

# Konfigurieren der Zwei-Faktor-Authentifizierung in AMP für Endgeräte

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Zugriffskontrolle](#)

[Zwei-Faktor-Authentifizierung](#)

[Konfigurieren](#)

[Berechtigungen](#)

[Zwei-Faktor-Authentifizierung](#)

## Einführung

In diesem Dokument werden der Kontotyp und die Schritte zum Konfigurieren der Zwei-Faktor-Authentifizierung in der Konsole Advanced Malware Protection (AMP) für Endgeräte beschrieben.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco AMP für Endgeräte
- Zugriff auf die AMP für Endpoints-Konsole

### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- AMP für Endgeräte Konsole v5.4.202041417

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

## Hintergrundinformationen

### Zugriffskontrolle

In der AMP für Endpoints-Konsole gibt es zwei Arten von Konten: Administratoren und nicht privilegierten oder regulären Konten. Wenn Sie einen neuen Benutzernamen erstellen, müssen Sie deren Berechtigungsstufe auswählen, aber Sie können deren Zugriffsebene jederzeit ändern.

Administratoren haben die volle Kontrolle, können Daten von jeder Gruppe oder jedem Computer im Unternehmen anzeigen und Änderungen an Gruppen, Richtlinien, Listen und Benutzernamen vornehmen.

**Hinweis:** Ein Administrator kann einen anderen Administrator zu einem normalen Konto abweisen, kann sich aber nicht selbst abmelden.

Ein nicht privilegiertes oder reguläres Benutzerkonto kann nur Informationen für Gruppen anzeigen, denen Zugriff gewährt wurde. Wenn Sie ein neues Benutzerkonto erstellen, haben Sie die Wahl, ob Sie ihnen Administratorrechte gewähren möchten. Wenn Sie ihnen diese Berechtigungen nicht gewähren, können Sie auswählen, auf welche Gruppen, Richtlinien und Listen sie Zugriff haben.

## Zwei-Faktor-Authentifizierung

Die Two-Factor-Authentifizierung bietet eine zusätzliche Sicherheitsebene gegen nicht autorisierte Zugriffe auf das Konsolenkonto von AMP für Endpoints.

## Konfigurieren

### Berechtigungen

Wenn Sie ein Administrator sind, können Sie zum Ändern von Berechtigungen oder zum Gewähren von Administratorrechten zu Accounts > Users (Konten > Benutzer) wechseln, das Benutzerkonto auswählen und die Berechtigungen auswählen. Weitere Informationen finden Sie in diesem Bild.

The screenshot shows the 'Privileges' configuration page. At the top, there is a 'Grant Administrator Privileges' button and three action buttons: 'Remove All Privileges', 'Revert Changes', and 'Save Changes'. Below these are three checkboxes for permissions: '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', and 'Allow this user to set Endpoint Isolation status for the selected groups'. The 'Groups' section has a 'Clear' button and a 'Select Groups' dropdown menu, with 'None' selected. Below this, there are two buttons: 'Auto-Select Policies' and 'Auto-Select Policies and Lists'. The 'Policies' section also has a 'Clear' button and a 'Select Policies' dropdown menu, with 'None' selected.

Ein Administrator kann einem anderen Administrator auch Administratorrechte entziehen. Hierzu können Sie zum Administratorkonto navigieren, um die Option anzuzeigen, wie im Bild gezeigt.

## Privileges

Revoke Administrator Privileges

🔍 Administrator

👤 All Groups

⚙️ All Policies

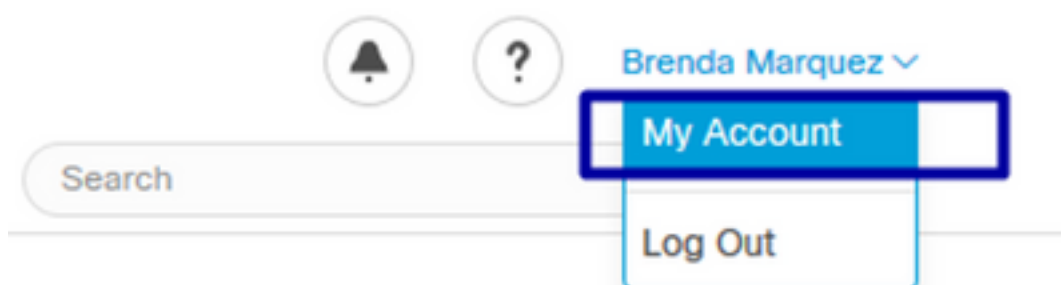
📄 All Outbreak Control Lists

**Hinweis:** Wenn Benutzerberechtigungen einige Daten ändern, werden sie in Suchergebnissen zwischengespeichert, sodass ein Benutzer sie für einen bestimmten Zeitraum sehen kann, obwohl er keinen Zugriff mehr auf eine Gruppe hat. In den meisten Fällen wird der Cache nach 5 Minuten aktualisiert.

## Zwei-Faktor-Authentifizierung

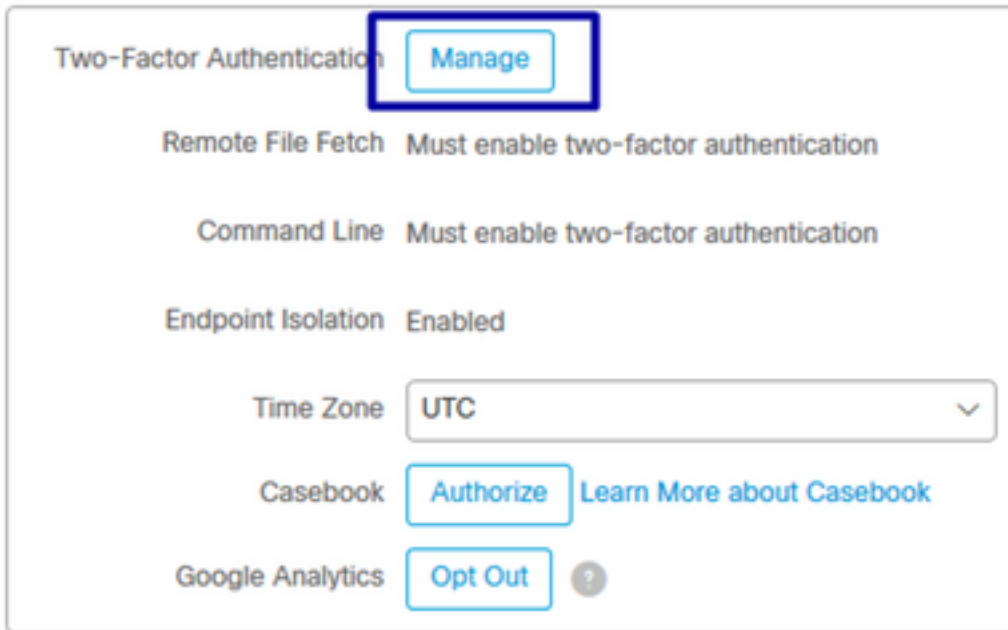
Mit dieser Funktion können Sie die Authentifizierung mit einer externen Zugriffsanforderung durchsetzen. Gehen Sie folgendermaßen vor, um dies zu konfigurieren:

**Schritt 1:** Navigieren Sie wie in diesem Bild zu Mein Konto rechts oben in der AMP für Endgeräte-Konsole.



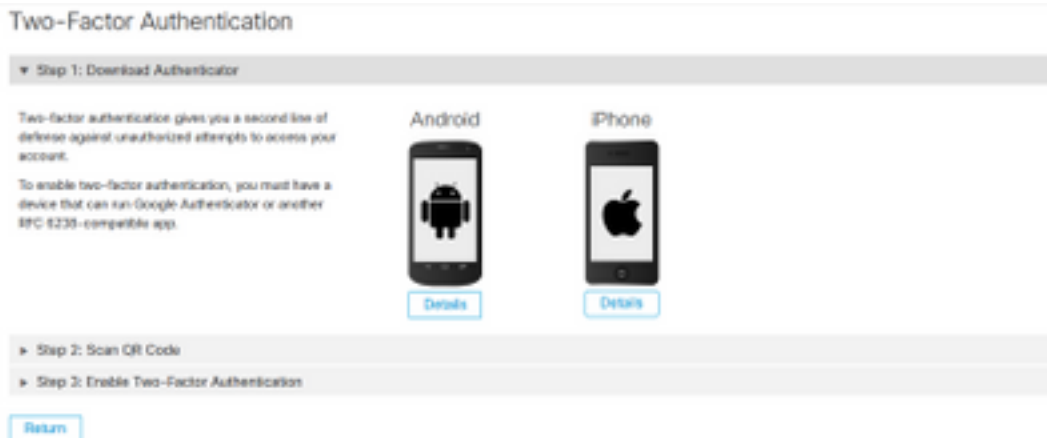
**Schritt 2:** Wählen Sie im Abschnitt Einstellungen die Option Verwalten aus, um eine einfache Anleitung mit drei Schritten anzuzeigen, die für die Aktivierung dieser Funktion erforderlich sind, wie im Bild gezeigt.

## Settings



**Schritt 3:** Es gibt drei schnelle Schritte:

a) Laden Sie den Authentifizierer herunter, den Sie für Android oder iPhone erhalten können, das Google Authenticator ausführen kann. Wählen Sie Details auf einem der Mobiltelefone aus, um einen QR-Code zu generieren, der Sie zur Download-Seite umleitet. Siehe dieses Bild.



b) QR-Code scannen, auf "Generate QR code" auswählen, der von Google Authenticator gescannt werden muss, wie in diesem Bild gezeigt.

## 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 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.

▶ Step 3: Enable Two-Factor Authentication

Return

c) Aktivieren Sie Zwei-Faktor-Authentifizierer, öffnen Sie Ihre Authentifizierungsanwendung in Ihrem Handy und geben Sie den Verifizierungscode ein. Wählen Sie Enable (Aktivieren) aus, um diesen Vorgang abzuschließen, wie im Bild gezeigt.

## 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

**Schritt 4:** Sobald er fertig ist, gibt er Ihnen einige Backup-Codes. Wählen Sie **In Zwischenablage kopieren**, um diese zu speichern, sehen Sie das Bild als Beispiel.

## 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

- 5c9a4c086
- f20ea706
- 7f1aeb53
- 44f50f0c
- 21e32ced
- 1e307301
- 42e2e109
- f56f3fde
- 7424df5f
- 2dafab11

Copy to clipboard

**Hinweis:** Jeder Sicherungscode kann nur einmal verwendet werden. Nachdem Sie alle Ihre Backup-Codes verwendet haben, müssen Sie zu dieser Seite zurückkehren, um neue Codes

zu generieren.

Weitere Informationen finden Sie im [Benutzerhandbuch zu AMP für Endgeräte](#).

Zusätzlich können Sie die [Konten](#) ansehen [und die Zwei-Faktor-Authentifizierung in AMP-Video aktivieren](#).