Best Practices for Barracuda RMM Credentials

https://campus.barracuda.com/doc/98217312/

From time to time, the Barracuda RMM Support team is asked for basic best practices when it comes to securing an environment. This article will address some of the most commonly asked questions and concerns.

Discourage users from using common passwords

Many users (and administrators) tend to use certain common passwords that are easy to remember. Malicious actors can easily crack these common passwords.

You may wish to distribute a list of common passwords to your users to discourage users from using them: https://en.wikipedia.org/wiki/List_of_the_most_common_passwords

Force users to use complex passwords

Complex passwords are harder for malicious actors to crack. Passwords that contain only alphanumeric characters are easy to discover with several publicly available tools. In Barracuda RMM, you can enforce password length and require that passwords include alphanumeric and special characters.

In Barracuda RMM 11 SP3, default password requirements were updated to require passwords 8 characters or longer, but existing passwords were not affected. New passwords, including changed and reset passwords, are required to be 8 characters or longer.

We recommend requiring existing users with simple passwords to create complex passwords by changing requirements and forcing password resets.

To enforce complex passwords

1. In Service Center, click **Configuration** > **User Management**.
2. Click **Global Account Settings**.
3. Under **Password Settings**, do the following:
    - Click the **Password minimum length is X characters** check box and type a minimum length.
    - Click the **Enforce alphanumeric passwords** check box.
    - Click the **Enforce special characters in passwords** check box.
4. Click **Save**.

5. Follow the To reset the password for a user account procedure below for the new requirements to take effect.

Force user passwords to expire

The longer a password exists, the higher the chance it will be compromised by a brute force attack, by an attacker gaining general knowledge about the user, or by the user sharing their password. Configuring passwords to never expire so that users are never required to change their passwords is a major security risk, allowing malicious users to use compromised passwords for as long as the valid user has authorized access.

On the other hand, the more often you force users to change passwords, the more likely they are to use a password that is easy to remember—likely on the list of common passwords or a reused password. Experts suggest a password expiry requirement of 180 days.

Users reusing the same passwords is an important concern in any organization. Many users want to recycle one or more passwords for their accounts. The longer a single password is used, the higher the likelihood of it being cracked by:

- brute force attack
- by an attacker gaining general knowledge about the user or social engineering/phishing
- or by the user sharing the password

If users are required to change their password, but they can recycle an old password, the effectiveness of a good password policy is reduced. Experts recommend preventing users from reusing the previous 6 passwords.

To set a password expiry requirement and keep a history of previous passwords

1. In Service Center, click **Configuration** > **User Management**.
2. Click **Global Account Settings**.
3. Under **Password Settings**, do the following:
4. Click the **Password expires after X days. Send notification X days before password expires** check box. Type the number of days the password is valid and number of days before expiry to email the user a notification.
5. Click the **Keep a history of X passwords** check box, then type the number of passwords to keep in the history.
6. Click **Save**.
7. Follow the *To reset the password for a user account* procedure below for the new requirements to take effect.

To reset the password for a user account

Resetting the password for a user sends that user an email that allows them to reset their password with no other intervention from an administrator.

1. In Service Center, click **Configuration** > **User Management**.
2. Click the name of the user account you want to reset the password for.
3. If the account is locked, clear the **Account is locked out** check box.
4. Click **Reset Password**.
5. Click **OK**.
6. Click **OK**.
7. Repeat steps for each user you want to reset their password.

Enable multi-factor authentication

For an additional level of security, administrators can enable multi-factor authentication for accounts.

Users with multi-factor authentication enabled are required to use a TOTP authentication app on their mobile device to generate an additional passcode to log in to Barracuda RMM. Any TOTP authentication app can be used, but the suggested apps are:

- Google Authenticator
- Microsoft Authenticator
- LastPass Authenticator
- Authy

To enable multi-factor authentication on user accounts

1. In the Service Center, click **Configuration** > **User Management**.
2. Do one of the following:
   - Select the checkboxes of the user accounts you want to enable multi-factor authentication on.
   - Select the checkbox in the table header to enable multi-factor authentication on all accounts.
3. Click **More Actions**, then **Enable multi-factor authentication**.
4. Click **Save**.

> You can also enable multi-factor authentication by selecting the Enabled check box on the Profile tab of the Modify User page of a user's User Configuration page.

Keep Barracuda RMM Up to Date

At Barracuda, we continually add security features to Barracuda RMM. To take advantage of these security features, keep your Service Center, Onsite Managers, and Device Managers up to date.

For example, all components of MW support TLS 1.2. Ensuring your Service Center, Onsite Managers, and Devices Managers are MW 11 SP4 or higher allows you to disable weaker protocols like TLS 1.0 on your Service Center Server, hardening your security and ensuring clients are communicating with stronger encryption protocols.

To update Service Center, see this page.

To update Onsite Managers and Device Managers:

1. In Service Center, click **Update Center** > **Products**.
2. Click the check boxes of the sites you want to upgrade.
3. Click the **Advanced Options** button.
4. Click the following check boxes:
    - **Update Onsite Managers for selected sites**
    - **Update Device Managers for selected sites**
5. Click the **Update** button.