

Barracuda RMM 12 Service Pack 4

<https://campus.barracuda.com/doc/96012416/>

Barracuda RMM 12.4 requires Microsoft .NET 4.8. If you attempt to install 12.4 without Microsoft .NET 4.8, the install will not proceed.

The install process offers you the option to install Microsoft .NET 4.8. If you don't have Microsoft .NET 4.8 on all servers, you can use the Barracuda RMM installer to install it. Microsoft .NET 4.8 may require one or more reboots.

After upgrading to 12.4, to use Premium Remote Control, download a new Premium Remote Control client to the Technician's computer. See the Installing Premium Remote Control on a Technician's PC procedure [on this page](#). Connections with the old Premium Remote Control clients fail.

Table of Contents

- Upgrade path
- New Features and Upgrades
- Announcements
- Resolved issues
- Known issues

Upgrade path

You can upgrade to Barracuda RMM 12 SP4 from Barracuda RMM 12 SP3 or higher.

Barracuda RMM can no longer be downloaded from the Partner Portal. To download Barracuda RMM, go to the [Download page on Barracuda Campus](#).

Onsite Manager and Device Manager Upgrade

For this release of Barracuda RMM, Onsite Managers and Device Managers older than 12 SP3 are updated to 12 SP4. The update happens in the background, with no manual intervention required, starting 15 days after Service Center is upgraded to Barracuda RMM 12 SP4 and is completed no more than 14 days after the OM and DM upgrade began.

New Features and Upgrades

- Windows Defender Antivirus Integration
- Intronis Backup Integration Updates
- New Device Quick Search Available on Every Page
- MSI Install Package for Device Manager for Windows
- Premium Remote Control Options Available at Site Creation
- Advanced Software Management Improvements
- Patch Now for Advanced Software Management
- Improved Device Status Display for Advanced Software Management
- Advanced Software Management Service Applied to New VARs by Default
- Device Overview Page Displays Full Windows 10 Versions for Devices
- Mac Improvements
- Include the Site, Device, and Alert Configuration names in Alert Email Subject Lines
- Changes to the Display of the Device Status Page
- Improvements to the Reports Page
- Updates to Rules in Auto-Application and Site and Service Groups
- Display Icons for Device Status on Patch Management Pages
- Activate and Disable Users on the User Management Page
- New Microsoft Patch Management Default
- New Filtering Options for Applying Policies Manually
- Usability Improvements
- Additions to User History
- Beta Testing of a New Central Dashboard

Windows Defender Antivirus Integration

Barracuda RMM 12 SP4 provides integration with Windows Defender Antivirus, Microsoft's antivirus solution for workstations running Windows 10, and servers running Windows Server 2016 and 2019.

Windows Defender Antivirus is free to use and provides critical protection for those systems. It is included with the operating systems listed above and does not need to be installed or deployed.

Barracuda RMM lets you control Windows Defender Antivirus settings with policies, letting you configure your protection, choose what devices to protect, and choose which files and folders on each system to exclude from protection.

When it is active and configured correctly, Microsoft Defender Antivirus fulfills the Site Security

Assessment requirements for the following categories:

- Server antivirus software detection
- Workstation Antivirus software detection
- Workstation Antivirus software evaluation
- Workstation Antivirus software status check

See [Managing Microsoft Defender Antivirus](#).

Intronis Backup Integration Updates

Computer names match in Barracuda RMM and ECHOPortal

To let you more easily identify devices you have integrated with Intronis Backup, computer names in Barracuda RMM and ECHOPortal now match.

Alert on Backups that Do Not Execute

To keep you better informed of the status of your Intronis Backups, you can now create an alert that lets you know if a backup does not execute.

Reports Reflect the Installed Version of the Intronis Backup Agent

To keep you informed of your version of the Intronis Backup Agent, reports now show the version number of the Intronis Backup Agent.

Export Reports from the Policy Report Page

You can now export a report from the Policy Report page.

Reports Include Missing Backups

To give you more transparency into backup jobs, SQL reports now include information on missing backups.

Easier customization of the Backup Report page

It's now easier to customize the categories displayed on the Intronis Backup Report page. By selecting or clearing the check box on the category icon, you can show and hide those categories in the Backup Report.

New Device Quick Search Available on Every Page

A new device quick search is available on the title bar of every page in Barracuda RMM. This search lets you quickly search for devices by full or partial device name or full or partial IP address. When you search for a device through the quick search, the page changes to the Status > Device Search page to display the results.

For more information, see [Searching for a Device Using Quick Search](#).

MSI Install Package for Device Manager for Windows

The install package for the Device Manager for Windows is now available in .msi format as well as .exe. This option lets administrators install Device Managers silently through domain policies or automation software.

Requirement

- Microsoft .NET Framework 4.6.0 or higher on target devices

See [Installing Device Managers](#).

Premium Remote Control Options Available at Site Creation

You can now automatically install Premium Remote Control on all devices when you create a site. The following options are available in the Site Creation Wizard:

- Automatically install Premium Remote Control
- Require Consent

The defaults for new sites are the options you have chosen through the Set default settings for new sites feature on the **Sites > Site Management** page. For more information, see [Setting Premium Remote Control Options](#).

Advanced Software Management Improvements

Patch Now for Advanced Software Management

Users with Advanced Software Management enabled can now use the ASM Patch Now button to send patches to applicable devices off schedule.

The Patch Now feature is available on the ASM Patch Report page and Device Report page.

See [Patching Third Party Applications with Patch Now](#).

Improved Device Status Display for Advanced Software Management

The status of devices (whether they are up or down) is now displayed beside each device on some Advanced Software Management pages. A colored icon now tells you the status of each device at a glance.

The status icon is now displayed on the following pages:

- **Advanced Software Management > Reports > Patch Report**
- **Advanced Software Management > Reports > Device Report**
- **Advanced Software Management > Settings > Approval Groups**

New Auto-Application Rules for the Default Advanced Software Management Policy

Auto-application rules have been added to the default Advanced Software Management policy. You can use these rules as they are or customize them.

The rules are:

- Device Role Category equals Windows Server
Or
- Device Role Category equals Windows Workstation

See [Understanding the Pre-Built Advanced Software Management policy](#).

Advanced Software Management Service Applied to New VARs by Default

Whenever a new VAR is created, a service titled "Advanced Software Management," containing the Advanced Software Management policy is applied to the VAR. If the VAR is not an Advanced Software Management customer, this service reports the status of patches for third-party software. If the VAR has a subscription, this service provides third-party patch configuration.

Device Overview Page Displays Full Windows 10 Versions for Devices

The full Windows 10 version is now displayed on the **Device Overview** page for Windows 10 devices. This information is displayed in the Operating System area, along with the installation type, either Client or Server.

This change does not affect auto inclusion rules, which continue to function based on the OS Build number.

Mac Improvements

We have introduced the following upgrades:

- The **OSX Site Prep Utility** Now Supports Catalina and Big Sur.
- For Mac devices, the recommended OS version is now 10.12 and higher.

Include the Site, Device, and Alert Configuration names in Alert Email Subject Lines

For faster alert processing, you now have the option to include the Site, Device, and Alert Configuration names in the Subject Line of the Alert Emails.

See [Setting Default Email Options](#).

Sort Devices by Upgrade Status on the Site Overview > Device Managers page

You can now sort devices by their status on the Device Managers tab of the Site Overview page. Click **Site Management > Sites**, then the name of the site. Click the Device Managers tab, then the up or down arrow in the **Upgrade Status** column to quickly view devices sorted into by their upgrade status.

Changes to the Display of the Device Status Page

As of Barracuda RMM 12 SP4, on the **Status > Device** page, the WMI, SSH, and SNMP columns are displayed by default for new users, new installs, and new VARs. For existing users, installs, and VARs, the current user preferences do not change.

Improvements to the Reports Page

The following improvements have been made to the **Reporting > Reports** page:

- Reports are displayed in a more readable way.
- The **Preview** button has been moved to a more accessible location.
- A search bar has been added to let you find your reports faster and easier.

Updates to Rules in Auto-Application and Site and Service Groups

The following changes have been made in the rules for auto-application and site and service groups:

Update to the Logical Drive Size Rule

When adding a new Logical Drive Size rule for auto-application or a site or service group, you can now identify the letter of the drive the threshold applies to. You can also apply to limit to all drives.

Existing **Logical Drive Size** rules continue to work the way they were set up.

The Device Name Rule Renamed

The rule formerly called **Device Name** is now named **Device System Name** to match the **Device Overview** page. This rule searches the **System Name** field.

Any existing **Device Name** rules you have are named **Device System Name** after upgrading and continue to work the way they were set up.

A New Device Name Rule

A new rule has been added. The **Device Name** rule searches a variety of name fields. The fields are searched in the following priority:

- **Alias**
- **Computer Name**
- **SSH Name**
- **SNMP Name**
- **Netbios Name**

See [Creating Automatic Inclusion Rules for Monitoring Policies](#).

Display Icons for Device Status on Patch Management Pages



The status of devices (whether they are up or down) is now displayed beside each device on some Patch Management pages. A colored icon now tells you the status of each device at a glance.

The status icon is now displayed on the following pages:

- **Patch Management > Settings > Approval Groups**
- **Patch Management > Reports > Patch Report**
- **Patch Management > Reports > Device Report**

Activate and Disable Users on the User Management Page

You can now quickly activate and disable users directly on the User Management page. Click the icon in the Status column to change the user's status:

- Active User: 
- Disabled User: 

See [Activating, Disabling, and Deleting a User Account](#).

New Microsoft Patch Management Default

The Microsoft Patch Management settings for new VARs now include all options enabled by default. This means that upgrades are included for Patch Management by default.

New Filtering Options for Applying Policies Manually

To save time when applying policies manually to Service Groups and Site Groups, you can now filter the group list in new ways.

When looking at Service Groups, you can filter on Folders. When looking at Site Groups, you can filter by Site.

Usability Improvements

To improve usability, several changes have been made:

- The description for the Advanced Software Management service is now clearer.
- You can now see the status of Device Managers on the Device Managers tab of the Site Management page for any site. A column with a status icon is displayed next to each device, showing if the status is up or down.

Additions to User History

The **User History** creates a record when:

- A Microsoft Defender policy is created.
- A Microsoft Defender policy is updated.
- A Microsoft Defender policy is deleted.
- A Microsoft Defender policy is copied.

Beta Testing of a New Central Dashboard

The preview of a new Central Dashboard that began in Barracuda RMM 12 SP2 continues in this release. This new Central Dashboard has been designed to improve performance and give you the tools to focus on the information that is important to you.

To test the new Central Dashboard, navigate to **Dashboards > Central Dashboard**, then click the **Enable Beta View** button. You can return to the standard dashboard at any time by clicking the **Disable Beta View** button.

The Central Dashboard Beta is still in development. To review the known issues of the Central Dashboard Beta, see Central Dashboard Beta Known Issues.

Announcements

Update to Application Server Requirements

- Application servers for Service Center are now required to have Microsoft .NET Framework 4.8 or higher.

Avast Password Manager Removed

References to Avast Password Manager have been removed because Avast no longer offers the product.

End of support for Windows 8

Because Microsoft has stopped updating Windows 8, Barracuda RMM will no longer support Windows 8 as of Barracuda RMM 12 Service Pack 5.

Resolved issues

Patch Management

MW-10364	Resolved an issue where devices that appeared to have a patch policy applied did not.
----------	---

Reporting

MW-8364	Resolved an issue where the Site Security Report failed with a subreport error.
---------	---

Installation, Upgrading, and Migration

MW-9922	Resolved an issue where certain sites did not communicate after their Onsite Managers were automatically upgraded after a release.
MW-10309	Resolved an issue where the SCDatabaseConfigurationTool failed to update the database configuration for the Update Service component.
MW-10598	Resolved an issue which could cause a Service Center database upgrade failure during a Service Center migration

Automated Tasks and Scripting

MW-7530	Resolved an issue where an Automated Task applied to device groups was not applied to new devices that were added to the group through Auto-Inclusion.
MW-9576	Resolved an issue where Automation on Windows-based systems did not detect Python version 3.
MW-9688	Resolved an issue where Service Center could become unavailable when processing a large amount of automated task results submitted by Onsite Managers and Device Managers.

Performance

MW-10311	Resolved an issue where the service center could become unavailable when processing a large amount of automated task package results submitted by Onsite Managers and Device Managers.
MW-10656	Improved performance for tasks related to the Maintenance Window.

Role Management

MW-9671	Resolved an issue in RMM 12 SP2 HF5 that allowed users who did not have Modify permissions to delete Device Managers.
---------	---

User Interface

MW-10545	Resolved a UTC date calculation issue that caused automated tasks to be displayed on the previous day in the Automation Calendar.
----------	---

Antivirus

MW-9946	Resolved an issue where devices were not always suspended correctly.
---------	--

Other

MW-7689	Resolved an issue where a Custom Device Discovery rule set to include all categories included devices that did not meet any of the categories.
MW-9018	Resolved an issue where VMWare performance counter data was no longer written to the database.
MW-9270	Resolved an issue where Advanced Software Management module was not re-installed to devices if the module was removed, and then a re-install was attempted.

MW-9876	Resolved an issue where the NanoServiceHost component on the Onsite Manager failed to start if the Onsite Manager database was unavailable.
---------	---

Known issues

Unicode characters in script results are displayed as "?" in Service Center.
Due to a third party issue, Premium Remote Control cannot connect to macOS Big Sur and Catalina devices.
The 12 SP4 installer does not recognize that SQL Server Management Studio is already installed, which results in a failed install if SQL Management Studio is already on your computer. If you already have SQL Management Studio installed, clear the SQL Tools checkbox during setup and the install will succeed.

Central Dashboard Beta Known Issues

The top bar is not functional.
The Infoservices toggle is not functional.

After upgrading to 12.4, to use Premium Remote Control, download a new Premium Remote Control client. Connections with the old Premium Remote Control clients fail. Due to a third party issue, Premium Remote Control cannot connect to macOS Big Sur and Catalina devices. The 12 SP4 installer does not recognize that SQL Server Management Studio is already installed, which results in a failed install if SQL Management Studio is already on your computer. If you already have SQL Management Studio installed, clear the **SQL Tools** checkbox during setup and the install will succeed.

Figures

1. user_active.jpg
2. user_inactive.jpg

© 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.