What's New in Barracuda RMM 11 Service Pack 4

https://campus.barracuda.com/doc/29492/

Barracuda RMM Data Accessible for Use with Third Party BI Tools

As of Barracuda RMM 11 SP4, the secure, private, data warehouse that stores your data is accessible to you through Microsoft's Open Data Protocol (OData).

Because Barracuda RMM data is accessible to you, you can use the OData-compatible third party BI tools of your choice to query the data in your company's private repository. Tools like Power BI and Tableau let you analyze your data and create powerful, truly custom reports that show only the data you want to focus on. This gives you the tools you need to parse and visualize large amounts of data, letting you perform tasks like identifying vulnerable devices and quantifying historical trends.

Using a Third Party BI tool is functionality that is available to all Barracuda RMM account holders, but is not enabled by default. For more information, contact your Barracuda RMM Account Representative.

Multi-Factor Authentication

To better protect accounts from hackers and malicious attacks, Barracuda RMM 11 SP4 introduces support for Multi-Factor Authentication. Barracuda RMM's Multi-Factor Authentication can be used with any TOTP authentication app, but the suggested apps are:

- Google Authenticator
- Microsoft Authenticator
- LastPass
- Authy

Multi-Factor Authentication works alongside your username and password as an additional way to verify your identity as you log in to Barracuda RMM. Multi-Factor Authentication provides an extra layer of security, blocking unauthorized users from accessing your sites.
Multi-Factor Authentication is not required. Administrators can enable or disable Multi-Factor Authentication on each individual user account they manage.

Password Reset

Barracuda RMM's new password reset feature lets users request to reset their password without

having to contact their administrator. A user who requests a password is sent an email link that they can use to change their password securely.

The User History feature now records when users request a password reset, so administrators can see who requests new passwords and how often.

Password Complexity

As of this release of Barracuda RMM, by default, Barracuda RMM passwords must be at least 8 characters long.
If your current policy for any site allows passwords shorter than 8 characters, that policy is updated to require passwords 8 characters or longer. Current passwords are not affected, but any new passwords created must be 8 characters or longer. When passwords are changed or reset, the new password must be 8 characters or longer.

For new installations of Service Center on-premise environments, the default administrator user is now required to create a password that is at least 8 characters long when they first log in.

Admin Password Expiry

Previously, passwords for administrators could not be set to expire. For security purposes, this option is now available.

Premium Remote Control improvements

Premium Remote Control is now more accessible and useful than ever—your best option for connecting to client devices. Premium Remote Control lets you connect remotely to managed devices, allowing you to transfer files, chat, and perform various administrative functions as you resolve issues without leaving your desk.

Premium Remote Control has a new option called Fast Launch, that lets you connect to client devices quicker. If you have installed the Premium Remote Control application on your computer, Fast Launch connects you to your client devices far faster.

Premium Remote Control now lets you connect to client devices from more locations on the Barracuda RMM User Interface and with fewer mouse clicks. Windows and macOS users can now access Premium Remote Control on a Device’s page, from a single click on the right menu, and also from the QuickLink

menu.

In addition, Premium Remote Control Session now lets you join a session that is already in progress. If a colleague is connected to a device and wants your input, you can start a Premium Remote Control and request to join the existing session.

Premium Remote Control available for technicians running macOS

Technicians working on macOS systems can now use Premium Remote Control, taking advantage of the power and convenience of Premium Remote Control.

Extended Premium Remote Control Compatibility

More Web Browsers are now compatible with Premium Remote Control without having to download plug ins or browser extensions. Now Safari and certain other browsers don’t require plug ins for compatibility with Premium Remote Control.

User History Additions

As of this release, the User History creates a record when:

- An administrator requests a password reset for a user
- A user requests a password reset
- A user completes a password reset
- Multi-factor authentication is enabled on an account
- Multi-factor authentication is disabled on an account
- A user configures multi-factor authentication on their account

User History now tracks patch management, creating records when:

- Patch Synchronization Options are changed.
- Automatic Patch Approval Rules are added, modified or deleted.
- Automatic Patch Approval Rules are run manually for existing patches.
- A user runs 'Patch Now' for specific patches or devices.
- Patch Product or Classifications are added or removed.
- Patch Cache Site Options are modified.

Support for TLS 1.2

Barracuda RMM 11 SP4 introduces support for TLS 1.2. New installs of Barracuda RMM use TLS 1.2 by default. See the Barracuda RMM Setup Guide for details.

Users who want to use TLS 1.2 exclusively must ensure their managed devices are up to date with all Microsoft Security Updates and the SQL server for their Service Center is hotfixed to the latest updates. At the time of publication, the following are required:

- KB3154518
- KB3140245

TLS 1.2 support includes any HTTPS communication between devices and Service Center, the following:

- Support Assistant
- Remote Tools
- Remote Control
- Installing Device Managers
- Installing Onsite Managers

> Premium Remote Control does not use TLS 1.2.