Barracuda RMM 12 Service Pack 5 Release Notes

https://campus.barracuda.com/doc/96023142/

Upgrade path

You can upgrade to Barracuda RMM 12 SP5 from Barracuda RMM 12 SP3 or higher.

- Service Center Barracuda RMM 12 SP3 Installer
- Onsite Manager Barracuda RMM 12 SP3 Installer

Onsite Manager and Device Manager Upgrade

For this release of Barracuda RMM, Onsite Managers and Device Managers older than 12 SP4 are updated to Barracuda RMM 12 SP5. The update happens in the background, with no manual intervention required, starting 15 days after Service Center has been upgraded to Barracuda RMM 12 SP5, and is completed no more than 14 days after the OM and DM upgrade began.

New Features and Upgrades

Internal Script Editing and Creation Tool in the Automation Library

Barracuda RMM's new internal script editor lets you write and edit scripts directly in the Automation Library without leaving Barracuda RMM.

Also with the new internal script editor, you can edit scripts just by clicking on their links in the Automation Library. This script editor lets you make the changes you need without editing the script externally and re-uploading.

See Adding a Script to Barracuda RMM.

Changes and Improvements to Automation

Cancel Pending Automation Tasks

You can now cancel scheduled automation tasks that have the status of Pending on the calendar.

Tasks will appear on the calendar and Execution results as "Cancelled by user".

See Canceling and Deleting Automated Tasks.

Schedule and Run Now Available from the Automation Library page

You can now schedule or immediately run scripts, automation packages and quick tasks from the Automation Library page.

See To schedule or immediately run a script, automation package or quick task in Viewing Scripts, Automation Packages, and Quick Tasks.

IP Range Restriction

Administrators can now restrict Barracuda RMM log ins to a specific range of IP addresses, preventing users outside that address range from logging in. This provides additional security by preventing unauthorized users from accessing Service Center.

For more information, see Configuring IP Ranges Allowed to Log In.

User History

The IP addresses of user log ins are now displayed for user history entries.

If a user attempts to log in from an IP address that is not in the allowed list, a user history is created stating a log in was blocked, with the user name and the IP address of the attempted log in.

See About User Histories.

Microsoft Defender Upgrades

Microsoft Defender Scan Now

You can now perform on demand scans of devices protected with Microsoft Defender. Scan Now performs a Quick Scan and is available for devices that have a Microsoft Defender AV Policy applied.

See Scanning a Device using Microsoft Defender.

Four New Reports Added

Four reports have been added to report on Microsoft Defender:

- Microsoft Defender Executive Summary
- Microsoft Defender Summary

- Microsoft Defender Device Details
- Aggregate Site Microsoft Defender Antivirus Summary

You can download any of these reports by searching for the name in **Update Center** > **Components**.

SentinelOne Antivirus and Site Security Assessments

SentinelOne antivirus now fulfills the requirements for the antivirus category of site security assessments.

New Intronis Backup Features

Devices Backed Up Outside of RMM Are Displayed on the Device Report Page and the Backup Report pages

Devices that have a Barracuda RMM Intronis Backup policy applied can also have Intronis backups that are controlled through Intronis Backup directly. Providing the Intronis Backup integration has been configured in RMM, managed devices with Intronis Backup agents that have been deployed outside of RMM appear on the Device Report and Backup Report pages. This includes devices with Exchange Information Store, Exchange Mailbox Level, Hyper V Standard, Hyper V Rapid Recovery, VMWare Standard, VMWare QuickSpin, and SQL Server backups.

See Using Intronis Backup in Barracuda RMM.

On the Device Report page, you can use filtering to display or hide these devices. See Viewing Intronis Backup Device Status.

Additionally, Backup Set names and Backup Job details for of all Backup Set types are now visible within RMM.

For Backup Sets that have been created outside of RMM, clicking the **Backup Set** name or the **Backup Job** details link will redirect to the ECHOplatform management portal.

Backup Sets Displayed on the Device Report Page

A new column was added to the Device Report page, displaying the number of backup sets that have been created for each device. Expand any device name to see more information on each backup set, including the type, backup set name, and the associated Intronis Backup policy, if applicable. You can also click a link to go to the associated Intronis Backup policy or to ECHOplatform if the device is backed up without an Intronis Backup policy. See Viewing Intronis Backup Device Status.

Additional Information Displayed on the Intronis Backup Report Page

For each backup, the Intronis Backup Report page now includes the following:

- Backup type — File and Folder, Physical Imaging Standard, Physical Imaging Rapid Recovery, Exchange Mailbox Level, Exchange Information Store, HyperV Standard, HyperV Rapid Recovery, VMWare Standard, VMWare QuickSpin, and System State.
- Backup set name — Click to go to the backup set.

You can now also click items in the **Details** column to be taken to more information on the status of backup sets, which is helpful for Warnings and Failed backups.

See Viewing Intronis Backup Status.

After the upgrade of Onsite Managers and Device Managers, the status of the Intronis Backup agent on the Device Report page is temporarily reset to **Agent Status Pending** until the agent changes state. After the upgrade of Service Center, standalone backup sets that are not controlled by a Barracuda RMM Intronis policy appear on the IBU Device Report page, but the Backup Report page does not display standalone backup set jobs until the Onsite Manager or Device Manager has been upgraded and an RMM Intronis Backup policy has been applied to the device .

Intronis Backup Aggregate Site Report

A new report has been added for Intronis Backup, the Intronis Backup Aggregate Site report. This report includes a summary of device backups for the sites you choose to report on, including the total usage for sites and a list of devices that were backed up without a **Barracuda RMM Intronis Backup** policy.

You can download this report by searching for **Intronis Backup Aggregate Site** in **Update Center** > **Components**.

Changes and Improvements to Custom Log File Monitors

The Custom Log File Monitor has been renamed to the Log File Monitor. In addition, Log File Monitors can be added to monitoring policies. See Adding a Monitor for Log Files.

Device Managers support macOS Monterey

Barracuda RMM 12 SP5 includes a new Device Manager that supports macOS Monterey.

Secure Sign On Tab Renamed

The **Secure Sign On** tab on the **Configuration** > **System Settings** page has been renamed **Authentication**.

Improved Site Deletion Confirmation

When you delete a site, the CAPTCHA has been replaced with a different confirmation challenge.

Announcements

Multi-Factor Authentication Required for the Next Release

For the next release of Barracuda RMM, multi-factor authentication is required.

Intel vPro Removed

Due to lack of use, the Intel vPro features have been deprecated and removed.

Unique Email Validation

Barracuda RMM will soon require user accounts have an unique email address for log in, and that the email be validated through an email link.

In the next release of Barracuda RMM, existing users can be logged in even if their emails are not unique and/or not validated. However, in the subsequent release, Barracuda RMM will require users have a unique and validated email to log in.

Consider letting your users know that in the future, they won't be able to have multiple accounts that use the same email address and that all email addresses will have to be validated.

Deprecation of Microsoft Office 365 Service Module v1.3.0.10

The Microsoft Office 365 Service Module V1.3.0.10 is deprecated. Partners should update to the Microsoft Office 365 2.0 Service Module, available from the Update Center.

Resolved issues

Remote Control

11786	Resolved an issue where trying to connect to an SSH enabled device in Barracuda RMM resulted in the following error: "**Network Error: Software caused connection abort.**"

Reporting

10900	Resolved an issue where **LastSyncTime** dates retrieved from OData were not correct.

Installation, Upgrading, and Migration

11130	Resolved an issue where the Service Center Database Configuration utility would hang when Service Center was installed using Separate Sites in IIS.

Automated Tasks and Scripting

2167	Resolved an issue where confirmation of a script or task being deleted took several minutes to appear.
5806	Resolved an issue in scripts where URLs that contained an ampersand (&) character were not accepted as string parameters.
11333	Resolved an issue where automated tasks were displayed as successful on the Automation Calendar, but the details said pending.

User Interface

9173	Resolved an issue where drop-down on the Windows **Inventory** page did not list any sites, resulting in the user being unable to view other sites.
11617	Resolved an issue where the **Status** > **Device** page did not load for some users.

Antivirus

9284	Resolved an issue where antivirus policies could not be deleted.

Other

6865	Resolved an issue where users were not aware that when configuring proxies, server addresses were invalid if the URI's scheme was not included.
9148	Resolved an issue where sorting the Beta Dashboard by alerts actually sorted by site name.
10399	Resolved an issue where devices could not be deleted.
10604	Resolved an issue where new devices could not be created.
11021	Resolved an issue where reset password emails were not sent to users.
11216	Resolved an issue where user passwords could not be reset.

Known Issues

MW-11479	If you delete a monitoring policy that includes a Log File monitor (previously known as Custom Log monitor), active alerts are cleared successfully. However, any tickets created from alerts in the Log File monitor continue to have the status of Open.
MW-11526	For Log File monitors, previously known as custom log file monitors, environment variables are accepted, however, the %HOMEDRIVE% environment variable does not work at this time.

MW-11647	An issue exists where Admins are able to block their own IP address with the new IP address restriction feature. If this issue occurs, contact Barracuda RMM Technical Support.

© Barracuda Networks Inc., 2024 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.