



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](#) (1 ページ)
- [RADIUS 認証用の Cisco Meraki の設定](#) (2 ページ)
- [通知およびレポート用 Cisco Meraki の設定](#) (4 ページ)
- [ソーシャル認証のための Cisco Meraki の設定](#) (5 ページ)
- [Cisco Meraki の SSID の手動設定](#) (6 ページ)
- [Cisco Meraki でのスキャン API の設定](#) (7 ページ)
- [Bluetooth Low Energy デバイスサポート](#) (8 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。

RADIUS 認証用の Cisco Meraki の設定

- 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のデフォルトのポリシー名として機能します。つまり、[Seamlessly Internet Provision] が選択されるキャプティブポータルルールに対してポリシー名を指定しない場合、ポリシー名「CaptiveBypass」がこのルールに対して適用されます。

ステップ 14 [Bandwidth] ドロップダウンリストから必要なオプションを選択し、顧客にプロビジョニングするインターネットの帯域幅を指定します。

ステップ 15 [Splash] ドロップダウンリストから [Bypass] を選択します。

ステップ 16 [Apply] をクリックします。

ステップ 17 ウォールドガーデンの範囲を設定します。ウォールドガーデンの範囲を表示するには、Cisco DNA Spaces ダッシュボードで、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。

- [Analytics] ドロップダウンリストから、[Analytics is enabled] を選択します。
- [Scanning API] ドロップダウンリストから、[Scanning API enabled] を選択します。
- [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 1: 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 ネットワークで使用でき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。
-

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。