付録

- 付録 （1 ページ）

付録

ワイヤレスコントローラ での Cisco CMX の設定

手順

ステップ 1 Cisco CMX ナビゲーションウィンドウから、[System] > [Settings] > [Controllers and Maps Setup] > [Advanced] を選択します。

ステップ 2 [Controllers] セクションで、ドロップダウンから [IP address] を選択し、ワイヤレスコントローラ の IP アドレスを入力します。[Controller SNMP Write Community] で、バージョンを選択して [Save] をクリックします。

ステップ 3 Cisco CMX ダッシュボードのメインエリアから、[Controller] エリアに移動し、ワイヤレスコントローラ の IP アドレスが緑色であることを確認します。これは ワイヤレスコントローラ と Cisco CMX 間の接続が成功したことを示します。

Controllers

IP Address	Version	Bytes In	Bytes Out	First Heard	Last Heard	Action
5.5.5.5	0.0.0.0	0	0	Never	Never	Edit Delete
10.32.168.50	8.2.145.58	261 MB	15 KB	02/20/17, 11:36 am	Just now	Edit Delete
172.19.30.203	8.2.121.0	15 KB	15 KB	02/20/17, 11:36 am	10s ago	Edit Delete
10.32.168.38	8.3.104.142	11 MB	15 KB	02/20/17, 11:36 am	Just now	Edit Delete
172.19.30.222	8.3.15.174	0	0	Never	Never	Edit Delete

（注）

ワイヤレスコントローラ の IP アドレスが緑色でない場合は、次のタスクの手順を参照してください。

ワイヤレスコントローラ でハッシュキーを設定

ワイヤレスコントローラ の IP アドレスのステータスが赤色の場合、ワイヤレスコントローラが読み取りコミュニティ文字列を使用して Cisco CMX に追加されている可能性があります。次のトラブルシューティング タスクを実行します。

手順

ステップ 1 Cisco CMX CLI から **cmxctl config controllers show** コマンドを実行し、SHA2 キーの値をコピーします。

```
[CMXadmin@CMX-jkp103 configuration]$ cmxctl config controllers show
+-------------+------------------------------------------------------------------+
| MAC Address | 00:50:56:ac:99:6e                                                |
+-------------+------------------------------------------------------------------+
| SHA1 Key    | d116d605fd88e72763a03871bc483786e463ae43                         |
+-------------+------------------------------------------------------------------+
| SHA2 Key    | 66a03889d03cbee5c10e35e641f0ea91109f32832017db60fb3a4cdaf3bf0a7e |
+-------------+------------------------------------------------------------------+
```

ステップ 2 ワイヤレスコントローラ CLI から、手順 1 の SHA2 文字列を使用して、**config auth-list add sha256-lbs-ssc** <*CMX-mac*> <*sha2KeyHashString*> コマンドを発行します。

ステップ 3 ワイヤレスコントローラ CLI で、**show auth-list** コマンドを実行します。

```
(Cisco Controller) >show auth-list

Authorize MIC APs against Auth-list or AAA ..... disabled
Authorize LSC APs against Auth-List ..... disabled
APs Allowed to Join
  AP with Manufacturing Installed Certificate.... yes
  AP with Self-Signed Certificate..... yes
  AP with Locally Significant Certificate..... yes

Mac Addr                  Cert Type    Key Hash
------------------------  ----------   ----------------------------------------
00:0c:29:dc:7b:b6         LBS-SSC-SHA256      77f9d7f3181be12080363a7a5584b0e4ebcf2cc6ddad1a24038213cd60faabbe
00:0c:29:e0:d1:82         LBS-SSC-SHA256      95386767056f5793b614ccd3f7dffc034b942e18b5288cb178f7587c077e9d42
00:50:56:8b:c7:da         LBS-SSC-SHA256      b25f3a38e908759a246818f078c582b8c85d0a32211f043e853374aa282ffad2
00:50:56:a3:25:ac         LBS-SSC-SHA256      eebf2eeb669751c50565380d778f6d2ac4e3beca60c0c2fb428e93f1b47e5838
00:50:56:ac:95:4d         LBS-SSC-SHA256      5081c89bc15fb0a1ddd3811454bb86048402af134b4e85f6128e8f2c4f63e795
00:50:56:ac:99:6e         LBS-SSC-SHA256      66a03889d03cbee5c10e35e641f0ea91109f32832017db60fb3a4cdaf3bf0a7e
34:40:b5:a2:a4:90         LBS-SSC-SHA256      57d59c436fb3da1e272631316eaeb4bce3512734f494ddd28012156be97b01ba
```

Cisco CMX 10.4 以降でのプロキシの設定

このタスクでは、Cisco CMX（10.4 以降）にプロキシゲートウェイを設定して、プライベートネットワークにインストールされている Cisco CMX サーバーと外部クラウドセットアップ間の通信を許可する方法を示します。

手順

ステップ 1 **cmxos sysproxy proxy http://** <*proxy-gateway-address*> <*port*>

このコマンドは、内部 Cisco CMX と外部 資産ロケータ サーバーとの通信を許可するプロキシゲートウェイを設定します。

ステップ 2 **cmxos sysproxy no_proxy localhost** <*website-address*>

このコマンドは、ネットワーク内の IP アドレスに対してプロキシが使用されないようにします。

ステップ 3 **cmxos sysproxy {enable | clear | disable}**

このコマンドは、プロキシを有効にします。

ステップ 4 **cmxctl stop -a**

ステップ 5 **cmxcl agent start**

ステップ 6 **cmxctl start**

ステップ 7 Cisco CMX を再起動して、実際の変更点を確認します。

Cisco PI から Cisco CMX へのマップのインポート

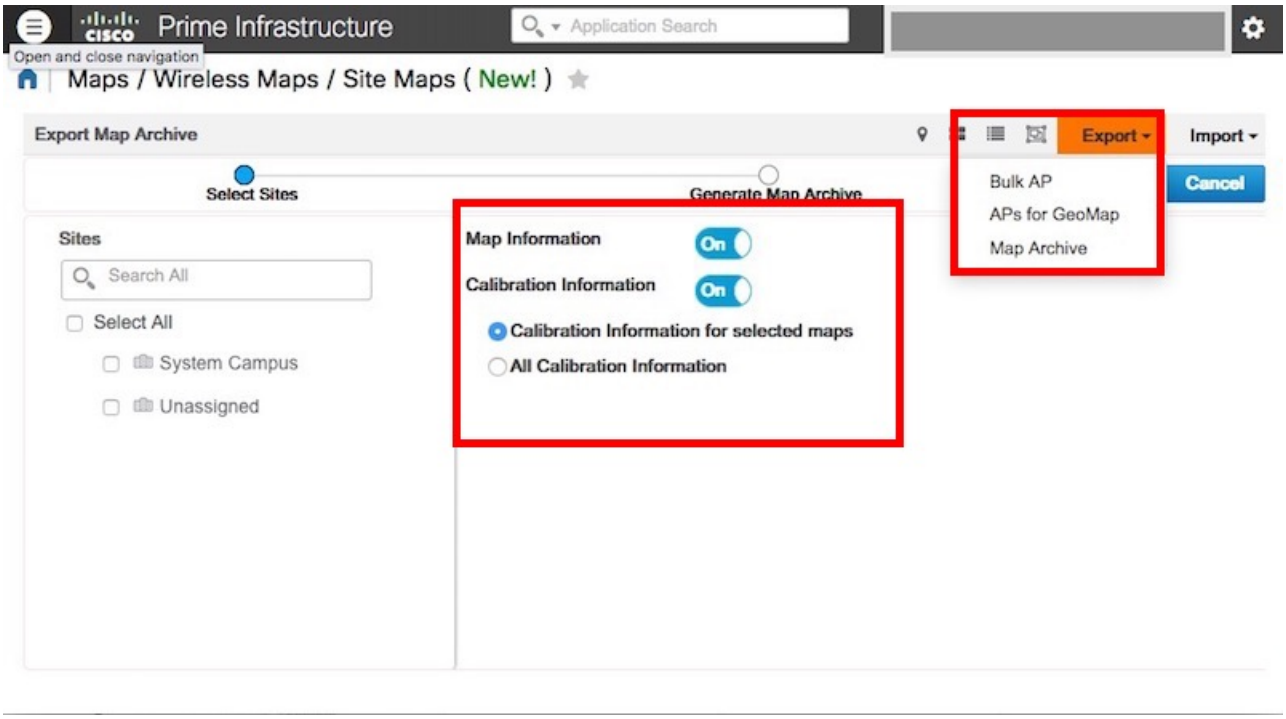
手順

ステップ 1 URL *https://<PrimeInfrastructure_IP_address>* を使用して Cisco PI にログインします。

a) [Maps] > [Wireless Maps] > [Site Maps] を選択します。

b) 右側のナビゲーションウィンドウから、[Export] > [Map Archive] を選択します。図に示されているように、すべてのデフォルトのチェックが保持されていることを確認してください。

付録



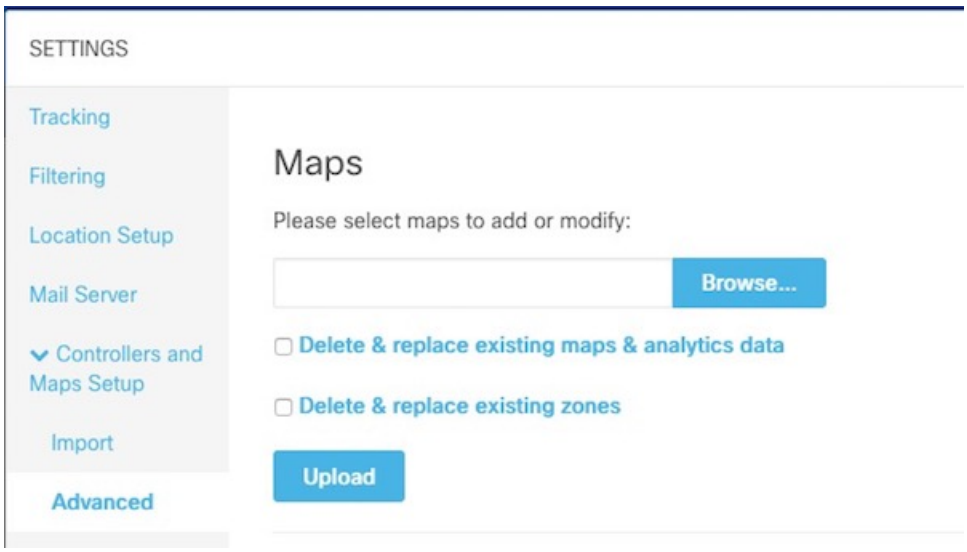
c) エクスポートするマップを選択し、[Export] をクリックします。

選択したマップが `ImportExport_xxxx.tar.gz` という名前の圧縮 .tar ファイル（例：`ImportExport_4575dcc9014d3d88.tar.gz`）としてブラウザのダウンロードディレクトリにダウンロードされます。

ステップ 2 URL *`https://<CMX_IP_address>`* を使用して Cisco CMX ダッシュボードにログインします。

a) [System] > [Settings] > [Controllers and Map Setup] > [Advanced] を選択します。

b) [Maps] で [Browse] をクリックし、Cisco PI（ステップ 1）からエクスポートしたマップを選択して、[Upload] をクリックします。



ステップ 3 アプリケーションのダッシュボードにログインします

ステップ 4 左側のメニューから [Maps] を選択します。

ステップ 5 [Upload] をクリックします。マップがアプリケーションにアップロードされます。

ステップ 6 マップがアプリケーションに正しくアップロードされていることを確認します。

Cisco Spaces から Cisco CMX トークンを取得する方法

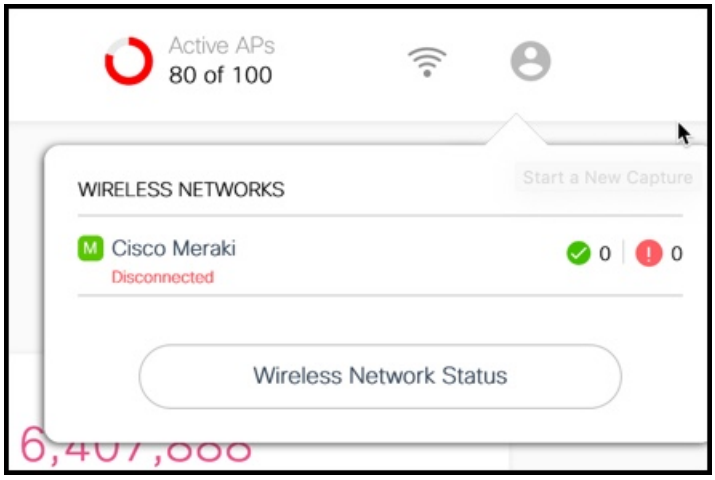
この付録では、Cisco CMX を Cisco Spaces アカウントに追加し、同じアカウントのトークンを取得する方法について説明します。このトークンは、Cisco CMX で設定できます。この手順は、資産ロケータ を正しく機能させるための前提条件です。

手順

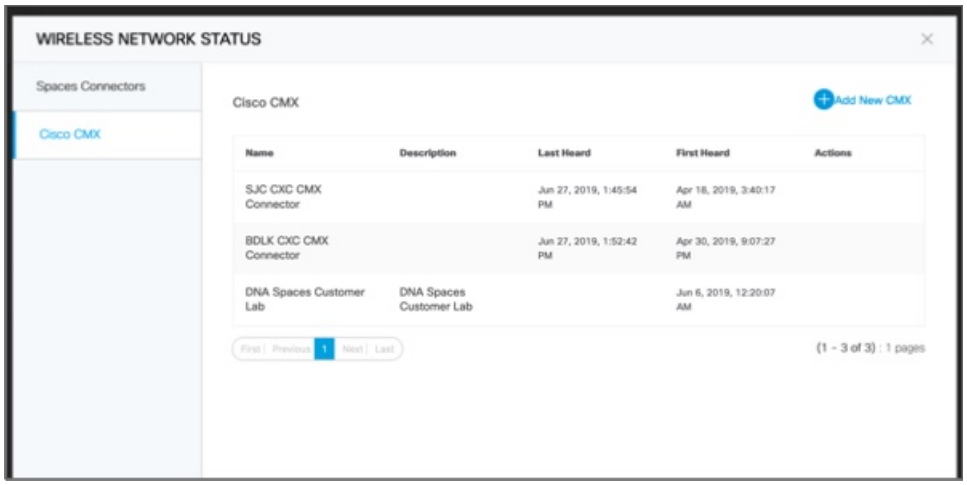
ステップ 1 Cisco Spaces アカウントにログインします。

ステップ 2 右上隅にある ボタンをクリックします。

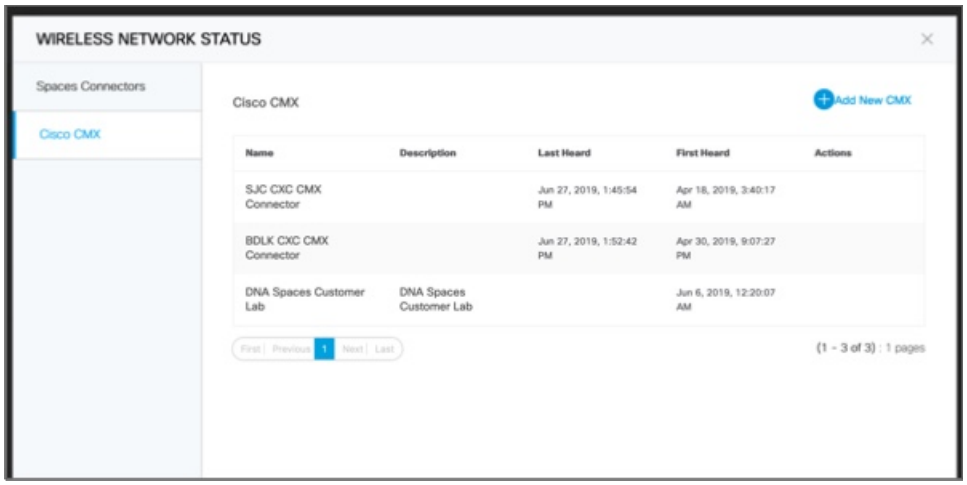
ステップ 3 [Wireless Network Status] をクリックします。



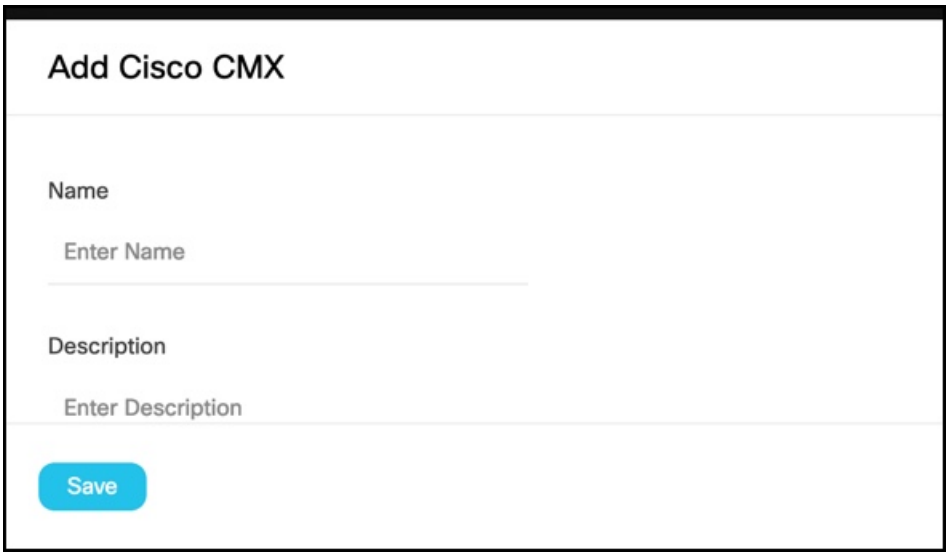
ステップ 4 表示される [Wireless Network Status] ページで [Cisco CMX] をクリックし、[Add New CMX] をクリックします



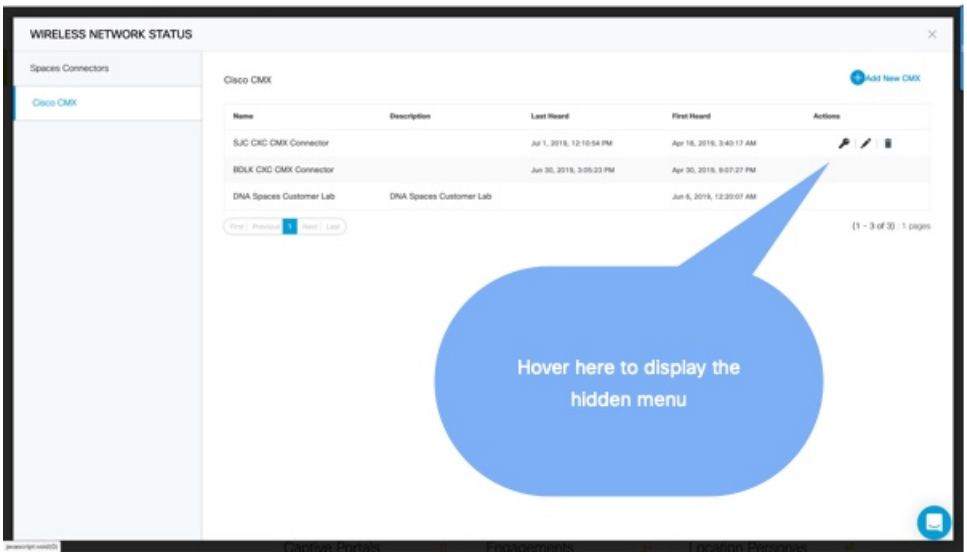
ステップ 5 表示される [Wireless Network Status] ページで [Cisco CMX] をクリックし、[Add New CMX] をクリックします



ステップ 6 Cisco CMX の [Name] と [Description] を入力し、[Save] をクリックします。



ステップ 7 追加した Cisco CMX の右端の領域をマウスオーバーすると、それぞれ非表示のメニューが表示されます。[Key] ボタンをクリックします。



ステップ 8 プロンプトが表示されたら Cisco Spaces ログイン情報を使用して認証し、[Submit] をクリックします。

ステップ 9 [Token] が表示されたら、[Copy] をクリックします。

次のタスク

これで、Cisco CMX にこのトークンを追加できます。

Cisco CMX を使用したロケーションサービス

Cisco CMX 10.6 以降の設定

Cisco CMX 10.6 以降での通知の設定

この手順では、タグのロケーション情報の更新が発生したときにアプリケーションに通知するように Cisco CMX で HTTPS 通知を設定する方法を示します。

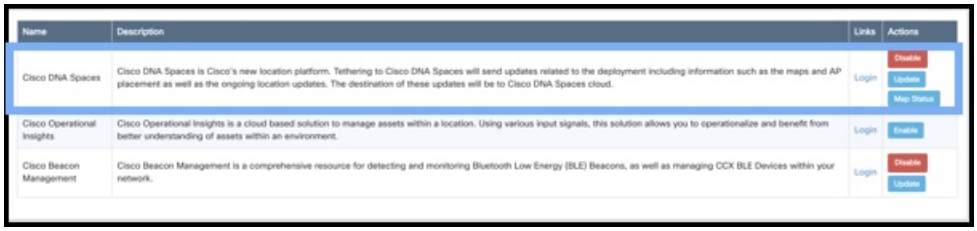
始める前に

アプリケーショントークンを取得します。付録の 「*Cisco Spaces* からトークンを取得する方法」を参照してください。

手順

ステップ 1 Cisco Spaces：Asset Locator ダッシュボードから、[Manage] > [Cloud Apps] を選択します。

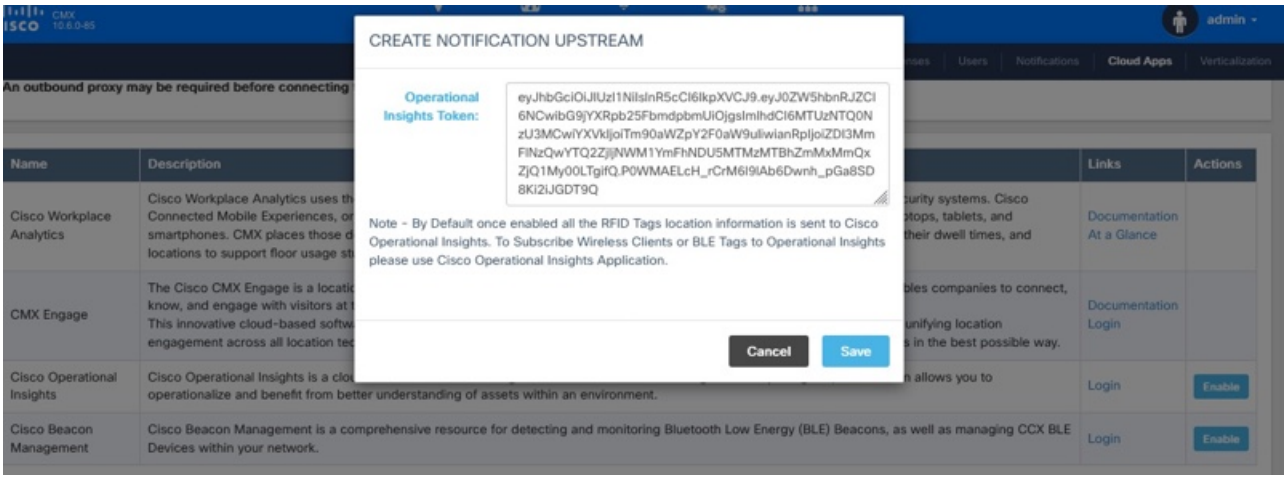
ステップ 2 [Cloud Applications] > [Cisco Spaces] セクションで、[Enable] をクリックします。



（注）
WARNING

資産ロケータ が存在する場合、有効にしないでください。これは廃止予定です。

ステップ 3 [Create Notification Upstream] ダイアログボックスに、Cisco Spaces から取得したトークンの値を入力します。



Cisco CMX 10.5 以前の設定

Cisco CMX での通知の設定（Cisco CMX 10.6 より前）

この手順では、タグのロケーションの更新が発生したときにアプリケーションに通知するように Cisco CMX で HTTPS 通知を設定する方法を示します。

始める前に

Cisco CMX コンフィギュレーション ガイドの「Creating Cisco CMX Connector and Retrieving Token」セクションからトークンを取得できます。

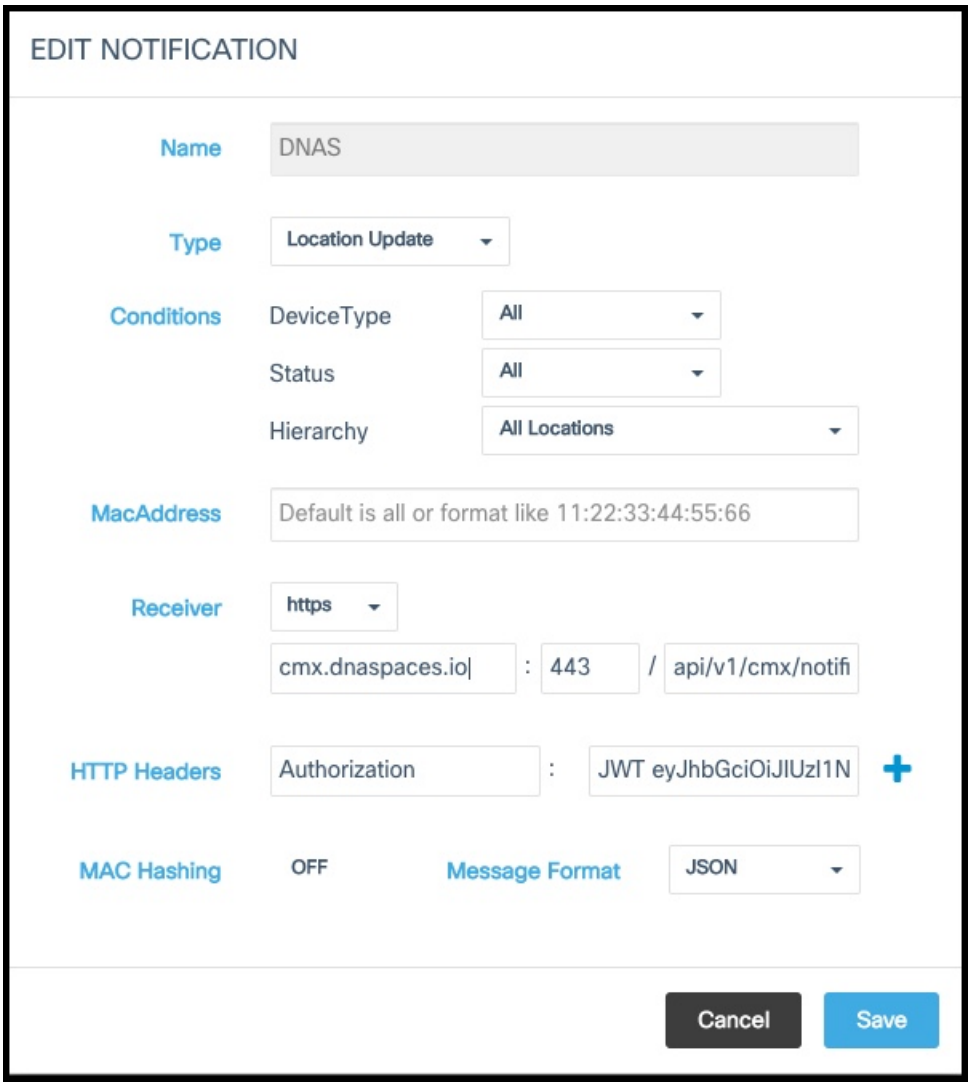
手順

ステップ 1 Cisco CMX ダッシュボードから、[Manage] > [Notification] > [+New Notification] に移動します。

ステップ 2 [Create New Notification] ダイアログボックスで、通知の [Name] を入力します。

付録

図 *1 : Create New Notification*



ステップ 3 [Conditions] で、[Device Type] および [Status] ドロップダウンボックスから [All] を選択し、[Hierarchy] ドロップダウンボックスから [All Locations] を選択します。

ステップ 4 [MAC Address] フィールドは空のままにしておきます。

ステップ 5 [Receiver] ドロップダウンリストから、[https] を選択します。

ステップ 6 アクティベーションメールの情報から、**ホストアドレス**フィールドに`https://cmx.dnaspaces.io`、ポート番号に *443* と入力します。

ステップ 7 **url** フィールドに **`api/v1/cmx/notifications/locationUpdate`** と入力します

ステップ 8 [MAC hashing] オプションをオフにします。

ステップ 9 [Message Format] ドロップダウンリストから、[JSON] を選択します。

ステップ 10 [作成（Create）] をクリックします。

Cisco CMX（10.3 より前）でのテレメトリの有効化

このタスクにより、Cisco CMX はテレメトリデータを 資産ロケータ に送信できます。テレメトリデータは、RFID タグによって収集され、Cisco CMX ロケーションエンジンを介して 資産ロケータ に送信される、温度や湿度などの非位置データです。

手順

ステップ 1 Cisco CMX CLI で、`/opt/cmx/etc/node.conf` に移動し、[location] セクションの下に次の行を挿入します。

```
user_options=-Dpublish-telemetry=true
```

ステップ 2 Cisco CMX を再起動します。

```
cmxctl stop -a
cmxctl agent start
cmxctl start
```

ステップ 3 Cisco CMX とそのすべてのサービスおよびプロセスが稼働していることを確認します。

```
cmxctl status
```

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。