

How to Add Multi-Factor Authentication Devices in Barracuda Cloud Control

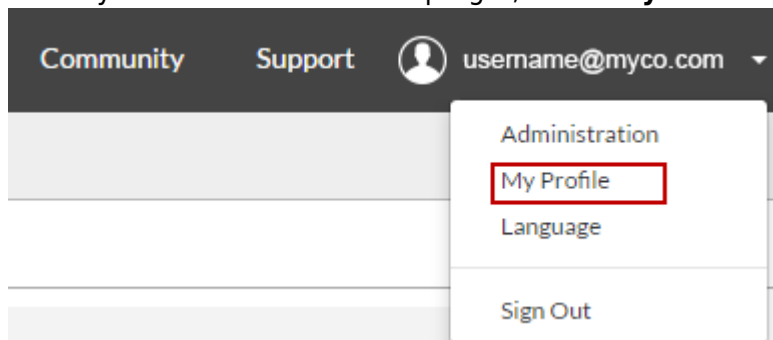
<https://campus.barracuda.com/doc/9517/>

When multi-factor authentication (MFA) is set to **Required** by an account administrator, users are sent an email to inform them that they are required to use MFA. Users can add multiple MFA devices for logging into Barracuda Cloud Control. For example, a user may have one secret code for their phone, and another for their tablet. When multiple devices are added, a user need only enter a time-based one-time password (ToTP) from one of the devices to log in. MFA becomes required for a user when logging in as soon as they add an MFA device. If MFA is optional, a user can delete all of their devices to disable MFA, however, if MFA is required, a user cannot delete their last MFA device.

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

Use the following steps to add and configure a device for Multi-Factor Authentication in Barracuda Cloud Control:


1. Log into Barracuda Cloud Control: <https://login.barracuda.com/>
2. Under your username on the top right, select **My Profile**.




3. In the **Multi-Factor Authentication** section, click **Add New Device** ; the **Add New Multi-Factor Authentication Device** page displays:

Add New Multi-Factor Authentication Device

To enable multi-factor authentication for your account:
Scan the QR code or enter the secret into your Barracuda Mobile or other multi-factor app, then enter the one-time authentication token provided.

Secret Code: 




Device Name:

MFA Code:

[Cancel](#) [Save](#)

4. Either scan the QR code, or enter the secret code into the authentication tool on your mobile device, and then click **Save**.
5. The device is added to the **Multi-Factor Authentication** section:

Device Name	Date Added	Options
skAndroid 	2014-03-21 03:43:34	Delete
		Add New Device

When setting up MFA for your device(s), Barracuda Networks strongly recommends configuring a second device as a backup in the event your primary device is lost, stolen, or replaced.

As an alternative, when configuring your primary device for MFA, you have the option to generate five one-time use passwords. Remember to store the passwords in a safe location.

Multi-Factor Authentication



Multi-factor authentication is enabled for your account. You may add more MFA devices. To disable MFA, you must delete all devices.

Device Name	Date Added	Options
testdev 	2023-04-24 09:32:08	<input type="button" value="Delete"/>
<input type="button" value="Add New Device"/>		

Generate One-Time Use Authentication Tokens

You may generate five, one-time use passwords. These are used in place of an authentication code in case you need to log into your account and your MFA device is lost. Once generated, copy or print them and store in a safe place. The passwords must be used in order from first to last.

Click "Generate" to create one-time passwords.

If you are unable to authenticate using the above options, contact [Barracuda Networks Technical Support](#) to reverify your credentials and restore access.

Figures

1. my_profile.png
2. add_new_device.png
3. new_device.png
4. MFACodes.png

© Barracuda Networks Inc., 2026 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.