

セキュアエンドポイントコンソールでの2要素認証の設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[アクセス制御](#)

[二要素認証](#)

[設定](#)

[権限](#)

[二要素認証](#)

概要

このドキュメントでは、Cisco Secure Endpoint Consoleで二要素認証を設定するアカウントのタイプと手順について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- セキュアエンドポイント
- Secure Endpointコンソールへのアクセス

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Secure Endpoint Console v5.4.20211013

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

アクセス制御

Secure Endpoint Consoleには、次の2種類のアカウントがあります。管理者および非特権または通常のアカウント新しいユーザ名を作成する場合は、ユーザの特権レベルを選択する必要がありますが、いつでもユーザのアクセスレベルを変更できます。

管理者は完全な権限を持ち、組織内の任意のグループまたはコンピュータのデータを表示し、グループ、ポリシー、リスト、およびユーザ名を変更できます。

注：管理者は、別の管理者を通常のアカウントに降格できますが、自分自身を降格することはできません。

非特権または通常のユーザアカウントは、アクセス権が付与されたグループの情報のみを表示できます。新しいユーザアカウントを作成する場合、管理者権限を付与するかどうかを選択できます。これらの権限を付与しない場合は、アクセスできるグループ、ポリシー、およびリストを選択できます。

二要素認証

二要素認証は、Secure Endpoint Consoleアカウントへの不正なアクセスに対する追加のセキュリティ層を提供します。

設定

権限

管理者の場合は、[Accounts] > [Users select the user account]に移動して権限を選択し、権限を選択します。次の図を参照してください。

Privileges

Grant Administrator Privileges Remove All Privileges Revert Changes Save Changes

Allow this user to fetch files (including Connector diagnostics) from the selected groups.

Allow this user to see command line data from the selected groups.

Allow this user to set Endpoint isolation status for the selected groups.

Groups Clear Select Groups

None

For the selected groups: Auto-Select Policies Auto-Select Policies and Lists

Policies Clear Select Policies

None

管理者は、別の管理者に対する管理者権限を取り消すこともできます。これを行うには、図に示すように、管理者アカウントに移動してオプションを表示できます。

Privileges

Revoke Administrator Privileges

🔍 Administrator

👤 All Groups

⚙️ All Policies

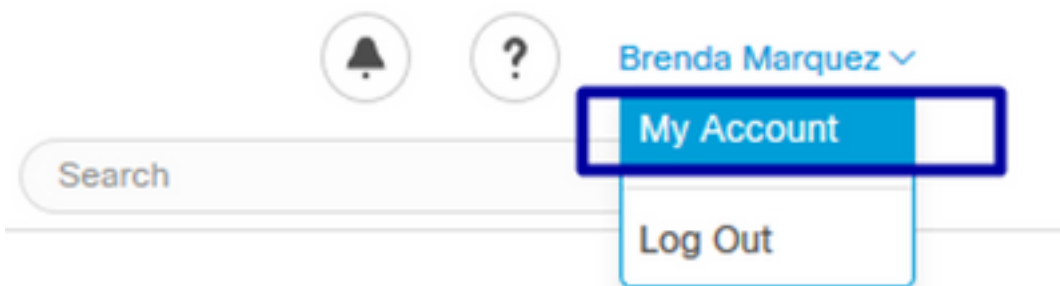
📄 All Outbreak Control Lists

注：ユーザ権限が変更されると、検索結果に一部のデータがキャッシュされるため、ユーザはグループにアクセスできなくなっても、そのデータを一定期間表示できます。ほとんどの場合、キャッシュは5分後に更新されます。

二要素認証

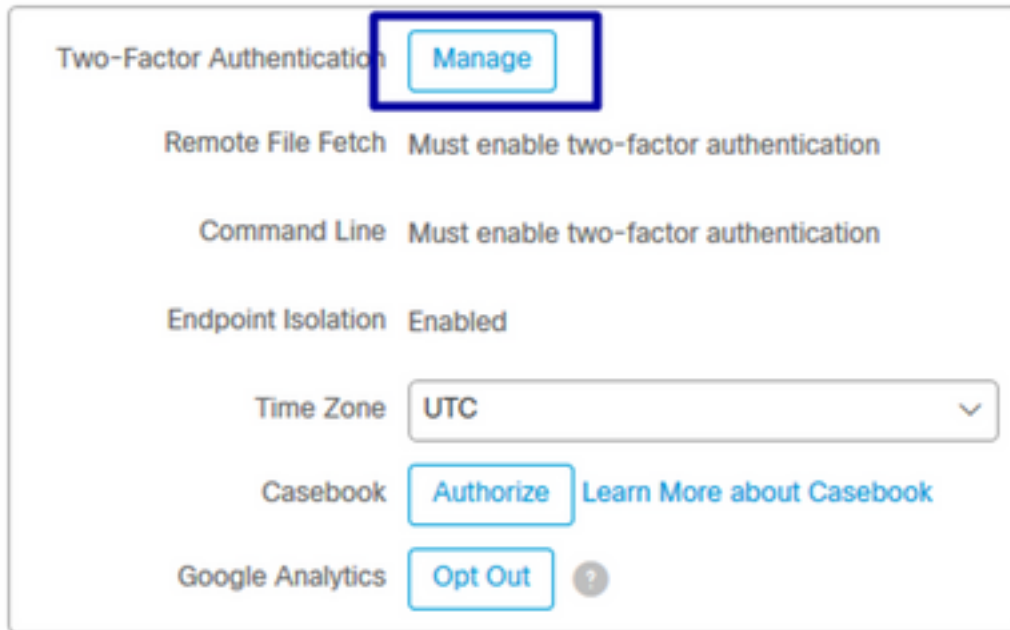
この機能を使用すると、外部アクセス要求による認証を強制できます。これを設定するには、次の手順を実行します。

ステップ1：次の図のように、Secure Endpoint Consoleの右上にある[My Account]に移動します。



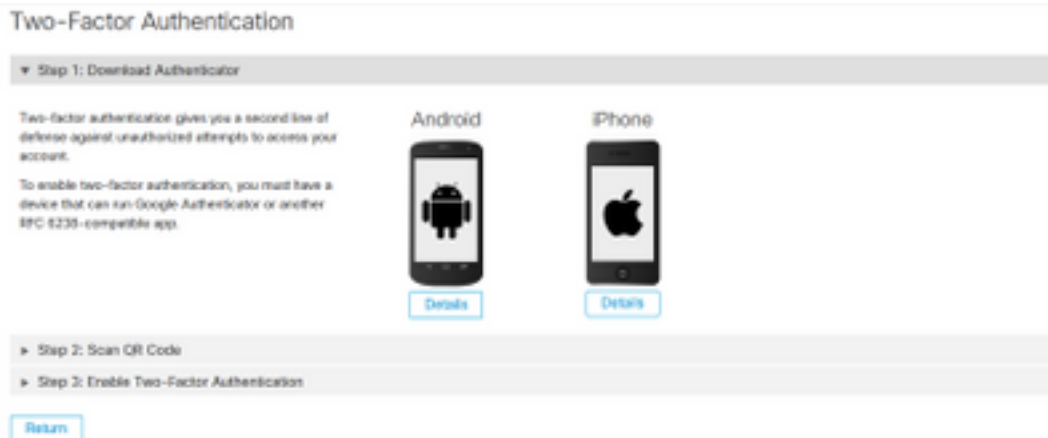
ステップ2:図に示すように、[Settings]セクションで[Manage]を選択すると、この機能を有効にするために必要な3つの手順を含む簡単なガイドが表示されます。

Settings



ステップ3 : 次の3つの手順があります。

a) Google Authenticatorを実行できるAndroidまたはiPhone用に取得できるオーセンティケーターをダウンロードします。任意の携帯電話で[Details]を選択して、ダウンロードページにリダイレクトするQRコードを生成します。次の図を参照してください。




b) QRコードをスキャンし、[Generate QR code]をオンにします。この図に示すように、Google Authenticatorでスキャンする必要があります。

Two-Factor Authentication

▶ Step 1: Download Authenticator

▼ Step 2: Scan QR Code



Warning: This QR code is your **personal one-time code**. This should be kept secure. Generate the QR code only when you have some privacy and are ready.

Add this two-factor authentication account to your device

Click "Generate QR Code" and scan the generated QR code into Google Authenticator or another RFC 6238-compatible app

If you cannot access your device

After completing Step 2, you will be given a set of backup codes. You can use a backup code to access your account and disable two-factor authentication until you can re-enable it with a new device. If you do not have access to any backup codes, contact Support.

Note: We do not recommend storing your Cisco Security password on the same device as your authenticator application. If your Cisco Security password is on the same device as your authenticator app and you lose your device, you should contact Support **immediately** to have your account password reset.

[Sample](#)
[Generate QR Code](#)

▶ Step 3: Enable Two-Factor Authentication

[Return](#)

c) Two-Factor Authenticatorを有効にし、携帯電話でオーセンティケータアプリケーションを開き、確認コードを入力します。図に示すように、[Enable]を選択してこのプロセスを終了します。

Two-Factor Authentication

▶ Step 1: Download Authenticator

▶ Step 2: Scan QR Code

▼ Step 3: Enable Two-Factor Authentication

1. Open your Authenticator app.
2. Enter the verification code from Authenticator.

Enter the verification code from Authenticator.

Please enter verification code

[Enable](#)

[Return](#)

ステップ4：完了すると、バックアップコードが表示されます。[クリップボードにコピー]を選択して保存し、例として画像を参照してください。

Two-Factor Authentication

▶ Step 1: Download Authenticator

▶ Step 2: Scan QR Code

▼ Step 3: Enable Two-Factor Authentication

Two-Factor Authentication has been enabled. Here are your backup codes.

Warning: This is the only time that the backup codes are shown. If you do not make a note of them, you will need to generate a new set. Your backup codes need to be kept safe, as this will be the only way that you will be able to get into your account if you lose access to your device.

In case you cannot access your device we have generated a set of backup codes that you can use. Each backup code on the list can only be used once. You can regenerate a new list of backup codes from Two-Factor Authentication Details on the Users page. Once a new set has been generated, any backup code in the old set is no longer valid. We suggest printing this list out and keeping it somewhere safe.

Backup Codes

- 5c9a4c84
- f20ea786
- 7f1aeb53
- a4f59f0c
- 21a32ced
- 1e3073b1
- 42e2e189
- f54f3fde
- 7424df5f
- 3dafab11

[Copy to clipboard](#)

注：各バックアップコードは1回のみ使用できます。すべてのバックアップコードを使用したら、新しいコードを生成するためにこのページに戻る必要があります。

詳細については、『[Secure Endpoint User Guide](#)』を参照してください。

また、「アカウント」と「二要素認証を[有効にする](#)」ビデオも視聴できます。