Barracuda Managed Workplace 12 Service Pack 3 Release Notes

https://campus.barracuda.com/doc/94537666/

Table of Contents

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

Upgrade Path

You can upgrade to Barracuda RMM 12 SP3 from Barracuda RMM 12 SP1 or higher.

- Service Center MW12 SP1 Installer
- Onsite Manager MW12 SP1

Customer Reported Issues

Also included is the resolution to twenty-five customer-reported issues. To view or search the fixed issues, visit the Resolved Issues Page and select 12 SP3 from the Version list.

New Features and Upgrades

- Integration with Intronis Backup Available for All Barracuda RMM Partners
- Changes to Integration with Intronis Backup
- Intronis Backup Policies
- Intronis Backup Alerts
- New Intronis Backup Reports
- Additions to User History
- Improved Patch Status Display on Device Overview > Patch Management Pages
- Improved Patch Group Display on the Patch Details Status Tab
- Beta Testing of a New Central Dashboard
- New installs of Onsite Manager now install Microsoft® SQL Server® 2017 Express
- Onsite Manager SQL Requirements

- Changes to Automatic Onsite Manager and Device Manager Upgrade
- Important Notice for BCS Users

Integration with Intronis Backup Available for All Barracuda RMM Partners

All partners with Intronis Backup accounts can now integrate Barracuda RMM with Intronis Backup.

Intronis Backup requires an additional license. Contact your Barracuda sales representative.

Changes to Integration with Intronis Backup

To create a more robust and secure integration, changes have been made to how Barracuda RMM integrates with Intronis Backup.

As of Barracuda RMM 12 SP3, only the built-in 'admin' user who set up Barracuda RMM can create integrations with Intronis Backup.

For more information, see Integrating with Intronis Backup.

Intronis Backup Policies

Barracuda RMM now has policies for Intronis Backup. Intronis Backup policies give you the ability to set up and control File and Folder backups and Physical Imaging Standard backups. Policies let you identify what you want to back up, where backups are stored, and how often Intronis performs backups.

For more information, see Working with Intronis Backup Policies.

Intronis Backup Alerts

You can attach alerts to Intronis Backup policies to warn you of incomplete backups or let you know when backups finish. Alerts can be set to create trouble tickets automatically and to send out emails when backups fail. These notifications keep you informed when your backups need attention.

For more information, see Adding Alert Configurations to Intronis Backup Policies.

New Intronis Backup Reports

The following new Intronis Backup reports are available from the Update Center:

- **Intronis Backup Device Report** Shows information on devices backed up with Intronis Backup policies through Barracuda RMM.
- **Intronis Backup Site Report** Shows information on sites containing devices backed up with Intronis Backup policies through Barracuda RMM.
- **Intronis Site Aggregation Report** Shows aggregate information on sites backed up with Intronis Backup policies through Barracuda RMM.

Additions to User History

The User History creates a record when an Intronis Backup policy is:

- Created
- Deleted
- Modified
- Applied to a device
- Removed from a device

The User History creates a record when:

- An Intronis Backup agent is redeployed.
- An Intronis Backup agent is uninstalled.
- A device with an Intronis Backup agent is rebooted.

For more information, see About User Histories.

Improved Patch Status Display on Device Overview > Patch Management Pages

The display of patch status on Device Patch Management pages has been improved. The following have been added/improved:

- Patches installed through **Patch Now** reflect their status more accurately on Device Patch Management pages.
- The table on Device Patch Management pages now includes a column that displays the date each patch status was last updated.

- Device Patch Management pages now display the last time/date the system checked for updates.

Improved Patch Group Display on the Patch Details Status Tab

For each patch, you can now more easily navigate to a list of devices with the status of installed, needed, or failed.

To see the improved tab, in Barracuda RMM, click **Patch Management** > **Patch Approval**. Filter the list, then click a patch link. Click the **Status** tab.

On this tab, you can now click the numbers in the status columns at the right to see the devices with each status.

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.

To give feedback on the new Central Dashboard, contact your Account Manager. To report a technical issue on the new Central Dashboard, contact Technical Support.

New installs of Onsite Manager now install Microsoft® SQL Server® 2017 Express

New installs of Onsite Manager include Microsoft® SQL Server® 2017 Express for systems. Due to this, new installs are supported on the following x64 operating systems:

- Windows 10
- Windows 8

- Windows 8.1
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016

Upgrades of Onsite Manager are not affected. However, review the update to Onsite Manager SQL Requirements.

Onsite Manager SQL Requirements

Onsite Manager no longer supports SQL 2005 Express and SQL 2008 Express. Onsite Managers running on these cannot be upgraded. If you have an Onsite Manager upgrade that fails on these versions of SQL, use one of the following procedures to upgrade the Onsite Manager:

- Moving an Onsite Manager - On Premise
- Moving an Onsite Manager - Hosted
- Moving an Onsite Manager - Hosting Provider

SQL 2008 R2 Express is still supported.

Changes to Automatic Onsite Manager and Device Manager Upgrade

Previously, the automatic upgrade of Onsite Managers and Device Managers began 30 days after a Service Center upgrade. It now starts 15 days after the Service Center upgrade.

Important Notice for BCS Users

Because of security improvements, on upgrade to Barracuda RMM 12 SP3, users who previously integrated with Barracuda Content Shield must reauthenticate their integration user.

Your Barracuda Content Shield integration will not work correctly until the user is re-integrated. However, your existing site mappings and other settings are preserved. Follow the procedure below to re-integrate your built-in admin user, and then your Barracuda Content Shield functions as normal.

To re-integrate your Barracuda Content Shield user

1. While logged in as the built-in Admin user, in **Service Center**, click **Configuration** > **User Management**.
2. Click the link of the built-in Admin user.
3. Click the **Link to BCC user** button.
4. Click **Link**.
5. Click **Save**.

Announcements

- Onsite Manager and Device Manager Upgrade
- Installation of SQL Server Management Studio 18.6 with SQL Management Tools
- Deprecation of the CloudCare Service Module
- Announcement for Ninite Script Users
- Deprecation of support for vPRO

Onsite Manager and Device Manager Upgrade

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

Installation of SQL Server Management Studio 18.6 with SQL Management Tools

SQL Server Management Studio 18.6 is now installed as well when the option to install SQL Management Tools is selected.

Deprecation of the CloudCare Service Module

This version of Barracuda RMM deprecates the CloudCare Service Module. This service module is no longer offered or supported. It will be automatically uninstalled.

Announcement for Ninite Script Users

Barracuda RMM had an agreement with Ninite that provided usage of certain Ninite Pro scripts for Barracuda RMM users free of charge. This agreement has since expired and, unfortunately, those specific Ninite Pro scripts are no longer available or functional. We recognize the inconvenience this has caused.

Barracuda RMM will continue to support any Ninite Pro scripts partners import into Barracuda RMM. Please read the Import Ninite Pro scripts knowledge base article for more information. To leverage MSI or executable deployment through Barracuda RMM automation, please read this knowledge base

article for more information.

For ongoing patch management requirements, we recommend using Barracuda Advanced Software Management, our integrated third-party software update and patch management tool. Reach out to your account manager or sales engineer to learn more about Barracuda Advanced Software Management.

To see the full list of unavailable scripts, click here.

Deprecation of support for vPRO

Support for vPRO has been deprecated and will be removed in an upcoming version of Barracuda RMM.

Resolved issues

Patch Management

MW-101	Resolved an issue where the Approval Groups page's filters were reset after devices were moved into an approval group.
MW-8680	Resolved an issue where patch status for Device Manager managed devices was not reported back to Service Center in some cases.

Remote Control

MW-1919	Resolved an issue where certain remote control features, such as Remote Assistance and installing Premium Remote Control, threw an unexpected error.
MW-8400	Resolved an issue where RDP and Premium Remote Control sessions failed to start after changing the hostname of the Service Center server.

Reporting

MW-7798	Resolved an issue where duplicate entries were returned for Virtual Machines on the Custom Asset Baseline Report and the Site Device Summary Report.
MW-8389	Resolved an issue where the Device Patch Summary Report threw an error when a delivery schedule was run with more than one device.

Installation, Upgrading, and Migration

MW-8549	Resolved an issue where the Device Manager setup failed with a File Not Found error.
MW-8837	Resolved an issue that caused Onsite Manager upgrades to fail when using the stand-alone Onsite Manager installer from the .zip package.

Monitoring and Alerting

MW-9628	Resolved an issue where alerts for Performance Counter monitors continued to trigger after the monitors were deleted.

Performance

MW-6722	Improved the loading time of the **Status** > **Alerts** page.

User Interface

MW-7495	Resolved an issue where a secondary credential prompt for Windows Authentication appeared when trying to log in to Service Center.
MW-7948	Resolved an issue where the **Patch Details** page stopped working after approvals were changed.
MW-8387	Resolved an issue where policy links in services displayed the **Monitoring** policy workflow even when they were not from a **Monitoring** policy.
MW-8422	Resolved an issue that caused an unexpected error when enabling Multifactor Authentication on user accounts.
MW-8434	Resolved an issue where the **Filter By** option didn't work when choosing devices for the **Automation** > **Calendar** > **Schedule**.
MW-8453	Resolved an issue where **Automation Policies** appeared duplicated in the User Interface.
MW-9478	Improved the **Firewall Rules** User Interface in **Antivirus** policies.

Other

MW-8071	Resolved an issue on the Trouble Ticket > Ticket Management page where the All Closed Today filter did not work when combined with the Assigned To filter.
MW-8078	Resolved an issue where users without the Admin role couldn't add devices to a Service Group on the Group page.
MW-8148	Resolved an issue where Service Module icons were not displayed in the Sites list on the Central Dashboard Beta view.
MW-8402	Resolved an issue where the Service Center URLs could change during upgrade if an old URL was present in the registry.
MW-8452	Resolved an issue that caused Onsite Managers to take up additional memory.
MW-8655	Resolved an issue in the Beta Dashboard where data was loaded from external domains.
MW-8951	Resolved an issue that caused devices managed by the Device Manager to rediscover themselves.
MW-8952	Resolved an issue that caused down devices managed by Device Managers to be deleted before the threshold was reached.
MW-9205	Resolved an issue that caused an incorrect syntax error in some system logs.

Known issues

Warning emails about down devices that will be deleted do not exclude sites that are on hold. The down devices of sites on hold are not deleted when the time threshold is released, even though warning emails are sent.
An issue exists when you re-add one or more devices that you have previously removed from an Intronis Backup policy that runs on an execution schedule. If you changed the execution schedule while the devices were not included in the policy, the schedule on the devices reflects the original schedule for up to an hour after the devices are re-added. This may result in an unexpected backup of devices that have been removed and re-added.
An issue exists with the display of agent deployment on the Intronis Backup Device report page. If you add a device to an Intronis Backup policy, but the device doesn't require a new agent (because the agent already on the device matches the Intronis Backup partner and customer used in the Intronis Backup deployment), the Device report page may display the wrong status in the Agent Status column. The status of "Agent Status Pending" is displayed instead of "Deployed". Backups proceed correctly even though the status is displayed incorrectly. To update the status, you can stop the Backup Agent Windows service on the device and then start it. Restarting the Backup Agent does not fix this issue.
An issue exists where the Intronis Backup Report page may not report on backup jobs correctly when backups from the same backup set occur multiple times within five minutes.

Central Dashboard Beta Known Issues

The top bar is not functional.
When filtering by Program, you may experience performance issues.
The **Infoservices** toggle is not functional.

Unavailable Ninite Scripts

The following are the Ninite scripts that are unavailable:

- **Install or Update 7-Zip**
- **Install or Update Ad-Aware**
- **Install or Update Adobe Flash**
- **Install or Update Adobe Flash for IE**
- **Install or Update Adobe Reader**
- **Install or Update CutePDF**
- **Install or Update FireFox**
- **Install or Update Google Chrome**
- **Install or Update Java**

- **Install or Update Malwarebytes**
- **Install or Update Microsoft Security Essentials**
- **Install or Update Spybot Search and Destroy**
- **Install or Update WinRAR**
- **Install or Upgrade OpenOffice**