com など）を持つユーザーに、すべてのシスコ URL でシングルサインオン（SSO）エクスペリエンスを提供します。

- レガシーまたは個々のアプリケーション IdP を置き換えて、フラグメンテーションと複雑さを回避します。
- 顧客の IdP とシスコの間でのメタデータ交換を使用した SAML ベースの認証をサポートします。
- SAML 応答には、firstName、lastName、email、company、countryCode などの必須ユーザー属性が必要です。
- 認証のみのワークフローと、認証と承認の複合ワークフローの両方を容易にします。

Figure 1: 認証ワークフロー

Cisco Customer Identity を使用した SSO のセットアップ

組織のアイデンティティ プロバイダーを Cisco Customer Identity (CCI) と統合することにより、指定されたドメインのユーザーに対してすべてのシスコアプリケーションでシングルサインオン (SSO) を有効にします。この統合認証により、ユーザー体験が向上し、アプリケーションセキュリティが強化されます。

シスコアプリケーションに一元化された認証が必要な場合は、このタスクを使用します。SSO のセットアップは、個々のアプリケーションレベルではなく、シスコドメインレベルで実行されるため、組織内のすべてのユーザーに一貫性のある安全なアクセスが提供されます。[シスコの SSO イネーブルメントチーム](#) と連携して、必要なメタデータと証明書を交換することにより、SSO が確実に機能し、組織のセキュリティ要件を満たします。

Before you begin

次の要件が満たされていることを確認します。

- **CCI-Okta** : シスコのアイデンティティプロバイダー
- **フェデレーション パートナー ドメイン** : 外部組織のアイデンティティ プロバイダー
- **保護対象アプリケーション** : 認証を必要とするシスコのアプリケーション
- **SAML プロトコル** : セキュア認証メッセージング

SSO を設定するには、次の手順を実行します。

Procedure

ステップ 1 ユーザーとして、次の詳細またはメタデータファイルを用意して、Cisco Spaces SSO イネーブルメントチームが SSO 統合できるようにします。

- **SubjectNameID** : キーアカウントリンク属性 (通常はユーザーの電子メール)。
- **リモート IDP 発行者の URI** : 顧客の IdP の SAML メタデータ EntityID。
- **リモート IDP シングルサインオン URL** : CCI から SAML 認証要求を受信するエンドポイント。
- **リモート IDP 署名証明書** : SAML 署名を検証するための公開キー証明書 (PEM または DER)。

ステップ 2 シスコから次の詳細情報が返ります。

- **Assertion Consumer サービス URI** : 認証後に SAML アサーションを受信するエンドポイント。
- **Audience URI** : IdP のシスコのエンティティ記述子。
- **SP 署名証明書** : 認証リクエストの署名を検証するための公開キー証明書。

ステップ 3 応答で、シスコに次の必須属性を提供します。

- firstName
- lastName
- email
- company (会社名)
- countryCode (US、UK、BE、JP などの 2 文字コード)

標準的なフェデレーションユーザージャーニー

1. 認証が必要なシスコアプリケーションに移動します。アプリケーションは CCI/Okta セキュリティレイヤによって保護されています。
2. ログインプロセスを開始するには、[ログイン (Login)] をクリックします。システムにより認証フローにリダイレクトされます。
3. [CCI ログイン (CCI Login)] ウィンドウに、パートナー組織のドメインに属する電子メールアドレス (username@PartnerDomain.com 形式) を入力します。この電子メールアドレスは、フェデレーションのセットアップで事前に設定されている必要があります。



Note システムにより、電子メールからパートナードメインが自動で検出され、組織のフェデレーション パートナー ドメイン ログインページ (ホーム組織のアイデンティティプロバイダー (IdP)) にリダイレクトされます。

4. 組織のログインページで、自分のユーザー名とパスワードを入力します。必ず組織のシステムに通常使用しているものと同じログイン情報を使用します。
5. 追加の認証要件 (MFA が設定されている場合) を完了します。



Note 認証に成功すると、自動で CCI にリダイレクトされます。組織の IdP は、セキュアな SAML アサーションを CCI に送信して、ユーザーのアイデンティティを確認します。

6. CCI により認証が処理され、元のシスコアプリケーションにリダイレクトされます。アプリケーションは認証ステータスの確認を受信します。
7. アクセスが許可され、認証が完了します。アプリケーションのトップページに正常にランディングされます。権限設定に基づいて、アプリケーションへのフルアクセスが利用できるようになりました。

Cisco Spaces 用シングル サインオン

Cisco 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 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 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 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 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 Spaces ダッシュボードに移動します。Cisco 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。

- 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** に設定した場合、以下が必要になります。

- 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。

- **role** の値は必須であり、ユーザーの詳細を送信するときに IDP で使用可能である必要があります。

- Cisco Spaces ダッシュボード > [管理者管理 (Admin Management)] から個々のユーザーを招待する必要はありません。ユーザー招待とアクティブ化は、特定の顧客 IDP および Cisco Spaces による認証プロセスと承認プロセスの両方に基づきます。

Cisco Spaces ダッシュボードの既存のデフォルトロールを使用するか、Cisco Spaces ダッシュボードで新しいロールを作成し、その特定のロール名を使用できます。

カスタムロールを使用する場合は、Cisco Spaces > [管理者管理 (Admin Management)] > [ロール (Roles)] でカスタムロールを作成し、IDP 応答で **role** 文字列値としてロール名を渡します。

- 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

- Entity ID

- 応答 URL (Assertion Consumer Service の URL と呼ばれます)

- 次の情報を含むシスコのメタデータファイル：

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 Spaces のアイドル タイムアウト

Cisco DNA Spaces ドキュメント

Cisco DNA Spaces 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。

[Spaces LaunchPad] セクションから、ドキュメント、発表、導入ガイド、ユースケース、サポート情報を表示することもできます。これを行うには、Cisco DNA Spaces UI の右下にある [Spaces LaunchPad] アイコンをクリックします。



第 III 部

Cisco Spaces Home

- [Cisco Spaces ダッシュボード](#) (21 ページ)
- [Cisco Spaces : アプリケーション](#) (27 ページ)
- [パートナーアプリの管理](#) (33 ページ)
- [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 (37 ページ)
- [Cisco DNA Spaces](#) を使用するための Cisco Meraki の設定 (45 ページ)



第 3 章

Cisco Spaces ダッシュボード

- [Cisco Spaces ナビゲーション](#) (21 ページ)
- [Cisco Spaces ダッシュボード](#) (21 ページ)
- [Cisco DNA Spaces の機能](#) (23 ページ)
- [ユーザー プロファイル](#) (25 ページ)
- [Cisco Spaces アカウント詳細の表示](#) (25 ページ)

Cisco Spaces ナビゲーション

Cisco Spaces ダッシュボードにログインすると、Cisco Spaces アプリケーションが Cisco Spaces [ホーム (Home)] ページに表示されます。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、[ロケーション階層 (Location Hierarchy)]、[モニター (Monitor)]、[管理者管理 (Admin Management)]、[セットアップ (Setup)] といった Cisco 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 Spaces** をクリックするか、3 本線メニューの [ホーム (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。アプリケーション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 Spaces アプリケーション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 Spaces** をクリックして、アプリケーションからホームページに移動できます。

Cisco Spaces ダッシュボード

Cisco Spaces ダッシュボードは Cisco Spaces アプリケーションのデフォルトのホームページです。Cisco Spaces GUI には、Magnetic 設計の実装が採用されています。Magnetic 設計は、固定されたヘッダーと折りたたみ可能な左側のナビゲーションウィンドウに従います。

Cisco Spaces にログインした後に、次の図に示すように [ホーム (Home)] ウィンドウが表示されます。

Cisco Spaces [ホーム (Home)] ウィンドウには、[ダッシュボード (Dashboard)] ドロップダウンリスト (左側のナビゲーションペイン) が含まれており、Cisco Spaces ライセンスごとに利用可能なアプリケーションを検索して表示できます。

[Dashboard] ドロップダウンリストを使用して、選択したアプリケーションを選択して移動します。Cisco Spaces [ホーム (Home)] ウィンドウに戻るには、ドロップダウンリストから [ダッシュボード (Dashboard)] オプションを選択します。

メニューバー

メニューバーの左側にある [Menu] アイコン () をクリックして、次のメニュー項目にアクセスします。

- 自宅 (Home)
- ロケーション階層
- 統合
- 設定
- モニター
- 管理者管理
- IoT サービス
- 設定

アイコン

一般的なタスクを実行するには、メニューバーの右側にあるアイコンをクリックします。

アイコン	説明
	[Support] : ヘルプセンター、サポート、およびドキュメントのリンクを表示します。
	詳細については、 ユーザープロフィール (25 ページ) を参照してください。

Cisco Spaces : コネクタ 3.0

Cisco Spaces : コネクタ (このドキュメントで以降は単にコネクタと表記) は、シスコ ワイヤレスコントローラやデータ用のスイッチなどのさまざまなネットワークデバイスに接続する複数のサービスを効率的に管理する機能を備えた完全に再設計されたバージョンのコネクタです。コネクタプラットフォームを使用すると、クラウドに新しいサービスを簡単に追加/削除できます。クラウドからのデバッグ、ログのアップロード、および再起動機能により、高度なトラブルシューティングが可能になります。コネクタは、CPU、メモリ、接続、およびアップ/ダウンステータスを含む各サービスの詳細なメトリックも提供します。

コネクタは Cisco Spaces の次世代コネクタであり、拡張されたユーザーエクスペリエンス、複数のサービスをサポートするアーキテクチャ、シンプルさ、モジュール性、シームレスなアップグレード、およびハイアベイラビリティを提供します。コネクタは、アクティブ/アクティブ高可用性セットアップをサポートします。コネクタ 2.x の以前のリリースとは異なり、高可用性ペアを具体的に設定および監視できます。すべてのサービスとデバイス構成はコネクタレベルで管理されるため、高可用性と簡単にペアリングできます。

コネクタとデバイスのステータスも、各インスタンスからコネクタレベルで集計されるため、簡単に監視できます。コネクタは、高可用性ペアの各インスタンスに完全な可視性を提供します。各インスタンスでのサービスの実行状況、アップグレードステータスなどを表示できます。サービスの再起動など、特定のインスタンスでアクションを実行することもできます。

Cisco DNA Spaces の機能

Cisco DNA Spaces ダッシュボードの主な機能は次のとおりです。

Cisco Spaces アプリケーション

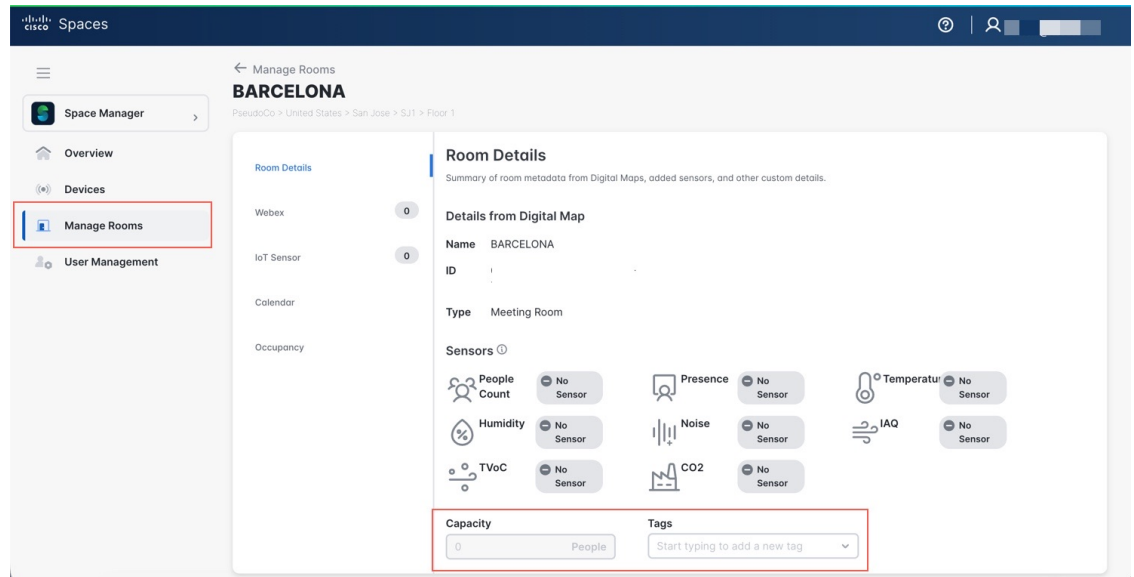
Cisco Spaces [ホーム (Home)] ページでは、使用可能なすべてのアプリケーションを表示できます。左側のナビゲーション ウィンドウで、[ダッシュボード (Dashboard)] をクリックします。

[ホーム (Home)] ページでは、アプリケーションがユースケース別にグループ化されています。[検索 (Search)] フィールドを使用して、アプリケーションや機能を検索します。

Space Manager (スペースマネージャ) アプリケーション

スペースマネージャ (Space Manager) アプリケーションで、[スペース管理 (Space Management)] タブの名前が [部屋の管理 (Manage Rooms)] に変更されます。すべての機能は同じままです。新しい **エクスポート** 機能を使用して、部屋の詳細を CSV ファイルとしてダウンロードできます。選択した部屋について、[キャパシティ (Capacity)] および [タグ (Tag)] のメタデータを部屋の詳細に追加して、追加情報を確認できます。これらの変更は、部屋をより効率的に管理できるように設計されています。

図 2: 部屋の管理



ロケーション階層

統合

統合機能を使用すると、Catalyst Center、Office 365、Google カレンダーなど、さまざまなシステムおよびサードパーティアプリケーションと Cisco Spaces を統合できます。この統合により、占有率、スペースの使用状況、およびアクセスデータの共有が可能になり、会議室の予約が同期されます。これにより、Spaces 展開の価値と効率を最大化できます。

設定

設定機能オプションを使用すると、Cisco Spaces でのロケーションコンピューと通知を設定できます。

モニター

モニター（**Monitor**）機能では、Cisco Spaces とそのアプリケーション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。

管理者管理

管理者管理機能を使用すると、Cisco 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。

設定

無線ネットワーク

ワイヤレス ネットワーク

さまざまな方法で Cisco 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 Spaces の設定」を参照してください。

ワイヤレス ネットワーク ステータス

[Wireless Network Status] 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。

ユーザー プロファイル

前回のログインとタイムスタンプの詳細を表示できます。[履歴の表示 (View History)] をクリックして、最近および失敗したログイン試行を表示します。

ユーザープロフィール機能には次のオプションがあります。

- **マイアカウント (My Account)** : クリックして、[マイアカウント (My Account)] ウィンドウを表示します。詳細については、[Cisco Spaces アカウント詳細の表示 \(25 ページ\)](#) を参照してください。
- **変更ログの表示 (View Change Log)** : クリックすると、特定のアカウントの全ユーザーに関するアクティビティの詳細を表示する [変更ログ (Change Log)] タブが [マイアカウント (My Account)] ウィンドウで開きます。詳細については、[Cisco Spaces アカウント詳細の表示 \(25 ページ\)](#) を参照してください。

Cisco Spaces アカウント詳細の表示

[マイアカウント (My Account)] ウィンドウを使用して、Cisco Spaces プロファイルの詳細、アカウントアクティビティ、およびその他のアカウント関連情報を表示します。[マイアカウント (My Account)] ウィンドウには、次のタブがあります。

- **マイプロフィール (My Profile)** : 名、姓、電子メール、携帯電話番号などの基本的なプロフィール情報を表示します。
- **アカウントアクティビティ (Account Activity)** : アカウントアクティビティが失敗した IP アドレス、日付、ブラウザなど、失敗したアカウントアクティビティの詳細を表示します。
- **設定 (Preferences)** : このタブには、次のオプションが含まれています。

- **新しいドメインの追加 (Add new domain)** : クリックして、SSO 認証用の新しいドメインを追加します。
- **サポートアクセスの有効化 (Enable Support Access)** : このオプションをクリックして、Cisco Spaces サポートチームに対してアカウントへのアクセスを有効または無効にすることができます。このオプションを有効にすると、Cisco Spaces サポートチームが例外的な状況で問題を検出してデバッグするために役立ちます。



(注)

- デフォルトでは、[Enable Support Access] オプションが有効になっています。
- アクセスが有効になると、Cisco Spaces サポートチームは顧客の Cisco Spaces アカウントにアクセスできるようになります。

- **変更ログ (Change Log)** : ユーザーアクティビティ、時間、アプリケーション、セッション、ユーザーなど、変更ログの詳細を表示します。ログの詳細をフィルタ処理するには、[フィルタ (Filter)] オプションをクリックします。

Cisco Spaces の新しい UI では、**変更ログの表示 (View Change Log)** 機能 ([ホーム (Home)] > [プロフィール (Profile)]) を使用して、**ロケーションとマップアプリケーション**と**スペースの使用状況アプリケーション**の監査証跡アクティビティを追跡します。



第 4 章

Cisco Spaces : アプリケーション

Cisco Spaces はさまざまなユースケース指向アプリケーションを提供します。パートナーアプリケーションを Cisco Spaces に追加することもできます。

- [Cisco Spaces アプリケーション \(27 ページ\)](#)
- [機能, on page 28](#)
- [パートナーアプリ \(30 ページ\)](#)
- [IoT Device Marketplace アプリケーション \(30 ページ\)](#)

Cisco Spaces アプリケーション

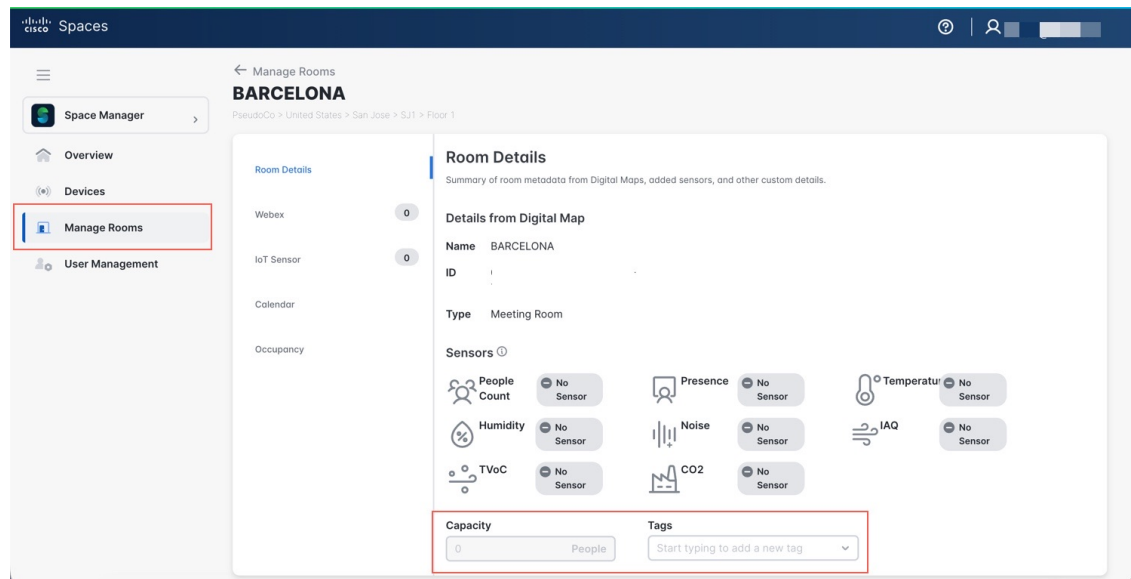
Cisco Spaces [ホーム (Home)] ページでは、使用可能なすべてのアプリケーションを表示できます。左側のナビゲーション ウィンドウで、[ダッシュボード (Dashboard)] をクリックします。

[ホーム (Home)] ページでは、アプリケーションがユースケース別にグループ化されています。[検索 (Search)] フィールドを使用して、アプリケーションや機能を検索します。

Space Manager (スペースマネージャ) アプリケーション

スペースマネージャ (**Space Manager**) アプリケーションで、[スペース管理 (Space Management)] タブの名前が [部屋の管理 (Manage Rooms)] に変更されます。すべての機能は同じままです。新しい **エクスポート** 機能を使用して、部屋の詳細を CSV ファイルとしてダウンロードできます。選択した部屋について、[キャパシティ (Capacity)] および[タグ (Tag)] のメタデータを部屋の詳細に追加して、追加情報を確認できます。これらの変更は、部屋をより効率的に管理できるように設計されています。

図 3: 部屋の管理



機能

使用可能なアプリケーションは次のとおりです。

- Space Manager (スペースマネージャ) :** **Space Manager**アプリケーションでは、さまざまなデバイス、センサー、およびワークスペースを設定でき、特定の建物、フロア、または会議室のリッチマップにレンダリングされた、リアルタイムの稼働率データおよび環境テレメトリ（ヒートマップ、室内の電波品質、気温、湿度、およびノイズレベル）にアクセスできます。
- Space Experience (スペースエクスペリエンス) :** **Space Experience**アプリケーションでは、**Cisco Smart Workspaces**のサイネージを作成して管理し、**Cisco Webex** デバイスまたは非 **Webex** デバイスの新しいサイネージをオンボードして、テレメトリパラメータを設定して、サイネージを公開できます。
- Space Utilization (スペースの使用状況) :** **Space Utilization**アプリケーションは、これまでの物理スペースの使用状況に関する洞察を提供し、物理スペースの使用を効果的に最適化するのに役立ちます。これらの洞察は、ネットワークと **Wi-Fi** インフラストラクチャに統合されたセンサーを通じて収集されたデータから得られるものです。
 詳細については、『[Cisco Spaces: Space Utilization App Guide](#)』[英語]を参照してください。
- 現在の状況 (Right Now) :** **Right Now** アプリケーションは、自分が現在いるロケーションの訪問者の詳細を示す **Right Now** ポートを提供します。**Right Now** アプリケーションを使用して、**密度ルール**を作成することもできます。**密度ルール**を使用して、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することもできます。

- **ロケーション分析 (Location Analytics)** : **Location Analytics** アプリケーションを使用すると、対象ロケーションの訪問者のレポートを表示できます。
- **検出と特定 (Detect and Locate)** : Cisco Spaces : **Detect and Locate** アプリケーションは、展開における 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トルに表示されます。**Detect and Locate** アプリケーションの詳細については、『[Cisco Spaces Detect and Locate Configuration Guide](#)』を参照してください。
- **Asset Locator (アセットロケータ)** : **Asset Locator** アプリケーションにより、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。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** アプリケーションの詳細については、『[Cisco Spaces Asset Locator コンフィギュレーションガイド](#)』を参照してください。
- **IoT Explorer (IoTエクスプローラ)** Cisco Spaces : **IoT** サービスは、Cisco Spaces 内のプラットフォームサービスで、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 デバイスを登録、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 Spaces IoT Services Configuration Guide](#)』を参照してください。
- **Captive Portals (キャプティブポータル)** : **Captive Portal** アプリケーションを使用すると、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。
- **Engagements (エンゲージメント)** : **Engagements** アプリケーションを使用すると、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。
- **Location Personas (ロケーションペルソナ)** : Cisco 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。**Location Personas** アプリケーションを使用すると、既存のタグに別の顧客を追加したり、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。

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ー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。ウェルカムメッセージ、通知、プロモーション、アプリケーション、ビデオ、ヘルプラインなど、ユーザー体験を向上させるための一連のカスタマイズオプションが用意されています。これらの機能は、Cisco Spaces で利用可能なさまざまなポータルモジュールを使用して実装できます。

キャプティブポータルルール

Cisco 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。

エンゲージメントアプリ

Cisco 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。**Engagement Rule**（エンゲージメントルール）アプリケーションを使用して通知を送信するように設定できます。Cisco 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 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

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ун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 Marketplace <https://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。



第 5 章

パートナーアプリの管理

- [App Center の概要](#) (33 ページ)
- [アプリを有効にする](#) (34 ページ)

App Center の概要

Cisco Spaces - パートナーダッシュボードは、Cisco Spaces パートナーに、アプリケーションを表示、更新、追加、およびテストするための単一の場所を提供します。Cisco Spaces は Cisco Spaces - パートナー アプリケーションセンターとシームレスに統合されています。パートナーは、アクセスポイントが収集する位置データにアクセスし、このデータを使用してビジネスアプリを拡張できます。Cisco Spaces - パートナーダッシュボードにログインして、アプリケーションを作成し統合します。



(注) この機能は、Cisco Spaces Extend ライセンスでのみ使用できます。

Cisco Spaces プラットフォームとパートナー主導のエコシステムの組み合わせにより、サードパーティのアプリケーション開発者と連携し、Cisco Spaces と Cisco Spaces - Partner Firehose API の力を活用して、個々の企業や顧客向けにカスタマイズされたアプリケーションを構築することができます。

アプリケーション開発者は、パートナー API (Cisco Spaces - Partner Firehose API) を使用して、アプリケーションを作成して公開します。パートナーエコシステムにより、独立系ソフトウェアベンダーは、分野に関連した、事前検証済みで、テスト済みのロケーションベースのソリューションアプリケーションを実現して、Cisco Spaces - パートナー アプリケーションセンターでライブアプリケーションを公開できます。登録済みパートナーとして、Cisco Spaces - パートナー アプリケーションセンターにアクセスできます。

顧客は、Cisco Spaces - パートナー アプリケーションセンターからアプリケーションを表示してアクティブ化できます。たとえば、顧客は Cisco Spaces - パートナー アプリケーションセンターから利用可能なアプリケーションをクリックし、ビジネスユースケースのためにアプリケーションをアクティブ化することを選択できます。アプリケーションが承認され、Cisco Spaces - パートナー アプリケーションセンターでライブになると、Cisco Spaces のすべての顧

客からアクティブ化のために利用できるようになります。顧客がアプリケーションをアクティブ化すると、顧客のデータが Cisco Spaces - Partner Firehose API 経由のイベントとしてアプリケーションに流れ始めます。

パートナーアプリケーション管理の詳細については、「[Cisco Spaces の概要 - パートナーエコシステム](#)」のオンラインヘルプを参照してください。

アプリを有効にする

Cisco Spaces パートナーはパートナーダッシュボードを使用してアプリケーションを作成および公開します。顧客アプリケーションを作成して公開すると、それらのアプリケーションは Cisco Spaces - パートナーダッシュボードに表示されます。Cisco Spaces 管理者は新しいアプリケーションを承認する必要がある、アプリケーションが承認されると、そのアプリケーションは Cisco Spaces - ダッシュボードの [アプリケーションセンター (App Center)] に表示されます。

顧客が使用できるようにするには、[App Center] からアプリをアクティブ化する必要があります。これらのアプリは、顧客の要件に応じて、選択した場所でアクティブ化できます。アプリには複数のイベントが含まれていて、パートナーはこれらのアプリのイベントを有効にしてアクティブにします。

イベントは、Firehose API を介してトリガーされます。これらの API がデバイスのステータスをチェックしてから、イベントが適切にトリガーされます。詳細については、『[Firehose API](#)』を参照してください。

Cisco Spaces パートナーがすでにアクティブ化されているアプリケーションに新しいイベントを追加すると、顧客がアクセス許可を受け入れて新しいイベントにサブスクライブした場合にのみ、Firehose API を介して送信されます。この機能強化の前は、新しいイベントに顧客の許可は必要ありませんでした。

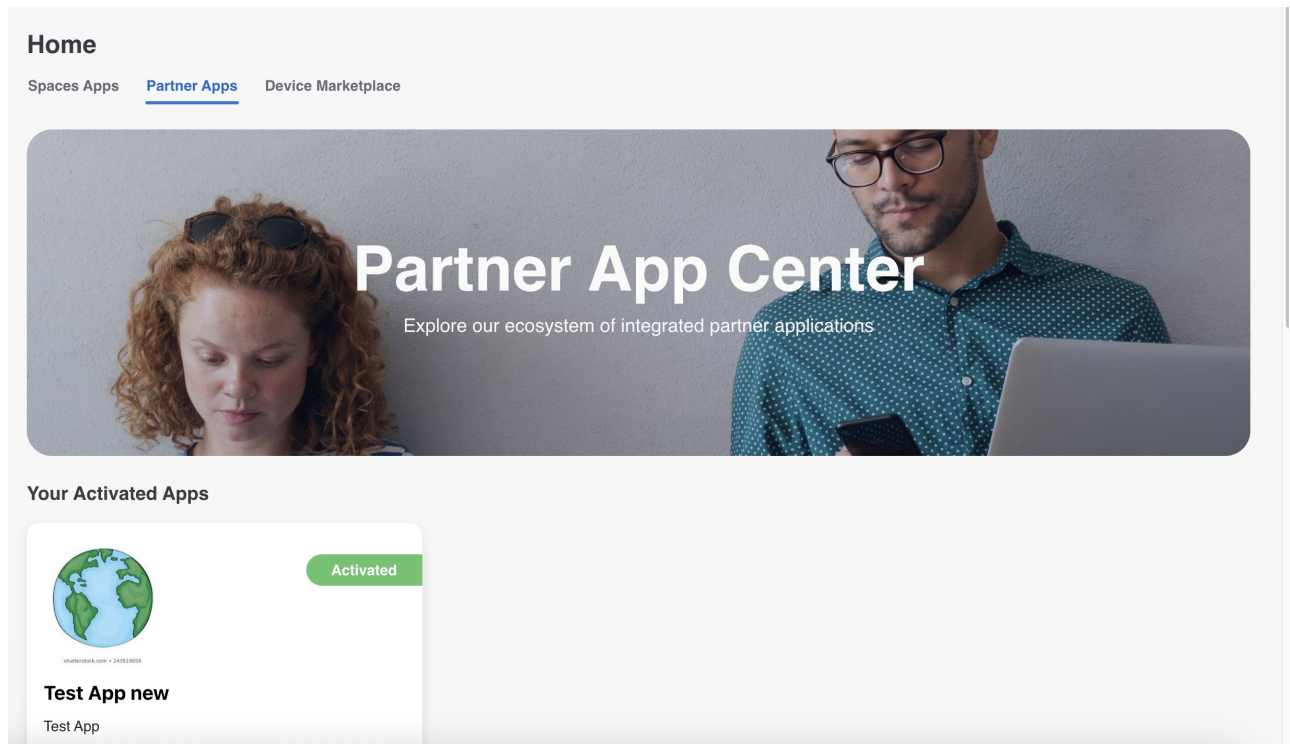
アプリタイトルに [New Permission Required] 通知メッセージが表示されます。これらの新しいアプリイベントにサブスクライブするには、新しいアプリのアクセス許可をクリックして同意する必要があります。新しいイベントがアプリに追加されたことを示す電子メール通知も顧客に送信されます。

手順

ステップ 1 Cisco Spaces ダッシュボードで [アプリケーションセンター (App Center)] をクリックします。

[App Center] ウィンドウに、公開されたアプリが表示されます。アプリのタイトルには、アプリケーションの名前、簡単な説明、およびアプリが [Cloud] または [On-prem] のどちらでホストされているかが表示されます。

図 4 : App Center



- ステップ 2** (オプション) [Filter By] セクションのオプションを使用して、アプリケーションをフィルタします。
- ステップ 3** アクティベートするアプリをクリックします。
- ステップ 4** [Activate] をクリックします。
- 対応するアプリのアクティベーションウィンドウが表示されます。各アプリケーションには、顧客の認証設定によって異なるアクティベーション手順があります。
- ステップ 5** [Sign Up & Onboarding] の設定を完了します。
- ステップ 6** [Continue] をクリックします。
- ステップ 7** [Permissions] セクションで、位置データの要件を読みます。
- ステップ 8** [Accept Permission] をクリックします。
- ステップ 9** アプリをアクティベートしたいロケーションを選択してください。[Enable for all locations] チェックボックスをオンにして、すべての場所を選択できます。
- ステップ 10** [次へ (Next)] をクリックします。
- 特定の顧客の Web サイトが表示され、続行するには、必要な顧客認証を完了する必要があります。
- ステップ 11** 画面の指示に従って、アプリのアクティベーションを完了します。



第 6 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。

- [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 \(38 ページ\)](#)
- [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 \(40 ページ\)](#)
- [Cisco DNA Spaces 拡張ベンチマーク \(44 ページ\)](#)

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

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。

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。

手順

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 [セキュリティ (Security)] > [アクセス制御リスト (Access Control Lists)] > [アクセス制御リスト (Access Control Lists)] を選択します。

ステップ 3 表示される [アクセス制御リスト (Access Control List)] ウィンドウで、Cisco 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	許可	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	TCP	HTTPS	任意	任意	任意
2	許可	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	TCP	任意	HTTPS	任意	任意

(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。

- シスコ ワイヤレス コントローラ ダッシュボードで、[セキュリティ (Security)] > [アクセス制御リスト (Access Control Lists)] を選択します。
- Cisco Spaces 用に設定されたアクセス制御リストの [追加アクション (More Actions)] をクリックします。
- [Add Remove URL] をクリックします。
- ソーシャル URL 名を入力し、[Add] をクリックします。
- 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 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。

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

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 Spaces 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はありません。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 を使用して Cisco Spaces をシスコ ワイヤレス コントローラに接続する

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 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 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 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 で Cisco 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 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 で Cisco Spaces クラウドに到達できる必要があります。ただし、Cisco 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 AireOS ワイヤレス コントローラ バージョン 8.3 以降を Cisco 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。

手順

ステップ 1 DigiCert CA ルート証明書をインポートします。

- 次のリンクからルート証明書をダウンロードします。

<https://cacerts.digicert.com/DigiCertGlobalRootCA.crt.pem>

- 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。
- {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。
- 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
```

- y** を入力してアップロードを開始します。
- 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 の発行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 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 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 Spaces ダッシュボードで、[ワイヤレスネットワークの追加（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 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

IP Address..... <Local System IP Address>

Connectivity..... https: UP

Service Status Active

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 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。Map Service 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。

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 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 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 Spaces を **WLC Direct Connect** または **Cisco Spaces コネクタ** と共に使用している場合、コントローラは「**Foreign controller**」モードである必要があります。

Cisco DNA Spaces 拡張ベンチマーク

表 5: 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 7 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](#) での SSID の有効化 (45 ページ)
- [RADIUS 認証用の Cisco Meraki](#) の設定 (46 ページ)
- [通知およびレポート用 Cisco Meraki](#) の設定 (48 ページ)
- [ソーシャル認証のための Cisco Meraki](#) の設定 (49 ページ)
- [Cisco Meraki](#) の SSID の手動設定 (50 ページ)
- [Cisco Meraki](#) でのスキャン API の設定 (51 ページ)
- [Bluetooth Low Energy デバイスサポート](#) (52 ページ)

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。

手順

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。

手順

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。

(注)

キャプティブポータルでは、RADIUS アカウンティングの有効化は必須ではありません。アカウンティングの該当するユースケースは、OpenRoaming と認可変更 (CoA) です。

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。

手順

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。

(注)

キャプティブポータルでは、RADIUS アカウンティングの有効化は必須ではありません。アカウンティングの該当するユースケースは、OpenRoaming と認可変更 (CoA) です。

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。

手順

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。

手順

ステップ 1 Cisco Meraki ダッシュボードで、[ワイヤレス (Wireless)] > [設定 (Configure)] > [アクセス制御 (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 [ウォールガーデン範囲 (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、[変更を保存 (Save Changes)] をクリックします。

Cisco Meraki のソーシャル認証が正常に設定されます。

表 6: ソーシャル ネットワークのドメイン名

Facebook	Twitter	LinkedIn	
*.facebook.com	*.twitter.com	*.linkedin.com	
*.fbcdn.net	*.twimg.com	*.licdn.net	
*.akamaihd.net		*.licdn.com	
*.connect.facebook.net			

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。

手順

- 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、必要なウォールガーデンの範囲を入力します。
ウォールガーデンの範囲を表示するには、Cisco 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 Spaces にインポートします。

Cisco 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。

手順

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。

Bluetooth Low Energy デバイスサポート

Bluetooth Low Energy (BLE) デバイスは、Cisco Catalyst ワイヤレスネットワークでサポートされていましたが、Cisco Meraki ネットワークで使えるようになりました。

この機能拡張により、Cisco Spaces プラットフォームは Cisco Meraki を使用して BLE デバイスとシームレスに統合できます。この機能拡張により、Cisco Meraki BLE デバイスは、Firehose IoT テレメトリイベント、IoT Explorer、サイネージ、RightNow など、さまざまな Cisco Spaces アプリケーションでアクセスできるようになりました。



(注) この機能を動作させるには、Cisco Meraki ネットワークで特定の設定を実行し、Cisco Spaces へのデータ送信を有効にする必要があります。さらにサポートが必要な場合は、[Cisco Spaces サポートチーム](#) にお問い合わせください。



第 **IV** 部

Cisco Spaces : アプリケーション

- Cisco Spaces : 行動メトリクスアプリケーション (55 ページ)
- Cisco Spaces : ライブ占有率 アプリケーション (67 ページ)
- Cisco Spaces : Camera Metrics (カメラメトリクス) アプリケーション (73 ページ)
- Cisco Spaces : オープンローミング (OpenRoaming) アプリケーション (77 ページ)
- Cisco Spaces : ロケーション分析アプリケーション (79 ページ)
- Cisco Spaces : 影響分析アプリケーション (93 ページ)
- Cisco Spaces : スペースの使用状況アプリケーション (97 ページ)
- Cisco Spaces: Smart Workspaces アプリケーション (99 ページ)
- Cisco Spaces : 環境分析アプリケーション (101 ページ)
- Cisco Spaces : Asset Locator アプリケーション (103 ページ)
- Cisco Spaces : IoT Explorer アプリケーション (105 ページ)
- Cisco Spaces : キャプティブポータルアプリケーション (111 ページ)
- Cisco Spaces : Engagements (エンゲージメント) アプリケーション (219 ページ)
- Cisco Spaces : ロケーションペルソナアプリケーション (243 ページ)



第 8 章

Cisco Spaces : 行動メトリクスアプリケーション

この章では、行動メトリクス（Behavior Metrics）アプリケーションとレポートについて説明します。

- [行動メトリクスの概要（55 ページ）](#)
- [行動メトリクスレポートの表示（56 ページ）](#)
- [ベンチマーク（57 ページ）](#)
- [\[Report\] タブ（58 ページ）](#)
- [行動メトリクス（ビジネスメトリクス）（59 ページ）](#)
- [\[Workspaces\] 分野（行動メトリクス）（62 ページ）](#)
- [\[Education\] 分野（行動メトリクス）（64 ページ）](#)
- [ロケーションのピン留め（66 ページ）](#)

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 ヶ月かかります。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ると、通知が送信されます。



(注) 行動メトリクスが機能強化され、[Sub Vertical] レベルのベンチマーク指標が表示されるようになりました。これは、副業種が定義されているカテゴリ平均メトリックとアカウントに適用されます。

副業種が定義されていない場合、カテゴリの平均指標は業種の階層レベルのベンチマークに基づいて計算されます。

行動メトリクスレポートの表示

行動メトリクスアプリケーションで、チャートデータを表示するには、各ロケーションレベルで100回以上の訪問が必要です。そのため、訪問データが多いロケーションのみがチャートでの可視化の対象になります。

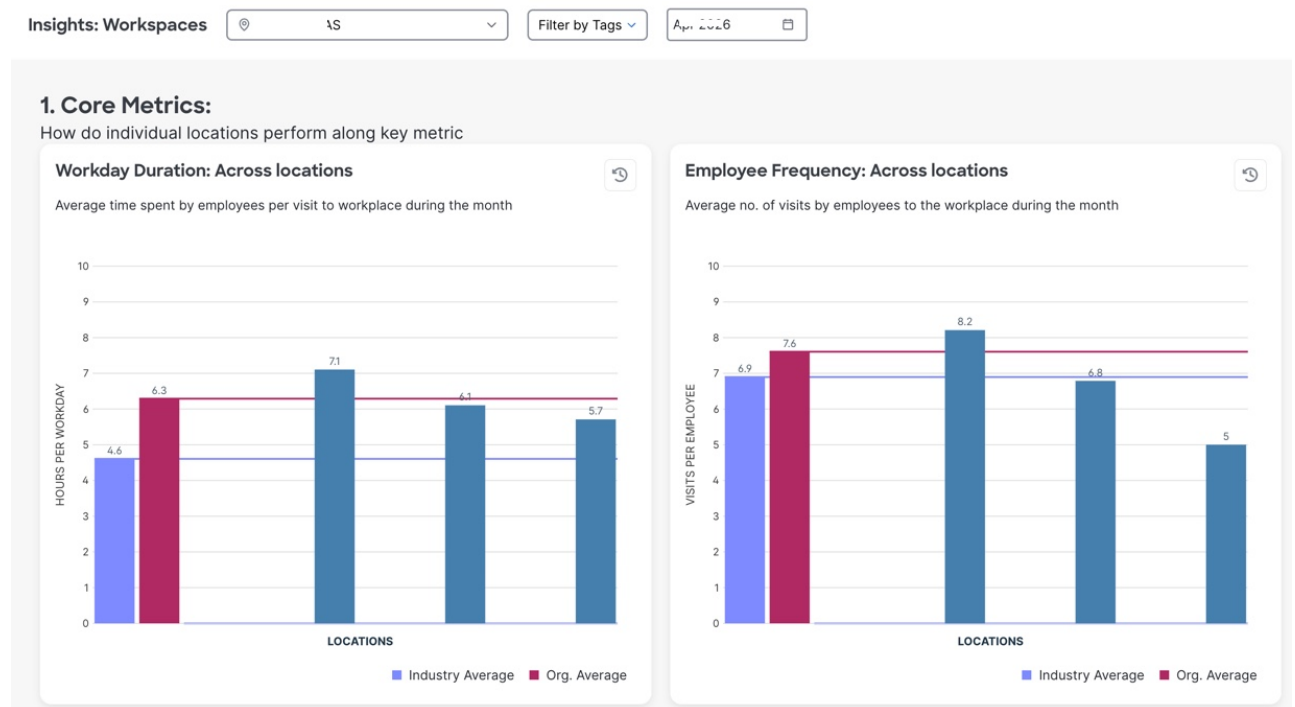
行動メトリクスアプリのさまざまなレポートを表示するには、次の手順を実行します。

手順

ステップ 1 Cisco Spaces ダッシュボードで、[行動メトリクス (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 5: 行動メトリクスレポート



ステップ2 ウィンドウ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。

(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、[行動メトリクス (Behavior Metrics)] ウィンドウの上部に、[小売業 (Retail)] というタイトルが[行動メトリクス (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。その他の事業の場合は、[Generic] が表示されます。

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、**Visit Duration Distribution (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 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、[Average Visit Duration (平均訪問時間)] グラフで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。さらに、米国の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、**Average Visit Duration (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。一部のレポートでは、州のタグを選択すると、2つのバーが追加で表示されます。1つのバーは州名とともに平均値を表示し、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、**Average Visit Duration (平均訪問時間)** 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。[Average Visit Duration] などの一部のグラフでは、ブランドを選択すると、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 Francisco」がフィルタリングされている場合、Cisco San Francisco の「平均訪問時間」が組織の平均とともに表示されます。さらに、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。

重要ロケーション (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。

- [Group] 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 ヶ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 ヶ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、履歴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）（62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示す折れ線グラフが表示されます。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。さらに、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。さらに、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示す折れ線グラフが表示されます。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。さらに、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。さらに、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

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。さらに、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

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。さらに、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（リピーター訪問者による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。

このグラフでは、グラフの青いドットは、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ター訪問数に与える影響を特定できます。

このグラフでは、グラフの青いドットは、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、小売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。

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。

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。この情報はロケーションビューで表示されます。
- [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。この情報はロケーションビューで表示されます。

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。この情報はロケーションビューで表示されます。
- [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。この情報はロケーションビューで表示されます。

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。この情報はロケーションビューで表示されます。
- [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。この情報はロケーションビューで表示されます。

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。この情報はロケーションビューで表示されます。
- [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。この情報はロケーションビューで表示されます。
- [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。

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す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 ヶ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 ヶ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割合として表示されます。

学生

- [Student: %Share By floor] : このレポートには、特定のフロアでの学生の滞在回数がパーセンテージで表示されます。この情報はロケーションビューで表示されます。
- [Student: %Share By zone] : このレポートには、さまざまなゾーンでの学生の滞在回数がパーセンテージで表示されます。この情報はロケーションビューで表示されます。

Presence

- [Presence: By floor] : このレポートには、フロア別の学生のプレゼンス（在席情報）が人時で表示されます。この情報はロケーションビューで表示されます。
- [Presence: By zone] : このレポートには、ゾーン別の学生のプレゼンス（在席情報）が人時で表示されます。この情報はロケーションビューで表示されます。

Visit Duration

- [Visit Duration: By floor] : このレポートには、学生が平日に各フロアで過ごした時間が表示されます。この情報はロケーションビューで表示されます。
- [Visit Duration: By zone] : このレポートには、学生が平日に各ゾーンで過ごした時間が表示されます。この情報はロケーションビューで表示されます。

密度

- [Density: By floor] : このレポートには、各フロアの 1000 平方フィートあたりの学生のプレゼンスが示されます。この情報はロケーションビューで表示されます。
- [Density: By zone] : このレポートには、各ゾーンの 1000 平方フィートあたりの学生のプレゼンスが示されます。この情報はロケーションビューで表示されます。
- [Density Index] : このレポートには、大学での 1000 平方フィートあたりの毎月の学生のプレゼンス（人時）が示されます。

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: 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、デフォルトでは、ピン留めされたロケーションの値がすべてのグラフに表示されます。棒グラフでは、各ピンの位置は棒で表されます。

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。

手順

ステップ 1 [Behavior Metrics] ウィンドウで、[Pin Locations] 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します。

ステップ 3 [Apply] をクリックします。



第 9 章

Cisco Spaces : ライブ占有率 アプリケーション

この章では、**ライブ占有率** アプリケーションについて説明します。

- [ライブ占有率 の概要 \(67 ページ\)](#)
- [Wi-Fi 占有率 \(68 ページ\)](#)
- [設定 \(70 ページ\)](#)

ライブ占有率 の概要

ライブ占有率 アプリケーションは、**ロケーション階層**に変更があった場合のカウンタの問題に対処するように強化されています。この機能強化の前に、新しいロケーションの追加、既存のロケーションの削除、または [TimeZone] などの重要なパラメータの更新などの [Location Hierarchy] の変更により、Wi-Fi の古いカウンタまたは誤ったカウンタが導入されました。

この機能強化により、[Location Hierarchy] の変更後にカウンタが無効になるため、現在の日の [Presence] チャートのカウンタがリセットされます（現在の時刻までのすべての既存の数値が削除されます）。

ライブ占有率 アプリケーションは、次のライセンスタイプで使用できます。

- SEE
- EXTEND
- SWITCH_EXT
- SMART_VENUES
- SMART_OPERATIONS
- SMART_OPERATIONS_BASE
- ACT (UI では Advantage と表示)
- UNLIMITED
- PREMIER_W

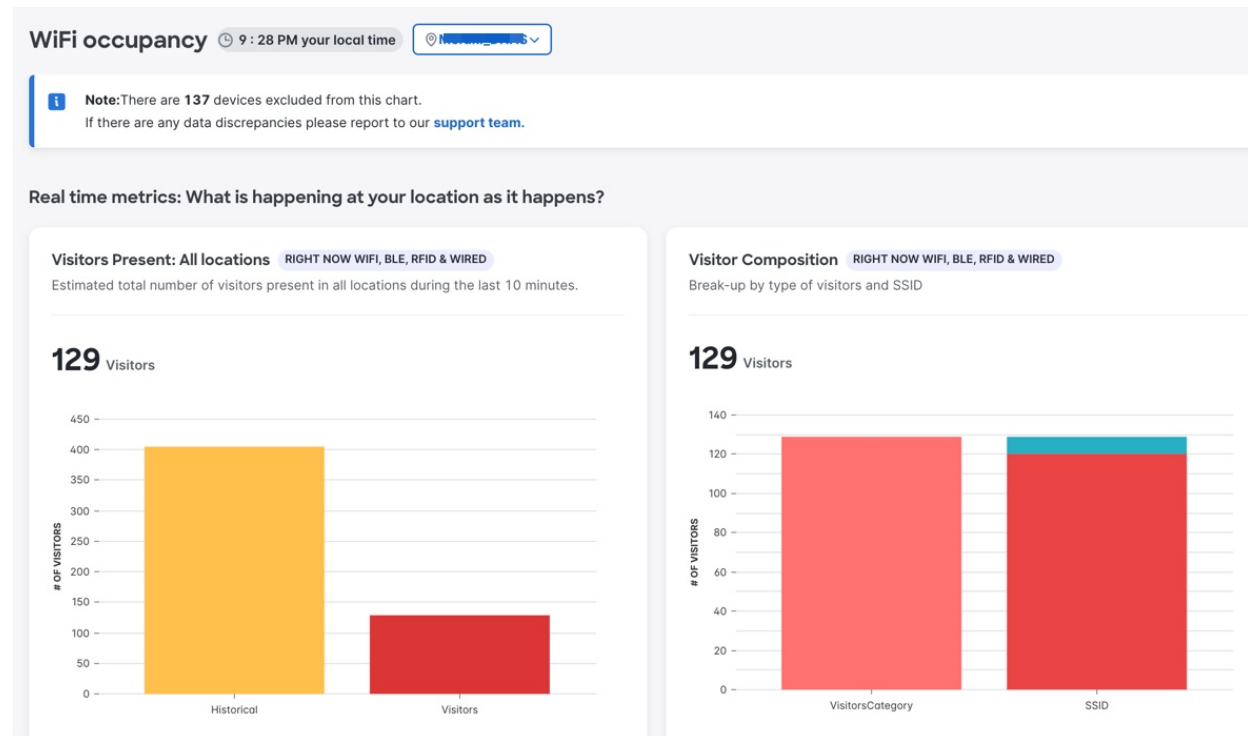
• PREMIER_CW

Wi-Fi 占有率

Wi-Fi占有率レポートには、自分が現在いるロケーションの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。

Wi-Fi 占有率は、訪問者と見なされない除外されたデバイスの数、またはデータ処理中にフィルタ処理されたデバイスの数を表示できるように機能強化されました。除外されたデバイスの数は、[Wi-Fi占有率 (WiFi occupancy)]の[注記 (Note)]セクションにメッセージとして表示されます。

図 6: ライブ占有率 アプリケーション





(注)

- ロケーション階層でロケーションが削除または変更された場合、またはタイムゾーンが変更された場合、既存の [Presence] チャートのカウントはリセットされます。
- BLE 処理の場合：
 - IoT の最新情報の一部として BLE グループ情報を受信する必要があります
 - RSSI 値は -85 より大きくする必要があります
- プローブデバイスの場合：
 - シスコ コネクタおよびその他のデバイスタイプ : RSSI 値が -70 より大きい必要があります
 - Cisco Meraki : RSSI 値は -100 より大きい必要があります。

指定された信号強度しきい値を満たすプローブデバイスのみが、Firehose データストリームの一部としてデバイスロケーション更新イベントを共有できます。

ライブ占有率レポートの表示

ライブ占有率 レポートを表示するには、次の手順を実行します。

手順

ステップ 1 Cisco Spaces ダッシュボードで、**ライブ占有率** を選択します。

ライブ占有率 アプリケーションが表示されます。

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 **ライブ占有率** レポートが表示されます。

レポート上部の **ライブ占有率** セクションに、使用システムのローカル時間が表示されます。

ライブ占有率 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 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と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。

設定

[設定 (Settings)] メニューは、**ライブ占有率** アプリケーション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。

デバイスを含めるまたは除外する

[デバイスを含める/除外する (Include/Exclude Devices)] タブを使用して、**ライブ占有率** レポートの Wi-Fi、BLE、および RFID デバイスについて次のオプションから選択します。

- Wi-Fi デバイスオプションはデフォルトで含まれていて、その選択を解除することはできません。
特定の SSID に接続されているデバイスを **ライブ占有率** 分析から除外するには、[追加/編集 (Add/Edit)] または [除外リストの追加/編集 (Add/Edit excluded list)] をクリックし、[SSID を除外する (Exclude SSIDs)] リストから目的の SSID を選択します。
- BLE タグ : **ライブ占有率** レポートに BLE タグを含めるには、[BLE タグを含める (Include BLE Tags)] をオンにします。

ライブ占有率 分析から特定のデバイス グループを除外するには、[追加/編集 (Add/Edit)] または [除外リストの追加/編集 (Add/Edit excluded list)] をクリックし、[BLEデバイスを除外 (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** : **ライブ占有率** レポートに RFID タグを含めるには、[RFIDタグを含める (Include RFID Tags)] を選択します。



-
- (注) • RFID タグと BLE タグを選択すると、対応するデバイス数も **ライブ占有率** 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 10 章

Cisco Spaces : Camera Metrics（カメラメトリクス）アプリケーション

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（73 ページ）](#)
- [カメラメトリックレポートの表示（74 ページ）](#)

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。

カメラメトリクスアプリケーションは、既存の Cisco Meraki カメラとともに Cisco Meraki MV93 クラウド管理型スマートカメラもサポートしています。



(注)

- Camera Metrics アプリは、[Setup] の [Camera] オプションを使用して Cisco 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 Spaces を設定する \(401 ページ\)](#) 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 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 Spaces ユーザーアカウントの場合、「Looks like you haven't setup your Meraki Camera」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 [Setup Guide] リンクとともに表示されます。
- Camera Metrics データはリアルタイムデータではなく、足跡データが Cisco Spaces ダッシュボードに反映されるまでに約 2 時間かかります。[Presence] チャートと [Peak Presence] チャートは、1 日が終わると更新されます。
- カメラメトリクス データはネットワークまたは建物のロケーションまで表示され、データを表示するには、ネットワークまたは建物のロケーションの下でカメラを設定する必要があります。

カメラメッセージキューイングテレメトリトランスポート (MQTT) ブローカの認証サポート

Cisco Spaces クラウドは、Cisco Meraki カメラから MQTT 更新を受信するためのパスワードベースの認証をサポートするように更新されました。バックグラウンドネットワーク同期プロセスにより、認証の詳細が Cisco Meraki ダッシュボードで自動的に更新されます。

カメラメトリックレポートの表示

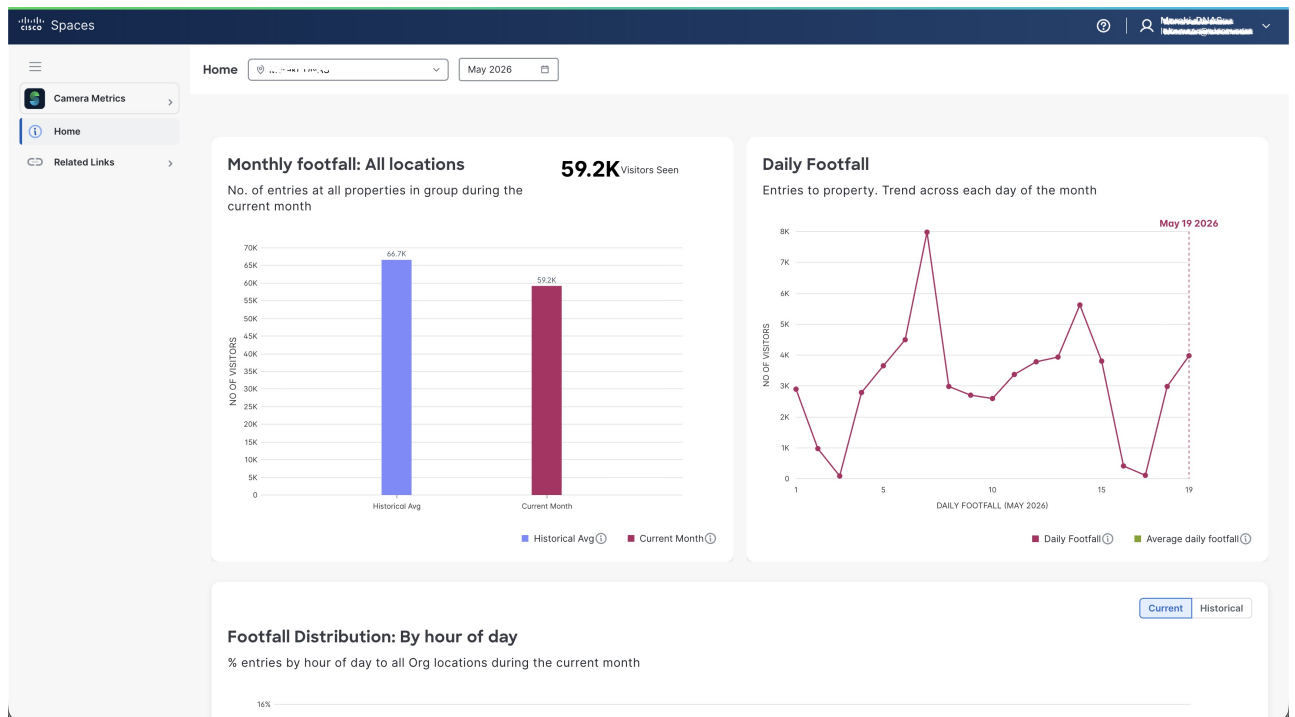
カメラメトリックレポートを表示するには、次の手順を実行します。

手順

ステップ 1 Cisco 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 7: カメラメトリックレポート



ステップ 2 (オプション) [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 Spaces に導入されたため、2020 年以降の年のみを選択できます。

レポートには次のグラフが含まれます。

- **[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 カ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ヵ月間の平均数）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ヵ月間の平均数）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ヵ月間の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ヵ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ヵ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 11 章

Cisco Spaces : オープンローミング (OpenRoaming) アプリケーション

- [OpenRoaming \(オープンローミング\) アプリケーションの概要 \(77 ページ\)](#)

OpenRoaming (オープンローミング) アプリケーション の概要

OpenRoaming は、Wi-Fi の面倒なゲスト オンボーディング プロセスと不正な SSID への接続リスクを排除して、安全でシームレスな自動ネットワーク接続を実現します。OpenRoaming により、複数の SSID から選択したり、設計が不十分なキャプティブポータルで安全ではない共有クレデンシャルを入力したりする必要がなくなるため、インターネットにアクセスしようとするモバイルデバイスユーザーにとっては特に便利です。OpenRoaming では、信頼できる ID プロバイダを使用してサインインすることでユーザーがゲストネットワークに接続できるようになり、ユーザーモビリティが強化されます。

詳細については、『[Cisco Spaces : OpenRoaming コンフィギュレーションガイド](#)』を参照してください。



第 12 章

Cisco Spaces : ロケーション分析アプリケーション

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。

- [ロケーション分析アプリケーションの概要 \(79 ページ\)](#)
- [ロケーション分析レポートの表示 \(81 ページ\)](#)
- [レポートの比較 \(83 ページ\)](#)
- [カスタムレポートの作成 \(85 ページ\)](#)
- [ウィジェットを追加 \(89 ページ\)](#)

ロケーション分析アプリケーションの概要

ロケーション分析アプリケーションを使用すると、建物内のさまざまなエリアや地域と異なるロケーションにおける、人々の足取り、訪問者数、訪問パターン、滞在時間の分布を把握して分析できます。従業員の訪問状況もレポートに含まれます。

ロケーション分析アプリケーションを使用して、訪問数、訪問者の洞察、および滞在時間分布データを含むレポートを表示し、希望するフィルタ条件に従ってカスタムレポートも作成します。

ロケーション分析アプリケーションのメインメニューには、[レポート (Reports)] と [カスタムレポート (Custom Reports)] の 2 つのオプションがあります。

レポート

左側のパネルで [レポート (Reports)] をクリックしてリストを展開し、[概要 (Overview)] をクリックしてレポートを表示します。[概要 (Overview)] ウィンドウには、訪問数、訪問者の詳細、および滞在時間分布データがタイル形式とグラフ形式の両方で表示されます。タイルの矢印アイコンをクリックすると、詳細をグラフ形式で表示できます。

カスタム レポート

ロケーション分析アプリケーションで、[レポート (Reports)] > [概要 (Overview)] を選択すると、訪問者/訪問の傾向/滞在時間分布を含むロケーション分析レポートがタイル形式とグ

ラフ形式の両方で表示されます。使用可能なフィルタパラメータに基づいてレポートを比較することもできます。詳細については、[レポートの比較（83 ページ）](#)を参照してください。



- (注)
- デフォルトでは、過去 365 日間のすべてのロケーション、すべての SSID のレポートが表示されます。必要に応じて、ウィンドウの上部にあるフィルタを使用して、レポートを変更します。
 - データのないロケーション分析アプリケーションを初めて使用する場合は、左側のメニューにある [ロケーション分析 (Location Analytics)] をクリックしてサンプルレポートを表示し、訪問者の詳細がどのように表示されるかを把握してください。

[概要 (Overview)] ウィンドウには、選択したパラメータに従って、**訪問者数**、**訪問数**、**日次平均訪問者数**、および **日次平均訪問数** に関連する情報が表示されます。

- **訪問者数** は、選択した基準に基づき、一意の訪問者の合計数として定義されます。
- **訪問数** は、特定のロケーションへの合計訪問数として定義されます。
- **日次平均訪問者数** は、選択した期間で毎日加算した訪問者の総数を、日数で割った日次平均として定義されます。
- **日次平均訪問数** は、選択した期間で毎日加算した訪問の総数を、日数で割った日次平均として定義されます。

[概要 (Overview)] ウィンドウは、次の情報をタイル形式で表示します。

- 訪問者数：日次平均訪問者数
- 訪問者数：新規と再訪問者の比較
- 訪問数：日次平均訪問者数
- 訪問数：平均滞在時間

[概要 (Overview)] ウィンドウは、次の情報をグラフ形式で表示します。

- 訪問者数の傾向
- 訪問数の傾向
- 滞在時間の分布

ロケーション分析レポートの表示

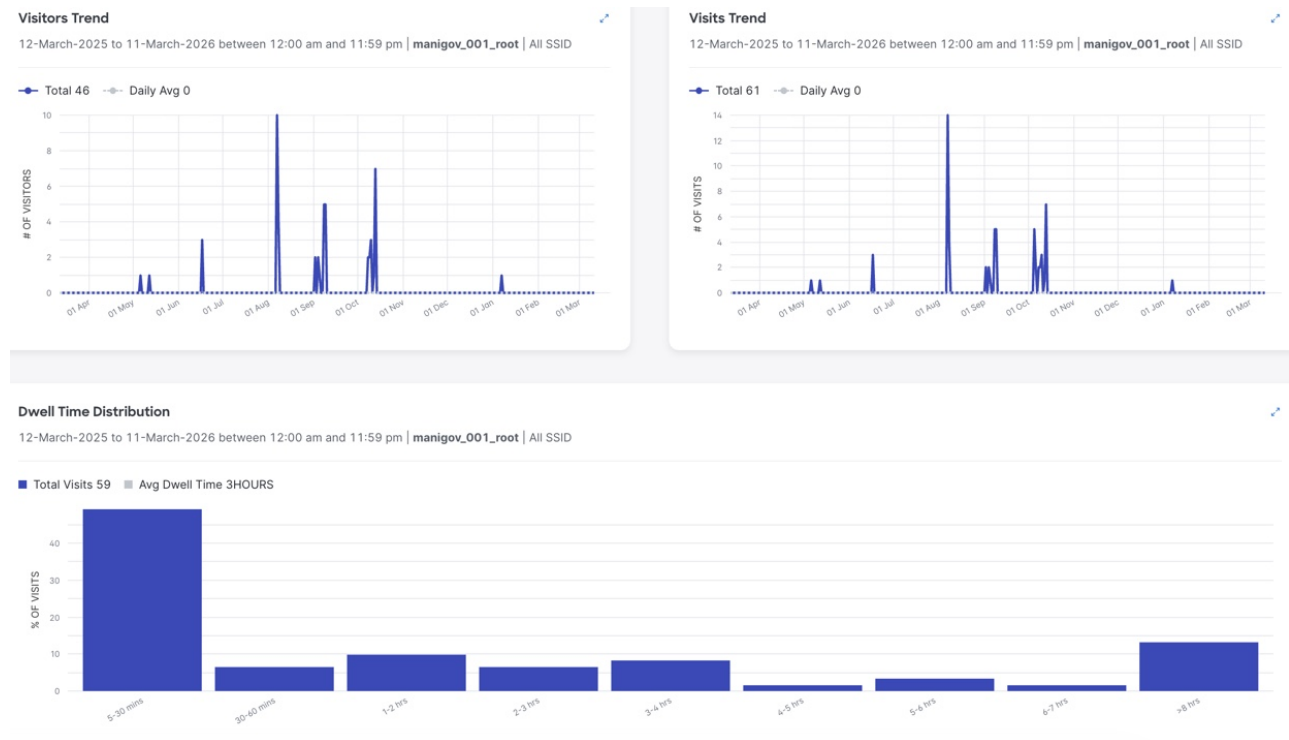
手順

ステップ 1 Cisco Spaces [ホーム (Home)] ページで、[ダッシュボード (Dashboard)] をクリックし、[ロケーション分析 (Location Analytics)] を選択します。

[ロケーション分析 (Location Analytics)] [ホーム (Home)] ページが表示されます。

ステップ 2 左側のパネルから、[レポート (Reports)] > [概要 (Overview)] を選択します。

[レポート (Reports)] メニューに [概要 (Overview)] ウィンドウが表示されます。



(注)

- デフォルトでは、ルートロケーション、すべての SSID、および過去 365 日間のレポートが表示されます。ロケーション、日付範囲、SSID でレポートをフィルタリングできます。
- SSID フィルタオプションは、ACT ライセンスユーザーのみが使用できます。SEE および EXTEND ライセンスユーザーは使用できません。ただし、日付範囲フィルタを使用して、グループ、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。

ステップ 3 [すべてのロケーション (All Locations)] 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)

ACT ライセンスユーザーはフロアとゾーンのレポートを表示できます。SEE および EXTEND ライセンスユーザーはネットワークロケーションのみをフィルタリングできます。

ステップ 4 [日付 (Date)] ドロップダウンリストから、レポートを表示する日付範囲を選択します。

次のオプションを使用できます。

表 7: 日付範囲オプション

日付の範囲	説明
今日	本日の各時間ごとの合計訪問数
昨日	前日の各時間ごとの合計訪問数
今週	今週の各曜日の合計訪問数
先週	前週の各曜日の合計訪問数
今月	当月の各日の合計訪問数
先月	前月の各日の合計訪問数
今年	今年の各日の合計訪問数
Custom	指定した期間の各日の合計訪問数が表示されます。 [カスタム日付範囲 (Custom Date Range)] ポップアップウィンドウで、開始日と終了日を指定し、[適用 (Apply)] をクリックします。

(注)

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 [全SSID (All 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。

[概要 (Overview)] ウィンドウには、選択したフィルタオプションに従ってロケーション分析レポートが表示されます。

ステップ 6 ロケーション分析レポートでは、次の情報をタイル形式で表示できます。

表 8: ロケーション分析レポート情報

レポート項目	説明
ビジター	選択したフィルタパラメータに基づく訪問者の合計数と日次平均訪問者数
ビジター	選択したフィルタパラメータに基づく訪問者の合計数。 新規訪問者 と 再訪問者 の数は、パーセンテージ情報とともに個別に表示されます。

レポート項目	説明
アクセス	選択したフィルタパラメータに基づく合計訪問数と日次平均訪問数。総訪問数と日次平均訪問数は、パーセンテージ情報とともに個別に表示されます。 (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。
滞在時間の分布	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、選択 SSID への訪問の滞在時間内訳を表示します。
Path ウィジェット	訪問者のロケーション間での移動パターンと、同じネットワーク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 ウィジェット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 ウィジェットは、ACT ライセンスアカウントのみで使用できます。

(注)

また、訪問者数の傾向、訪問数の傾向、および滞在時間の分布情報は、グラフ形式で表示することもできます。

レポートの比較

さまざまなフィルタパラメータに基づいてロケーション分析レポートを比較し、傾向や訪問者パターンを分析できます。レポートを比較するには、**[ロケーション分析 (Location Analytics)]** > **[レポート (Reports)]** を選択します。レポートメニューには、次の3つのオプションがあります。[ロケーションの比較 (Compare Locations)]、[日付の比較 (Compare Dates)]、および [SSIDの比較 (Compare SSIDs)]。

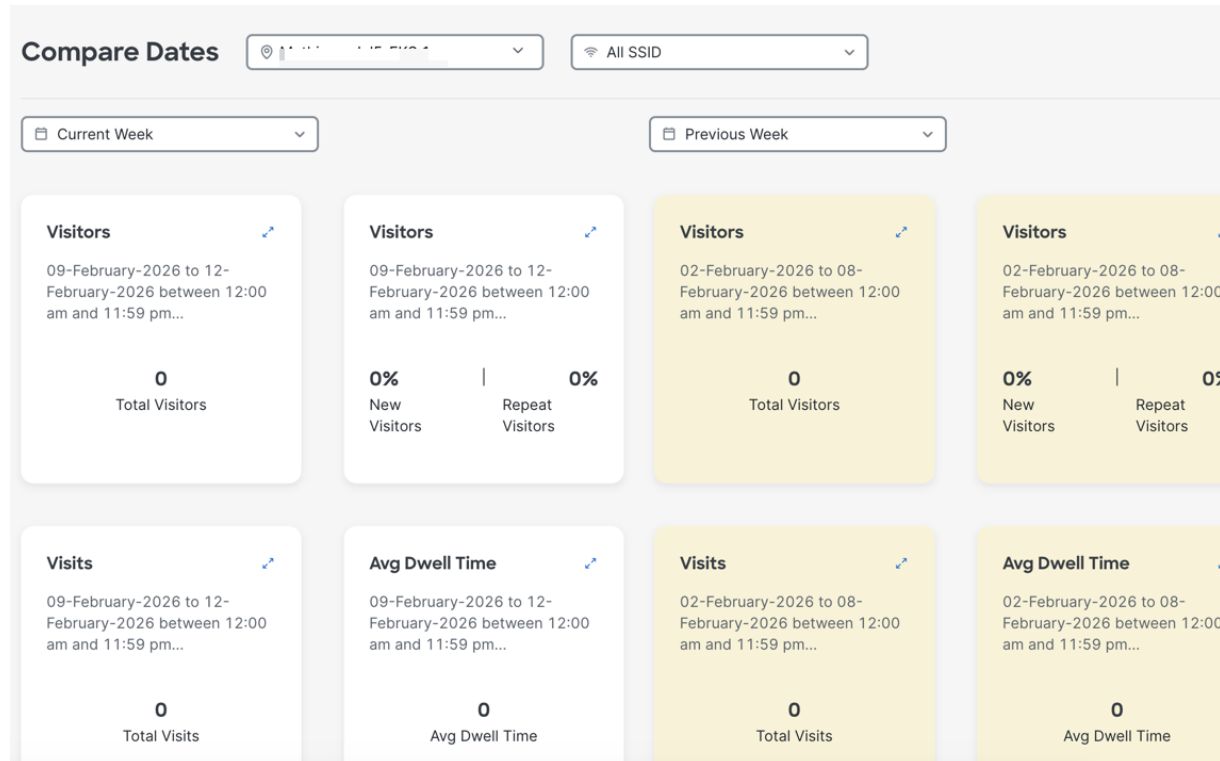
- **ロケーションの比較 (Compare Location)** : このタブを使用して、2つのロケーションレポートを比較し、訪問者の傾向を表示できます。デフォルトでは、訪問者が多い2つのロケーションがレポートの対象になります。訪問者データをチャートとして表示するには、少なくとも2つのネットワークロケーションでデータを使用できる必要があります。[ロケーションの比較 (Compare Location)] ウィンドウで、上部に表示される [ロケーション (ロケーション)] ドロップダウンリストから、比較してレポートを表示するロケーションを選択します。
- **日付の比較 (Compare Dates)** : このタブを使用して、2つの特定の日付または日付範囲を選択し、レポートを表示します。デフォルトでは、1番目のレポートでは今週が日付範囲として選択され、2番目のレポートでは前週が選択されます。[日付の比較 (Compare Dates)] ウィンドウで、上部に表示される [日付 (Date)] ドロップダウンリストから、必要な日付範囲オプションを選択して、レポートを比較して表示します。
- **SSIDの比較 (Compare SSIDs)** : このタブを使用して、2つの異なる SSID を比較し、訪問者の傾向を表示できます。デフォルトでは、訪問者が多い2つの SSID がレポートの対象になります。[SSIDの比較 (Compare SSIDs)] ウィンドウで、上部に表示される [SSIDs] ドロップダウンリストから、必要な SSID を選択して比較してレポートを表示します。

選択した比較オプションに応じて、ロケーション分析レポートが[ロケーション分析 (Location Analytics)] ウィンドウの左側と右側に表示されます。左側のロケーション分析レポート（白色のバックグラウンド）と、右側に表示されるレポート（黄色のバックグラウンド）を比較できます。



(注) ウィンドウの上部にあるフィルタパラメータを使用して、ロケーション分析レポートを表示することもできます。

図 8: レポートの比較オプション



カスタムレポートの作成

デフォルトのレポートタイプに適用できるフィルタに基づいてカスタムロケーション分析レポートを作成するには、**カスタムレポート** オプションを使用します。

使用可能なデフォルトのレポートタイプに基づいて、カスタムレポートを作成できます。

カスタムレポート 機能を使用すると、デフォルトのロケーションレポートを表示できるだけでなく、カスタム調整レポートも作成できます。[カスタムレポート (Custom Reports)] ウィンドウには、使用可能なすべてのレポート、デフォルトの概要レポート、比較オプション付きのレポート、および各カテゴリのレポート数が表示されます。

次の3つのカテゴリがあります。

- すべてのレポート
- 概要
- レポートの比較 (すべてのカテゴリを含むレポート)

ロケーション分析アプリケーションの **カスタムレポート** 機能を使用して、デフォルトのフィルタパラメータでレポートを作成し、これをデフォルトのロケーション分析レポートとして保存して参照してください。デフォルトのロケーション分析レポートを作成する際、すべてのロ

ケーション、過去 365 日間の範囲、および使用可能なすべての SSID などのデフォルトのフィルタパラメータが考慮されます。グローバルレベルのフィルタパラメータは、このデフォルトのロケーション分析レポートをフィルタ処理するために使用できません。

デフォルトのロケーション分析レポートに加えて、使用可能なレポートタイプと複数のウィジェットフィルタを含めることでカスタムレポートを作成できます。

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。

手順

- ステップ 1** Cisco Spaces ダッシュボードで、[ロケーション分析 (Location Analytics)] > [カスタムレポート (Custom Reports)] を選択します。
- ステップ 2** [Create New Report] をクリックします。
- [新規レポートの作成 (Create New Report)] ウィンドウが表示されます。

Create New Report

Report Name *

Overview

Use Metrics and Graph widgets to create an overview. Common Filters: Location and Date range

Compare Locations

Compare two locations side by side

Compare Dates

Compare two date ranges

Compare SSIDs ACT

Compare two SSIDs side by side

Path Report ACT

Know where visitors come from
Monthly Dwell Time Report and go to after a visit

- ステップ 3** [レポート名 (Report Name)] フィールドに、新しいレポートの名前を入力します。
- ステップ 4** レポートの種類を選択します。

次のオプションを使用できます。

- 概要
- ロケーションの比較 (Compare Locations)
- 日付の比較 (Compare Dates)
- SSIDの比較 (Compare SSIDs) (ACT ライセンスユーザーのみが利用可能)
- パスレポート (Path Report) : このレポートタイプはACTライセンスで使用できます。パスレポートレポートタイプで利用できるレポートフィルタは、場所および日付です。

(注)

パスレポートで、フォーカスエリアに表示される訪問数は、さまざまな場所から来た訪問者による合計訪問数を表します。この数は、ホームページウィジェットに表示された訪問数とは独立しているため、比較できません。

(注)

カスタムレポートに対して選択できるレポートタイプは1つだけです。

レポートタイプを追加または選択せずに、カスタムレポートを作成することもできます。レポートタイプを指定せずにカスタムレポートを作成する場合、レポートの作成時にすべてのデフォルトのレポートフィルタ値が考慮されます。

デフォルトの値は次のとおりです。

- ロケーション : ルートロケーション
- 日付範囲 : 365 日
- SSID : すべての SSID

ステップ 5 [Next] をクリックします。

ステップ 6 (オプション) レポートフィルタを選択せずに、[スキップして作成 (Skip & Create)] をクリックして、カスタムレポートを作成します。

ステップ 7 必要なレポートフィルタを選択するには、スライドボタンをクリックします。

次のオプションを使用できます。

- Location
- 日付
- SSID

必要なレポートフィルタを検索して選択するには、[検索 (Search)] オプションを使用します。

(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) および EXTEND 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いて、グループ、フロアおよびゾーンのロケーションをフィルタ処理することはできません。

ステップ 8 [日付 (Date)] レポートフィルタをクリックし、[日付範囲の選択 (Choose Date Range value)] ドロップダウンから、日付範囲フィルタを選択してレポートを表示します。

ステップ 9 [SSID] レポートフィルタをクリックし、右側のパネルから、レポートをフィルタ処理する SSID を選択します。

次の SSID オプションを選択できます。

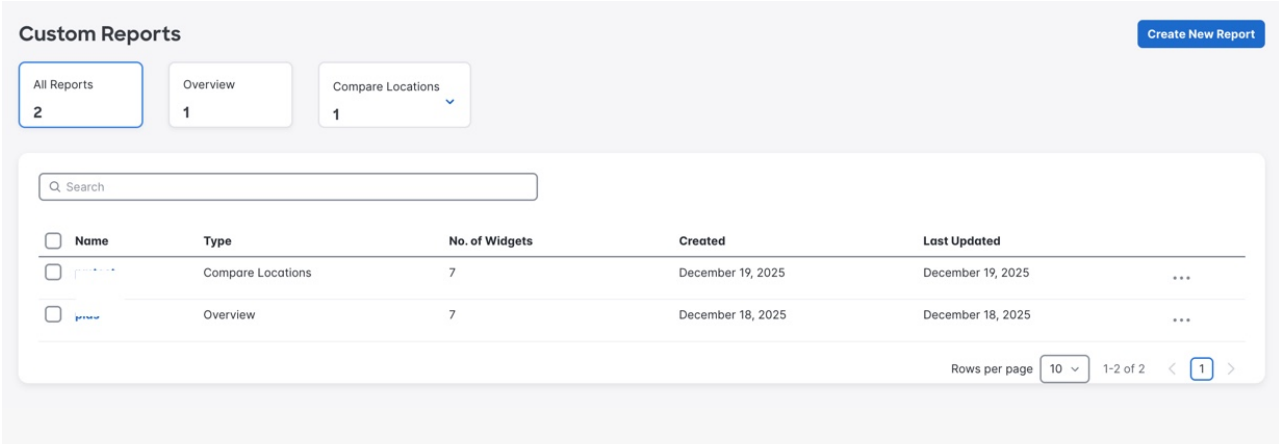
- [All SSIDs] : フィルタリングされたロケーションで SSID を使用してキャプチャされた、指定された期間の訪問データを表示します。
- [Cisco Spacesで設定されたカスタムSSID (Custom SSID configured in Cisco Spaces)] : 特定の SSID を使用してキャプチャされた、フィルタリングされたロケーションの指定された期間の訪問データを表示します。

(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、日付範囲フィルタを使用して、グループ、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。

ステップ 10 [作成 (Create)] をクリックします。

作成されたカスタムレポートは、[カスタムレポート (Custom Reports)] ウィンドウにリストされます。レポートの名前、タイプ、ウィジェットの数、作成日、および最終更新日を確認できます。[カスタムレポート (Custom Reports)] ウィンドウの上部には、グローバルレベルで使用可能なレポート フィルタも表示されます。



The screenshot shows the 'Custom Reports' section of the Cisco Spaces application. At the top, there are three tabs: 'All Reports' (selected, showing 2 items), 'Overview' (showing 1 item), and 'Compare Locations' (showing 1 item). Below the tabs is a search bar. The main area contains a table with the following columns: Name, Type, No. of Widgets, Created, and Last Updated. There are two rows of reports listed. The first row is 'Compare Locations' with 7 widgets, created on December 19, 2025. The second row is 'Overview' with 7 widgets, created on December 18, 2025. At the bottom right, there is a 'Rows per page' dropdown set to 10, and a pagination indicator showing '1-2 of 2' with a page number '1' in a box.

Name	Type	No. of Widgets	Created	Last Updated
Compare Locations	Compare Locations	7	December 19, 2025	December 19, 2025
Overview	Overview	7	December 18, 2025	December 18, 2025

(注)

- レポートを削除するには、該当する行の3つのドットアイコン (***) をクリックし、[削除 (Delete)] をクリックします。

- [名前 (Name)] チェックボックスをオンにしてすべてのレポートを選択し、[カスタムレポート (Custom Reports)] ウィンドウの右上にある [削除 (Delete)] をクリックしてレポートを削除します。

ウィジェットを追加

レポートの編集に、カスタムレポートにさらにウィジェットを追加できます。

手順

- ステップ 1** [ロケーション分析 (Location Analytics)] ウィンドウで、左側のパネルから [カスタムレポート (Custom Reports)] をクリックします。
- ステップ 2** 編集するレポートを選択します。
選択したロケーション分析レポートが表示されます。
- ステップ 3** ウィンドウの右上にある、3 つのドットのアイコンをクリックします。
- ステップ 4** [レポートの編集 (Edit Report)] をクリックします。
レポートが編集モードで表示されます。
- ステップ 5** [ウィジェットの追加 (Add Widgets)] をクリックします。
[ウィジェットの追加 (Add Widget)] ポップアップウィンドウが表示されます。

図 9: ウィジェットを追加

Add Widget

Name Your Widget

Choose the widget you want to add

Visitors Visits Dwell

Widget Information

Number of Visitors

Visit Range

All Day (12am-11:59pm)

View By

by Day

Cancel Add

ステップ 6 次の情報を入力します。

- a) **ウィジェットの名前 (Name Your Widget)** : 追加する新しいウィジェットの名前を入力します。
- b) **追加するウィジェットを選択 (Choose the widget you want to add)** : 追加するウィジェットをクリックします。使用可能なウィジェットは、[訪問者数 (Visitors)]、[訪問数 (Visits)]、および[滞在 (Dwell)]です。
- c) **ウィジェット情報 (Widget Information)** : [ウィジェット情報 (Widget Information)] ドロップダウンリストから、ウィジェットに含める必要がある情報を選択します。オプションは、ウィジェットの選択によって異なります。次のオプションを使用できます。
 - 訪問者数 (Visitors) ウィジェットの場合 : 訪問者の数 と 新規と再訪問の比較
 - 訪問数 (Visits) ウィジェットの場合 : 訪問数 と 新規と再訪問の比較
 - 滞在 (Dwell) ウィジェットの場合 : 分布 ディストリビューション
- d) **訪問範囲 (Visit Range)** : [訪問範囲 (Visit Range)] ドロップダウンリストから、レポートの日付範囲を選択します。

次のオプションを使用できます。

- 終日 (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。
- 深夜 (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。
- 早朝 (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。
- 朝 (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。

- **営業時間 (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。
- **夕方 (Evening)** : 夕方 (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。
- **夜間 (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。

ステップ 7 [Next] をクリックします。

[ウィジェットの追加 (Add Widget)] ポップアップには、[ロケーション (Location)]、[日付範囲 (Date Range)]、および[SSIDs]のタブが含まれます。これらのタブをクリックして、必要なオプションを選択して追加できます。

ステップ 8 [ロケーション (Locations)] タブをクリックします。

- a) (オプション) [ロケーションの検索 (Search Location)] フィールドに、名前を入力し、ロケーションを検索します。ロケーション検索を実行するには、3 文字以上を入力する必要があります。
- b) ルートロケーションを選択するか、クリックして展開して必要なゾーンまたはフロアを選択します。
- c) [表示基準 (View By)] ドロップダウンリストから、選択したロケーションについてレポートを表示する期間を選択します。
 - **日 (Day)** : 指定された期間の各日の訪問データが表示されます。
 - **時間帯 (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、2022 年 11 月の時間帯レポートで、午後 2 時に表示される訪問数は、2022 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。
 - **週 (Week)** : 指定された期間の各週の訪問データが表示されます。
 - **曜日 (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。

ステップ 9 [日付範囲 (Date Range)] タブをクリックします。

- a) [日付範囲 (Date Range)] ドロップダウンリストから、レポートを表示する期間を選択します。

日付範囲として[Custom (カスタム)]を選択した場合は、[開始日 (Start Date)]および[終了日 (End Date)]フィールドに開始日と終了日を入力します。
- b) [表示基準 (View By)] ドロップダウンリストから、レポートを表示する期間を選択します。

デフォルトでは、[ロケーション (Locations)] タブで選択した [表示基準 (View By)] オプションが表示されます。必要に応じて期間を更新でき、変更は[ロケーション (Locations)]および[SSIDs] タブに反映されます。

ステップ 10 [SSIDs] タブをクリックします。

- a) [SSIDs] ドロップダウンリストで、SSID を選択します。
- b) [表示基準 (View By)] ドロップダウンリストから、レポートを表示する期間を選択します。

デフォルトでは、前のタブで選択した [表示基準 (View By)] オプションが表示されます。必要に応じて期間を更新でき、変更は他のタブに反映されます。

ステップ 11 [Add] をクリックします。

[ウィジェットをここに配置 (Place Widget Here)] というプロンプトが表示され、青で強調表示されているエリアをクリックして新しいウィジェットを挿入できます。



第 13 章

Cisco Spaces : 影響分析アプリケーション

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 \(93 ページ\)](#)
- [インパクトキャンペーン \(イベント\) の追加 \(94 ページ\)](#)
- [影響分析レポートの表示 \(95 ページ\)](#)

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унツ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。
 - アカウンツで使用可能な訪問データが30日未満の場合、イベントの作成は制限されます。このシナリオでは、デフォルトのデータが表示されます。
 - Cisco DNA Spaces アカウンツへの読み取り専用アクセス権のみがあるユーザーは、そのアカウンツ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。

手順

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 Campaign] 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。

手順

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 14 章

Cisco Spaces : スペースの使用状況アプリケーション

- ・ [スペースの使用状況アプリケーションを使用する \(97 ページ\)](#)

スペースの使用状況アプリケーションを使用する

Cisco Spaces スペースの使用状況 (Space Utilization) アプリケーションは、これまでの物理スペースの使用状況に関する洞察を提供し、スペースの使用を最適化するのに役立ちます。これらの洞察は、空間のネットワークおよびコラボレーションインフラストラクチャ内に組み込まれたセンサーを介して収集されたデータから得られます。

このアプリケーションを使用すると、キャンパス、建物、またはフロア内の任意の物理的なスペースの占有率と利用率を表示できます。この情報には、人数、ピーク使用率、部屋の使用率、物理的なスペースでの滞在時間などのデータが含まれます。

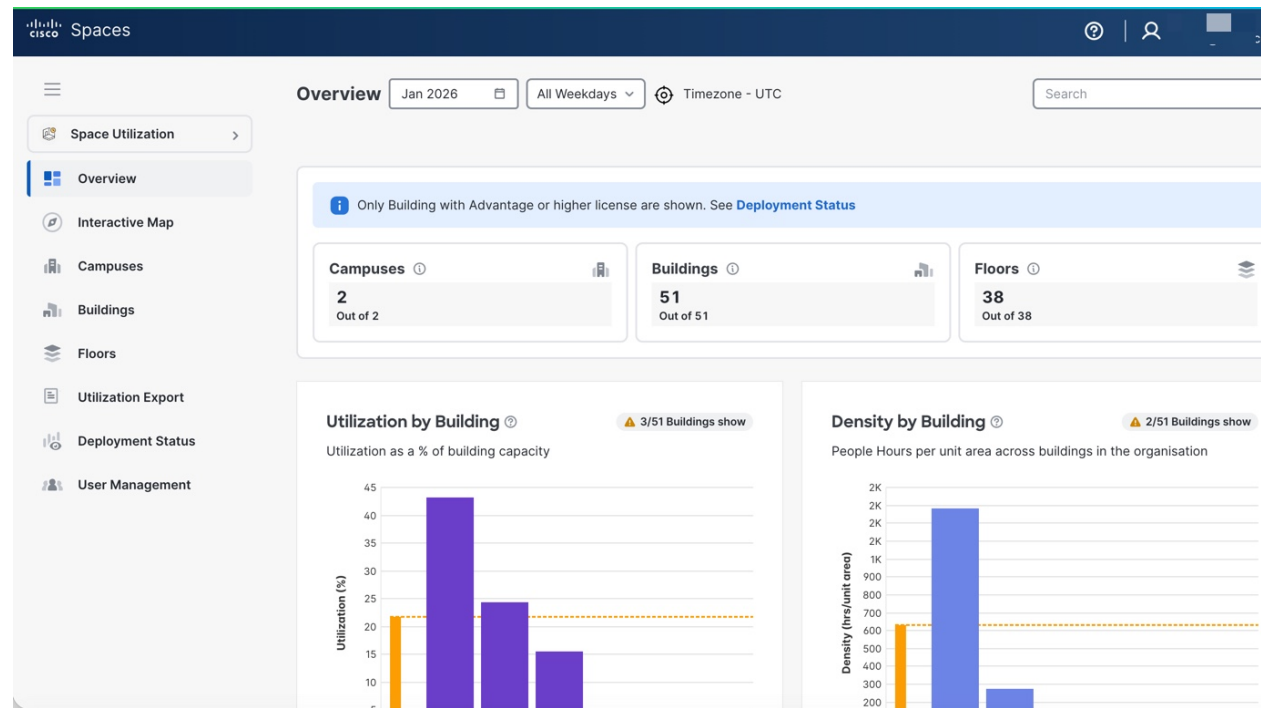
ワークスペースや教育分野の Cisco Spaces アカウントでは、[Floor Occupancy] と [Room Occupancy] の両方のメトリックが表示されます。デフォルトでは、その他すべての分野のアカウントには、次のメッセージが表示されます「*Occupancy charts are only available to Workspaces / Education vertical* (占有チャートは、ワークスペース/教育業種でのみ使用できます)」。

部屋の占有率レポート機能を使用して、室内にいる人数を含むデータ (15 分ごとに集約) を含む占有率レポートを生成できます。この機能により、15 分、30 分、60 分など、任意のレポート時間間隔に基づいて人数カウントデータを柔軟にダウンロードして分類できます。

スペースの使用状況アプリケーションの用語一覧の拡張により、**スペースの使用状況アプリケーション**内のすべてのビューで利用可能なさまざまなメトリックとチャートに対する統合された包括的な定義のセットが提供されます。これらの定義により、ユーザーの理解が向上し、データの表示方法と計算方法が明確になります。

スペースの使用状況アプリケーションを使用する

図 10: スペースの使用状況アプリケーション





第 15 章

Cisco Spaces: Smart Workspaces アプリケーション

Space Manager アプリケーションを使用すると、建物、フロア、会議室のさまざまな環境でのリアルタイムの占有状況や、湿度、電波品質、ノイズレベルなどの環境更新を確認できます。また、**Space Experience** アプリケーションでは Cisco Spaces を介してサイネージを管理できます。



(注) これらのアプリケーションには、次のタイプのライセンスが関連付けられています。

- ACT (UI では Advantage と表示)
- UNLIMITED
- PREMIER_W
- PREMIER_CW

• [Cisco Spaces : Smart Workspaces](#) での操作 (99 ページ)

Cisco Spaces : Smart Workspaces での操作

Cisco Smart Workspaces ソリューションをサポートするために、次の2つの新しいアプリケーションが利用可能です。



第 16 章

Cisco Spaces : 環境分析アプリケーション

- [Cisco Spaces : 環境分析アプリケーションの使用 \(101 ページ\)](#)

Cisco Spaces : 環境分析アプリケーションの使用

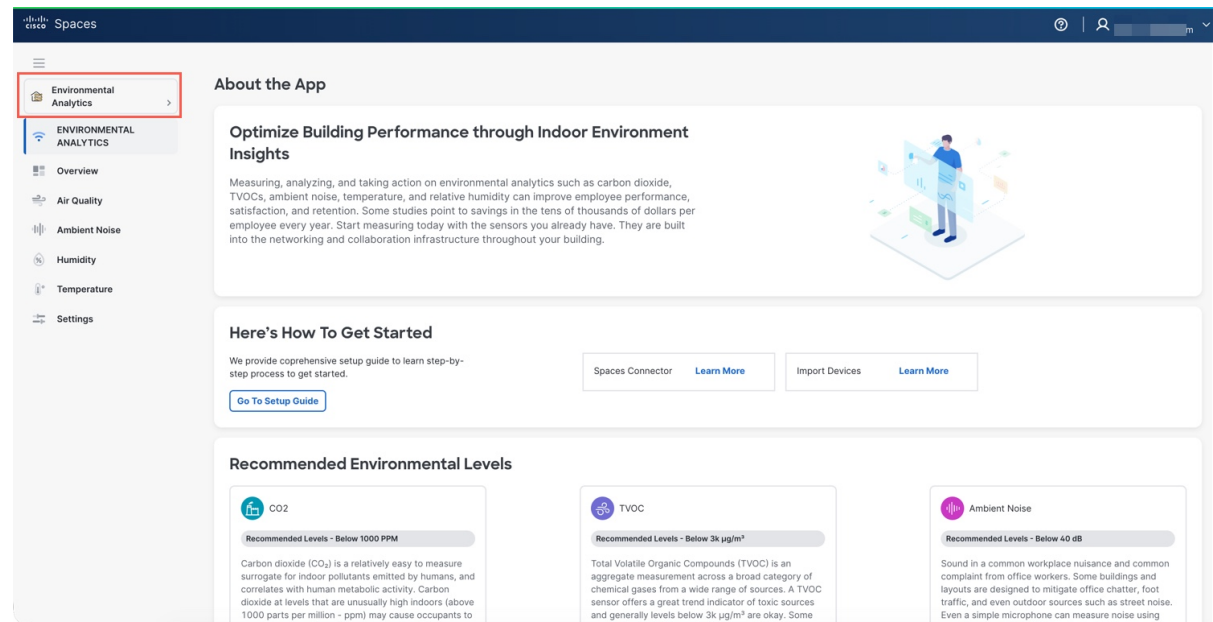
Cisco Spaces : 環境分析アプリケーション

Cisco Spaces 環境分析アプリケーションを使用すると、屋内環境のインサイトとメトリックを利用して、建物のパフォーマンスを最適化できます。これらのインサイトは、ネットワーク内の建物全体のネットワーキングおよびコラボレーションインフラストラクチャに統合されたセンサーから得られます。

環境分析アプリケーションを使用して、二酸化炭素レベル、総揮発性有機化合物（TVOC）、周囲ノイズ、温度、相対湿度などの重要な環境メトリックを測定および評価します。この貴重なデータを利用して、必要な是正措置を講じて、最適な屋内条件を確保し、施設内の全体的な環境品質を向上させます。

詳細については、『[Cisco Spaces: Environmental Analytics App Configuration Guide](#)』を参照してください。

図 11: 環境分析アプリケーション



(注) Cisco Spaces 環境分析 アプリケーションは **ACT** ライセンスに関連付けられています。



第 17 章

Cisco Spaces : Asset Locator アプリケーション

Cisco Spaces : Asset Locator アプリケーションは、アセットの監視やアセット、センサー、アラートシステム、運用ワークフローのパフォーマンス最適化を可能にします。

- [Cisco Spaces : Asset Locator アプリケーションの使用 \(103 ページ\)](#)

Cisco Spaces : Asset Locator アプリケーションの使用

Cisco Spaces : Asset Locator アプリケーションでは、一定量のタグとセンサーを利用して、継続的に統合し、監視することで、アセットの連携した運用を管理できます。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。

Cisco Spaces : Asset Locator の詳細については、「[アセットロケータ](#)」を参照してください。



第 18 章

Cisco Spaces : IoT Explorer アプリケーション

- [Cisco Spaces : IoT Explorer](#) (105 ページ)
- [Cisco Spaces : IoT Explorer の使用](#) (105 ページ)
- [温度監視 : ユースケースの概要](#) (106 ページ)
- [アセットトラッキング : ユースケースの概要](#) (107 ページ)
- [プレゼンス検出 : ユースケースの概要](#) (108 ページ)

Cisco Spaces : IoT Explorer

Cisco Spaces : IoT Explorer アプリケーションにより、アセット、センサー、アラートシステム、およびワークフローのパフォーマンスの監視および最適化が可能になります。

Cisco Spaces : IoT Explorer の使用

Cisco Spaces : IoT Explorer アプリケーションは、アセット、Internet of Things (IoT) センサー、アラートシステム、運用ワークフローの管理、監視、最適化のための包括的な単一リソースです。

IoT Explorer アプリケーションは、Operational Insights および Cisco Asset Locator アプリケーションの第 3 世代の拡張バージョンです。IoT Explorer アプリケーションは、Cisco Spaces でデバイス主導の IoT ユースケースを検討しているユーザーに迅速な価値をもたらし、ACT ライセンスレベルで IoT サービスに価値を追加するように設計されています。

このアプリケーションは、以下に示す 3 つのユースケースを実現します。

- 温度監視 : 空間を監視し、温度変化の通知を受け取る
- アセットトラッキング : アラートを見つけ、監視し、設定して、アセットの場所に関する洞察を得る

- スペースの占有/プレゼンス検出 : 物理的なスペースがどのように占有されているかをリアルタイムで把握

これらの各ユースケース内で、ルール/アラートの作成、データログの表示、デバイスまたはセンサーのリアルタイムのロケーションとステータスの表示を行うことができます。IoT Explorer アプリケーションの UI は、ユースケースを簡単に設定できるように設計されています。

IoT Explorer アプリケーションは、MAC 組織固有識別子 (OUI) 標準に準拠するデバイスと、最初の出現から 24 時間後も更新を送信し続けるデバイスのみをフィルタ処理します。

Cisco Spaces : IoT Explorer の詳細については、「[Cisco Spaces: IoT Explorer コンフィギュレーション ガイド](#)」を参照してください。

温度監視 : ユースケースの概要

温度監視のユースケースを使用して、屋内環境を管理および監視します。スケーラブルで合理化されたオンボーディングプロセスを備えた新しい温度センサーを追加し、センサーが特定のしきい値を上回ったり下回ったりしたときにチームメンバーにすばやく通知するルールを作成することができます。

温度モニタリングのユースケースでは、ルールまたはイベントをトリガーするには、デバイスの温度値がルールで定義されている指定条件内にある必要があります。たとえば、ルールでデバイスの温度条件が 5°C ~ 10°C と定義されている場合、イベントがトリガーされるのは、デバイスの温度が 5°C 未満になるか、10°C を超えた後に、5 ~ 10°C の範囲に戻ったときです。

詳細については、「[デバイスの温度監視の構成](#)」を参照してください。

Cisco Spaces ダッシュボードは、**IoT Explorer** アプリケーションの[温度監視 (Temperature Monitoring)] セクションで MT センサーデバイスのインポートをサポートします。

温度モニタリングのユースケースは、次の場合に役立ちます。

- 温度が範囲外になったときにアラートを受け取る
- 時間の経過に伴う温度変化を監視するイベントログを設定する
- すべての空間の温度に関する洞察を得る
- アセットのコンプライアンスを維持する

デバイスの温度監視の構成

手順

ステップ 1 Cisco Spaces ダッシュボードで、Cisco Spaces : IoT Explorer アプリタイルをクリックします。

ステップ 2 [Temperature Monitoring] をクリックします。

ステップ 3 [Get Started] をクリックします。

ステップ 4 [Use Case Name] フィールドに、ユースケースの名前を入力します。

ステップ 5 [Description] フィールドに、ユースケースの説明を入力します。

ステップ 6 [Create Use Case] をクリックします。

温度監視のユースケースは、センサー、ルール、およびユーザーをセットアップするためのさまざまなオプションを使用して作成されます。

ステップ 7 次のタブを使用して、構成を実行します。

- [Configure] : センサー、ルール、およびユーザーを構成します。
- [Sensors] : デバイスに接続されているセンサーを検索して管理します。
- [Rules] : アセットに接続されたセンサーを監視するルールを作成します。ルールを機能させるには、ルールをアクティブにし、アクションが自動的に実行されるトリガーが必要です。
- [Users & Roles] : ユーザーを追加し、その役割を管理します。
- [Events] : イベントを検索および管理します。設定したルールによってイベントがトリガーされると、イベントがここに表示されます。

新しいユースケースが作成され、[Active Use Cases] 領域に表示されます。

アセットトラッキング : ユースケースの概要

アセットトラッキングのユースケースを使用して、アセットタグを追加して、重要なオブジェクトの場所を管理および監視し、マップ上のアセットを検索します。スケーラブルで合理化されたオンボーディングプロセスを備えた新しいアセットタグを追加し、アイテムがゾーンを離れたときにチームメンバーにすばやく通知するルールを作成することもできます。関連するすべてのランダムな MAC Wi-Fi デバイスが、このユースケースに表示されます。

アセットトラッキングのユースケースは、以下に役立ちます。

- アセットがゾーン、フロア、または建物を離れたときの通知を構成する
- リアルタイムでアセットを見つける
- デバイスの使用頻度に関する洞察を得る

アセットロケーションのトラッキングとモニタリングの構成

手順

ステップ 1 Cisco Spaces ダッシュボード で、**IoT Explorer** アプリタイルをクリックします。

ステップ 2 [Asset Tracking] をクリックします。

ステップ 3 [Get Started] をクリックします。

ステップ 4 [Use Case Name] フィールドに、ユースケースの名前を入力します。

ステップ 5 [Description] フィールドに、ユースケースの説明を入力します。

ステップ 6 [Create Use Case] をクリックします。

アセットトラッキングのユースケースは、アセットの管理、ルールの設定、ユーザーの追加を行うためのさまざまなオプションを使用して作成されます。

ステップ 7 次のタブを使用して、構成を実行します。

- [Configure] : センサー、ルール、およびユーザーを構成します。See
- [Locator] : 名前または場所を使用してセンサーを検索します。フロアマップイメージ上のすべてのデバイスをリアルタイムで追跡できます。
- [Assets] : センサーを検索して管理します。
- [Rules] : センサーを監視するルールを作成します。ルールを機能させるには、ルールをアクティブにし、アクションが自動的に実行されるトリガーが必要です。
- [Users & Roles] : ユーザーを追加し、その役割を管理します。
- [Events] : イベントを検索および管理します。

作成された新しいユースケースは、[Active Use Cases] 領域に表示されます。

プレゼンス検出 : ユースケースの概要

プレゼンス検出のユースケースを使用して、デスク、部屋、オフィスの占有状態のライブデータを管理および監視します。スケーラブルで合理化されたオンボーディングプロセスを備えた新しい占有状態センサーを追加し、スペースが一定期間占有されたときにチームメンバーにすばやく通知するルールを作成することもできます。インポートしたマップにセンサーを手動で配置することもできます。

プレゼンス検出のユースケースは、具体的に次のような点で役立ちます。

- データログルールを作成することにより、スペース使用率に関する洞察を得る
- マップを活用して、ライブのスペース占有状況をすばやく確認する
- 過去の占有データを施設チームメンバーと共有する
- スペースが空いたときに通知するルールを設定する

このユースケースでは、次のセンサーがサポートされています。

- パッシブ赤外線センサー（PIR）
- Meraki カメラ

プレゼンス検出の構成

手順

ステップ 1 Cisco Spaces ダッシュボードで、**IoT Explorer** アプリタイルをクリックします。

ステップ 2 [Presence Detection] をクリックします。

ステップ 3 [Get Started] をクリックします。

ステップ 4 [Use Case Name] フィールドに、ユースケースの名前を入力します。

ステップ 5 [Description] フィールドに、ユースケースの説明を入力します。

ステップ 6 [Create Use Case] をクリックします。

プレゼンス検出のユースケースは、アセットの管理、ルールの設定、ユーザーの追加を行うためのさまざまなオプションを使用して作成されます。

ステップ 7 次のタブを使用して、構成を実行します。

- [Configure] : センサー、ルール、およびユーザーを構成します。
- [Occupancy View] : 名前または場所を使用してセンサーを検索します。フロアマップ画像から、占有スペースと非占有スペースを追跡できます。
- [Sensors] : センサーを検索して管理します。
- [Rules] : センサーを監視するルールを作成します。ルールを機能させるには、ルールをアクティブにし、アクションが自動的に実行されるトリガーが必要です。
- [Users & Roles] : ユーザーを追加し、その役割を管理します。
- [Events] : イベントを検索および管理します。

作成された新しいユースケースは、[Active Use Cases] 領域に表示されます。



第 19 章

Cisco Spaces : キャプティブポータルアプリケーション

この章では、Cisco 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 (111 ページ)
- キャプティブポータルルール (152 ページ)
- SSID, on page 159
- レポート, on page 163
- ユーザー管理, on page 167
- アクセスコード (168 ページ)
- 信頼できるデバイス, on page 181
- 設定 (187 ページ)
- ポータルの認定デバイス リスト (197 ページ)
- Cisco Spaces キャプティブポータルの動作 (198 ページ)
- 顧客の認証手順 (204 ページ)
- 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 (215 ページ)

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

- 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（261 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、使用するソーシャルアプリケーションで該当する設定を行い、そのソーシャルアプリケーションを Cisco 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（187 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 9:

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。

手順

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。

手順

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 for all 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 for all 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 \(121 ページ\)](#) 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 \(129 ページ\)](#) 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 \(117 ページ\)](#) 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

次のとおり、Cisco Spaces のポータルモジュールがあります。

- **Header/Branding**—このモジュールを使用してポータルのページタイトルとブランド名を定義します。

[ページタイトル (Page Title)] フィールドを使用してキャプティブポータルのページタイトルを変更します。更新されたページタイトルが使用する Cisco Spaces : キャプティブポ

タルアプリケーションに表示されます。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ター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ー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 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。

手順

- 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（120 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せん。
- 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。

手順

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。

手順

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、[ポータル言語の設定](#) (119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

```
[{"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": "b"}, {"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"}, {"Guarani": "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"}, {"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"}, {"Wallloon": "wa"}, {"Welsh": "cy"}, {"Wolof": "wo"}, {"Western Frisian": "fy"}, {"Xhosa": "xh"}, {"Yiddish": "yi"}, {"Yoruba": "yo"}, {"Zhuang": "za"}, {"Zulu": "zu"}]
```

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](#) (129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 \(206 ページ\)](#) 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 \(124 ページ\)](#) 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 \(204 ページ\)](#) 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 \(123 ページ\)](#) 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 \(208 ページ\)](#) 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 \(126 ページ\)](#) 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 \(214 ページ\)](#) 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、「[ソーシャルサインイン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 \(211 ページ\)](#) 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 \(127 ページ\)](#) 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 \(213 ページ\)](#) 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 \(128 ページ\)](#) を参照してください。



(注) [OptIn] 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 \(129 ページ\)](#) 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ますようになりました。

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。

手順

- 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 \(129 ページ\)](#) 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を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 \(187 ページ\)](#) 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 \(129 ページ\)](#) 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。

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。

手順

- 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 \(129 ページ\)](#) 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が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が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 \(187 ページ\)](#) 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 \(129 ページ\)](#) 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。

Social Sign In 認証のためのポータル設定

Cisco 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



(注) 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、そのソーシャルネットワークのアプリケーションを Cisco Spaces で設定する必要があります。[設定 (Settings)] オプションを使用して、Cisco 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 \(196 ページ\)](#) 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。

手順

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 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 \(129 ページ\)](#) 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 \(196 ページ\)](#) 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

- 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 \(129 ページ\)](#) を参照してください。
- [+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。
- 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。

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。

手順

-
- 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（129 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を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（129 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。

手順

-
- 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（129 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 \(168 ページ\)](#) 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 \(129 ページ\)](#) 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。

手順

- 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。

手順

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なります。
- [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えるようになります。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。

ポータルブランド名の定義

Cisco Spaces では **Header/Branding** モジュールを使用してポータルにブランド名とページタイトルを追加できます。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。

ポータルブランド名とページタイトルを定義するには、次の手順を実行します。

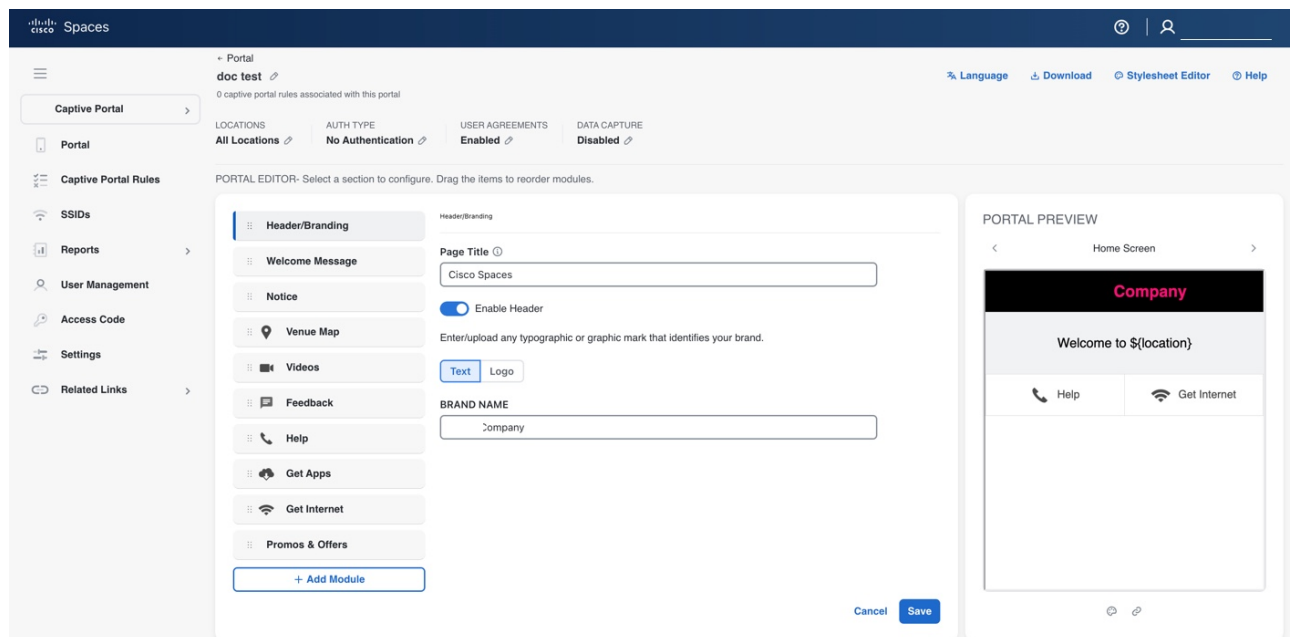
手順

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 [ヘッダー/ブランディング (Header/Branding)] モジュールをクリックします。

ステップ 3 [ページタイトル (Page Title)] フィールドで、ページタイトルを編集します。

図 13: Header/Branding モジュール



(注)

- 既存のポータルのページタイトルは、デフォルトで **Cisco Spaces** になります。新規作成されたポータルでは、アカウント名がデフォルトのページタイトルとなります。ページタイトルは編集できます。
- この機能は、Cisco Spaces のベータ版 UI でのみ使用できます。

ステップ 4 [ヘッダーの有効化 (Enable Header)] をクリックして、ポータルプレビューを表示します。

ステップ 5 ブランドのタイプを選択します。

- [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 6 [Save] をクリックします。

ポータルにブランド名とページタイトルが正常に定義されます。

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 \(154ページ\)](#) 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ター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。

手順

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 \(215ページ\)](#) を参照してください。

ステップ 4 リピーター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

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（215 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（154 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。

手順

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 \(154 ページ\)](#) 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。

手順

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（154 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。

手順

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 \(154 ページ\)](#) 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。

手順

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 \(154 ページ\)](#) 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。

手順

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 \(154 ページ\)](#) 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。

手順

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。

- [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。
- [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。
- [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。
- 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。
- [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 \(154 ページ\)](#) 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 \(129 ページ\)](#) 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。

手順

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 \(154 ページ\)](#) 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。

手順

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 \(154ページ\)](#) 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。

手順

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

[AddModule] 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。

手順

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 \(215 ページ\)](#) 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 \(154 ページ\)](#) 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。

手順

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。

ポータルスタイルシートを編集するには、次の手順を実行します。

手順

- 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。

手順

- 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。

手順

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。

- [Portal Name] フィールドに、ポータルのファイル名を入力します。
- 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。
- 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。

手順

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。

手順

-
- 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一覧が表示されます。
 - ステップ 4 編集するポータル右端に表示される [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。
-

ポータルロケーションの編集

ポータルロケーションを編集するには、次の手順を実行します。

手順

-
- 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。

手順

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。

手順

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。

手順

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。

手順

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。

- 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。
- 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。
- 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。プレビューセッ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、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ため 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 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、[#unique_173](#)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 \(111 ページ\)](#) 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 \(129 ページ\)](#) を参照してください。
- キャプティブポータルにはRADIUS認証を使用することを強くお勧めします。RADIUS 認証は、インターネットのシームレスなプロビジョニング、インターネットの拒否、およびセッション期間と帯域幅の定義を許可するために必須です。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 \(46 ページ\)](#) 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](#)で説明されている設定を行います。
 - ワイヤレスネットワークが Cisco Catalyst 9800 シリーズ コントローラの場合、「[DNA Spaces 上のRADIUSサーバーを使用したキャプティブポータル](#)」に記載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](#)（153 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。

手順

- 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、[#unique_173](#)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 \(191 ページ\)](#) 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。

- 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。
- 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。
- 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が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 \(115 ページ\)](#) 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 \(153 ページ\)](#) 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一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、「[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ー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。

手順

- 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、[#unique_178](#)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 \(115 ページ\)](#) 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。
- [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。
 - [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。
 - [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。

SSID

サービスセット識別子 (SSID) は、ワイヤレスネットワーク識別子であり、

- ユーザーが使用デバイスを特定のワイヤレスネットワークに接続できるようにします
- 企業がさまざまな場所にある複数のネットワークを区別して管理できるようにします
- Cisco Spaces 内でさまざまなキャプティブポータルを割り当てるための基礎として機能します。

SSID とは、顧客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 を保持できます。Cisco Spaces では、要件に応じて、ビジネス拠点で同じ SSID またはさまざまな SSID を使用して、異なるキャプティブポータルを表示できます。

SSID は、Cisco Unified Wireless Network (UWN) 向けシスコ 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 システムで定義されます。SSID に対してキャプティブポータルを表示するには、SSID を Cisco 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「Detail」リンクがあります。必要に応じて、ワイヤレスネットワーク用にインポートされた SSID をグリッドから削除できます。

SSID の [手動設定 (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方法が表示されます。たとえば、Meraki SSID の [手動設定 (Configure Manually)] リンクは、Cisco Meraki の設定手順につながります。

Cisco 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。この機能により、ネットワーク同期に遅延があるときに不要な 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 Spaces にインポートまたは設定するには、次の手順を実行します。

- ロケーション階層を作成します。このプロセスの詳細については、「[ロケーション階層の概要](#)」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 を作成するには、「[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, on page 37](#)」の章を参照してください。
 - Meraki 用に SSID を作成するには、「[Cisco Meraki での SSID の有効化, on page 45](#)」セクションを参照してください。
- Meraki の SSID をインポートするには、Cisco Spaces と Meraki が接続されていることを確認してください。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。または、Cisco 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。
- 既存の SSID の場合、ACL リストに現在のドメインとそれぞれの IP を保持することを推奨します。

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 \(160 ページ\)](#)」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



Note

- 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 Spaces に SSID を手動で追加する必要があります。
- Cisco CMX と Cisco AireOS シリーズ ワイヤレス コントローラや Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを使用する場合、SSID は 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 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 名を確認します。
- Cisco Spaces クラウド RADIUS サーバーは、Web RADIUS 認証で 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 Cisco Spaces に手動でインポートするには、次の手順を実行します。

Procedure

- ステップ 1 Cisco Spaces ダッシュボードで、[Home] を選択します。
- ステップ 2 [Spaces アプリケーション (Spaces App)] タブの [訪問者オンボーディングおよびエクスペリエンス (Visitor Onboarding & Experiences)] エリアで、[キャプティブポータル (Captive Portal)] をクリックします。
- ステップ 3 表示される [キャプティブポータル (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 [SSID のインポート/設定 (Import/Configure SSID)] ウィンドウで、[ワイヤレスネットワーク (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。

What to do next



Note Cisco 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 (GUI)

Cisco Meraki ネットワークから Cisco Spaces に SSID をインポートし、キャプティブポータル機能を有効にして、さらに設定できるようにします。

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 Spaces と連携できるように SSID を設定する必要があります。



Note 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。

Procedure

- ステップ 1** Cisco Spaces ダッシュボードで、[ホーム (Home)] を選択します。
- ステップ 2** [Spaces アプリケーション (Spaces App)] タブの [訪問者オンボーディングおよびエクスペリエンス (Visitor Onboarding & Experiences)] エリアで、[キャプティブポータル (Captive Portal)] をクリックします。
- ステップ 3** 表示される [キャプティブポータル (Captive Portal)] ウィンドウで、左ペインの [SSIDs] を選択します。[Import/Configure SSID] をクリックします。
- ステップ 4** 表示される [インポート/設定 (Import/Configure)] ウィンドウで、[ワイヤレスネットワーク (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 5** [組織 (Organization)] ドロップダウンリストから、SSID をインポート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 6** 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 7** 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 8** 表示されるウィンドウで、[アクティブ化 (Activate)] をクリックして、Meraki の SSID に関する Cisco Spaces の設定を更新します。

[SSID Configuration Sync] ウィンドウに、Meraki で設定する必要がある SSID の更新が表示されます。

ステップ 9 [更新 (Update)] をクリックします。

Note

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。

What to do next



Note

インポートされた SSID をロードするために Cisco Spaces を Meraki ネットワークと同期させる必要があるため、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。

レポート

レポートは、データ要約のために次の機能を実行します。

- カスタマイズ可能な期間におけるキャプティブポータルの使用状況に関する洞察を提供
- 複数の場所にまたがる情報の表示
- 特定の場所とタイムフレームに注目してフィルタ処理可能。

Cisco Spaces には、次のキャプティブポータルレポートが用意されています。

デフォルトでは、レポートには過去 1 年間の全ロケーションのデータが含まれます。ロケーションおよび期間でレポートをフィルタ処理できます。

レポートを表示するには、[レポート (Reports)] を [キャプティブポータル (Captive Portal)] ウィンドウの左ペインでクリックします。

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には、次のレポート機能があります。

- 使用する SSID に接続している各デバイスを識別して記録します。
- 同じ顧客が複数のデバイスで接続した場合でも、顧客固有のデバイス数を提供します。
- オンボーディングレポート内のプロモーションとオファーのエンゲージメントを追跡できます。

デバイスオンボーディングレポートの [プロモーションとオファーのパフォーマンス (Promos & Offers Performance)] セクションにプロモーションのビュー数が含まれるようになりました。この機能を使用すると、特定のプロモーションのビュー数とクリック数を追跡できます。

オンボーディングジャーニー

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。

- **SSIDに接続 (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。
- **表示されたキャプティブポータル (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。
- **プロビジョニングされたインターネット (Provisioned Internet)** : 指定された期間中に、選択され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 Spaces の展開日以降、全ロケーションにおけるこのメトリクスが、[インターネットにプロビジョニングされた一意のデバイスの総数 (Total Unique Devices Provisioned Internet)] のレポートの上部に表示されます。

SSID 別の新規および再アクセスデバイスの日次傾向

このセクションには、指定された期間に選択ロケーションから SSID に接続した、新規および再アクセス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。
- **再アクセスデバイス (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再アクセス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は、グラフの上部に表示されます。

キャプティブポータルでのメニューボタンのクリック回数

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メニューボタンをクリックした回数で計算されます。

- **メニューボタン数 (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。
- **クリック数 (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クリックされた合計回数。

顧客獲得

このレポートには、特定の期間に選択したロケーションから最近獲得した一意の顧客に関する洞察が表示されます。また、これらの顧客から収集される個人データおよびデモグラフィックデータについても説明します。



- (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、ソーシャル ID など）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

顧客獲得は、次の特徴を備えたメトリックです。

- 個人識別子によって特定された一意の新規顧客の総数を追跡する
- 「認証なし」または「アクセスコード」で認証された顧客を除外する
- 新しいデバイス接続に対する取得率を示すパーセンテージを提供する。
- SSID に接続された新規デバイス (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対象 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。
- 特定された新規顧客 (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。Cisco Spaces のインストール日以降で全ロケーションに関するこれらのメトリックは、このレポートの上部にある [特定された顧客 (Customers Identified)] の下に表示されます。
- [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。
- 完了したデータキャプチャ (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

プッシュ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数を示し、Y軸はカウントを示します。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。

顧客のデモグラフィック プロファイル属性

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、言語などのプロフィールの詳細が表示されます。

国数 (Countries)：国データが収集された顧客総数のうち、さまざまな国からの顧客の割合を円グラフでこのパネルに表示します。国の合計数は円グラフの中央に表示されます。顧客数が最も多い国は、顧客数とともに表示されます。[すべて表示 (Show All)] ボタンをクリックすると、少なくとも1人の顧客がいる国をすべて表示できます。国名は、認証プロセス中に指定された電話番号の国番号に基づいて決定されます。

言語 (Languages)：言語データが収集された顧客総数のうち、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。[すべて表示 (Show All)] ボタンをクリックすると、少なくとも1人の顧客がいる言語をすべて表示できます。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。

性別 (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。

ユーザー管理

新しいユーザーに関連するロールとロケーションアクセスを割り当て、適切なポータルアクセスと管理権限を付与します。

[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ケーションの読み取りと書き込み権限を持つユーザーのみが、[ユーザー管理 (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。

- **クリエイティブユーザー (Creative User)** : このユーザーは、アクセス権が付与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 Spaces の他の機能にアクセスできません。このロールは、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、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。

アクセスコードマネージャまたはクリエイティブユーザーを定義するには、次の手順を実行します。

Procedure

ステップ 1 Cisco Spaces ダッシュボードで、[ホーム (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。

Note

[ユーザー管理 (User Management)] オプションは、キャプティブポータルアプリケーションで読み取りと書き込み権限を持つユーザーのみが Cisco Spaces ダッシュボード で使用できます。

ステップ 4 [Invite User] をクリックします。

ステップ 5 [ユーザーを招待 (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、[次へ (Next)] をクリックします。

ステップ 6 [ロール (Role)] ドロップダウンリストから、[クリエイティブユーザー (Creative User)] または [アクセスコードマネージャ (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 [ロケーション階層 (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。[Done] をクリックします。

ステップ 9 [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。ユーザー名は[ユーザー (Users)] タブに表示されます。[ユーザーの検索 (Find Users)] フィールドを使用して、ユーザーを検索できます。

アクセスコード

アクセスコードの作成

Cisco Spaces により、アクセスコードを使用して事業の場所のインターネット 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にアクセスコードを作成し、これらのコードを使用してそれぞれの場所のインターネットアクセスを制御できます。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 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、使用するキャプティブポータルのアクセスコード認証を設定します。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 \(127 ページ\)](#)」を参照してください。

使い捨てアクセスコードを作成することもできます。>[**アクセスコード (Access Code)**] > [**アクセスコードの作成 (Create Access Code)**] を選択して、新しい一回限りのアクセスコードを作成します。詳細については、[使い捨てアクセスコードを作成する \(171 ページ\)](#) を参照してください。

アクセスコードの設定要件

- アクセスコードを作成または管理できるのは、アカウント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 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 Spaces アカウント管理者ユーザーのみです。アクセスコードオプションは、Cisco Spaces ダッシュボード の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使用できます。
- アクセスコードレベルで設定された**セッション期間**と**帯域幅制限**が、キャプティブポータルによって考慮されます。認証中に、値はコントローラに渡され、セッションの継続時間と帯域幅についてコントローラで行われたデフォルト設定を上書きします。

アクセスコードとインターネットプロビジョニング

Cisco Spaces では、アクセスコードを顧客と共有できます。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 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手順については、「[アクセスコード認証の手順（211ページ）](#)」を参照してください。

効果的なアクセスコード管理

インターネットプロビジョニングのセキュリティと機能を維持するには、次のガイドラインに従ってください。

- アカウント管理者またはアクセスコードマネージャロールを持つユーザーにのみ、アクセスコードの作成および管理権限を付与します。
- Cisco Spaces アカウント管理者ユーザーのみを介してアクセスコードマネージャになるようにユーザーを招待します。
- アクセスコードレベルで設定されたセッション期間および帯域幅の制限は、認証プロセス中、デフォルトのコントローラ設定よりも優先されることに留意してください。

共有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。

手順

ステップ 1 Cisco Spaces ダッシュボードで、[キャプティブポータル (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)

[アクセスコード (Access Code)] オプションは、Cisco 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 Spaces ダッシュボードで使用できます。Cisco Spaces ユーザーの作成の詳細については、「[Cisco Spaces ユーザーの招待（357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、[Shared Access Code] タブをクリックします。

ステップ 6 [Shared Access Code] タブで、作成するアクセスコードのタイプを選択します。次のオプションがあります。

- [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でき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 ヶ月間有効です。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 7 [作成 (Create)] をクリックします。

使い捨てアクセスコードを作成する

[アクセスコードの作成 (Create Access Code)] ウィンドウで、[一回限りのアクセスコード (Single Use Access Code)] オプションを選択して、ワンタイムのアクセスコードを作成します。

選択したロケーションの定義済みテンプレートを作成するには、[設定 (Settings)] > [アクセスコードテンプレート (Access Code Template)] にある [アクセスコードテンプレートの有効化 (Enable Access Code Template)] チェックボックスをオンにします。

このオプションが有効になっている場合は、最初にテンプレート（ロケーションで使用可能）を選択してから、使い捨てアクセスコードを作成します。



(注) Cisco Spaces : キャプティブポータル アプリケーションの **[設定 (Settings)]** > **[アクセスコードテンプレート (Access Code Templates)]** で **[アクセスコードテンプレートの有効化 (Enable Access Code Template)]** チェックボックスがオフになっている場合、現在のアクセスコード作成プロセスに変更はありません。

使い捨てのアクセスコードを作成するには、次の手順を実行します。

手順

ステップ 1 Cisco Spaces ダッシュボードで、**[キャプティブポータル (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)

[アクセスコード (Access Code)] オプションは、Cisco Spaces アカウント管理者またはアクセスコードマネージャのユーザーのみが、Cisco Spaces ダッシュボードで使用できます。Cisco Spaces ユーザーの作成に関する詳細は、「[Cisco Spaces ユーザーの招待 \(357 ページ\)](#)」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 選択したロケーションで**アクセスコードテンプレート**を使用できる場合は、テンプレートを選択する必要があります。

- a) **[テンプレートの選択 (Choose a template)]** エリアで、アクセスコードテンプレートを選択して、新しいアクセスコードのセットを作成します。
- b) **[Next]** をクリックします。
- c) **[アクセスコードの生成 (Generate Access Code)]** エリアで、次の手順を実行します。

- **[Access code name]** : 新しい使い捨てアクセスコードの名前を入力します。
- **ロケーションの選択 (Choose Location)** : テンプレートを作成するネットワークのロケーションをドロップダウンリストから選択します。
- **アクセスコード数 (# of Access Code)** : 作成するアクセスコードの数を入力します。
- **このアクセスコードの有効期間を定義 (Define a validity period for this access code)** : チェックボックスをオンにして、カレンダーを使用して次の日付を入力し、アクセスコードの有効期間を設定します。
 - **Start Date**
 - **End Date**

ステップ 6 選択したロケーションで **アクセスコードテンプレート** を使用できない場合は、次の手順を実行します。

- a) [アクセスコードの作成 (Create Access Code)] ウィンドウで、[一回限りのアクセスコード (Single Use Access Code)] タブをクリックします。
- b) [Single Use Access Code] タブで、次の手順を実行します。
 - [Access code name] : 新しい使い捨てアクセスコードの名前を入力します。
 - [Access code type] : アクセスコードタイプを選択するには、[Numeric] または [Alphanumeric] ラジオボタンをクリックします。
 - [# of Access Code] : 作成するアクセスコードの数を入力します。デフォルト値は 1 です。
 - [# of Characters] : アクセスコードに必要な文字数を入力します。使い捨てのアクセスコードには、3 文字以上を含める必要があります。
 - [Limit session by time] : スライダーを使用して、セッションの制限時間を設定します。有効な範囲は 30 分～3 ヶ月です。
 - [Define a validity period for this access code] : カレンダーを使用して次の日付を入力し、アクセスコードの有効期間を設定します。
 - **Start Date**
 - **End Date**
 - [Limit bandwidth] : チェックボックスをオンにして、帯域幅を 1 Mbps に制限します。

ステップ 7 [Create] をクリックします。

- 生成されたアクセスコードは 1 回限りの使用です。アクセスコードが以前に使用されている場合は、次のエラーメッセージが表示されます。
`invalid access code`
- 新しいアクセスコードのステータスは、[View Access Codes] ウィンドウに [Available] と表示されます。アクセスコードを使用すると、ステータスが [Used] に変わります。
- [編集 (Edit)] をクリックして開始日と終了日を編集し、[更新 (Update)] をクリックして変更を保存します。詳細については、[アクセスコードの編集 \(176 ページ\)](#) を参照してください。

アクセスコードテンプレートの作成

アクセスコードテンプレートを使用すると、ネットワークまたは建物の場所に合わせてカスタマイズされたアクセスコードを簡単かつ迅速に生成できます。

選択したネットワークまたは建物の場所のアクセスコードテンプレート機能を有効にするには、[設定 (Settings)] > [アクセスコードテンプレート (Access Code Templates)] タブで [アクセスコードテンプレートの有効化 (Enable Access Code Template)] チェックボックスをオンにします。

アクセスコードテンプレート機能を有効にすると、新しいアクセスコードテンプレートを作成した後、選択したテンプレートに基づいて一回限りのアクセスコードを作成できます。



(注) この機能は一回限りのアクセスコードにのみ適用され、最大制限数に基づいて設定できます。特定のロケーションに対してテンプレートが作成されていない場合は、アクセスコードを作成する従来の方法が使用されます。

手順

ステップ 1 Cisco Spaces ダッシュボードで、[メニュー (Menu)] アイコンをクリックし、[ホーム (Home)] > [SMART VENUES] > [キャプティブポータル (Captive Portals)] アプリケーションタイトルを選択します。

オプションで、[ダッシュボード (Dashboard)] ドロップダウンリスト (Cisco Spaces [ホーム (Home)] ウィンドウの左側のナビゲーションペイン) から [キャプティブポータル (Captive Portals)] を選択します。

[ポータル (Portal)] ウィンドウが表示されます。左側のナビゲーションペインでは、**キャプティブポータル** アプリケーションの使用可能なタブを表示できます。

ステップ 2 左側のナビゲーションペインで [設定 (Settings)] をクリックします。

[設定 (SETTINGS)] ウィンドウには、[SMSゲートウェイ (SMS Gateway)]、[ソーシャルアプリケーション (Social Apps)]、[アクセスコードテンプレート (Access Code Templates)]、および [信頼できるデバイステンプレート (Trusted Devices Templates)] の 4 つのタブが表示されます。

ステップ 3 [アクセスコードテンプレート (Access Code Templates)] をクリックします。

ステップ 4 アクセスコードテンプレートを作成する設定を有効にするには、[アクセスコードテンプレートの有効化 (Enable Access Code Template)] チェックボックスをオンにします。

[テンプレートの作成 (Create Template)] オプションが表示されます。有効にすると、アクセスコードは事前定義されたテンプレートを使用した場合のみ生成できるようになるため、標準化された安全なプロセスが保証されます。これは、一回限りのアクセスコードを作成するときのみ適用されます。

ステップ 5 選択したロケーションの定義済みテンプレートを作成するには、[テンプレートの作成 (Create Template)] をクリックします。

[アクセスコードテンプレートの作成 (Create Access Code Template)] ウィンドウが表示されます。

ステップ 6 一回限りのアクセスコードを生成するための新しいテンプレートを作成するには、次の手順を実行します。

- **テンプレート名 (Template Name)** : 一回限りの新しいアクセスコードテンプレートの名前を入力します。
- **ロケーションの選択 (Choose Location)** : テンプレートを作成するネットワークのロケーションをドロップダウンリストから選択します。
- **アクセスコードタイプ ([Access code type])** : アクセスコードタイプを選択するには、[数字 (Numeric)] または [英数字 (Alphanumeric)] ラジオボタンをクリックします。

- **文字数 (# of Characters)** : 作成するアクセスコードの文字数を入力します。
- **[Limit session by time]** : スライダーバーを使用して、セッションの制限時間を設定します。有効な範囲は 30 分～3 ヶ月です。
- **[Limit bandwidth]** : チェックボックスをオンにして、帯域幅を 1 Mbps に制限します。
- **このアクセスコードの有効期間を定義 (Define a validity period for this access code)** : チェックボックスをオンにして、カレンダーを使用して次の日付を入力し、アクセスコードの有効期間を設定します。
 - **Start Date**
 - **End Date**
- **このアクセスコードの有効期間を定義 (Define a validity period for this access code)** :
- **アクセスコードの一括作成を許可 (Allow bulk access code creation)** : チェックボックスをオンにして、一括作成を許可するアクセスコードの制限を入力します。

ステップ 7 [作成 (Create)] をクリックします。

作成された新しいテンプレートは、[アクティブテンプレート (Active Template)] エリアに表示されます。

次のタスク

[アクセスコード (Access Code)] ウィンドウに移動し、テンプレートを選択して、一回限りのアクセスコードを作成できます。

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。

手順

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、[#unique_202](#)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とも、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。

手順

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、[#unique_202](#)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。

手順

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、[#unique_202](#)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。

手順

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、[#unique_202](#)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。

手順

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、[#unique_202](#)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。

手順

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、[#unique_202](#)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。

手順

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、[#unique_202](#)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。

手順

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。

信頼できるデバイス

アクセスコードマネージャには次の機能があります。

- 管理者は、リストを信頼し、ダッシュボードを使用して、デバイスを直接導入準備できます。
- Cisco Spaces RADIUS エンジンを経由したオンボーディングテンプレートと認証プロファイルの適用を自動化します
- 大規模なデバイスアクセスのプロビジョニング、モニタリング、管理を合理化します。

Cisco Spaces ダッシュボードでは、アクセスコードマネージャ機能により、信頼できるデバイスのオンボーディングと管理が改善されました。管理者は、ダッシュボードから直接デバイスを信頼できるようになり、コントローラを手動で設定したり、複数のシステムにログインしたりする必要がなくなりました。ダッシュボードでは、キャプティブ ポータル ブラウザを使用しないデバイスがサポートされているため、安全なオンボーディングが可能になり、管理者は設定可能なテンプレートを使用してセッション期間と帯域幅制限を設定できます。

ダッシュボードで作成されたオンボーディング テンプレートと認証プロファイルが、Cisco Spaces RADIUS エンジンによって自動的に解釈および適用されるようになり、環境全体での一貫性が維持されます。デバイスのオンボーディングステータスとポリシー適用がリアルタイムで監視できるため、必要に応じて迅速な検証とトラブルシューティングが可能です。

テンプレート管理

管理者が再利用可能なテンプレートを作成、更新、廃止し、ロケーションまたは SSID によりテンプレートを割り当て、組み込みの予防対策とデバイスの関連付けを維持することで、テンプレート管理が合理化されます。ゲストの滞在や運用ポリシーに合わせて、必要に応じてデバイスのアクセスをプロビジョニングまたは取り消すことができます。MAC アドレス検証機能と集中監査機能の向上により、ネットワークセキュリティが強化されています。

これらの更新により、デバイスのオンボーディングと管理がより効率的かつ安全になり、Cisco Spaces の展開全体で大規模な運用ニーズがサポートされるようになりました。

サマリーセクション

[信頼できるデバイス (Trusted Devices)] ウィンドウには、追加されたデバイス数、アクティブなデバイス数、期限切れのデバイス数など、デバイスの要約が表示されます。

デバイスセクション

デバイスを信頼できるものとして追加するには、テンプレートが必要です。作成されたテンプレートがない場合は、[設定 (Settings)] > [信頼できるデバイスのテンプレート (Trusted Devices Templates)] に移動し、新しいテンプレートを作成します。

テンプレートがすでに使用可能な場合は、[+新しいデバイス (+New Devices)] をクリックして新しいデバイスを信頼できるデバイスとして追加します。

[デバイス (Devices)] セクションには、[期限切れのデバイス (Expired Devices)] と [アクティブなデバイス (Active Devices)] の 2 つのオプションがあります。すべてのデバイスが期限切れステータスの場合、[アクティブなデバイス (Active Devices)] オプションは [新しいデバイス (+New Devices)] に切り替わります。[検索 (Search)] フィールドを使用して、デバイスの詳細を検索します。

Figure 14: 信頼できるデバイス

Label	Template	Mac Address	Last Connected	Valid Till	Added By	Actions
Test	doc	01:23:45:67:89:AB	Never	21/10/2025, 13:00:13	jicisco.com	Edit Delete
Device 2	doc	00:1A:2B:3C:4D:5E	Never	21/10/2025, 13:00:58	ico.com	Edit Delete

[期限切れのデバイス (Expired Devices)] をクリックして、[期限切れのデバイス (Expired Devices)] セクションと期限切れデバイスの詳細を表示します。次の情報を表示できます。

- ラベル
- テンプレート
- MAC アドレス (MAC Address)
- 有効期限の終了
- 追加者
- アクション

[エクスポート (Export)] をクリックして、デバイスの詳細を CSV 形式でエクスポートします。

**Note**

この機能を使用するには、レイヤ2 キャプティブポータルを設定し、RADIUS をコントローラと統合します。

テンプレートの作成

デバイスがキャプティブポータルワークフローをバイパスできるようにします。これは、キャプティブポータルをサポートしていないデバイスで役立ちます。

信頼できるデバイステンプレートを作成して、キャプティブポータルの制限から除外するデバイスを定義します。

Procedure

ステップ 1 Cisco Spaces ダッシュボードで、[メニュー (Menu)] アイコンをクリックし、[ホーム (Home)] > [SMART VENUES] > [キャプティブポータル (Captive Portals)] アプリケーションタイトルを選択します。

オプションで、[ダッシュボード (Dashboard)] ドロップダウンリスト (Cisco Spaces [ホーム (Home)] ウィンドウの左側のナビゲーションペイン) から [キャプティブポータル (Captive Portals)] を選択します。

[ポータル (Portal)] ウィンドウが表示されます。左側のナビゲーションペインでは、**キャプティブポータル** アプリケーションの使用可能なタブを表示できます。

ステップ 2 左側のナビゲーションペインで [設定 (Settings)] をクリックします。

[設定 (SETTINGS)] ウィンドウには、[SMSゲートウェイ (SMS Gateway)]、[ソーシャルアプリケーション (Social Apps)]、[アクセスコードテンプレート (Access Code Templates)]、および [信頼できるデバイステンプレート (Trusted Devices Templates)] の3つのタブが表示されます。

ステップ 3 [信頼できるデバイステンプレート (Trusted Devices Templates)] をクリックします。

ステップ 4 テンプレートを作成するには、[テンプレートの作成 (Create Template)] をクリックします。

[テンプレートの作成 (Create Template)] ウィンドウが表示されます。

Figure 15: テンプレートの作成

Create Template



Enable devices to bypass the Captive portal workflow. Useful for devices not supporting Captive portals

Template Name

Choose Location

Choose SSID

☐ Limit Validity☐ Limit Bandwidth[Cancel](#)[Create](#)

ステップ 5 [テンプレートの作成 (Create Template)] ウィンドウで、次のパラメータを入力します。

- [テンプレート名 (Template Name)] : テンプレートの名前を入力します。
- [ロケーションの選択 (Choose Location)] : [ロケーションの選択 (Choose Location)] ドロップダウンリストからロケーションを選択します。
- [SSIDの選択 (Choose SSID)] : [SSIDの選択 (Choose SSID)] ドロップダウンリストから SSID を選択します。
- [有効期限 (Limit Validity)] : 有効性を制限するには、[有効期限 (Limit Validity)] チェックボックスをオンにして、スライダーで期限を設定します。有効な範囲は 30 分～2 ヶ月 (約 60 日間) です。
- [帯域幅の制限 (Limit Bandwidth)] : 帯域幅を制限するには、[帯域幅の制限 (Limit Bandwidth)] チェックボックスをオンにして、スライダーで帯域幅を設定します。帯域幅は 50 KB/秒 (kbps) ～無制限です。

ステップ 6 [作成 (Create)] をクリックします。

新しいテンプレートが正常に作成され、[設定 (Settings)] > [信頼できるデバイステンプレート (Trusted Device Templates)] タブに表示されました。

What to do next

テンプレートを選択して、デバイスを追加できます。

デバイスの追加

デバイス管理用に信頼できるデバイスをキャプティブポータルに追加します。

このタスクで、MAC アドレスを使用してキャプティブポータルに新しいデバイスを追加します。

Before you begin

追加するすべてのデバイスの MAC アドレスを持っていることを確認します。

Procedure

ステップ 1 Cisco Spaces ダッシュボードで、[メニュー (Menu)] アイコンをクリックし、[ホーム (Home)] > [SMART VENUES] > [キャプティブポータル (Captive Portals)] アプリケーションタイルを選択します。

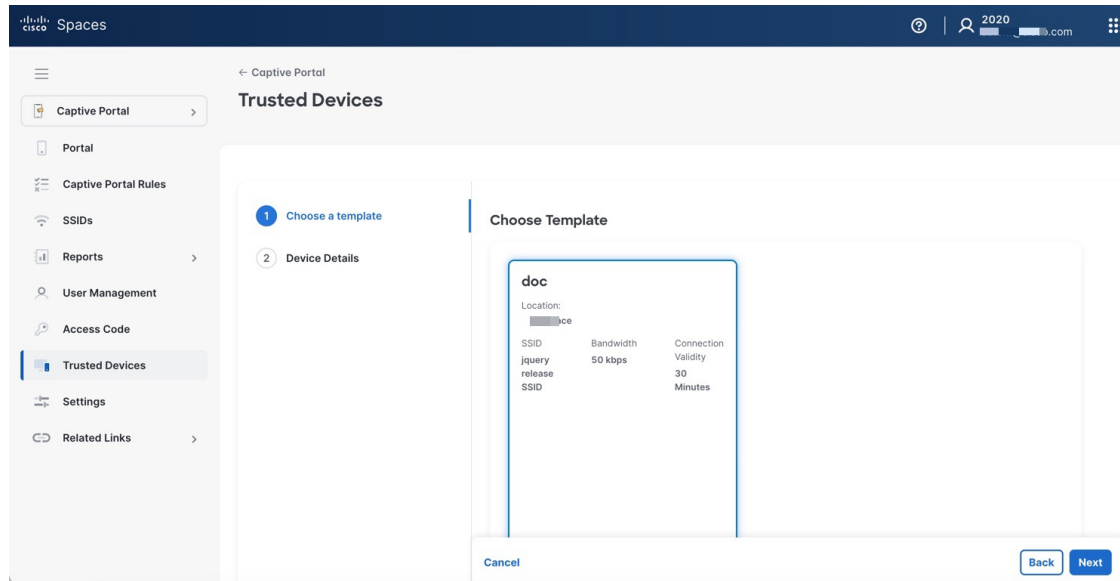
オプションで、[ダッシュボード (Dashboard)] ドロップダウンリスト (Cisco Spaces [ホーム (Home)] ウィンドウの左側のナビゲーションペイン) から [キャプティブポータル (Captive Portals)] を選択します。

[ポータル (Portal)] ウィンドウが表示されます。左側のナビゲーションペインでは、**キャプティブポータル** アプリケーションの使用可能なタブを表示できます。

ステップ 2 左側のナビゲーションペインで、[信頼できるデバイス (Trusted Devices)] をクリックします。

ステップ 3 [信頼できるデバイス (Trusted Devices)] ウィンドウで、[+新しいデバイス (+New Devices)] をクリックします。

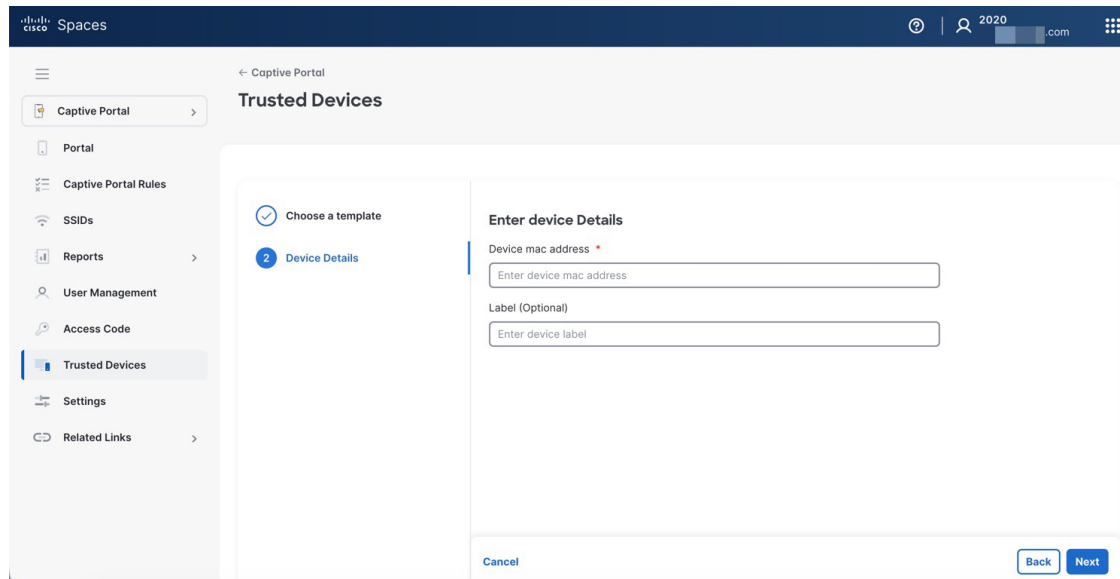
Figure 16: デバイスを追加する。



ステップ 4 テンプレートを選択し、[次へ (Next)] をクリックします。

ステップ 5 [デバイスの詳細 (Device Details)] セクションでは、デバイスの MAC アドレスを入力し、ラベルの説明を入力します。デバイスの MAC アドレスは必須です。

Figure 17: デバイスの詳細の追加



ステップ 6 [次へ (Next)] をクリックして、新しい信頼できるデバイスを追加します。
新しく信頼できるデバイスが正常に保存されたことを示す成功メッセージが表示されます。

新しい信頼できるデバイスの詳細が、[デバイス (Device)] セクションの下にある[信頼できるデバイス (Trusted Devices)] ウィンドウに表示されます。

What to do next

続行して複数の信頼できるデバイスを追加したり、既存のデバイスの詳細を編集したりできます。[編集 (Edit)] (鉛筆アイコン) を使用してデバイスの詳細を更新するか、[削除 (Delete)] (ゴミ箱アイコン) を使用してデバイスを削除します。

設定

Cisco Spaces : キャプティブポータルアプリケーションの[設定 (Settings)] ウィンドウには、次のタブが含まれます。

- **SMSゲートウェイ (SMS Gateway)** : SMS を介してユーザーに關与するための SMS ゲートウェイを設定します。SMS 認証を使用する場合に必須です。
デフォルトゲートウェイは有料で利用できます。ただし、SMSゲートウェイをすでに導入している場合は、Cisco Spaces : キャプティブポータル と統合できます。
- **ソーシャルアプリケーション (Social Apps)** : ソーシャルメディアアプリケーションを追加します。
- **アクセスコードテンプレート (Access Code Template)** : テンプレートを有効にして作成し、デバイスを関連付けます。
- **信頼できるデバイス (Trusted Devices)** : アクセスコードマネージャ機能により、信頼できるデバイスのオンボーディングと管理を行います。

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。

手順

- 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
- NYNEX
- 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。

手順

-
- 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

一時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。

手順

-
- 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。

手順

-
- 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。

手順

-
- 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。

手順

- 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、ロケーションパーソナルルール、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。

手順

- ステップ 1** [Add Locations] ボタンをクリックします。

特定のメタデータのロケーションにルールを適用する

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 [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。

手順

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 [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。

手順

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スマートリンクとテキスト変数 \(215 ページ\)](#) 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スマートリンクとテキスト変数 \(215 ページ\)](#) 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スマートリンクとテキスト変数 \(215 ページ\)](#) 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スマートリンクとテキスト変数 \(215 ページ\)](#) 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 \(125 ページ\)](#)

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 \(49 ページ\)](#)
- [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 \(38 ページ\)](#)

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。

手順

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 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。

手順

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

手順

- 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。

手順

- 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。

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 10:

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

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)
iPhone 6 Plus	9.3.2	CNA、Safari
Huawei Honor	6.0.1 および 6.0	Google Chrome
Huawei P8	5.0.1	Google Chrome
Microsoft Lumia 950	Windows 10	CNA およびネイティブブラウザ
Nokia Lumia 1320	Windows 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 El Capitan 10.11.6	CNA
Macbook Pro 13-inch Retina display	Mac OS X El Capitan 10.11.6	CNA

Cisco 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 \(121 ページ\)](#)」を参照してください。顧客は、利用規約への同意、SMS による検証、電子メールによる検証、またはソーシャル認証の使用を含む認証手順を実行する必要があります。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 \(204 ページ\)](#)」を参照してください。必要な認証手順が完了すると、Cisco Spaces が、当該のデバイスにインターネットをプロビジョニングするよう、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 ウィンドウは終了して、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) iOS 11.0 ~ 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。

CNA が無視され、Mobile Safari または Chrome 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ガーデン範囲にない) URL にアクセスした場合、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。顧客がポータルのメニューまたはリンクをクリックすると、[ログイン (Login)] 画面が表示されます。顧客は認証手順を完了して、インターネットをプロビジョニング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、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、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 \(129 ページ\)](#) 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。この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 が

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 \(121 ページ\)](#) 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、SMS 認証、E メール認証、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 \(204 ページ\)](#) を参照してください。必要な認証手順が完了すると、Cisco Spaces が、当該のデバイスにインターネットをプロビジョニングするよう、ワイヤレスネットワーク (CUWN, Meraki) に要求を送信します。インターネットが正常にプロビジョニングされると、CNA ウィンドウが閉じます。

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。顧客がポータルのメニューまたはリンクをクリックすると、[ログイン (Log in)] 画面が表示されます。インターネットアクセスをプロビジョニングするには、顧客が前述の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行われると、顧客が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、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 \(129 ページ\)](#) 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。この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、デバイスで生成される 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 \(121 ページ\)](#) 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、SMS 認証、Email 認証、またはソーシャル認証を含む場合があります。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（204 ページ）](#)を参照してください。顧客が認証を完了すると、Cisco Spacesがワイヤレスネットワーク（CUWN、Meraki）に対してこのデバイスのインターネットアクセスを提供するように要求を送信します。インターネットアクセスが正常に提供されると、顧客が以前にクリックしたメニューまたはリンクの Web ページが同じブラウザに表示されます。



(注) インターネットアクセスがプロビジョニングされた後、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を移動できます。



(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（129 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（121 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、Eメール認証、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（204 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 Spaces が、当該のデバイスにインターネットアクセスをプロビジョニングするように、ワイヤレスネットワーク（CUWN、Meraki）に要求を送信します。インターネットが正常にプロビジョニングされると、CNA ウィンドウが閉じます。



(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 \(129 ページ\)](#)」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 に接続した後で、許可リストにならない（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 に対す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 \(121 ページ\)](#)」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、E メール 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 \(204 ページ\)](#)」を参照してください。必要な認証手順が完了すると、Cisco Spaces が、当該のデバイスにインターネットをプロビジョニングするよう、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 ページが同じブラウザに表示されます。

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 \(121 ページ\)](#)」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、E メール 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 \(204 ページ\)](#)」を参照してください。必要な認証手順が完了すると、Cisco Spaces が、当該のデバイスにインターネットをプロビジョニングするよう、ワイヤレスネットワーク（CUWN, Meraki）に要求を送信します。インターネットアクセスがプロビジョニングされると、CNA ウィンドウは閉じます。



- (注) インターネットアクセスがプロビジョニングされた後、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を移動できます。



- (注) インターネットプロビジョニング中にエラーが発生すると、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 \(129 ページ\)](#)」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 \(121 ページ\)](#)」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、SMS 認証、E メール認証、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 \(204 ページ\)](#)」を参照してください。必要な認証手順が完了すると、Cisco 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。顧客が選択したページに加えて、ブラウザで CNA のホームページを含む別のタブが開きます。

あるいは、顧客は、キャプティブポータルのウィンドウを終了して、そのままブラウザを使用することもできます。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 \(129 ページ\)](#)」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。

手順

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、携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 \(206 ページ\)](#) 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、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ーの認証手順は、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。

手順

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)

同じ携帯電話番号を使用して複数のデバイスを接続できますが、新しいデバイスを接続するたびに、以前のユーザーアイデンティティが添付されます。

ただし、OTP を入力できるのは 1 分間に 3 回までです。3 回試行すると、それ以上のログイン試行は一時的に制限されます。

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 によるリピーターユーザーの認証手順

さまざまなシナリオでのリピーターユーザーの認証手順は、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、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。
- **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。

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。

手順

- 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、リピーター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 認証によるリピーター ユーザーの認証手順

Cisco Spaces では、新しいユーザーの認証ワークフローの一環として、電子メールアドレスを一度だけ入力する必要があります。ドメイン関連のすべての検証と MX レコードのチェックは特定の期間キャッシュされ、キャッシュされている期間内の同じドメインの他のユーザーに対して同じチェックが繰り返されることはありません。

たとえば、10 人のユーザーがキャプティブポータルに同時に接続し、同じドメイン (xyz@abc.com) に属する電子メールアドレスを入力した場合、ドメイン検証と MX レコードチェックは、指定されたキャッシング期間中に一度だけ実行されます。ただし、ユーザー ID が有効かどうかを検証するために、10 人のユーザーすべてに対して SMTP 接続とメールボックスのチェックが実行されます。

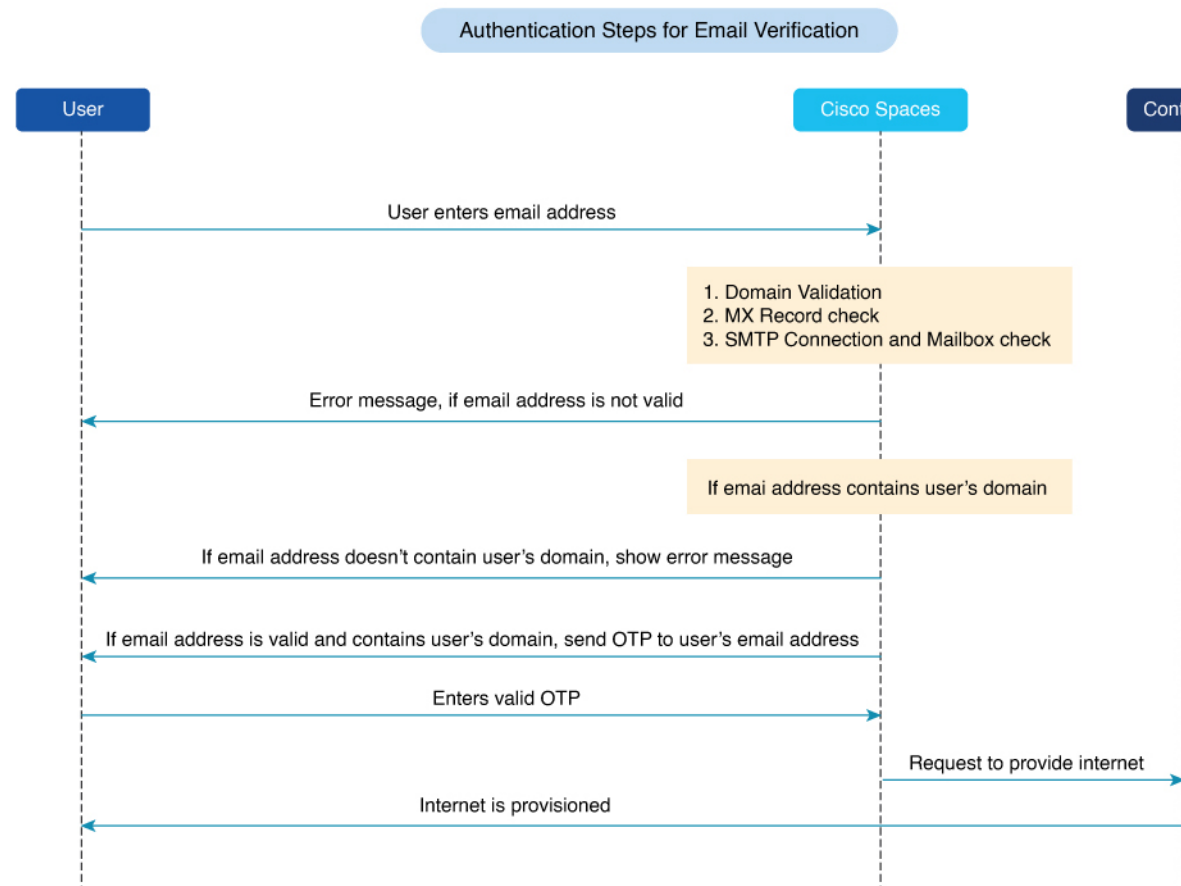
SMTP 接続を確立するには、次の手順を実行します。

1. SMTP サーバーへのソケット接続を確立し、応答を確認します。
2. **ELHO** コマンドを実行し、応答を確認します。
3. **MAIL FROM** コマンドを実行し、応答を確認します。
4. **RCPT TO** コマンドを実行し、応答を確認します。



(注) キャプティブポータルの新規ユーザーオンボーディングワークフローの一環として、ユーザーの電子メールアドレスが一度だけ記録されます。Cisco Spaces がメールボックスチェックから応答を受信しなかった場合でも、Cisco Spaces への認証が許可されます。ただし、次のアクセス時に電子メールアドレスを再度入力する必要があります。メールボックスチェックプロセスの一環として、Cisco Spaces では、ユーザーが指定した電子メールアドレスに電子メール要求が送信されることはありません。

図 18: 認証ワークフロー



認証シナリオ

さまざまなシナリオでのリピーターユーザーの認証手順は、次のとおりです。

- **前回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がロードされ、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、有効な電子メール ID を入力する必要があります。

- **データキャプチャが有効でない場合**：キャプティブポータルがロードされ、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。
- **データキャプチャが有効で、顧客が登録を完了した場合**：キャプティブポータルがロードされ、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。
- **データキャプチャが有効で、登録情報が古くなっている場合**：キャプティブポータルがロードされ、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。フォームを更新し、[接続 (Connect)] をクリックすると、インターネットにアクセスできます。

登録情報

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、データキャプチャフォームを[性別 (Gender)] フィールドなしで設定した場合です。登録プロセスを完了します。その後、データキャプチャフォームに[性別 (Gender)] フィールドを必須フィールドとして追加しました。
- **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、<Last Name> を任意にしてデータキャプチャフォームを設定した場合です。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、フォームで姓を必須としました。
- **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、**Age Criteria (年齢基準)** という必須のビジネスタグを **Child** および **Adult** という選択肢で設定した場合です。顧客は **Age Criteria** に **Child** を選択して登録を完了しました。その後、選択肢の表示を **Kids** と **Adult** に変更しました。



- (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、[規約を承認し続行 (Accept Terms and Continue)] オプションが表示されます。インターネットにアクセスするか、次の認証手順に進むには、[規約を承認し続行 (Accept Terms and Continue)] オプションをクリックする必要があります。

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。

手順

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 [ログイン (Log In)] ウィンドウで、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 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。

- 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。
- 時間によるセッションの制限** または **帯域幅の制限** を設定する必要がある場合は、ネットワーク用に Cisco Spaces Radius サーバーを設定していることを確認してください。Cisco Spaces RADIUS サーバーをセットアップするには、「[RADIUS 認証用の Cisco Meraki の設定](#)」および「[インターネットプロビジョニングおよび RADIUS 認証用のシスコ ワイヤレス コントローラの設定](#)」を参照してください。

アクセスコード認証によるリピーターユーザーの認証手順

さまざまなシナリオでのリピーターユーザーの認証手順は、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、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。
- **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。

手順

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。

手順

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 \(125 ページ\)](#) 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 \(194 ページ\)](#) 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ター ユーザーの認証手順

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

スマートリンクオプションにより、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ー別またはユーザー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。オプトインユーザー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、オプトインユーザー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ケーションで、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。

- ポータルのカスタム 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 [メッセージ (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 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取得します。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 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、静的変数と動の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 11: 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。
\$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。
これらの変数は Welcome モジュールには適用されませんが、カスタム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、次の動変数を含めることができます。

表 12: 動変数一覧

動変数名	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定義または編集 」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。

手順

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 [変数の追加 (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 20 章

Cisco Spaces : Engagements（エンゲージメント）アプリケーション

Cisco Spaces は、Cisco Spaces に対応した施設内にいる顧客を識別する Wi-Fi 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（220 ページ）](#)
- [エンゲージメント ルールの作成（220 ページ）](#)
- [エンゲージメントルールの管理（228 ページ）](#)
- [エンゲージメント ルール レポート（231 ページ）](#)
- [訪問者エンゲージメント（232 ページ）](#)
- [エンゲージメント URL（233 ページ）](#)
- [以前の訪問の条件（233 ページ）](#)
- [通知タイプ（234 ページ）](#)
- [通知の頻度（234 ページ）](#)
- [エンゲージメントルールのロケーションフィルタ（235 ページ）](#)
- [消費者用の通知タイプ（236 ページ）](#)
- [ビジネスユーザーの通知タイプ（237 ページ）](#)

- [通知のためのトリガー API の設定 \(241 ページ\)](#)

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 \(48 ページ\)](#) 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 \(43 ページ\)](#) 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](#)
 - [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 \(ローカルモード\)](#)
 - [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 \(フレックスモードまたは Mobility Express\)](#)
- 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 \(257 ページ\)](#) 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、[#unique_249](#)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 \(129 ページ\)](#) 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。

手順

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、[#unique_252](#)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 \(236 ページ\)](#) 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。

手順

- 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。

ビジネスユーザー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。

ビジネスユーザーまたは外部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。

手順

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] 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、[#unique_252](#)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 \(237 ページ\)](#) 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 ユーザーです。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ー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。

手順

- 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。

手順

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。

手順

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。

手順

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。

手順

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。

手順

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。

手順

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。ルールがバ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 \(231 ページ\)](#) 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内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内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. [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. [Done] をクリックします。選択したメタデータと変数の詳細が、[Filter by Metadata] 領域に表示されます。

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で、メタデータ変数を選択します。

4. [Done] をクリックします。選択したメタデータが [Filter by Metadata] 領域に表示されます。

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、「[スマートリンクとテキスト変数](#)」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 \(233 ページ\)](#) 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、「[スマートリンクとテキスト変数](#)」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 \(233 ページ\)](#) 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、「[スマートリンクとテキスト変数](#)」の項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 \(233 ページ\)](#) 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、「[スマートリンクとテキスト変数](#)」の項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。



(注) [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、「[スマートリンクとテキスト変数](#)」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 の設定の詳細については、[エンゲージメント URL \(233 ページ\)](#) 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APIURI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 13: 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。
\$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。

静的変数名	説明
\$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 14: 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定義および編集 」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。

手順

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、電話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 \(215 ページ\)](#) 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 Smart Link とテキスト変数 \(238 ページ\)](#) を参照してください。



第 21 章

Cisco Spaces : ロケーションペルソナアプリケーション

Cisco 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 Spaces ルールでこれらのタグを使用できます。Cisco Spaces では、ロケーションペルソナ (Location Personas) アプリケーションを使用してタグを作成できます。また、Location Personas アプリケーションを使用して、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。

- [タグの作成または変更 \(243 ページ\)](#)
- [使用例：ロケーションペルソナルール \(プロファイルルール\) \(246 ページ\)](#)
- [ロケーションペルソナルールの管理 \(250 ページ\)](#)
- [ロケーション ペルソナルール レポート \(252 ページ\)](#)

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。

手順

- 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、[ロケーションパーソナルルールのロケーションフィルタ（249 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。

- 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（248 ページ）](#) を参照してください。

- 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、[#unique_277](#)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)

プロフィー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、プロフィー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ルール (プロフィールルール)

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。

手順

- 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、プロフィー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処理

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。

手順

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。

手順

-
- 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。

手順

-
- 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。

手順

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 [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。

手順

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。

ロケーションパーソナルールの管理

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。

手順

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。

手順

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。

手順

- 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。

手順

- 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パー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パーソナルールを削除するには、削除するロケーションパー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パーソナルールの表示

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パーソナルールを表示するには、次の手順を実行します。

手順

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 ロケーションパー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パー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 パーソナルール レポート

ロケーション パーソナルール レポートには、ロケーションパー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パー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。

手順

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 **V** 部

ロケーション階層

- [Cisco DNA Spaces](#) におけるロケーション階層 (257 ページ)
- [ロケーション階層の定義](#) (261 ページ)
- [ロケーション階層の管理](#) (277 ページ)



第 22 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 \(257 ページ\)](#)
- [ロケーション階層を定義するための前提条件 \(259 ページ\)](#)
- [ロケーション階層での累積数の表示 \(260 ページ\)](#)

ロケーション階層の概要

Cisco 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一構造のロケーションをインポートできます。

Cisco Spaces の顧客にはそれぞれデフォルトの顧客名（ルート名）が提供され、この顧客名は Cisco 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 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、ロケーションパーソナル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 Catalyst 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 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

ロケーション階層は Meraki MT をサポートします。MT センサーからデータを受信するために必要な構成は、**Cisco Spaces** と Meraki の統合を使用して更新されます。MT センサーは**ロケーション階層**に自動的にインポートされます。

Cisco Meraki のロケーション階層でサポートされているデバイスのリストは次のとおりです。

- アクセスポイントモデル：MR、Z1、CW、VMR
- カメラモデル：MV
- センサーモデル：MT
- セキュリティアプライアンスモデル：MX、Z3

Cisco Meraki ネットワークのインポート

Cisco Spaces タグを持つ Cisco Meraki ネットワークは、バックグラウンド同期プロセスの実行中に **Cisco Spaces** の**ロケーション階層**に自動的にインポートされます。これらのタグ付きネットワークの自動インポートをサポートするには、Meraki 組織が**ロケーション階層**に存在する必要があります。**Cisco Spaces**は、Cisco Meraki ネットワークに追加されたタグ名である必要があります。



- (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 Spaces** の顧客は、**Cisco Prime Infrastructure** ベースのマップから **Catalyst Center** ベースのマップに **Cisco Spaces** で移行できます。**ロケーション階層**と既存の **Cisco 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推奨するのは、**Cisco 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、問題なくデータが引き継がれるようにすることです。
 - マップを操作するときは、**Google Chrome** ブラウザを使用することをお勧めします。マップの操作は、**Google Chrome** で最もよくサポートされています。他のブラウザでのマップアクションは制限されています。

Cisco Smart ワークスペース サポート

Cisco Smart ワークスペースのユースケースをサポートするために、次の新機能がロケーション階層に導入されました。

次のロケーション階層のバックグラウンド同期がサポートされるようになりました。

- Meraki ネットワークまたはフロアロケーションでの Meraki MT センサーデバイスの同期。
- Cisco Webex デバイスと会議室およびデスクとの同期。



- (注) バックグラウンド同期プロセス中に、構成テンプレートネットワークの Meraki スキャン API 通知 URL が自動的に更新されます。

Meraki ネットワーク向けカメラゾーンのサポート

Meraki にカメラゾーンを持つ新しく追加されたネットワークの場合、ゾーンがネットワークとともに [ロケーション階層 (Location Hierarchy)] に追加されます。

既存のネットワークの場合、Meraki で追加、変更、または削除されたカメラゾーンは、バックグラウンド同期プロセス中に [Location Hierarchy] と同期されます。



- (注) 現在、Cisco Spaces ダッシュボードにカメラゾーンを表示する GUI サポートは利用できません。

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 \(45 ページ\)](#)
- [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 \(38 ページ\)](#)
- [Cisco WLC Direct Connect を使用して Cisco Spaces をシスコ ワイヤレス コントローラに接続する \(41 ページ\)](#)
- [Cisco WLC Direct Connect を使用した Cisco 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 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 Cisco Spaces : コネクタ を使用して接続する](#)

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子ロケーションの 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。特定のテナントアカウントの管理ユーザーの合計数は、[ユーザー (Users)] セクションの下に表示されます。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 23 章

ロケーション階層の定義

- [ロケーション階層の定義 \(261 ページ\)](#)

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 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 Spaces では Cisco-DNASpaces タグのみがサポートされています。

Cisco 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 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 Spaces タグの付いていない AP は、次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 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 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。

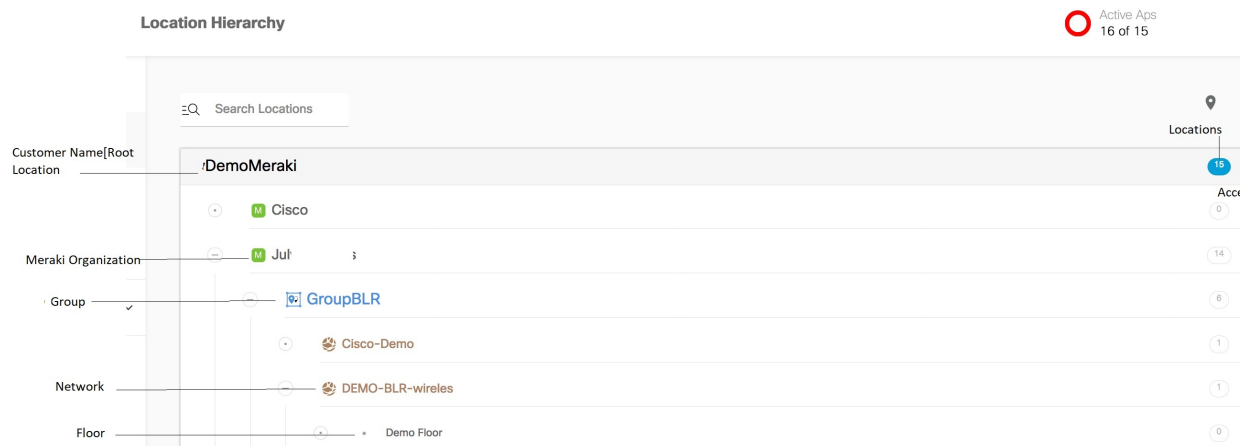
ロケーション階層を作成する前に、すべての前提条件が満たされていることを確認してください。ロケーション階層を作成するための前提条件については、[ロケーション階層を定義するための前提条件](#)（259 ページ）を参照してください。

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 19: 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](#)（265 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、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。

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。

手順

- 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ун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。

手順

- 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。

手順

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

[セットアップ (Setup)] > [ワイヤレスネットワーク (Wireless Network)] ウィンドウで、API キーを使用して Cisco Meraki のロケーションを初めてインポートします。

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。

手順

- ステップ 1** [ロケーション階層 (Location Hierarchy)] ウィンドウで、顧客名 (ルート名) の [他のアクション (More Actions)] アイコンをクリックし、次に [ワイヤレスネットワークに接続 (Connect Wireless Networks)] をクリックします。
- ステップ 2** [ワイヤレスネットワークに接続 (Connect your wireless network)] ウィンドウで、[セットアップに移動 (Go to Setup)] をクリックします。
- ステップ 3** [ワイヤレスネットワークに接続 (Connect your wireless network)] ウィンドウで、[+新規追加 (+Add New)] をクリックします。
- ステップ 4** Cisco Meraki をワイヤレスネットワークとして選択します。
ワイヤレスネットワークに [Meraki APIキーによる接続 (Connect via Meraki API Key)] が表示されます。
- ステップ 5** [接続 (Connect)] をクリックして、API キーを使用して Cisco Meraki と Cisco Spaces を接続します。
[APIキーによる接続 (Connect via API key)] ポップアップウィンドウが表示されます。
- ステップ 6** [APIキー (APIKey)] フィールドに、ネットワーク情報を取得するための Cisco Meraki API キーを入力し、[接続 (Connect)] をクリックします。
最初に、その Cisco Meraki API キーの組織のリストが表示されます。選択した組織に基づいて、ネットワークの場所が一覧表示され、選択したネットワークがロケーション階層にインポートされます。
- ステップ 7** [ポストURL (Post URL)] と [秘密鍵 (Secret Key)] パラメータを入力して、Meraki スキャン API を設定します。
- ステップ 8** [ネットワークのインポート (Import Networks)] をクリックして、Cisco Meraki ネットワークをロケーション階層にインポートします。
最初に、その Cisco Meraki API キーの組織のリストが表示されます。選択した組織に基づいて、ネットワークの場所が一覧表示され、選択したネットワークがロケーション階層にインポートされます。

インポート後、ネットワークの場所が[ロケーション階層 (Locations Hierarchy)] ウィンドウに一覧表示されます。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。

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（259 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 Map Service 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）

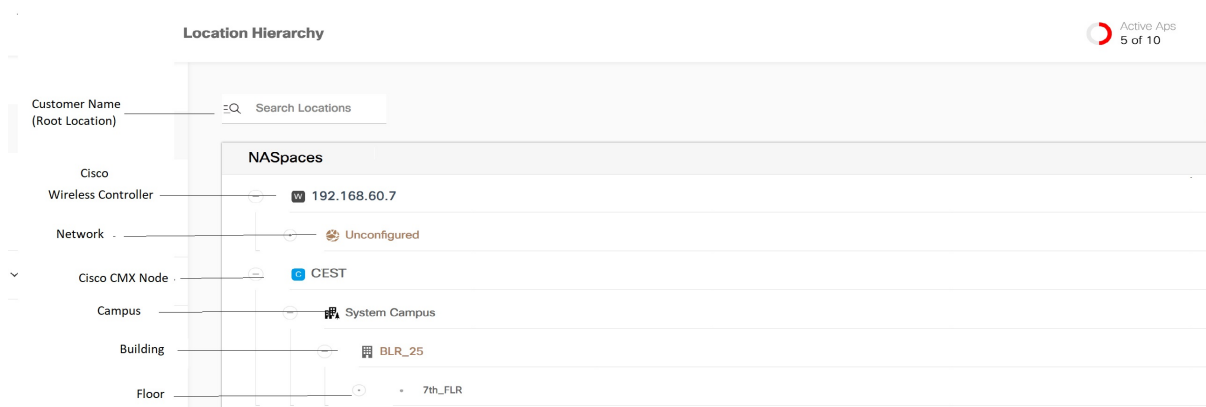


(注)

- Map Service 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、Map Service 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 20: 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、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 Cisco Spaces 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 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て、通知とレポートのロケーション更新を設定できます。

Cisco Spaces ネットワーク同期サーバーは、CMX テザリングの AP 同期をサポートするようになりました。CMX テザリングの場合、Cisco Prime の AP に加えられた変更は、Cisco Spaces 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 Infrastructure 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 Spaces の Map Service 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。

手順

-
- ステップ 1** Cisco Spaces ダッシュボードで、[セットアップ (Setup)] > [ワイヤレスネットワーク (Wireless Networks)] の順に選択します。
- 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 Spaces ダッシュボードを Cisco CMX に接続するためのトークンを生成するには、[CMX テザリング トークン (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 [キー (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 **[クラウドアプリケーション (Cloud Applications)]** ウィンドウで、**Cisco Spaces** の **[アクション (Actions)]** 列にある **[有効 (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 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 **[マップサービス (Map Service)]** ウィンドウに表示され、ロケーションが自動的に Cisco Spaces ダッシュボードの **[ロケーション階層 (Location Hierarchy)]** に表示されます。

(注)

- **[ロケーション階層 (Location Hierarchy)]** からロケーションを削除すると、**[マップサービス (Map Service)]** から削除されます。
- Cisco CMX で **Cisco Spaces** サービスを有効にするには、Cisco 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 \(291 ページ\)](#) を参照してください。
- Cisco Prime Infrastructure でのロケーションの更新を Cisco Spaces で自動的に同期するには、Cisco CMX の **[マップ同期 (Map Sync)]** ボタンをクリックする必要があります。

Map Service 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

設定は Cisco 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。

Cisco Prime Infrastructure または Catalyst Center からマップをエクスポートできます。Cisco Prime Infrastructure または Catalyst Center からエクスポートされ、**[マップサービス (Map Service)]** を使用して Cisco Spaces にインポートされたマップは、**[ロケーション階層 (Location Hierarchy)]** に自動的に表示されます。

Cisco Prime Infrastructure 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。

手順

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

ステップ 2 **[設定/スタートアップ (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 Spaces にアップロードする必要があります。

ステップ 8 Cisco Spaces ダッシュボードで、[セットアップ (Setup)] > [マップサービス (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 Spaces ダッシュボードで [ロケーション階層 (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 Spaces にインポートされたマップは、**ロケーション階層**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 \(291 ページ\)](#) を参照してください。

- Cisco Prime でのロケーションの更新を Cisco Spaces で同期するには、最新のマップを **Map Service** 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](#)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（272 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。Map Service 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、[Map Service 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（274 ページ）](#)を参照してください。



(注)

- [Access Point prefix] オプション ([Connect WLC/Catalyst 9800 Directly] または [Connect via Spaces Connector] のいずれか) を使用してロケーションを追加していた場合に、ライセンス制限に従って AP をインポートできます。
- ライセンス制限に達すると、コントローラで使用可能なライセンス制限を超える AP はロケーション階層と同期されませんでした。[Unconfigured] にある AP よりも、共通のプレフィックスを持つ AP が優先されるようになりました。[Unconfigured] にある AP は同期プロセス中に削除され、コントローラで共通のプレフィックスを持つ AP の同期が優先されます。
- 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ー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、プロキシミティー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、Map Service 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ー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、プロキシミティー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

手順

- ステップ 1 ロケーションを Cisco Spaces にインポートするには、Cisco 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 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、[次へ (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 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 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 [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、ロケーションパーソナル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 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 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 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 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るようになりました。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 \(WLC Direct Connect または Cisco DNA Spaces コネクタを使用\) \(295 ページ\)](#) を参照してください。

Map Service 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 Spaces に接続されている場合、Map Service 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 - 建物 - フロア）に場所をインポートできます。



(注) Cisco Prime Infrastructure または Catalyst Center からマップをエクスポートできます。Cisco Prime Infrastructure または Catalyst Center からエクスポートされ、[マップサービス (Map Service)] を使用して Cisco Spaces にインポートされたマップは、[ロケーション階層 (Location Hierarchy)] 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。

手順

- ステップ 1 Cisco Prime Infrastructure にログインします。
- ステップ 2 [設定/スタートアップ (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 Spaces にアップロードする必要があります。
- ステップ 9** Cisco Spaces ダッシュボードで、[セットアップ (Setup)] [マップサービス (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 Spaces ダッシュボードで [ロケーション階層 (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 Spaces にインポートされたマップは、**ロケーション階層**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] から削除されます。
- (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 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 \(291 ページ\)](#) を参照してください。



第 24 章

ロケーション階層の管理

• [ロケーション階層の管理](#) (277 ページ)

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。

手順

- 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

ワイヤレスネットワークの展開に基づいて、ワイヤレスネットワークを Cisco Spaces に接続する方法は複数あります。

Cisco 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。[ワイヤレスネットワークの接続（Connect Wireless Networks）] 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。

[ワイヤレスネットワークの接続 (Connect your wireless network)] ウィンドウで、[セットアップに移動 (Go to Setup)] をクリックして、[セットアップ (Setup)] > [ワイヤレスネットワーク (ワイヤレスネットワーク)] に移動してワイヤレスネットワークを追加します。

次のワイヤレスネットワーク オプションを使用できます。

- **AireOS コントローラ/Catalyst 9800 ワイヤレスコントローラ (AireOS Controller/Catalyst 9800 Wireless Controller)** : シスコ ワイヤレス コントローラまたは Cisco CMX オンプレミステザリングを使用する Cisco Aironet アクセスポイントの場合は、これを選択します。次の機能が含まれています。
 - Spacesコネクタ経由 (Via Spaces Connector) : コントローラを Cisco Spaces に接続するには、VM に Cisco Spaces : コネクタ をインストールする必要があります。
 - シスコ ワイヤレス コントローラを直接接続 (Connect Cisco Wireless Controllers directly) : ワイヤレスコントローラには、直接インターネット接続が必要です。Cisco AireOS ワイヤレスコントローラ リリース 8.3 以降および Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ リリース 16.10 以降が必要です。
 - CMXテザリング経由で接続 (Connect via CMX Tethering) : CMX テザリング経由で接続する場合、Cisco CMX リリース 10.6 以降のバージョンがサポートされます。
- **Cisco Meraki** : Cisco Meraki ネットワークに Cisco Meraki アクセスポイントがある場合に選択します。これには **API キーによる接続方式**が含まれます。



(注) ワイヤレスネットワークの追加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 \(261 ページ\)](#)」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。

手順

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。

手順

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 Metadata 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。

手順

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。

手順

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。

手順

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。

手順

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。

手順

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。

手順

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する必要があります。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。

手順

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。

手順

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。

手順

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。

手順

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。

手順

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 [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。

手順

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

手順

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。

手順

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。

(注)

- [Map Service] UI からゾーンのロケーションを削除すると、同じものが [Location Hierarchy] から削除されます。
- 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。

次のタスク

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。

手順

- 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。

手順

- 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。

手順

-
- 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。

手順

-
- 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。

手順

-
- 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。

手順

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。

手順

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。

手順

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。

手順

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

手順

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。

手順

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。

手順

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。

手順

-
- 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。

手順

-
- 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。

手順

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、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 (WLC Direct Connect 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。

手順

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 [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。

手順

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 \(297 ページ\)](#) を参照してください。

ステップ 6 [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。

手順

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。

手順

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。

手順

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。

手順

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。



第 **VI** 部

ロケーション階層 2.0

- [ロケーション階層](#) (303 ページ)



第 25 章

ロケーション階層

Cisco Prime Infrastructure または Catalyst 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ロケーション階層に反映されます。

[ロケーション階層 (Location Hierarchy)] ウィンドウでは、デフォルトの顧客名 (ルートロケーション) が自動的に選択され、[マップ (Map)] タブにはマップにロケーションが表示されます。

[ロケーション階層 (Location Hierarchy)] ウィンドウの左側のペインには、インポートされたルートロケーションとデフォルトの顧客名 (ルート名) が表示されます。プラス記号をクリックすると、階層を展開して表示できます。ルートロケーションにある建物と関連するフロアを表示できます。

左側のペインからルートロケーションを選択すると、キャンパス、建物、グループ、フロア、ゾーンの数に関連する追加情報も表示できます。

選択したロケーション、建物、またはフロアに関する追加情報が以下のタブに表示されます。

- **マップ (Map)** : マップ上で選択したロケーションを表示します。
- **ロケーション情報 (Location Info)** : ロケーションデータ情報を表示します。
- **ネットワークデバイス (Network Devices)** : 接続されているネットワークデバイスと実行中のデバイスをすべて表示し、これらのデバイス数を表示します。
- **メタデータ (Metadata)** : 設定されたメタデータ情報を表示します。
- **ロケーション (Locations)** : ロケーションノードを表示します。
- **ユーザー (Users)** : ユーザーを表示します。
- **ライセンス使用状況 (License Usage)** : ライセンスタイプ、アクセスポイント、Webex デバイス、Meraki カメラ、ロケーション、および建物単位の情報を表示します。

[ロケーション階層 (Location Hierarchy)] ウィンドウでは、次の追加タスクを実行できます。

- **検索 (Search)** : [検索 (Search)] フィールドにロケーション名を入力し、**Enter** キーを押します。検索語は 4 文字以上にする必要があります。[最近の検索 (Recent Searches)] エリアには、検索結果が表示されます。

- **名前の変更 (Rename)** : ロケーションの横にある 3 つのドットをクリックし、[ロケーション名の変更 (Rename Location)] をクリックしてロケーション名を編集します。
- **削除 (Delete)** : ロケーションの横にある 3 つのドットをクリックし、[ロケーションの削除 (Delete Location)] をクリックして、[ロケーション階層 (Location Hierarchy)] からそのロケーションを削除します。

ロケーション階層は、特定のフロアでリッチマップが利用可能な場合、それらが表示されます。リッチマップをアップロードするオプションは、現在、Cisco Spaces サポートチームによって管理されています。[3D] トグルボタンをクリックすると、2D フロアマップと 3D フロアマップを切り替えることができます。

ロケーション階層には、Cisco Spaces ユーザーがアクセスできるロケーションのみが表示されます。これらのロケーションへのアクセス可能性は、ロールを作成または編集するか、[管理者管理 (Admin Management)] で Cisco Spaces ユーザーを招待または編集するときに定義されます。

- [ロケーション情報の表示 \(304 ページ\)](#)
- [ロケーション情報の更新 \(308 ページ\)](#)
- [ネットワークデバイスの表示 \(310 ページ\)](#)
- [メタデータの設定 \(311 ページ\)](#)
- [ロケーションの表示, on page 312](#)
- [ユーザーの表示, on page 313](#)

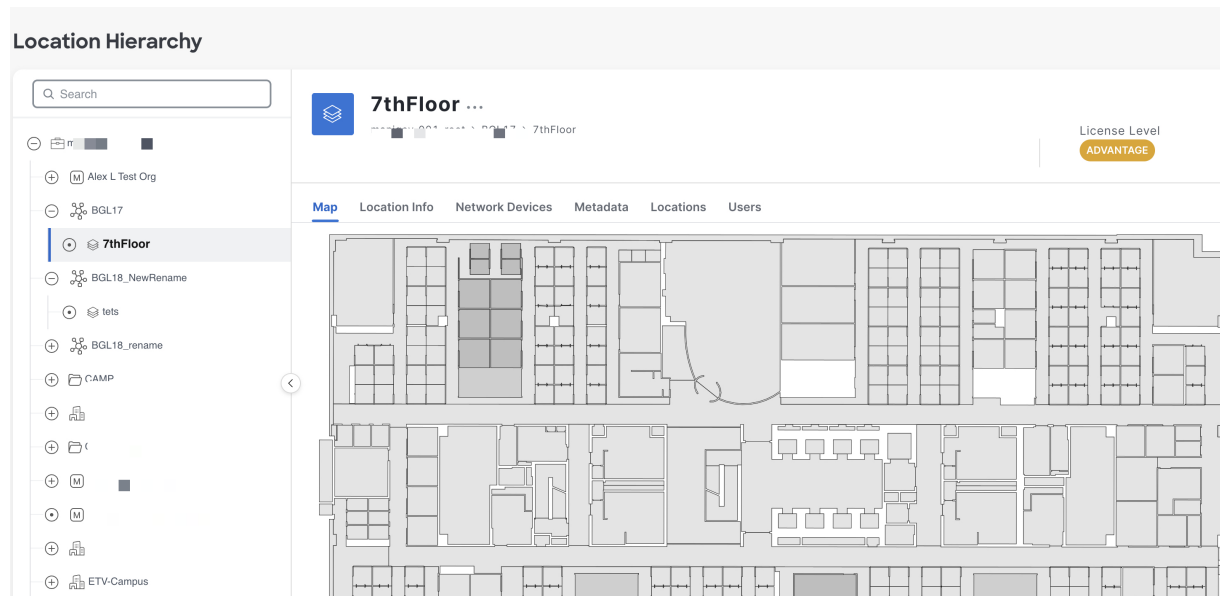
ロケーション情報の表示

[マップ (Map)] タブ (Cisco Spaces ダッシュボード > メニューアイコン (☰) > [ロケーション階層 (Location Hierarchy)] > [ルートロケーション (Root Location)]) を使用して、マップ上に選択したロケーション、キャンパス、建物、およびフロアの情報を表示します。

ルートロケーションを選択すると、デフォルトの世界地図が表示されます。

ただし、場合によっては、自動的にマップ上の正確な位置にズームインされ、プロッターアイコンとともに表示されます。プロッターアイコンをクリックすると、ロケーションアドレス、総面積、最大キャパシティ、タイムゾーンの詳細などの追加情報を表示できます。正確な位置は、緯度と経度の情報に基づいてプロットされます。

図 21: マップタブ



建物を選択すると、デフォルトの世界地図が表示されます。

フロアを選択すると、正確なフロアマップイメージが表示されます。ポリゴンツール () を使用してゾーンを作成します。詳細については、[ゾーンの作成 \(305 ページ\)](#) を参照してください。

選択した場所に応じて、次の情報が表示されます。

- マニュアルの構成
- キャンパス
- 建物
- フロア
- ゾーン
- アラート (Alerts)

ゾーンの作成

[マップ (Map)] タブを使用して、**ロケーション階層** に Cisco CMX ゾーンを作成します。



(注) 現在、Cisco Meraki のゾーンベースレポートは、**Right Now (現在の状況)** アプリケーションおよび **Firehose** デバイスのロケーション更新イベントでのみサポートされています。

手順

-
- ステップ 1** Cisco Spaces にログインします。
- ステップ 2** Cisco Spaces ダッシュボードで、[メニュー（Menu）] アイコン（) をクリックし、[ロケーション階層（Location Hierarchy）] を選択します。
- [ロケーション階層（Location Hierarchy）] ウィンドウが表示されます。
- ステップ 3** 左側のペインで、必要なフロアの場所に移動します。
- フロアマップが表示されます。
- ステップ 4** マップ上のポリゴンツール（) をクリックします。
- カーソルがプラスのアイコンに変わります。
- ステップ 5** 必要なマップエリアをクリックし、カーソルを移動して、選択した多角形のゾーンを描画します。
- ステップ 6** ダブルクリックして、ゾーンの作成を完了します。
- 右側のペインにポップアップウィンドウが表示されます。
- ステップ 7** [Zone Name（ゾーン名）] フィールドに、ゾーンの名前を入力します。
- ステップ 8** ゾーンを区別するオーバーレイカラーを選択します。
- ステップ 9** [Save] をクリックします。
- 新しいゾーンが作成され、[Location Hierarchy（ロケーション階層）] ウィンドウが更新され、ルートロケーションが表示されます。
 - 左側のペインで、新しいゾーンを作成したフロアに移動すると、Cisco CMX ゾーンがフロア階層の下に新しい項目として表示されます。
- ステップ 10** （オプション）ゾーンの詳細を更新するには、マップ上のポリゴンアイコンをクリックします。
-

フロアロケーションのゾーンの作成

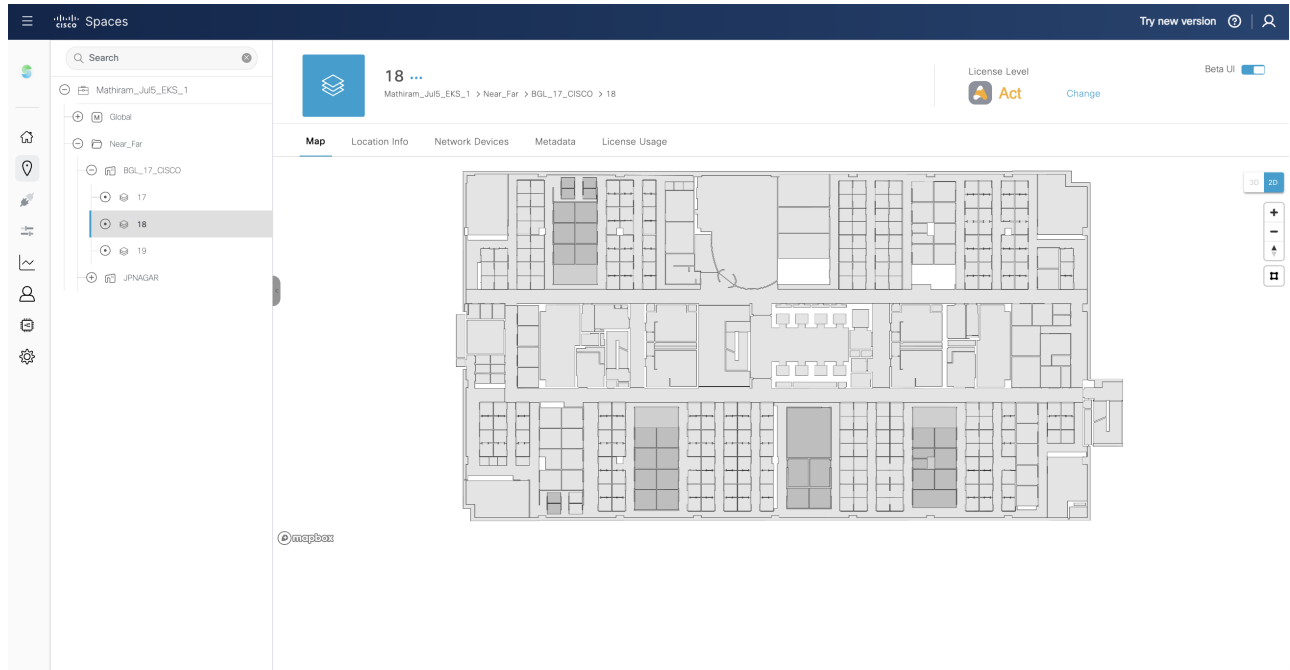
手順

-
- ステップ 1** Cisco Spaces にログインします。
- ステップ 2** Cisco Spaces ダッシュボードで、[メニュー（Menu）] アイコン（) をクリックし、[ロケーション階層（Location Hierarchy）] を選択します。
- [ロケーション階層（Location Hierarchy）] ウィンドウが表示されます。

ステップ3 左側のペインで、必要なフロアの場所に移動します。

フロアマップが表示されます。

図 22: マップタブ



ステップ4 マップ上のポリゴンツール（）をクリックします。

カーソルがプラスのアイコンに変わります。

ステップ5 必要なマップエリアをクリックし、カーソルを移動して、選択した多角形のゾーンを描画します。

ステップ6 ダブルクリックして、ゾーンの作成を完了します。

右側のペインにポップアップウィンドウが表示されます。

ステップ7 [Zone Name（ゾーン名）] フィールドに、ゾーンの名前を入力します。

ステップ8 ゾーンを区別するオーバーレイカラーを選択します。

ステップ9 [Save] をクリックします。

- 新しいゾーンが作成され、[Location Hierarchy（ロケーション階層）] ウィンドウが更新され、ルートロケーションが表示されます。
- 左側のペインで、新しいゾーンを作成したフロアに移動すると、そのゾーンがフロア階層の下に新しい項目として表示されます。

ステップ10 （オプション）ゾーンの詳細を更新するには、マップ上のポリゴンツール（）をクリックします。

ロケーション情報の更新

ロケーション情報を表示および編集するには、[ロケーション情報 (Location Info)] タブ (Cisco Spaces ダッシュボード > [メニュー (Menu)] アイコン (≡) > [ロケーション階層 (Location Hierarchy)] > [ルートロケーション (Root Location)]) を使用します。

選択したロケーションについて、ノードタイプとネットワーク参照の詳細が表示されます。

図 23: ロケーション情報タブ

The screenshot shows the 'Location Info' tab in the Cisco Spaces dashboard. It displays a hierarchy starting with 'ROOT' under 'NODE TYPE' and 'qasetupv2test1' under 'NETWORK REFERENCE'. Below this, there is a 'Location Data' section with an 'Edit' link. A yellow warning box states: 'Note: Some location data fields are inherited from its parent location. Inherited fields are highlighted in orange color. We strongly recommended you to update the location data for each location separately to avoid discrepancy.' The data table below shows various fields, with some values highlighted in orange to indicate inheritance.

Brand	Testing
Total Area	100 Square Feet
Occupancy Limit (MAX CAPACITY)	11
Country	NA
State	NA
City	Hosur
Zipcode	635126
Latitude	NA
Longitude	NA
Time Zone	Asia/Dubai

[編集 (Edit)] をクリックしてロケーション情報を更新します。詳細については、[ロケーション情報の編集 \(309 ページ\)](#) を参照してください。



(注) 親ロケーションから継承したロケーションデータフィールドはオレンジ色で強調表示されます。不整合を避けるために、ロケーションデータはロケーションごとに個別に更新することを強く推奨しています。

ロケーション情報の編集

手順

ステップ 1 Cisco Spaces にログインします。

ステップ 2 Cisco Spaces ダッシュボードで、[メニュー (Menu)] アイコン (☰) をクリックし、[ロケーション階層 (Location Hierarchy)] を選択します。

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

ステップ 3 左側のペインで、必要な場所に移動します。

ステップ 4 [ロケーション情報 (Location Info)] タブをクリックします。

ステップ 5 [ロケーションデータ (Location Data)] の横にある [編集 (Edit)] をクリックします。

スライドインウィンドウが表示されます。

ステップ 6 必要に応じて、以下のロケーション情報を更新します。

- a) **ロケーション名 (Location Name)** : ロケーションの名前を編集します。
- b) **ブランド (Brand)** : ブランド名を編集します。
- c) **総面積 (Total Area)** : 合計エリアの詳細を編集します。
- d) **単位 (Unit)** : 入力される合計エリアの単位を選択します。オプションは[平方フィート (Square Feet)] および[平方メートル (Square Meter)] です。
- e) **占有制限 (最大キャパシティ) (Occupancy Limit (Max Capacity))** : 占有制限/最大キャパシティの詳細を編集します。
- f) **アドレス (Address)** : アドレスの詳細を入力し、表示されるオプションから選択します。選択したアドレスは、右側に表示されるマップにプロットされます。
- g) **緯度 (Latitude)** : 選択したアドレスの緯度を表示します。この値は編集できません。
- h) **経度 (Longitude)** : 選択したアドレスの経度を表示します。この値は編集できません。
- i) **タイムゾーン (Time Zone)** : [タイムゾーンの検索 (Search Timezone)] フィールドに検索語を入力し、使用可能なオプションから検索または選択します。

ステップ 7 [Save] をクリックします。

アクセス ポイント プレフィックスの編集

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。

[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。

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。

手順

ステップ 1 Cisco Spaces にログインします。

ステップ 2 Cisco Spaces ダッシュボードで、[メニュー (Menu)] アイコン (☰) をクリックし、[ロケーション階層 (Location Hierarchy)] を選択します。

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

ステップ 3 左側のペインで、必要なネットワークに移動します。

ステップ 4 [ロケーション情報 (Location Info)] タブをクリックします。

ステップ 5 [アクセスポイントの使用プレフィックス (Access Point Prefix Used)] の横にある [追加/編集 (Add/Edit)] をクリックします。

ステップ 6 [Add/Edit Prefix (プレフィックスの追加/編集)] ウィンドウの [プレフィックス (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アクセスポイントが一覧表示されます。

ステップ 7 [プレフィックスの追加 (Add Prefix)] をクリックします。

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 [追加されたプレフィックス (Added Prefixes)] の下にリストされます。[プレフィックスの追加 (Add Prefix)] は、入力されたプレフィックスを持つ AP が利用できる場合にのみ有効です。

ステップ 8 [Save] をクリックします。

プレフィックスを追加した後、**未構成**のネットワークの下にある、このプレフィックスを持つ 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、[追加されたプレフィックス (Added Prefixes)] の下にあるプレフィックスにカーソルを合わせ、[削除 (Delete)] アイコンをクリックします。

ネットワークデバイスの表示

[ネットワークデバイス (Network Devices)] タブ (Cisco Spaces ダッシュボード > [メニュー (Menu)] アイコン (☰) > [ロケーション階層 (Location Hierarchy)] > [ルートロケーション (Root Location)]) を使用して、選択したノードの下にある全ネットワークデバイスを表示します。ルートロケーションには、ロケーション階層内で使用可能なすべての接続済みデバイスが表示されます。

選択した場所に応じて、次の情報が表示されます。

- **[アクセスポイント (Access Points)]** : AP の名前、MAC アドレス、およびロケーション階層パスを表示します。特定の AP を検索するには、[テーブルを検索 (Search Table)] フィールドを使用します。階層パスをコピーするには、[ロケーション] フィールドの横にあるコピーアイコンをクリックします。[セットアップ (Setup)] ウィンドウに移動して、AP を設定します。
- **カメラ (Cameras)** : カメラ名、シリアル番号、MAC アドレス、トリップワイヤのステータス (設定/非設定) など、接続されたカメラの詳細を表示します。特定のカメラを検索するには、[テーブルを検索 (Search Table)] フィールドを使用します。[Meraki カメラを接続する (Connect your Meraki Camera)] ウィンドウに移動して、追加のデバイスを接続します。
- **セキュリティアプライアンス (Security Appliances)** : それぞれの場所でのセキュリティアプライアンスデバイスの詳細なリストを表示します。
- **Webex デバイス (Webex Devices)** : 接続されている Cisco Webex デバイスを表示します。
- **リンクされたデバイス (Linked Devices)** : このロケーションに設定されているリンクされたデバイスを表示します。IoT デバイス、非 Webex サイネージ、およびスマート PUD をリンクできます。

メタデータの設定

メタデータ情報を表示するには、[メタデータ (Metadata)] タブ (Cisco Spaces ダッシュボード > メニュー (Menu) アイコン (☰) > [ロケーション階層 (Location Hierarchy)] > [ルート場所 (Root Location)]]) を使用します。メタデータがまだ設定されていない場合は、[メタデータの追加 (Add Metadata)] をクリックしてメタデータを追加します。詳細については、[メタデータの追加 \(312 ページ\)](#) を参照してください。

図 24: メタデータタブ

The screenshot shows the Cisco Spaces Metadata tab. At the top, there are statistics for various categories: Org (04), Campus (18), Group (07), Building (72), Wireless Controller (02), Floor (80), and Zone (29). A 'License Level' badge indicates 'ADVANTAGE'. Below the statistics is a navigation bar with tabs: Map, Location Info, Network Devices, Metadata (selected), Locations, and Users. The main content area displays a table with the following data:

Metadata Key	Value	Actions
Org	Org	Edit Delete
Campus	Campus	Edit Delete

選択した場所に応じて、次の情報が表示されます。

- **メタデータキー (Metadata Key)** : メタデータキーを表示します。
- **値 (Value)** : メタデータキーの値を表示します。値には英数字と特殊文字も使用できます (例: xyz123@)。

メタデータの追加

手順

ステップ 1 Cisco Spaces にログインします。

ステップ 2 Cisco Spaces ダッシュボードで、[メニュー (Menu)] アイコン (☰) をクリックし、[ロケーション階層 (Location Hierarchy)] を選択します。

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

ステップ 3 左側のペインで、必要な場所に移動します。

ステップ 4 [メタデータ (Metadata)] タブをクリックします。

ステップ 5 [メタデータの追加 (Add Metadata)] をクリックします。

ステップ 6 [キー (Key)] フィールドに、メタデータキーを入力するか選択します。

ステップ 7 [値 (Value)] フィールドにキーの値を入力します。

ステップ 8 (オプション) [メタデータの追加 (Add Metadata)] をクリックして、複数のメタデータキーと対応する値を追加します。

キーを削除するには、メタデータキーの横にある [削除 (Delete)] アイコンをクリックします。

ステップ 9 [Save] をクリックします。

新しいメタデータキーと値が [メタデータ (Metadata)] タブに表示されます。[編集 (Edit)] アイコンをクリックして、キー情報を更新します。

ロケーションの表示

[ロケーション (Locations)] タブ (Cisco Spaces ダッシュボード [メニュー (Menu)] アイコン (☰) [ロケーション階層 (Location Hierarchy)] [ルートロケーション (Root Location)]) を使用して、ロケーションタイプやレベルなどのロケーション情報を表示します。

[ロケーションタイプ (Location Type)] と [レベル (Level)] ドロップダウンオプションを使用して、ロケーション設定を選択します。ロケーションタイプは次のとおりです:

- Network
- キャンパス

- Group
- マニュアルの構成

選択したロケーションについて、次の詳細を表示します。

- ロケーション
- AP
- Camera
- 最大キャパシティ
- 総面積（平方フィート）
- Time Zone

ロケーションの横にある必須のチェックボックスをオンにして、[グループの作成（Create Group）] をクリックしてロケーションを追加し、独自のグループを作成します。

ユーザーの表示

[ユーザー（Users）] タブ（Cisco Spaces [ダッシュボード（Dashboard）] [メニュー（Menu）] アイコン  [ロケーション階層（Location Hierarchy）] [ルートロケーション（Root Location）]）を使用して、ユーザーとそのロール権限を表示します。

次の詳細の表示

- ユーザー
- Role
- 権限：読み取りと書き込み
- 権限：読み取り専用
- ロケーション

[検索（Search）] オプションを使用してユーザーを検索します。ユーザーをクリックすると、[管理者管理（Admin Management）] > [ユーザーの編集（Edit User）] ウィンドウで権限設定を編集できます。



第 **VII** 部

統合

- [Cisco Catalyst Center（旧 Cisco DNA Center）統合（317 ページ）](#)
- [カレンダーの統合（321 ページ）](#)
- [Cisco DNA Spaces と ServiceNow アプリケーションの統合（327 ページ）](#)



第 26 章

Cisco Catalyst Center（旧 Cisco DNA Center） 統合

この章では、Cisco Spaces と Catalyst Center の統合について説明します。

- [概要（317 ページ）](#)
- [Cisco Spaces と Catalyst Center の統合（318 ページ）](#)

概要

Cisco Spaces を使用すると Cisco Catalyst Center（旧 Cisco DNA Center）と統合できるようになります。これにより、Cisco Spaces を使用して Catalyst Center サイトをモニターできます。



- (注) 現在、Catalyst Center と Cisco 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。

詳細については、『*Catalyst Center* ユーザーガイド』の「Cisco Spaces 統合について」を参照してください。

<https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/products-user-guide-list.html>

前提条件

- Catalyst Center、リリース **2.1.2.3** 以上。
- Cisco Spaces : コネクタ を使用してワイヤレスネットワークを Cisco Spaces に接続する必要があります。接続するには、Cisco Spaces ダッシュボードにログインして、**[セットアップ (Setup)] > [ワイヤレスネットワーク (Wireless Networks)]** の順に選択します。
- Catalyst Center は、OCSP/CRL を使用した SSL/TLS 証明書の失効ステータスを確認します。TCP 80 は、デバイスおよび他のシステムへのアウトバウンド通信に Catalyst Center によって使用されるポートです。証明書失効ステータスを正常に確認するには、次の URL が直接、および Catalyst Center 用に設定されたプロキシサーバー経由の両方で到達可能である

必要があります。そうしないと、Catalyst Center が cisco.com に接続したときに証明書失効チェックがスキップされます。

<http://validation.identrust.com>

<http://commercial.ocsp.identrust.com>

詳細については、『Cisco Catalyst Center セキュリティのベストプラクティスガイド』の「通信ポート」を参照してください。

Cisco Spaces と Catalyst Center の統合

Cisco Spaces と Catalyst Center を統合するには、次の手順を実行します。

手順

- ステップ 1 Cisco Spaces にログインします。
- ステップ 2 ウィンドウで [メニュー (Menu)] アイコン (≡) をクリックし、[統合 (Integrations)] を選択します。
- ステップ 3 Catalyst Center [統合 (Integrations)] ウィンドウで、[新規インスタンス (New Instance)] をクリックします。
- ステップ 4 [新しいトークンの作成 (Create new token)] ポップアップウィンドウで、Catalyst Center インスタンス名を入力し、[トークンの作成 (Create Token)] をクリックします。

新しいトークンが正常に作成されたことを示す成功メッセージが表示され、そのトークンが Catalyst Center [統合 (Integration)] ウィンドウに表示されます。

(注)
新しいトークンの有効期間は 2 日間です。
- ステップ 5 [トークンのコピー (Copy Token)] をクリックして、このテナントトークンを Catalyst Center で使用します。
- ステップ 6 Catalyst Center にログインします。
- ステップ 7 [メニュー (Menu)] アイコン (≡) をクリックし、[システム (System)] > [設定 (Settings)] を選択します。
- ステップ 8 [CMXサーバー/Cisco Spaces (CMX Servers/Cisco Spaces)] をクリックします。
- ステップ 9 [CMXサーバー/Cisco Spaces (CMX Servers/Cisco Spaces)] ウィンドウの Cisco Spaces セクションで、[アクティブ化 (Activate)] をクリックします。
- ステップ 10 [Cisco Spacesの統合 (Integrate Cisco Spaces)] ポップアップウィンドウで、テナントトークンを貼り付け、[接続 (Connect)] をクリックします。

Cisco Spaces で統合が完了すると、次の成功メッセージが表示されます。「*This cluster is integrated with Cisco Spaces successfully* (このクラスタは Cisco Spaces と正常に統合されました)」。ステータスは [アクティブ化 (Activated)] と表示されます。

Cisco Spaces トークンをアクティブにした後、Cisco Spaces を Catalyst Center サイトに割り当て、それらのサイトのモニターを開始できます。詳細については、「[Catalyst Center ユーザーガイド](#)」を参照してください。



第 27 章

カレンダーの統合

この章では、サードパーティの統合について説明します。

Google カレンダーの統合

Google カレンダーとの統合により、Google アカウントで Cisco Spaces に接続できます。これにより、会議室の予約情報が同期されます。Cisco Spaces デジタルサイネージは、Google カレンダーの予約情報を使用して、コンテキストに乏しい従来の会議室のリストではなく、マップベースの直感的なアプローチで利用可能な会議室を表示できます。

Office 365 予定表統合

Office 365 カレンダーを統合することで、Microsoft アカウントを Cisco Spaces に紐づけて、会議室のブッキング情報を同期できます。Cisco Spaces デジタルサイネージは、Office 365 カレンダー予約情報を取り込んで、マップベースのインターフェイスを使用して利用可能な部屋に簡単にアクセスし、可視化できます。この方法では、従来型の部屋リストよりも状況がわかりやすく、使いやすいエクスペリエンスが提供されます。

- [カレンダー GUI の統合 \(321 ページ\)](#)
- [Google カレンダーの統合 \(322 ページ\)](#)
- [Office 365 カレンダーの統合 \(323 ページ\)](#)

カレンダー GUI の統合

Microsoft 365 カレンダーの統合機能が Cisco Spaces で導入されました。この機能を活用して、Microsoft 365 カレンダーアカウントを Cisco Spaces アプリケーションに接続し、Cisco Spaces ダッシュボード **[メニュー (Menu)]** > **[統合 (Integrations)]** で統合された予定表の詳細を表示します。

インポートされた予定表が Cisco Spaces : Space Manager (スペースマネージャ) アプリケーションに表示されます。

Google カレンダーの統合

Google カレンダーの統合により、Google アカウントを Cisco Spaces と連携し、会議室の予約情報を同期できます。Cisco Spaces デジタルサイネージを使用すると、コンテキストのない従来のリストではなく、直感的にわかるマップにより利用可能な部屋を簡単に確認できます。この統合により、使いやすいデジタルサイネージアプリケーションでダイナミックな予定表データが表示されるため、会議室が有効活用できます。

手順

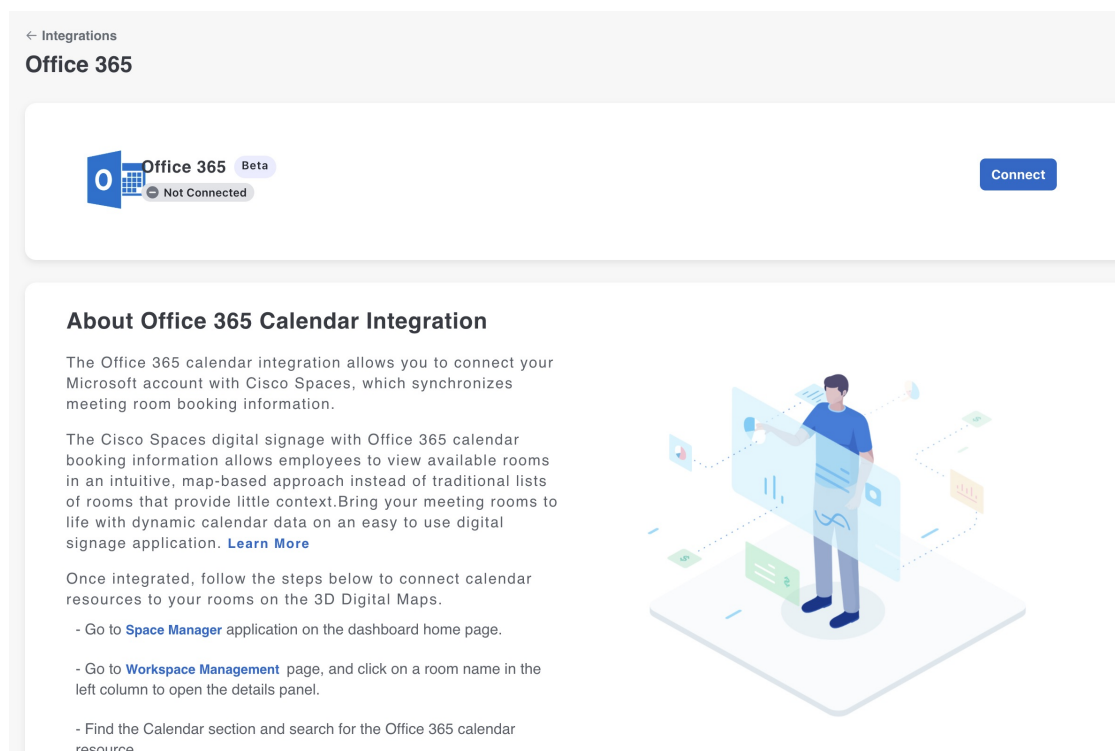
ステップ 1 Cisco Spaces にログインします。

Cisco Spaces [ホーム (Home)] ウィンドウが表示されます。

ステップ 2 左上の隅から、[メニュー (Menu)] アイコン (☰) をクリックし、[統合 (Integrations)] > [Google カレンダーの統合 (Google Calendar Integrations)] を選択します。

[Google カレンダーの統合 (Google Calendar Integrations)] ウィンドウが表示されます。

図 25: Google カレンダーの統合



ステップ 3 [Connect] をクリックします。

- ステップ 4** [サインイン - Google アカウント (Sign in - Google Accounts)] ポップアップウィンドウで、Google アカウントのログイン情報を入力します。
- 記載されている [サインイン - Google アカウント (Sign in - Google Accounts)] ポップアップウィンドウからカレンダー予約を利用できる有効な Google アカウントを選択していることを確認してください。
- ステップ 5** アカウントを確認したら、[続行 (Proceed)] をクリックします。
- ステップ 6** [dnaspaces.ioに移動 (Go to dnaspaces.io)] > [続行 (Continue)] をクリックして、Google アカウントを Cisco Spaces と統合します。
- 「Calendar integration is successfull (カレンダーの統合に成功しました)」とのメッセージが表示されます。
- ステップ 7** 統合された Google カレンダーの詳細は、[マイ統合 (My Integrations)] エリアで、接続されたリソース数とともに表示されます。緑色のチェックマークは、統合が成功したことを示します。
- 統合されたカレンダーは、Cisco Spaces : Smart Workspaces アプリケーションで使用できます。
- Google カレンダーの統合を削除するには、タイルビューで [削除 (Remove)] をクリックします。
 - 現在のアカウント統合を切断するには、[切断 (Disconnect)] をクリックし、指示に従います。

次のタスク

3D デジタルマップで予定表のリソースを部屋に正常に接続するには、次の手順を実行します。

1. **Cisco Smart Workspaces** アプリケーションに移動します。
2. [ワークスペース管理 (Workspace Management)] ウィンドウに進み、左側の列からルーム名を選択して [詳細 (Details)] パネルにアクセスします。
3. [詳細 (Details)] パネルから、[予定表 (Calendar)] エリアに移動し、Google カレンダーリソースを検索します。

Office 365 カレンダーの統合

Office 365 カレンダーを統合すると、Microsoft アカウントを Cisco Spaces とシームレスに接続でき、その結果、会議室の予約情報が同期されます。Cisco Spaces デジタルサイネージを Office 365 カレンダーの予約情報と組み合わせて使用すると、利用可能な部屋を表示するためのユーザーフレンドリで直感的なマップベースのアプローチが提供されます。このアプローチは、状況がわかりにくい従来の部屋のリストよりも非常に効果的です。使いやすいデジタルサイネージアプリケーションでダイナミックな予定表データを用いて、会議室を有効活用できます。

手順

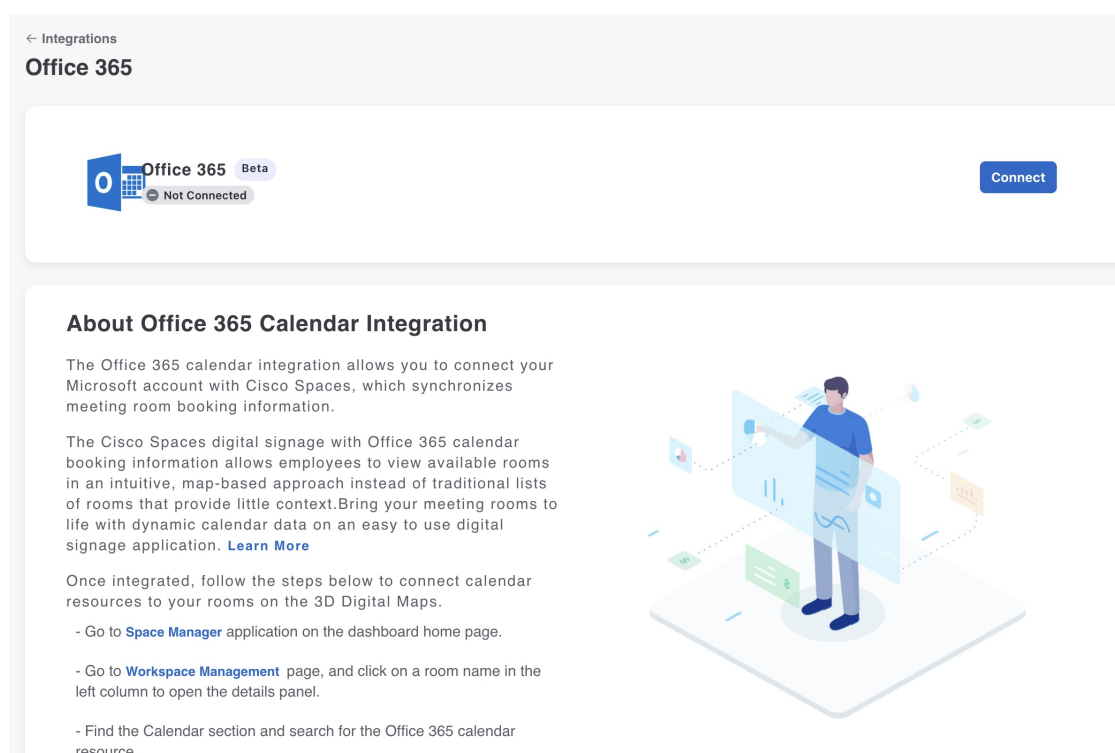
ステップ 1 Cisco Spaces にログインします。

Cisco Spaces [ホーム (Home)] ウィンドウが表示されます。

ステップ 2 左上の隅から、[メニュー (Menu)] アイコン (☰) をクリックし、[統合 (Integrations)] > [Office 365] を選択します。

[Office 365 の統合] ウィンドウが表示されます。

図 26 : Office 365 の統合



ステップ 3 [Connect] をクリックします。

ステップ 4 画面の指示に従って、Office 365 アカウントのログイン情報を入力して、Office 365 カレンダーを統合します。

ステップ 5 アカウントを検証したら、[続行 (Proceed)] をクリックします。

ステップ 6 [dnaspaces.ioに移動 (Go to dnaspaces.io)] > [続行 (Continue)] をクリックして、office 365 アカウントを Cisco Spaces と統合します。

「Calendar integration is successfull (カレンダーの統合に成功しました)」とのメッセージが表示されます。

ステップ 7 統合された Office 365 カレンダーの詳細は、[マイ統合 (My Integrations)] エリアで、接続されたリソース数とともに表示されます。緑色のチェックマークは、統合が成功したことを示します。

統合されたカレンダーは、Cisco Spaces : Smart Workspaces アプリケーションで使用できます。

- Office 365 カレンダーを削除するには、タイルビューで[削除 (Delete)] をクリックします。
- 現在のアカウント統合を切断するには、[切断 (Disconnect)] をクリックし、指示に従います。

次のタスク

3D デジタルマップで予定表のリソースを部屋に正常に接続するには、次の手順を実行します。

1. **Cisco Smart Workspaces** アプリケーションに移動します。
2. [ワークスペース管理 (Workspace Management)] ウィンドウに進み、左側の列からルーム名を選択して [詳細 (Details)] パネルにアクセスします。
3. [詳細 (Details)] パネルから、[予定表 (Calendar)] エリアに移動し、Google カレンダーリソースを検索します。



第 28 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](#) (327 ページ)

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。

手順

- 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。
- プロキシミティレポートを開きます。**
 - [Create Report]** をクリックします。
 - [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。
 - レポートを生成する MAC アドレスを確認します。
 - [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。
 - [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。
 - [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。
 - [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 **VIII** 部

設定

- [Cisco DNA Spaces SDK の統合](#) (333 ページ)
- [通知](#) (339 ページ)



第 29 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 Spaces SDK の統合](#)（333 ページ）
- [Cisco Spaces の統合](#)（333 ページ）

Cisco Spaces SDK の統合

Cisco 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 Spaces SDK により、iOS または Android アプリケーションの開発者は、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 Spaces SDK を使用すると、開発者は、iOS および Android の通知フレームワークを介して、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、[メニュー（Menu）] アイコン(☰) > [設定（Configure）] > [Cisco Spaces SDK] からアクセスできます。これにより、ネイティブアプリ（iOS および Android）を Cisco Spaces に登録できます。

Cisco Spaces の統合

Cisco Spaces ソフトウェア開発キット（SDK）は、iOS プラットフォームと Android プラットフォームに対応する、プラットフォームに依存しない SDK であり、Cisco Spaces の顧客は、これを使用して、アプリケーションがモバイルデバイスで OpenRoaming ユーザープロファイルを提供および管理できるようにします。詳細については、Cisco Spaces [SDK デベロッパー資料](#)を参照してください。

始める前に

Google による API キーベースの機能の廃止に伴い、Google Cloud Messaging（GCM）を介して Firebase JSON を使用する新しいメソッドが Cisco Spaces ソフトウェア開発キット（SDK）（**Cisco Spaces ダッシュボード** > **[設定（Configure）]** > **[Cisco Spaces SDK]**）に導入されました。

このリリース以前は、Cisco Spaces で API キーを設定する必要がありましたが、現在は Firebase JSON に変更されています。

Cisco Spaces はこれを利用して、SDK を使用して Android デバイスでプッシュ通知をトリガーします。

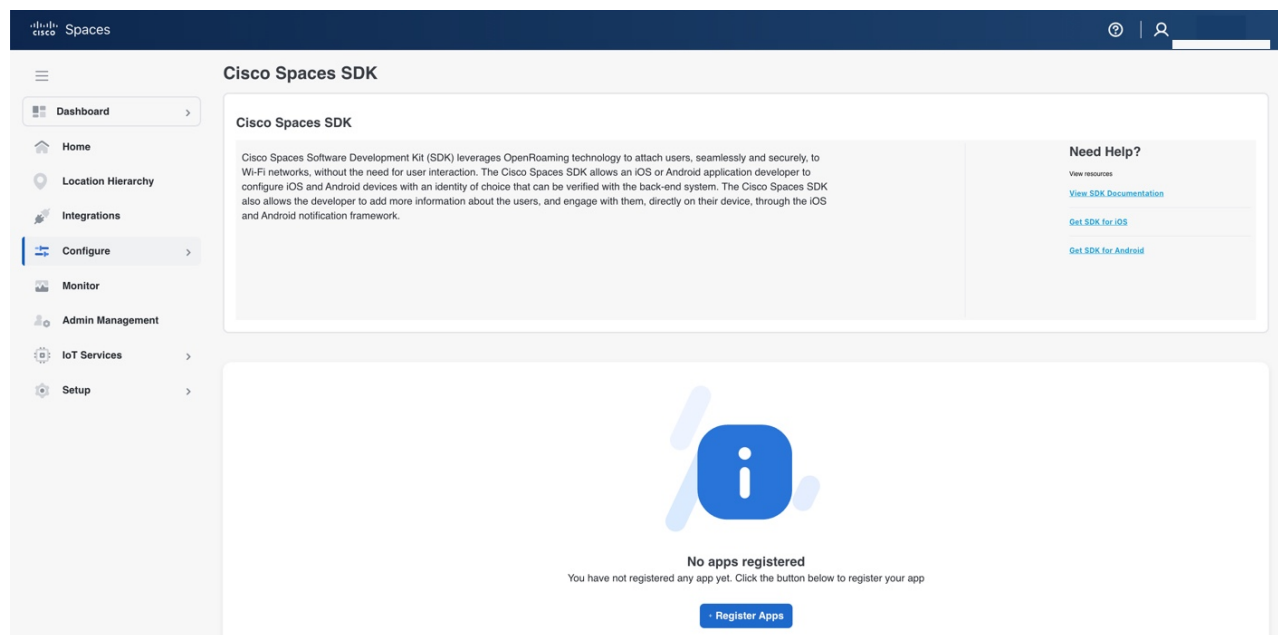
手順

ステップ 1 Cisco Spaces にログインします。

Cisco Spaces [ホーム（Home）] ウィンドウが表示されます。

ステップ 2 左上隅にある [メニュー（Menu）] アイコン（☰）をクリックして、**[設定（Configure）]** > **[Cisco Spaces SDK]** を選択します。

図 27: Cisco Spaces SDK



[Cisco Spaces SDK] ウィンドウが表示されます。

ステップ 3 [Register App] をクリックします。

ステップ 4 新しいアプリケーションの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。

新しいアプリケーションを正常に登録するには、次のセクションに情報を入力します。

- アプリの登録
- プロファイルの設定
- プッシュ通知
- 認証

図 28: アプリケーションの登録セクション

ステップ 6 [アプリケーションの登録 (Register App)] セクションで、次のように入力します。

- [App Name] : アプリケーションの名前を入力します。
- **バンドル ID (Bundle Identifier)** : iOS プラットフォームでアプリケーションを識別するバンドル ID (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 [プロファイルの設定 (Configure Profile)] セクションで、以下を入力します。

- **表示されるオペレータ名 (Displayed Operator Name)** : 有効な識別子を入力してください。この名前は、ユーザーの Android または iOS デバイスで Wi-Fi SSID 名として表示されます。
- **ドメイン (Domain)** : プロファイルの一意のドメイン名を入力します。
 - ドメイン名はオープンローミング (OpenRoaming) アプリケーションで使用できます。詳細については、「[ネットワークコントローラの設定](#)」を参照してください。
 - このドメイン名は、コントローラの設定に追加する必要があります。
 - 複数のアプリケーションがある場合は、各アプリケーションに一意のドメイン名が必要です。
- **ローミングコンソーシアムOI (Roaming Consortium OIs)** : [ローミングコンソーシアムOI (Roaming Consortium OIs)] ドロップダウンリストから、ローミングコンソーシアム組織 (RCO) 識別子の配列の横にあるチェックボックスをオンにします。これは任意です。

ステップ 9 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 10 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 11 [Next] をクリックします。

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 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) [秘密鍵を入力 (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 13 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) [秘密鍵を入力 (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 14 [アプリケーションの登録 (Register App)] をクリックして、アプリケーションの登録を完了します。登録されているアプリケーションが表示されます。

図 29: 登録済み **Android** および **iOS** アプリケーション

The screenshot displays a configuration page for Cisco Spaces with three application entries. Each entry is a card with a header, a status section, an API key field, and a 'View Configurations' link.

- Android**
 - Status: Registered, Push Notification Disabled
 - API Key of Android: [Redacted]
 - WiFi Profile: Configured
 - View Configurations [dropdown arrow]
- IOS_Test_App**
 - Status: Registered, Push Notification: Disabled
 - API Key of iOS: [Redacted]
 - WiFi Profile: Configured
 - View Configurations [dropdown arrow]
- Android_Test_App**
 - Status: Registered, Push Notification Disabled
 - API Key of Android: [Redacted]
 - WiFi Profile: Configured
 - View Configurations [dropdown arrow]

次の操作を実行できます。

- [設定の表示 (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。
- [削除 (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 15 (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 16 (任意) [Update] をクリックします。



第 30 章

通知

- [通知設定の概要 \(339 ページ\)](#)
- [カテゴリの管理 \(340 ページ\)](#)
- [サブスクライバの管理 \(342 ページ\)](#)

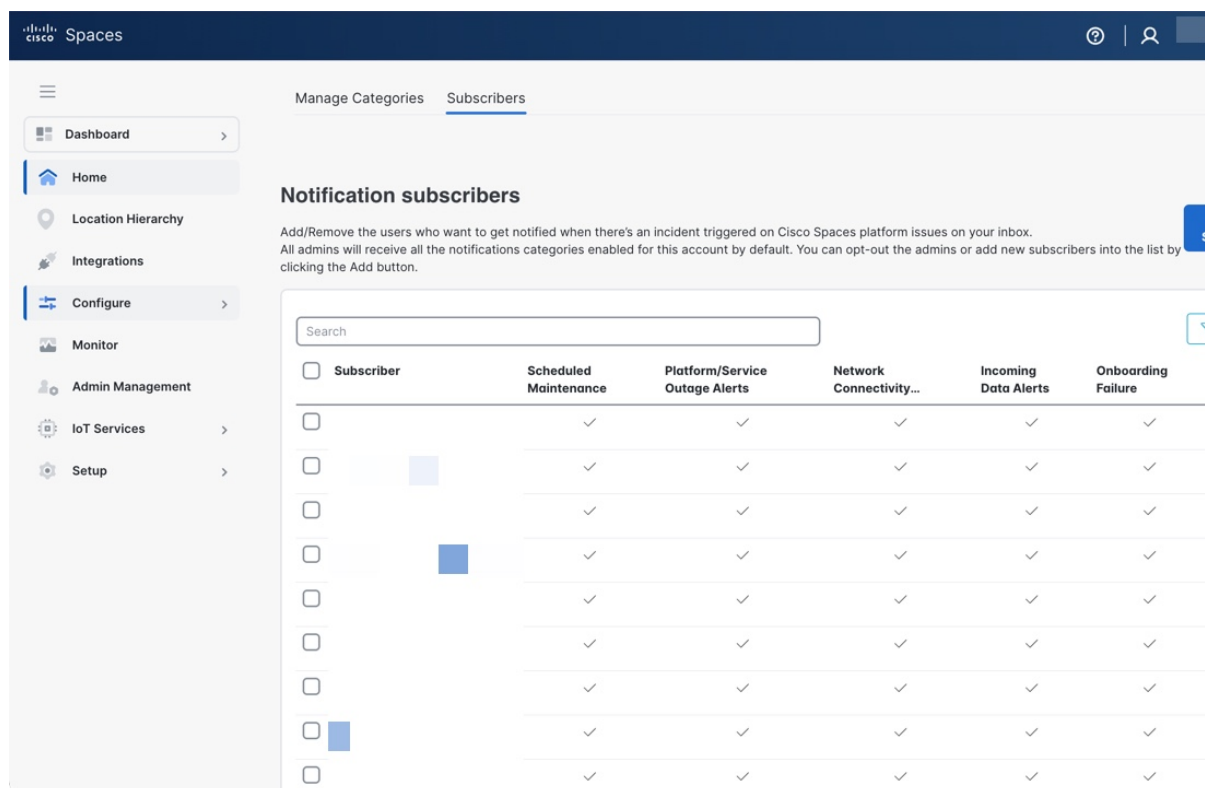
通知設定の概要

Cisco Spaces の **通知** 機能を使用すると、サブスクライバ通知 ([**設定 (Configure)**] > [**通知 (Notifications)**]) を設定し、重大なインシデントに関する通知を受信できます。Cisco Spaces プラットフォームでインシデントが発生したときに電子メール通知を受信するには、この機能を有効にします。

サブスクライバの通知は、Cisco Spaces クラウドまたはロケーションの問題に関する更新を提供し、タイムリーに対処するのに役立ちます。



(注) この機能は、管理者アクセス（読み取り専用および読み取り/書き込み）を持つすべてのユーザーが Cisco Spaces ベータ GUI で使用できます。



次のタブを使用します。

- **カテゴリの管理 (Manage Categories)** : 読み取り/書き込みアクセスを持つ管理者の場合は、[設定 (Configure)] > [通知 (Notifications)] > [カテゴリの管理 (Manage Categories)] に移動して、アカウントのサブスクライバ通知を設定します。
- **サブスクライバ (Subscribers)** : サブスクライバを管理するには、[サブスクライバ (Subscribers)] タブ ([設定 (Configure)] > [通知 (Notifications)] > [サブスクライバ (Subscribers)]) に移動します。

すべての管理者およびサブスクライバは、アカウントに対して有効になっているカテゴリに基づいて通知を受信します。

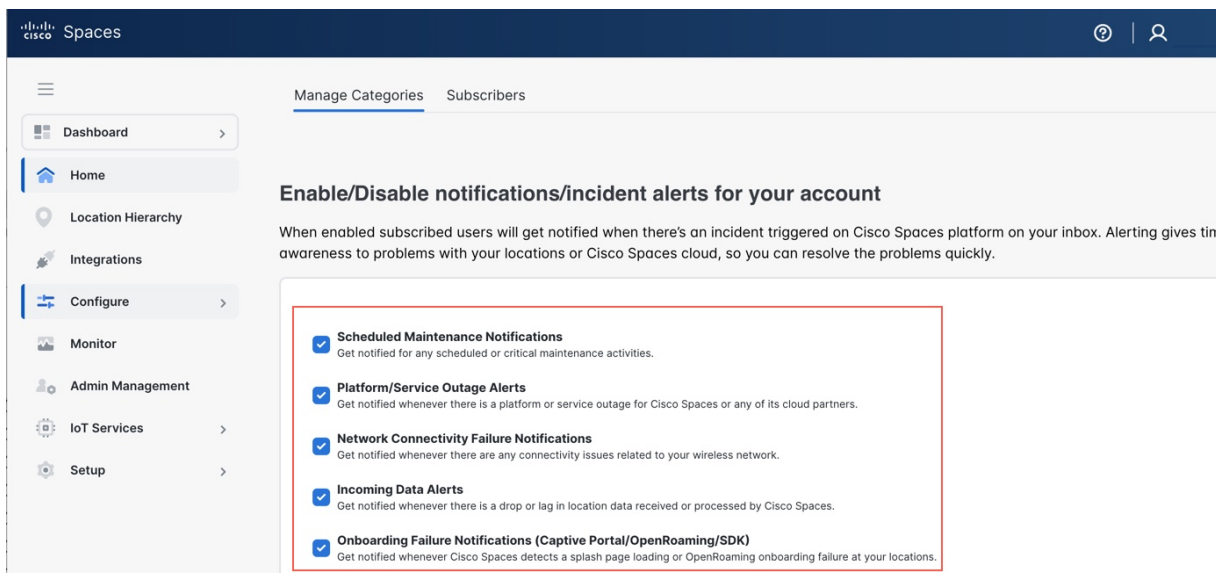
カテゴリの管理

[カテゴリの管理 (Manage Categories)] タブでは、通知を有効にするために使用できるカテゴリを選択できます。アカウントの通知とインシデントアラートの有効化または無効化に使用できるカテゴリを使用します。

次に、[カテゴリの管理 (Manage Categories)] タブ内のカテゴリを示します。

- **定期メンテナンス通知 (Scheduled Maintenance Notifications)** : スケジュール設定済みまたはクリティカルなメンテナンスアクティビティがある場合に通知を受けるには、[定期メンテナンス通知 (Scheduled Maintenance Notifications)] チェックボックスをオンにします。
- **プラットフォーム/サービス障害アラート (Platform/Service Outage Alerts)** : [プラットフォーム/サービス障害アラート (Platform/Service Outage Alerts)] チェックボックスをオンにして、Cisco Spaces プラットフォームまたはサービス障害、またはそのクラウドパートナーのいずれかに障害が発生するたびに通知を受けます。
- **ネットワーク接続障害通知 (Network Connectivity Failure Notifications)** : ワイヤレスネットワークに関連する接続の問題がある場合に通知を受信するには、[ネットワーク接続障害通知 (Network Connectivity Failure Notifications)] チェックボックスをオンにします。
- **着信データアラート (Incoming Data Alerts)** : Cisco Spaces で受信または処理されたロケーションデータにドロップまたは遅延がある場合に通知を受けるには、[着信データアラート (Incoming Data Alerts)] チェックボックスをオンにします。
- **オンボーディング失敗通知 (キャプティブポータル/オープンローミング/SDK) (Onboarding Failure Notifications (Captive Portal/OpenRoaming/SDK))** : [オンボーディング失敗通知 (キャプティブポータル/オープンローミング/SDK) (Onboarding Failure Notifications (Captive Portal/OpenRoaming/SDK))] チェックボックスをオンにすると、Cisco Spaces はロケーションでスプラッシュページのロードまたはオープンローミングオンボーディングエラーを検出するたびに通知を受けます。

図 30: 通知カテゴリ



通知を有効にすると、サブスクリバは、Cisco Spaces プラットフォームでインシデントがトリガーされるたびにメールボックスで通知を受信します。アラートは、ロケーションまたは

Cisco Spaces クラウドの問題を適切なタイミングで提供することで、問題を迅速に解決できます。

サブスクライバの管理

[サブスクライバ (Subscribers)] タブでは、サブスクライバを追加または編集できます。Cisco Spaces プラットフォームでインシデントがトリガーされるたびにメールボックスで通知を受信するサブスクライバを追加または削除できます。

デフォルトでは、すべての Cisco Spaces 管理者がアカウントで有効になっているすべてのカテゴリの通知を受信します。[サブスクライバの追加 (Add Subscriber)] ボタンをクリックすることで、特定の管理者をオプトアウトしたり、新しいサブスクライバをリストに追加したりできます。

[通知サブスクライバ (Notification subscribers)] ウィンドウの [検索 (Search)] フィールドを使用して、サブスクライバを検索します。

サブスクライバの詳細

表に、サブスクライバに関する詳細情報が表示されます。

表 15: サブスクライバの詳細

フィールド	説明
サブスクライバ	サブスクライバの電子メールアドレス
定期メンテナンス	チェックマークは、この通知カテゴリがサブスクライバに対して有効になっていることを示します。
プラットフォーム/サービス障害アラート	チェックマークは、この通知カテゴリがサブスクライバに対して有効になっていることを示します。
ネットワーク接続障害	チェックマークは、この通知カテゴリがサブスクライバに対して有効になっていることを示します。
着信データアラート	チェックマークは、この通知カテゴリがサブスクライバに対して有効になっていることを示します。
オンボーディングに失敗しました	チェックマークは、この通知カテゴリがサブスクライバに対して有効になっていることを示します。

フィールド	説明
処理	[アクション (Action)] 列の下にある 3 つのドットをクリックして、次のいずれかを実行します。 - 通知カテゴリのオプトインまたはオプトアウトを管理する - サブスクライバを削除する。 (注) 読み取りおよび書き込みアクセスを持つ管理者は、通知カテゴリをオプトインまたはオプトアウトし、サブスクライバを削除することができます。

図 31: 通知サブスクライバ

The screenshot displays the 'Notification subscribers' interface in Cisco Spaces. It includes a sidebar with navigation options like Dashboard, Home, Location Hierarchy, Integrations, Configure, Monitor, Admin Management, IoT Services, and Setup. The main content area shows a table of subscribers. The table has columns for Subscriber, Scheduled Maintenance, Platform/Service Outage Alerts, Network Connectivity Failure, Incoming Data Alerts, and Onboarding Failure. Two subscribers are listed: 'co.com' and 'o.com'. The 'o.com' row is selected. A red box highlights the 'Manage Opt-in/Opt-out' and 'Remove Subscriber' buttons in the bottom right corner of the table.

サブスクライバの追加

アラートリストにサブスクライバを追加する必要があります。Cisco Spaces プラットフォームでトリガーされたインシデントがある場合、登録しているユーザーにのみ通知されます。

新しいサブスクライバを追加するには、次の手順を実行します。

手順

ステップ 1 Cisco Spaces にログインします。

Cisco Spaces [ホーム (Home)] ウィンドウが表示されます。

ステップ 2 左上の隅から、[メニュー (Menu)] アイコン (☰) をクリックし、[設定 (Configure)] > [通知 (Notifications)] > [サブスクライバ (Subscribers)] を選択します。

ステップ 3 [サブスクライバの追加 (Add Subscriber)] をクリックします。

図 32: サブスクライバの追加

Add new user to the alert list ×

Email

i@cisco.com

Choose the types of alerts

Get notified when there's an incident triggered on Cisco Spaces platform issues on your inbox. Alerting gives timely awareness to problems with your locations or Cisco Spaces cloud, so you can resolve the problems quickly.

☐ **Scheduled Maintenance Notifications**
Get notified for any scheduled or critical maintenance activities.

☒ **Platform/Service Outage Alerts**
Get notified whenever there is a platform or service outage for Cisco Spaces or any of its cloud partners.

☒ **Network Connectivity Failure Notifications**
Get notified whenever there are any connectivity issues related to your wireless network.

☐ **Incoming Data Alerts**
Get notified whenever there is a drop or lag in location data received or processed by Cisco Spaces.

Add

[アラートリストに新しいユーザーを追加 (Add new user to the alert list)] スライドインウィンドウが表示されます。

ステップ 4 [電子メール (Email)] フィールドに、新規サブスクライバのメールアドレスを入力します。

ステップ 5 必要な **通知カテゴリ** のチェックボックスをオンにします。

オプトインすると、5 つの通知カテゴリの通知とインシデントアラートを受信できます。複数のカテゴリを選択できます。

ステップ 6 [Add] をクリックします。

新しいユーザーが通知サブスクライバリストに追加されます。

次のタスク

[通知サブスクライバ (Notification subscribers)] ウィンドウには、新しいサブスクライバの詳細が表示されます。[アクション (Actions)] 列を使用して、サブスクリプションを管理します。



第 **IX** 部

モニター

- ・ [モニタリングとサポート](#) (349 ページ)



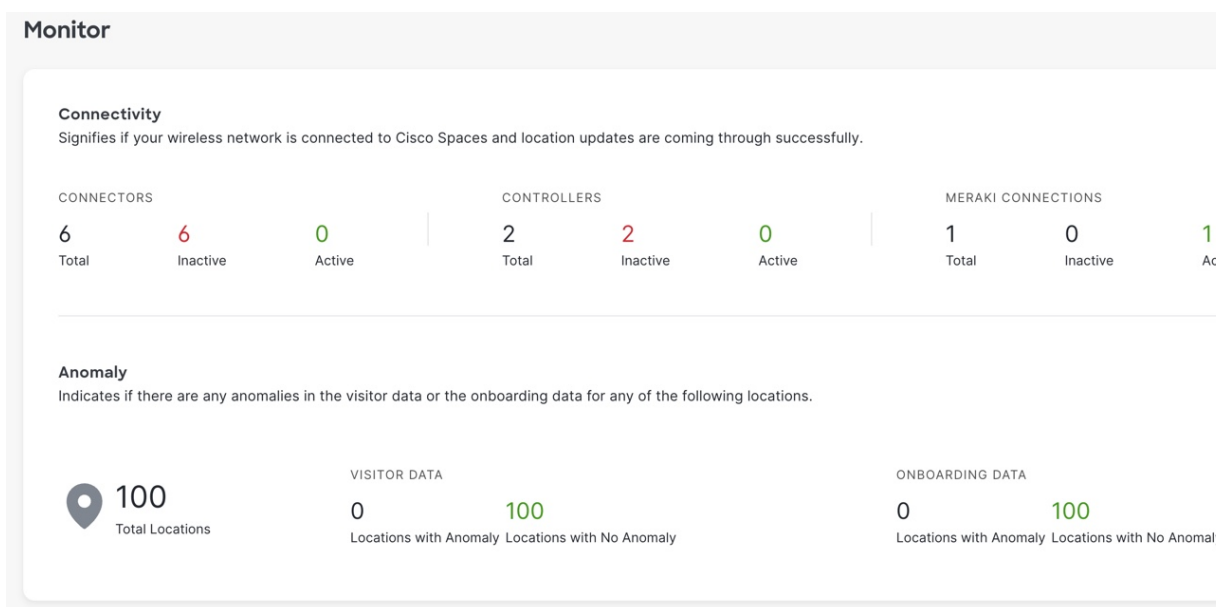
第 31 章

モニタリングとサポート

この章では、Cisco 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。

[モニター (Monitor)] ウィンドウにアクセスするには、**Cisco 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、[モニター (Monitor)] を選択します。

図 33: モニタ (Monitor)



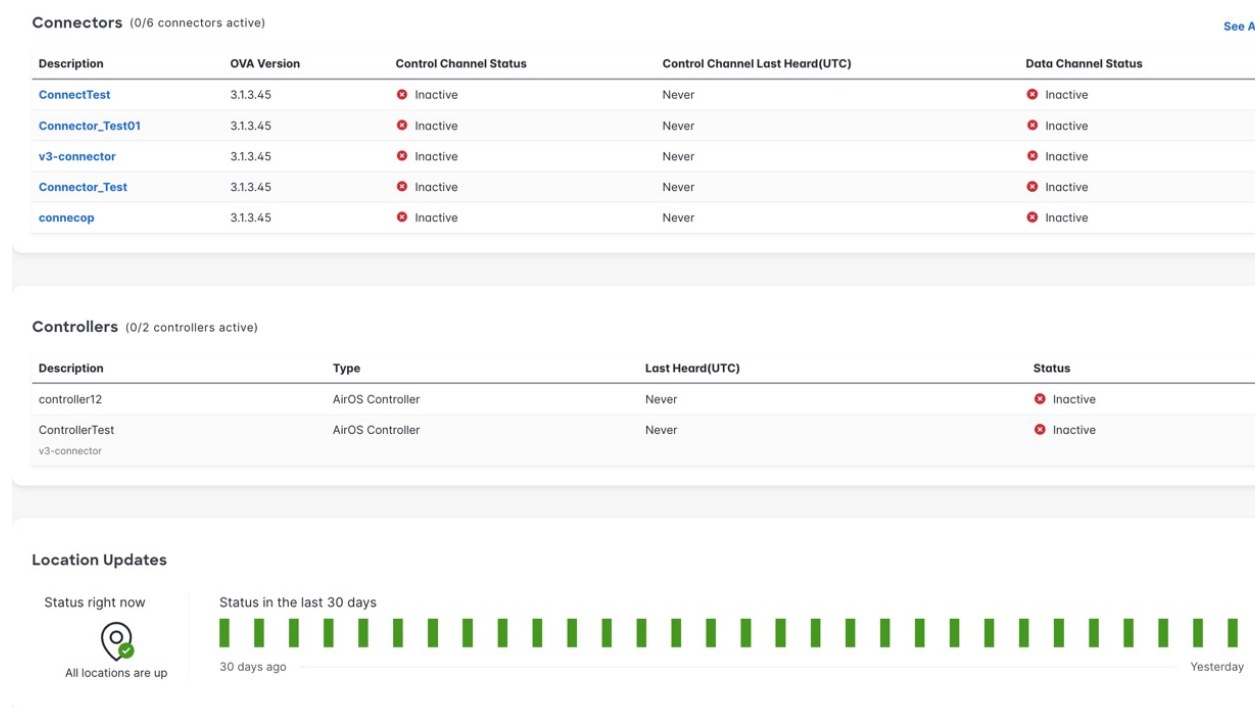
- [モニタリング \(349 ページ\)](#)
- [アプリ遅延 \(352 ページ\)](#)
- [エンタープライズアプリ \(353 ページ\)](#)
- [パートナーアプリ \(353 ページ\)](#)

モニタリング

このセクションでは、[モニター (Monitor)] セクションに表示される Cisco Spaces の正常性の詳細について説明します。

Cisco Spaces の [モニター (Monitor)] セクションを以下に示します。

図 34: 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「down」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 アプリケーション (DNA Apps)** : Cisco Spaces アプリケーションの現在のステータスを表示します。すべての Cisco Spaces アプリケーション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。
- パートナーアプリケーション (Partner apps)** : Cisco Spaces と統合されたパートナーアプリケーションの現在のステータスを表示します。このセクションは、Cisco Spaces と統合されているパートナーアプリケーションが期待どおりに機能している場合、「Up」と

マークされます。パートナーアプリケーションを Cisco Spaces と統合していない場合、またはパートナーアプリケーション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ケーション (Enterprise Apps)** : Cisco Spaces と統合されたエンタープライズアプリケーションの現在のステータスを表示します。このセクションは、Cisco Spaces と統合されているエンタープライズアプリケーション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ケーションを Cisco 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ケーション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、サブスクリバの正常性、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、サブスクリバの正常性、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、サブスクリバの正常性、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、サブスクリバの正常性、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 Kafka 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 **X** 部

管理者管理

- [Cisco Spaces のユーザーとアカウントの管理](#) (357 ページ)



第 32 章

Cisco Spaces のユーザーとアカウントの管理

この章では、Cisco Spaces ユーザーおよびアカウントを招待および管理する方法について説明します。

- [Cisco Spaces ユーザーの管理](#) (357 ページ)
- [Cisco Spaces アカウントの管理](#) (362 ページ)
- [ロケーションベースの RBAC](#) (362 ページ)

Cisco Spaces ユーザーの管理

Cisco 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 Spaces ダッシュボードでは、[メニュー (Menu)] アイコン(☰)をクリックし、[管理者管理 (Admin Management)] を選択して、管理ユーザーを管理し、ロールを作成します。

次のタブを使用できます。

- **管理者 (Admins)** : [管理者 (Admins)] タブを使用して Cisco Spaces ユーザーを表示し、新しい管理者を招待します。
[検索 (Search)] フィールドを使用して、既存のユーザーを検索します。
- **ロール (Roles)** : [ロール (Roles)] タブを使用してロールを検索し、新しいロールを作成して管理します。

Cisco Spaces ユーザーの招待

Cisco 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 **Dashboard Admin** は、他のユーザーを Cisco Spaces に招待できます。

Cisco 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。



(注)

- **Dashboard Admin Role** が他のロールタイプ（アプリケーション）へのアクセスを必要とする場合、たとえば **BLEManager** など、Cisco 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、**DNA Spaces** にのみアクセスできます。

Cisco Spaces では、さまざまなアプリケーション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。

使用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（アプリケーション）を含めることができます。



(注)

- Catalyst Center から **Mapservice** への重複ペイロードのインポートが制限されます。[インポート履歴 (Import History)] セクションに、次のエラーメッセージが表示されます。
「Warning: Import ignored due to no changes in request payload (警告: リクエストペイロードに変更がないためインポートは無視されます)」。
- 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、**DNA Spaces** と同時の場合にのみ **MapServices** をロールに割り当てられます。たとえば、**MapServices** への読み取りおよび書き込みアクセスと、**DNA Spaces** 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、**DNA Spaces** サービスと同時の場合にのみ、**Location Analytics** をロールに割り当てられます。たとえば、**Location Analytics** への読み取りおよび書き込みアクセスと、**DNA Spaces** 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。[ロケーション分析 (Location Analytics)] タイルは、Cisco Spaces ユーザーアカウントが [ロケーション分析 (Location Analytics)] へのアクセス権を持たない場合に無効になります。

Cisco Spaces ユーザーを招待するには、次の手順に従ってください。

手順

ステップ 1 Cisco Spaces ダッシュボードで、[メニュー (Menu)] アイコン (☰) をクリックし、[管理者管理 (Admin Management)] > [管理者 (Admins)] タブを選択します。

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) [電子メール (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) [ロール名 (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、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、[ロールの新規作成 (Create New Role)] を使用してユーザーロールを定義できます。
 - [ロールの新規作成 (Create New Role)] をクリックして新しいユーザーロールを作成します。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 \(359 ページ\)](#)」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 [ロール (Roles)] タブに一覧表示されます。
 - ロール名を選択すると、権限タイプとアプリケーションの詳細が [管理者を招待 (Invite Admin)] ウィンドウの下部に表示されます。

ステップ 4 選択したロールを特定の場所に制限する場合は、[このロールを特定の場所に制限 (Restrict this role to specific locations)] チェックボックスをオンにします。

- a) [ロケーションの追加 (Add Locations)] をクリックします。
- b) [ロケーションの選択 (Choose Locations)] ウィンドウで、ロケーション階層から必要なロケーションに対してチェックボックスをオンにします。選択されたロケーションが [選択されたロケーション (Selected Locations)] エリアに表示されます。
- c) [Done] をクリックします。

ステップ 5 [Invite] をクリックします。

(注)

- [管理者を招待 (Invite Admin)] オプションは、読み取りおよび書き込み権限を持つ Cisco Spaces 管理者のみが使用できます。
- キャプティブポータルなどの一部のアプリケーションには、その特定のアプリケーション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 キャプティブポータル アプリケーションユーザーは、キャプティブポータル アプリケーションの [ユーザー管理 (User Management)] オプションから、ユーザーロール **Creative User** または **Access Code Manger** を持つユーザーを招待できます。Admin Management ユーザーが [ユーザー管理 (User Management)] ウィンドウに表示されます。ただし、キャプティブポータルアプリケーションの [ユーザー管理 (User Management)] オプションからは、[管理者管理 (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 Spaces のユーザーロールを作成するには、次の手順を実行します。

手順

ステップ 1 Cisco Spaces ダッシュボードで、[メニュー (Menu)] アイコン (≡) をクリックし、[管理者管理 (Admin Management)] > [ロール (Roles)] > タブを選択します。

(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 2 [Create Role] をクリックします。

ステップ 3 [ロールの新規作成 (Create New Role)] スライドインウィンドウで、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 (アプリケーション) の詳細については、[Cisco Spaces ユーザーの招待 \(357 ページ\)](#) 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ケーション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スペース (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 [読み取り/書き込み (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。

ステップ 4 [このロールを特定の場所に制限 (Restrict this role to specific locations)] チェックボックスをオンにして、ロールのアクセスを特定の場所に制限します。

[+ロケーションの追加 (+ Add Locations)] オプションが表示されます。

ステップ 5 [+ロケーションの追加 (+ Add Locations)] をクリックしてロケーションを選択します。

- a) [ロケーションの選択 (Choose Locations)] スライドインウィンドウで、ロケーションに対するチェックボックスをオンにします。選択されたロケーションが[選択されたロケーション (Selected Locations)] ペインに表示されます。
- b) [更新 (Update)] をクリックします。

ステップ 6 [Create Role] をクリックします。

[管理者の招待 (Invite Admin)] ウィンドウの [ロール名 (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 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 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。

手順

ステップ 1 Cisco Spaces ダッシュボードで、[メニュー (Menu)] アイコン (☰) をクリックし、[管理者管理 (Admin Management)] を選択します。

[管理者 (Admin)] ウィンドウには、Cisco Spaces ユーザーの電子メール ID のリストが表示されます。

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。

[管理者を招待 (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。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 \(359 ページ\)](#)」を参照してください。

ステップ 4 [Update] をクリックします。

Cisco Spaces ユーザーの削除

あるユーザーが Cisco 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 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 Spaces ユーザーを削除するには、次の手順を実行します。

手順

ステップ 1 Cisco Spaces ダッシュボードで、[メニュー (Menu)] アイコン (☰) をクリックし、[管理者管理 (Admin Management)] を選択します。

[管理者 (Admin)] ウィンドウには、Cisco 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 [管理者の削除 (Delete Admins)] をクリックします。

Cisco Spaces アカウントの管理

ここでは、Cisco Spaces アカウントを管理する方法について説明します。

Cisco Spaces からのサインアウト

Cisco Spaces からサインアウトするには、次の手順を実行します。

手順

ステップ 1 Cisco 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 [ユーザーアカウント (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。

ロケーションベースの RBAC

ロールベースアクセスコントロール (RBAC) は、特定の場所をサポートするように拡張されました。[このロールを特定の場所に制限 (Restrict this role to specific locations)] オプションを使用して、ロールの作成中 ([管理者管理 (Admin Management)] > [ロール (Roles)] > [ロールの作成 (Create Role)]) およびユーザーの招待フロー中 ([管理者管理 (Admin Management)] > [管理者の招待 (Invite Admin)]) に特定の場所をサポートします。



第 **XI** 部

設定

- [ワイヤレスネットワークのセットアップ \(365 ページ\)](#)
- [有線ネットワークのセットアップ \(373 ページ\)](#)
- [Map Service の設定 \(375 ページ\)](#)
- [ロケーションとマップを設定する \(377 ページ\)](#)
- [Meraki カメラの設定 \(401 ページ\)](#)
- [センサーの設定 \(407 ページ\)](#)
- [データエクスポートの設定 \(409 ページ\)](#)
- [Cisco Webex の設定 \(417 ページ\)](#)
- [pxGrid クラウドのセットアップ \(421 ページ\)](#)
- [アクセスポイント自動ロケーションの設定 \(425 ページ\)](#)



第 33 章

ワイヤレスネットワークのセットアップ

この章では、多様なワイヤレスネットワークと連動するように Cisco Spaces を設定する方法と、さまざまな方法でこれらのネットワークを設定する方法について説明します。

- [さまざまなワイヤレスネットワークで機能するための Cisco Spaces の設定 \(365 ページ\)](#)
- [ワイヤレスネットワークバー \(366 ページ\)](#)
- [Meraki API キーメソッドのセットアップ \(370 ページ\)](#)

さまざまなワイヤレスネットワークで機能するための Cisco Spaces の設定

次のオプションに基づいて、ワイヤレスネットワークを使用して Cisco Spaces をセットアップできます。

- Cisco AireOS ワイヤレスコントローラ
- Cisco Catalyst 9800 ワイヤレスコントローラ
- Cisco Meraki

手順

ステップ 1 Cisco Spaces にログインします。

ステップ 2 Cisco Spaces ダッシュボードで[メニュー (Menu)] アイコン (☰) をクリックし、[セットアップ (Setup)] > [ワイヤレスネットワーク (Wireless Networks)] の順に選択します。

ステップ 3 [Connect your wireless Network] ウィンドウで、[Add New] をクリックします。

[ワイヤレスネットワークの接続 (Connect your wireless Network)] ウィンドウが表示され、[Cisco AireOS/Catalyst] および [Cisco Meraki] オプションが表示されます。

- **Cisco AireOS/Catalyst** の場合、次の方式で設定できます。

- **Spaces コネクタ経由** : Cisco Spaces : コネクタ を使用して Cisco Spaces を シスコ ワイヤレス コントローラに接続します。
- **CMX テザリング経由で接続** : Cisco CMX を使用して Cisco 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、次の方式で設定できます。
 - **APIキーによる接続 (Connect via API Key)** : Cisco Meraki API キーを使用して Cisco Spaces を Cisco Meraki に接続します。

[Meraki] ダッシュボードにログインし、[Account Name] > [My Profile] > [API Access] セクションを選択し、[Generate] をクリックして API キーを生成します。このキーを Cisco Spaces ダッシュボードの [APIキーによる接続 (Connect via API Key)] フィールドに入力して、ネットワークを Cisco Spaces に追加します。詳細については、[Meraki API キーメソッドのセットアップ \(370 ページ\)](#) を参照してください。

(注)
新しい Cisco Spaces アカウントの場合は、[開始 (Get Started)] オプションをクリックします。

ステップ 4 [選択 (Select)] をクリックして、Cisco Spaces に接続するときの優先方式を選択します。
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。

ステップ 5 [Customize Setup] をクリックします。
次のメッセージが表示されます。「Successfully saved the configuration (設定が正常に保存されました)」。

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に対応するバーが、[ワイヤレスネットワークの接続 (Connect your wireless network)] ウィンドウに表示されます。たとえば、[Spacesコネクタ経由 (Via Spaces Connector)] を選択すると、[Spacesコネクタ経由で接続 (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。
さまざまな方法を使用して優先ワイヤレスネットワークに接続する手順と機能が表示されます。

ステップ 8 画面の指示に従って[ワイヤレスネットワークを追加](#)します。

ワイヤレスネットワークバー

ワイヤレスネットワークを Cisco Spaces に接続するには、[セットアップ (Setup)] > [ワイヤレスネットワーク (Wireless Network)] > [ワイヤレスネットワークの接続 (Connect your wireless network)] ウィンドウで使用可能なオプションを使用します。

図 35: ワイヤレス ネットワーク

Connect your wireless network

What type of wireless network do you have?

Cisco Spaces works with most Cisco wireless networks including Cisco Meraki.

AireOS Controller/Catalyst 9800 Wireless Controller Choose this for Cisco Aironet Access Points with Cisco Wireless Controllers or CMX On-Prem Tethering. Select	Cisco Meraki Choose this for Cisco Meraki networks with Meraki Access Points Select

選択内容に基づいて、Cisco Meraki に対して以下のタブが表示されます。

- **Meraki API キーによる接続 (Connect via Meraki API Key)** : このオプションを使用して、Cisco Spaces を Cisco Meraki クラウドコントローラに Cisco Meraki API キーを使用して接続します。画面の指示に従って、**ネットワークのインポート** オプションを使用して、Cisco Meraki 組織と関連する子ロケーションをロケーション階層にインポートします。



(注) Meraki を Cisco Spaces に接続するには、**API キーによる接続** を使用することを推奨します。

次の手順を実行します。

1. **Meraki の接続** : API キーを使用して Cisco Meraki を Cisco Spaces に接続します。
2. **Meraki スキャン API の設定** : Cisco Meraki スキャン API は、ネットワークをロケーション階層にインポートした後に自動的に設定されます。



(注) 手動で設定する場合は、**Post URL** と URL バリデータおよび**秘密キー**を使用して、Cisco Meraki ダッシュボードで手動で検証し、Cisco Spaces との接続を確立します。

3. **Meraki ネットワークをロケーション階層にインポート** : [ネットワークのインポート (Import Networks)] をクリックして、Cisco Meraki ネットワークをインポートします。

選択した接続方法に基づいて、Cisco AireOS に対して次のバーが表示されます。

- **Spacesコネクタ経由で接続 (Connect via Spaces Connector)** : Cisco Spaces : コネクタ を使用してシスコ ワイヤレス コントローラに Cisco Spaces を接続するには、このオプションを使用します。



(注) **Spacesコネクタ経由で接続オプションを使用する場合**、シスコ ワイヤレス コントローラをアップグレードしたり、ワイヤレス ネットワークを再設定したりする必要はありません。

次の手順を実行します。

1. **Spaces コネクタ OVA のインストール** : Cisco Spaces : コネクタ OVAを仮想マシンとしてダウンロードしてインストールします。
2. **Spaces コネクタの設定** : [コネクタの作成 (Create Connector)] をクリックして、新しいコネクタを作成します。Cisco Spaces : コネクタ を設定するには、トークンが必要です。トークンを設定するには、ブラウザから <https://<your connector IP>/> に接続する必要があります。オプションで、HTTPS プロキシ経由で Cisco Spaces : コネクタ を接続するように設定できます。
[コネクタの表示 (View Connectors)] をクリックして、使用可能なコネクタを表示します。
3. **コントローラの追加** : [コントローラの追加 (Add Controllers)] をクリックして、シスコ ワイヤレス コントローラを追加します。[コントローラの表示 (View Controllers)] をクリックして、使用可能なコントローラを表示します。
4. **マップのインポート** : [マップのインポート/同期 (Import/Sync Maps)] をクリックして、マップをインポートまたは同期します。Cisco Prime Infrastructure または Catalyst Center (バージョン 1.3.1 以降) のマップをアップロードして、Cisco Spaces : Detect and Locate、アセットトラッカー、および IoT サービスを使用する必要があります。
5. **ロケーション階層のセットアップ** : [ロケーションの追加 (Add Locations)] をクリックして、インポートしたマップをロケーション階層に追加します。



(注)

- [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 アプリケーションの場合、[OpenRoaming ホットスポットの追加 (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、[OpenRoaming コントローラ設定 (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。
- ネットワーク設定プロトコル (NETCONF) のサポートは、ホットスポットクライアントバージョン v2.2.95 および Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ バージョン 17.12 から利用できます。

詳細については、『[Cisco Spaces : コネクタ コンフィギュレーションガイド](#)』を参照してください。

- **AireOS コントローラ/Catalyst 9800 ワイヤレスコントローラの直接接続**：このオプションを使用して、Cisco 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 コントローラに直接接続します。



(注)

このワイヤレスネットワークに接続するには、ソフトウェアバージョン 8.8 MR2 以降の AireOS コントローラ、またはソフトウェアバージョン 16.12.2 以降の Catalyst 9800 ワイヤレスコントローラが必要です。ワイヤレスコントローラはインターネットに直接接続できる必要があります。

次の手順を実行します。

1. **ルート証明書のインストール**：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。
2. **AireOS コントローラでトークンを設定**：トークンとコントローラを表示するには、[トークンを表示 (View Token)] および [コントローラを表示 (View Controllers)] オプションを使用します。
3. **マップのインポート**：[セットアップ (Setup)] ウィンドウの [WLC/Catalyst 9800 に直接接続 (Connect WLC/Catalyst 9800 Directly)] および [Spaces コネクタ経由で接続 (Connect Via Spaces Connector)] でマップを管理できます。

- **マップのインポート/同期**：Cisco Prime Infrastructure または Catalyst Center マップをアップロードして、検出と特定、アセットトラッカー、IoT サービスとシームレスに連携します。
- **[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。

4. ロケーション階層のセットアップ

- **CMX テザリング経由で接続**：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 [トークンの新規作成 (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。

[ワイヤレスネットワークの接続 (Connect your wireless network)] ウィンドウで利用できるその他のオプションは次のとおりです。

表 16: ワイヤレスネットワークの接続のオプション

設定手順の表示	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。
システム要件	Cisco Spaces のシステム要件を示します。
よくある質問	Cisco Spaces に関するよくある質問へのリンクが表示されます。
Cisco AireOS/Catalyst	CMX ノード (CMX オンプレミス) を [ロケーション階層 (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 [ロケーション階層 (Location Hierarchy)] ウィンドウにインポートする手順を表示します。

Meraki API キーメソッドのセットアップ

Cisco Meraki オプションを使用して、Cisco Spaces を Meraki と統合します。Meraki アカウントのログイン情報を使用して Cisco Meraki クラウドに接続し、ロケーションを Cisco Spaces にインポートして、Meraki ネットワークをアクティブ化または同期します。

手順

- ステップ 1** Cisco Spaces ダッシュボードで、[メニュー (Menu)] アイコン (≡) をクリックし、[セットアップ (Setup)] > [ワイヤレスネットワーク (Wireless Network)] > [新規追加 (Add New)] > [Cisco Meraki] > [APIキーによる接続 (Connect via API key)] を選択します。
- ステップ 2** Meraki ダッシュボードで、[Organization] > [Configure] > [Settings] に移動し、[Dashboard API Access] を有効にします。
- ステップ 3** Meraki ダッシュボードで、[Username] > [My Profile] > [API Access] に移動し、API トークンを生成します。生成された API トークンは英数字の値です。
- ステップ 4** 生成された API トークンをコピーして、Cisco Spaces ダッシュボードに入力します。
- ステップ 5** Cisco Spaces ダッシュボードで次の手順を実行します。
- [Connect our Meraki] ポップアップウィンドウで、コピーした API トークンを [API KEY] フィールドに貼り付けます。

Connect your Meraki



Connect via API key

Enter your Meraki API Key to fetch the network information

API KEY

Add API

Connect

- [Connect] をクリックします。Meraki との同期が成功すると、接続ステータスがアクティブとして表示されます。
 - [Configure Meraki scanning API] 領域から、[Post URL] と [Secret Key] の値をコピーします。
- ステップ 6** Meraki ダッシュボードで、特定のネットワークに移動し、[Network-wide] > [Configure] > [General] を選択します。
- ステップ 7** [Location and Scanning] まで下にスクロールし、[Analytics and Scanning API] を有効にします。
- ステップ 8** [ポストURL (Post URLs)] フィールドにポスト URL と秘密鍵を貼り付けます。

- ステップ 9** Web ブラウザのアドレスバー（Meraki URL）から、`network_id`（/n/の後）をコピーします。例：
https://xxxx.meraki.com/your-net/n/network_id/。
- ステップ 10** 投稿 URL `<network_id>` をネットワーク ID を含めるように編集します。
- ステップ 11** [Location and Scanning] フィールドから、`validator id` をコピーします。
- ステップ 12** 投稿 URL `<URLValidator>` をバリデータを使用して編集します。
- ステップ 13** [Validate] をクリックして、投稿 URL 関数を検証します。
- ステップ 14** Cisco Spaces ダッシュボードで、[Meraki ネットワークをロケーション階層にインポート（Import Meraki Networks into Location Hierarchy）] から [ネットワークのインポート（Import Networks）] を選択します。
- 同期が成功したら、ネットワークが [ロケーション階層（Location Hierarchy）] に表示されるかどうかを確認します。
- （注）
Cisco Meraki ダッシュボードで IP アドレス制限が有効になっている場合、Cisco Spaces サポートに連絡して Cisco Spaces IP アドレスを許可リストに追加します。
-



第 34 章

有線ネットワークのセットアップ

・有線ネットワークのセットアップ (373 ページ)

有線ネットワークのセットアップ

Cisco Spaces : コネクタを使用すると、有線ネットワークとワイヤレスネットワークを Cisco Spaces に接続できます。

有線ネットワークをセットアップするには、Cisco Catalyst 9300 シリーズ スイッチが必要であり、Cisco Spaces : コネクタが仮想マシンにインストールされている必要があります。

Cisco Spaces : コネクタ 3.0 が、メニュー () > [Setup] > [Wired Network] セクションで利用できるようになりました。[Wired Network] で 2.x と 3.0 の両方のコネクタを作成できます。

サービスの関連付け、インスタンスの追跡、メトリックの可視化などのコネクタ 3.0 機能を [Wired Network] セクションで利用できます。

Cisco Spaces : コネクタのセットアップの詳細については、次の場所にある Cisco Spaces : コネクタ コンフィギュレーションガイドを参照してください。

https://www.cisco.com/c/en/us/td/docs/wireless/spaces/connector/config/b_connector_30.html。

2023 年 12 月以降、Cisco Spaces : コネクタ 2.x はメンテナンスモードに入り、2024 年 6 月までセキュリティ更新のみが利用可能になります。延長サポートは重大なバグ修正に限定され、2024 年 10 月まで提供されます。コネクタ 3 にアップグレードすることを強く推奨します。

コネクタ 2.x からコネクタ 3 に移行するには、「[Migrate from Connector 2.x to Connector 3](#)」を参照してください。



第 35 章

Map Service の設定

この章では、**Map Service** で使用できる機能について説明します。

- [Map Service の設定 \(375 ページ\)](#)

Map Service の設定

Cisco Spaces の **Map Service** を使用して、異なるサイトにある同じ名前の複数のキャンパスを Catalyst Center から Cisco Spaces **ロケーション階層** にインポートまたは同期します。Catalyst Center 内のサイト間でキャンパスを移動し、これらの変更を Cisco Spaces **ロケーション階層** にシームレスにインポートして同期できます。

Cisco Spaces の **Map Service** には、インポートされたマップデータと **ロケーション階層** 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 Catalyst Center からエクスポートされ、[マップサービス (Map Service)] を使用して Cisco Spaces にインポートされたマップは、[ロケーション階層 (Location Hierarchy)] に自動的に表示されます。
- さまざまなソース、Catalyst Center、Cisco Prime Infrastructure、または Cisco Meraki からマップをインポートまたは同期する場合、サポートが拡張され、ネットワーク階層が単一のビジネス指向の階層に正規化および統合されます。
- [Location Hierarchy] からロケーションを削除すると、[Map Service] から削除されます。
- [マップサービス (Map Service)] UI からゾーンのロケーションを削除すると、同じものが [ロケーション階層 (Location Hierarchy)] から削除されます。
- AP インポート制限は、Cisco 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)
- マップを操作するときは、Google Chrome ブラウザを使用することをお勧めします。マップの操作は、Google Chrome で最もよくサポートされています。他のブラウザでのマップアクションは制限されています。
 - 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。

Cisco Prime InfrastructureからCatalyst Centerへのマップ階層移行のサポート：Cisco Spaces ロケーション階層は、Cisco Prime InfrastructureからCatalyst Centerへのネストされたサイトの移行データのインポートをサポートします。

Cisco DNA Center のネストされたサイト階層のサポート：新しいサイトをCatalyst CenterからCisco Spacesの既存のサイト階層の上にインポートまたは同期できます。

計画されたアクセスポイント（AP）インポートのサポート：計画された AP を Map Service にインポートできます。

マップのアップロード

[マップのアップロード (Maps Upload)] をクリックして、Cisco Prime Infrastructure または Catalyst Centerからマップをアップロードします。[マップのアップロード (Maps Upload)] ポップアップウィンドウで、必須アクションを選択し、[ファイルの選択 (Select File)] をクリックして、送信元からダウンロードしたマップをアップロードします。



- (注) [アップロード履歴 (Upload History)] をクリックして、マップのアップロード履歴の詳細を表示します。

Cisco Catalyst Wireless 9164I Wi-Fi 6E シリーズ アクセスポイント（AP）サポート

Cisco Catalyst Wireless 9164I Wi-Fi 6E シリーズ AP サポートが [Map Service] に追加されました。

Map Service を使用して、Cisco Catalyst Wireless 9164I Wi-Fi 6E シリーズ AP を Cisco Spaces にインポートできるようになりました。



第 36 章

ロケーションとマップを設定する

- [ロケーションとマップ \(377 ページ\)](#)
- [ロケーションのインポート \(381 ページ\)](#)
- [ネットワークマップの追加 \(395 ページ\)](#)
- [デジタルマップの追加 \(397 ページ\)](#)

ロケーションとマップ

Cisco Spaces のロケーションとマップ機能を使用すると、Cisco Meraki、Catalyst Center、Cisco Prime Infrastructure などさまざまなソースからのネットワーク階層をインポートし、正規化して、単一のビジネス指向のロケーション階層に統合できます。この機能をプラットフォームとして使用して、ネットワーク階層構造を標準化し、標準化されたロケーション階層ビューを提供します。

ネットワークソースからインポート/同期してロケーション階層を作成する従来の方法とは別に、Microsoft Excel (.xlsx) ファイルからビジネス中心の階層を作成する新しいオプションが含まれています。Microsoft Excel (.xlsx) ファイルのインポートでは、複数のロケーションのメタデータ情報を一括で追加/更新できます。

Cisco Spaces はネットワーク階層に一致する論理的なロケーション階層を作成しますが、ほとんどの Cisco Spaces ユーザーには、分類法や、異なるチーム/人物によって管理されるため、階層/名前が異なるソースがもう 1 つあります。ロケーションとマップ機能を使用すると、ビジネス指向の階層を作成し、さまざまなネットワークソースの階層をビジネス階層にマージ/統合して、クリーンな統合階層にすることができます。これにより、さまざまな成果の管理に役立ちます。

物理的なビジネスロケーションとネットワーク展開に基づいて、ビジネスロケーションをインポートし、Cisco Spaces 内で整理できます。階層は、特定のブランド、地域、キャンパス、およびビジネスに関連するその他の分類に基づいてまとめることができます。

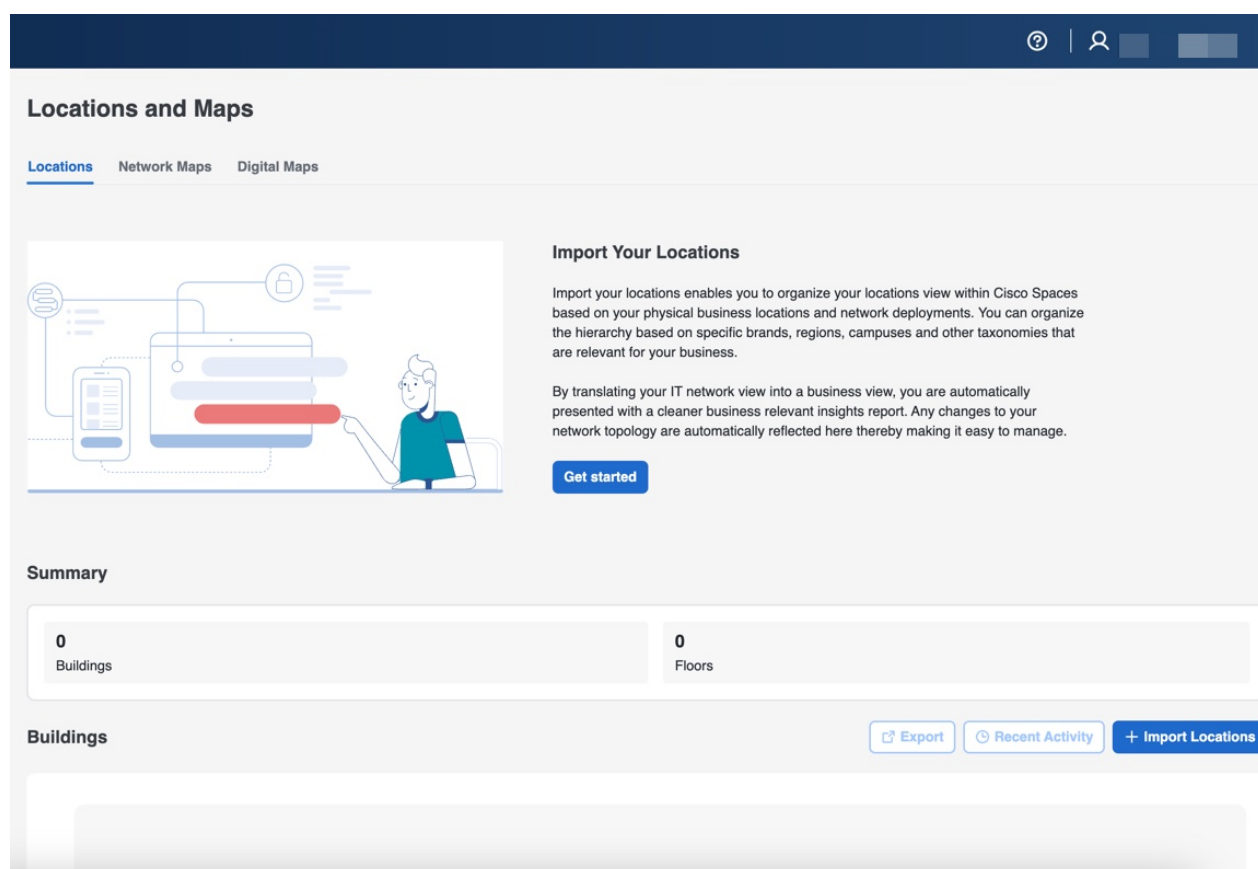
Cisco Spaces のロケーションとマップ機能は、IT ネットワークビューをビジネスビューに変換し、よりビジネス関連のインサイトレポートを表示するのに役立ちます。ネットワークトポロジへの変更は Cisco Spaces に自動的に反映されるため、管理が容易になります。

[ロケーションとマップ (Locations and Maps)] ウィンドウには次のタブがあります。

- **ロケーション (Locations)** : このタブを使用して、ロケーションを追加または管理します。
- **ネットワークマップ (Network Maps)** : このタブを使用してネットワークマップを追加します。
- **デジタルマップ (Digital Maps)** : このタブを使用して、デジタルマップを追加または管理します。

これらのタブで利用できる [フィルタ (Filter)] オプションを使用して [フィルタ (Filter)] スライドインウィンドウを開き、フィルタオプションを選択してロケーションデータを適用して表示します。

図 36: ロケーションとマップ



ロケーションタブ

[ロケーション (Locations)] タブの [サマリー (Summary)] セクションには、建物とフロアの数が表示されます。[ロケーション (Locations)] タブの [建物 (Buildings)] セクションには、インポートされたロケーションに関連する次の情報が表示されます。

- 名前
- パス

- フロア数
- ソース
- 必須ロケーション情報

次のタスクを実行します。

- [ロケーションの検索 (Search Locations)] フィールドに建物名を入力し、指定した建物情報をフィルタ処理します。
- ロケーションデータをエクスポートするには、[エクスポート (Export)] をクリックします。[ダウンロード (Download)] をクリックすると、同じものをダウンロードできます。
- [最近のアクティビティ (Recent Activity)] をクリックして [最近のアクティビティ (Recent Activity)] ウィンドウを開き、最近のアクティビティの詳細を表示します。
- [ロケーションのインポート (Import Locations)] をクリックして、ロケーションをインポートします。詳細については、[ロケーションのインポート \(381 ページ\)](#) を参照してください。

ネットワークマップタブ

[ネットワークマップ (Network Maps)] タブには、インポートされたロケーション情報も表示されます。[ネットワークマップ (Network Maps)] タブの [建物 (Buildings)] セクションには、インポートされたロケーションに関連する次の情報が表示されます。

- 名前
- パス
- フロア数
- APの数
- 送信元
- ネットワークマップのステータス

次のタスクを実行します。

- [ロケーションの検索 (Search Locations)] フィールドに建物名を入力し、指定した建物情報をフィルタ処理します。
- [最近のアクティビティ (Recent Activity)] をクリックして [最近のアクティビティ (Recent Activity)] ウィンドウを開き、最近のアクティビティの詳細を表示します。
- [ネットワークマップの追加 (Add Network Map)] をクリックして、ネットワークマップを追加します。詳細については、「[ネットワークマップの追加 \(395 ページ\)](#)」を参照してください。

デジタルマップタブ

[デジタルマップ (Digital Maps)] タブには、インポートされたロケーション情報も表示されます。

[建物 (Buildings)] セクションは[デジタルマップ (Digital Maps)] タブにあり、インポートされたロケーションに関連する次の情報が表示されます。

- 名前
- パス
- フロア数
- APの数
- ステータス
- アクション

次のタスクを実行します。

- [ロケーションの検索 (Search Locations)] フィールドに建物名を入力し、指定した建物情報をフィルタ処理します。
- [最近のアクティビティ (Recent Activity)] をクリックして[最近のアクティビティ (Recent Activity)] ウィンドウを開き、最近のアクティビティの詳細を表示します。
- [アクション (Actions)] 列の[デジタルマップの追加 (Add Network Map)] をクリックして、デジタルマップを追加します。詳細については、[デジタルマップの追加 \(397ページ\)](#)を参照してください。
- また、[アクション (Actions)] 列の[CADファイルのアップロード (Upload CAD File)] をクリックして、選択したロケーションにデジタルマップを追加することもできます。

デジタルマップ：ユーザー体験の強化

Cisco Spaces ダッシュボードでは、次の機能強化が加えられました。

- [フロアの選択 (Select Floor)] ウィンドウは、ユーザーの労力を最小限に抑えるように再設計されました。新しい設計では、ユーザーが必要とするエントリの数が減り、各フロアのフロアレベル番号と短縮名が自動的に生成されるため、プロセスがより迅速かつ効率的になります。
- ファイルアップロードプロセスが強化され、効率が向上しました。複数のフロアのファイルを同時にアップロードし、それぞれを並行して処理できるようになりました。以前は1つのフロアのアップロード中に表示されていたフルページローダーが、各フロア用の個々のローダーインジケータに置き換えられ、各アップロードのステータスを明確に表示できるようになりました。

いずれかのフロアファイルにさらに時間が必要な場合は、他のアップロードの進行に影響を与えずに、その特定のアップロードをキャンセルするオプションがあります。これによ

り、正常なアップロードの管理が改善され、より効果的な時間割り当てが可能になります。

- **推定時間と電子メール通知を使用するマップ処理ステータスレポート**：マップ処理機能が強化され、マップ生成に時間のかかる場合に報告された問題に対処しました。この機能強化により、マップを正常に送信すると、ウィンドウで推定処理時間が表示されます。[Digital Maps] リストビューで各建物のステータスメッセージにカーソルを合わせることで、暫定的な ETA やエラーの詳細を含む処理ステータスを表示することもできます。さらに、送信者はマップステータスの変更に関する電子メール通知を受け取ります。
- **マップの再処理/CAD ファイルの再送信**：マップの再処理の使用方法が強化され、必要な変更を正確に指定できる機能が追加されました。これにより、ターンアラウンド時間を短縮できます。一般的な理由のリストから選択し、再処理要求の証拠として補足ドキュメントまたは画像とともに追加のコメントを指定できます。

ネットワークマップのキャリブレーション

ネットワークマップのキャリブレーションツールを使用すると、2D ネットワークマップ画像と 3D デジタルマップを正確に配置できます。[Digital Map Editor] からツールにアクセスして、クライアントとアクセスポイントの位置が正確に表示されるように、GPS マーカーを正確に配置できます。

ネットワーク マップ キャリブレーション リンクは、ネットワークマップに関連付けられているマップに対してのみユーザーインターフェイスで有効になります。

ロケーションのインポート

[ロケーション (Locations)] タブを使用して、ビジネス階層をインポートします。

手順

ステップ 1 Cisco Spaces にログインします。

ステップ 2 Cisco Spaces ダッシュボードで、[メニュー (Menu)] アイコン (≡) をクリックし、[セットアップ (Setup)] > [ロケーションとマップ (Locations and Maps)] を選択します。

[ロケーションとマップ (Locations and Maps)] ウィンドウは、[ロケーション (Locations)] タブが選択された状態で表示されます。使用可能なその他のタブは [ネットワークマップ (Network Maps)] および [デジタルマップ (Digital Maps)] です。

ステップ 3 [ロケーション (Locations)] タブで、[ロケーションの追加 (Add Locations)] をクリックします。ロケーションがすでにインポートされ利用可能な場合は、[ロケーションのインポート (Import Locations)] オプションが表示されます。

[建物の詳細のアップロード (Upload Building Details)] ウィンドウには、ロケーションをアップロードするためのさまざまな方法が表示されます。

図 37: 建物の詳細をアップロード

Upload Building Details

Select a method from below to upload your locations

Import buildings from Excel sheet (preferred)

Have a spreadsheet with details of your business locations? You can use that to import your buildings, update location info, time zone, address, etc which are critical for apps in Cisco Spaces.

Import locations from Prime Infrastructure

Use this method if you have an export from Prime Infrastructure. You can always import the network hierarchy from Prime and connect them to the business locations using excel import anytime.

Import locations from DNA Center

Have a DNA Center deployment in place. You can connect Cisco Spaces to DNA Center, and all your sites/buildings defined in DNA Center will be synced by Cisco Spaces.

Import locations from Meraki

If you have a Meraki deployment, use this method to connect to your Meraki Cloud account to sync the network hierarchy, maps, access points, Meraki video devices, etc.

Cancel Next

ステップ 4 次の方法を使用してロケーションをインポートします。

- [Excel シートからの建物のインポート](#) (推奨)
- [Cisco Prime Infrastructure からロケーションをインポート](#)
- [Catalyst Center からロケーションをインポート](#)
- [Cisco Meraki からロケーションをインポート](#)
- [手動によるロケーションの追加](#)

インポートされたロケーションの詳細が、[ロケーション (Locations)] タブに表示されます。

- [サマリー (Summary)] セクションには、建物、フロア、欠落しているロケーションメタデータ情報、および確認が必要なロケーションの詳細が表示されます。
- [ロケーション (Locations)] タブの [建物 (Building)] セクションには、名前、パス、フロア数、送信元などのロケーションの詳細が表示されます。
- 必要なロケーションメタデータが更新されていない場合、[建物 (Building)] セクションの [必須ロケーション情報 (Essential Location Info)] フィールドにアラートが表示されます。

ステップ 5 [必須ロケーション情報 (Essential Location Info)] フィールドの [アラート (Alert)] アイコン (🚨) をクリックして、必要に応じて不足しているメタデータを追加します。

ポップアップウィンドウには、欠落しているロケーションメタデータに関連する情報が表示されます。[ここをクリック (Click Here)] をクリックしてロケーション情報を更新してください。

ステップ 6 [確認 (Review)] をクリックして、ロケーションレビューを表示し、続行します。詳細については、「[ロケーションを確認](#)」を参照してください。

Excel シートから建物をインポートする以外の方法を使用してロケーションをインポートすると、[確認 (Review)] オプションが表示されます。

ステップ 7 (オプション) [ロケーション (Locations)] タブで、必要に応じて次のオプションを使用します。

- **エクスポート (Export)** : インポートされたビジネスロケーションの詳細を Microsoft Excel ファイル (.xls) にエクスポートします。[ダウンロード (Download)] をクリックすると、同じものをダウンロードできます。
- **[最近のアクティビティ (Recent Activity)]** : クリックすると、最近のアクティビティの詳細が表示されます。ウィンドウの [最近のアクティビティ (Recent Activity)] スライドには、アクティビティの最近の履歴が表示されます。
 - ファイル名
 - ユーザ
 - タイプ
 - 時間
 - ステータス
- **[フィルタ (Filter)]** : クリックしてフィルタオプションを表示します。表示される [フィルタ (Filter)] スライドインウィンドウで、[ロケーション (Locations)] ドロップダウンリストからロケーションを選択し、必要なフィルタオプションを選択し、[適用 (Apply)] をクリックします。フィルタオプションは、[送信元 (Source)]、[フロア数 (# of Floors)]、および [ロケーションメタデータ (Location Metadata)] です。

Microsoft Excel シートからの建物のインポート

Microsoft Excel (.xlsx) ファイルをインポートしてロケーションを追加するには、[Excelシートから建物をインポート (Import buildings from Excel sheet)] オプションを使用します。Cisco Spaces アプリケーションに重要な建物、ロケーションメタデータ、タイムゾーン、アドレスなどを含むロケーションをインポートするには、この方法を選択することを推奨します。

手順

ステップ 1 Cisco Spaces にログインします。

- ステップ 2** Cisco Spaces ダッシュボードで、[メニュー (Menu)] アイコン (≡) をクリックし、[セットアップ (Setup)] > [ロケーションとマップ (Locations and Maps)] を選択します。
- [ロケーションとマップ (Locations and Maps)] ウィンドウは、[ロケーション (Locations)] タブが選択された状態で表示されます。
- ステップ 3** [ロケーション (Locations)] タブで、[ロケーションの追加 (Add Locations)] をクリックします。ロケーションがすでにインポートされ利用可能な場合は、[ロケーションのインポート (Import Locations)] オプションが表示されます。
- [建物の詳細のアップロード (Upload Building Details)] ウィンドウには、ロケーションをアップロードするためのさまざまな方法が表示されます。
- ステップ 4** [Excelシートからの建物のインポート (Import buildings from Excel sheet)] をクリックし、[次へ (Next)] をクリックします。
- ステップ 5** [ロケーションの詳細のインポート (Import Location Details)] ウィンドウで、Microsoft Excel (.xlsx) ファイルをドラッグアンドドロップするか、[ここをクリックしてアップロード (Click here to upload)] をクリックして、インポートするビジネスロケーションの詳細を含む Microsoft Excel (.xlsx) ファイルをアップロードします。
- (注)
- テンプレートがない場合は、[ロケーションの詳細のインポート (Import Location Details)] ウィンドウにあるリンクからテンプレートをダウンロードし、建物の詳細とともに正しい形式でアップロードできます。
- ステップ 6** [Next] をクリックします。
- [ロケーションの詳細のインポート (Import Location Details)] ウィンドウでは、左側の列に Microsoft Excel (.xlsx) ファイルのロケーション情報が、右側の列に既存のロケーションレベルおよびグループレベルの情報が表示されます。
- ステップ 7** [ロケーションの詳細のインポート (Import Location Details)] ウィンドウで、[CSVの列 (Column from CSV)] 列のインポートされたロケーションメタデータを、[リンク先 (Link to)] ドロップダウン下の対応する階層およびグループレベルにマッピングし、それに応じて、それぞれのロケーションメタデータを割り当てます。
- [リンク先 (Link to)] ドロップダウンで利用できるオプションは次のとおりです。
- **ロケーション情報 (Location Info)** : 国、市区町村、占有率、バンド、アドレス、タイムゾーンなどのロケーションのメタデータ情報に使用します。対応するメタデータ値も割り当てる必要があります。
 - **階層レベル (Hierarchy Level)** : Microsoft Excel (.xlsx) ファイルから [レベル (Level)] 列の値をマッピングするには、これを使用します。Microsoft Excel (.xlsx) ファイルには、複数の [レベル (Level)] 値を設定できます。Microsoft Excel (.xlsx) ファイルからのレベル値は、ロケーション階層の [階層レベル (Hierarchy Level)] としてマッピングされます。
- 階層レベルごとに、グループ化レベルの値を割り当てることができます。オプションは、[グループ化レベル1 (Grouping Level1)]、[グループ化レベル2 (Grouping Level2)]、および [グループ化レベル3 (Grouping Level3)] です。

Microsoft Excel (.xlsx) ファイルでは、**NYC1 Campus** を **レベル1**、**NYC2 Campus** を **レベル2** に設定できます。[ロケーションの詳細のインポート (Import Location Details)] ウィンドウでは、**レベル1** および **レベル2** を [リンク先 (Link to)] ドロップダウンリストの [階層レベル (Hierarchy Level)] にマッピングできます。**レベル1**の場合、グループ化値を [グループ化レベル1 (Grouping Level1)] に割り当て、**レベル2**の場合は [グループ化レベル2 (Grouping Level2)] を割り当てられます。

- **ロケーション名 (Location Name)** : Microsoft Excel (.xlsx) ファイルの [ロケーション (Location)] 列の値にマッピングするには、これを使用します。

(注)

[ロケーション名 (Location Name)] に値を割り当てる必要はありません。ロケーション名は Excel ファイルから直接取得されるため、変更することも、ヘッダー列にマッピングすることもできません。

- **ロケーションID (Location ID)** : ロケーション ID は、ロケーションのインポートが正常に完了すると自動生成されます。

ステップ 8 [Next] をクリックします。

[ロケーションのマージ (Merge Locations)] ウィンドウが表示されます。

- Cisco Spaces のロケーション階層が、Microsoft Excel (.xlsx) ファイルをインポートすることによって検出された新しいロケーションを含めるように更新されたことを示すメッセージ。
- [ロケーションのマージ (Merge Locations)] ウィンドウには、**Excel シートから建物をインポートする** メソッドを使用してインポートされた新しいロケーションの数とそのレベルが表示されます。
- [ロケーションのマージ (Merge Locations)] ウィンドウには、[CSVで見つかったロケーション (Locations found in CSV)]、[アクション (Actions)]、および [既存のロケーション (Existing Locations)] の 3 つの列が表示されます。
- 階層を確認し、[アクション (Action)] ドロップダウンリストを使用して必要なアクションを実行する必要があります。
- [ロケーションの検索 (Search Location)] フィールドを使用して、検索条件を入力し、ロケーション名を検索できます。

ステップ 9 [CSVで見つかったロケーション (Locations found in CSV)] で、プラス記号をクリックしてロケーションを展開します。

ステップ 10 [アクション (Actions)] ドロップダウンリストから、インポートしたロケーションを、右側に表示される既存のロケーション階層とマージするために必要なアクションを選択します。

次のオプションがあります。

- [新規作成 (Create New)] : インポートしたロケーションを既存のロケーション階層内の新しいロケーションとして作成する場合は、このオプションを選択します。
- [対象とマージ (Merge With)] : Microsoft Excel (.xlsx) ファイルからインポートされたロケーションが繰り返されており、そのロケーションがロケーション階層にすでに存在する場合は、このオプ

ションを選択します。ロケーションをマージすると元に戻せないため、このアクションは注意して実行することを推奨します。

- [スキップ (Skip)] : ロケーション階層へのロケーションのインポートをスキップする場合は、このオプションを選択します。ロケーションをスキップすると元に戻せないため、注意してこのアクションを実行することを推奨します。

(注)

既存のロケーション階層には次の機能があります。

- 既存のキャンパスまたは建物がない場合、新しくインポートされたロケーションが新しいエントリとして追加されます。
- 類似の名前のロケーションがある場合、新しいロケーションを既存のロケーションとマージできます。

ステップ 11 [Next] をクリックします。

[ロケーションのマージ (Merge Locations)] セクションに表示されるマージロケーションの更新を確認する必要があります。処理されたロケーションの数を表示できます。

ステップ 12 [Submit] をクリックします。

ロケーションの詳細が正しくアップロードされたことを示すメッセージが表示されます。

[デジタルマップの追加] (Add Digital Maps) をクリックして [デジタルマップを追加](#)するか、[ロケーションの表示 (View Locations)] をクリックしてロケーションを表示できます。

ステップ 13 [このウィンドウを閉じる (Close this window)] をクリックして [ロケーション (Locations)] タブに戻ります。

[ロケーション (Locations)] タブの [建物 (Building)] セクションには、名前、パス、フロア数、送信元などのロケーションの詳細が表示されます。[サマリー (Summary)] セクションには、建物、フロア、欠落しているロケーションメタデータ情報、および確認が必要なロケーションの詳細が表示されます。

Cisco Prime Infrastructure からのロケーションのインポート

[Prime Infrastructureからロケーションをインポート (Import locations from Prime Infrastructure)] オプションで、エクスポートファイルを使用して Cisco Prime Infrastructure から Cisco Spaces へロケーションを追加します。Cisco Prime Infrastructure からネットワーク階層をインポートし、ビジネスロケーションに接続できます。

手順

ステップ 1 Cisco Spaces にログインします。

- ステップ 2** Cisco Spaces ダッシュボードで、[メニュー (Menu)] アイコン (☰) をクリックし、[セットアップ (Setup)] > [ロケーションとマップ (Locations and Maps)] を選択します。
- [ロケーションとマップ (Locations and Maps)] ウィンドウは、[ロケーション (Locations)] タブが選択された状態で表示されます。
- ステップ 3** [ロケーション (Locations)] タブで、[ロケーションの追加 (Add Locations)] をクリックします。インポートされたロケーションがすでに利用可能な場合、[ロケーションをインポート (Import Location)] オプションが表示されます。
- [建物の詳細のアップロード (Upload Building Details)] ウィンドウには、ロケーションをアップロードするためのさまざまな方法が表示されます。
- ステップ 4** [Prime Infrastructureからロケーションをインポート (Import locations from Prime Infrastructure)] をクリックし、[次へ (Next)] をクリックします。
- [ロケーションの詳細をインポート (Import Location Details)] ウィンドウが表示されます。
- ステップ 5** [ロケーションの詳細をインポート (Import Location Details)] ウィンドウで、Cisco Prime Infrastructure マップファイルを .GZ ファイル (圧縮アーカイブファイル) としてドラッグアンドドロップするか、[ここをクリックしてアップロード (Click here to upload)] をクリックして、Cisco Prime Infrastructure マップ情報を含む .GZ ファイルをアップロードします。
- ステップ 6** [Next] をクリックします。
- ロケーションの詳細をインポート (Import Location Details)] には、マップデータが処理中であることを示すメッセージが表示されます。Map Service は、同じ処理を行うために時間がかかります。[最近のアクティビティ (Recent Activity)] セクションでマップデータの処理ステータスを確認できます。
- マップデータが正常に処理されたら、マップデータをロケーションとマージする必要があります。
- ステップ 7** [このウィンドウを閉じる (Close this window)] をクリックして、ウィンドウを閉じます。
- [ロケーション (Locations)] タブの [[建物 (Building)] セクションには、新しくインポートされたロケーションの詳細が表示されます。同じロケーション情報が Cisco Spaces ロケーション階層にも表示されます。
- Cisco Prime Infrastructure からのマップのインポートによってロケーション階層に新しいロケーションが追加されたことを示すアラートメッセージが [ロケーション (Location)] タブに表示されます。
- ステップ 8** [確認 (Review)] をクリックして確認し、必要なアクションを実行します。
- [ロケーションのマージ (Merge Locations)] ウィンドウが表示されます。
- Cisco Spaces のロケーション階層が、Cisco Prime Infrastructure マップのインポートによって検出された新しいロケーションを含めるように更新されたことを示すメッセージ。
 - [ロケーションのマージ (Merge Locations)] ウィンドウには、**Prime Infrastructureからのロケーションのインポート**方式を使用してインポートされた新しいサイトと建物の数が表示されます。
 - [ロケーションのマージ (Merge Locations)] ウィンドウには、[Prime マップからのロケーション (Locations from Prime Map)]、[アクション (Actions)]、および [既存のロケーション (Existing Locations)] の 3 つの列が表示されます。

- 階層を確認し、[アクション (Action)] ドロップダウンリストを使用して必要なアクションを実行する必要があります。
- [ロケーションの検索 (Search Location)] フィールドを使用して、検索条件を入力し、ロケーション名を検索できます。

ステップ 9 [Primeマップからのロケーション (Locations from Prime Map)] で、プラス記号をクリックしてロケーションを展開します。

ロケーション階層には、キャンパス、建物、およびフロアが含まれます。

ステップ 10 [アクション (Actions)] ドロップダウンリストから、インポートしたロケーションを、右側に表示される既存のロケーション階層とマージするために必要なアクションを選択します。

次のオプションがあります。

- **対象とマージ (Merge With)** : Cisco Prime Infrastructure からインポートされたロケーションが繰り返されており、そのロケーションがロケーション階層にすでに存在する場合は、このオプションを選択します。ロケーションをマージすると元に戻せないため、このアクションは注意して実行することを推奨します。
- **削除 (Delete)** : インポートしたロケーションを既存のロケーション階層から削除する場合は、このオプションを選択します。ロケーションを削除すると元に戻せないため、このアクションは注意して実行することを推奨します。
- **新規作成 (Create New)** : 既存のロケーション階層に新しいロケーションを作成または追加する場合は、このオプションを選択します。
- **受諾 (Accept)** : Cisco Prime Infrastructure からインポートされたロケーションを、既存のロケーション階層と同様に受け入れる場合は、このオプションを選択します。

(注)

既存のロケーション階層には次の機能があります。

- 既存のキャンパスまたは建物がない場合、新しくインポートされたロケーションが新しいエントリとして追加されます。
- 類似の名前のロケーションがある場合、新しいロケーションを既存のロケーションとマージできます。

ステップ 11 [Next] をクリックします。

[ロケーション (Locations)] セクションに表示されるマージロケーションの更新を確認する必要があります。処理されたロケーションの数を表示できます。

ステップ 12 [Submit] をクリックします。

ロケーションの詳細が正しくアップロードされたことを示すメッセージが表示されます。

[デジタルマップの追加] (Add Digital Maps) をクリックして[デジタルマップを追加](#)するか、[ロケーションの表示 (View Locations)] をクリックしてロケーションを表示できます。

ステップ 13 [このウィンドウを閉じる (Close this window)] をクリックします。

[ロケーション (Locations)] タブの [建物 (Building)] セクションには、名前、パス、フロア数、送信元などのロケーションの詳細が表示されます。

[サマリー (Summary)] セクションには、建物、フロア、欠落しているロケーションメタデータ情報、および確認が必要なロケーションの詳細が表示されます。

Cisco Catalyst Center からのロケーションのインポート

DNA Centerからのロケーションのインポート (Import locations from DNA Center) オプションを使用して、Catalyst Center からロケーションを追加します。Cisco Spaces を Catalyst Center に接続でき、Catalyst Centerで定義されたすべてのサイトまたは建物が Cisco Spaces と同期されます。

手順

ステップ 1 Cisco Spaces にログインします。

ステップ 2 Cisco Spaces ダッシュボードで、[メニュー (Menu)] アイコン (≡) をクリックし、[セットアップ (Setup)] > [ロケーションとマップ (Locations and Maps)] を選択します。

[ロケーションとマップ (Locations and Maps)] ウィンドウは、[ロケーション (Locations)] タブが選択された状態で表示されます。

ステップ 3 [ロケーション (Locations)] タブで、[ロケーションの追加 (Add Locations)] をクリックします。ロケーションがすでにインポートされ利用可能な場合は、[ロケーションのインポート (Import Locations)] オプションが表示されます。

[建物の詳細のアップロード (Upload Building Details)] ウィンドウには、ロケーションをアップロードするためのさまざまな方法が表示されます。

ステップ 4 [DNA Centerからのロケーションのインポート (Import locations from DNA Center)] をクリックし、[次へ (Next)] をクリックします。

Catalyst Center からロケーションをインポートするには、Catalyst Center マップを Cisco Spaces と統合する必要があります。

ステップ 5 (オプション) [DNA Centerのマップの統合方法を表示 (View How to Integrate DNA Center Maps)] をクリックします。

[Cisco DNA Centerの統合 (Cisco DNA Center Integration)] ウィンドウが表示されます。

Cisco Spaces はマップ同期のために Catalyst Center と統合され、デバイスのロケーションの更新が Catalyst Center に提供されます。Cisco Spaces を Catalyst Center と統合するには、[トークンの作成 (Create Token)] をクリックしてトークンを作成し、Catalyst Center でトークンを構成します。

(注)

Catalyst Center での Cisco Spacesの統合機能は、一部のユーザーが使用できます。追加のサポートについては、[Cisco Spaces サポートチーム](#)にお問い合わせください。

ステップ 6 [Next] をクリックします。

[ロケーションの詳細をインポート (Import Location Details)] ウィンドウが表示されます。

ステップ 7 指示に従って Catalyst Center に接続します。

ステップ 8 [完了 (Finish)] をクリックします。

[ロケーション (Locations)] タブの [[建物 (Building)] セクションには、ロケーションの詳細が表示されます。[サマリー (Summary)] セクションには、建物、フロア、欠落しているロケーションメタデータ情報、および確認が必要なロケーションの詳細が表示されます。

Cisco Merakiからのロケーションのインポート

[Meraki からのロケーションのインポート (Import locations from Meraki)] オプションを使用して、Cisco Meraki からロケーションを追加します。Cisco Meraki を展開している場合は、この方法を使用して Cisco Meraki Cloud アカウントに接続し、ネットワーク階層、マップ、アクセスポイント、Meraki ビデオデバイスを同期します。

手順

ステップ 1 Cisco Spaces にログインします。

ステップ 2 Cisco Spaces ダッシュボードで、[メニュー (Menu)] アイコン (☰) をクリックし、[セットアップ (Setup)] > [ロケーションとマップ (Locations and Maps)] を選択します。

[ロケーションとマップ (Locations and Maps)] ウィンドウは、[ロケーション (Locations)] タブが選択された状態で表示されます。

ステップ 3 [ロケーション (Locations)] タブで、[ロケーションの追加 (Add Locations)] をクリックします。ロケーションがすでにインポートされ利用可能な場合は、[ロケーションのインポート (Import Locations)] オプションが表示されます。

[建物の詳細のアップロード (Upload Building Details)] ウィンドウには、ロケーションをアップロードするためのさまざまな方法が表示されます。

ステップ 4 [Merakiからロケーションをインポート (Import locations from Meraki)] をクリックし、[次へ (Next)] をクリックします。

[ロケーションの詳細をインポート (Import Location Details)] ウィンドウが表示されます。

Cisco Meraki からロケーションをインポートするには、Cisco Meraki を Cisco Spacesに接続する必要があります。

- ステップ5** (オプション) [Merakiの統合方法の表示 (View How to Integrate Meraki)] をクリックして、手順を表示します。
- ステップ6** [ロケーションの詳細をインポート (Import Location Details)] ウィンドウで、[次へ (Next)] をクリックします。
- ステップ7** Cisco Meraki の接続手順を読み、[次へ (Next)] をクリックします。
- [Connect your wireless network] ウィンドウが表示されます。このオプションを使用して Cisco Merakiに接続できます。
- ステップ8** すでに接続している場合は、ロケーション階層を使用してロケーションを追加します。

手動によるロケーションの追加

Microsoft Excel (.xlsx) ファイルまたはネットワークマップをインポートせずに、[手動でのロケーションの追加 (Add locations manually)] オプションを使用して、ルートロケーションの直下に独立した建物を追加します。

手順

- ステップ1** Cisco Spaces にログインします。
- ステップ2** Cisco Spaces ダッシュボードで、[メニュー (Menu)] アイコン (☰) をクリックし、[セットアップ (Setup)] > [ロケーションとマップ (Locations and Maps)] を選択します。
- [ロケーションとマップ (Locations and Maps)] ウィンドウは、[ロケーション (Locations)] タブが選択された状態で表示されます。
- ステップ3** [ロケーション (Locations)] タブで、[ロケーションの追加 (Add Locations)] をクリックします。ロケーションがすでにインポートされ利用可能な場合は、[ロケーションのインポート (Import Locations)] オプションが表示されます。
- [建物の詳細のアップロード (Upload Building Details)] ウィンドウには、ロケーションをアップロードするためのさまざまな方法が表示されます。
- ステップ4** [手動でのロケーションの追加 (Add locations manually)] をクリックし、[次へ (Next)] をクリックします。

図 38: ロケーションの追加

Add Location

×

Please enter the location details

Location Name

Enter Location Name

Brand

Enter Brand

Total Area

Enter Area

Max Capacity

Enter Maximum Capacity

Address

Previous

Add

ステップ 5 [ロケーションの追加 (Add location)] ウィンドウで、次のロケーションの詳細を入力して新しいロケーションを追加します。

- **ロケーション名 (Location Name)** : 新しいロケーションの名前。
- **ブランド (Brand)** : 新しいロケーションのブランド。
- **総面積 (Total Area)** : 新しいロケーションの総面積詳細。
- **最大キャパシティ (Max Capacity)** : 新しいロケーションの最大キャパシティ情報。
- **アドレス (Address)** : 新しいロケーションのアドレス。アドレスを手動で入力するか、マーカーをドラッグして、右側に表示されるマップからアドレスを選択できます。
- **タイムゾーン (Time Zone)** : ドロップダウンリストでタイムゾーンを選択します。
- **緯度 (Latitude)** : 新しいロケーションの緯度。
- **経度 (Longitude)** : 新しいロケーションの経度。

ステップ 6 [Add] をクリックします。

新しいロケーションが追加されたことを示す成功メッセージが表示されます。手動でロケーションを追加する場合は、[[別のロケーションの追加 (Add Another Location)] をクリックします。

ステップ 7 [Done] をクリックします。

[ロケーション (Locations)] タブの[建物 (Building)] セクションには、ロケーションの詳細が表示されます。[サマリー (Summary)] セクションには、建物、フロア、欠落しているロケーションメタデータ情報、および確認が必要なロケーションの詳細が表示されます。

ロケーション情報の更新

インポートされたロケーションのロケーションメタデータが欠落している場合、[ロケーション (Locations)] タブにアラートメッセージが表示されます。

手順

ステップ 1 Cisco Spaces にログインします。

ステップ 2 Cisco Spaces ダッシュボードで、[メニュー (Menu)] アイコン (☰) をクリックし、[セットアップ (Setup)] > [ロケーションとマップ (Locations and Maps)] を選択します。

[ロケーションとマップ (Locations and Maps)] ウィンドウは、[ロケーション (Locations)] タブが選択された状態で表示されます。

ステップ 3 [必須ロケーション情報 (Essential Location Info)] フィールドの横にある [建物 (Buildings)] セクションで、[アラート (Alert)] アイコンをクリックして、欠落しているロケーションメタデータを更新します。

[ロケーション情報の更新 (Update Location Info)] ウィンドウが表示されます。

ステップ 4 [ロケーション情報の更新 (Update Location Info)] ウィンドウで、必要に応じて次のロケーションの詳細を更新します。

- **ロケーション名 (Location Name)** : 新しいロケーションの名前。
- **ブランド (Brand)** : 新しいロケーションのブランド。
- **総面積 (Total Area)** : 新しいロケーションの総面積詳細。
- **最大キャパシティ (Max Capacity)** : 新しいロケーションの最大キャパシティ情報。
- **アドレス (Address)** : 新しいロケーションのアドレス。アドレスを手動で入力するか、マーカーをドラッグして、右側に表示されるマップからアドレスを選択できます。
- **タイムゾーン (Time Zone)** : ドロップダウンリストでタイムゾーンを選択します。
- **緯度 (Latitude)** : 新しいロケーションの緯度。
- **経度 (Longitude)** : 新しいロケーションの経度。

ステップ 5 [Save] をクリックします。

場所を確認

[ロケーションとマップ (Locations and Maps)] ウィンドウには、インポートされたロケーション階層を確認する必要がある場合にアラートメッセージが表示されます。場所を確認し、必要なアクションを実行する必要があります。

手順

ステップ 1 [ロケーションとマップ (Locations and Maps)] ウィンドウで、[プレビュー (Preview)] をクリックしてロケーション レビューを表示し、続行します。

[ロケーションの確認 (Review Locations)] ウィンドウには、ロケーションのインポート元となるすべてのソース (Cisco Meraki や Catalyst Center など) が表示されます。各ロケーションでインポートされたサイト、建物、およびキャンパスの数を表示することもできます。

ステップ 2 確認する送信元のロケーションを選択し、[次へ (Next)] をクリックします。

[ロケーションの確認 (Review Locations)] ウィンドウには、左側の列に選択した送信元のインポートされたロケーション階層レベルが、右側の列に既存の接続先ロケーション階層レベルが表示されます。特定のロケーションを検索するには、[ロケーションの検索 (Search Locations)] フィールドを使用します。

ステップ 3 [アクション (Action)] ドロップダウンリストにあるオプションを使用し、推奨アクションを選択して、送信元ロケーション階層の各レベルを、右側の列の関連する接続先ビジネス階層レベルとマージします。

デフォルトでは、Cisco Spaces はインポートされたロケーション階層を確認するためのいくつかのアクションを推奨します。使用可能なアクションは、マージ、承認、新規作成、および削除です。

- 送信元ロケーション階層で最上位ノードに選択したアクションは、下位のノードに自動的に順次適用されます。
- キャンパスノードの下レベルが関連する接続先のビジネス階層レベルとすでにマージされている場合、送信元ロケーション階層からそのキャンパスノードを削除することはできません。
- 送信元ロケーション階層の建物を接続先のビジネス階層のキャンパスにマージすることはできません。
- 送信元ロケーション階層のサイトを、接続先のビジネス階層のキャンパスにマージできます。
- 送信元ロケーション階層の名前が Cisco Spaces ロケーション階層で使用可能なビジネス階層と一致する場合、Cisco Spaces は一致する接続先レベルを自動的に表示し、マージアクションを続行します。
- 送信元ロケーション階層が新しい場合は、作成アクションを選択すると、Cisco Spaces ロケーション階層に新しいビジネス階層が自動的に作成されます。

ステップ 4 [既存のロケーション (Existing Locations)] ドロップダウンリストから、関連する接続先レベルを選択し、Cisco Spaces ロケーション階層で使用可能なビジネス階層を使用して、任意の送信元ロケーションからインポートされたロケーション階層をマージして統合します。

[既存のロケーション] ドロップダウンリストには、Cisco Spaces ロケーション階層で使用可能なすべての接続先ノードが表示されます。ドロップダウンリストで、ビジネス階層のインポート元を表示できます。

ステップ 5 [Next] をクリックします。

[ロケーションのマージ (Merge Locations)] ウィンドウには、関連する分析データに関して、アクションの概要とその意味が表示されます。続行する前に、このアラート情報を確認することを推奨します。

(注)

削除対象として選択したロケーションに、関連付けられたルールが含まれている場合、削除アクションを続行できません。アクションを見直し、それに応じてマージ設定を更新する必要があります。

削除対象として選択したロケーションに、関連付けられたレポートが含まれている場合は、削除アクションを続行できます。ロケーションがマージされた後に、レポートが再度生成されます。

ステップ 6 [同意して続行 (Agree and Continue)] をクリックします。

選択したレビューアクションが処理され、ロケーションがレビュー済みとしてマークされます。送信元ロケーションレベルを、関連する接続先ノードとマージする場合、送信元ロケーションレベルのすべてのプロパティがビジネス階層の接続先ノードに適用されます。

ネットワークマップの追加

[ネットワークマップ (Network Maps)] タブを使用してネットワークマップを追加し、関連付けられたネットワークマップとともにロケーションを表示します。ロケーションをインポートできるのは、送信元にそのロケーションに関連付けられているネットワークマップがある場合のみです。現在、Cisco Prime Infrastructure、Catalyst Center、Cisco Meraki、および Cisco Connected Mobile Experiences にはネットワークマップが含まれています。

手順

ステップ 1 Cisco Spaces にログインします。

ステップ 2 Cisco Spaces ダッシュボードで、[メニュー (Menu)] アイコン (☰) をクリックし、[セットアップ (Setup)] > [ロケーションとマップ (Locations and Maps)] を選択します。

[ロケーションとマップ (Locations and Maps)] ウィンドウが表示されます。

ステップ 3 [ネットワークマップ (Network Maps)] タブをクリックします。

ステップ 4 [ネットワークマップの追加 (Add Network Map)] をクリックします。

[建物の詳細をアップロード (Upload Building Details)] ウィンドウが表示されます。

ステップ 5 ネットワークマップを含む次の方法を使用してロケーションをインポートします。

- [Cisco Prime Infrastructure](#) からロケーションをインポート
- [Catalyst Center](#) からロケーションをインポート
- [Cisco Meraki](#) からロケーションをインポート

- [Cisco CMX からロケーションをインポート](#)
- [手動によるロケーションの追加](#)

インポートされたロケーションの詳細は、[ロケーションとマップ (Locations and Maps)] の [ネットワークマップ (Network Maps)] タブの下に表示されます。

ステップ 6 [プレビュー (Preview)] をクリックして表示し、ロケーションレビューを続行します。詳細については、「[ロケーションを確認](#)」を参照してください。

ステップ 7 (オプション) [ネットワークマップ (Network Maps)] タブで、必要に応じて次のオプションを使用します。

- **エクスポート (Export)** : インポートされたビジネスロケーションの詳細を Microsoft Excel ファイル (.xls) にエクスポートします。[ダウンロード (Download)] をクリックすると、同じものをダウンロードできます。
- [最近のアクティビティ (Recent Activity)] : クリックすると、最近のアクティビティの詳細が表示されます。[最近のアクティビティ (Recent Activity)] スライドインウィンドウには、次の情報が表示されます。
 - ファイル名
 - ユーザ
 - タイプ
 - 時間
 - ステータス
- [フィルタ (Filter)] : クリックしてフィルタオプションを表示します。表示される [フィルタ (Filter)] スライドインウィンドウで、[ロケーション (Locations)] ドロップダウンリストからロケーションを選択し、必要なフィルタオプションを選択し、[選択 (Select)] をクリックして適用します。

Cisco CMX からのロケーションのインポート

[CMXからロケーションをインポート (Import locations from CMX)] オプションを使用して、Cisco CMX からロケーションをインポートします。ロケーションをインポートするには、Cisco CMX を Cisco Spaces とテザリングする必要があります。

手順

ステップ 1 Cisco Spaces にログインします。

ステップ 2 Cisco Spaces ダッシュボードで、[メニュー (Menu)] アイコン (☰) をクリックし、[セットアップ (Setup)] > [ロケーションとマップ (Locations and Maps)] を選択します。

[ロケーションとマップ (Locations and Maps)] ウィンドウが表示されます。

ステップ 3 [ネットワークマップ (Network Maps)] タブをクリックします。

ステップ 4 [ネットワークマップの追加 (Add Network Map)] をクリックします。

[建物の詳細のアップロード (Upload Building Details)] ウィンドウには、ロケーションをアップロードするためのさまざまな方法が表示されます。

ステップ 5 [CMXからロケーションをインポート (Import locations from CMX)] をクリックし、[次へ (Next)] をクリックします。

[ロケーションの詳細をインポート (Import Location Details)] ウィンドウが表示されます。

ステップ 6 (オプション) [CMXをテザリングする方法 (Learn how to tether CMX)] をクリックすると、Cisco CMX を Cisco Spaces とテザリングする手順が表示されます。詳細については、「[Cisco CMX Tethering](#)」を参照してください。

ステップ 7 [ロケーションの詳細をインポート (Import Location Details)] ウィンドウで、[次へ (Next)] をクリックします。

ステップ 8 Cisco CMX を接続する手順を読み、[次へ (Next)] をクリックします。

[Connect your wireless network] ウィンドウが表示されます。このオプションを使用して Cisco CMX に接続します。

ステップ 9 すでに接続している場合は、ロケーション階層を使用してロケーションを追加します。

デジタルマップの追加

[デジタルマップ (Digital Maps)] タブを使用して、ロケーション階層内に建物のデジタルマップを追加します。フロアのコンピュータ支援設計 (CAD) ファイルをアップロードして、3D フロアプランに変換する必要があります。

[サマリー (Summary)] エリアには、デジタルマップがインポートされた建物の数、マップレビューが保留中の建物の数、およびエラーのある建物の数が表示されます。

[建物 (Buildings)] エリアには、利用可能なロケーションが表示されます。

手順

ステップ 1 Cisco Spaces にログインします。

ステップ 2 Cisco Spaces ダッシュボードで、[メニュー (Menu)] アイコン (☰) をクリックし、[セットアップ (Setup)] > [ロケーションとマップ (Locations and Maps)] を選択します。

[ロケーションとマップ (Locations and Maps)] ウィンドウが表示されます。

ステップ 3 [デジタルマップ (Digital Maps)] タブをクリックします。

- ステップ 4** [アクション (Actions)] 列で、[デジタルマップの追加 (Add Digital Maps)] をクリックします。
- [デジタルマップの追加 : DNAのサポート (Add Digital Map: Support DNA)] ウィンドウが表示されます。
- 表示される CAD ファイル (.dwg) またはベクター PDF の関連情報を読み取ります。
 - [続行 (Proceed)] をクリックします。
- ステップ 5** アドレスを確認するには、次の手順を実行してから、[アドレスの確認 (Confirm Address)] をクリックします。
- ロケーションを選択するには、[検索 (Search)] フィールドに建物名を入力するか、マップを直接クリックすることでマーカーを配置します。
 - または、必要に応じて、マーカーをクリックしてドラッグし、マップ上のロケーションを調整します。
- マップ上の建物のロケーションが正しいことを確認します。
- (注)
- 右側のパネルに表示されるマップからロケーションを選択する場合は、現在のロケーションを使用して地理座標を入力する権限を Cisco Spaces に付与する必要があります。
- ステップ 6** デジタルマップに追加するフロアを選択し、[次へ (Next)] をクリックします。[フロア名 (FloorName)] の横にあるチェックボックスをオンにして、リストされているすべてのフロアを選択します。
- 続行する前に、すべてのフロアが対応するレベル番号と短縮名で正確にリストされていることを確認してください。レベル番号と短縮名は、フロアラベルに基づいて自動生成されます。この手順は、さまざまなサイネージのユースケースを有効にするために重要です。
- (オプション) 新しいフロアを追加するには、[新しいフロアの追加 (Add New Floor)] をクリックし、次の詳細を入力します。
- フロア名 (Floor Name)** : 新しいフロアの名前を入力します。
 - レベル番号 (Level Number)** : 新しいフロアのレベル番号を選択します。
 - 短縮名 (Short Name)** : 新しいフロアの短縮名を入力します。
- ステップ 7** デジタルマップの生成に使用するソースファイルをアップロードします。指定されたアップロードセクションにファイルをドラッグアンドドロップするか、[添付ファイルのアップロード (Upload attachment)] をクリックしてローカルにあるファイルを参照してアップロードできます。
- [一括アップロード (Bulk Upload)] をクリックすると、CAD ファイルまたはベクトル化された PDF のアップロードを短時間で実行できます。
- [追加情報 (Additional Info)] セクションを活用して、アップロード情報を入力します。
- 変換するあらゆる要素のすべてのレイヤ (構造、家具、名前、ID など) が含まれている CAD ファイルを使用することを推奨します。名前または ID を持つ要素のみがセンサーの割り当てに対応できます。
- (注)
- フロアごとに1つのCADファイルのみをアップロードします。相互参照(XREF)はサポートされていません。
 - サポートされているファイルタイプは、ZIP、AutoCAD 描画ファイル (DWG)、AutoCAD 描画相互変更ファイル (DXF)、ポータブルドキュメントフォーマット (PDF) です。

ステップ 8 [Submit] をクリックします。

各 CAD ファイルとロケーションメタデータが処理され、マップがデジタル化されます。[デジタルマップ (Digital Maps)] タブにアラートメッセージが表示されます。

ステップ 9 [レビュー (Review)] をクリックします。

ステップ 10 [デジタルマップの確認 (Review Digital Maps)] ウィンドウで、確認する建物を選択し、[次へ (Next)] をクリックします。

デジタル化されたマップが表示されます。

ステップ 11 (オプション) フロアまたはスペースを選択し、必要に応じてクリックして更新します。

ポップアップウィンドウが表示され、名前を編集したり、タイプカテゴリを更新したりできます。

ステップ 12 [この建物を公開 (Publish this Building)] をクリックします。

デジタル化されたマップは公開され、Cisco Smart Workspaces、環境メトリックアプリケーションなど、他のアプリケーションで使用できます

Cisco Spaces ロケーション階層では、選択したロケーションについて、そのロケーションにデジタルマップがある場合、デジタルマップがデフォルトで表示されます。

変更を破棄する場合は、[この建物をスキップ (Skip this building)] をクリックします。



第 37 章

Meraki カメラの設定

この章では、Meraki カメラに関して Cisco 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 Spaces を設定する](#) (401 ページ)

Cisco Meraki カメラと連動するように Cisco Spaces を設定する

Cisco 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 9800 ワイヤレスコントローラベース 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 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

手順

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 Spaces ダッシュボードで、[メニュー (Menu)] アイコン (≡) をクリックし、[セットアップ (Setup)] > [カメラ (Camera)] を選択します。

[カメラに接続 (Connect your Camera)] ウィンドウが表示されます。

ステップ 3 [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 [カメラに接続 (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、[開始 (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 までをスキップします。別の接続方法で接続する場合は、[新規追加 (Add New)] を使用して対応するウィジェットを追加します。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、[新規追加 (Add New)] は無効になります。

ステップ 4 [選択 (Select)] をクリックして、Cisco Meraki を Cisco 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。この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 Spaces の設定](#)」を参照してください。

ステップ 5 [Continue Setup] をクリックします。

[ワイヤレスネットワークに接続 (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** 方式の場合、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 方式の場合、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 6 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、[接続 (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します。

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 の内容が次のメッセージに置き換えられます。

「Connected as [e-mail using which you have connected] ([接続に使用した電子メール] で接続)」。

- b) **Meraki API キー**を介した分析用 **Meraki カメラ**ウィジェットの場合、ウィンドウに [APIキー (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 の内容が次のメッセージに置き換えられます。「Connected with [masked API key] ([マスクされた API キー]で接続)」。

ステップ 7 [Merakiカメラに接続 (Connect your Meraki Camera)] ウィンドウで、ステップ 2 で表示された [インポートネットワーク (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 までをスキップします。

ステップ 8 [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 9 [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 10 [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 11 [Finish] をクリックします。

Cisco Meraki の Meraki カメラ設定が Cisco Spaces と自動的に同期されます。通常、48 時間後に自動設定されます。遅延がある場合は、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 12 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 Spaces の [Meraki カメラに接続 (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) [名前 (Name)] フィールドで、MQTT サーバーを設定する対象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) [設定 (Settings)] タブをクリックし、[検知 (Sense)] をクリックします。
- e) [検知API (Sense API)] の右側にある [有効 (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 [MQTTブローカの編集 (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 (Host)** : 次のホストの詳細を入力します。

- 米国リージョンでホストされているユーザーの場合 : `mqtt.dnaspaces.io`
- 欧州リージョンでホストされているユーザーの場合 : `mqtt.dnaspaces.eu`
- シンガポールリージョンでホストされているユーザーの場合 : `mqtt.ciscospaces.sg`

- **ポート (Port)** : ポート番号 1883 を入力します。Cisco Meraki からのトラフィックがポート 1883 で許可されていることを確認する必要があります。

i) [Save] をクリックします。

ステップ 13 カメラの入口/出口ラインを設定するには、ステップ 4 で [Merakiカメラに接続 (Connect your Meraki Camera)] ウィンドウの [トリップワイヤを引く (Draw Trip Wire)] をクリックします。

(注)

カメラメトリクス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 1メートル程度 (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 14 表示される [トリップワイヤを引く (Draw Trip Wire)] ウィンドウで、[ロケーションを選択 (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、[実行 (Done)] をクリックします。

ステップ 15 [トリップワイヤを引くカメラを選択 (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、[次へ (Next)] をクリックします。

ステップ 16 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、Cisco 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 17 ライン両端のポイントをクリックして、XY 座標を設定します。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 [トリップワイヤステータス (Trip-wire status)] エリアに自動的に表示され、ステータスが [設定 (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 [設定 (Set)] に変更されます。

ステップ 18 [完了 (Finish)] をクリックします。

カメラは Cisco Spaces で使用するよう設定されています。

次のタスク

Cisco Spaces **Right Now** アプリケーションは、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。

手順

ステップ 1 [\[Cisco Spaces\]](#) にログインします。

ステップ 2 Cisco Spaces ダッシュボードで、[メニュー (Menu)] アイコン (☰) をクリックし、[設定 (Settings)] > [カメラ (Camera)] を選択します。

[Merakiカメラに接続 (Connect your Meraki Camera)] ウィンドウが表示されます。

ステップ 3 [Merakiカメラに接続 (Connect your Meraki Camera)] ウィンドウで、手順 4 で表示された [カメラを表示 (View Cameras)] をクリックします。

Cisco 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 [編集 (Edit)] アイコンをクリックします。

ステップ 5 表示される [トリップワイヤを編集 (Edit Trip Wire)] ウィンドウで、トリップワイヤの詳細を編集し、[実行 (Done)] をクリックします。



第 38 章

センサーの設定

- [センサー \(407 ページ\)](#)
- [センサーの要求 \(407 ページ\)](#)

センサー

Cisco DNA Spaces ダッシュボードの **[Setup]** > **[Sensors]** オプションを使用して、ワイヤレスネットワークにセンサーを要求します。

センサーの要求

各センサーの MAC アドレスを使用して、センサーをワイヤレスネットワークに登録します。

手順

- ステップ 1** Cisco Spaces にログインします。
- ステップ 2** Cisco Spaces ダッシュボードで、[メニュー (Menu)] アイコン (☰) をクリックし、**[セットアップ (Setup)]** > **[センサー (Sensors)]** を選択します。
- ステップ 3** [Claim Sensors] をクリックします。
[Claim Sensor(s)] スライドインペインが表示されます。
- ステップ 4** [Enter a new tag] フィールドに、要求するセンサーの MAC アドレスを入力します。
- ステップ 5** Enter キーを押します。複数の MAC アドレスを追加し、同時に複数のセンサーに登録するには、区切り文字としてカンマを使用します。
- ステップ 6** [Claim] をクリックします。
場所、ステータス、SSID、MAC アドレスなどのセンサーの詳細が [Sensor Management] ウィンドウに表示されます。

センサーの要求を解除するには、MAC アドレスをクリックして、[Unclaim] をクリックします。



第 39 章

データエクスポートの設定

- [データエクスポート](#) (409 ページ)
- [Spaces データエクスポート送信元 IP](#) (410 ページ)
- [エクスポートデータの作成](#) (410 ページ)

データエクスポート

Cisco Spaces のデータエクスポート機能を使用すると、CSV ファイルとして raw レベルのデータを、使用可能なストレージ先に自動エクスポートを設定できます。

Cisco Spaces は、ユーザー獲得データ、ユーザー訪問データ、プロキシミティルール一致データなど、特定の場所におけるユーザーのさまざまなデータをキャプチャします。

エクスポートは、顧客のストレージ接続先に直接アップロードされるフラットファイル (CSV) として提供されます。パブリックインターネット経由で宛先サーバーにアクセスできない場合には、必要に応じて、VPN 接続経由で転送できます。アップロードの頻度は、顧客の要件やデータ量に合わせてカスタマイズできます。これにより、お客様のシステムへの完全に自動化された取り込みがサポートされます。

VPN を介した SFTP 接続のルーティングの詳細については、[Cisco Spaces のサポート](#)にお問い合わせください。



- (注)
- Cisco Spaces ダッシュボード SEE ライセンスの顧客アカウントの場合、キャプティブポータル、エンゲージメントおよびロケーションペルソナなどのデータエクスポートタイプはエクスポートできません。
 - ACT ライセンスの顧客アカウントの場合、すべてのデータタイプをエクスポートできません。
 - 顧客取得データのエクスポートは、認証タイプ：認証なし (No Authentication) およびアクセスコード (Access Code) のポータルのデータをサポートしていません。

Spaces データエクスポート送信元 IP

データエクスポートでは、次の送信元 IP（リージョンに基づく）を使用してデータをエクスポートします。

リージョン	送信元 IP
.io	52.55.122.128 54.174.253.222 34.205.82.138 3.208.52.128 52.206.67.43 34.192.26.106 54.88.200.142
.eu	52.48.33.123 52.208.167.15 52.208.15.59 54.220.148.167 54.220.45.63
.sg	18.140.83.198 13.215.167.226 18.143.125.54 3.1.251.174

エクスポートデータの作成

手順

ステップ 1 Cisco Spaces で、[メニュー（Menu）] アイコン（☰）をクリックし、[セットアップ（Setup）]>[データエクスポート（Data Export）] を選択します。

ステップ 2 [Create New Export] をクリックします。

[新規データエクスポートの作成（Create New Data Export）] ウィンドウには、次の構成オプションが時系列で表示されます。

- データ タイプ

- ロケーション (Locations)
- Schedule
- ファイル形式 (File Format)
- Connection
- Summary

図 39: 新しいデータエクスポートの作成

Create New Data Export

1 Data Type

Select the data type that you want to export

Data Type

Select data type

- Visits**
Visits details such as Visit start time, Visit end time, Visit dwell time, client mac, etc.
- Right Now - People Count (WiFi)**
Real time count of the people present at the locations and connected to WiFi.
- Right Now - People Count (Camera)**
Real time count of the people present at the locations and seen on camera.
- Captive portal - Customer Acquisition**
Devices & acquisition data such as device mac address, name, email, phone number, social network info etc.
- Engagement - Rule Activity**
Visitor engagement data such as #of engagements, engagement types, url, messages, device mac address etc.
- Location Personas - Rule Activity**

Cancel Next

ステップ 3 [データ型 (Data Type)] ドロップダウンリストから、データ型を選択します。
次のデータタイプが使用可能です。

表 17: データ型

データ型	説明
アクセス	ログのタイムスタンプ、タイムゾーン、現地の日付、現地の時間、現地の分、デバイス ID、ユーザー ID、ユーザー名、MAC アドレス、訪問開始タイムスタンプ、訪問終了タイムスタンプ、訪問時間、位置情報
Right Now : 人数 (Wi-Fi)	ログのタイムスタンプ、現地の日付、現地の時間、現地の分、関連ユーザー数、推定プローブ数、推定密度、位置情報
Right Now : 人数 (カメラ)	ログのタイムスタンプ、現地の日付、現地の時間、現地の分、人数、位置情報
キャプティブポータル : 顧客獲得	ログのタイムスタンプ、タイムゾーン、現地の日付、現地の時間、現地の分、獲得タイプ、デバイス ID、ユーザー ID、MAC アドレス、獲得ハンドル、オプトイン、電話番号、電子メール、名、姓、性別、年齢、ビジネスタグの名前、ビジネスタグの値、ソーシャルネットワーク、ソーシャルネットワークのプロファイル URL、ソーシャルネットワークの画像、CPF 番号、位置情報
ロケーションペルソナ : ルールアクティビティ	ログのタイムスタンプ、タイムゾーン、現地の日付、現地の時間、現地の分、デバイス ID、ユーザー ID、MAC アドレス、プロファイルタグの名前、ルール名、位置情報
エンゲージメント : ルールアクティビティ	ログのタイムスタンプ、タイムゾーン、現地の日付、現地の時間、現地の分、デバイス ID、ユーザー ID、MAC アドレス、エンゲージメントタイプ、エンゲージメント先、メッセージ、ルール名、位置情報
オープンローミング : ユーザーデータ	ログのタイムスタンプ、タイムゾーン、現地の日付、現地の時間、MAC アドレス、ユーザー名、ステータスタイプ、アカウントセッション ID、アカウント入力オクテット、アカウント入力パケット、アカウント出力オクテット、アカウント出力パケット、プロファイル名、デバイスクラスタグ、CUI ユーザー名、アプリ参照 ID、位置情報

(注)

- [Location Information] 領域には、選択した構成に応じて次のフィールドが表示されます。これらのフィールドはすべてオプションであり、選択してデータのエクスポートに含めることができます。

- ロケーション名
- ロケーション タイプ
- 階層パス
- 市区町村郡
- 都道府県
- 国
- キャパシティ
- エリア

- サンプルのエクスポートには、選択したデータタイプの最近の 1 時間のデータが表示されます。
- データタイプごとに、[Location Hierarchy] でレベルと、エクスポートに含めるロケーション情報を選択する必要があります。
- ロケーションの選択は、[Data Type] フィールドで選択したロケーションタイプに基づいています。
- ロケーション選択オプションは、[Engagement]、[Captive Portal] および [Location Personas] のデータタイプでは使用できません。
- Cisco Spaces は、ユーザー獲得データ、ユーザー訪問データ、エンゲージメントルール一致データなど、特定の場所におけるさまざまなユーザーデータをキャプチャします。
- カスタムデータのエクスポートについては、[Cisco Spaces サポート](#)にお問い合わせください。

ステップ 4 [次へ (Next)] をクリックして、[ロケーション (Locations)] に移動します。

ステップ 5 [すべてのロケーションでこのエクスポートを有効にする (Enable this export for all locations)] チェックボックスをオンにして、使用可能な全ロケーションを選択し、[次へ (Next)] をクリックして、[スケジュール (Schedule)] に移動します。

個別にエクスポートするロケーションを選択する場合は、[すべてのロケーションでこのエクスポートを有効にする (Enable this export for all locations)] チェックボックスをオフにして、対象のロケーションを選択します。

ステップ 6 [エクスポートスケジュール (Export Schedule)] エリアで、[繰り返し (Recurrence)] ドロップダウンリストからエクスポートの間隔を選択して、データのエクスポートをスケジュール設定します。エクスポートは、構成されたタイムゾーンに基づいてスケジュールされます。

次のオプションがあります。

- **Hourly (毎時)** : 1 時間ごとにデータのエクスポートをスケジュール設定するには、このオプションを選択します。[Timezone] ドロップダウンリストから必要なタイムゾーンを選択します。
- **[Daily]** : このオプションを選択して、データのエクスポートを毎日スケジュールします。[タイムゾーン (Timezone)] ドロップダウンリストから必要なタイムゾーンを選択し、データをエクスポートする時刻も選択します。

- [Weekly] : このオプションを選択して、データのエクスポートを毎週スケジュールします。曜日を選択し、[タイムゾーン (Timezone)] ドロップダウンリストから必要なタイムゾーンを選択し、データをエクスポートする時刻も選択します。

ステップ 7 [次へ (Next)] をクリックして、[ファイル形式 (File Format)] に移動します。

ステップ 8 [デリミタ (Delimiter)] エリアで、データ区切り記号のコード設定を選択します。

次のオプションがあります。

- [Pipe]
- [Comma]
- [Tab]
- [Custom character] : [Custom character] フィールドに、好みの文字を入力します。/, \, &, ', " 以外の特殊文字を使用できます。

(注)

オプション **パイプ**、**カンマ**、および **タブ** では、追加の入力を指定する必要があります。

ステップ 9 圧縮エクスポートが必要な場合は、[Compress export data] で [Yes] または [No] を選択します。

(注)

データのエクスポートには圧縮形式を選択することをお勧めします。

ステップ 10 [ファイル名形式 (File Name Format)] フィールドで、ファイル名のプレフィックスを入力し、日付と時刻の形式を選択します。

ステップ 11 [日付と時刻の形式を選択 (Select Date & Time Format)] ドロップダウンリストから、形式を選択します。

ステップ 12 [次へ (Next)] をクリックして、[接続 (Connection)] に移動します。

ステップ 13 [接続タイプ (Connection Type)] エリアで、[接続先の選択 (Select Destination)] ドロップダウンから、接続先のタイプを選択します。

選択した接続タイプに応じて、設定パラメータを入力します。使用可能な接続タイプは次のとおりです。

- SFTP
- Amazon S3
- Microsoft Azure Blob Storage
- Google Cloud Storage
- Box

a) 接続タイプが **SFTP** サーバーの場合、次のパラメータを入力します。

- [SFTP Host] : サーバーのホスト名または IP アドレスを、hostname.server.com の形式で入力します。
- ポート (Port) : **SFTP** サーバーに接続するときのポート番号を入力します。
- [Username] : ユーザー名を入力します。

- **パスワードを使用 (Use Password)** : このラジオボタンを選択し、**SFTP** サーバーに接続するためのパスワードを入力します。
- **秘密鍵を使用 (Use Private Key)** : このラジオボタンを選択して、**SFTP** サーバーに接続するための秘密鍵を使用します。[Upload Private Key] オプションを使用して秘密鍵をアップロードし、パスフレーズを入力する必要があります。

(注)

- SFTP 構成に基づいて、[Upload Private Key] または [Use Private Key] を選択して接続を確立できます。
- パスワードまたはパスフレーズの選択は、SFTP サーバーに基づいています。
- OpenSSH キーベースの認証はサポートされていないため、RSA 秘密キーを使用することを推奨します。

- **アップロードパス (Upload Path)** : エクスポートデータのアップロードパスを入力します。

b) 接続タイプが **Amazon S3** の場合、次のパラメータを入力します。

- **アクセスキー (Access Key)** : Amazon S3 バケットのアクセスキーを入力します。
- **秘密鍵 (Secret Key)** : Amazon S3 バケットの秘密鍵を入力します。
- **リージョン (Region)** : [リージョン (Region)] ドロップダウンリストから、Amazon S3 バケットのリージョンを選択します。
- **バケット名 (Bucket Name)** : 選択したリージョンに応じて、バケット名を入力します。
- **アップロードパス (Upload Path)** : エクスポートデータのアップロードパスを入力します。

c) 接続タイプが **Microsoft Azure Blob Storage** の場合は、次のパラメータを入力します。

- **アカウント名 (Account Name)** : Microsoft Azure Blob Storage のストレージアカウント名を入力します。
- **アカウントキー (Account Key)** : Microsoft Azure Blob Storage のアカウントキーを入力します。
- **コンテナ名 (Container Name)** : コンテナ名を入力します。
- **アップロードパス (Upload Path)** : エクスポートデータのアップロードパスを入力します。

d) 接続タイプが **Google Cloud Storage** の場合は、次のパラメータを入力します。

- **バケット名 (Bucket Name)** : バケット名を入力します。
- **アップロードパス (Upload Path)** : エクスポートデータのアップロードパスを入力します。

(注)

data-out@dna-spaces.iam.gserviceaccount.com サービスアカウントを追加し、アイデンティティおよびアクセス管理 (IAM) サービスで **Storage Object Admin** (ストレージオブジェクト管理者) としてのロールを指定する必要があります。

- e) 接続タイプ **Box** の場合、[アップロードパス (Upload Path)] フィールドに、データをエクスポートするために **Box** で作成したフォルダ名を入力し、[認証 (Authenticate)] をクリックします。
1. データエクスポートを認証するために、**Box** アカウントを使用できることを確認します。
 2. **Box** に認証するための同じユーザー名とパスワードのログイン情報を入力します。認証にシングルサインオン (SSO) 方式はサポートされていません。

(注)

認証に成功したら、**Box** の場所にあるファイルにアクセスするための **Cisco Spaces** へのフルアクセス権が与えられます。データをエクスポートするための完全な権限を **Cisco Spaces** に付与するには、[boxへのアクセスを許可 (Grant access to box)] をクリックします。

カスタムデータエクスポートは、現在、**Box** の宛先ではサポートされていません。

ステップ 14 [Connect] をクリックします。

接続が成功すると、次のメッセージが表示されます: 「Connection Established」。

ステップ 15 [次へ (Next)] をクリックして、[サマリー (Summary)] に移動します。

ステップ 16 [Add a name to your data export] フィールドに、データエクスポートの名前を入力します。

ステップ 17 データエクスポートの詳細を確認し、[Export] をクリックします。

エクスポートを構成すると、接続タイプのアップロードパスでサンプルファイルが使用可能になります。

[エクスポートの新規作成 (Create New Export)] ウィンドウに、データエクスポートの詳細 (名前、接続タイプ、スケジュール、次のエクスポートの詳細、最後に成功したエクスポート情報など) が表示されます。



第 40 章

Cisco Webex の設定

この章では、Cisco Webex と Cisco DNA Spaces の統合方法について説明します。

- [Cisco Webex の統合](#) (417 ページ)
- [Cisco Webex の設定](#) (418 ページ)
- [アクティベーションコードの生成](#) (419 ページ)

Cisco Webex の統合

Cisco Webex と Cisco Spaces の統合により、**Webex Control Hub** アカウントの Cisco Webex デバイスは、**Webex Control Hub** と Cisco Spaces 間のクラウド間統合を実行できます。



(注) Cisco Webex の統合では **Cisco Smart Workspaces** ユーザーのみがサポートされています。

この統合は以下をサポートします。

- [Webex Control Hub] からの Cisco Webex ワークスペース、デバイス、ワークスペースの場所、フロアの詳細などの Cisco Webex エンティティの同期。同期プロセスは、Cisco Spaces ダッシュボードでトークンが設定された後、3 時間ごとにバックエンドでスケジュールされます。[Setup] > [Webex] を選択して、トークンを設定します。
- Cisco Webex デバイスは、温度、電波品質、占有率などのデバイスデータを送信し、Cisco Smart Workspaces で使用されます。

Cisco Webex 統合の一部として、Cisco Spaces は、**Cisco Webex** ナビゲータの永続的な Web アプリとの統合をサポートしています。顧客が **Cisco Webex Control Hub** と Cisco Spaces の統合をアクティブ化すると、Control Hub で、この統合をサポートする必要な設定が更新されます。



(注) 現在、この統合を利用できるのは **Cisco Smart Workspaces** ユーザーのみです。

Cisco Webex の設定

Cisco Webex アカウントを Cisco Spaces に接続してから、Cisco Webex ネットワークをロケーション階層にインポートできます。

手順

ステップ 1 Cisco Spaces にログインします。

ステップ 2 Cisco Spaces ダッシュボードで、[Menu] アイコン（☰）をクリックし、[Setup] > [Webex] を選択します。

ステップ 3 [Connect your Webex] ウィンドウで、[Connect] をクリックします。

Webex トークンスライダが表示されます。

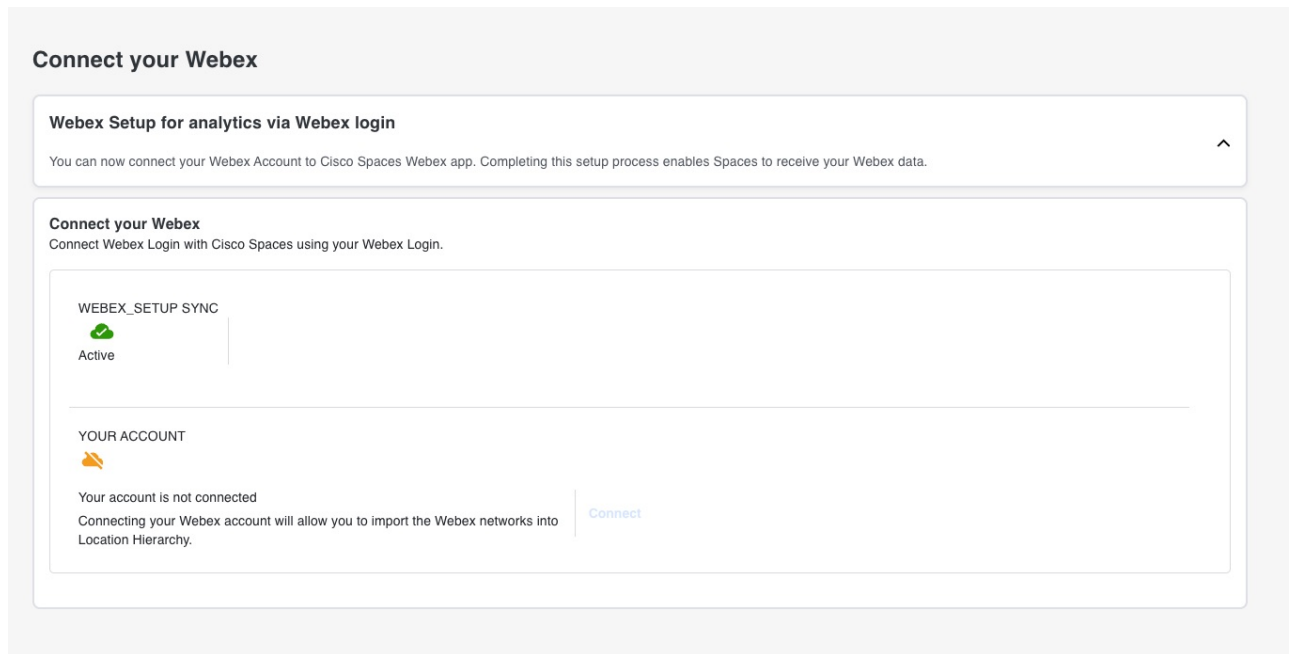
ステップ 4 [Enter or copy-paste your Webex Token] フィールドに、Cisco Webex トークンを入力します。

[Webex Control Hub] からトークンを取得できます。アクティベーションコードの生成についての詳細は、「[アクティベーションコードの生成（419 ページ）](#)」を参照してください。

ステップ 5 [Connect] をクリックします。

Cisco Webex ネットワークを [Location Hierarchy] にインポートしているときに、少なくとも 1 人のユーザーが自分の Cisco Spaces アカウントを Cisco Webex アカウントに正常に接続した場合、Cisco Webex 同期ステータスは、特定のテナント（アカウント）内のすべてのアクティブユーザーに対して [Active] と表示されます。

図 40: Cisco Webex 同期ステータス

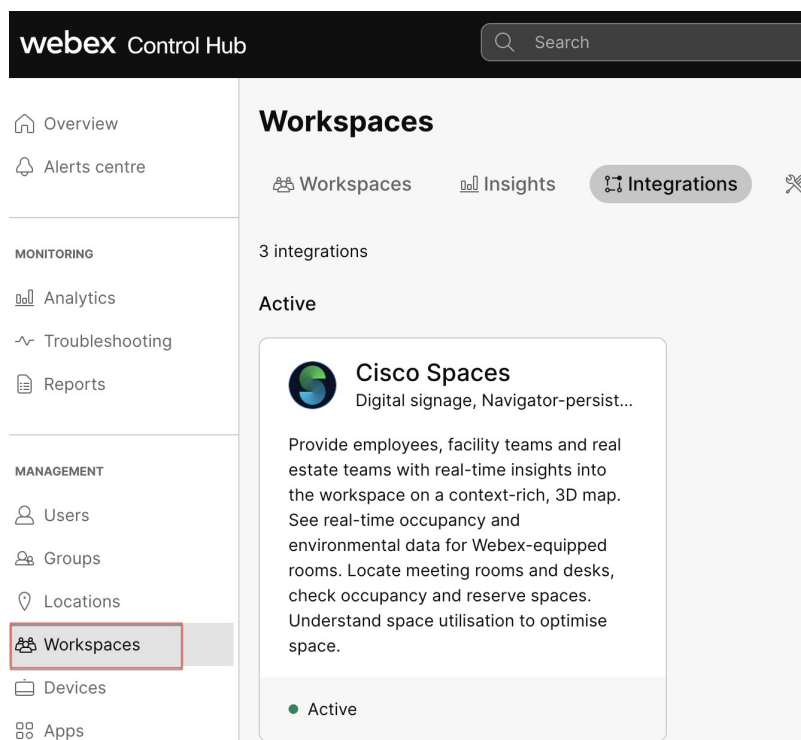


アクティベーションコードの生成

手順

- ステップ 1 [Cisco Webex Control Hub] アカウントの電子メール ID を入力してサインインします。
- ステップ 2 [Cisco Webex Control Hub] ダッシュボードで、**[Management]** > **[Workspaces]** を選択します。
- ステップ 3 [Integrations] タブをクリックします。

図 41 : Cisco Webex Control Hub



ステップ 4 [Cisco Spaces] アプリのタイルで、[Details] をクリックします。

[Cisco Smart Workspaces] アプリ統合の詳細ウィンドウが表示されます。

ステップ 5 ウィンドウの右上隅にある [Activate] をクリックします。

ステップ 6 [Cisco Smart Workspaces] によって要求された権限を確認し、[Terms and Conditions] チェックボックスをオンにします。

ステップ 7 [Activate] をクリックします。

ステップ 8 [Copy to Clipboard] オプションを使用してアクティベーションコードをコピーし、コードを **Cisco Spaces** に貼り付けて **Cisco Webex** を統合します。

生成されたアクティベーションコードの有効期限の詳細は、[Activate Integration: Cisco Smart Workspaces] ウィンドウに表示されます。



第 41 章

pxGrid クラウドのセットアップ

- [pxGrid クラウドのアクティブ化 \(421 ページ\)](#)
- [Cisco pxGrid トークンの生成 \(OTP\) \(422 ページ\)](#)
- [製品向けアプリケーションのアクティブ化 \(422 ページ\)](#)

pxGrid クラウドのアクティブ化

Cisco pxGrid クラウドは、ネットワークのセキュリティを損なうことなく、Cisco Identity Services Engine (Cisco ISE) とクラウドベースのソリューションの間でコンテキスト情報を共有できるようにする、シスコの新しいクラウドサービスです。Cisco ISE とクラウドベースのソリューション間のシームレスなデータ統合を可能にする統合フレームワークを提供します。セキュアでカスタマイズ可能な Cisco pxGrid クラウドを使用すると、共有したいデータのみを共有し、ユーザーアプリケーションに関連するコンテキストデータのみを使用できます。



(注) アクティベーションを実行するには、Cisco ISE および Cisco pxGrid Cloud に対する管理者権限が必要です。

手順

ステップ 1 Cisco Spaces にログインします。

ステップ 2 Cisco Spaces ダッシュボードで、[メニュー (Menu)] アイコン (☰) をクリックし、[セットアップ (Setup)] > [pxGridクラウド (pxGrid Cloud)] を選択します。

[pxGridクラウドのアクティブ化 (Activate pxGrid Cloud)] ウィンドウが表示されます。[ドキュメントの表示 (View Documentation)] をクリックすると、Cisco pxGrid クラウド ソリューション ガイドの追加の手順が表示されます。

ステップ 3 [トークン (Token)] フィールドに、pxGrid クラウドアプリケーションから生成されたトークンを入力します。画面の指示に従って、トークンを作成します。トークンの生成の詳細については、「[Cisco pxGrid トークンの生成 \(OTP\) \(422 ページ\)](#)」を参照してください。

ステップ 4 [pxGrid クラウドを有効化 (Activate pxGrid Cloud)] をクリックします。

アクティベーションが成功したことを示すメッセージが表示されます。

ステップ 5 [了解 (Got it)] をクリックします。

ステップ 6 [更新してステータスを確認 (Refresh to check status)] をクリックします。アプリケーションタイトルに緑のチェックマークが表示され、アプリケーションが接続されていることを示します。

製品のアプリケーションをアクティベートするために進みます。製品のアプリケーションのアクティベートに関する詳細については、「製品向けアプリケーションのアクティブ化 (422 ページ)」を参照してください。画面の指示に従って、製品をアクティベートします。

Cisco pxGrid トークンの生成 (OTP)

手順

ステップ 1 Cisco DNA クラウドにログインします。

ステップ 2 Cisco pxGrid クラウドポータルで [メニュー (Menu)] アイコン (☰) をクリックし、[アプリケーションストア (App Store)] を選択します。

ステップ 3 [マイアプリケーション (My Apps)] をクリックします。

ステップ 4 [マイアプリケーション (My Apps)] ウィンドウで、顧客固有のアプリケーションタイトルを選択し、[アプリケーションに接続 (Connect to App)] をクリックします。

生成されたワンタイムパスワード (OTP) は、[生成されたOTP (OTP Generated)] ポップアップウィンドウに表示されます。

ステップ 5 生成された OTP をコピーするには、[コピー (Copy)] アイコンを使用します。

この OTP は 60 分間有効です。

製品向けアプリケーションのアクティブ化

Cisco pxGrid クラウドでは、ネットワークのインフラストラクチャを変更することなく、プラグアンドプレイ展開できます。Cisco pxGrid クラウドポータルを使用して、製品のアプリケーションをアクティブ化します。



(注) 正常なアクティブ化 (ストリームの作成) を行うには、Cisco ISE で必要なすべての範囲を有効にします。詳細については、『Cisco pxGrid Cloud Solution Guide』を参照してください。

手順

-
- ステップ 1** Cisco DNA クラウドにログインします。
- ステップ 2** Cisco pxGrid クラウドポータルで [メニュー (Menu)] アイコン (☰) をクリックし、[アプリケーションストア (App Store)] を選択します。
- ステップ 3** [マイアプリケーション (My Apps)] をクリックします。
- ステップ 4** [マイアプリケーション (My Apps)] ウィンドウで、顧客固有のアプリケーションタイトルを選択し、[製品のアクティブ化 (Activate Product)] をクリックします。
- [製品向けアプリケーションのアクティブ化 (Activate App for Products)] ウィンドウが表示されます。
- ステップ 5** 続行するには、[実行 (Let's Do it)] をクリックします。
- [アプリケーションの選択 (Select an App)] ウィンドウが表示されます。デフォルトでは、[アプリケーション名 (App Name)] フィールドには、ステップ 3 で選択したアプリケーション タイトル名が表示されます。互換性のある製品およびサポートされている地域の詳細も表示されます。
- ステップ 6** [Next] をクリックします。
- [製品の選択 (Select Product)] ウィンドウが表示されます。
- ステップ 7** [製品タイプ (Product Type)] ドロップダウンリストから、選択したアプリケーションをアクティブ化する製品タイプを選択します。
- ステップ 8** [製品 (Product)] ドロップダウンリストから、選択したアプリケーションをアクティブ化する製品を選択します。
- [オンプレミス接続 (On-Prem Connections)] ウィンドウに登録されている製品のみを選択できます。[検索 (Search)] オプションを使用して製品を検索することもできます。
- ステップ 9** [製品向けアプリケーションの設定 (Configure App for Product)] ウィンドウで、設定の範囲を設定します。
- ステップ 10** [サマリー (Summary)] ウィンドウで設定を確認し、[製品向けアプリケーションを有効にする (Activate App for Products)] をクリックします。
- アプリケーションのアクティベーションステータスは、[製品のアクティベーション (Product Activation)] ウィンドウで [有効 (Activated)] と表示されます。
- Cisco pxGrid クラウド統合の成功した統合ステータスを表示するには、Cisco Spaces ダッシュボードを更新します。
-



第 42 章

アクセスポイント自動ロケーションの設定

- [アクセスポイント自動ロケーション \(425 ページ\)](#)
- [AP の自動検出の前提条件 \(427 ページ\)](#)
- [AnyLocate の測定データの生成 \(428 ページ\)](#)
- [デバイスを配置する \(430 ページ\)](#)
- [デバイスの配置の編集 \(434 ページ\)](#)
- [AnyLocate の測定データステータスの表示 \(435 ページ\)](#)
- [AP の表示 \(437 ページ\)](#)

アクセスポイント自動ロケーション

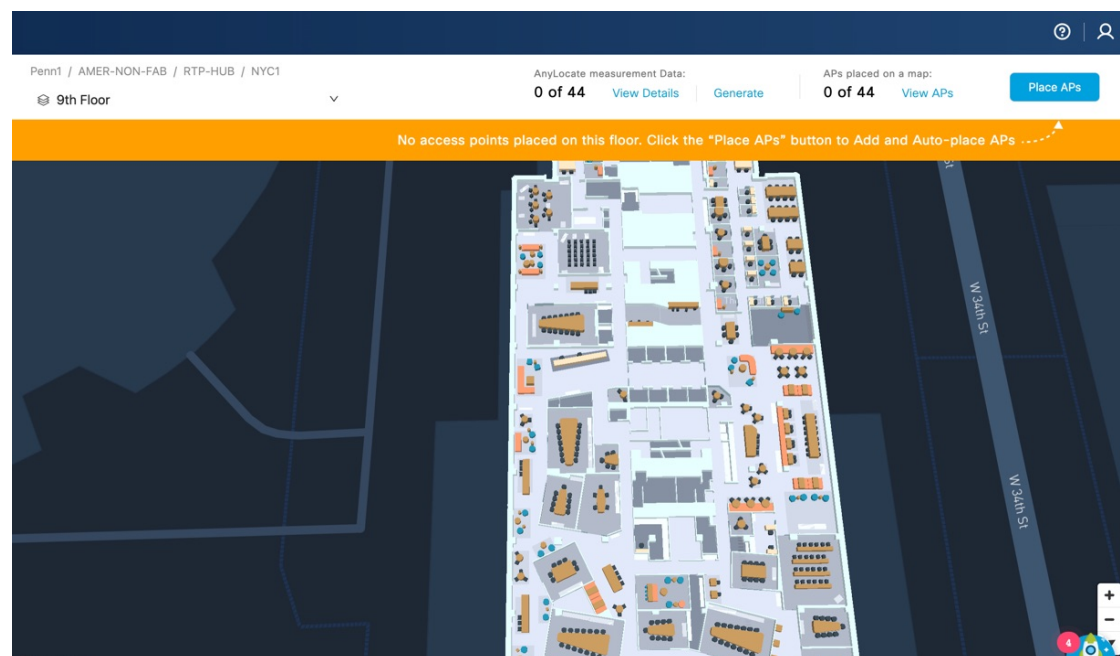
アクセスポイント自動ロケーションソリューションは、さまざまなレンジングテクノロジーとアルゴリズムを組み合わせることで、グローバル座標で AP を効果的に自己位置特定するのに役立ちます。

このソリューションは、Fine Timing Measurement (FTM) と全地球航法衛星システム (GNSS) (利用可能な場合) を活用して、正確で自動化された最新の AP ロケーションを提供します。GNSS にアクセスできない場合は、フロアごとにいくつかの手動アンカーを配置する必要があります。この機能には、隣接する AP が最大電力で相互に通信できる AP 密度が必要です。アクセスポイント自動ロケーション機能の精度は、建物のタイプと AP 間の距離によって異なります。

範囲オーケストレーションを AP で有効にするために必要な設定は、Cisco Catalyst 9800 シリーズワイヤレスコントローラの **アクセスポイント自動ロケーション** 機能を使用して行います。詳細については、『*Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide*』の「**アクセスポイント自動ロケーション**」のセクションを参照してください。

Cisco Spaces では、AP の自動ロケーションソリューションをサポートするために、[メニュー (Menu) (≡)] > [セットアップ (Setup)] > [デバイスの配置 (Device Placement)] で新機能の [デバイスの配置 (Device Placement)] を使用できます。

図 42: デバイスの配置



AP 自動ロケーション ソリューションは、Cisco Spaces のデジタルマップ上で AP を自動的に特定します。管理者がフロアプラン上の既知のロケーションを持つ複数の AP をアンカーにすると、この機能は残りの AP の位置を特定し、リッチマップに自動的に配置します。AP にグローバル ポジショニング システム (GPS) 機能がある場合、アンカーはマップ上で自動的に配置されます。

アクセスポイント自動ロケーションの制限事項

この機能は、**default-site-tag** ではサポートされていません。

サポートされるプラットフォーム

AP の自動検出機能は、次のプラットフォームとバージョンでサポートされています。

表 18: サポートされるプラットフォームとバージョン

製品	プラットフォーム	リリース
Cisco Catalyst 9100 ファミリア アクセスポイント	• Cisco Catalyst 9130 シリーズ アクセスポイント • Cisco Catalyst 9136 シリーズ アクセスポイント • Cisco Catalyst 9164 シリーズ アクセスポイント • Cisco Catalyst 9166 シリーズ アクセスポイント	必要な最小バージョンは Cisco IOS XE 17.12.1
Cisco Catalyst 9800 シリーズ 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 IOS XE 17.12.x
Cisco Spaces	Cisco Spaces: コネクタ 3	ロケーションサービス 3.1.0.94 以降



(注) サポートされているプラットフォームに加えて、Cisco Spaces クラウドアカウントも必要です。

AP の自動検出の前提条件

デバイスを正しく配置するには、次の前提条件を満たし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 Cisco Spaces : コネクタに接続しており、両方を Cisco Spaces クラウドアカウントで使用できる必要があります。詳細については、『Cisco Spaces: コネクタ 3 コンフィギュレーションガイド』の「[Cisco Catalyst 9800 シリーズ ワイヤレスコントローラにコネクタを接続する](#)」を参照してください。
- フロアに AP を配置するには、リッチマップを使用する必要があります。ロケーションとマップ機能を使用して、リッチマップを追加します。詳細については、「[ロケーションとマップの設定](#)」を参照してください。
- サイトタグはフロアに必須です。Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの GUI を使用してサイトタグを作成します。Cisco Spaces に配置する AP は、サイトタグに関連付けられている必要があります。サイトタグの設定方法について詳しくは、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ ソフトウェア コンフィギュレーションガイドの「[サイトタグの設定](#)」を参照してください。
- AP の詳細時間測定 (FTM) 測距データを生成します。[詳細の表示 (View Details)] をクリックして、測距データの可用性を確認し、[AP 間の測距データを生成](#)します。

AnyLocate の測定データの生成

AP の自動検出プロセスを開始する前に、AP を Cisco Spaces に自動的に配置するために、AP の AnyLocate の測定データを生成する必要があります。測距プロセスにより、選択したエリアの AP チャンネルが共通チャンネルに変更され、FTM を使用して AP 間の距離が特定されます。このプロセスは、一度だけ、または AP が別の環境に移動または追加されたときに実行する必要があります。

Cisco Spaces を使用して、AP の Fine Time Measurement (FTM) の測距データを生成し、フロアマップに配置します。FTM 測距データは RSSI よりも復元力があり、精度が高くなります。サイトタグを選択し、そのサイトタグに関連付けられているすべての AP の測距データを生成します。

始める前に

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの GUI を使用して、次のことを行います。

- [Geolocation Derivation Using Ranging](#) (測距を使用した地理位置情報の逸脱) を有効にすると、**Geolocation Derivation Using Ranging** と対応する AP を、AP の地理位置情報を決定するために測距を使用するロケーションサービスに参加させることができます。
- [アクセスポイント測距パラメータの設定 (Configuring Access Point Ranging Parameters)] https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-12/config-guide/b_wl_17_12_cg/m_ap_crash_file_upload_ewlc.html#configuring-access-point-ranging-parameters-gui : AP が FTM プロトコルをサポートできるようにします。



(注)

- AnyLocate の測定データプロセスは、デフォルトのサイトタグではサポートされていません。
- このプロセスは中断を意味するため、ネットワークがあまりビジー状態でないときに測距プロセスのスケジュールを設定することを推奨します。このプロセスには約 10 分かかります。
- AnyLocate の測定測距プロセスは、サイトタグごとにトリガーできますが、デフォルトのサイトタグではサポートされていません。

手順

ステップ 1 [\[Cisco Spaces\]](#) にログインします。

ステップ 2 Cisco Spaces ダッシュボードで、[メニュー (Menu)] アイコン (☰) をクリックし、[セットアップ (Setup)] > [デバイスの配置 (Device Placement)] を選択します。

ステップ 3 [デバイスの配置 (Device Placement)] ウィンドウで、[生成 (Generate)] をクリックします。

Day-0 構成シナリオでは、使用可能な AP 測距データはなく、GUI に表示される [生成 (Generate)] オプションをクリックして、AP 測距データ生成プロセスを開始する必要があります。[AnyLocate の測定データの生成 (Generate AnyLocate measurement Data)] ウィンドウには、サイトタグ、測距対応 AP の数、コントローラ、および AP モデル情報が表示されます。

図 43: AnyLocate の測定データの生成

Generate AnyLocate measurement Data

NOTE: We do not support generating ranging data for default site tags. Please configure your site tags in your controller. [Learn More](#)

Select the site tags where you want to generate AnyLocate measurement data

Search

Site Tag	Ranging Capable APs	Controller	AP Model
☐ default-site-tag ⓘ	0/3		
☒ Cafe-17	10/10		C9130 CW91 CW91
☐ SJC17-Floor3	20/20		C9130 CW91
☐ SJC17-Floor2	16/16		C9130 C9130
☐ SJC17-No-FTM	1/1		C9130
☐ default-site-tag ⓘ	1/1		C9130

Selected Site Tags: 1 Total APs: 10

Cafe-17 ×

Cancel Next

ステップ 4 [サイトタグ (Site Tag)] 列で、AnyLocate の測定データを生成するサイトタグを選択します。

選択したサイトタグと対応するコントローラの詳細が、ウィンドウの右側に表示されます。[サイトタグ (Site Tag)] チェックボックスをオンにして、すべてのサイトタグを選択することもできます。

(注)

デフォルトのサイトタグの測距データの生成は、Cisco Spaces ではサポートされていません。

ステップ 5 [Next] をクリックします。

ステップ 6 AnyLocate の測定データを生成するスケジュールオプションを選択します。次のオプションを使用できます。

- 後で実行するようにスケジュールする (Schedule it for later) : AnyLocate の測定データを生成する日時を指定するには、このオプションを選択します。

- **すぐに生成（Generate Now）**：AnyLocate の測定データの生成を続行するには、このオプションを選択します。

ステップ 7 [Generate] をクリックします。

デバイスを配置する

デバイスの配置機能を使用して、フロアマップに AP を配置します。Cisco Spaces は、さまざまな測距技術とアルゴリズムを使用して、グローバル地理座標に従って AP を配置します。AP をマップ上に正しく配置するには、各フロアに対してサイトタグを設定する必要があります。

手順

ステップ 1 [Cisco Spaces] にログインします。

ステップ 2 Cisco Spaces ダッシュボードで、[メニュー（Menu）] アイコン（☰）をクリックし、[セットアップ（Setup）] > [デバイスの配置（Device Placement）] を選択します。

ステップ 3 [デバイスの配置（Device Placement）] ウィンドウで、[フロア（Floor）] ドロップダウンリストから、デバイスを配置する必要があるフロアを選択します。

- リッチマップは AP を配置するために必須です。リッチマップが利用できないロケーションには、AP を配置できません。
- [マップのないロケーションを表示（Show Locations without Map）] チェックボックスをオンにして、リッチマップのないロケーションをフィルタリングして表示します。

ステップ 4 Day 0 構成シナリオでは、AP がフロアに配置されていないことを示すメッセージが表示されます。[AP の配置（Place APs）] をクリックしてデバイスを配置します。

[AP の配置（Place APs）] ウィンドウは、[AP の選択（Choose APs）]、[AP の配置（Place APs）]、および [確認と公開（Review & Publish）] の 3 つのセクションで表示されます。

ステップ 5 [AP の選択（Choose APs）] セクションで、特定のフロアに配置する AP が含まれているクラスタに対応するチェックボックスをオンにします。

（注）

- デフォルトでは、[ネイバー AP を自動的にグループ化（Automatically group neighbor APs）] チェックボックスがオンになっており、AP は自動的にグループ化されます。AP のグループ化を解除し、単一のリストとして表示するには、このチェックボックスをオフにします。
- 利用可能なすべての AP クラスタと合計 AP 数が表示されます。
- 各クラスタについて、コントローラ、スイッチ、およびサイトタグ情報を表示できます。
- 複数のクラスタを選択してフロアに割り当てることができます。

- デフォルトのサイトタグを持つ AP は、AP グループ化から除外されます。
- AP グループ化機能は、コネクタの 2023 年 5 月リリースで使用できます。AP グループ化機能を有効にするには、コネクタを最新バージョンにアップグレードすることを推奨します。

- a) (オプション) AP クラスタをクリックして展開し、グループネイバーの下で使用可能な AP を表示します。

右側のパネルに、選択した AP 名と数が表示されます。次の AP 情報を表示できます。

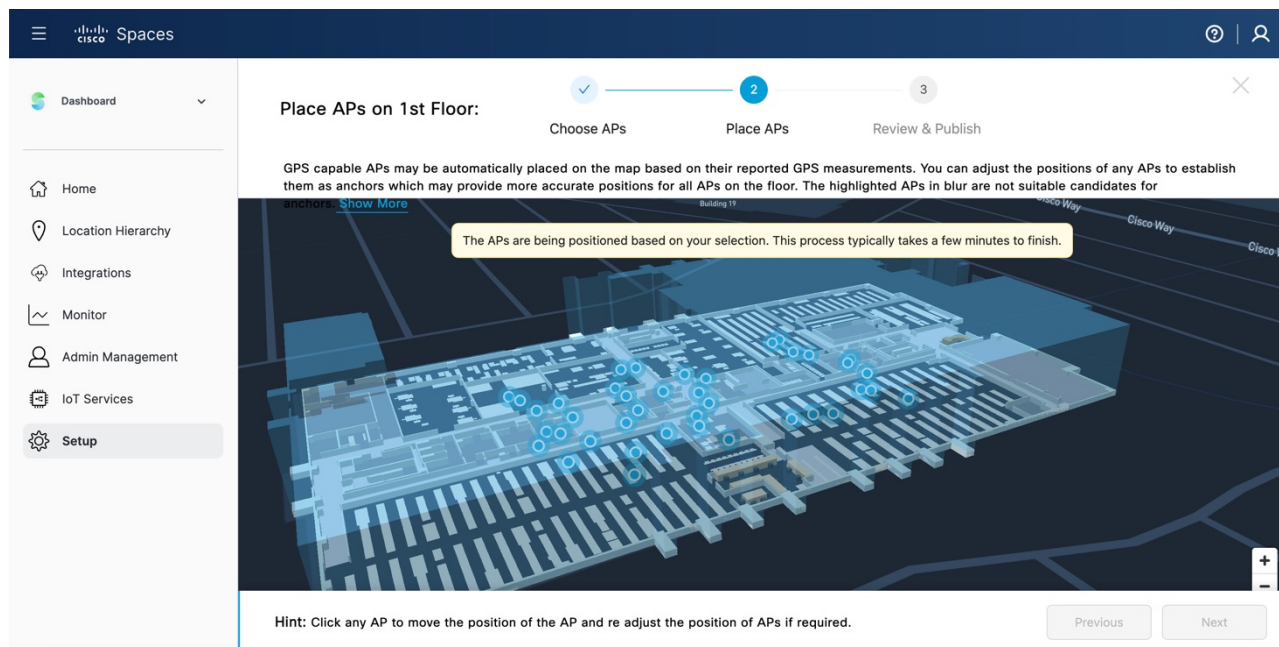
- 名前
- AP Model
- MAC アドレス (MAC Address)
- Controller
- サイト タグ
- Switch Name
- IP Address

- b) (オプション) AP を検索するには、[検索 (Search)] フィールドに AP 名を入力し、**Enter** を押します。
- c) (オプション) [フィルタ (Filter)] をクリックして、フィルタリングパラメータを入力し、使用可能な AP を表示します。

ステップ 6 [Next] をクリックします。

ステップ 7 [APの配置 (Place APs)] セクションでは、自動的に配置された AP を表示できます。

図 44: AP の自動配置



APが正常に配置されると、次のメッセージが表示されます。「The AP placement is complete for this floor. Please verify AP positions and make adjustments if needed or click "Next" to proceed (このフロアの AP の配置が完了しました。AP の位置を確認し、必要に応じて調整するか、[次へ]をクリックして続行してください。)」

(注)

- 青色で強調表示されている AP は、アンカー AP として適していません。
- すべての GPS 対応 AP は、報告された GPS 測定値に基づいて自動的にマップに配置されます。任意の AP の位置を調整して、フロア上のすべての AP に、より正確な位置を提供するアンカーとしてこれらの AP を設定できます。
- GPS 対応 AP がいない場合、AP は AP 間の相対的な位置データに基づいて配置されます。

a) 必要な AP を選択し、手動で位置を調整します。

(注)

AP は次のように色分けされています。

- 自動配置された AP は青色
- 手動で調整された AP は明るい緑色と暗い緑色

追加の GPS モジュールが接続されている AP は、暗い緑色で表示されます。AP をクリックすると、右側のパネルに追加情報が表示されます。

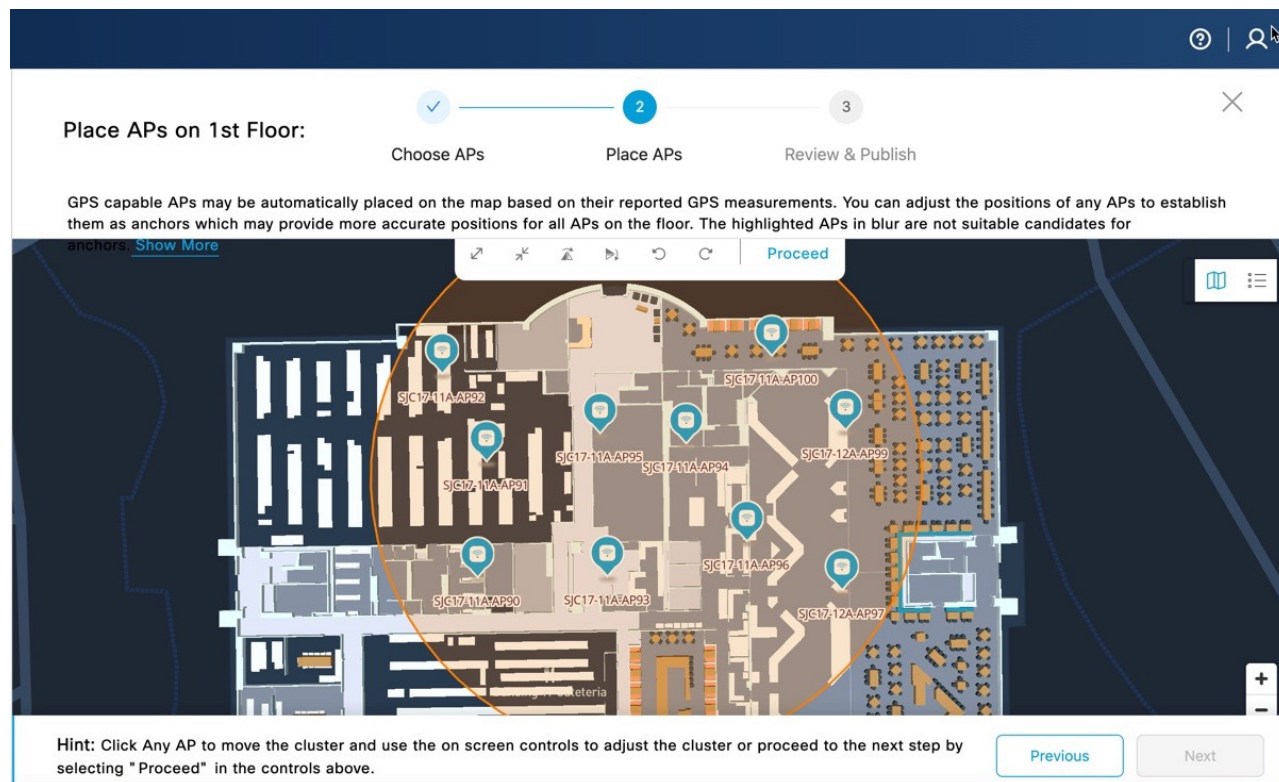
b) 4つの AP の配置を調整すると、再校正を確認するメッセージが表示されます。[再校正 (Recalibrate)] をクリックして、アルゴリズムを再度実行し、AP を自動配置します。

[スキップ (Skip)] をクリックして、この手順をスキップします。

- c) (オプション) APの配置を調整するには、(リッチマップの上部にある  [Proceed](#)) 各コントロールを使用して必要に応じてAPグループの位置を再調整し、[位置の確認/続行 (Confirm Position/Proceed)] をクリックします。

APグループ全体を反転または回転して、グループの配置を調整できます。新しい配置を確認すると、APグループリングは使用できなくなります。

図 45: APの配置セクション



ステップ 8 [Next] をクリックします。

ステップ 9 [確認と公開 (Review & Publish)] セクションで、AP を選択します。

[アクセスポイントの詳細 (Access Point Details)] スライドインウィンドウが表示されます。

- a) デフォルトの AP の高さを編集し、必要に応じて AP 固有のパラメータを変更します。

AP のデフォルトの高さを設定すると、マップに配置されているすべての AP は同じ AP の高さパラメータを継承し、Cisco Spaces : Detect and Locate アプリケーションで共有されます。

- b) [Save] をクリックします。

ステップ 10 [公開 (Publish)] をクリックします。

ポップアップメッセージが表示されたら、[完了 (Done)] をクリックします。配置された AP は、Cisco Spaces : Detect and Locate アプリケーションで表示できます。

デバイスの配置の編集

[AP の配置の変更 (Modify AP Placement)] オプションを使用して、フロアにある AP の配置を更新します。このオプションは、選択したフロアの AP がすでにフロアマップに配置されている場合にのみ、[デバイスの配置 (Device Placement)] ウィンドウで有効になります。

AP の配置に変更があった場合、[デバイスの配置 (Device Placement)] ウィンドウにメッセージが表示されます。[表示 (View)] をクリックして [AP 通知 (APs Notifications)] スライドインウィンドウを表示します。削除された AP、または別のフロアに移動された AP を確認し、必要なアクションを実行できます。

次の AP の詳細を表示します。

- AP Name
- Mac Address
- レポート時間
- 詳細
- ステータス
- コントローラ IP アドレス

手順

ステップ 1 [Cisco Spaces] にログインします。

ステップ 2 Cisco Spaces ダッシュボードで、[メニュー (Menu)] アイコン (☰) をクリックし、[セットアップ (Setup)] > [デバイスの配置 (Device Placement)] を選択します。

ステップ 3 [デバイスの配置 (Device Placement)] ウィンドウで、[フロア (Floor)] ドロップダウンリストから、デバイスの配置を編集する必要があるフロアを選択します。

ステップ 4 [AP の配置の変更 (Modify AP Placement)] をクリックします。

ステップ 5 [AP の選択 (Change APs)] エリアで、更新する必要がある AP のチェックボックスをオンまたはオフにします。

フロアに関連付けられたサイトタグは、AP モデル、MAC アドレス、コントローラ、スイッチ名などの AP の詳細とともに表示されます。

選択した AP は、[選択済み AP (Selected APs)] セクションの下に表示されます。

ステップ 6 [Next] をクリックします。

ステップ 7 [APの配置 (Place APs)] エリアでは、AP の自動配置を表示できます。

Cisco Spaces は、AP の場所を計算し、フロアマップに配置します。AP を含むリッチマップと、計算された各 AP に対する計算された信頼度パーセンテージを表示します。計算された AP が正しく配置されない場合は、AP の配置を手動で調整できます。

ステップ 8 [Next] をクリックします。

ステップ 9 [確認して公開 (Review and Publish)] エリアで、AP の配置の精度を確認し、[公開 (Publish)] をクリックします。

AnyLocate の測定データステータスの表示

AP ロケーションを処理するには、AnyLocate の測定データが必要です。測定データを生成すると、測距プロセスに参加している AP のワイヤレス接続が中断されることがあります。

手順

ステップ 1 [Cisco Spaces] にログインします。

ステップ 2 Cisco Spaces ダッシュボードで、[メニュー (Menu)] アイコン (≡) をクリックし、[セットアップ (Setup)] > [デバイスの配置 (Device Placement)] を選択します。

ステップ 3 [デバイスの配置 (Device Placement)] ウィンドウで、[詳細を表示 (View Details)] をクリックします。

[AnyLocate の測定データステータス (AnyLocate Measurement Data Status)] ウィンドウが表示されます。次の AnyLocate の測定データステータスを表示できます。

- AP およびサイト数用に生成された測距データ
- サイトタグのない AP の数
- 測距データをサポートしていない AP
- 範囲データを生成するスケジュールがあるサイトタグの数

ステップ 4 (オプション) [管理/履歴の表示 (Manage / View History)] をクリックして、測距データ生成の履歴を表示します。

[測距データ履歴 (Ranging Data History)] ウィンドウには、実行済みとスケジュール設定済みの両方の履歴ステータスが表示されます。測距データ生成スケジュールをキャンセルするには、[キャンセル (Cancel)] をクリックします。

ステップ 5 [AP間測距データステータス (AP to AP Ranging Data Status)] ウィンドウでは、次のオプションを表示します。

- **サイトタグ (Site Tag)** : サイトタグを表示します。デフォルトのサイトタグは、AP 測距データではサポートされていません。

- **測距対応AP（Ranging Capable APs）**：フロアに配置されている AP の総数から、測距データを生成できる AP の数を表示します。数字をクリックすると、スライドインウィンドウに詳細が表示されます。
- **コントローラ（Controller）**：コントローラを表示します。
- **APモデル（AP model(s)）**：AP モデルを表示します。
- **ステータス（Status）**：測距データが生成されているかどうかのステータスを表示します。サイトタグに測距データが生成されない場合、ステータスは [使用不可（Not Available）] と表示されます。[生成（Generate）] をクリックすると、データを生成して続行できます。測距データがすでに生成されている場合、ステータスは [使用可能（Available）] と表示されます。必要に応じて、[再生成（Re-Generate）] をクリックしてデータを再生成できます。
- **最終生成（Last Generated）**：測距データ生成のタイムスタンプの詳細を表示します。

図 46: AnyLocate の測定データステータス

Site Tag	Ranging Capable APs	Controller	AP Model(s)	Status	Last Generated
default-site-tag	0/3			Not Available	--
Cafe-17	10/10		C9136I-B, CW9164I-B, CW9166I-B	Available, Re-Generate	28th Nov, 2023, 10:59:32 am
SJC17-Floor3	20/20		C9136I-B, CW9166I-B	Available, Re-Generate	28th Nov, 2023, 10:59:32 am
SJC17-Floor2	16/16		C9130AXI-B, C9136I-B	Available, Re-Generate	28th Nov, 2023, 10:59:32 am
SJC17-No-FTM	1/1		C9130AXE-B	Not Available, Generate	--
default-site-tag	1/1		C9136I-B	Not Available	--

ステップ 6 [閉じる（Close）]（) アイコンをクリックして、ウィンドウを閉じます。

AP の表示

手順

ステップ 1 [\[Cisco Spaces\]](#) にログインします。

ステップ 2 Cisco Spaces ダッシュボードで、[メニュー (Menu)] アイコン (☰) をクリックし、[セットアップ (Setup)] > [デバイスの配置 (Device Placement)] を選択します。

ステップ 3 [デバイスの配置 (Device Placement)] ウィンドウで、[フロア (Floor)] ドロップダウンリストから、配置された AP の詳細を表示するフロアを選択します。

ステップ 4 [AP の表示 (View APs)] をクリックします。

スライドインウィンドウには、フロアに配置された AP の詳細が表示されます。

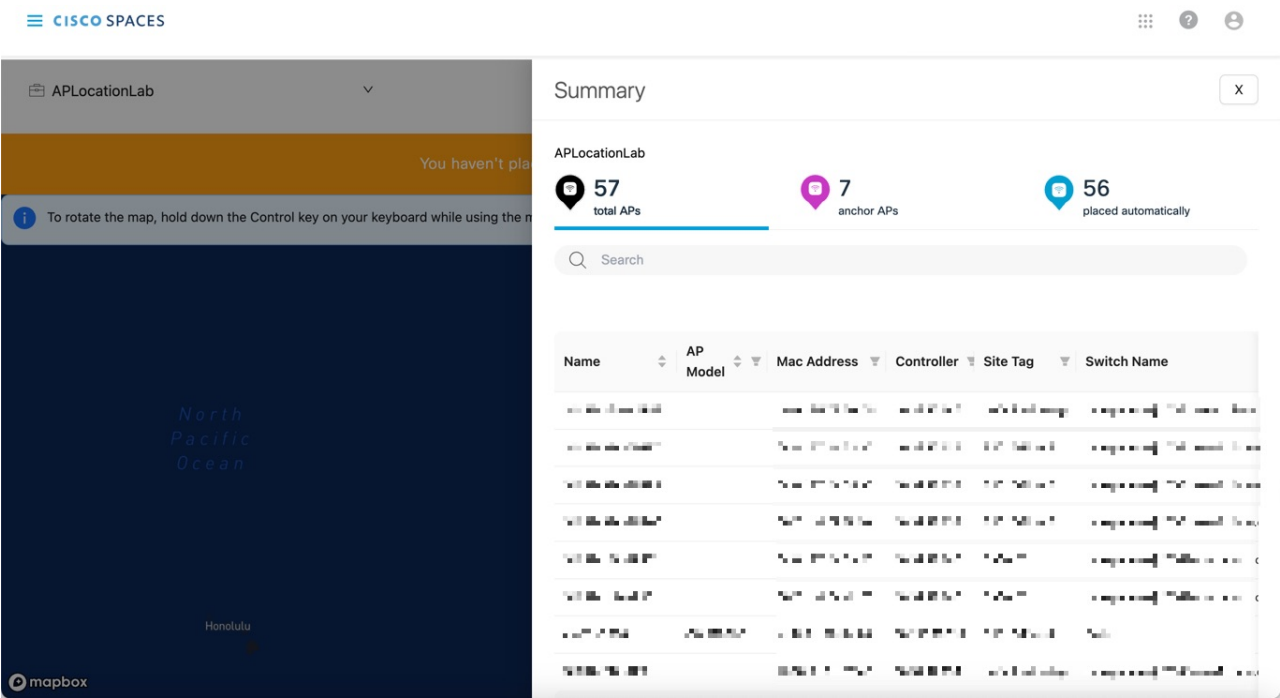
次の AP 間の測距データステータスを表示できます。

- AP の総数
- アンカー AP の数
- 自動的に配置された AP の数

ステップ 5 次の AP の詳細を表示します。

- 名前
- AP Model
- MAC アドレス
- Controller
- サイト タグ
- Switch Name

図 47: AP の詳細を表示



ステップ 6 [閉じる (Close)] (✕) アイコンをクリックして、スライドインウィンドウを閉じます。

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。

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。

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。