

## BCC Mobile App for iOS and Multi-Factor Authentication

<https://campus.barracuda.com/doc/69960194/>

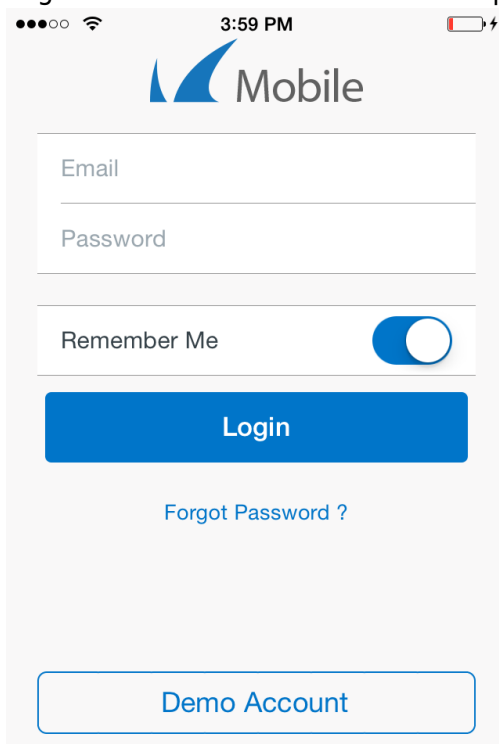
BCC Mobile Apps are now deprecated. They are no longer available for download and are no longer supported. If you already have one of the mobile apps installed, you can continue using it.

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. Use the Barracuda iOS Mobile App to generate a secondary authentication token. For more information, refer to [Understanding Multi-Factor Authentication in Barracuda Cloud Control](#).

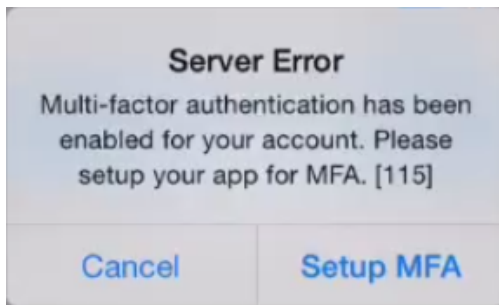
### Initial Setup

Use the following steps to set up the Barracuda iOS Mobile App to generate a secondary authentication for Barracuda Cloud Control account MFA:

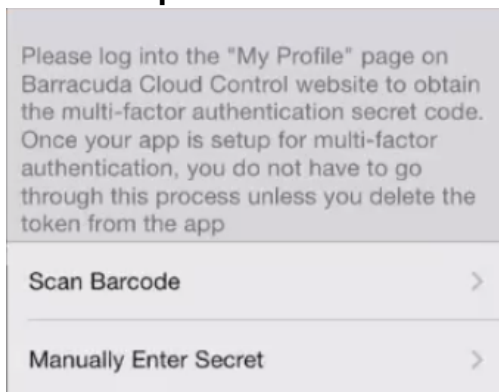
1. Log in to the Barracuda iOS Mobile App on your mobile device:



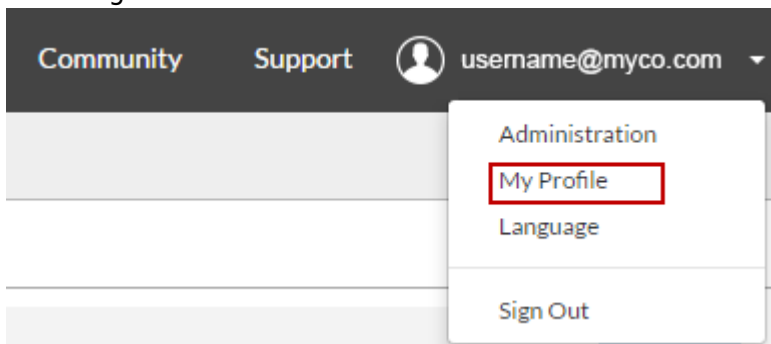
2. The first time you log in after MFA is enabled on your Barracuda Cloud Control account, a Server Error message displays:



3. Click **Set Up MFA**. The **Multi-Factor Auth** page displays:



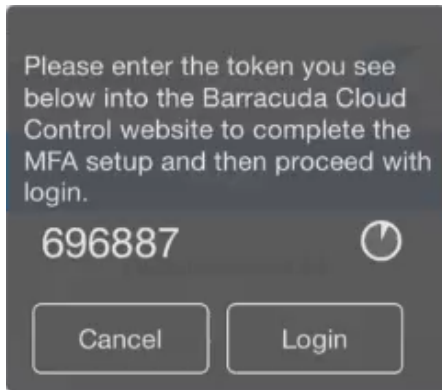
4. On your desktop system, log in to your Barracuda Cloud Control account, go to the **Home > My Profile** page, and go to the **Multi-Factor Authentication** section. Set up MFA using one of the following methods:



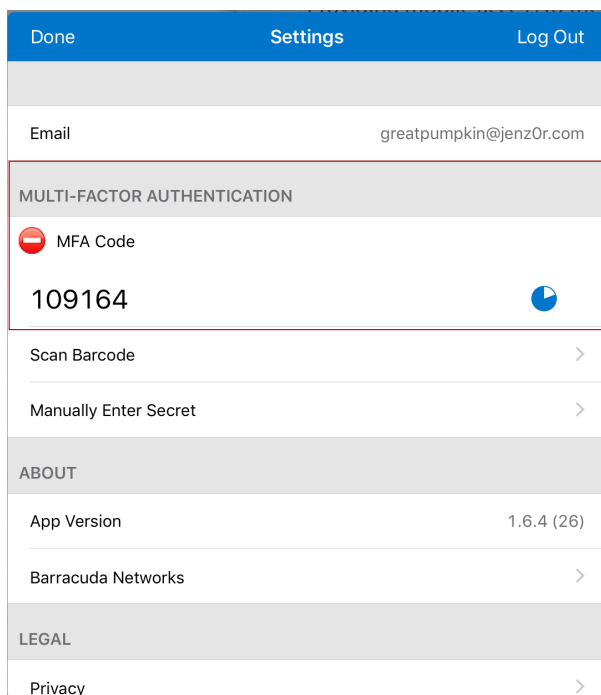
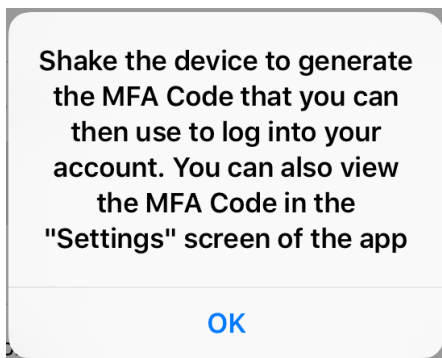
- **Scan Barcode**
- **Manually Enter Secret**

#### Scan Barcode Method

1. Tap **Scan Barcode**, and using your iOS device, scan the barcode presented in the **Home > My Profile > Multi-Factor Authentication** section on your desktop system.
2. Once you successfully scan the barcode, the token is generated:

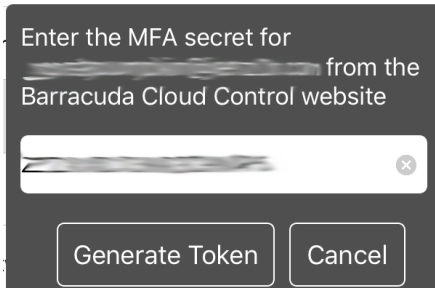


3. Enter the generated token into the associated field in the **Home > My Profile > Multi-Factor Authentication** section.
4. After initial setup, just shake the iOS device to generate a new token to log in to your Barracuda Cloud Control account:



## Manually Enter Secret Method

### 1. Tap **Manually Enter Secret**:

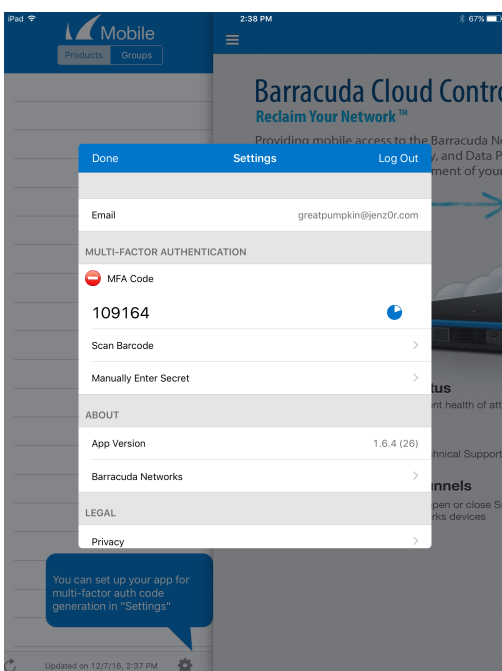


2. Enter the secret code found in the **Home > My Profile > Multi-Factor Authentication** section into the iOS device, and then tap **Generate Token**.
3. Enter the generated token into the associated field in the **Home > My Profile > Multi-Factor Authentication** section.

Note that when you log out, the token remains. Users can shake the device even when logged out of the application to get a list of MFA tokens configured through the application.

## Access token / Change MFA Settings


In addition to generating the token by shaking your iOS device, you can also access the token on the **Settings** page on your device. Additionally, if at any point you need to reset token generation on the device, select the desired method from the **Settings** page, and complete the onscreen instructions:

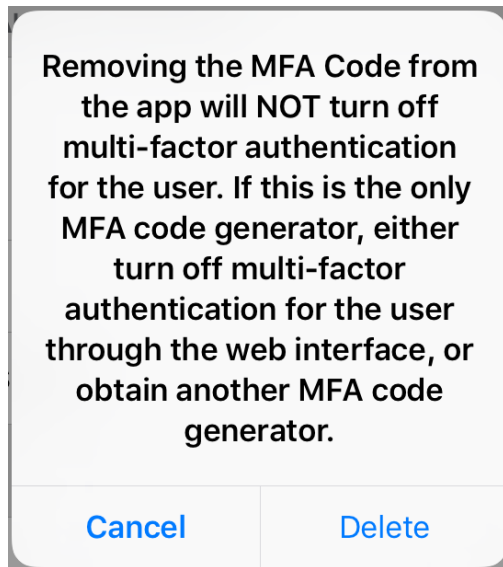


---

## Delete Token

---

If you want to delete the token from the iOS Mobile App, tap the delete icon (  ). You are presented with a warning message:



## Figures

1. iphone\_login.PNG
2. set\_up\_mfa.png
3. barcodeORmanual.png
4. my\_profile.png
5. tokengeneration.png
6. ipadShakeCrop.png
7. ipadCodeToEnterCrop.png
8. ipad\_generateTokenCrop.png
9. ipadCodeToEnter.png
10. deletelcon2.png
11. ipad\_delete\_crop.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.