



デバイスとサービ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 に導入準備できます。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 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 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](#) を参照してください。

この章は、次のセクションで構成されています。

- [SSH デバイスのオンボーディング](#) (1 ページ)

SSH デバイスのオンボーディング

SSH デバイスに保存されている、高レベルの権限を持つユーザーのユーザー名とパスワードを使用して、デバイスをオンボーディングできます。

SSH デバイスのオンボーディング

始める前に

実行する前に、次の前提条件を満たしていることを確認してください。

- SSH デバイスがサポートする暗号が Security Cloud Control でサポートされていることを確認してください。現時点では、Security Cloud Control は、SSH デバイスのオンボーディング用に限定された暗号セットをサポートしています。サポートされている暗号は次のとおりです：aes128-ctr、aes192-ctr、aes256-ctr、aes128-gcm、aes128-gcm@openssh.com、aes256-gcm、aes256-gcm@openssh.com。サーバーがサポートする暗号を確認するには、SDC にログインし、コマンド `ssh -vv <ip_address>` を実行します。
- Cisco IOS デバイスをオンボーディングするには、ネットワーク内にオンプレミス Secure Device Connector (SDC) が必要です。SDC の説明と展開シナリオへのリンクについては、[Secure Device Connector](#) を参照してください。

- デバイスをオンボーディングする前に、「[Secure Device Connector を使用した Cisco Security Cloud Control への接続](#)」を参照してください。

手順

- ステップ 1 左側のペインで **セキュリティデバイス** をクリックします。
- ステップ 2 青色のプラスボタン  をクリックして、デバイスをオンボーディングします。
- ステップ 3 [統合 (Integrations)] タイルをクリックします。グレー表示されている場合は、ネットワークに展開されていて、Security Cloud Control テナントで使用されているアクティブな Secure Device Connector がないことを意味します。
- ステップ 4 **Secure Device Connector** ボタンをクリックして、このデバイスが通信するネットワーク内の SDC を選択します。デフォルトの SDC が表示されますが、SDC 名をクリックすることで SDC を変更できます。
- ステップ 5 デバイスに名前を付けます。
- ステップ 6 [統合 (Integrations)] ドロップダウンメニューで、[汎用SSH (Generic SSH)] を選択します。
- ステップ 7 デバイスの場所として FQDN または IPv4 アドレスを入力します。デフォルト SSH ポートは 22 です。
- ステップ 8 [実行 (Go)] をクリックします。Security Cloud Control はデバイスを特定し、設定を統合する準備をします。
- ステップ 9 SSH フィンガープリントを [ダウンロード (Download)] し、ローカルに保存します。これまでに SSH 経由でこのデバイスに接続したことがない場合は、このフィンガープリントを使用してデバイスを確認できます。
- ステップ 10 オンボーディングするデバイスの [ユーザー名 (Username)] と [パスワード (Password)] にログイン情報を入力します。Security Cloud Control は、正しいログイン情報がないと既存の設定を正常に読み取ることができません。
- ステップ 11 (オプション) このデバイスに以前に [イネーブルパスワード (Enable Password)] を設定した場合は、それを入力します。
- ステップ 12 (オプション) ドロップダウンメニューから [設定コマンド (Configuration Command)] を選択するか、テキストボックスにカスタムコマンドを入力します。このコマンドは、デバイスの設定として使用されます。OOB が有効になっている場合、Security Cloud Control は変更をチェックします。[設定 (Configuration)] ページで現在の値を表示できます。デバイスが Security Cloud Control に正常にオンボーディングされた後に、このコマンドの変更が可能になることに注意してください。
- ステップ 13 [接続 (Connect)] をクリックします。

(注)

ログイン情報が正しくない場合は、接続の詳細を確認するように求められます。ここでログイン情報を再入力できます。ログイン情報を修正せずに確認を終了すると、デバイスの [インベントリ] ページに統合インスタンスが表示されますが、デバイスは導入準備または同期されていません。

ステップ 14 (オプション) このデバイスにラベルを追加します。

ステップ 15 [続行 (Continue)] をクリックします。

ステップ 16 デバイスは Security Cloud Control にオンボーディングされます。[終了 (Finish)] をクリックします。

ステップ 17 [インベントリ] ページに戻ります。デバイスが正常にオンボーディングされると、設定ステータスが [同期 (Synced)]、接続状態が [オンライン (Online)] と表示されます。

(注)

デバイスがオンボーディングされると、実行する設定コマンドの変更が可能になります。カスタムコマンドを使用するか、[CLI マクロ](#)を作成できます。

ステップ 18 (オプション) 必要に応じて、デバイスの [ノート (Notes)] ページにデバイスに関するノートを入力できます。詳細については、「[デバイスノート](#)」を参照してください。

関連情報 :

- [デバイス管理用の CLI マクロ](#)
- [Cisco IOS または SSH から Security Cloud Control への変更の読み取り](#)
- [設定変更の読み取り、破棄、チェック、および展開](#)

Security Cloud Control からデバイスを削除

Security Cloud Control からデバイスを削除するには、次の手順を使用します。

手順

ステップ 1 Security Cloud Control にログインします。

ステップ 2 左側のペインで **セキュリティデバイス** をクリックします。

ステップ 3 削除するデバイスを見つけ、そのデバイスの行でデバイスをチェックして選択します。

ステップ 4 右側にある [デバイスアクション (Device Actions)] パネルで、[削除 (Remove)] を選択します。

ステップ 5 プロンプトが表示されたら、[OK] を選択して、選択したデバイスの削除を確認します。[キャンセル (Cancel)] を選択して、デバイスをオンボードしたままにします。

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。