

Security Cloud Control Firewall Management でのデバイスのオンボーディング

ライブデバイスとモデルデバイスの両方を Security Cloud Control Firewall Management にオンボーディングできます。モデルデバイスはアップロードされた構成ファイルであり、Security Cloud Control Firewall Management を使用して表示および編集できます。

ほとんどのライブデバイスおよびサービスでは、Secure Device Connector が Security Cloud Control Firewall Management をデバイスまたはサービスに接続できるように、オープンな HTTPS 接続が必要となります。

SDC とそのステータスの詳細については、 Secure Device Connector について を参照してください。

- Cisco Meraki MX デバイスのオンボーディング （1 ページ）

Cisco Meraki MX デバイスのオンボーディング

この章では、Cisco Meraki MX デバイスをオンボーディングする手順について説明します。

Meraki MX の Security Cloud Control へのオンボーディング

MX デバイスは、Security Cloud Control と Cisco Meraki ダッシュボードの両方で管理できます。Security Cloud Control は、設定の変更を Cisco Meraki ダッシュボードに展開します。ダッシュボードはその設定をデバイスに安全に展開します。

Before you begin

- Security Cloud Control の管理対象デバイスへの接続については、「直接クラウド接続のインバウンドアクセスを許可」を参照してください。
- まず、Meraki ダッシュボードで Meraki MX を登録する必要があります。Cisco Meraki ダッシュボードにアクセスできないと、組織は Cisco Meraki クラウドによって認識されません。その結果、デバイスをオンボードするための API トークンを生成できません。

- Security Cloud Control は、ホストに関連付けられたすべてのビットをゼロに設定することにより、無効な CIDR プレフィックス表記の IP アドレスと IP アドレス範囲を有効な形式に変換します。
- Meraki MX デバイスまたはテンプレートのオンボーディングでは、Secure Device Connector（SDC）を介した接続は必要なくなりました。以前にオンボーディングされた Meraki MX デバイスがあり、SDC を使用して Security Cloud Control に接続する場合、その接続は引き続き機能します。デバイスを削除して再度オンボーディングするか、接続ログイン情報を更新すると、接続が停止します。
- MX デバイスを Security Cloud Control で管理するために Cisco Meraki クラウドに接続する必要はありません。MX デバイスがクラウドに接続したことがない場合、デバイスの接続は**到達不能**としてリストされます。このステータスは正常であり、デバイスを管理したり、ポリシーをデバイスに展開したりする機能には影響しません。

Procedure

ステップ 1 Meraki MX デバイスをオンボードするときは、Meraki API キーを生成する必要があります。このキーにより、ダッシュボードが要求を認証できるようになります。これにより、デバイスを安全にオンボーディングできます。Meraki API キーの生成と取得の詳細については、「Meraki API キーの生成と取得」を参照してください。

ステップ 2 API キーを使用して Cisco Meraki デバイスを Security Cloud Control にオンボードします。

Meraki API キーの生成と取得

以下の手順に従って、API アクセスによる Security Cloud Control の Meraki ダッシュボードへのアクセスを有効にします。

Before you begin

Meraki MX の Security Cloud Control へのオンボーディング, on page 1 に関する注意事項と前提条件を確認します。

Procedure

ステップ 1 Meraki ダッシュボードにログインします。

ステップ 2 **[組織（Organization）] > [設定（Settings）]** の順に選択します。

ステップ 3 [ダッシュボードAPIアクセス（Dashboard API Access）] セクションで、[Cisco Merakiダッシュボード APIへのアクセスを有効にする（Enable access to the Cisco Meraki Dashboard API）] をオンにします。このオプションをオンにしないと、MX デバイスを Security Cloud Control にオンボーディングするための API キーを生成できません。

ステップ 4 [変更の保存（Save Changes）] をクリックします。

ステップ 5 Cisco Meraki ダッシュボードで、**ユーザー名**をクリックしてから、[マイプロファイル（My Profile）] をクリックします。

ステップ 6 API アクセスヘッダーを見つけて、[新しいAPIキーの生成（Generate new API key）] をクリックします。API キーをコピーし、使用する準備が整うまでメモに貼り付けておきます。API キーを貼り付ける前にその API キーを含むウィンドウまたはタブを閉じると、コピーした API キーにアクセスできなくなります。

Note デバイスごとに必要な API キーは 1 つのみです。新しいキーを生成せずに、Meraki デバイスを再オンボーディングできます。

「Meraki デバイスの Security Cloud Control へのオンボーディング」に進みます。

Security Cloud Control への MX デバイスのオンボード

次の手順を使用して、Cisco Meraki デバイスをオンボードします。

Before you begin

Meraki API キーの生成と取得, on page 2。

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 **セキュリティデバイス**を選択します。

ステップ 3 青色の追加ボタン（）をクリックします。

ステップ 4 [Meraki] タイルをクリックします。

ステップ 5 このデバイスが通信する Secure Device Connector について を選択します。デフォルトの SDC が表示されますが、青色の [変更（Change）] リンクをクリックして変更できます。

ステップ 6 [Cisco Merakiへの接続（Connect to Cisco Meraki）] ページで、次の手順を実行します。

a) コピーした API アクセスキーを貼り付けて、[接続（Connect）] をクリックします。
キーが不完全または正しくない場合、デバイスをオンボードできません。

b) ドロップダウンリストを使用して、正しい組織を選択します。生成された組織のリストはCisco Meraki ダッシュボードから取得され、このリストにはデバイスとテンプレートが含まれています。[選択（Select）] をクリックします。

c) ドロップダウンリストを使用して、正しいネットワークを選択します。生成されたネットワークのリストは、Cisco Meraki ネットワークから取得されます。[選択（Select）] をクリックします。

d) （オプション）デバイスに固有のラベルを追加します。これらのラベルでデバイスのリストをフィルタリングできます。[続行（Continue）] をクリックします。

デバイスのオンボーディングプロセスが開始されます。プロセスが完了すると、[セキュリティデバイス（Security Devices）] ページにリダイレクトされます。

Meraki テンプレートの Security Cloud Control へのオンボーディング

Cisco Meraki テンプレートは、単一のポリシーで複数の場所またはネットワークを管理するための優れた方法です。これらのテンプレートは、Security Cloud Control と Cisco Meraki ダッシュボードの両方を使用して管理できます。Security Cloud Control は設定の変更を Cisco Meraki ダッシュボードにデプロイし、その後ダッシュボードは設定をテンプレートに安全にデプロイします。Security Cloud Control が Meraki と通信する方法の詳細。

Note テンプレートを Security Cloud Control にオンボーディングするには、まず Meraki ダッシュボードでテンプレートを作成する必要があります。Cisco Meraki ダッシュボードへのアクセス権がない場合、Cisco Meraki クラウドは組織を認識せず、ユーザーはデバイスの API トークンを生成できません。Cisco Meraki ダッシュボードで、**[組織（Organization）] > [設定テンプレート（Configuration templates）]** をクリックします。詳細については、「設定テンプレートを使用してネットワークを一括管理する」を参照してください。

Meraki テンプレートを導入するには、次の 3 つの手順を完了する必要があります。

Procedure

ステップ 1 Meraki ダッシュボードでテンプレートネットワークを作成します。Cisco Meraki テンプレートのベストプラクティスの詳細については、「Meraki Templates Best Practices」を参照してください。

ステップ 2 Meraki API キーを生成して取得します。Meraki テンプレートをオンボーディングするときは、Meraki API キーを生成する必要があります。このキーでダッシュボードを認証し、デバイスを安全にオンボーディングすることができます。

ステップ 3 このキーを使用して Meraki テンプレートを Security Cloud Control にオンボーディングします。

Meraki API キーの生成と取得

以下の手順に従って、API アクセスによる Security Cloud Control の Meraki ダッシュボードへのアクセスを有効にします。

Procedure

ステップ 1 Meraki ダッシュボードにログインします。

ステップ 2 **[組織（Organization）] > [設定（Settings）]** の順に選択します。

ステップ 3 [ダッシュボードAPIアクセス（Dashboard API Access）] セクションで、[Cisco MerakiダッシュボードAPIへのアクセスを有効にする（Enable access to the Cisco Meraki Dashboard API）] をオンにします。このオプションをオンにしないと、MX デバイスを Security Cloud Control にオンボーディングするための API キーを生成できません。

ステップ 4 [変更の保存（Save Changes）] をクリックします。

ステップ 5 Cisco Meraki ダッシュボードで、**ユーザー名**をクリックしてから、[マイプロファイル（My Profile）] をクリックします。

ステップ 6 API アクセスヘッダーを見つけて、[新しいAPIキーの生成（Generate new API key）] をクリックします。API キーをコピーし、使用する準備が整うまでメモに貼り付けておきます。API キーを貼り付ける前にその API キーを含むウィンドウまたはタブを閉じると、コピーした API キーにアクセスできなくなります。

Note テンプレートごとに必要な API キーは 1 つのみです。テンプレートの再オンボーディングに新しいキーを生成する必要はありません。

Meraki テンプレートの Security Cloud Control へのオンボーディング

以下の手順に従って、Cisco Meraki テンプレートをオンボーディングします。

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 **セキュリティデバイス**を選択します。

ステップ 3 青色の追加ボタン（）をクリックします。

ステップ 4 [Cisco Merakiへの接続（Connect to Cisco Meraki）] をクリックします。

ステップ 5 コピーした API アクセスキーを貼り付けます。キーが不完全または正しくない場合、デバイスをオンボードできません。[接続（Connect）] をクリックします。

ステップ 6 ドロップダウンリストを使用して、テンプレート名として [組織（Organization）] を選択します。生成された組織のリストは Cisco Meraki ダッシュボードから取得され、このリストにはデバイスとテンプレートが含まれています。目的のテンプレートを選択し、[選択] をクリックします。

ステップ 7 （オプション）デバイスに固有のラベルを追加できます。これらのラベルでデバイスのリストをフィルタリングできます。

ステップ 8 [続行（Continue）] をクリックします。

デバイスのオンボーディングプロセスが開始されます。完了すると、Security Cloud Control により [セキュリティデバイス（Security Devices）] にリダイレクトされます。テンプレートが Security Cloud Control に同期されると、[セキュリティデバイス（Security Devices）] ページにテンプレートに関連付けられたデバイ

スの名前が表示され、[デバイスの詳細（Device Details）] ウィンドウにテンプレートにバインドされたネットワークの数が表示されます。

Meraki MX の接続ログイン情報の更新

Meraki ダッシュボードから新しい API キーを生成する場合は、Security Cloud Control Firewall Management で接続ログイン情報を更新する必要があります。

Security Cloud Control Firewall Management では、デバイス自体の接続ログイン情報を更新することはできません。必要に応じて、Cisco Meraki ダッシュボードで API キーを手動で更新します。ログイン情報を更新して通信を復元するには、Security Cloud Control Firewall Management UI で API キーを手動で更新する必要があります。

Note Security Cloud Control がデバイスの同期に失敗した場合、Security Cloud Control の接続ステータスに [無効なログイン情報（Invalid Credentials）] と表示されることがあります。この状況では、API キーを使用しようとした可能性があります。選択した Meraki MX の API キーが正しいことを確認します。

次の手順を使用して、Cisco Meraki MX デバイスのログイン情報を更新します。

Procedure

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。

ステップ 2 **セキュリティデバイス**を選択します。

ステップ 3 [デバイス（Devices）] タブをクリックし、[Cisco Meraki（Meraki）] タブをクリックします。

ステップ 4 接続ログイン情報を更新する Meraki MX を選択します。

ステップ 5 [デバイスアクション（Device Actions）] ペインで、[ログイン情報の更新（Update Credentials）] をクリックします。

ステップ 6 Security Cloud Control Firewall Management がデバイスにログインするために使用する **API キー**を入力し、[更新（Update）] をクリックします。この API キーは、変更されていない限り、Cisco Meraki MX のオンボーディングに使用したのと同じログイン情報です。これらの変更は、デバイスに展開する必要はありません。

Security Cloud Control Firewall Management からのデバイスの削除

Security Cloud Control Firewall Management からデバイスを削除するには、次の手順を実行します。

手順

ステップ 1 Security Cloud Control のホームページで、[ファイアウォール（Firewall）] をクリックします。
ステップ 2 **セキュリティデバイス**を選択します。
ステップ 3 削除するデバイスを選択します。
ステップ 4 [デバイスアクション（Device Actions）] ペインで、[削除（Remove）] をクリックします。
ステップ 5 デバイスの削除を確認するには、[OK] をクリックします。
デバイスをオンボーディングされたままにするには、[キャンセル（Cancel）] をクリックします。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。