About Managing Microsoft Patches

https://campus.barracuda.com/doc/27813/

Click the video below for an introduction to managing Microsoft patches:

Managing Microsoft patches involves acquiring, testing, and installing updates on a managed computer.

The goal of managing Microsoft patches is to create a consistently configured environment that is secure against known vulnerabilities in Microsoft operating system and application software.

By using patch management, you can:

- Control updates to Microsoft applications and operating systems.
- Increase security on the client-side network against known vulnerabilities in Microsoft operating system and application software.
- Ensure standard patch levels across managed systems.
- Automate Microsoft updates to ensure security.

You can set up Microsoft patch management so that it's completely automated, or you can set up controls so that you can test patches before approving them. You decide how automatic or manual you want Microsoft patch management to be.

- Microsoft patch management is not supported when devices are connected over VPN. If you have devices at separate locations for a single customer, we recommend that you deploy an Onsite Manager for each site, or that you deploy Device Managers.
- The terms *patch* and *update* are interchangeable.

Understanding Microsoft Patch Management

Barracuda RMM duplicates the management model of **Windows Server Update Services (WSUS)** for all Microsoft updates. When you make decisions about what to do with patches for groups of computers, the native Windows functionality handles the installation based on rules you set in the Patch policies (see What is a Patch Policy?).

Computers with Device Manager installed receive information about patches from Service Center and download the files from **Microsoft Update** directly (see What is Microsoft Update?). End users will see notifications and messages from Service Center.

Patching Non-Microsoft Applications

All non-Microsoft software updates are handled through automation. For example, to update **Adobe** products, you can use the built-in **Ninite** scripts. Go to **Automation** > **Library** and search for "**Install** or **Update**" for a list of scripts provided with Barracuda RMM for updating software.

Synchronizing Updates

Microsoft updates are differentiated by product (or product family) and classification.

Product A product is a specific product or product family from which the individual product is derived. For example, Microsoft Windows is a product family from which Windows Server 2016 is a member. You can get updates for current and future versions of the product.

Classification A classification is the type of update. For any given product or product family, updates could be available among multiple update classifications (for example, Windows XP family **Critical Updates** and **Security Updates**). Microsoft provides critical and security-related patches on the second Tuesday of the month and non-security patches on the fourth Tuesday.

What is a Patch Policy?

A patch policy is a collection of rules that manages Microsoft updates on devices or groups.

When a Microsoft patch policy is first applied to a device, it will check into the Onsite Manager to download a cookie, download an agent and upload its patch status. The device will check in with patch management in under an hour if there are no communication or configuration issues.

Once patch management is enabled, devices check in for new instructions with the Onsite Manager or

Service Center at least once every 22 hours.

What is a Windows Update Agent?

A Windows Update Agent is included on all modern Microsoft operating systems so that updates can be managed by users or administrators. On an unmanaged device, the rules are provided through the **Windows Control Panel**. Using Barracuda RMM, the rules are provided through patch policies.

What is Microsoft Update?

Microsoft Update is a repository that provides downloadable updates for Microsoft operating systems and applications. Microsoft Update works with updating software in Windows. The updating software identifies which version of Windows and other Microsoft products are used on the device.

> Windows Update is the classic update service that only offers updates for Windows. Microsoft Update extends this service to cover other Microsoft programs. For more information about Microsoft Update, visit the Microsoft website.

Prerequisites for Patch Management

Devices that you want to patch manage must be WMI-enabled.

On Domain networks, **WSUS**-related **Group Policy Object (GPO)** must be set to **Not Configured** since Barracuda RMM does not use **GPO** settings to define the update server for managed clients. Any **WSUS** policies that are in place on the Domain will interfere with the normal operations of patch management.

Figures

1. PosterPatchManagement.png