How to Set Up and Manage Multi-Factor Authentication in Barracuda Cloud Control

https://campus.barracuda.com/doc/69960198/

Multi-factor authentication (MFA), also known as two-factor authentication, is a security feature that requires two forms of authentication to access Barracuda Cloud Control. When enabled, MFA provides an extra layer of security to your account.

For security purposes, Barracuda recommends that users lock their MFA-enabled devices with a personal identification number (PIN).

By default, MFA is optional. The account administrator can specify whether MFA is required for all users on a Barracuda Cloud Control account:

- **Required, all users on an account** – MFA is set to **Required** on the **Home > Admin > Options** page; all users on the account are required to enter a secondary token in addition to their login credentials.
- **Optional** – MFA is set to **Optional** on the **Home > Admin > Options** page; users on an account can select whether they want to use MFA using the settings on their **Home > My Profile** page.

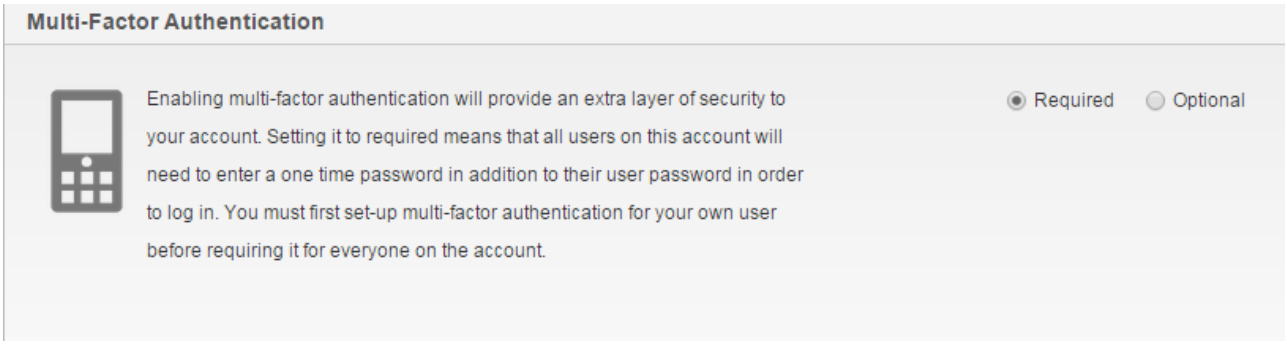
  To disable MFA when it is optional, a user must delete all of their MFA devices from the **Multi-Factor Authentication** section on their **My Profile** page.

Set MFA to Required for all Users (Account-Wide)

After the account administrator sets MFA to required and clicks **Save**, they are immediately redirected to the MFA set up page if they have not yet configured an MFA device.

Use the following steps to set MFA to **Required**:

1. Log into Barracuda Cloud Control as the administrator on the account: https://login.barracuda.com/
2. Cick **Options**.
3. In the **Multi-Factor Authentication** section, click **Required**:



4. Click **Save**. All users belonging to this account (or accounts that administer it) are now required to log in using MFA.
   If MFA is not yet enabled for the current admin user, the user is immediately taken to the MFA setup page. If a Barracuda Partner account has access to a customer account where MFA is required, the Partner users are required to have MFA set up.

MFA Required User Login

When MFA is enabled, users receive an email notification. When the user logs in, they must complete the following steps:

1. Log into https://login.barracuda.com/ using your login credentials, and click **Sign In**.
2. The user is then presented with the secret code on the MFA set up page.
3. Copy the **Secret Code**, or using your authentication tool on your mobile device, scan the code. A one-time login token, known as a time-based one-time password (ToTP), generates.
4. Enter the ToTP on the login page, and click **Continue**. The user is logged into Barracuda Cloud Control.
5. The user is now required to enter a password and ToTP upon subsequent log in.

User-Enabled MFA

When MFA is set to optional, users can select to log in using MFA. For more information, refer to Adding MFA Devices in Barracuda Cloud Control.

Figures