Using Multi-factor Authentication in Barracuda RMM

https://campus.barracuda.com/doc/98216886/

With Barracuda RMM 12 Service Pack 6, new features were added to increase your user security further. The inclusion of Multi-Factor Authentication (MFA) was on our overall roadmap. We have availed three options: authentication app (typically on a mobile device), email authentication and SMS text authentication . This article will address some of the concerns we have heard from partners concerning these processes.

The need to verify an email address that has been set up for months (if not years) in Barracuda RMM

This has caused some confusion, and we apologize for that, as the verification was set up for two distinct reasons. The first is that emails were never required to be verified for login to Barracuda RMM, it was simply a "fire and forget" setup. Equally, emails could be shared among many logins or could have been bogus emails entirely. With Barracuda RMM 12 SP6, this was changed to require a unique email address per login and those email accounts are required to be able to receive emails to verify.

We do not want to use multi-factor authentication to log in to Barracuda RMM

We understand that some partners (and their clients) may not be receptive to this change. This was a vital security decision to ensure that the data of each partner (and their clients) remains secure. We at the Barracuda RMM support team understand this can cause some brief trials and tribulations. Still, our development team implemented Multi-factor Authentication to safeguard you and your clients in an ever-aggressive world of security threats.

My chosen authenticator app code is not working on my mobile device

This common issue is fixed by updating your settings for your time on your mobile device. It is most often caused by users setting up the time on their mobile device in the following ways:

- Using the wrong timezone for the user's phone and geographical location
- Manually setting the time rather than using the automatic timing server according to the phone manufacturer or service provider
- Use of a third-party app on their mobile for the time that changes the timing

Any changes to the timing on a mobile device can cause issues with MFA not only in Barracuda RMM but any other MFA-utilized logins. If MFA is off by even a few seconds, users might not be able to log in.

Please Note

While Barracuda RMM uses several authenticator apps to be able to generate codes for MFA, we do not support the functionality of said devices nor the apps themselves.

We do not want to use a mobile app for authentication

While you cannot disable MFA from a user account, each account can be set up to use a mobile app or email verification. To set up email verification, you must first verify the email address on that given account. To change the account to use email verification, please do the following:

- Log into your Barracuda RMM Dashboard
- Navigate to **Configuration**
- Click on **User Management**
- Select the **User** you want to change settings for
- Under the **Profile**, you can **change the Multi-Factor Authentication Option**
    - **Email**
        - On login, an email will be sent to the defined account in the user profile with a code
        - *The email will come from the configured email in Configuration > System Settings > Alert Configuration*
    - **Mobile**
        - On login, a text message will be sent to the defined phone number in the user profile with a code
        - *The text can be, at times, delayed due to AWS API experiencing some issues*
        - Additionally, some partners have expressed that some carriers at times are not permitting the text through

Which MFA should I use?

From time to time, the Barracuda RMM Support team is asked which MFA option is the one we recommend. While we believe that the choice is up to the individual user and partner, we recommend using the MFA Authentication App on a mobile device as the most secure option. As for which app specifically, that is up to individual preference, and we do not recommend one over another.

Email verification sends a blank code

While this can be frustrating, we have seen a small handful of users experiencing this issue. We ask that you collect the following information for the Barracuda RMM support team so that we can fix this so you are able to log in:

- **Are you Cloud-Hosted or On-Premise?**
  - If the URL you are using to log in includes xxxx.mw-rm.barracudamsp.com, then you are cloud-hosted
- If cloud-hosted, **which cloud is your environment hosted on**
  - The first part before mw-rm will be the cloud (be that us01, eu03, au02, etc.)
- **VAR Domain** used to log in
- **User account login name**
- **User email address for that account**

Once you have this information, please get in touch with the Barracuda RMM support team, and we will be able to assist and set up the email code for you.