What's New in this Release

https://campus.barracuda.com/doc/91128471/

Automatic Upgrade of Onsite Managers and Device Managers

As of Barracuda Managed Workplace 12 Service Pack 1, Onsite Managers and Device Managers older than two major versions are automatically updated to the latest version when Service Center is upgraded. The update happens in the background, with no manual intervention, starting 30 days after the upgrade to 12 SP1, and will be completed no more than 14 days after starting. For this version, OMs and DMs version 11 SP4 MR2 and older are upgraded to 12 SP1.

You can still choose to update OMs and DMs manually.

The upgrade of OMs and DMs older than 8.2 may fail. Follow the Performing the Upgrade to 10.0 Onsite Managers procedure in the Setup Guide to prepare older OMs and DMs for auto-upgrade.

To facilitate performance improvement, issue resolution, and new feature adoption, automatic upgrade of OMs and DMs is included in all future Barracuda Managed Workplace releases.

Third Party Firewall Tests Added to Site Security Assessment

A new firewall test has been added to **Site Security Assessment**. Previously, only **Windows Firewall** was scored in **Site Security Assessment**. The new **Third Party Firewall Status Check** test, in the **Antivirus Security** category, passes if a firewall that is not **Windows Firewall** is installed and enabled on the device.

For more information about the third party firewall test and how it interacts with **Windows Firewall** tests, see Firewall-related Security Tests.

Advanced Software Management Tests Added to Site Security Assessment

Two new tests have been added to the **Site Security Assessment**.

The **Third party patch data collection** test passes if third party patch data for **Windows** devices is successfully collected.

The **Third party software security update evaluation** test passes if third party security updates are current.

Changes to Site Security Assessment

Site enrollment

As of **Barracuda Managed Workplace 12 SP1**, all sites are enrolled in **Site Security Assessment**:

- New sites are enrolled in **Site Security Assessment** when they are created.
- Existing sites are enrolled in **Site Security Assessment** on upgrade to **12 SP1**.

New Site Default Security Schemas

You can set any **security schema** to be the one applied to new sites when they are created. You can change the **new site default security schema** at any time.

Unassessed Devices Column added to the Site Security Dashboard

The **Site Security Dashboard** now includes an **Unassessed Devices** column to display how many **Windows** devices are not eligible for **Site Security Assessment**.

Integration with Barracuda Content Shield for Users Hosted on the Barracuda Cloud

Barracuda Content Shield delivers a powerful web threat protection and content filtering solution for **MSPs** and their customers. Powered by **Barracuda's** extensive threat intelligence network, **Barracuda Content Shield** protects users from accessing malicious sites and inappropriate content, helping to keep your customers' businesses safer and their employees more productive.

As of MW12 SP1, Barracuda Managed Workplace provides free integration with **Barracuda Content Shield** for users hosted on the **Barracuda Cloud**. Users hosted on the **Barracuda Cloud** can use this integration to view a summary of **Barracuda Content Shield** threats, agents, and licenses, and to easily navigate to the **Barracuda Content Shield** portal.

As of MW12 SP1, this feature is not available to users who are not hosted on the **Barracuda Networks Cloud**.

Deployment Script for Barracuda Content Shield Plus

A script to deploy **Barracuda Content Shield Plus** to **Windows** devices is available from the **Automation Library**. For more information, see Deploying Barracuda Content Shield Plus.

User History

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

- A user connects their **Barracuda Cloud Control** account to integrate another **Barracuda** project.
- A user removes a **Barracuda Cloud Control** account connection.
- An attempt to connect to a **Barracuda Cloud Control** account fails.
- A user removes an Onsite Manager from a site.
- A user deselects the **New Site Default Security Schema**.
- A user selects a different **New Site Default Security Schema**.
- A user applies a security schema to all sites.

Performance Improvement

The load time of the **Central Dashboard** has improved, especially for users with larger numbers of sites, groups, and devices.

New Axcient Monitoring Policy

The new **Axcient** monitoring policy replaces the **Axcient** service module, which is deprecated in this release of Barracuda Managed Workplace. If you used the **Axcient** service module, download the **Axcient** monitoring policy from the Update Center.

New Symantec Backup Exec Monitoring Policy

The new **Symantec Backup Exec** monitoring policy replaces the **Symantec Backup Exec** service module, which is deprecated in this release of Barracuda Managed Workplace. If you used the **Symantec Backup Exec** service module, download the **Symantec Backup Exec** monitoring policy

from the Update Center.

New Symantec Endpoint Protection Monitoring Policy

The new **Symantec Endpoint Protection** monitoring policy replaces the **Symantec Endpoint Protection** service module, which is deprecated in this release of Barracuda Managed Workplace. If you used the **Symantec Endpoint Protection** service module, download the **Symantec Endpoint Protection** monitoring policy from the Update Center.

Additions to the Reporting Data Layer

Several new tables have been added to the **Reporting Data Layer** database, in the areas of **Advanced Software Management** and **macOS** support. See the Data Layer Documentation for full details.

Remove Onsite Managers from Sites

A new feature is available to users who have a role that includes the **Modify Site** permission. You can now remove Onsite Managers from sites that have at least one Device Manager.

You may want to do this in the case of the accidental deployment of an **OM** to a site, or for sites that previously had desktop computers but does not contain only laptops or mobile devices. You can also use an Onsite Manager to deploy Device Managers, and then remove the Onsite Manager, to create a site that is only managed by Device Managers.

When you remove the Onsite Manager from a site, the number of devices is likely to go down, since it will contain only the devices managed by a Device Manager after the removal.

F or more information, see Deleting the Onsite Manager from a Site in the Setup Guide for your version of Barracuda Managed Workplace:

- Installing and Removing Onsite Manager - Hosted
- Installing and Removing Onsite Manager - On Premise

Improvement to start up time

A change has been made that improves start up time for certain functions, like automation and remote tools. To take advantage of this change for a site, you must re-run the site prep tool, or to improve performance for a single device, on the target device, enable **Remote Service Management** in your **firewall** application.

Improvements to the Automation Calendar Week View

The **Week** View of the **Automation Calendar** has been improved for users who have a large number of automated tasks. If you have more than five automated tasks in any hour during the week, that hour displays a summary of the tasks instead of each individual task. The summary displays information about completed tasks, tasks in progress, and future tasks. For more information, see Using the Summary Boxes in the Automation Calendar Week View in the User Guide.

Changes to the Avast Business Antivirus - Antivirus Definition Files Out of Date Monitor

Previously, the **Avast Business Antivirus - Antivirus Definition Files Out of Date** monitor alerted if no virus definitions had been downloaded for over two days. Due to changes in the way **Avast** updates antivirus, this monitor now alerts if virus definitions have not been completely updated for seven days.