Two-Factor Authentication

Introduction to Two-Factor Authentication

Two-Factor Authentication (also known as TFA, 2FA, two-step verification, multi-factor authentication or MFA) is a method of adding another layer of security for user verification when connecting to Meraki Dashboard (or for client VPN users authentication). This is done by using a security identifier method in addition to a 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.

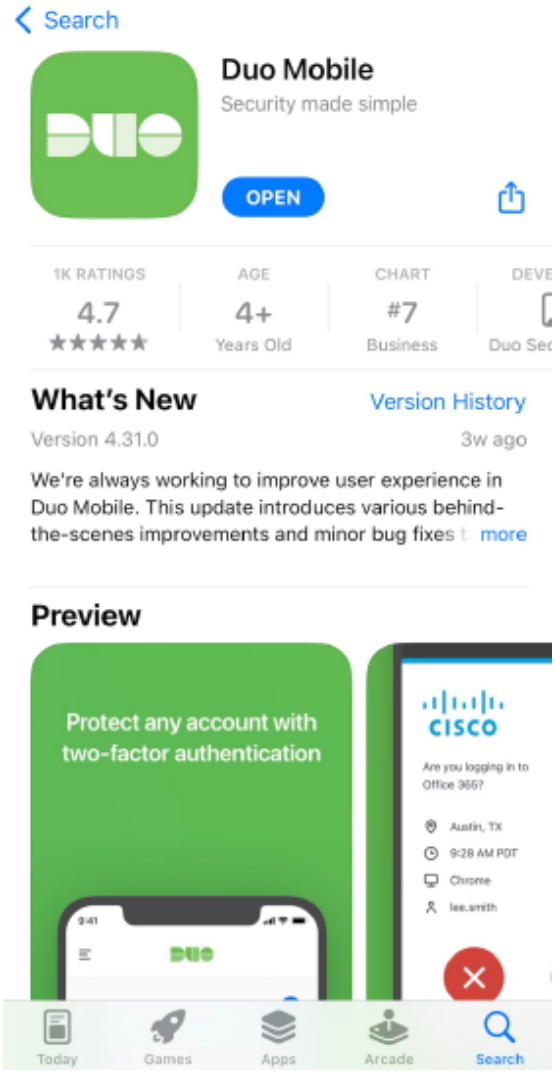
When Two-Factor Authentication is not enabled, the user will see a banner "Two-factor Authentication is not currently enabled on your Meraki Dashboard account. For an extra layer of security, we recommend enabling it at your earliest convenience." Clicking on the [x] button will *not* permanently remove the banner.

Using Duo Mobile for Two-Factor Authentication in Dashboard

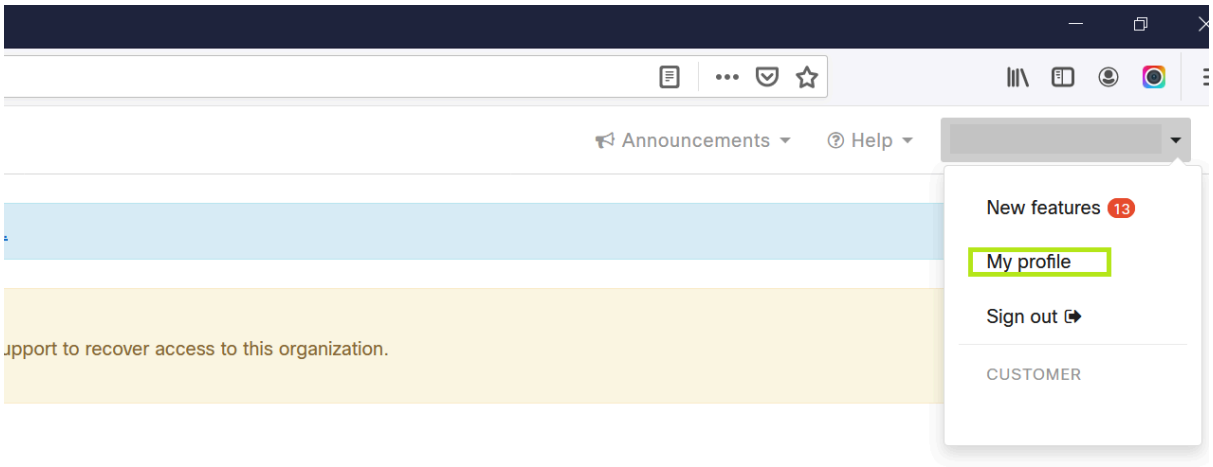
The option to utilize Duo Mobile on an iOS or Android device is useful because it can provide two-factor authentication regardless of SMS service. It also allows users to back up Duo-protected accounts for recovery to the same device or to a new device.

Configuration

1. Visit your smartphone's mobile app store and download the Duo Mobile app.



2. Once the app is downloaded, log into Dashboard and navigate to the **My Profile** page on the top right.



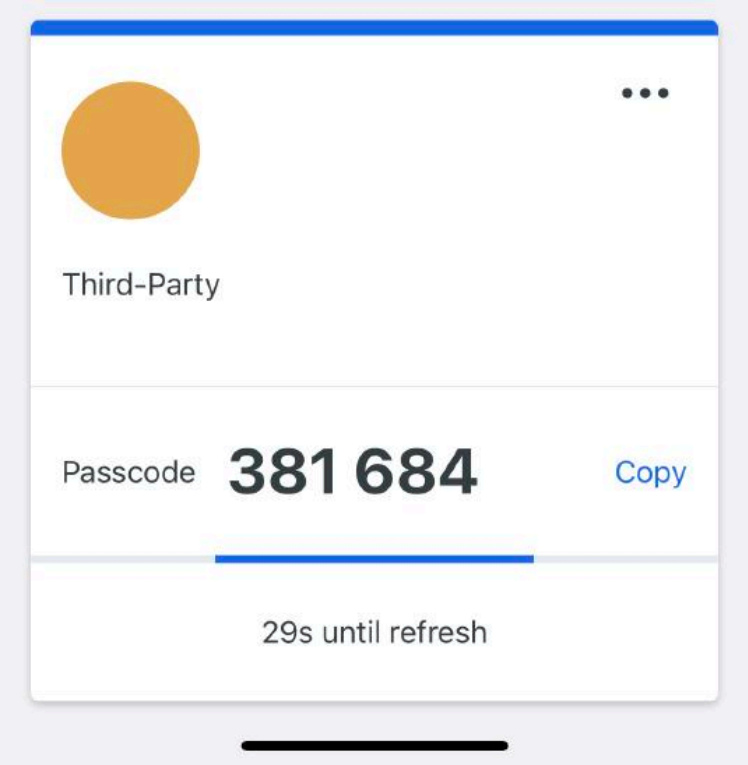
4. Scroll to the Section labeled **Two-factor authentication**
5. Click **Set up two-factor authentication**.
6. On the next page, under **Set up app,** follow the steps listed to add your Dashboard account to Duo Mobile as a token.
7. Check that the token is working by submitting the current, active token into the **Code** field under **Verify your device** on Dashboard.

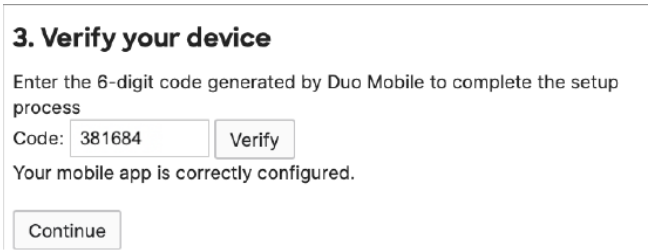
Notice that the token changes every 30 seconds.

Example (iOS):

On the Phone

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, you will be prompted to enter the active verification code found on the authenticator.

> Note: It is recommended that Duo Mobile users enable Duo Restore (iOS, Android). This will allow for easy account recovery to the same device or a new device.

> Note: If it is needed to change the authenticator app after setup, you will need to first Disable Two-factor authentication then start the Configuration again.

One-Time Backup Codes

After configuring two-factor authentication, it is highly recommended to take note of the eight provided backup codes. These codes can be used to access your account in the event the configured method of authentication is not possible (such as your mobile device getting damaged or lost). Please take note of these codes in a secure manner.

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 **Two-factor authentication** section of the page to find your **One-time codes** (in a numbered list; one through eight).

> As the name suggests, these codes may be used only one time each. You may click **Generate a new set of one-time codes** at any time to refresh the eight codes. Any unused codes from the previous set will be void at that time.

Using SMS for Two-Factor Authentication

> This feature is currently only available in the United States. 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: United Kingdom, Canada, Mexico, France, Spain, Italy, and Germany.

Configuration

In order to set up a phone number 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 **Two-factor authentication** section of the page.
5. Click **Set up two-factor authentication** (or **Enable SMS**, if an authenticator app is already configured).
6. On the next page, scroll to **Use SMS authentication instead**.
7. In the **Setup your phone** section, enter your phone number in the **Phone Number** field as directed.
8. Under Test your phone, click on the **Send code** button. A code is sent to the phone number submitted in the previous step.
9. Enter the received code into the **Code** field and click the **Verify** button.
10. Once the phone number has been successfully configured, click **Next**.
11. *Optionally,* enter a backup phone number. Click **Set backup**.
12. Click **Next**.
13. Confirm the information and click **Turn on SMS authentication**.
14. You will be prompted to verify your password to finalize the process.

Changing/Updating 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 **Two-factor authentication** section of the page.

5. Click **Edit** right next to the current registered phone number (Primary or Backup).
6. In the **Setup your phone** section, enter the *new* phone number in the **Phone Number** field.
7. In the **Test 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 (RECOMMENDED). Click **Set backup**.
11. Click **Next**.
12. Confirm the information and click **Save changes**.
13. You will be prompted to verify your password to finalize the process.

Meraki 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 TFA must be disabled following the steps outlined here. You will then be able to update the phone number once you have regained access.

Using Two-Factor Authentication 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.

Client VPN does not natively support two-factor auth, a third-party solution is required for this configuration. As such, please refer to your two-factor auth solution's documentation for additional information and troubleshooting.

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

1. 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).
2. 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.

Client VPN does not support the use of xauth, two-factor auth solutions that use xauth are not supported.

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
- RSA SecurID: http://www.emc.com/security/rsa-securid/index.htm

Disabling Two-Factor Authentication

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 **Two-factor authentication** section of the page.
5. Click **Turn off two-factor authentication**.
6. You will be prompted to verify your password to finalize the process.
7. Furthermore, you may select **Remove** next to your previously established phone number(s) so it will not be saved for future configuration.

The organization-wide security configuration "Force users to set up and use two-factor authentication" overrides the ability for individuals to disable TFA on their accounts. In order for an individual to complete the process of disabling TFA, this configuration must be disabled from every organization their account is associated with.

Note: disabling this organization-wide security configuration change will *not* disable TFA for any users. Likewise, *re-enabling* the organization-wide security configuration will force everybody in the organization to follow the policy (both new administrators and existing administrators who temporarily disabled their individual TFA).

If you are unable to disable TFA because you no longer have access to the original/current phone number, Meraki Support may assist after following the steps outlined here.

Recovering Access to Accounts Protected by Two-Factor Authentication

Meraki offers two ways to ensure access to a TFA-protected account is not lost: the option to configure a backup phone number (available for SMS authorization), and a list of one-time codes to use in place of a TFA code (available for both SMS authorization and Duo Mobile). These two methods should be treated as the primary troubleshooting steps to temporarily bypass two-factor authentication and regain access to an account.

Note: It is recommended that Duo Mobile users enable Duo Restore (iOS, Android). This will allow for easy account recovery to the same device or a new device.

If the above solutions are not possible, the only alternative is for Meraki Support to disable the account's TFA configurations so the user can regain access. Since TFA is an important security mechanism, Meraki Support will not disable the configuration without first positively identifying the account owner.

Please note that 2FA removal requests **cannot** be resolved via our Support phone lines.

For security purposes, a Meraki Support case requesting 2FA disablement must be open from the Meraki Support Home page under the 'No dashboard Access?' section.

The organization-wide security configuration "Force users to set up and use two-factor authentication" overrides Meraki Support's ability to disable TFA for an individual user. In order to complete the process of disabling TFA for the individual, this configuration must be disabled from every

organization the account is associated with.

Note: disabling this organization-wide security configuration change will not disable TFA for any users, it will merely provide Meraki Support the ability to manually disable TFA for the locked-out account.

There are two methods to verify account ownership for the account recovery process:

Method 1

1. Open a case from the Support home page.
   - This email must be the email address of the account TFA is to be disabled on.
   - The case 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 in question.
   - Email or phone approval is **not** acceptable for this. The approval must come as a comment on the case.
   - This permission may be granted by an organization administrator with Full access, and SAML administrators with Full access. Approval by network administrators or administrators with read-only access will not be accepted.

Dashboard organizations should always have **at least two organization admins with full permissions**. This is best practice in case one account is locked out or if access to that account's email address is lost.

Method 2

If a second organization administrator with full access does not exist or is otherwise unavailable, please proceed with this method of verification.

1. Open a case from the Support home page.
   - This email **must** be the email address of the account TFA is to be disabled on.
   - The case must include the full name of the organization that the account resides in.
2. The Support Operations Specialist will request more information about the organization and its contents and settings to verify the validity of the request.
3. The Support Operations Specialist will request documentation to further prove ownership of the account, organization, and its contents.
4. Once verification has been completed, the Support Operations Specialist will provide you with a digital Docusign document. Please fill it out, sign digitally, and return it by attaching it to the support case.

Once one of the above methods has been finished, TFA may then be disabled.