Two-Factor Authentication

Introduction to Two-Factor Authentication

Two Factor Authentication, also known as 2FA, two-step verification or TFA is a method of adding another layer of security for user verification by using a security identifier method in addition to username and password. It is generally something that only the actual intended user may possess and it is inherently separated from the original login method. Some examples include phone apps, SMS verification or keyfobs.

Recovering Access to Accounts Protected by Two-Factor Authentication

Two Factor Authentication (TFA) is an important security mechanism, and cannot be disabled by Cisco Meraki without positively identifying the account owner. There are two methods available to ensure access is not lost: a backup phone number (with SMS auth), and a list of one-time codes (with Google Authenticator).

The two methods above are the primary options for disabling or temporarily bypassing two-factor authentication. If these methods cannot be utilized for any reason, the only alternative is to provide proof of identity after contacting Cisco Meraki Technical Support. There are two methods to request removal of SMS and Google Authentication for TFA.

Method 1:

1. Open a case by emailing licensing@meraki.com.  
   - This email must be sent from the email address of the account TFA is to be disabled on.  
   - It must include the full name of the organization that the account resides in.
2. A second organization administrator must comment on the case through Dashboard granting approval to disable TFA on the account.  
   - Email or phone approval is not acceptable for this. The approval must come as a comment on the case.  
   - This permission can be granted only by an organization administrator with Full access.

Method 2:

Please note that 2FA removal requests cannot be resolved via our support phone lines. 2FA disablement needs to be requested and processed by the admin email that needs assistance via a Meraki case for security purposes. See steps on recovering access below.

This feature is currently only available in the United States and the United Kingdom. If you are in a different country, SMS authentication is still a beta feature, and we cannot guarantee its reliability. Please feel free to test your phone number on the set up page. SMS authentication has been known to work in the following additional countries: Canada, Mexico, France, Spain, Italy, and Germany.

Please note that 2FA removal requests cannot be resolved via our support phone lines. 2FA disablement needs to be requested and processed by the admin email that needs assistance via a Meraki case for security purposes.

Please note that 2FA removal requests cannot be resolved via our support phone lines.
Alternatively, if a second organization administrator with full access does not exist or is otherwise unavailable:

1. Open a case by emailing licensing@meraki.com.  
   - This email must be sent from the email address of the account TFA is to be disabled on.

2. Once in communication with a Cisco Meraki Support Specialist, explain that TFA needs to be disabled for the account and provide the requested documentation.

3. The Support Operations Specialist will request more information about the organization and its contents and settings to verify the validity of the request.

4. Once this step has been completed, a Cisco Meraki Support Specialist will provide you a document which must be signed, notarized, and mailed to Cisco Meraki Headquarters (address found below).
   ◦ When this is received by support, it will then be scanned and attached to the case before TFA is disabled.
   ◦ It is strongly recommended to send this letter with tracking, in case of postal issues.
   ◦ Unless otherwise specified by the Support Ops Team, use the following address format:
     Cisco Meraki- Support Operations  
     500 Terry A Francois Blvd  
     4th Floor, C/O [SUPPORT OPS SPECIALIST’S NAME]  
     San Francisco, CA 94158

---

## Setting up and Changing Phone Numbers

In order to change the phone number used for Two-factor authentication on the dashboard, follow these steps:

1. Log into the dashboard with a valid username and password.

2. Once logged in, locate the **My Profile** option on the dashboard. It is on the top right corner of the screen.

3. Click on **My Profile**.

4. Scroll down to the **SMS Authentication** section of the page.

5. Click **Edit** right next to the current registered phone number.

6. Enter the new phone number in the **Phone Number** field.

7. In the **Setup your phone** section, click on the **Send code** button. A code is sent to the new phone number.

8. Enter the code into the **Code** field and click the **Verify** button.

9. Click **Next**.

10. Optionally, enter a backup phone number. Click **Next**.

11. Confirm the information and click **Save changes**.

---

## Updating a 2FA Phone Number

Support cannot update the phone number being used. If you are unable to change the number because you no longer have access to the original/current number, then 2FA must be disabled following the steps outlined [here](#). You will then be able to update the phone number.
Using Two-Factor Auth with Client VPN

Cisco Meraki Client VPN incorporates several methods for authenticating users before they are allowed onto the network. For admins who want to incorporate an additional level of security, client VPN also allows for the use of third-party two-factor auth solutions, requiring users to go through a second authorization step.

Two-factor auth can be incorporated in one of two ways:

- Included as part of the authentication. Users are prompted for a username and password as normal but must provide additional information as required by the third-party solution (appending a key to the password, for example).
- A push notification, where an agent on a RADIUS server holds an accept message until the user pushes an 'accept' button or equivalent on their side. By default on the Meraki platform, the RADIUS session will time out after a short period of time. This may be too short a time span for some solutions, please contact Meraki Support if you need this timeframe extended.

Both of the above methods are compliant under the PCI DSS 3.0 standard, as two-factor security for remote access.

Additional Resources

For reference, the following sites outline examples of two-factor auth that may be used with client VPN:

- DuoSecurity: https://www.duosecurity.com/docs/radius

Using Google Authenticator for Two-factor Authentication in Dashboard

Administrators can require two-factor authentication for logging into Dashboard. One of the options available to users is the Google Authenticator. This service is useful because it can provide two-factor authentication regardless of SMS service.

Configuration

1. Download Google Authenticator onto your Smartphone by visiting your mobile app store and downloading the Google Authenticator app.
2. Edit the Dashboard Profile and Verify

3. Once the app is downloaded log into Dashboard and navigate to the My Profile page on the top right.
4. Find the Section labeled SMS authentication and select the appropriate hyperlink from the listed options. This example uses an Android device:

Two-factor authentication
Primary phone number       Edit | Remove
Backup phone number        It is recommended that you set up a backup number. Edit
SMS authentication is OFF.

You can also set up offline access on a mobile device Android, iPhone, or BlackBerry.

5. Add your Dashboard account to Google Authenticator as a token
   - On Google Authenticator, select the “+” button and tap the button "scan barcode".
   - Scan the second barcode on the Dashboard page. This is unique to your account and will sync a Google Authentication token to your login.
   - You should now see a new token on your authenticator. Notice that the token changes every 30 seconds. Check that the token is working by entering in the current, active token on the verify window on Dashboard.
6. Once verified, select Continue and then OK to turn on two-factor authentication.

Note: The Dashboard account will be logged out once OK is clicked.

Starting with the next login, the user will be prompted to enter the active verification code found on the authenticator.
Note: For China users that cannot access to Google Play to download Google Authenticator, Microsoft Authenticator is the alternative solution.

Refer to the below Meraki Community Post for the detail setup with Microsoft Authenticator.

http://cs.co/TFA