Cisco DNA Spaces：検出と検索 コンフィギュレーション ガイド

初版：2019 年 1 月 29 日

最終更新：2021 年 9 月 22 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。

目 次

Full Cisco Trademarks with Software License ?

はじめに：

対象読者 vii

表記法 vii

通信、サービス、およびその他の情報 viii

第 I 部：

製品概要 9

第 1 章

製品概要 1

Cisco DNA Spaces：検出と検索 の概要 1

ライセンス 3

第 II 部：

使用する前に 5

第 2 章

設定 7

Cisco DNA Spaces：検出と検索 アカウントのリクエスト 7

第 3 章

データ ソース 9

位置のデータソースの設定 9

位置のデータソースの設定 9

第 4 章

導入情報 11

導入情報 11

第 III 部：

トラッキングとトレース 13

第 5 章 マップの管理 15
マップの管理 15
Cisco DNA Spaces：検出と検索 へのマップのアップロード 15
Cisco DNA Spaces：検出と検索 でのマップの表示 15
ゾーンの作成 21

第 6 章 スティッキークライアント 23
付箋 23

第 7 章 クライアントの履歴 25
クライアントの履歴 25
クライアントの履歴の表示と再生 25

第 8 章 位置精度 31
位置精度 31
位置精度のテスト 31

第 9 章 グローバル検索 37
グローバル検索 37
グローバル検索 37

第 10 章 デバイス トラッキング 39
デバイス トラッキング 39
デバイストラッキングの有効化または無効化 39
しきい値とカットオフの設定 40
追跡済みデバイスのフィルタリング 40
追跡済みデバイスのフィルタリング 40

第 11 章 カラムの管理 43
カラムの管理 43

第 12 章 セッションの有効期限の管理 45
セッションの有効期限 45
セッションの有効期限の管理 45

第 IV 部： 通知の管理 47

第 13 章 ノースバウンド通知の使用 49
ノースバウンド通知の使用 49
Location Update（ノースバウンド通知） 49
Absence（ノースバウンド通知） 53
Association（ノースバウンド通知） 54
In/Out（ノースバウンド通知） 55

第 V 部： Hyperlocation と FastLocate 59

第 14 章 Hyperlocation の設定 61
Cisco Hyperlocation の有効化 61
Cisco Hyperlocation の設定方法 62

第 15 章 Cisco FastLocate の設定 65
Cisco FastLocate の設定 65
Cisco FastLocate の設定方法 66

第 VI 部： ユーザの管理 69

第 16 章 ユーザの管理 71
ユーザの管理 71
ユーザーロールの設定とユーザーの招待 71
ユーザーとユーザー ロールの変更 72

第 VII 部 : よくある質問 75

第 17 章 FAQ の管理 77

サポートを受けるには 77

Cisco DNA Spaces：検出と検索 アカウントに保存される情報とその保存期間は？ 77

第 VIII 部 : API 79

第 18 章 API 81

Rest API の使用 81

対象読者

このドキュメントは、組織内の資産の使用状況を監視、管理、および最適化するために Cisco DNA Spaces を展開する Cisco Digital Network Architecture（DNA）Spaces ネットワーク管理者および IT 管理者を対象としています。

- 表記法 （vii ページ）
- 通信、サービス、およびその他の情報 （viii ページ）

表記法

このマニュアルでは、次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、キーワード、およびユーザーが入力するテキストは**太字**で記載されます。
イタリック体	文書のタイトル、新規用語、強調する用語、およびユーザーが値を指定する関数は、イタリック体で示しています。
[ ]	角カッコの中の要素は、省略可能です。
{x | y | z }	どれか1つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x | y | z]	どれか1つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
string	引用符を付けない一組の文字。文字列を引用符で囲まないでください。引用符で囲むと、文字列に引用符が含まれます。
`courier` フォント	システムが表示する端末セッションおよび情報は、`courier` フォントで示しています。
<>	パスワードのように出力されない文字は、山カッコで囲んで示しています。

表記法	説明
[]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

（注） 「注釈」です。役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。

ヒント 「問題解決に役立つ情報」です。

注意 「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

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、シスコ サービス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、シスコ サポート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 Marketplace 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 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。

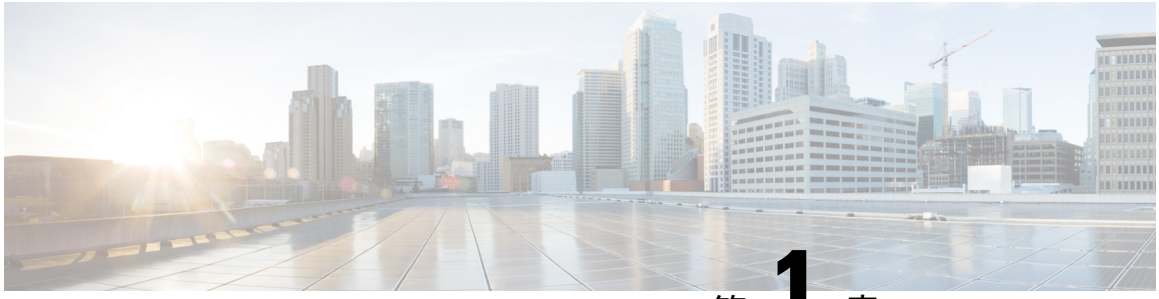
Cisco バグ検索ツール

Cisco 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 Cisco バグ追跡システムへのゲートウェイとして機能する、Web ベースのツールです。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。

第 I 部

製品概要

- 製品概要 （1 ページ）



第 1 章

製品概要

- Cisco DNA Spaces：検出と検索 の概要 （1 ページ）
- ライセンス （3 ページ）

Cisco DNA Spaces：検出と検索 の概要

Cisco DNA Spaces：検出と検索 では、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。

Cisco DNA Spaces：検出と検索 を使用して、ネットワーク内のビルと、ビル内に展開された Wi-Fi アクセスポイント（AP）の固定物理レイアウトを表示できます。GPS マーカー、位置計算用の除外ゾーンまたは包含ゾーンなど、他の固定コンポーネントを確認できます。Cisco DNA Spaces：検出と検索 では、ネットワーク内の Wi-Fi デバイスの動的な性質も確認できます。次のデバイスの計算された位置を表示できます。

- [Associated Wi-Fi devices]：緑色の点で表示されます。IP アドレスや製造元など、シスコ ワイヤレス コントローラ のデバイスに関する情報が含まれます（取得可能な場合）。これらのデバイスがいつ表示されたかの履歴も保持されます。
- [Active RFID Wi-Fi Tags]：この情報は、タグデータを使用するアプリケーションのトラブルシューティングに役立ちます。
- [Rogue Access Points]：コントローラが検出し、「不正」とラベル付けされた AP。AP の MAC アドレスが、推定される位置とともに表示されます。
- [Rogue Clients]：コントローラが検出し、「不正」とラベル付けした Wi-Fi クライアント。クライアントの MAC アドレスが、推定される位置とともに表示されます。
- [Unassociated Wi-Fi devices]：これらのタイプのデバイスの位置とその数がベストエフォートベースで計算され、表示されます。

注　これらのデバイスは、ネットワークに関連付けられていない限り、MAC アドレスを変更でき、有効な位置の履歴がないことに注意してください。

Cisco DNA Spaces は、アクティブなデバイスのみを追跡する位置プラットフォームです。アクティブなデバイスとは、5 分以下の頻度で定期的に Wi-Fi プローブパケットを送信するデバイスで、これらのプローブはデバイスの位置を計算するために使用されます。デバイスがプローブを送信する頻度はデバイス主導であり、確定的ではありません。

Cisco DNA Spaces のクライアントの数（関連付けられているものとプロービングされているもの両方）を コントローラ の数と比較することはできません。これらのシスココンポーネントの設計に根本的な違いがあるためです。コントローラ と Cisco DNA Center の両方が関連付けられているデバイスがアクティブと見なされます。関連付けられたデバイスは、単にネットワークに関連付けられているデバイスです。また、Cisco DNA Center はデバイスの位置について Cisco DNA Spaces に依存しているため、Cisco DNA Center は単なる未配置デバイスとして関連付けられているデバイスのみを表示します。

Cisco CMX デバイスの Cisco DNA Spaces へのテザリングは、顧客の Cisco DNA Spaces への移行を支援するために使用する設計になっています。これにより、顧客はデバイスが Cisco DNA Spaces に最初どのように表示されるかを確認できます。ここでも、Cisco CMX と Cisco DNA Spaces のデバイスの数を比較することはできません。テザリングされたデバイスでは、精度に関するトラブルシューティングを Cisco CMX で行う必要があります。

コントローラ では、アクティブなデバイスを常時プロービングする必要はありません。一方、Cisco DNA Spaces では 5 分以下の頻度で定期的なプロービングが必要です。そのため、コントローラ でアクティブと表示されるクライアントデバイスが Cisco DNA Spaces にはない可能性があります。これらを、位置を確認できないデバイスと呼びます。

次に、Cisco DNA Spaces にデバイスがないと表示される可能性のある理由を一覧で示します。

- デバイスがマップに配置されていない AP によって報告されている場合。コントローラ に接続されている AP の多くがマップに追加されていない場合、これらの AP によって報告されたデバイスは表示されません。
- 関連付けられたクライアントが、バッテリの電力を節約するためにプロービングを減らしている場合。これは正確な位置検出に直接影響します。関連付けられたクライアントがウルトラパワー リザーブ モード（スリープモードで画面が空白になる）に入り、プローブを送信しない場合。これにより、Cisco DNA Spaces はデバイスの位置を検出できなくなります。ユーザーがホーム画面のロックを解除するか、コンテンツのストリーミングを開始すると、デバイスは再びアクティブになり、ワイヤレスネットワークへのプローブの送信を開始します。Cisco DNA Spaces は、このような非アクティブまたはスリープ状態のデバイスを検出できません。
- Cisco DNA Spaces は、Wi-Fi デバイスが定期的に Wi-Fi プローブパケットの更新を送信し、デバイスのステータスがアクティブであることを確認することを期待します。ただし一部のデバイスは、Wi-Fi プローブを送信していないにもかかわらず、コントローラ によりアクティブと見なされ、そのようなデバイスは位置を確認できないデバイスと見なされます。

Cisco DNA Spaces：検出と検索 で使用されているオープンソースの詳細については、以下を参照してください。

https://www.cisco.com/c/en/us/about/legal/open-source-documentation-responsive.html。

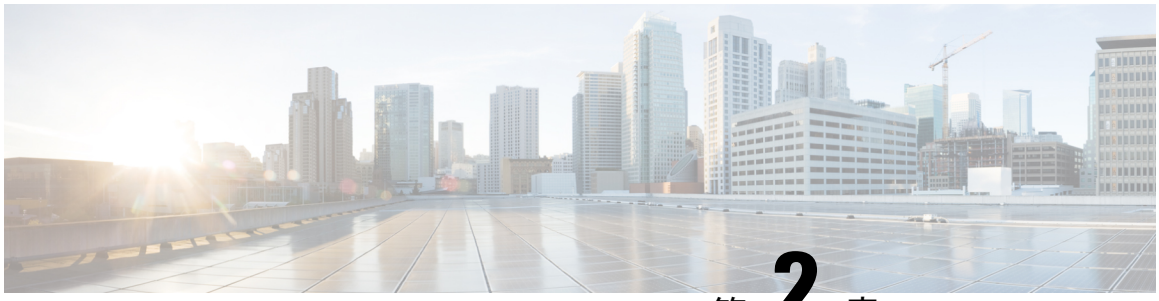
ライセンス

Cisco DNA Spaces：検出と検索 は Cisco DNA Spaces の ACT ライセンスに含まれています

第 II 部

使用する前に

- 設定 （7 ページ）
- データ ソース （9 ページ）
- 導入情報 （11 ページ）



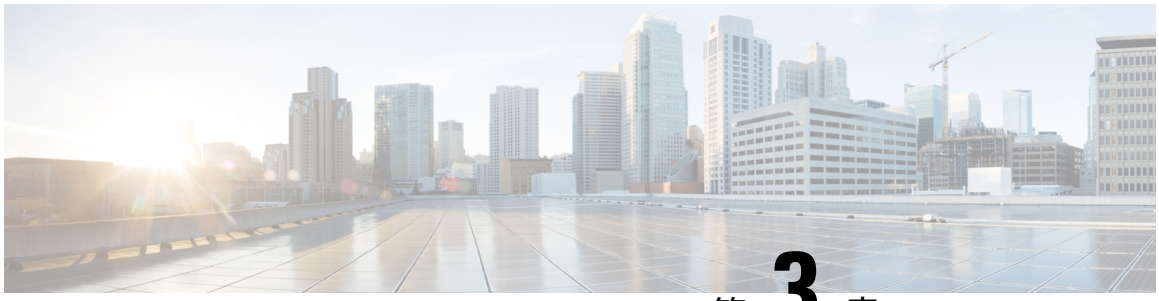
第 2 章

設定

• Cisco DNA Spaces：検出と検索 アカウントのリクエスト （7 ページ）

Cisco DNA Spaces：検出と検索 アカウントのリクエスト

Cisco DNA Spaces でのアカウントをリクエストするには、 Cisco DNA Spaces ダッシュボードでのデモまたはライブアカウント作成のリクエストを、cisco-dnaspaces-support@external.cisco.com に電子メールで送信します。詳細については、「Getting Started with DNA Spaces Dashboard」を参照してください。



第 3 章

データ ソース

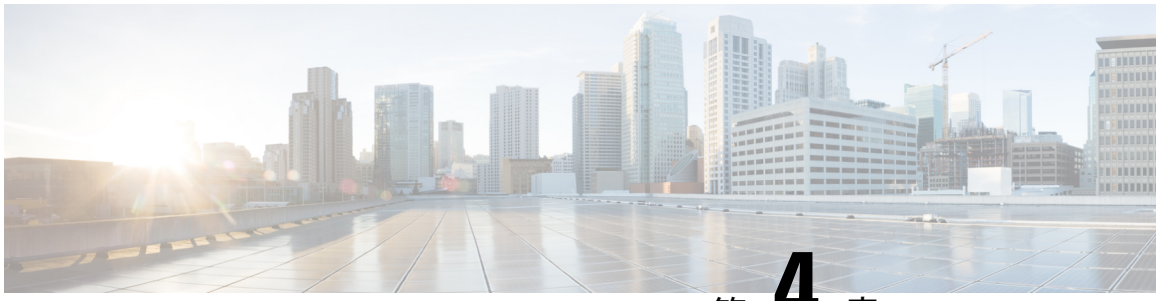
• 位置のデータソースの設定 （9 ページ）

位置のデータソースの設定

位置のデータソースの設定

位置のデータソースとして、次のいずれかを設定できます。

- Cisco DNA Spaces のコネクタ設定。 『Cisco DNA Spaces Configuration』を参照してください。
- シスコ ワイヤレス コントローラ の設定：コントローラ をデータソースとして 検出と位置特定 を設定できます。『Cisco WLC Configuration』を参照してください。
- Cisco CMX のテザリング：Cisco CMX をデータソースとして、Cisco CMX を使用して、ワイヤレスデバイスの位置の計算が行われます。Cisco DNA Spaces：検出と検索 にはワイヤレスクライアントとタグが表示されます。



第 4 章

導入情報

-
- 導入情報 （11 ページ）

導入情報

左側のナビゲーションペインで **[Deployment Information]** に移動して、複数のフロアおよびコントローラへの展開の概要を取得します。

[Deployment Information] ページから、次の情報を表示できます。

- アクティブなアクセスポイント（AP）
- 非アクティブな AP
- コントローラ に接続されている AP
- アップロードしたマップに配置された AP

[Deployment Information] ページには 2 つのグラフが表示されます。1 つのグラフには コントローラ から収集された情報が含まれ、もう 1 つのグラフには Cisco DNA Spaces マップから収集された情報が含まれます。これで、2 つのグラフの情報を比較し、情報が同じかどうかを確認できます。

次の図から、**[APs connected to Controller]** のグラフを確認できます。ここでは、コントローラに関する情報を確認できます。このグラフは、コントローラ には11 の AP が接続されていますが、実際には 8 つの AP のみが コントローラ にデータを送信していることを示しています。3 つの AP は コントローラ にデータを送信していません。このグラフはまた、3 つの AP が Cisco DNA Spaces マップ上に 配置されていないことも示しています。最後に、このグラフは 8 つの AP が Cisco DNA Spaces マップ上に配置されていることを示しています。

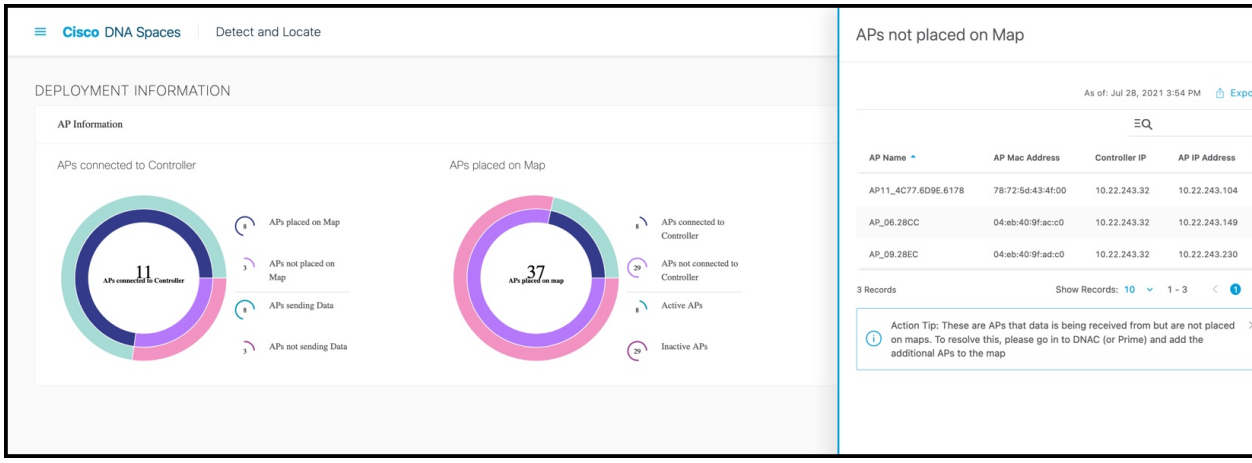
次の図から、**[APs placed on Map]** のグラフも確認できます。このグラフは、Cisco DNA Spaces マップに関する情報を表示しています。グラフは、Cisco DNA Spaces マップ上に 37 の AP があることを示しています。この数には、アクティブ、非アクティブ、および古いアクセスポイントが含まれます。このうち、8 つの AP は コントローラ に接続されており、29 の AP は Cisco DNA Spaces マップ上に存在しますが、いずれの コントローラ にも接続されていません。

また、非アクティブな AP はどれか、またなぜ非アクティブなのかも識別できます。非アクティブな AP は Cisco DNA Spaces マップ上に配置されていますが、受信したデータを報告しません。AP がコントローラに接続されていないか、接続されていても測定データを送信していないため、データは報告されません。この情報の詳細は、グラフと照合して確認できます。次の図で、**[APs placed on Map]** セクションを見ると、29 の AP が非アクティブ（**[Inactive APs]**）で、29 の AP が コントローラ に接続されていない（**APs not connected to the コントローラ**）ことを確認できます。

図 *1 :*

各メトリックをクリックすると、AP の詳細なリストが表示されます。

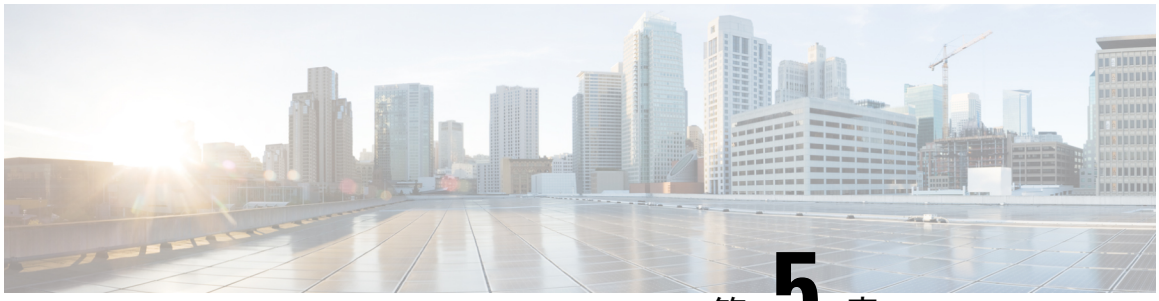
図 *2 :*



第 III 部

トラッキングとトレース

- マップの管理 （15 ページ）
- スティッキークライアント （23 ページ）
- クライアントの履歴 （25 ページ）
- 位置精度 （31 ページ）
- グローバル検索 （37 ページ）
- デバイス トラッキング （39 ページ）
- カラムの管理 （43 ページ）
- セッションの有効期限の管理 （45 ページ）



第 5 章

マップの管理

• マップの管理 （15 ページ）

マップの管理

Cisco DNA Spaces：検出と検索 へのマップのアップロード

最初の設定タスクの 1 つは、Cisco Prime Infrastructure からエクスポートされたマップを Cisco DNA Spaces：検出と検索 にアップロードすることです。通常、マップデータには、フロアイメージ、フロア座標、アクセスポイント（AP）、キャリブレーションデータ、およびフロア上の AP に関する詳細が含まれます。

始める前に

Cisco DNA Spaces：検出と検索 が Cisco DNA Spaces を介して起動されると、マップは Cisco CMX テザリングを通じて自動的に同期されます。

ステップ 1 Cisco DNA Spaces：検出と検索にログインします。

ステップ 2 左側のナビゲーションペインで、**[Maps]** をクリックし、**[Upload]** ボタンをクリックします。

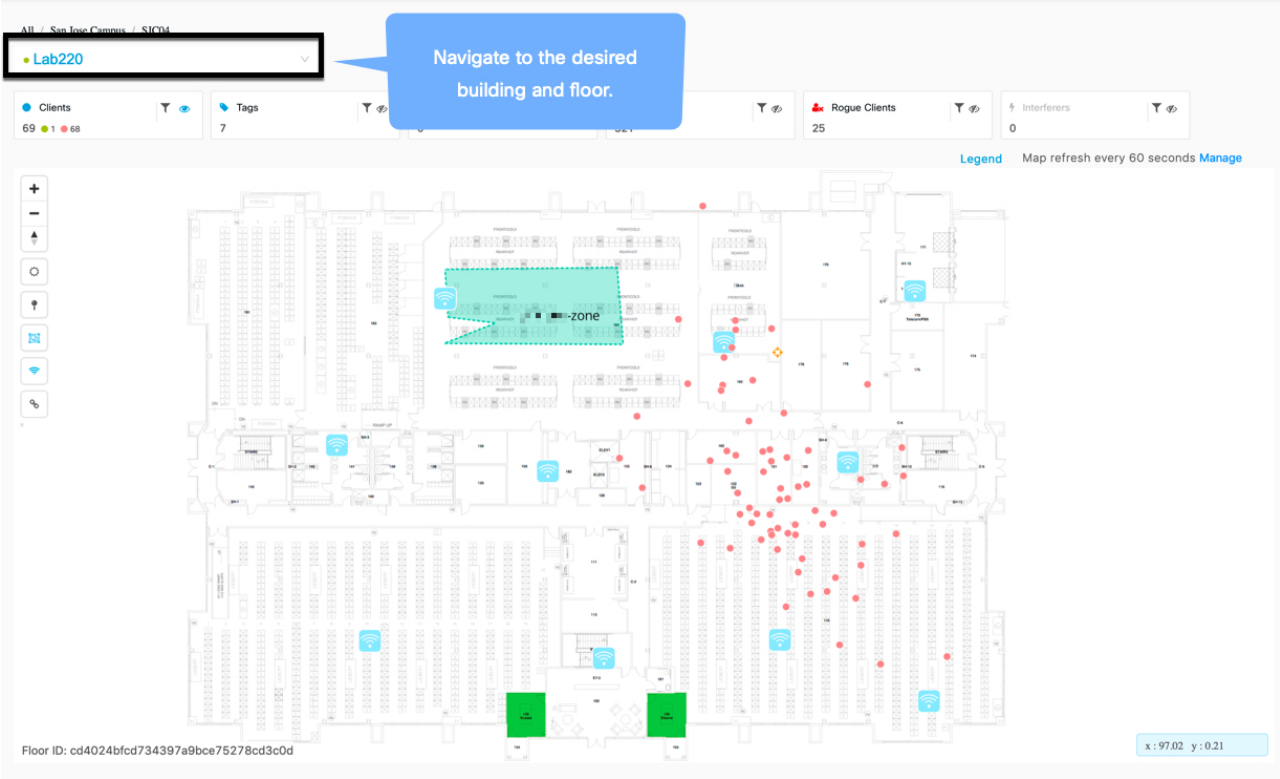
ステップ 3 マップが保存されている場所（コンピュータ上）を検索します。以前 Cisco Prime InfrastructureCisco Prime Infrastructure からエクスポートしたマップを選択します。

ステップ 4 マップが正常にアップロードされたかどうかを確認します。

Cisco DNA Spaces：検出と検索 でのマップの表示

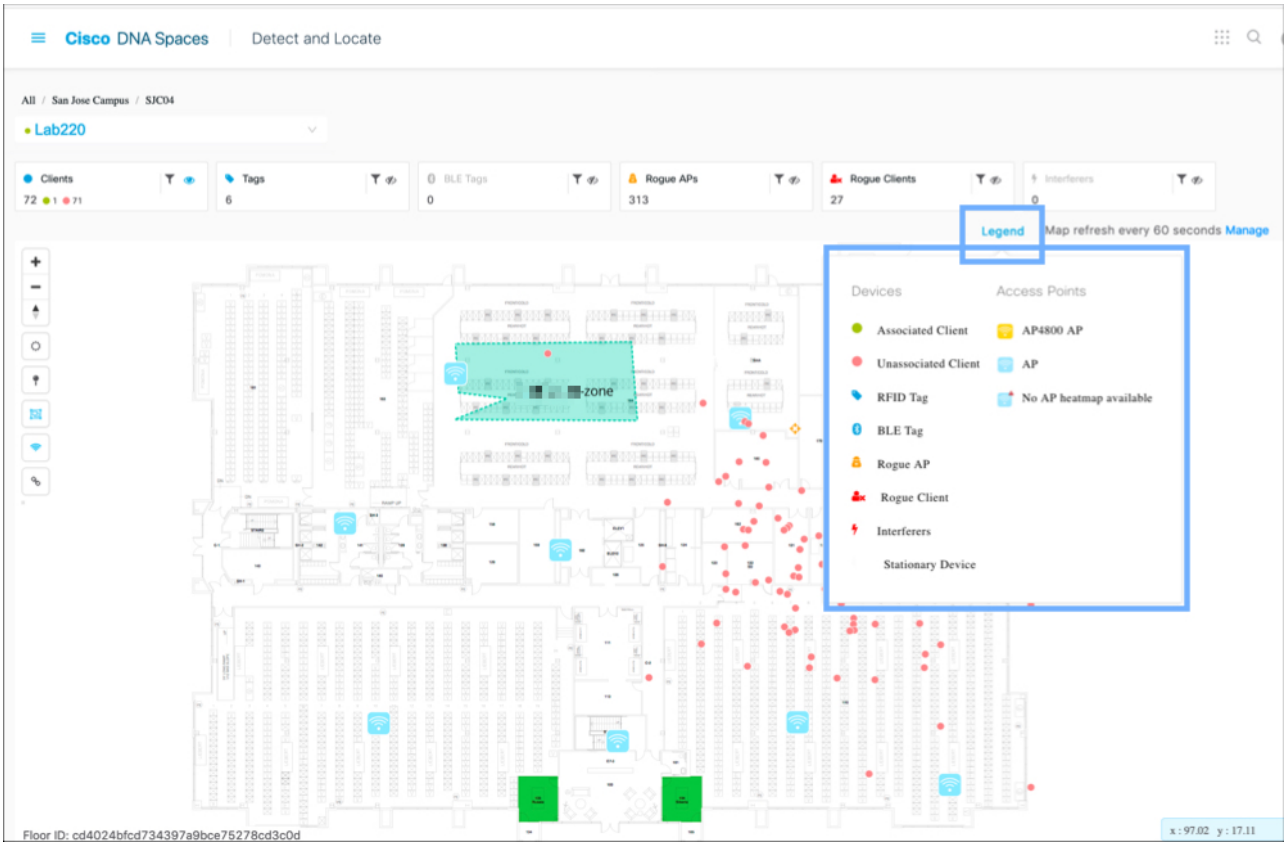
ステップ 1 Cisco DNA Spaces：検出と検索 ダッシュボードから、ドロップダウンリストを使用して、目的のキャンパス、ビル、およびフロアに移動します。

図 *3 : Cisco DNA Spaces*：検出と検索 ダッシュボード



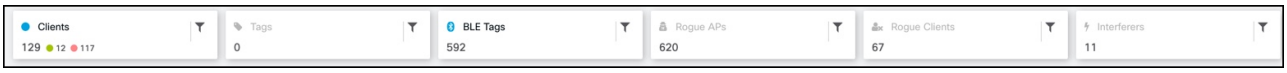
ステップ 2 **[Legend]** をクリックして、マップ上のさまざまなマーキングを確認します。

図 *4* : 凡例



ステップ 3 画面トップのツールバーから、任意の組み合わせのアイコンを選択して、デバイスのビューをカスタマイズします。

図 *5* : *[Dashboard]*：合計数ツールバー



- [Clients]：すべてのクライアントデバイス（接続済みで検出済み）。
  - 赤色の点 は、プロービングのクライアントを示します。クリックすると、クライアントに関する詳細が表示されます。
  - 番号 に関連付けられた点は、プロービングクライアントのクラスタを示します。クリックすると、そのクラスタ内のすべてのクライアントの詳細が表示されます。ズームインしてクライアントを個別に表示することもできます。
  - 緑色の点 は、接続されているクライアントを示します。クリックすると、クライアントの詳細が表示されます。

- [Rogue Access Points]：Cisco CMX インフラストラクチャの一部ではない、または管理されていない AP。クリックすると、詳細が表示されます。
- [Rogue Clients]：不正アクセスポイントに接続しているクライアント。
- [Interferers]：無線周波数干渉を引き起こす可能性のあるデバイス。.
- [Tags]：Wi-Fi タグに関連するベンダー固有の情報は、RAW 形式で表示されます。
- [BLE Tags]：トラックデバイスに接続された Bluetooth Low Energy タグ。

ステップ 4 （任意）アイコンをクリックして、表示された項目をフィルタリングします。これらのフィルタは永続的であり、セッション全体で有効です。

ステップ 5 次のアイコンの任意の組み合わせを選択して、[zones]、[access points]、[tags] 、[heat maps] などのダッシュボードの他の要素を有効または無効にします。

図 *6 : [Dashboard]*：左側のツールバー

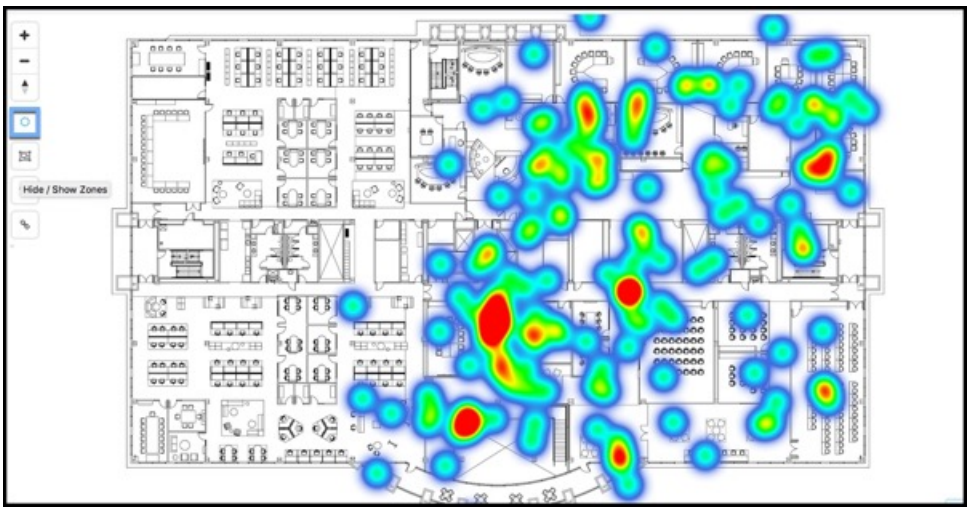
- [Zones] ：特定のフロアのゾーンを表示または非表示にします。

- [Access Point]：特定のフロアに展開されているすべての APをが表示または非表示にします。マップが 検出と位置特定 にアップロードされている場合、どの AP にデバイス位置（ 

）があり、どのAPのデバイス位置に問題があり、トラブルシューティングが必要か（ 

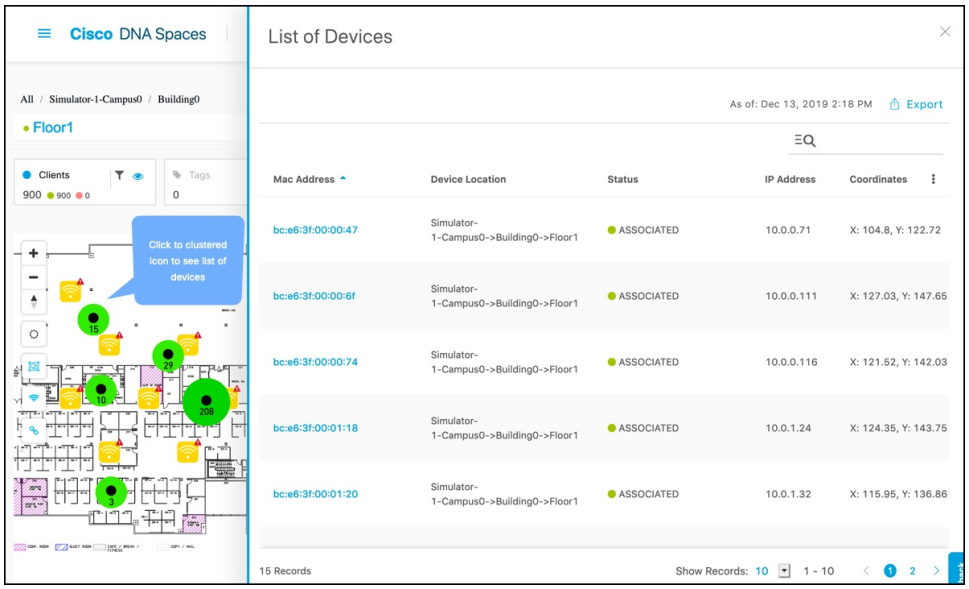
）がマップに表示されます。
- [Heatmap]：さまざまなクライアントの動きをヒートマップとして表示します。

図 7: ヒートマップ



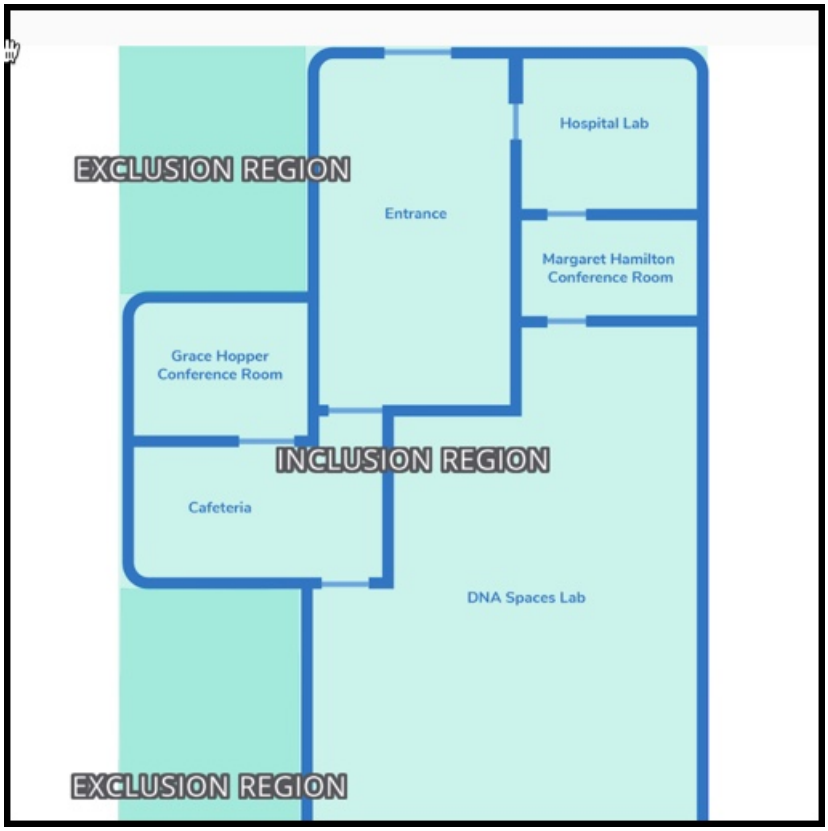
- [Clustering]：近接し、重複している可能性のあるデバイスをグループ化するには、クラスタリングを有効にします。クラスタ化されたアイコンをクリックすると、別のウィンドウにデバイスのリストが表示されます。

図 *8*：クラスタ



- **[Show/Hide Inclusion and Exclusion Regions]**：包含領域と除外領域の表示を有効にします。

図 *9*：包含領域と除外領域の表示/非表示

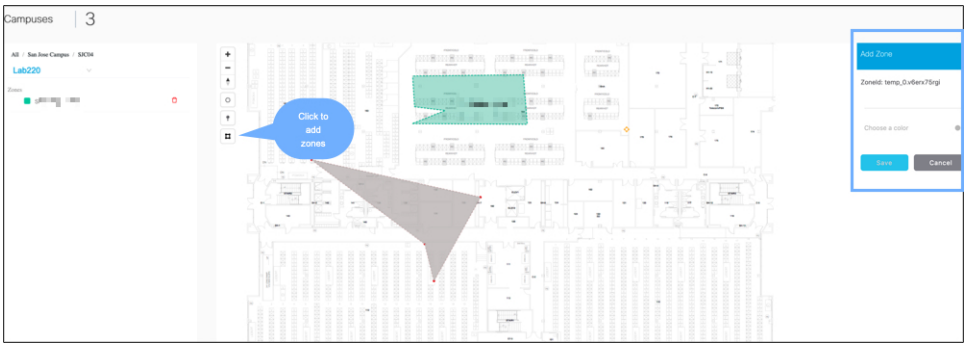


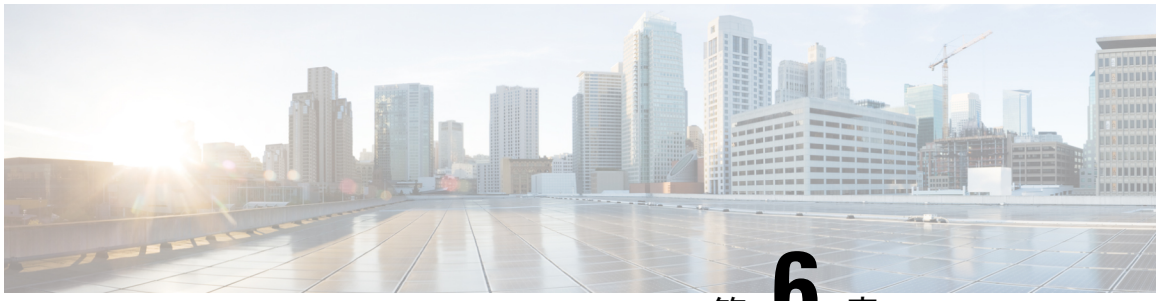
（注）
- フロアごとに 1 つの包含領域のみ設定可能です。
- デバイストラッキングが不要なエリアには、フロアごとに複数の除外ゾーンを追加できます。

ゾーンの作成

左側のナビゲーションペインで、**[Maps]** をクリックし、ゾーンを作成する必要があるロケーションを検索します。左側のツールバーから **[Create a Zone]** アイコンをクリックし、ゾーン境界を作成するマップをクリックします。ダブルクリックして、ゾーンの作成を完了できます。ゾーンをマップに配置した後、ゾーンの名前を追加します。ゾーンを拡大して表示できます。

図 *10* : ゾーンの作成





第 6 章

スティッキークライアント

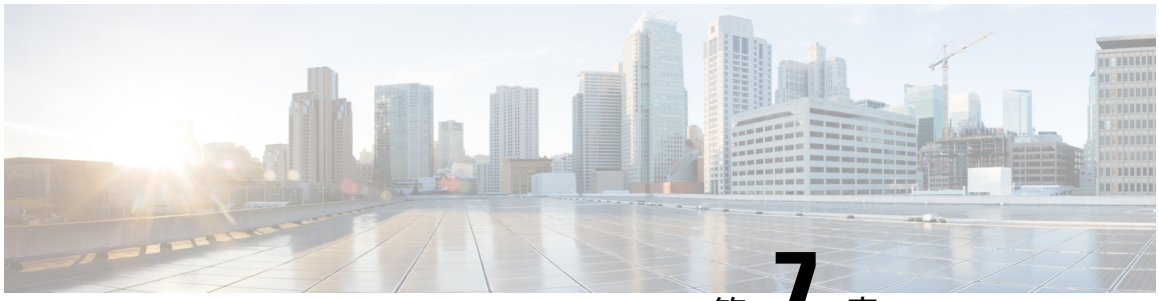
• 付箋 （23 ページ）

付箋

通常、関連付けられたクライアントは、周辺にある他の AP と比較して、接続されているアクセスポイントに最も近接しています。しかし、デバイスがあるアクセスポイントに接続し、別のアクセスポイントの範囲内に移動し、他のより近接した AP との関連付けが変更されない場合があります。このようなクライアントは、スティッキークライアントと呼ばれます。

たとえば、ユーザーが 1 階に入り、同じ階のアクセスポイントに接続したとします。ユーザーが 3 階に移動し、そこにとどまります。そのデバイスの接続された AP が 3 階に変更されると予測していても、これが変更されない場合、スティッキークライアントと呼びます。これは、より遠距離にある AP へのスティッキー性のためにローミングパターンが反映されないためです。

スティッキークライアントに関するこの情報はコントローラから取得され、Cisco DNA Spaces では計算されません。Cisco DNA Spaces がクライアントをスティッキーとしてタグ付けする場合、Cisco DNA Spaces によるデバイスの処理方法に違いはありません。Cisco DNA Spaces はコントローラからのメッセージを受信し続け、デバイスの状態を反映します。Cisco DNA Spaces：検出と検索 UIで、関連付けられているスティッキークライアントをクリックすると、デバイスが最も近い APに接続されていない、または別のフロアの AP に接続されていることを確認できます。



第 7 章

クライアントの履歴

• クライアントの履歴 （25 ページ）

クライアントの履歴

クライアントの履歴の表示と再生

クライアント再生機能では、敷地内でクライアントを検出し、クライアントの移動を追跡できます。一度に 1 人のクライアントについてのみ、アクティビティを追跡できます。

（注） クライアントの情報の追跡は 30 日間に制限されます。

ステップ 1 Cisco DNA Spaces ダッシュボードにログインして、Cisco DNA Spaces：検出と検索 をクリックします。

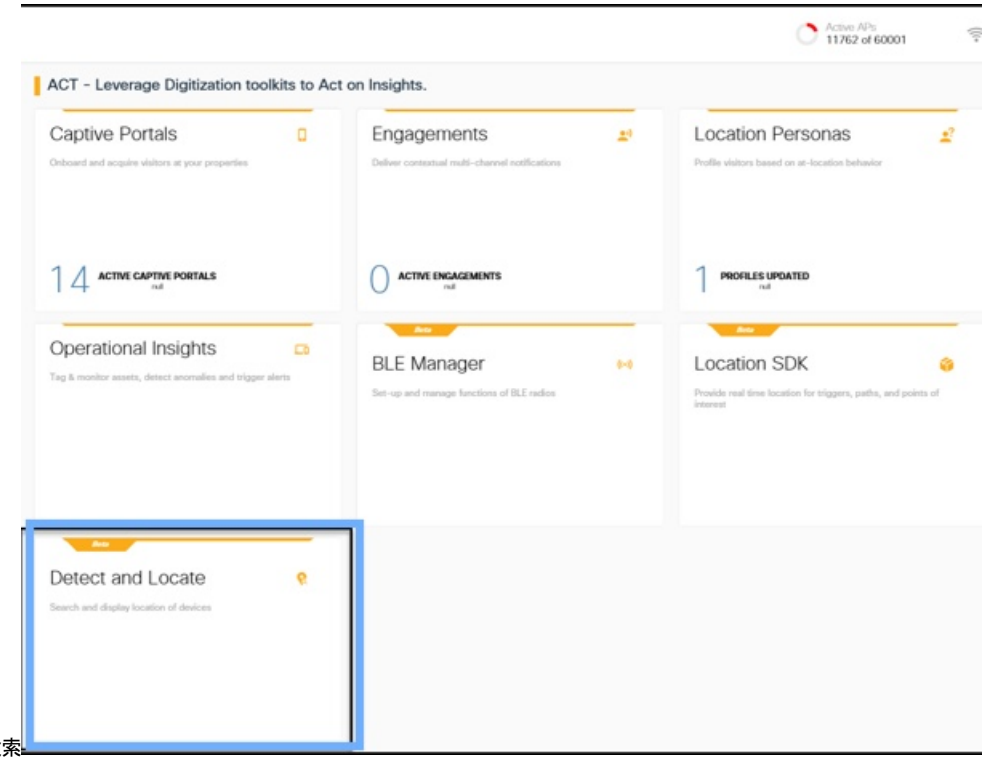
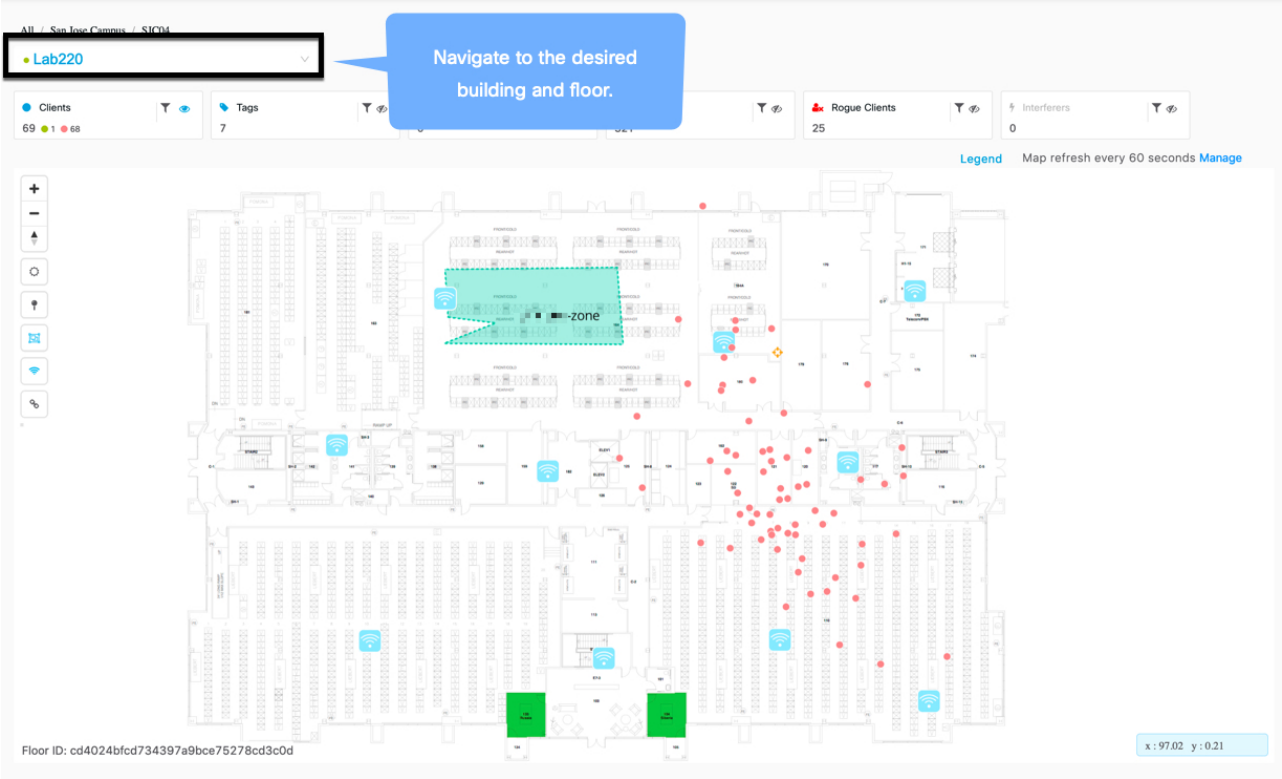


図*11:CiscoDNASpaces*：検出と検索

ステップ 2 Cisco DNA Spaces：検出と検索 ダッシュボードから、ドロップダウンリストを使用して、目的のキャンパス、ビル、およびフロアに移動します。

図 *12 : Cisco DNA Spaces* : 検出と検索 ダッシュボード

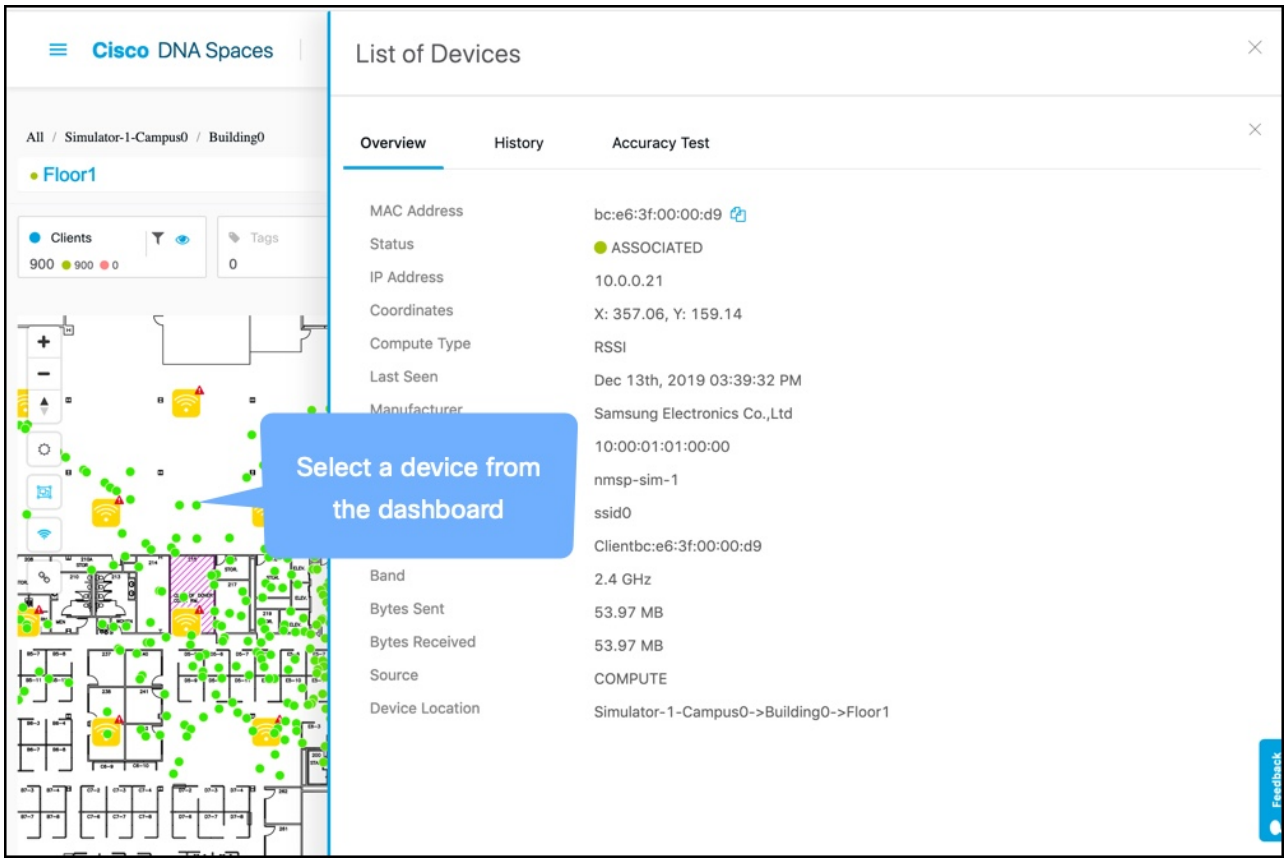


ステップ 3 上部ペインの **[Clients]** の目のアイコンで表示される **[Show/Hide]** ボタンを使用して、すべての追跡対象クライアント（接続済みおよび検出済み）がダッシュボードに表示されることを確認します。

図 *13 :* 目のアイコン

ステップ 4 マップ上の緑色の点のアイコンをクリックしてクライアントを選択し、**[Details]** を表示します。

図 *14 : Cisco DNA Spaces*：検出と検索 ダッシュボード



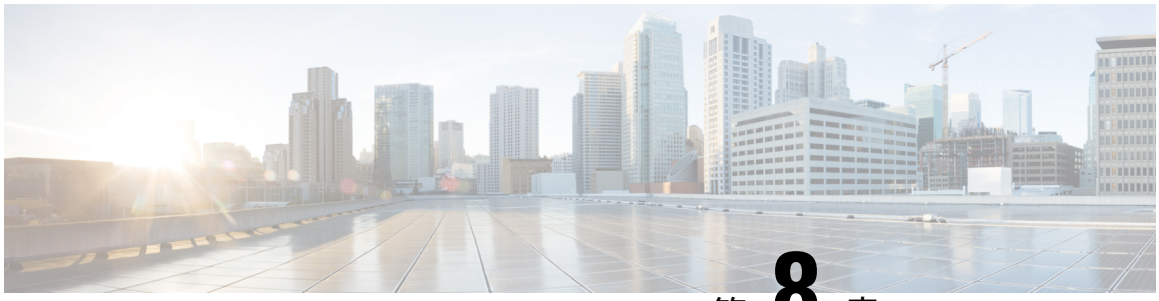
ステップ 5 **[History]** をクリックすると、過去 24 時間（デフォルト設定）にプロットされたクライアントの位置が表示されます。

図 *15 : Cisco DNA Spaces*：検出と検索 クライアントの履歴

ステップ 6 **クライアント履歴**は、次の 2 つの形式で表示されます。

- 線形タイムフレーム：クライアント履歴は線形タイムフレーム上に点で表示され、青色の線が開始時刻と終了時刻を表します。位置情報は点で表示されます。カーソルを合わせると、特定の時間の位置が表示されます。
- マップ：クライアントの位置は、マップ上に緑色と赤色の点で表示されます。赤色は、デバイスがまだプローブ中で、ネットワークに関連付けられていないことを示します。クライアントが手動でネットワークから切断されたか、またはネットワークの問題が原因で、クライアントがプロービングしている可能性があります。緑色は、デバイスが接続されていることを示します。また、緑色と赤色の点の形式でマップ上に点がプロットされ、青色の線で接続されていることも確認できます。

ステップ 7 ヒートマップとして表示されるクライアント履歴を確認します。ヒートマップはデバイスのロケーションチャープのプロットであり、デバイスが移動した位置を示します。これは、疑わしいデバイスの動作を特定するのに役立ち、欠落している機器の追跡にも使用できます。



第 8 章

位置精度

• 位置精度 （31 ページ）

位置精度

位置精度のテスト

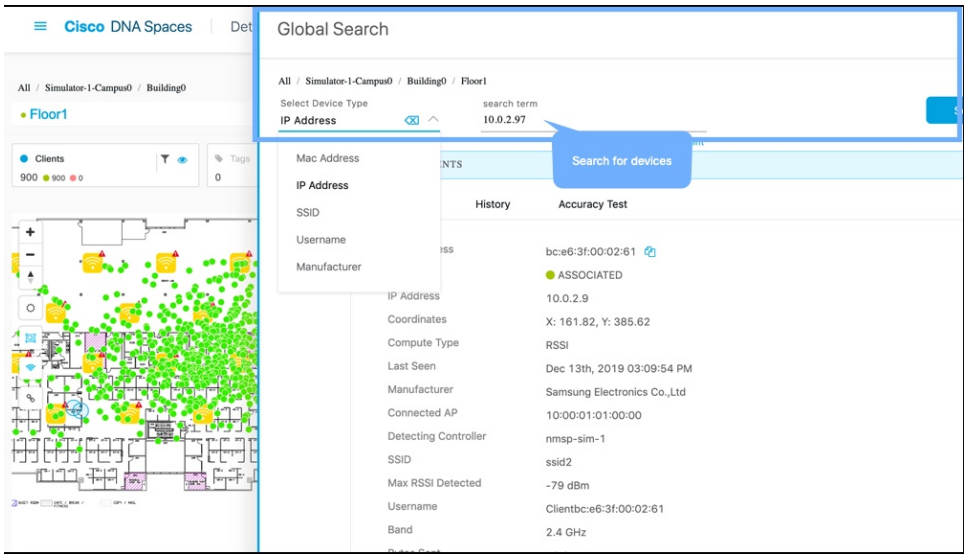
複数の位置ポイントを使用して、1 つのデバイスの位置精度テストを実行できます。位置精度テストツールを使用して、最善の位置精度エクスペリエンスを実現するためのアクセスポイント（AI）の配置と個数を検証できます。位置精度ツールにより、管理者は特定のロケーションの位置精度を定量化できます。位置精度テストにおいて、管理者はワイヤレス クライアント デバイスを使用して、デバイスの実際の位置と計算された位置の差を測定します。

（注）

- 表示更新時間は 3 秒で、再設定はできません。
- 位置精度テストは、外部アンテナ（Marlin 1、2、3、4 など）を使用する Axel-E AP ではサポートされていません。ただし、これらの Axel-AP では位置検出がサポートされています。

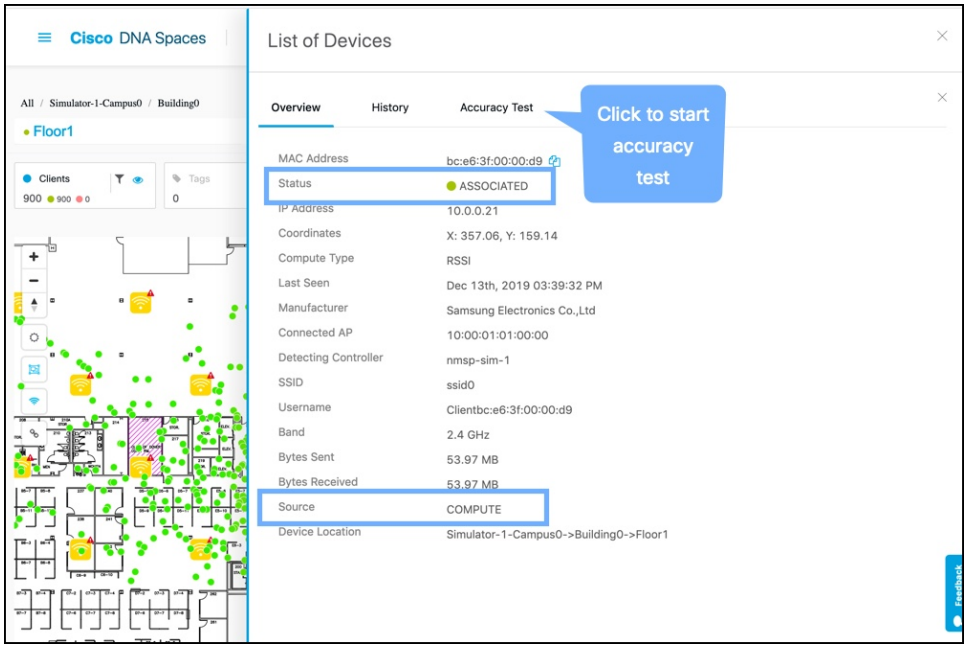
ステップ 1 Cisco DNA Spaces：検出と検索 ダッシュボードから、**[Search MAC, IP, SSID, Manufacturer]** テキストフィールドの MAC アドレスを使用してデバイスを検索します。

図 *16* : 検出と位置特定：ダッシュボード



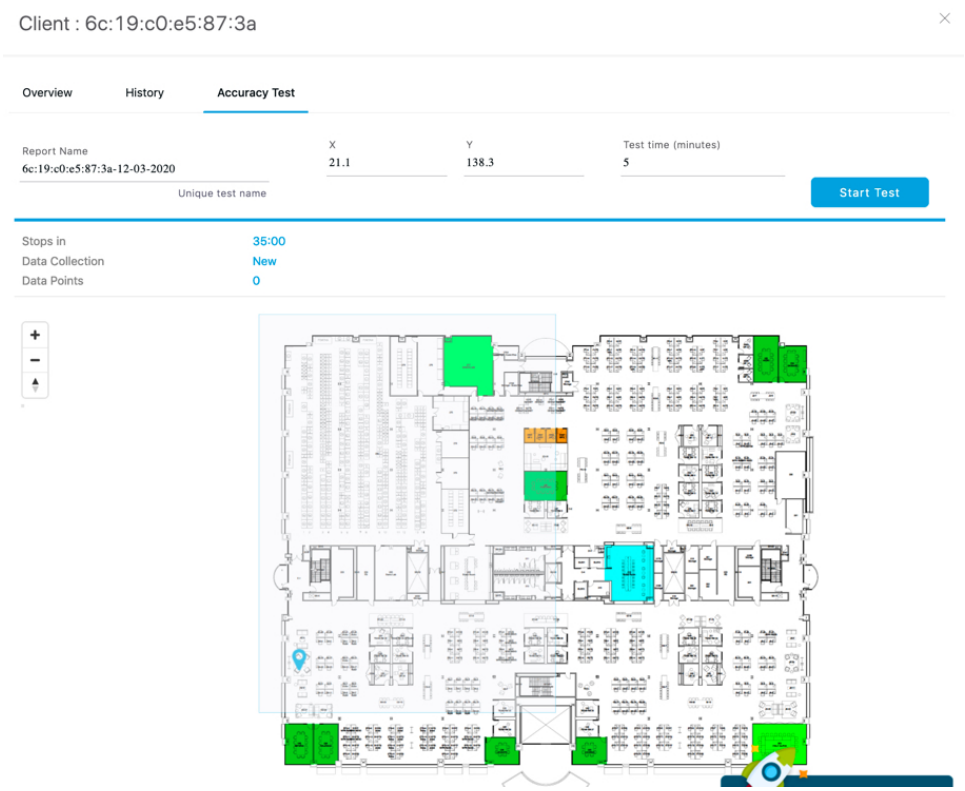
ステップ 2 デバイスの **[Status]** が「**ASSOCIATED**」で、**[Source]** が「**COMPUTE**」であることを確認します。**[Accuracy Test]** をクリックして、精度テストを開始します。

図 *17* : 検出と特定：精度テストの開始



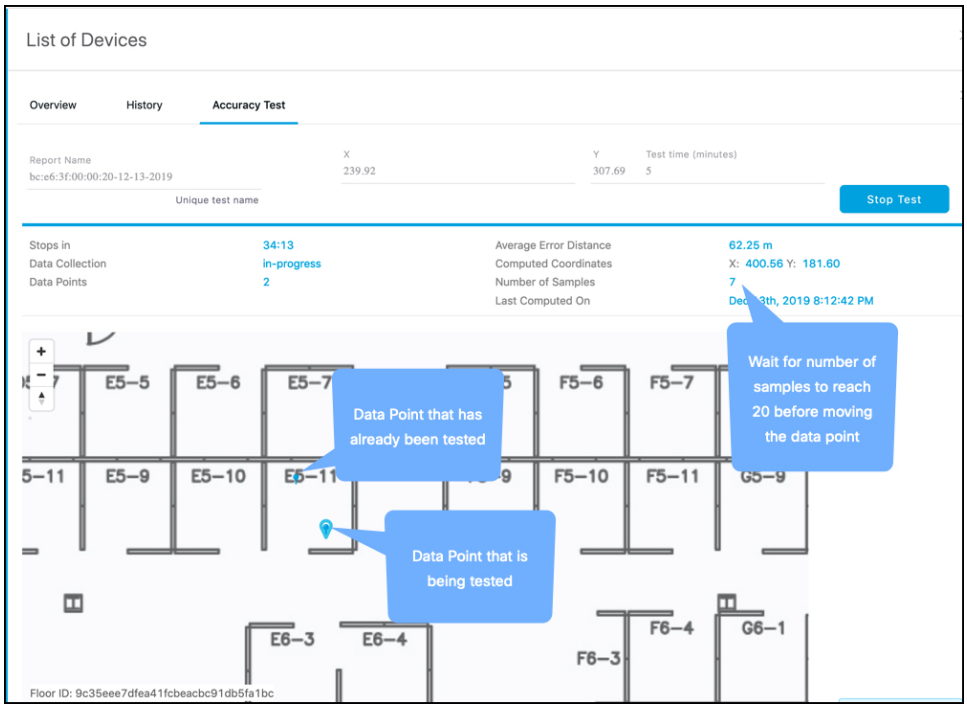
ステップ 3 一意のレポート名を入力します。青色のポインタをクライアントのリアルタイムの位置に移動するか、X 座標と Y 座標を調整します。**[Start Test]** をクリックして、位置精度テストを開始します。

図 *18 :* 検出と特定：精度テストの開始

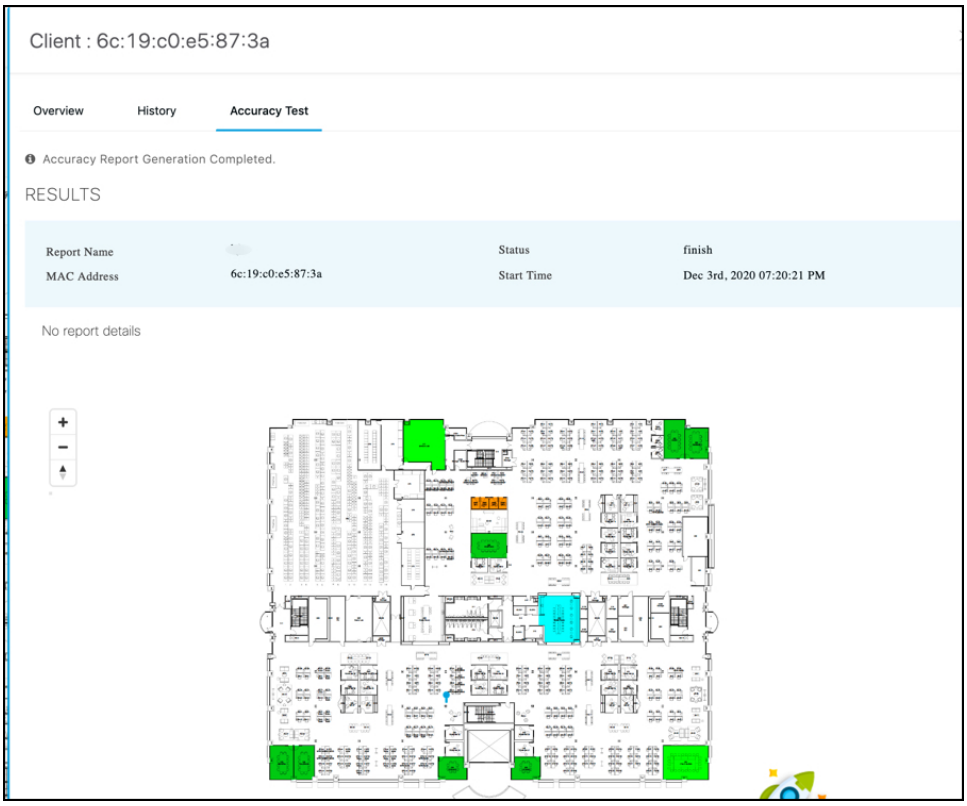


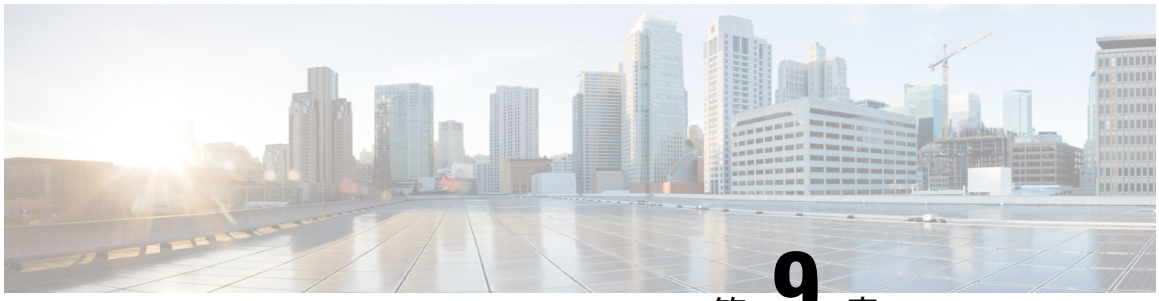
サンプル数が増加し始めていることがわかります。

ステップ 4 サンプル数が 20 に達するのを待ち、**[Stop Test]** をクリックします。データポイントを表す青色のポインタを新しいロケーションに移動し、**[Start Test]** を再度クリックします。



ステップ 5 位置精度をより正確に把握するには、複数のロケーションでこの手順を繰り返します。


Client : 6c:19:c0:e5:87:3a
Overview
History
Accuracy Test
Accuracy Report Generation Completed.
RESULTS
Report Name
MAC Address
6c:19:c0:e5:87:3a
Status
finish
Start Time
Dec 3rd, 2020 07:20:21 PM
No report details



第 9 章

グローバル検索

• グローバル検索 （37 ページ）

グローバル検索

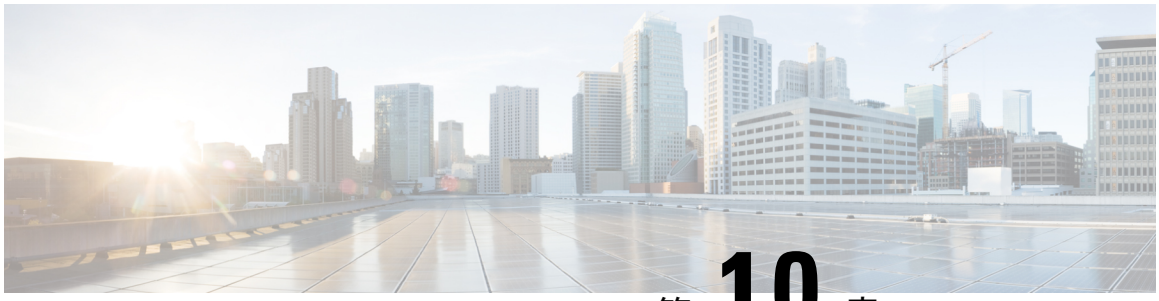
グローバル検索

Cisco DNA Spaces：検出と検索 アカウントで追跡されるすべてのアセットで、グローバル検索を実行できるようになりました。次のパラメータのいずれかに基づいてアセットを検索できます。

- メーカー
- IP アドレス
- SSID
- ユーザ名
- MAC アドレス

（注）

- **[Search]** フィールドに入力する情報では、大文字と小文字が区別されません。
- 文字列の一部のみを入力して検索することもできます。たとえば、検索フィールドに **bc** と入力すると、**bc** という文字を含むすべての結果が返されます。



第 10 章

デバイス トラッキング

- デバイス トラッキング （39 ページ）
- 追跡済みデバイスのフィルタリング （40 ページ）

デバイス トラッキング

デバイストラッキングの有効化または無効化

Cisco DNA Spaces：検出と検索 は、ネットワーク内の次のデバイスを追跡できます。

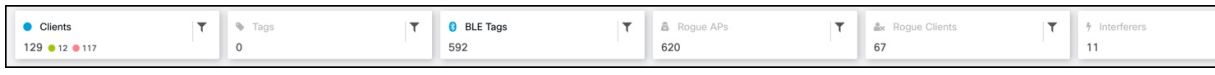
[Configure]、**[Tracking]** の順に選択して、デバイストラッキングを有効または無効にします。

- Wireless Clients
- 干渉（Interferers）
- Rogue Access Points
- RFID
- Rogue Clients

Cisco DNA Spaces：検出と検索 ダッシュボードから有効なコンポーネントを表示します。

それぞれの **[Show / Hide]** ボタン（目のアイコンで表示）を有効にすると、ダッシュボードでコンポーネントを表示できます。

図 *19 : [Dashboard]*：合計数ツールバー



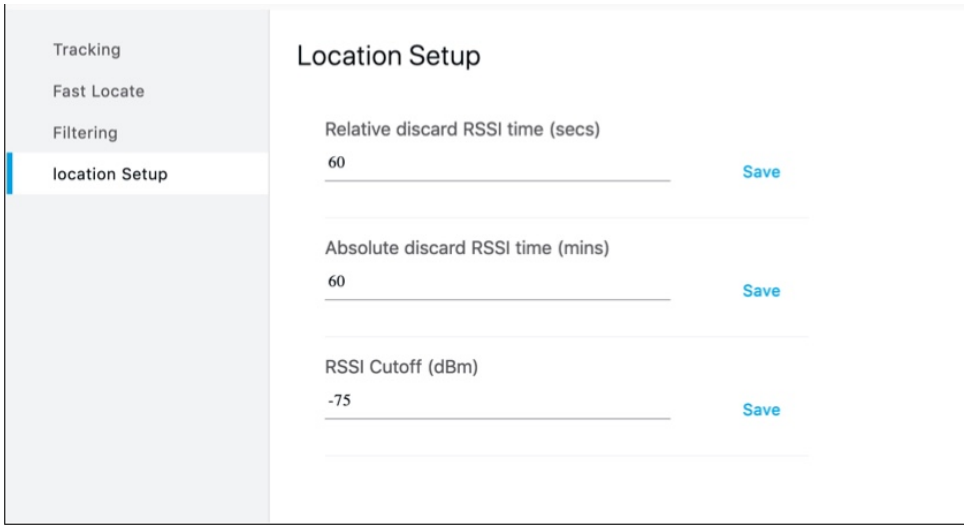
Cisco DNA Spaces：検出と検索 は、10 分のデバイス削除時間を維持します。コントローラ から更新（RSSI、AOA、情報、統計情報）を受信している限り、デバイスはアクティブなままで、ダッシュボードに表示されます。この削除時間内にデバイスの更新（RSSI、AOA、情報、統計情報）を受信しないと、デバイスはシステムから削除されます。

しきい値とカットオフの設定

[Configure]>[Location Setup] を選択して、さまざまなしきい値とカットオフを設定します。

- **[Relative discard RSSI time (secs)]**：ここに指定する期間（秒単位）の経過後に、RSSI 測定が古いものと見なされ、位置計算に使用されなくなります。この時間は、最新の RSSI サンプルからの時間であり、絶対時間ではありません。たとえばこの値を 3 分に設定し、2 つのサンプルが 10 分と 12 分で受信される場合、両方のサンプルが保持されます。ただし、15 分に受信された追加サンプルは無視されます。
- **[Absolute discard RSSI time (mins)]**：最新サンプルに関係なく、ここに指定する時間の経過後に、RSSI 測定が古いものと見なされ、位置計算に使用されなくなります。
- **[RSSI Cutoff (dBm)]**：サーバーが AP 測定を無視する RSSI カットオフ値を dBm 単位で入力します。

図 *20 :* しきい値とカットオフの設定



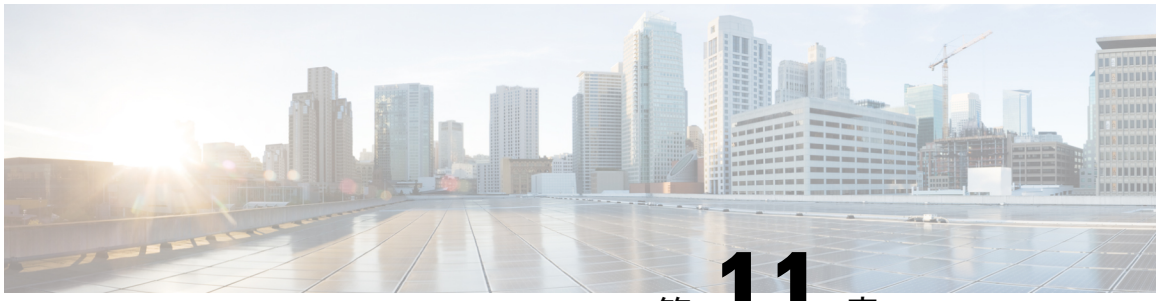
追跡済みデバイスのフィルタリング

追跡済みデバイスのフィルタリング

[CONFIGURE] > [Filtering] タブのさまざまなパラメータで、追跡したデバイスをフィルタリングできます。

- **[RSSI Cutoff]**：弱いプロービングクライアントをフィルタリングするためのカットオフ値を指定します。このカットオフ値により、Cisco DNA Spaces：検出と検索 は初期段階にあり精度の低いプローブ中のクライアントを除外できます。

- **[Enable Locally Administered MAC Filtering]**：トグルボタンを使用して、ローカルで管理される MAC フィルタリングを有効または無効にできます。
- **[Exclude Probing Only client]**：トグルボタンを使用して、プローブ専用クライアントを除外または含めることができます。
- **[Allow MAC Address]**：許可される MAC アドレスのリスト。
- **[Disallow MAC Addresses]**：許可されない MAC アドレスのリスト。
- **[Enable MAC Filtering]**：このトグルボタンを使用して、MAC フィルタリングを有効または無効にできます。
- **[Allow Location SSID Filtering]**：許可される SSID のリスト
- **[Disallowed Location SSID Filtering]**：許可されない SSID のリスト。



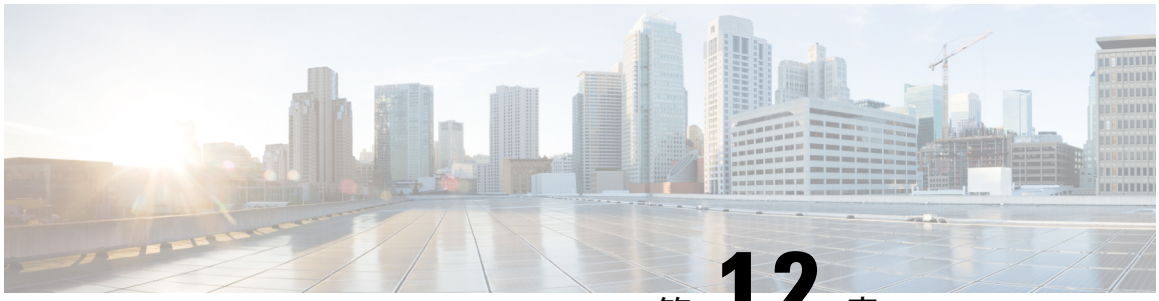
第 11 章

カラムの管理

- カラムの管理 （43 ページ）

カラムの管理

[Manage Columns] ボタンをクリックして、カラムの並べ替え、非表示、表示を行います。



第 12 章

セッションの有効期限の管理

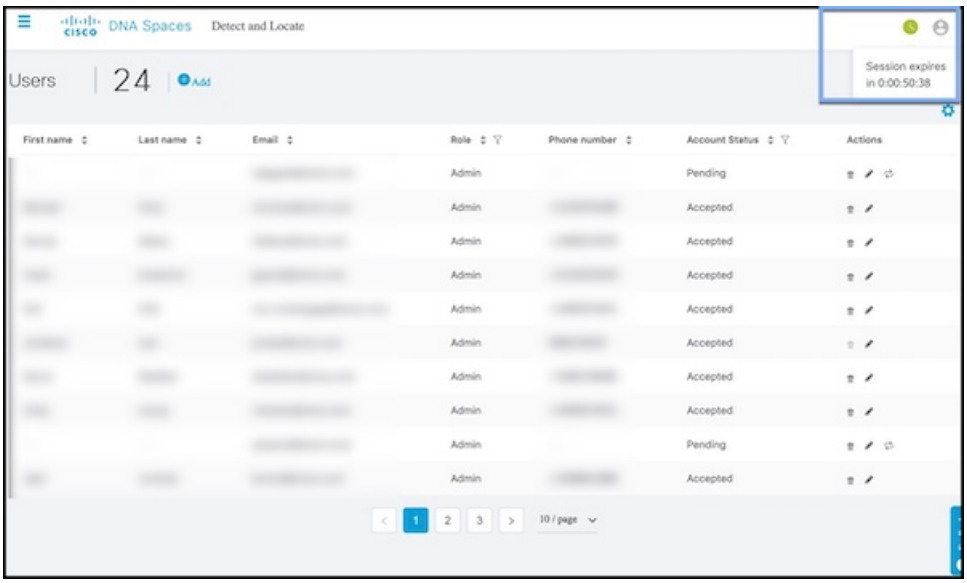
- セッションの有効期限 （45 ページ）

セッションの有効期限

セッションの有効期限の管理

検出と位置特定ダッシュボードの右上隅にある緑色のアイコンをクリックすると、セッションの有効期限の詳細が表示されます。

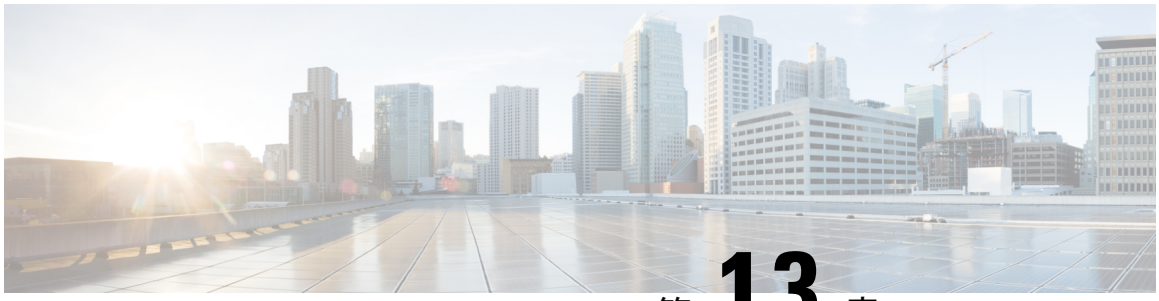
図 *21* : セッションの有効期限



第 IV 部

通知の管理

- ノースバウンド通知の使用 （49 ページ）



第 13 章

ノースバウンド通知の使用

- ノースバウンド通知の使用　（49 ページ）

ノースバウンド通知の使用

Cisco DNA Spaces：検出と検索 は、選択した通知エンドポイントに通知を送信するように設定できます。設定された通知は、**[NOTIFICATIONS]** メニューから確認できます。

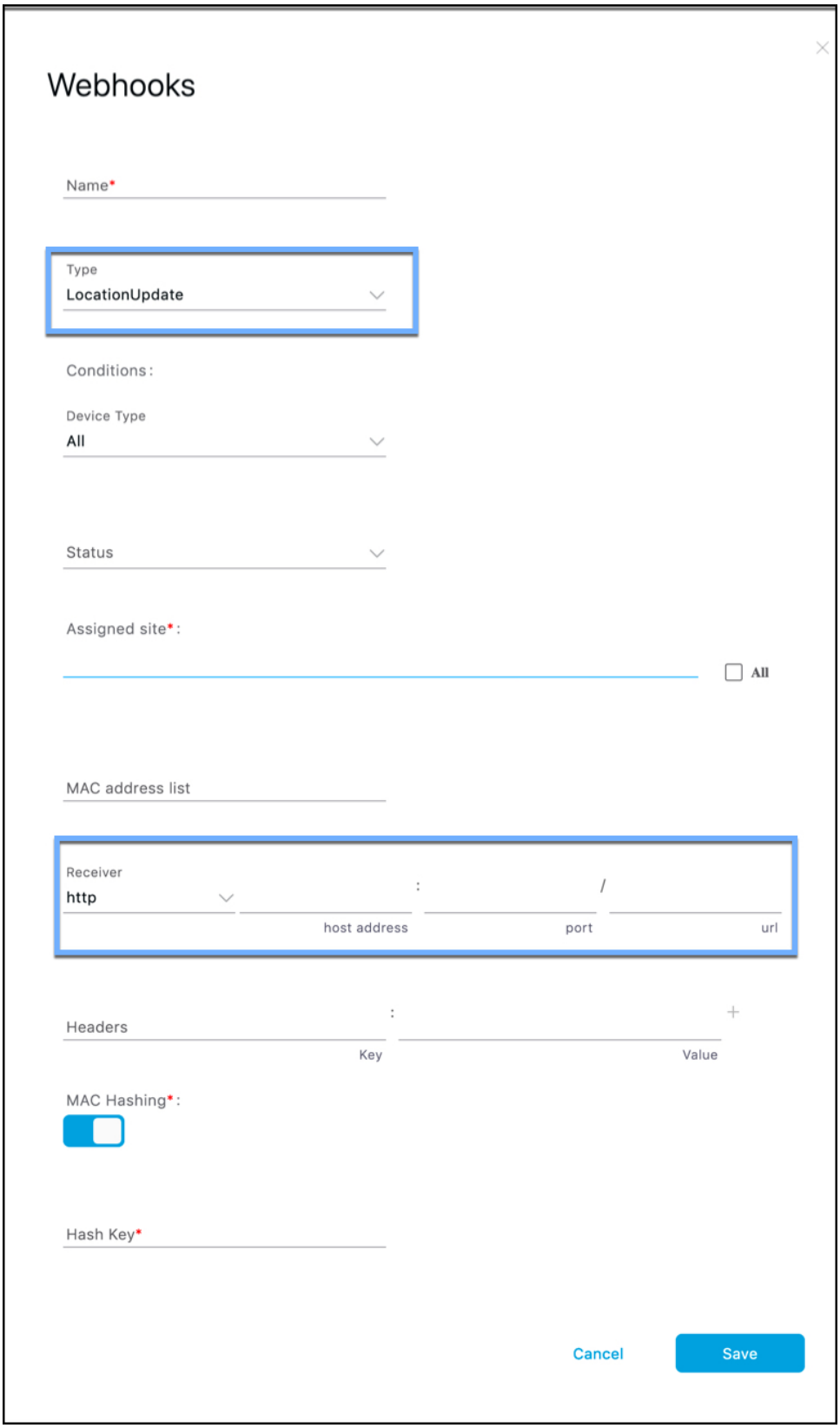
現在、次の通知タイプがサポートされています。

- **[Association]**：デバイスがネットワークに関連付けられたとき、またはネットワークから分離されたときに通知を生成します。
- **[Absence]**：15 分経過してもデバイスが検出されない場合に通知が生成されます。
- **[LocationUpdate]**: デバイスが位置（キャンパス、ビル、またはフロア間など）を変更した場合に生成されます。
- **[In/Out]**：デバイスが位置階層の特定のエリア内に移動するか、そのエリアから外へ移動していると検出された場合に、通知が生成されます。

Location Update（ノースバウンド通知）

このタイプの通知は、デバイスが位置（キャンパス、ビル、またはフロア間など）を変更した場合に生成されます。サポートされるデバイスタイプは、Rogue Client、Client、RFID Tag、Rogue AP、Interferer です。

図 *22 : [Location Update]*


Webhooks
Name*
Type
LocationUpdate
Conditions :
Device Type
All
Status
Assigned site* :
All
MAC address list
Receiver
http
:
/
host address
port
url
Headers
:
Key
Value
MAC Hashing* :
Hash Key*
Cancel
Save

[Location Update] ページに表示されるフィールドは次のとおりです。

- **[Status]**：デバイスがネットワークに関連付けられているかどうかに基づいて通知の生成を制限するように設定できます（プロービング）。デバイスのステータスが重要でない場合は、**[All]** を選択できます。
- **[Assigned Site]**：マップ階層をドリルダウンして、1 つ以上のエリア（フロア、キャンパス、ゾーン、ビル）にチェックを付けます。デバイスの位置が重要でない場合は、**[All]** チェックボックスをオンにします。
- **[MAC Address list]**：特定のデバイスの通知を生成する場合は、特定の MAC アドレスをここに入力します。
- **[Receiver]**：通知メッセージを送信する送信先を入力します。HTTP および HTTPS のみがサポートされています。ホスト名、ポート番号、および URL を入力します。
- **[Headers]**：これらのヘッダー内の通知とともに、追加情報（例：会社名などの会社固有の情報）を送信するように設定できます。複数のヘッダーを入力できます。
- **[MAC Hashing]**：MAC アドレスのハッシュを有効（または無効）にして、通知で送信される MAC アドレスを保護できます。これを行うには、ハッシュキーを入力する必要があります。

通知サブスクリプションのサンプル（JSON）

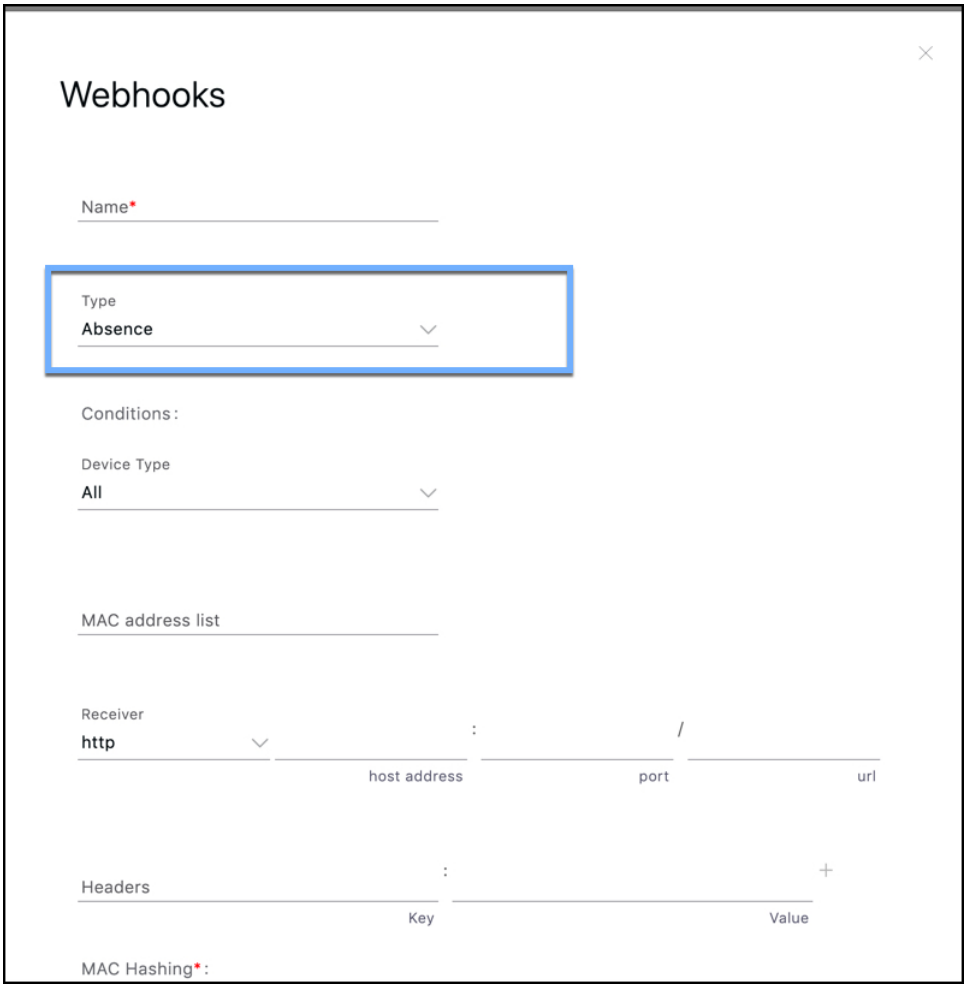
次に、Location Update 通知サブスクリプションのサンプルを示します。

```
{
    tenantId: '1001',
    id: "552a1a14-20cb-4581-855d-f3c9f120248e",
    name: "Test LocationUpdate Notification",
    type: "LocationUpdate",
    userid: "miczhao",
    enabled: true,
    internal: false,
    conditions: {
        deviceType: "Client",
        status: "Associated",
        hierarchy: {
            name: "System Campus -> SJC-24“,
            level: “CAMPUS”,
              campus: [“d12365e0ce514780aa2b5f01c7edaacd”],
              building: [“dbaf32ce320f4fe2a8935aebc387c8be”],
        }
        macAddressList: "11:22:33:44:55:66;11:22:33:44:55:67"
    },
    receiver: {
        url: "https://data.customer.com:443",
        messageFormat: "JSON",
        qos: "AT_MOST_ONCE",
        headers: {"Content-Type": "application/json", Accept: "application/json"}
    },
    enableMacScrambling: true,
    macScramblingSalt: "salt"
}
}
```

Absence（ノースバウンド通知）

このタイプの通知は、デバイスが 15 分以上検出されない場合に生成されます。サポートされているデバイスタイプは、**[Client]** と **[RFID Tag]** です。

図 *23 : Absence*



[Absence] ページのフィールドについて、次に説明します。

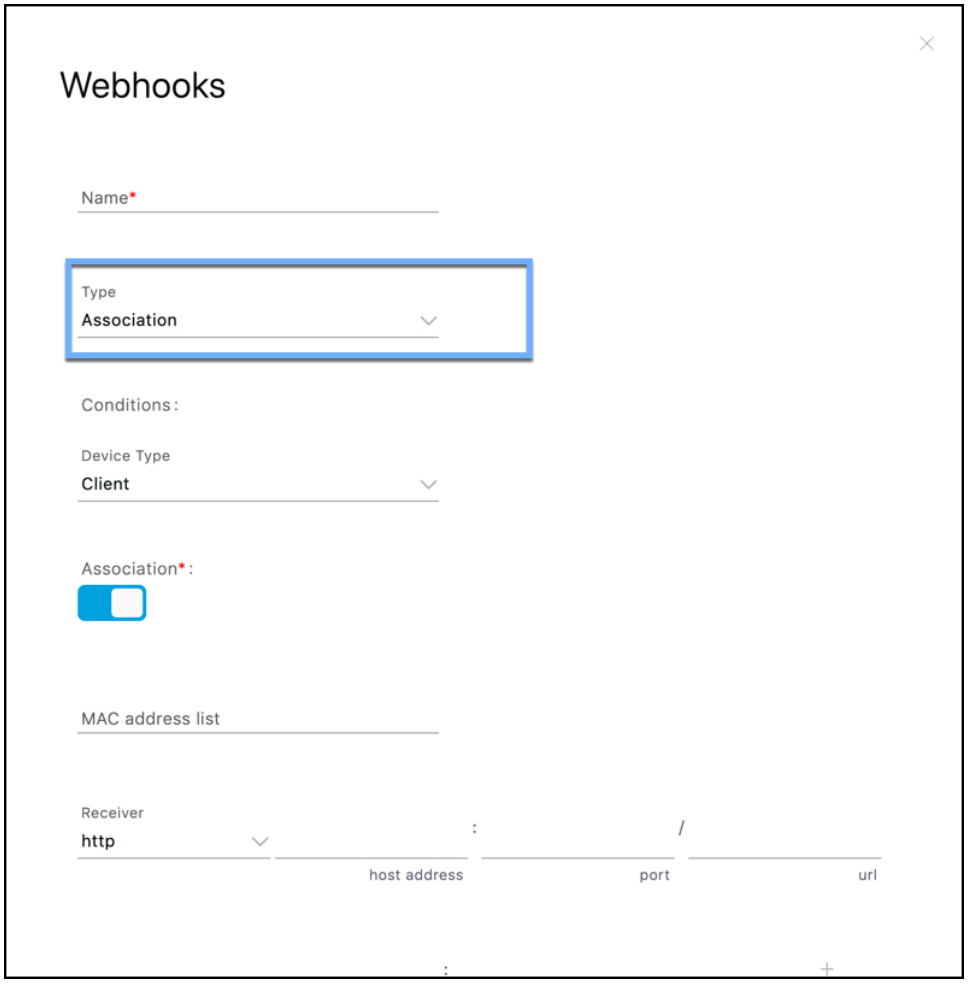
- **[MAC Address list]**：デバイス固有の通知の場合は、ここに特定の MAC アドレスを入力します。
- **[Receiver]**：通知メッセージの送信先を入力します。HTTP および HTTPS のみがサポートされています。ホストの IP アドレス、ポート番号、および URL を入力します。
- **[Headers]**：会社名などの会社固有の情報など、ヘッダーを追加できます。複数のヘッダーを追加できることに注意してください。

- **[MAC Hashing]**：MAC アドレスのハッシュを有効（または無効）にして、通知で送信される MAC アドレスを保護できます。これには、ハッシュキーを入力する必要があります。

Association（ノースバウンド通知）

このタイプの通知は、1 つ以上のデバイスがネットワークに関連付けられるか、ネットワークから関連付け解除されると生成されます。

図 *24 : Association*



- **[Association]**：デバイスがネットワークに関連付けられている場合に通知を生成するには、このボタンを有効にします。デバイスがネットワークから関連付け解除されたときに通知を生成するには、このボタンを無効にします。
- **[Status]**：デバイスがネットワークに関連付けられているかどうかに基づいて通知の生成を制限するように設定できます（プロービング）。デバイスのステータスが重要でない場合は、**[All]** を選択します。

- **[MAC Address list]**：特定のデバイスの通知を生成する場合は、特定の MAC アドレスをここに入力します。
- **[Receiver]**：通知メッセージを送信する送信先。HTTP および HTTPS のみがサポートされています。ホスト名、ポート番号、および URL を入力します。
- **[Headers]**：これらのヘッダー内の通知とともに、追加情報（例：会社名などの会社固有の情報）を送信するように設定できます。複数のヘッダーを追加できます。
- **[MAC Hashing]**：MAC アドレスのハッシュを有効（または無効）にして、通知で送信される MAC アドレスを保護できます。これには、ハッシュキーを入力する必要があります。

通知サブスクリプションのサンプル（JSON）

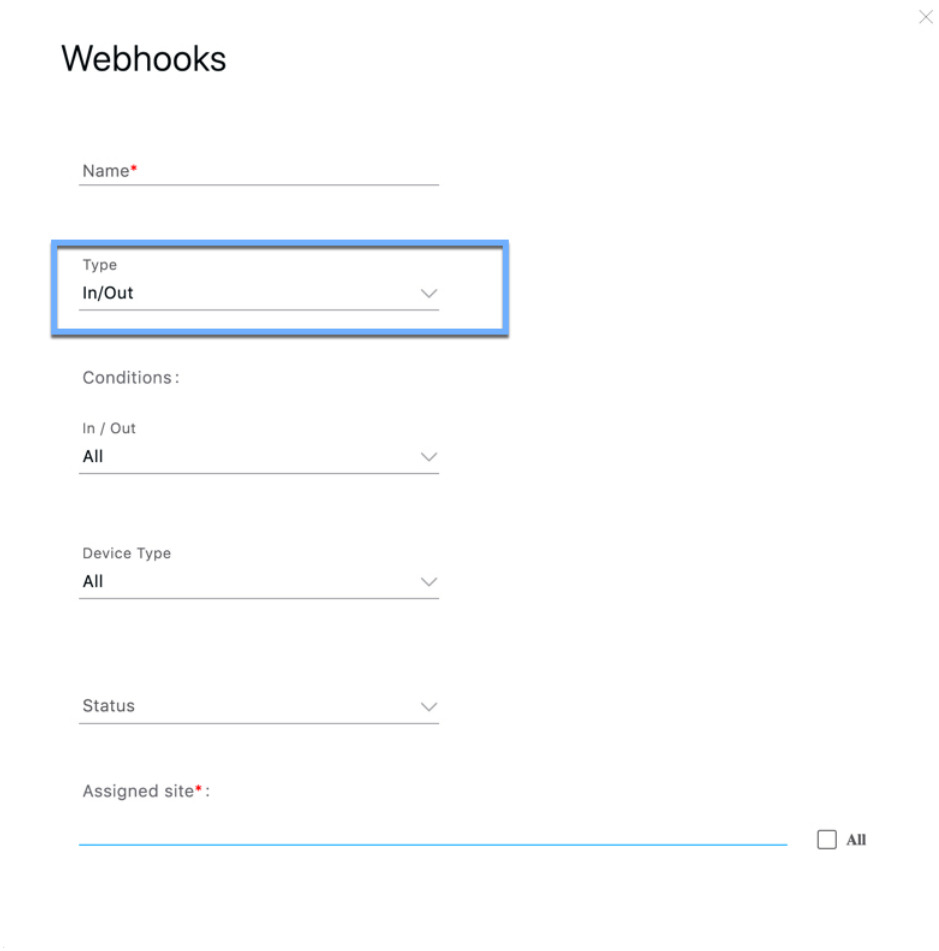
次に、Association 通知サブスクリプションの例を示します。

```
{
    tenantId: '2001',
    id: "552a1a14-20cb-4581-855d-f3c9f120248e",
    name: "Test Association Notification",
    type: “Association”,
    userid: “testuser”,
    enabled: true,
    intenal: false,
    conditions: {
        association: true,
        deviceType: “Client”,
        hierarchy: {
              name: “System Campus -> Building-24 -> 3rd Floor”,
              level: “FLOOR”,
              campus: [“d12365e0ce514780aa2b5f01c7edaacd”],
              building: [“dbaf32ce320f4fe2a8935aebc387c8be”],
              floor: [“2747871a29af4ab1989a4fb52b143552”]
        }
    },
    receiver: {
        url: "https://data.customer.com:443",
        messageFormat: "JSON",
        qos: "AT_MOST_ONCE",
        headers: {"Content-Type": "application/json", Accept: "application/json"}
    },
    enableMacScrambling: true,
    macScramblingSalt: "hashit"
}
```

In/Out（ノースバウンド通知）

このタイプの通知は、デバイスが位置階層の特定のエリア内に移動するか、そのエリアから外へ移動していると検出された場合に生成されます。

図 *25 : Absence*



[In/Out]：移動のタイプを選択します。

- デバイスが設定済みの **[Assigned Site]** に入ったときに通知を生成する場合は、**[In]** を設定します。
- デバイスが設定済みの**[Assigned Site]** を離れたときに通知を生成する場合は、**[Out]** を設定します。
- デバイスの **[Assigned Site]** への出入りが必要なく、 **[Assigned Site]** 内の単純な位置の変更で十分な場合は、**[No Change]** を設定します。
- **[In]** と **[Out]** の両方で通知を生成する場合は、**[All]** を設定します。
- **[Status]**：デバイスがネットワークに関連付けられているかどうか（プロービング）に基づいて通知の生成を制限するために設定します。デバイスのステータスが重要でない場合は、[All] を選択できます。

- **[Assigned Site]**：マップ階層をドリルダウンして、1 つ以上のエリア（フロア、キャンパス、ゾーン、ビル）を選択します。デバイスの位置が重要でない場合は、**[All]** チェックボックスをオンにします。このフィールドは必須です。
- **[MAC Address list]**：特定のデバイスの通知を生成する場合は、特定の MAC アドレスをここに入力します。
- **[Receiver]**：通知メッセージを送信する送信先。HTTP および HTTPS のみがサポートされています。ホスト名、ポート番号、および URL を入力します。
- **[Headers]**：これらのヘッダー内の通知とともに、追加情報（例：会社名などの会社固有の情報）を送信するために設定します。複数のヘッダーを追加できます。
- **[MAC Hashing]**：MAC アドレスのハッシュを有効（または無効）にして、通知で送信される MAC アドレスを保護できます。これには、ハッシュキーを入力する必要があります。

通知サブスクリプションのサンプル（JSON）

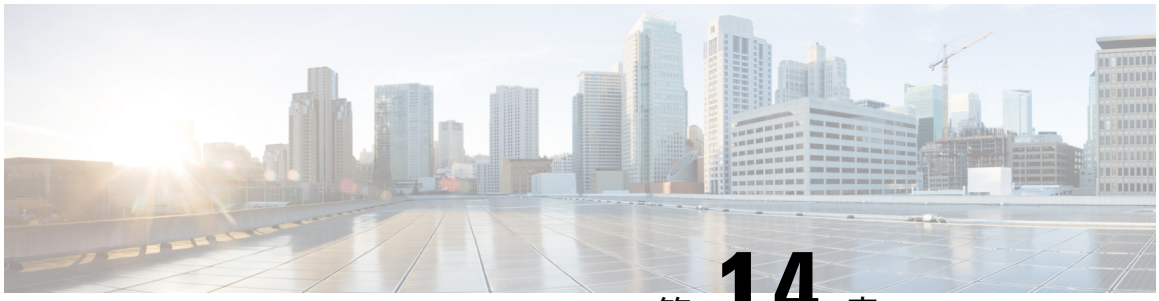
次に、In/Out 通知サブスクリプションのサンプルを示します。

```
{
    tenantId: '2001',
    id: "552a1a14-20cb-4581-855d-f3c9f120248e",
    name: "Test InOut Notification",
    type: “InOut”,
    userid: “testuser”,
    enabled: true,
    intenal: false,
    conditions: {
        inout: “All”,
        deviceType: “Client”,
        status: “Associated”,
        hierarchy: {
              name: “System Campus -> Building-24 -> 3rd Floor”,
              level: “FLOOR”,
              campus: [“d12365e0ce514780aa2b5f01c7edaacd”],
              building: [“dbaf32ce320f4fe2a8935aebc387c8be”],
              floor: [“2747871a29af4ab1989a4fb52b143552”]
        }
        macAddressList: "11:22:33:44:55:66;11:22:33:44:55:67"
    },
    receiver: {
        url: "https://data.customer.com:443",
        messageFormat: "JSON",
        qos: "AT_MOST_ONCE",
        headers: {"Content-Type": "application/json", Accept: "application/json"}
    },
    enableMacScrambling: true,
    macScramblingSalt: "hashit"
}
}
```

第 V 部

Hyperlocation と FastLocate

- Hyperlocation の設定 （61 ページ）
- Cisco FastLocate の設定 （65 ページ）



第 14 章

Hyperlocation の設定

• Cisco Hyperlocation の有効化 （61 ページ）

Cisco Hyperlocation の有効化

Cisco Hyperlocation ソリューションは、ソフトウェアおよびハードウェアのイノベーションの組み合わせによって高度なロケーション機能を実現するテクノロジースイートです。この Cisco Hyperlocation ソリューションにより、Cisco DNA Spaces に接続されたクライアントの位置精度が大幅に向上します。このソリューションは、Wi-Fi 信号の到達角度（AoA）を使用して、接続されたモバイルデバイスの位置を判定します。

Cisco Hyperlocation は、hyperlocation モジュールと hyperlocation アンテナを備えた次のアクセスポイントで使用できます。

- Cisco Aironet 3700 シリーズ アクセスポイント（HyperLocation アンテナが必要）
- Cisco Aironet 4800 シリーズ アクセス ポイント

Cisco Hyperlocation は、次のコンポーネントを使用して展開できます。

- 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
- Cisco DNA Spaces
- Cisco DNA Spaces：コネクタ

（注） Cisco CMX は Cisco Hyperlocation に必要ありません。

Cisco DNA Spaces は、高度なロケーションアルゴリズムを使用して、ワイヤレスクライアントから収集した位置情報から位相差を抽出します。これにより、Cisco DNA Spaces は最適な展開において、関連付けられたワイヤレスクライアントを最大 1 メートルの精度（50% のエラー距離）で特定できます。

位置の精度が向上すると、RSSI ベースの位置と比較して、より詳細な分析データが提供されます。

Cisco Hyperlocation は、次のコントローラで使用できます。

- シスコ ワイヤレス コントローラ でサポート
- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ でサポート

Cisco Hyperlocation の設定方法

このタスクでは、ネットワークで Cisco Hyperlocation を有効にする方法について説明します。このタスクでは、Cisco DNA Spaces がクライアントデバイスから Hyperlocation パケットを受信しているかどうかを確認する方法も示します。

[Packet rate frequency]：すべてのアクティブデバイスおよび関連付けられたデバイスから、Cisco DNA Spaces は 10 秒ごとにパケットを受信します。標準 RSSI の場合、パケットの頻度はデバイスのプロービングによって異なります。ただし、Wi-Fi プローブパケットの一般的な頻度は 30 秒から 1 分です。

始める前に

- ご使用の コントローラ のバージョンがネットワークの Cisco Hyperlocation のアクセスポイントと互換性があることを確認します。
- Cisco DNA Spaces が コントローラ のバージョンをサポートしていることを確認します。「互換性マトリクス」のセクションを参照してください。
- Cisco CMX と Cisco DNA Spaces のアカウントの両方が同じ コントローラ に接続されている場合は、Cisco CMX 上の Cisco Hyperlocation を必ず無効にします。

ステップ 1 コントローラ の Hyperlocation を有効にします。

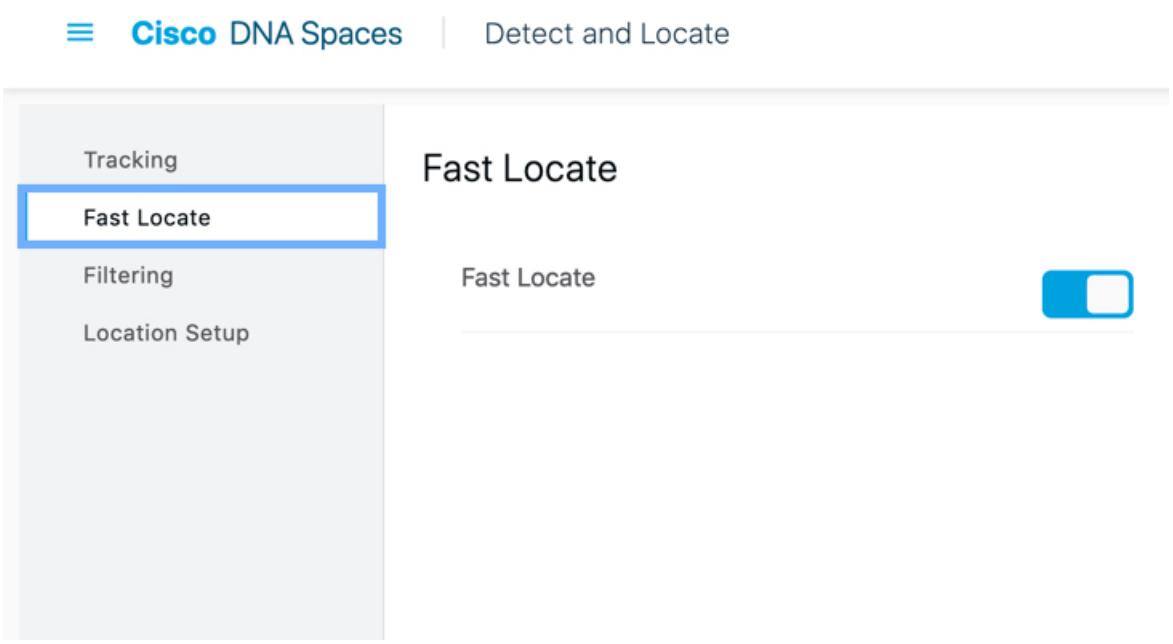
手順については、インストールされているバージョンのそれぞれの設定ガイドを参照してください。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ については、『**Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide**』を参照してください。

ステップ 2 Cisco DNA Spaces：検出と検索 の Hyperlocation を有効にします。

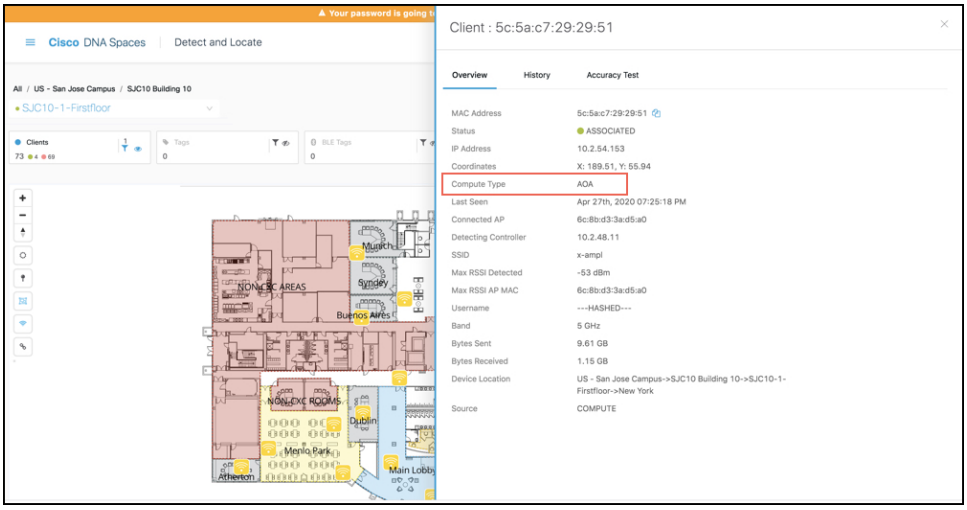
Cisco DNA Spaces：検出と検索 ダッシュボードに移動します。左側のナビゲーションペインで **[Configure]** をクリックし、**[Fast Locate]** オプションを有効にします。

図 *26 : Cisco DNA Spaces*：検出と検索 の *Hyperlocation* の有効化



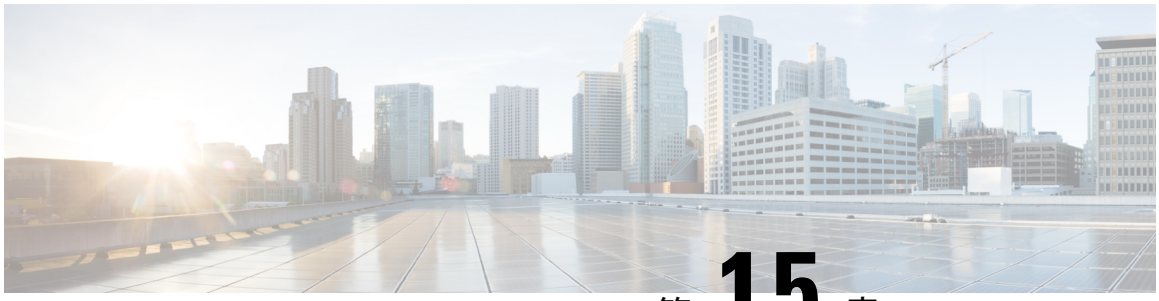
ステップ 3 Cisco DNA Spaces：検出と検索 がクライアントデバイスから到達角度（AoA）パケットを受信しているかどうかを確認します。

Cisco DNA Spaces：検出と検索 ダッシュボードに移動し、クライアントデバイスの **[Compute Type]** が「AoA」または「Fusion」かどうかを確認します。



- [Angle of Arrival (AoA)]：AoA は AoA フェーズ測定を使用して、デバイスの位置を三角測量します。デバイスの周囲にあるいくつかの hyperlocation AP が、これらの AoA フェーズ測定値を報告します。AoA コンピューティングタイプは、デバイスがこれらの hyperlocation AP の凸包内にある場合にのみ、デバイスのより正確な位置に到達できます。

- [Fusion]：Fusion は、RSSI 位置計算とAoA 位置計算の結果を結合します。これらの計算は、デバイスの最も可能性の高い位置を推定します。**[Compute Type]** フィールドは、デバイスは Hyperlocation AP の凸包内にないことをロケーションエンジンが検出して結論付けた場合には「Fusion」です。



第 15 章

Cisco FastLocate の設定

• Cisco FastLocate の設定 （65 ページ）

Cisco FastLocate の設定

Cisco FastLocate テクノロジーは接続されたワイヤレスクライアントのロケーション更新レートを向上させ、これにより Cisco DNA Spaces がより多くのロケーションデータポイントをキャプチャできます。

可能な場合、デバイスの位置計算にデータパケットとプローブフレームからの RSSI が使用されます。RSSI 展開の良好なロケーション精度テストの結果は 10 メートルです。Cisco FastLocate によりこの結果の精度が改善することはありません。ただし、アクティブデバイスの更新頻度が 30 秒に 1 回以上の場合、結果は 10 メートル未満の値に改善されます。

Cisco FastLocate テクノロジーは、中央でスイッチされる WLAN と FlexConnect（ローカルでスイッチされる WLAN）の両方で使用できます。

次の コントローラ が Cisco FastLocate をサポートしています。

- シスコ ワイヤレス コントローラ リリース 8.1.123.0 でサポート
- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のすべてのリリースでサポート

次の Wi-Fi 6 のアクセスポイントが Cisco FastLocate をサポートしています。

- Cisco Aironet 9120 シリーズ アクセスポイント
- Cisco Aironet 9130 シリーズ アクセスポイント

次のアクセスポイントが Cisco FastLocate をサポートしています。

- Cisco Aironet 2800 シリーズ アクセス ポイント
- Cisco Aironet 3800 シリーズ アクセス ポイント
- Cisco Aironet 4800 シリーズ アクセス ポイント

Cisco FastLocate の設定方法

このタスクでは、ネットワークで Cisco FastLocate を有効にする方法を示します。また、Cisco DNA Spaces がクライアントデバイスから Cisco FastLocate パケットを受信しているかどうかを確認する方法も示します。

[Packet rate frequency]：すべてのアクティブデバイスおよび関連付けられたデバイスから、Cisco DNA Spaces は 10 秒ごとにパケットを受信します。標準 RSSI の場合、パケットの頻度はデバイスのプロービングによって異なります。ただし、Wi-Fi プローブパケットの一般的な頻度は 30 秒から 1 分です。

始める前に

- Cisco FastLocate のサポートされているアクセスポイントが、コントローラ のインストール済みバージョンと互換性があることを確認します。コントローラ のバージョンが Cisco DNA Spaces と互換性があるかどうかを確認するには、互換性マトリクスを参照してください。
- Cisco CMX と Cisco DNA Spaces の両方のアカウントが同じ コントローラ に接続されている場合は、Cisco CMX の Hyperlocation を無効にして、Cisco FastLocate ストリームを Cisco DNA Spaces で使用できるようにします。

ステップ 1 コントローラ の Hyperlocation を有効にします。

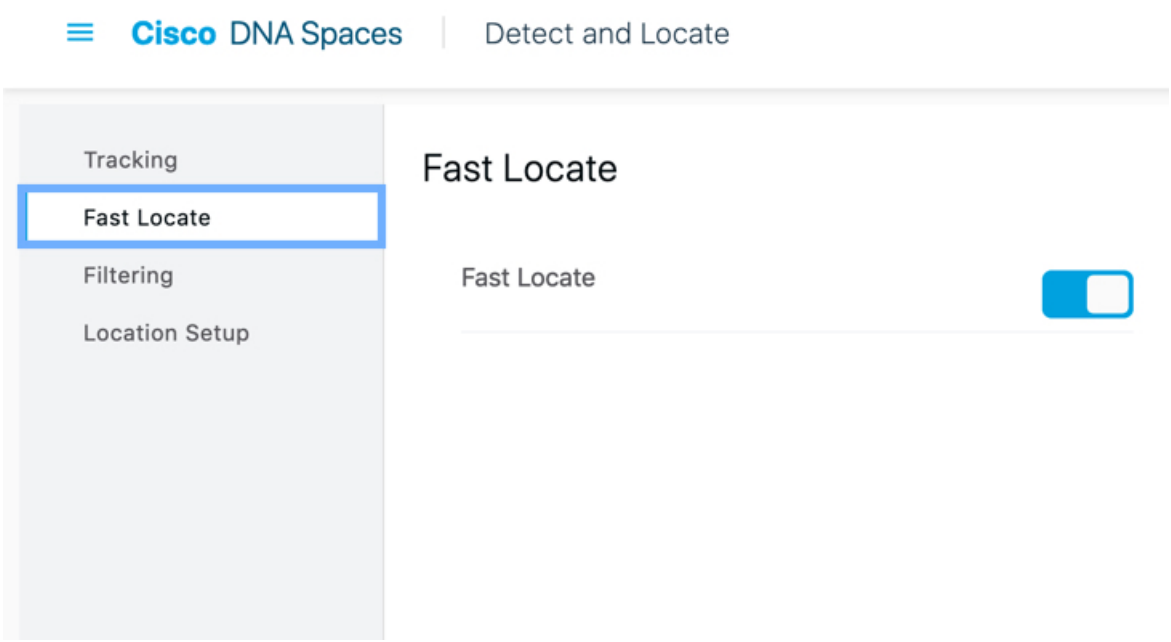
手順については、インストールされているバージョンのそれぞれの設定ガイドを参照してください。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ については、『**Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide**』を参照してください。

ステップ 2 Cisco DNA Spaces：検出と検索 上で Cisco FastLocate を有効にします。

Cisco DNA Spaces：検出と検索 ダッシュボードに移動し、左側のナビゲーションペインで **[Configure]** をクリックし、**[Fast Locate]** を有効にします。

図 *27 : Cisco DNA Spaces*：検出と検索 で *Cisco FastLocate* を有効にする

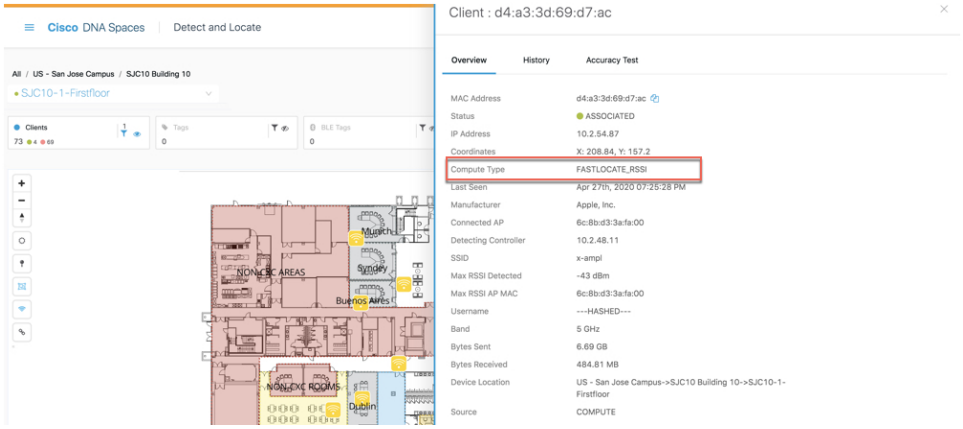


ステップ 3 Cisco DNA Spaces：検出と検索 がクライアントデバイスから Cisco FastLocate RSSI パケットを受信しているかどうかを確認します。

Cisco DNA Spaces：検出と検索 ダッシュボードに移動し、クライアントデバイスの **Compute_Type** が「Fastlocate_RSSI」かどうかを確認します。

（注） Cisco FastLocate を有効にした後でも、次の場合に、クライアントデバイスで RSSI の **Compute_Type** が引き続き表示されることがあります。

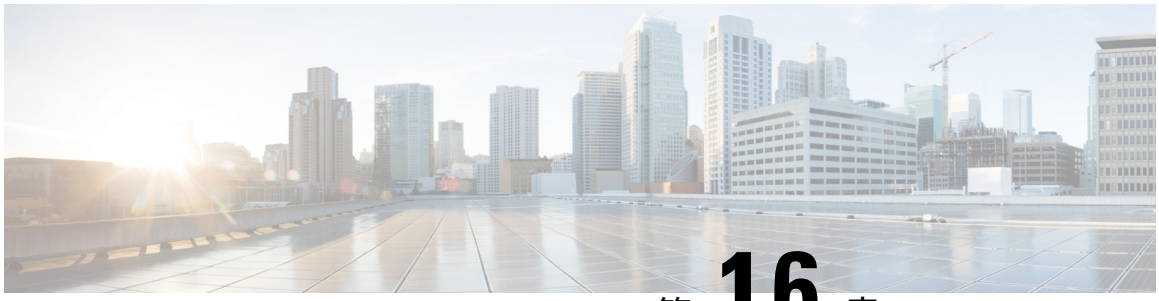
- クライアントデバイスがアクティブでない場合。
- たとえば、クライアントデバイスのタイプによって、iPad や特定の携帯電話でこれが確認できる場合があります。


Cisco DNA Spaces
Detect and Locate
All / US - San Jose Campus / SJC10 Building 10
SJC10-1-Firstfloor
Clients
73
Tags
0
BLE Tags
0
NON-EC AREAS
Munich
Sydney
Buenos Aires
NON-EXC ROOMS
Dublin
Client : d4:a3:3d:69:d7:ac
Overview
History
Accuracy Test
MAC Address
d4:a3:3d:69:d7:ac
Status
ASSOCIATED
IP Address
10.2.54.87
Coordinates
X: 208.84, Y: 157.2
Compute Type
FASTLOCATE_RSSI
Last Seen
Apr 27th, 2020 07:25:28 PM
Manufacturer
Apple, Inc.
Connected AP
6c:8b:d3:3a:fa:00
Detecting Controller
10.2.48.11
SSID
x-ampl
Max RSSI Detected
-43 dBm
Max RSSI AP MAC
6c:8b:d3:3a:fa:00
Username
---HASHED---
Band
5 GHz
Bytes Sent
6.69 GB
Bytes Received
484.81 MB
Device Location
US - San Jose Campus->SJC10 Building 10->SJC10-1-Firstfloor
Source
COMPUTE

第 VI 部

ユーザの管理

- ユーザの管理 （71 ページ）



第 16 章

ユーザの管理

• ユーザの管理 （71 ページ）

ユーザの管理

ユーザーロールの設定とユーザーの招待

Cisco DNA Spaces：検出と検索 ユーザーにはロールベース アクセスコントロール（RBAC）が提供され、ユーザーまたはユーザーグループにはさまざまなユーザーロールが提供されます。ユーザーロールは、各ロールに関連付けられた権限によって区別され、制限されます。使用可能な権限は、**AdminAccess**、**ReadOnlyAccess**、および **SiteAdminAccess** です。これらは、関連付けられたユーザーがアクセスできるロケーションとサイトを定義します。ユーザーの Cisco DNA Spaces：検出と検索 ダッシュボードには、ユーザーロールで定義されたロケーションのみが表示されます。

表 *2:* 権限とその内容

権限	内容
AdminAccess	システム全体に対する読み取り、書き込みアクセス。
ReadOnlyAccess	読み取り専用アクセス。
SiteAdminAccess	サイトレベルでの読み取り、書き込みアクセス。

始める前に

マップがアップロードされていることを確認します。

ステップ 1 左側のナビゲーションペインで、**[Admin]**、**[User Roles]** を選択し、**[Add]** を選択します。

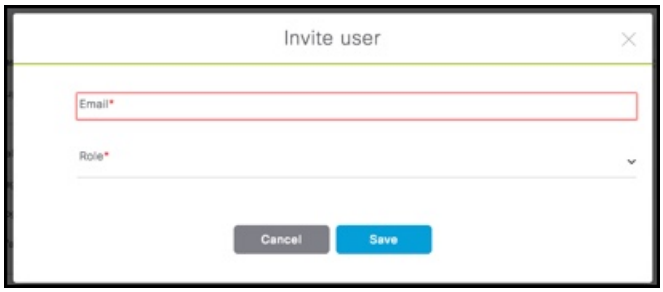
ステップ 2 **[Role]** ダイアログボックスで、次の手順を実行します。

a) [Name]：ユーザーロールの名前を入力します。

b) [Permissions]：ドロップダウンリストから権限を選択します。

c) ドロップダウンリストから **[Sites]** を選択します。

ステップ 3 電子メール ID を入力し、ステップ 2 で設定した **[Role]** を選択して、ユーザーを招待します。



ユーザーとユーザー ロールの変更

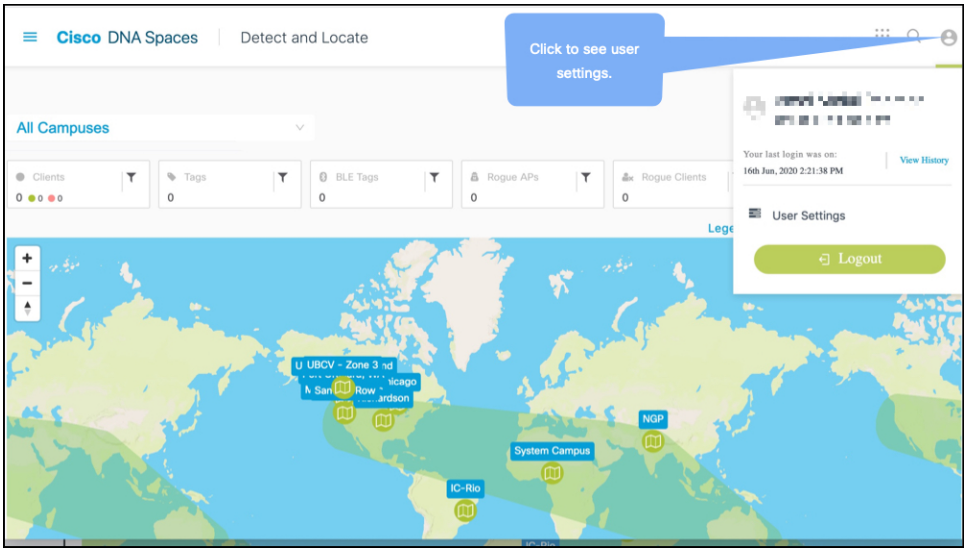
管理者はユーザーの個人情報を変更できません。ユーザーはまた、**[User Management]** タブから自身の個人情報を変更できません。

検出と位置特定 管理者はユーザーロールのみ変更できます。検出と位置特定 管理者は、**[User Management]>[App Users]** からユーザーの詳細を編集することで、特定のユーザーのロールを編集できます。

[User Management]>[Administrators] に表示されるユーザーは、Cisco DNA Spaces ダッシュボードで定義された管理者です。このタイプのユーザーは検出と位置特定からは編集できず、Cisco DNA Spaces ダッシュボードからのみ編集できます。

ステップ 1 ユーザーの詳細を変更するには、ユーザーは検出と位置特定ダッシュボードでそれぞれのアカウントにログインし、**[Admin]**、そして **[User Settings]** に移動する必要があります。

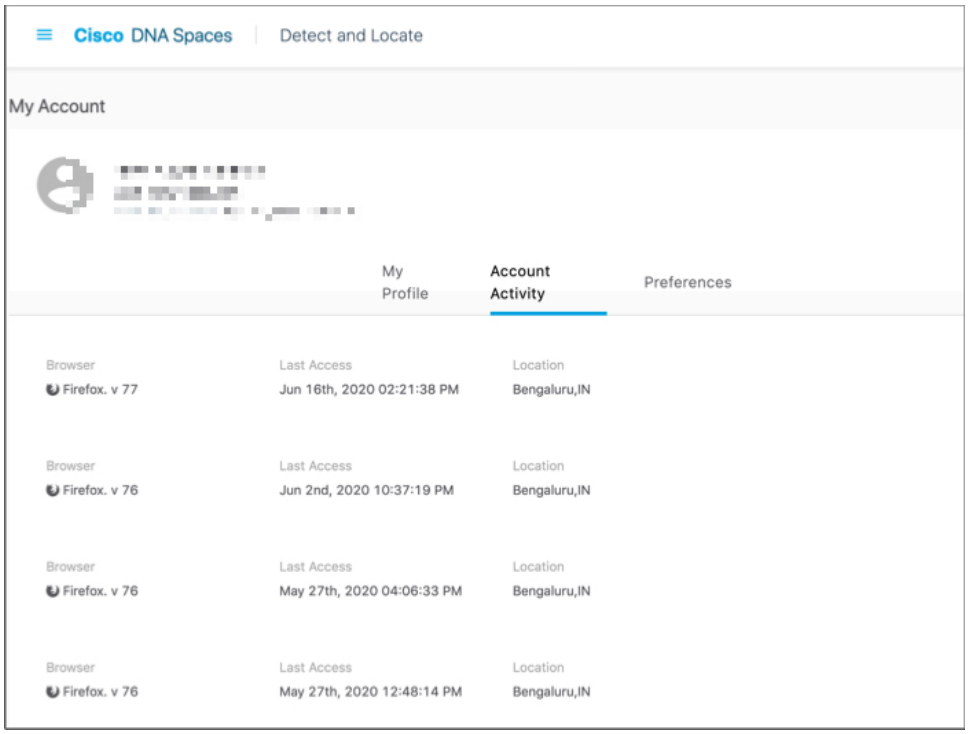
図 *28 :* ユーザー設定から個人情報を変更する



ステップ 2 **[Preferences]** タブでは、次の項目を設定できます。

- [Map auto refresh (in seconds)]：資産の動きを反映して、ロケーションリストとマップが自動的に更新される頻度を選択します。
- [Client display icon]：検出と位置特定 ダッシュボードでのクライアントの表示方法を指定します。

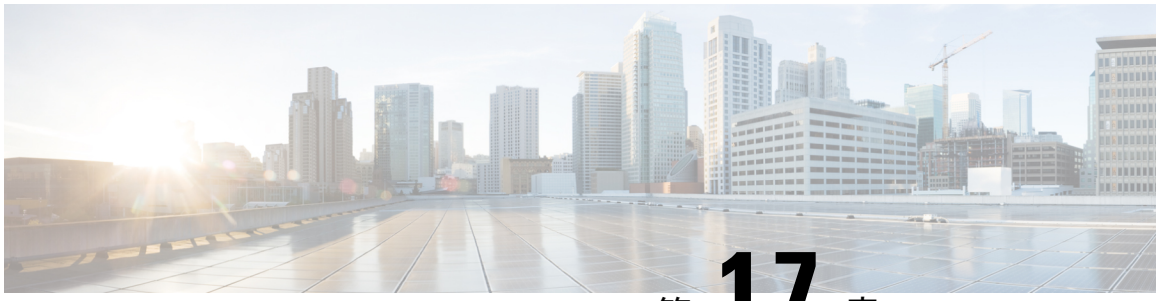
ステップ 3 **[Activity]** タブから、使用されているブラウザ、アクセス時間、位置など、ダッシュボードのアクセスアクティビティを確認できます。


Cisco DNA Spaces
Detect and Locate
My Account
My Profile
Account Activity
Preferences
Browser
Firefox. v 77
Last Access
Jun 16th, 2020 02:21:38 PM
Location
Bengaluru,IN
Browser
Firefox. v 76
Last Access
Jun 2nd, 2020 10:37:19 PM
Location
Bengaluru,IN
Browser
Firefox. v 76
Last Access
May 27th, 2020 04:06:33 PM
Location
Bengaluru,IN
Browser
Firefox. v 76
Last Access
May 27th, 2020 12:48:14 PM
Location
Bengaluru,IN

第 VII 部

よくある質問

• FAQ の管理 （77 ページ）



第 17 章

FAQ の管理

- サポートを受けるには （77 ページ）
- Cisco DNA Spaces：検出と検索 アカウントに保存される情報とその保存期間は？ （77 ページ）

サポートを受けるには

Cisco DNA Spaces：検出と検索 アカウントに関連する問題についてサポートを受けるには、cisco-dnaspaces-support@external.cisco.com にメールを送信します。

Cisco DNA Spaces：検出と検索 アカウントに保存される情報とその保存期間は？

Cisco DNA Spaces：検出と検索 アカウントには次の情報が保存されます。

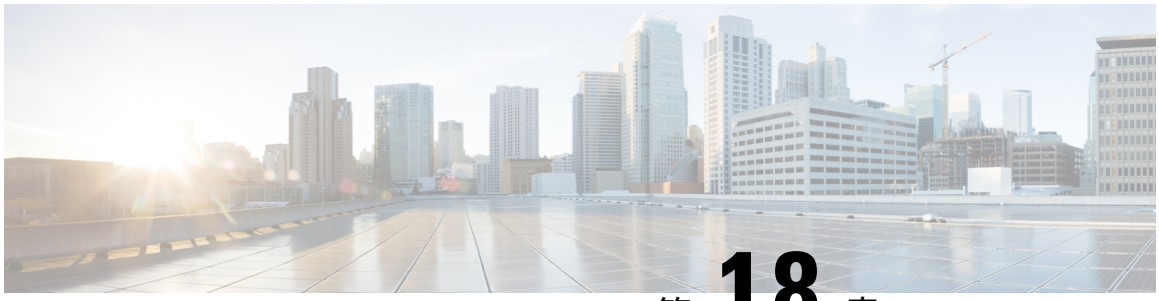
- クライアントの位置
- マップ

この情報は、Cisco DNA Spaces：検出と検索 アカウントが削除されるまで保持されます。

第 VIII 部

API

• API （81 ページ）



第 18 章

API

• Rest API の使用　（81 ページ）

Rest API の使用

REST API を使用して、Cisco DNA Spaces：検出と検索 の情報を取得、追加、または変更できます。REST API は次の 5 つのカテゴリーに分類されます。

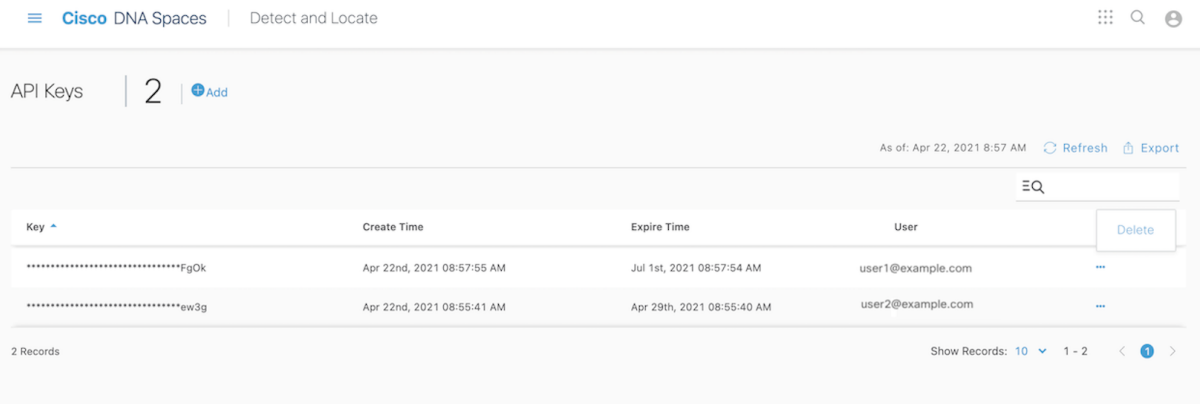
- **アクティブクライアントの位置用 API**：クライアントの数と位置データを取得するための API。
- **クライアントの位置履歴用 API**：特定のデバイスの MAC アドレスと詳細を取得する API。
- **通知用 API**：サブスクリプションベースの通知用の API。
- **マップ用 API**：マップ階層をアップロード、移動、マップ要素を取得、削除するための API。
- **アクセスポイント用 API**：アクセスポイントの詳細を取得するための API。

API Key

REST API を使用するには、API キーを生成する必要があります。API キーはシスコ独自の JSON Web トークン（JWT）で、ユーザーを認証および承認するために、各 HTTP リクエストヘッダーで必要です。

Cisco DNA Spaces：検出と検索 から API キーを生成できます。**[Notifications]** > **[API Keys]**に移動し、**[Add]** をクリックします。キーが期限切れになるまでの日数を設定するよう求められます。有効な範囲は 7 日ー 365 日です。キーが生成されたら、キーを安全に保存します。

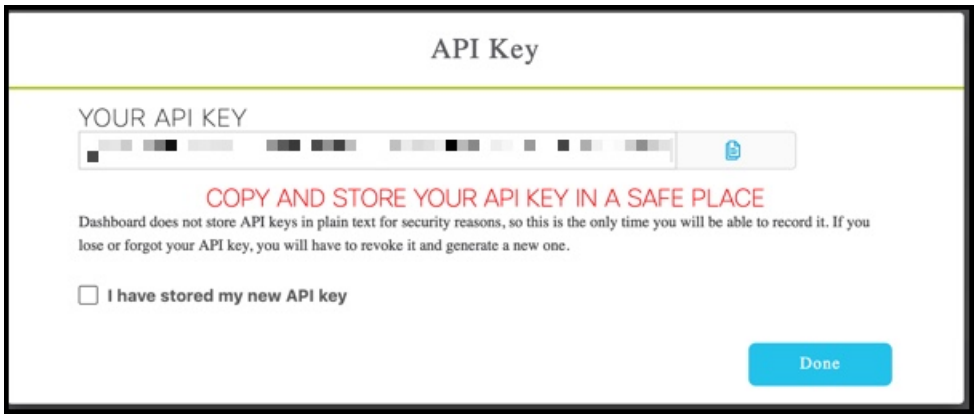
図 *29 : API* キー



[API Keys] ウィンドウには、キー名（一部のみ表示）、キーが作成された日時、キーが期限切れになる日時、およびキーを作成したユーザーの電子メール ID が表示されます。キーを削除するには、**[Actions]** カラムの 3 つの点のアイコンをクリックし、**[Delete]** をクリックします。キーを削除しても、キーは失効せず、有効期限が切れるまで使用できます。

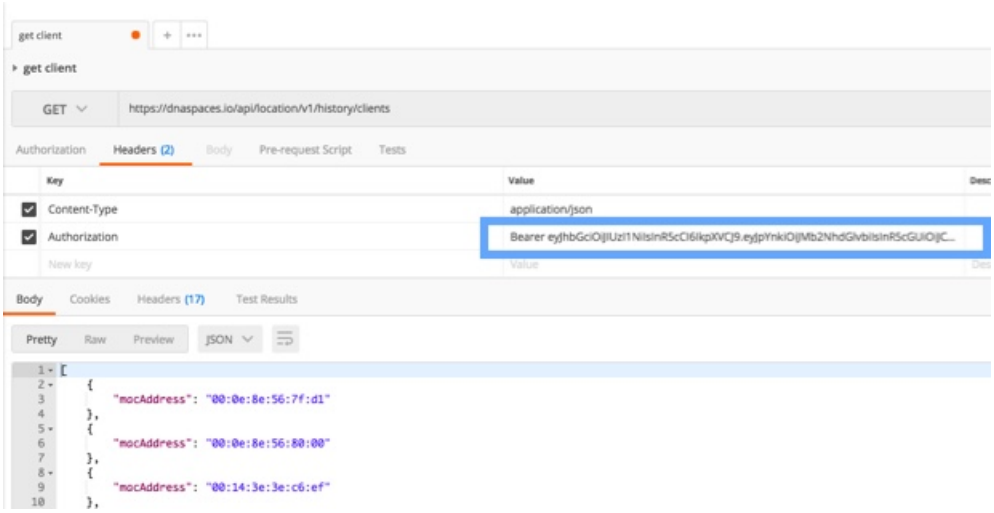
（注） API キーは作成時にのみ表示されるため、安全に保存する必要があります。Cisco DNA Spaces：検出と検索 は API キーの値を保存しません。認証済みユーザはそれぞれ、最大 5 つのキーを持つことができます。

図 *30 : API* キーのコピー



次に示すのは、**認証ヘッダー**として API キーが使用されている POSTMAN クライアントの例です。

図 *31 : API* キー


get client
get client
GET
https://dnaspaces.io/api/location/v1/history/clients
Authorization
Headers (2)
Body
Pre-request Script
Tests
Key
Value
Content-Type
application/json
Authorization
Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpYnkiOiJlMb2NhdGlvbiIsInR5cGUiOiJlC...
New key
Value
Body
Cookies
Headers (17)
Test Results
Pretty
Raw
Preview
JSON
[
{
"macAddress": "00:0e:8e:56:7f:d1"
},
{
"macAddress": "00:0e:8e:56:80:00"
},
{
"macAddress": "00:14:3e:3e:c6:ef"
},

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。