

Configuration de l'authentification à deux facteurs dans la console Secure Endpoint

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Contrôle d'accès](#)

[Authentification à deux facteurs](#)

[Configurer](#)

[Privilèges](#)

[Authentification à deux facteurs](#)

Introduction

Ce document décrit le type de comptes et les étapes à suivre pour configurer l'authentification à deux facteurs dans Cisco Secure Endpoint Console.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Terminaux sécurisés
- Accès à la console Secure Endpoint

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Console de terminal sécurisé v5.4.20211013

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Contrôle d'accès

Il existe deux types de comptes dans la console Secure Endpoint : les comptes d'administrateurs et les comptes non privilégiés ou réguliers. Lorsque vous créez un nouveau nom d'utilisateur, vous devez sélectionner son niveau de privilège, mais vous pouvez modifier son niveau d'accès à tout moment.

Les administrateurs ont un contrôle total, peuvent afficher les données de n'importe quel groupe ou ordinateur de l'organisation et apporter des modifications aux groupes, stratégies, listes et noms d'utilisateur.

 Remarque : un administrateur peut rétrograder un autre administrateur vers un compte normal, mais ne peut pas se rétrograder lui-même.

Un compte d'utilisateur non privilégié ou normal ne peut afficher que les informations relatives aux groupes auxquels il a accès. Lorsque vous créez un nouveau compte d'utilisateur, vous avez le choix de lui accorder ou non des privilèges d'administrateur. Si vous ne leur accordez pas ces privilèges, vous pouvez sélectionner les groupes, stratégies et listes auxquels ils ont accès.

Authentification à deux facteurs

L'authentification à deux facteurs fournit une couche de sécurité supplémentaire contre les tentatives non autorisées d'accès à votre compte Secure Endpoint Console.

Configurer

Privilèges

Si vous êtes un administrateur, afin de modifier les autorisations ou d'accorder des privilèges d'administrateur, vous pouvez naviguer vers Comptes > Utilisateurs sélectionner le compte d'utilisateur et choisir les autorisations, voir cette image.

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

Un administrateur peut également révoquer les privilèges d'administrateur d'un autre administrateur. Pour ce faire, vous pouvez accéder au compte d'administrateur pour afficher l'option, comme illustré dans l'image.

Privileges

Revoke Administrator Privileges

 Administrator

 All Groups

 All Policies

 All Outbreak Control Lists

 Remarque : lorsque les autorisations utilisateur changent, certaines données sont mises en cache dans les résultats de la recherche afin qu'un utilisateur puisse les voir pendant un certain temps même s'il n'a plus accès à un groupe. Dans la plupart des cas, le cache est actualisé après 5 minutes.

Authentification à deux facteurs

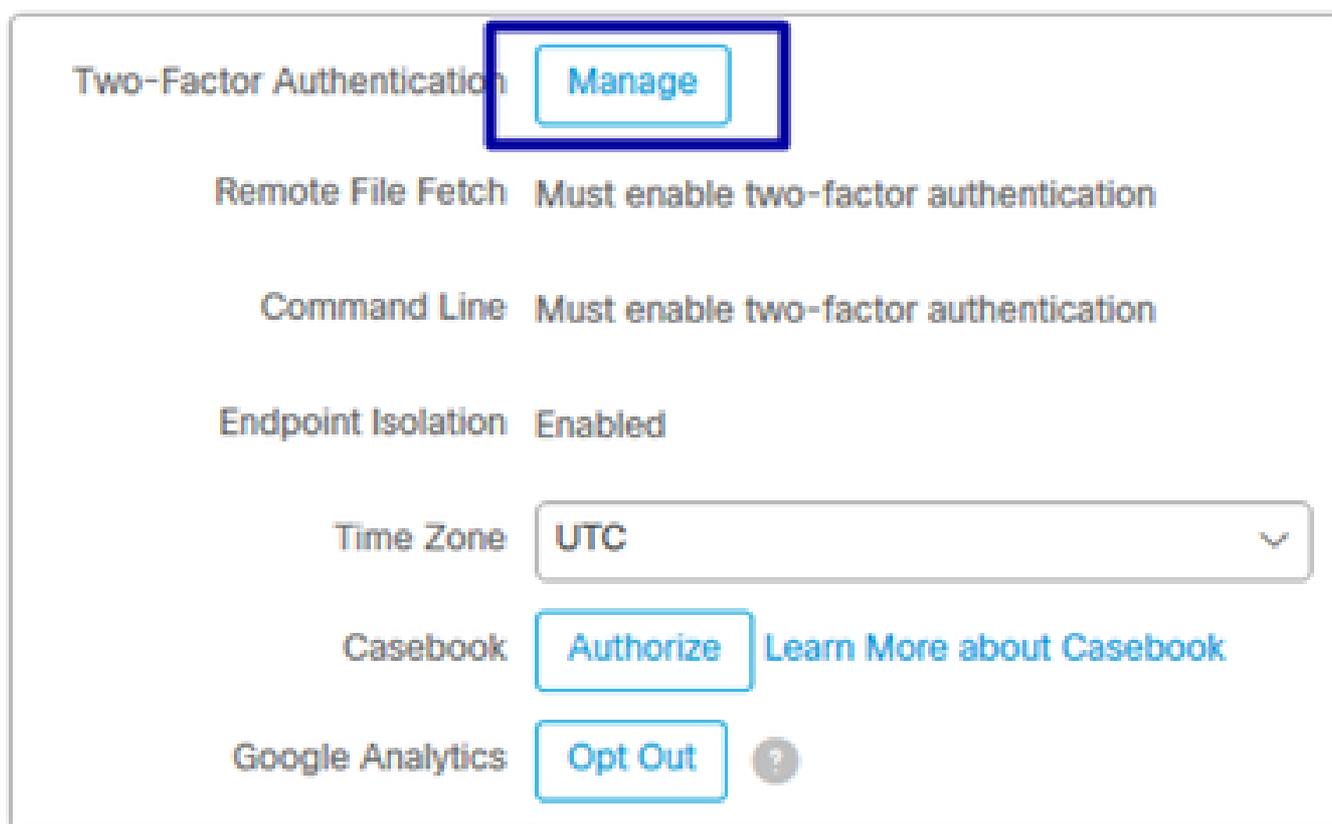
Cette fonctionnalité vous permet d'appliquer l'authentification avec une demande d'accès externe. Afin de configurer ceci, suivez cette procédure :

Étape 1. Accédez à Mon compte en haut à droite de la console Secure Endpoint, comme dans cette image.



Étape 2. Dans la section Paramètres, sélectionnez Gérer, afin de voir un guide simple avec trois étapes nécessaires pour activer cette fonctionnalité, comme illustré dans l'image.

Settings



Étape 3. Il existe trois étapes rapides :

a) Télécharger l'authentificateur, que vous pouvez obtenir pour Android ou iPhone qui peut exécuter Google Authenticator. Sélectionnez Détails sur l'un des téléphones portables pour générer un code QR qui vous redirige vers la page de téléchargement. Voir cette image.

Two-Factor Authentication

Step 1: Download Authenticator

Two-factor authentication gives you a second line of defense against unauthorized attempts to access your account.

To enable two-factor authentication, you must have a device that can run Google Authenticator or another RFC 6238-compatible app.

Android



[Details](#)

iPhone



[Details](#)

Step 2: Scan QR Code

Step 3: Enable Two-Factor Authentication

[Return](#)

b) Numériser le code QR, sélectionnez Générer le code QR, il doit être numérisé par Google Authenticator comme indiqué dans cette image.

Two-Factor Authentication

Step 1: Download Authenticator

Step 2: Scan QR Code



Sample

[Generate 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 3, 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.

Step 3: Enable Two-Factor Authentication

[Return](#)

c) Activez l'authentificateur à deux facteurs, ouvrez votre application d'authentification dans votre téléphone cellulaire et entrez le code de vérification. Sélectionnez Activer pour terminer ce processus, comme illustré dans l'image.

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

Étape 4. Une fois que c'est fait, il vous donne quelques codes de sauvegarde. Sélectionnez Copier dans le Presse-papiers afin de les enregistrer, voir l'image comme un exemple.

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

- 5cfa4c86
- 230aa7d6
- 7f1aeb53
- a4f59d0c
- 31e32ced
- 1e3073b1
- 42e2e109
- f54f3fde
- 7426d99f
- 26a6ab11

Copy to clipboard

 Remarque : chaque code de sauvegarde ne peut être utilisé qu'une seule fois. Après avoir utilisé tous vos codes de sauvegarde, vous devez revenir à cette page afin de générer de nouveaux codes.

Pour plus d'informations, vous pouvez consulter le [Guide de l'utilisateur de Secure Endpoint](#).

En outre, vous pouvez regarder la vidéo [Comptes et Activer l'authentification à deux facteurs](#).

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.