How to Remove Multi-Factor Authentication Devices from Barracuda Cloud Control

https://campus.barracuda.com/doc/69960204/

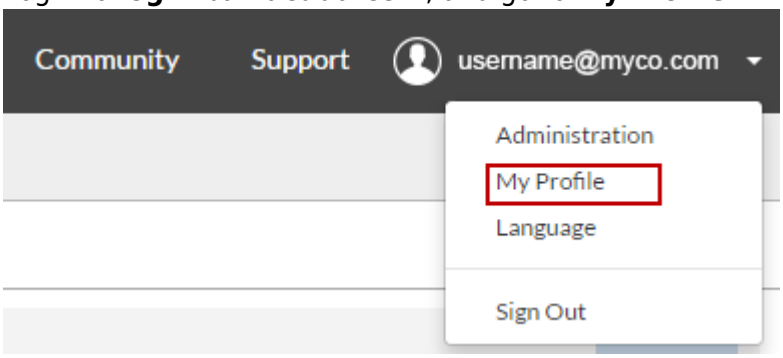
If multi-factor authentication (MFA) is enabled, and a user loses or breaks a device with the MFA secret associated with it, there are three ways to reset the secret associated with the MFA device:

1. If the user has an additional MFA device set up, they can log in with the secondary device and remove the MFA secret associated with the lost MFA device.
2. If the user does not have a secondary device, or if they cannot log in and remove the MFA secret, the account administrator can reset MFA for the user for use on a new device, however, *this removes all MFA devices the user has set up.*
3. If the user has saved one-time use passwords, these can be used to log into the account. Each code can be used only once, and they must be using in the order printed.

A. Reset MFA from a Secondary Device (User)

Use the following steps to log in with a secondary device and remove the MFA secret associated with the lost MFA device:

1. Log into **login.barracuda.com**, and go to **My Profile**.



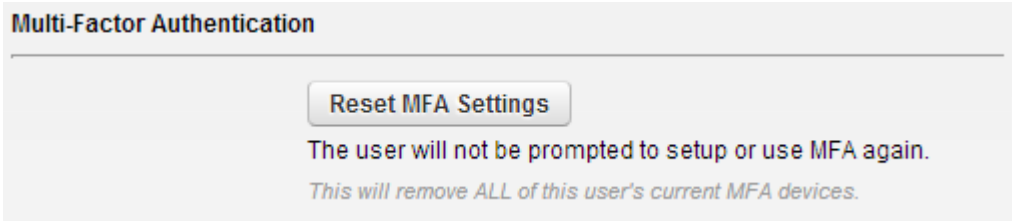
2. In the **Multi-Factor Authentication** section, click **Delete** in the **Options** field for the lost device.
3. In the **Delete MFA Device** dialog, enter the authentication code from any other MFA device, and then click **Delete**.

B. Reset MFA for a User from Account Administrator Role

Use the following steps to reset the MFA secret:

1. Log into **login.barracuda.com** as the Account Administrator.

2. Navigate to the **Home > Admin> Users** page.
3. Click on the name of the user.
4. In the **User Details** section, click **Reset MFA Settings**:



5. A confirmation dialog displays:

6. Click **OK** to confirm your selection.
7. An email notification is automatically sent to the user notifying them that the MFA devices have been reset.
    - If MFA is optional for this user account, the user can to log in with only a username and password. They must add a new MFA device on the **My Profile** page to re-enable MFA.
    - If MFA is required for this account, the user can initially log in with only a username and password, and will then be redirected to the MFA set up page where they can add a new MFA device. Thereafter the user must log in with their username, password, and authentication code.

C. Log in Using One-Time Use Passwords

Use the following steps to log in with a secondary device and remove the MFA secret associated with the lost MFA device:

1. Log into **login.barracuda.com**, and enter one of the codes from your list of one-time use passwords that you printed from the **Multi-Factor Authentication** section of the **My Profile** page after setting up MFA.
2. Go to the **Home > My Profile** page.
3. Click **Add New Device**; the **Add New Multi-Factor Authentication Device** page displays.
4. Either scan the QR code, or enter the secret code into the authentication tool on your mobile device, and then click **Save**.
5. In the **Multi-Factor Authentication** section, click **Delete** in the **Options** field for the lost

device; the **Delete MFA Device** dialog displays.

6. Enter the MFA code from the just added device, and then click **Delete** to confirm your selection.

Figures

1. my_profile.png
2. mfa_admin_reset.png
3. are you sure.png

© Barracuda Networks Inc., 2019 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.