

Configurazione dell'autenticazione a due fattori nella console dell'endpoint sicuro

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Controllo dell'accesso](#)

[Autenticazione a due fattori](#)

[Configurazione](#)

[Privilegi](#)

[Autenticazione a due fattori](#)

Introduzione

In questo documento viene descritto il tipo di account e la procedura per configurare l'autenticazione a due fattori in Cisco Secure Endpoint Console.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Endpoint sicuro
- Accesso a Secure Endpoint Console

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Secure Endpoint Console v5.4.20211013

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Controllo dell'accesso

Nella Secure Endpoint Console sono disponibili due tipi di account: gli account amministratori e gli account normali o senza privilegi. Quando si crea un nuovo nome utente, è necessario selezionare il livello di privilegio corrispondente, ma è possibile modificare il livello di accesso in qualsiasi momento.

Gli amministratori dispongono del controllo completo, possono visualizzare i dati da qualsiasi gruppo o computer dell'organizzazione e apportare modifiche a gruppi, criteri, elenchi e nomi utente.

 Nota: un amministratore può ridurre di livello un altro amministratore a un account normale, ma non può abbassare di livello se stesso.

Un account utente normale o senza privilegi può visualizzare solo le informazioni relative ai gruppi a cui è stato concesso l'accesso. Quando si crea un nuovo account utente, è possibile scegliere se concedere o meno i privilegi di amministratore. Se non si concedono tali privilegi, è possibile selezionare i gruppi, i criteri e gli elenchi a cui hanno accesso.

Autenticazione a due fattori

L'autenticazione a due fattori offre un ulteriore livello di protezione contro i tentativi non autorizzati di accesso all'account Secure Endpoint Console.

Configurazione

Privilegi

Se si è un amministratore, per modificare le autorizzazioni o concedere i privilegi di amministratore, è possibile passare a Account > Utenti e selezionare l'account utente e scegliere le autorizzazioni. Vedere questa immagine.

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 amministratore può inoltre revocare i privilegi di amministratore a un altro amministratore. A tale scopo, è possibile passare all'account amministratore per visualizzare l'opzione, come illustrato nell'immagine.

Privileges

Revoke Administrator Privileges

 Administrator

 All Groups

 All Policies

 All Outbreak Control Lists

 Nota: quando si modificano le autorizzazioni utente, alcuni dati vengono memorizzati nella cache dei risultati di ricerca in modo che un utente possa ancora visualizzarli per un determinato periodo di tempo anche se non ha più accesso a un gruppo. Nella maggior parte dei casi, la cache viene aggiornata dopo 5 minuti.

Autenticazione a due fattori

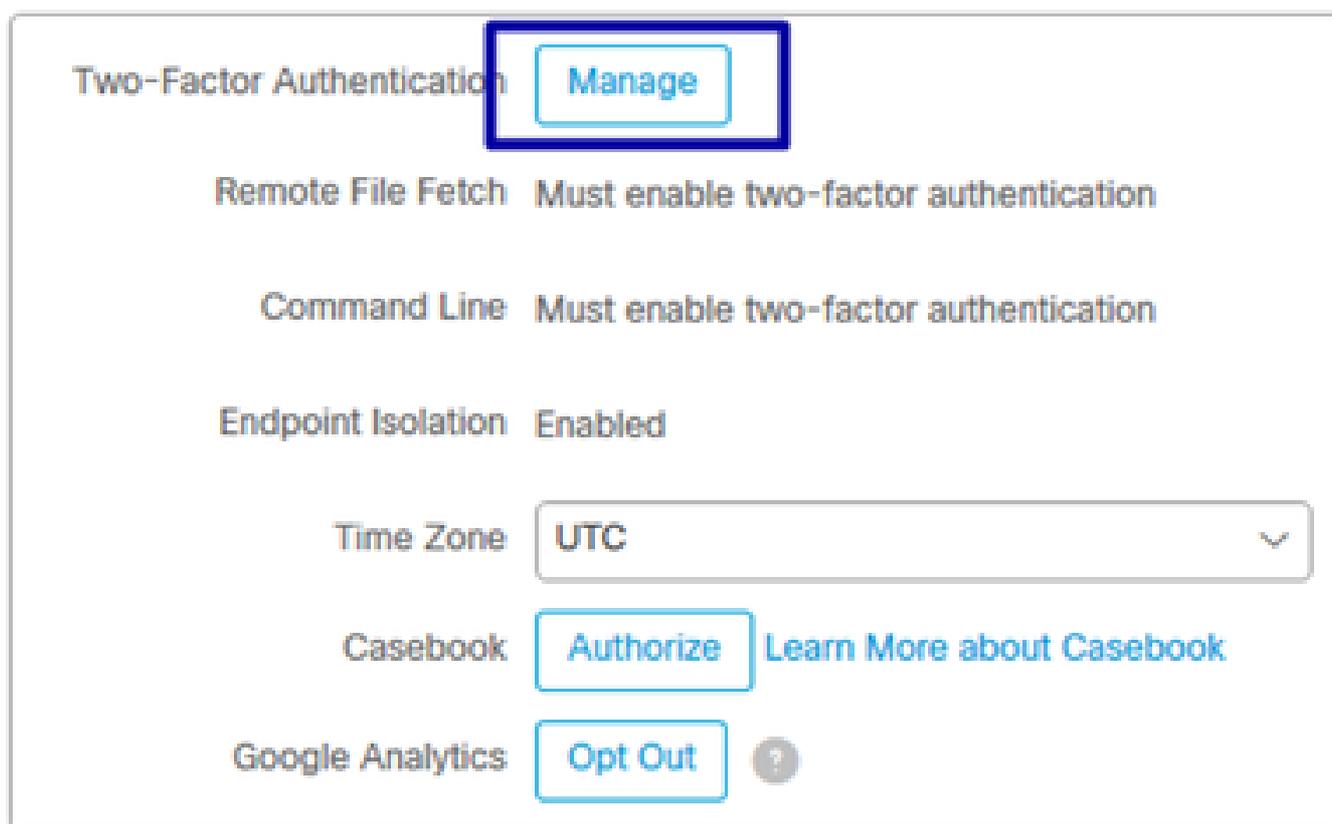
Questa funzionalità consente di applicare l'autenticazione con una richiesta di accesso esterno. Per configurare questa condizione, attenersi alla seguente procedura:

Passaggio 1. Passare a Account personale nella parte superiore destra di Secure Endpoint Console come in questa immagine.



Passaggio 2. Nella sezione Settings (Impostazioni), selezionare Manage (Gestisci) per visualizzare una guida chiara con i tre passaggi necessari per attivare questa funzione, come mostrato nell'immagine.

Settings



Passaggio 3. È possibile eseguire tre passaggi rapidi:

a) Scaricare l'autenticatore, che si può ottenere per Android o iPhone che può eseguire Google Authenticator. Selezionare Dettagli su uno qualsiasi dei telefoni cellulari per generare un codice a matrice che reindirizza l'utente alla pagina di download. Guardate questa immagine.

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) Digitalizzare il codice QR, selezionare Genera codice QR, che deve essere digitalizzato da Google Authenticator come mostrato in questa immagine.

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) Abilitare l'autenticatore a due fattori, aprire l'applicazione di autenticazione nel telefono cellulare e immettere il codice di verifica. Selezionare Attiva per completare il processo, come illustrato nell'immagine.

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

Passaggio 4. Una volta fatto, fornisce alcuni codici di backup. Selezionare Copia negli Appunti per salvarli. Vedere l'immagine come esempio.

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
- 21e32ced
- 1e3073b1
- 42e2e109
- f56f3fde
- 7426d95f
- 26a6ab11

Copy to clipboard

 **Nota:** ciascun codice di backup può essere utilizzato una sola volta. Dopo aver utilizzato tutti i codici di backup, tornare a questa pagina per generare nuovi codici.

Per ulteriori informazioni, consultare la [Guida dell'utente di Secure Endpoint](#).

È inoltre possibile guardare il video [Account e Abilita autenticazione a due fattori](#).

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).