Clearlogin - Multi-factor Authentication

In This Article

Overview

Multi-factor Authentication (MFA) refers to having multiple types of evidence (or factors) to verify a user signing into a website, application, or other resource. These factors include, but are not limited to:

- Something the user knows: Password, Security Question, PIN
- Something the user owns: Computer, Mobile Phone, USB Key, Access Badge or FOB
- Something the user is: Voice Recognition, Fingerprint, Facial or Retina Scan

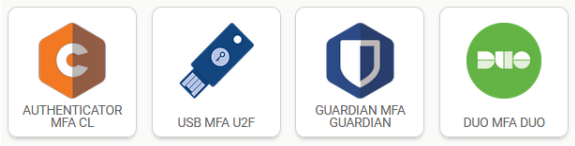
Additionally, a user's location or time of day can be used as factor for signing into a resource.

MFA Provider

An MFA provider is a service that supports MFA processes. Clearlogin is an MFA provider, it supports multiple types of MFA processes, and also has an MFA Authenticator app for Android and iOS. In addition to be an MFA provider, Clearlogin also supports the Cisco Duo MFA provider service.

Enable MFA in Clearlogin

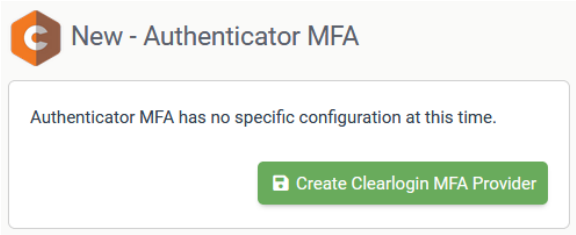
- Log into the **Admin Portal:** https://admin.clearlogin.com
- In the left-hand navigation bar, browse to: **Security** > **Multi-Factor Authentication (MFA)**
- Click on the MFA provider you wish to enable, and follow the below instructions for the provider you enable.



- If you have already enabled an MFA provider, click on the **New MFA Provider** button.

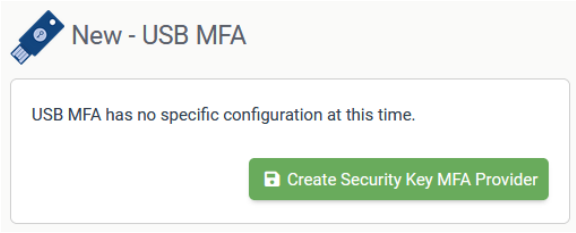
Expand to view the instructions for the MFA Provider you enabled.

- Clearlogin Authenticator MFA doesn't have any configuration steps. Just click on the **Create** button to enable it.



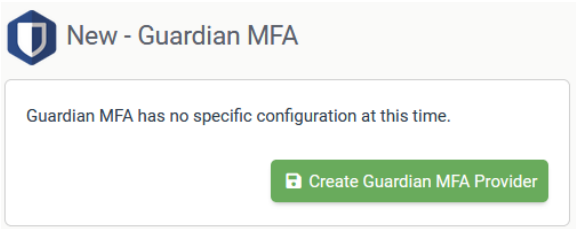
Clearlogin USB U2F (Universal 2 Factor) MFA requires a U2F USB device, and the latest version of Google Chrome or Mozilla Firefox. Apple does not currently support this standard with Safari, and the same is true with Microsoft Edge.

- Clearlogin USB U2F MFA doesn't have any configuration steps. Just click on the **Create** button to enable it.



> For information on how to configure a USB key with Clearlogin, refer to the **U2F USB Keys** article.

- Clearlogin **Guardian MFA** doesn't have any configuration steps. Just click on the **Create** button to enable it.



> For more information on how to use Clearlogin's **Guardian MFA** service, refer to the **Guardian MFA** article.

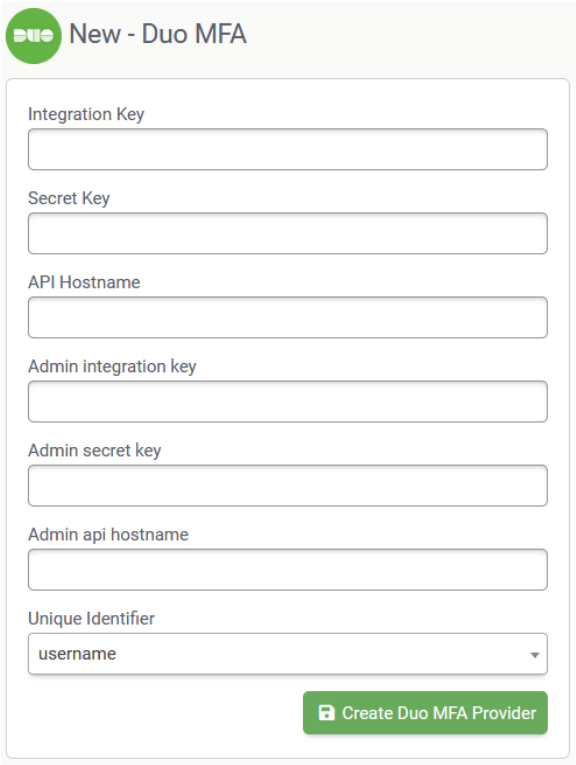
Before you enable Cisco Duo MFA, you will need to sign into your Duo admin portal and create an Auth API application:

- Sign into your Duo Admin Portal: https://admin.duosecurity.com
- Select **Applications** in the sidebar
- Click on **Protect an Application** and locate the entry for **Auth API** in the **applications** list.
- Click **Protect** to the far-right to configure the **application** and get your integration key, secret key, and **API** hostname.

- In Clearlogin, click the **DUO MFA** button to enable the Cisco Duo MFA provider.

- Enter the required configuration items and then click the **Create** button.

Integration Key	< Paste this in from the Duo admin portal >
Secret Key	< Paste this in from the Duo admin portal >
API Hostname	< Paste this in from the Duo admin portal >
Admin Integration Key	
Admin Secret Key	
Admin API Hostname	
Unique Identifier	This is the unique identifier used to match your Clearlogin users to your Duo users. If you were to select **username** we will use the Clearlogin username (eg. admin@clearlogin.com would be 'admin')



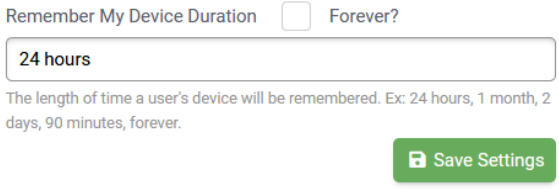
More MFA Settings

Here are some additional steps to take after enabling an MFA provider.

Remember My Device Duration

- Log into the **Admin Portal:** https://admin.clearlogin.com
- In the left navigation bar, browse to: **Security** > **Multi-Factor Authentication** > **Remember My Device Duration** (right side bar)

This determines the length of time a user's session will remain active before they are prompted to re-authenticate with MFA again. Default is 24 hours.



Enable MFA in Access Rules

- Log into the **Admin Portal:** https://admin.clearlogin.com
- In the left navigation bar, browse to: **Security** > **Access Rules**
- In the Multi-Factor Authentication (section) of each access rule, choose the MFA option for the users that match the rule. The choices vary based on which MFA providers are enabled.

> If you want to give your users the ability to choose more than one MFA provider when they login, create additional access rules with each MFA provider.

Multi-Factor Authentication (MFA)

Not Required

Select the Multi-Factor Authentication provider you wish to use for this rule, if any. If none are available you can configure MFA providers here.

Option	Description
Not Required	This is the default option, and this will not force the user to use MFA when logging in.
One-Time Password	Choose this option when you want your users to be prompted to enter a one-time passcode from an authenticator app (Microsoft Authenticator, Google Authenticator, etc.)
USB Key	Choose this option when you want your users to be prompted to use their U2F hardware USB key.
DUO	Choose this option when you want your users to be prompted to use their Cisco Duo account.
Guardian	Choose this option when you want your users to be prompted by the Guardian MFA feature.

MFA Open Enrollment

- Log into the **Admin Portal:** https://admin.clearlogin.com
- In the left-hand navigation bar, browse to: **Settings** > **Login**

Setting	Description
Disable MFA Open Enrollment	Select to turn off MFA open enrollment. Open enrollment allows any user to enroll in MFA at their own discretion. Enabling this will not disable MFA enrollment when it is made a requirement in an access rule. • Enabled • Disabled (default)