



# Endpoint Management

## **2016-3 PATCH MANAGEMENT WHITE-PAPER**

*Stan Lee*

*August 2016; Version 1.2b*

# Contents

Introduction .....	3
What's all-new .....	3
What's changed .....	3
What's improved .....	4
1.0: Manage patch activity at the Account- and Site-level .....	5
Overview .....	5
Contents.....	5
Removal of individual patch control on the site- and account-level.....	5
Changing of Patch Status .....	6
Removal of Account-level patch installation time .....	6
Addition of new options to view patching status .....	7
1.1: Device-level Management .....	8
Overview .....	8
2.0: Patch Policy Interface Refactor.....	9
Overview .....	9
Contents.....	9
Abstract.....	9
Support for Patching through Local Caches .....	10
Windows Update control .....	10
Refactor of Patch Approval methods .....	11
Tailored reboot controls .....	12
3.0: Site-level overriding of Account-level policy options.....	13
Overview .....	13
4.0: Performance improvements .....	14
Support for outdated Windows Update Agent versions.....	14
Improvements in handling Windows Update policies .....	14
5.0: Acknowledgements .....	14
Error 0x8024a204 .....	14

## Introduction

Welcome to the newest iteration of the Autotask Endpoint Management Patch Management engine. This new release represents a revolution for Patch Management, and there are a number of important points and acknowledgements that should be made when accommodating the new system – either as a newcomer or as an existing user of the legacy solution.

## What's all-new

The 2016-3 release introduces the concept of *Site-level policy overrides*, a system that allows users to view Account-level policies being applied at the site-level (Legacy nomenclature: allows users to view System-level policies being applied at the Profile-level) and configure individual settings to either change or add to them as they are applied to a smaller subset of devices.

Don't worry about altering a setting that will affect other Sites – with the new override system, users are now able to configure an Account-level policy's complicated areas, and alter only the most necessary elements at the level of individual Sites.

Users can now configure their Network Nodes to send Wake-on-LAN operations to devices 10 minutes before a patch policy is about to start, meaning that devices supporting the feature are always kept up-to-date regardless of scheduling. Got employees working office hours? Enable Wake-on-LAN in BIOS settings and patch your devices overnight for no downtime.

## What's changed

The new Patch Management solution adopts a philosophy of pure policy-based patching, as opposed to less-accountable device- and patch-specific methods previously employed. The net result of this is that all patch operations can be traced and reviewed, with predictable and sensible results every time. Users are granted the final say over patches on the device-level to save them having to amend policies for individual devices to strike the perfect balance between control and simplicity.

In order to accommodate this new feature before it is released, we recommend users not currently employing a policy system for Patch Management adopt one before the switch-over. The new system does not carry over patch approvals and hide operations from the Legacy system, so users wishing to preserve this data should port the information over to a Legacy-style policy now while the data is still present. **After the switchover, Sites *without* patch policies will not install patches.** (Legacy-style policies will be updated to new-style policies as part of the switch without any pause.)

AEM's new Patch Management engine 100% supports Microsoft Windows 10, allowing users control over individual patches for Windows 10 systems in an ecosystem entirely separated from Microsoft's own. For those users who have not yet made the switch-over, AEM's support for Legacy operating systems has also vastly improved, eliminating performance bottlenecks and ensuring smooth patching for all Windows systems being covered.

## **What's improved**

By paying close attention to how we speak to the system, we've managed to drastically improve efficiency when conducting patching operations. This means you, as the user, only ever see what you need to, and it takes less time than ever to get to you.

Continuing from our Local Cache functionality is the ability to use one or more devices in a single Site (Legacy nomenclature: "Profile") to serve patches for devices under a patch policy, reducing bandwidth usage and helping to centralise what was previously a disparate operation.

Local Patch Caches will continuously download new patches as the need for them arises; we recommend restricting individual sites to a single geographical area for the smoothest possible operation.

We've listened to your requirements for power management and we've struck a solid balance between administrative control and user freedom. Now, endpoints can be notified with a branded reboot reminder when their patch policy completes; although the system will never force a reboot on an endpoint without being explicitly instructed to, endpoints can have the point clearly communicated to them without impinging on their normal work schedules.

# 1.0: Manage patch activity at the Account- and Site-level

## Overview

Using the new Patch Management solution, users are now able to view patching information at the site- and account-level in a fraction of the time it would have taken previously. Patching operations proper are moved to policy configurations, with the ability to control individual patches without a policy becoming deprecated for the new release.

It is worth at this point encouraging administrative users to set up a patch policy now, if you do not utilise one currently, and porting your patch approvals and hide operations to it while you still have the data to-hand; following the release, this information will be lost.

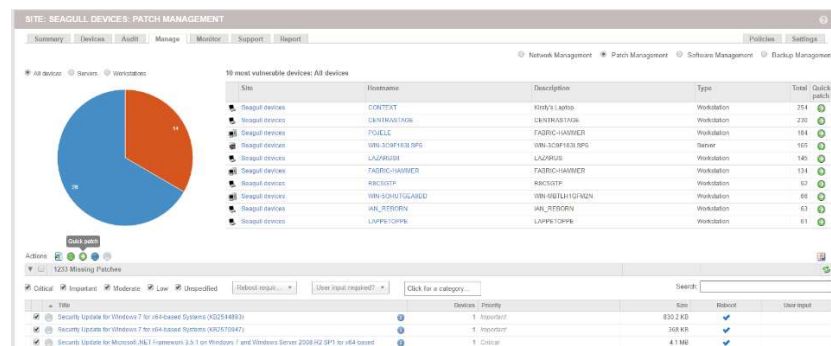
Users who do not do this will find their systems stop patching themselves after the release, as there is no policy issuing the commands to do so; however, there is no risk of patches that had previously been hidden now being installed on managed devices.

## Contents





- Removal of individual patch control on the site- and account-level
- Changing of patch status
- Removal of Account-level patch install time
- Addition of “Override” icon (detailed later in document)
- Addition of new options to view patching status

## Removal of individual patch control on the site- and account-level

In the legacy version of the Patch Management solution, the ‘Manage’ tab looks like this:



This page, now deprecated, allowed users to see the patch demands of their entire site or account's devices and perform the following operations:

-  Approve
  - Add to a list of approved patches that will be installed at the system-level patch installation time (see next section)
-  Quick Patch
  - Install the patch now on all systems that have requested the patch
-  Hide Patch
  - Hide the patch from this view
-  Reset Patch
  - Reset the status of the patch in this view (move back to 'Missing')

The new Patch Management solution operates rather differently. We have moved away from the ability to configure patches independently of each other outside of a policy, as the system offers very little in terms of accountability or historical data; furthermore, this system overcomplicates procedures that could easily be handled with a few basic user-defined rules, leading to a convoluted and unsightly interface that will soon become unmanageable with regular use.

The Site- and Account-level 'Manage' tab now functions purely as a manner in which to view configured patch policies; users are also able to view at-a-glance a list of devices most demanding of attention and a pie chart detailing how many devices are fully compliant with their policies.

To configure patches, turn to [2.0: Patch Policy Interface Refactor](#).

### *Changing of Patch Status*

As stated previously, the legacy status for patches were:

- Missing (Patches set for installation but missing on Endpoints)
- Installed (Patches that the solution has installed)
- Hidden (Patches that have been denied installation)

We have spoken to customers and found that the word "missing" could imply either that the patch had not been processed yet or that there had been errors installing it, and toggling a patch as "hidden" led users to believe patches were being individually hidden from Endpoints, whereas they were actually just being hidden from the interface. We have, as such, re-worded the statuses patches can be labelled as; these new statuses are:

- Available (Patches set for processing with Policies)
- Approved (Patches that the solution has installed or will install)
  - On the device-level, this changes to "Installed"
- Not Approved (Patches that have been denied installation)

These statuses are used in the Patch Policy interface, detailed in Section 2.0.

### *Removal of Account-level patch installation time*

There exists a setting in the Account-level Patch Management settings of the legacy interface:



This setting allows the user to choose the time when the product performs a sweep for patches approved at the account- or site-level and installs them on local Endpoints. Timing and patch installation is now handled entirely by policies, making this feature obsolete. It has been removed.

### Addition of new options to view patching status

This feature represents the most dramatic addition to the account- and site-level 'Manage' tab. Policies listed here now feature a number of icons and options:



1. 'Overrides Active' icon. This ability is expounded upon in section 3.
2. Pie chart button. This is a toggle used to determine whether the pie chart shown above this table shows data from machines targeted by all policies, or just the machines targeted by the policy being toggled here. When clicked, it should provide a visible indicator that it is selected.
3. Push changes. Use this to send changes made in a patch policy to the Endpoints receiving it.
4. Hourglass button. Spawns a dialogue box in the 'Manage' tab showing information from the last time the policy ran:

The screenshot shows a dialog box titled 'Account: PMPol2 Policy Results'. It displays the 'Last Run Time: 08 December 2015 13:00 EST'. Below this is a table with the following data:

Patch Description	Size	Devices in Scope	Successes	Failures
KB1234567 - Test Update for Mockup Purposes	3.44 MB	8	4	7
KB1234567 - Test Update for Mockup Purposes	3.44 MB	4	4	7
KB1234567 - Test Update for Mockup Purposes	3.44 MB	8	4	7
KB1234567 - Test Update for Mockup Purposes	3.44 MB	8	4	7
KB1234567 - Test Update for Mockup Purposes	3.44 MB	8	4	7

An 'OK' button is located at the bottom right of the dialog box.

- a. The patch titles link to a page carried over from legacy Patch Management showing all the machines in that profile that require this patch, divided up according to whether they have been approved, installed or not approved.
  - b. The information on this popup scrolls, there is no pagination.
  - c. 'Successes' and 'Failures' are hyperlinked numbers that lead to query pages showing the devices upon which the patch installation in question failed or succeeded.
5. Calendar button. Spawns a dialogue box in the 'Manage' tab showing the patches that will be installed the next time the policy runs. The layout is slightly different to the hourglass popup's, showing individual patches as their own collapsed tables, each one showing data on the machines that will have the patch installed on them:
    - a. Hostname of device
    - b. Description of device
    - c. (If viewed at account-level) Site of device
    - d. Device operating system

The information shown in the Calendar view is accurate as of last audit; changes made are not reflected automatically once the policy is saved. If the user changes their patch policy, they must first re-audit the targeted devices to see the data in the Calendar popup refresh.

6. Radio button, as appears throughout the policies screen. Shows applicable devices.
7. 'Run now' button. Will not appear if the policy is turned off.
8. Policy toggle.

## 1.1: Device-level Management

### *Overview*

In removing the ability to hide or approve individual patches at the Account-, Site- and Device-level, the product mandates users create new patch policies to make slight adjustments to patch approval settings. This is mitigated extensively with the introduction of [Site-level Overrides \(see Section 3.0\)](#), but users are also offered the ability to configure individual patch installations at the device-level, permitting exclusions or tolerances for individual patches without needing to alter entire policies.

When viewing the device-level 'Manage' tab, the layout will be slightly different to the one discussed earlier and in detail in Section 2.0. Where

- **Approve** is used to denote patches which have been marked for approval on the device in question by the Site- and/or Account-level policies targeting it. Patches that are approved are pushed to the device, and following their installation, are moved to the next table:
- **Installed** is used to denote patches historically-approved for this device, either by policy or as a result of user intervention. It replaces "available" for Site- and Account-level management, where it is used to show patches that have neither been explicitly approved or denied individually, and will instead be controlled by user filters.
- **Do Not Approve** denotes patches that have been approved by the policy targeting the machine, but that have historically been excluded from being installed on this particular machine. The only way to add patches to this table is by moving them here from the 'available' table; to remove the patch from a device and stop it from re-installing, it must be excluded here and then removed manually using the "Uninstall Windows Update by KB Number" component from the ComStore.



## 2.0: Patch Policy Interface Refactor

### Overview

In addition to being greatly simplified in terms of server load and speed, the new patch policy interface introduces a new routine for patch approval and exclusion, along with a number of much-demanded features to automate as much of the patching process as possible for administrators.

### Contents

- Abstract
- Support for Patching through Local Caches
- Windows Update control
- Refactor of patch approval methods
- Tailored reboot controls

### Abstract

The Patch Management solution being introduced in place of the legacy solution introduces a vast number of new features, each explained in some detail below. Despite the inclination towards change, however, considerable effort has gone into ensuring that features present in the legacy solution have been maintained in the new solution; this is part of a larger push to ensure that the migration from legacy to new Patch Management policies goes as smoothly as possible. Regard below a comparison of the legacy and new solutions to see the scale of the refactor.

Old	New																																								
<div><p>Name: <input type="text" value="fdfs"/></p><p>Policy type: Patch Management Created: 2015-09-11 08:30:49 UTC Modified: 2015-10-07 15:23:14 UTC</p><p>Targets: Type: <input type="text" value="Name"/></p><p>There are currently no targets specified.</p><p><a href="#">Add a target</a></p><p><b>PATCH MANAGEMENT POLICY OPTIONS</b></p><p>Please ensure that all of your devices are on the latest Agent version.</p><p>Schedule: <a href="#">Click to change</a> Run weekly on the following days: [Sun, Mon, Tue, Wed, Thu, Fri, Sat] at 00:00</p><p>Duration: Patching runs for 1 hours</p><p><b>POWER OPTIONS</b></p><p>Power: <input type="checkbox"/> Allow forced reboot(s) if required <input checked="" type="checkbox"/> Shut down after updates completed</p><p><b>PATCHES TO INSTALL</b></p><p>Install criteria: <input type="radio"/> Install all patches <input checked="" type="radio"/> Filter patches by <a href="#">Edit selection</a></p><table border="1"><thead><tr><th>Title</th><th>Priority</th><th>Size</th><th>Reboot</th><th>User input</th></tr></thead><tbody><tr><td>Security Update for Windows 7 for x64-based Systems (KB2570947)</td><td>Important</td><td>368 KB</td><td><input checked="" type="checkbox"/></td><td><input type="checkbox"/></td></tr><tr><td>Security Update for Windows 7 for x64-based Systems (KB2585542)</td><td>Important</td><td>1.8 MB</td><td><input checked="" type="checkbox"/></td><td><input type="checkbox"/></td></tr><tr><td>Update for Windows 7 for x64-based Systems (KB2647753)</td><td>Unspecified</td><td>1.9 MB</td><td><input checked="" type="checkbox"/></td><td><input type="checkbox"/></td></tr></tbody></table><p><a href="#">Save</a> <a href="#">Cancel</a></p></div>	Title	Priority	Size	Reboot	User input	Security Update for Windows 7 for x64-based Systems (KB2570947)	Important	368 KB	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Security Update for Windows 7 for x64-based Systems (KB2585542)	Important	1.8 MB	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Update for Windows 7 for x64-based Systems (KB2647753)	Unspecified	1.9 MB	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<div><p>Name: <input type="text" value="fdfs"/></p><p>Policy type: Patch Management Created: 2015-09-11 08:30:49 UTC Modified: 2015-10-07 15:23:14 UTC</p><p>Targets: Type: <input type="text" value="Name"/></p><p>There are currently no targets specified.</p><p><a href="#">Add a target</a></p><p><b>PATCH MANAGEMENT POLICY OPTIONS</b></p><p>Please ensure that all of your devices are on the latest Agent version.</p><p>Schedule: <a href="#">Click to change</a> Run weekly on the following days: [Sun, Mon, Tue, Wed, Thu, Fri, Sat] at 00:00</p><p>Duration: Patching runs for 1 hours</p><p><b>POWER OPTIONS</b></p><p>Power: <input type="checkbox"/> Allow forced reboot(s) if required <input checked="" type="checkbox"/> Shut down after updates completed</p><p><b>PATCHES TO INSTALL</b></p><p>Install criteria: <input type="radio"/> Install all patches <input checked="" type="radio"/> Filter patches by <a href="#">Edit selection</a></p><table border="1"><thead><tr><th>Title</th><th>Priority</th><th>Size</th><th>Reboot</th><th>User input</th></tr></thead><tbody><tr><td>Security Update for Windows 7 for x64-based Systems (KB2570947)</td><td>Important</td><td>368 KB</td><td><input checked="" type="checkbox"/></td><td><input type="checkbox"/></td></tr><tr><td>Security Update for Windows 7 for x64-based Systems (KB2585542)</td><td>Important</td><td>1.8 MB</td><td><input checked="" type="checkbox"/></td><td><input type="checkbox"/></td></tr><tr><td>Update for Windows 7 for x64-based Systems (KB2647753)</td><td>Unspecified</td><td>1.9 MB</td><td><input checked="" type="checkbox"/></td><td><input type="checkbox"/></td></tr></tbody></table><p><a href="#">Save</a> <a href="#">Cancel</a></p></div>	Title	Priority	Size	Reboot	User input	Security Update for Windows 7 for x64-based Systems (KB2570947)	Important	368 KB	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Security Update for Windows 7 for x64-based Systems (KB2585542)	Important	1.8 MB	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Update for Windows 7 for x64-based Systems (KB2647753)	Unspecified	1.9 MB	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Title	Priority	Size	Reboot	User input																																					
Security Update for Windows 7 for x64-based Systems (KB2570947)	Important	368 KB	<input checked="" type="checkbox"/>	<input type="checkbox"/>																																					
Security Update for Windows 7 for x64-based Systems (KB2585542)	Important	1.8 MB	<input checked="" type="checkbox"/>	<input type="checkbox"/>																																					
Update for Windows 7 for x64-based Systems (KB2647753)	Unspecified	1.9 MB	<input checked="" type="checkbox"/>	<input type="checkbox"/>																																					
Title	Priority	Size	Reboot	User input																																					
Security Update for Windows 7 for x64-based Systems (KB2570947)	Important	368 KB	<input checked="" type="checkbox"/>	<input type="checkbox"/>																																					
Security Update for Windows 7 for x64-based Systems (KB2585542)	Important	1.8 MB	<input checked="" type="checkbox"/>	<input type="checkbox"/>																																					
Update for Windows 7 for x64-based Systems (KB2647753)	Unspecified	1.9 MB	<input checked="" type="checkbox"/>	<input type="checkbox"/>																																					

### *Support for Patching through Local Caches*

In addition to using Windows Update as a source, users can now nominate a device to serve as a Local Cache for Patching (a “Patch Cache”). This is an augmentation of pre-existing Local Cache functionality; however, caches can now be one of three categories:

- Components
- Patches
- Both

Setting up a new Patch Cache is as simple as nominating a device - you can set a Network Node to perform the duties of a Patch Cache – and configuring where it stores its data. Caches can be configured to delete a patch a certain number of days after downloading it in order to save space. Once you have a Patch Cache set up, your devices in that site will default to it for patch downloads, treating the Windows Update service solely as a fall-back depending on user preference.

You can nominate any Desktop, Laptop or Server as a Patch Cache – not just Windows devices – provided it has up-to-date audit information. Once a cache has been nominated, find it easily from the Site Settings menu or via a new filter implemented for the release targeting Local Caches.

As soon as a device submits data on what patches it requires, the platform will filter the request through the relevant patching policies, and go on to instruct the Patch Cache to download these new patches. Once the patching window begins, devices will request these patches from the Cache/s nominated by the user.

### *Windows Update control*

Although the functionality to control Windows Updates remains in a policy all its own, a new feature has been added – a simple checkbox – to disable Automatic Updates on targeted machines. This will configure machines targeted in such a way that their intrinsic Windows Update functionality is disabled, permitting only the AEM Patch Management solution to work.

Deleting the policy does not remove this setting; the only way to re-enable Automatic Updates on machines that were targeted with this setting is to disable the option as part of the policy’s typical run. This option will override any Windows Update policy set on the Site.

## Refactor of Patch Approval methods

In-line with [Section 1](#), Patch Policies are now configured using three tools:

- Approve these patches
- Do not approve these patches
- Configure individual patches

The “install all patches” option has been removed; users now explicitly have to configure an approval filter. To install all patches automatically, use a filter like this:



**Approve these patches** has changed little from what exists currently on production; the value is shown in a second section – **Do not approve these patches**. This allows users to set conditions that override their approval – configurations such as “Approve critical security patches, but do not approve critical security patches with ‘Defender’ in the title” are entirely possible.

**Configure individual patches** is a new setting devised for the forthcoming update. Here the user is able to see three complete lists, the status of which are detailed above, which operates *independently* from the two settings above it.

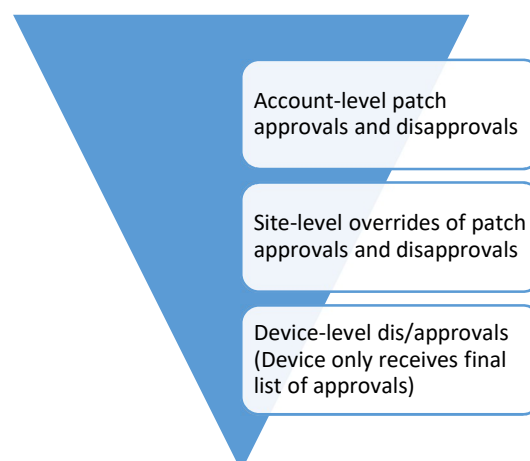
Put simply, users are able to configure filters for patches – “Allow critical patches” – but are then able to view a complete list of all patches submitted from **the entire account’s** devices’ audit data, with the ability to configure individual patches regardless of filters.

As such, this section overrides disapprovals, which override approvals.

The user is able to select from “Available patches” a patch that would have not been approved by the filter above it and explicitly state that that patch in particular is to be approved regardless of any filters defined that would exclude it. Furthermore, users who wish to make doubly sure of their exclusions are able to select individual patches that may already have been blocked by a filter and state explicitly that the selection is not to be approved under *any* circumstance.


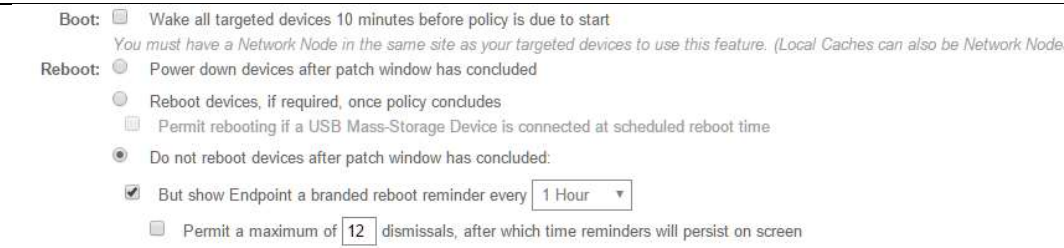
The ‘Approve’ and ‘Do Not Approve’ lists can have patches removed from them individually or via the action bar. The ‘removal’ process takes the patch being moved from its explicit list and pushes it into the “Available” section again, where it can be approved or disapproved by the filters above it.

With section 1.1 taken into consideration, the patch approval triangle will adopt the following form:



## Tailored reboot controls

The reboot section has been completely re-factored; very little of the legacy solution remains:

Legacy	
New	

Reboots are now configurable with much greater control, with actions only ever taking place following the conclusion of a patching policy.

We now support Wake-on-LAN requests, although a Network Node must be nominated to send the requests. If multiple nodes are nominated, all will send requests. When testing, be aware that Wake-on-LAN is a finicky setting – it must be enabled in BIOS/EFI and typically only works for Laptops when they have an active mains connection.

Users are given the option either to power down – as in Legacy – or reboot their machines, and from there, various options can be configured. Users can cancel reboots if USB Sticks are inserted – the default setting – to stop servers from rebooting into a LiveUSB (a common request).

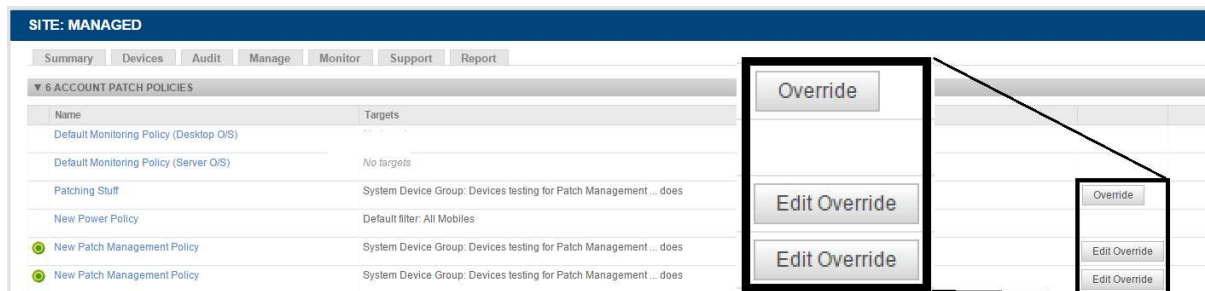
If the user chooses to mandate reboots, they can use a branded reboot reminder (the branding for which is taken from the user's Branding page, a new image called "Patch Reboot Window", with the same dimensions as the CSM image to encourage long images with a recognisable company name) which will either re-appear every x hours or will re-appear up to a point of x times, past which it will persist on screen without the ability to be dismissed.

### 3.0: Site-level overriding of Account-level policy options

#### Overview

You will have noticed the use of the term “site-level overrides” in the previous section. This is a new feature being introduced solely for Patch Management with CS-2016-3; its popularity will directly influence how likely the rest of the product is to be retrofitted to accommodate it.

Account-level policies can be made as normal and turned on at the site-level to affect devices there. Users wishing to make small adjustments to account-level policies as they are applied to individual sites no longer have to copy policies or make them from scratch, however; now, when an account-level policy is viewed from the site-level policies tab, the following option is visible:



Viewing a policy from an “Override” button (or “Edit Override” if the policy already has one active) allows the user to view the same policy with the following additional option for each section:

Override: ☒ ON

Local Cache: ☒ Download patches from Windows Update  
☐ Use a Local Cache to download and distribute updates  
☐ Permit devices to contact Windows Update for updates  
Use a nominated Local Cache for Patching to store all updates

WINDOWS AUTOMATIC UPDATES

Override: ☐ OFF

Update Control: ☐ Disable device-level Automatic Updates on targets  
This setting will override any active Windows Update policies

PATCH APPROVAL

Add Rule: ☐ OFF

Selecting “Override” (or “Add Rule” in the case of approval filters) will enable that section of the policy and allow the user to edit how it works for that Site only. If the user slides “Override” back to OFF, the settings will revert.

A potential pitfall is if administrators state as part of an Account-level policy that a Local Cache must be used, when there is not one nominated for a particular site. In this case, the Agent is configured to fall back to downloading patches from Windows Update; if this option is disabled, however, a line of text is populated in the Agent logs for the affected devices that have nowhere to download patches from, and the policy will fail on these devices.

## 4.0: Performance improvements

As part of the re-factor, large amounts of code have been pulled out and re-written. This has led to multiple fixes and improvements, coupled with a general faster user experience. The details of these improvements are listed below.

### *Support for outdated Windows Update Agent versions*

Versions of Windows 7 that shipped before Service Pack 1 come with an obsolete version of the Windows Update Agent (WUA) that does not play nicely with the commands sent by the Agent to perform a patch scan. The end-result of this is that Pre-SP1 Windows 7 machines will freeze to a near-halt immediately following the Agent installation as the command to perform a patch scan as part of the initial audit is processed.

As part of the refactor, a checking routine has been written which installs the latest version of WUA as well as several updates intended to speed up patch scanning and installation on Windows 7 machines when a device matching this description is audited. This WUA check is part of the patch scan code, meaning endpoints running W7 SP0 should see improvements on the first audit the machine performs post-update.

### *Improvements in handling Windows Update policies*

The options in the Windows Update policy have been re-written to be easier to understand and work with; furthermore, functionality on the agent-side has been significantly improved to ensure settings are always congruent between the agent and the platform.

## 5.0: Acknowledgements

### *Error 0x8024a204*

We have identified a peculiarity involving Microsoft's handling of patching which results in Endpoints displaying the following error when they have installed patches via a Local Cache (and not sourced them directly from Microsoft):



This error only appears when Endpoints access the “Windows Update” section of the settings menu, which should no longer be a necessary step as updates are delivered automatically without needing the involvement of Microsoft's own Patch Management routines.

We have sourced the issue to the particular method we use to place patches in Windows' update cache directory – while thoroughly tested and 100% functional in all cases, it triggers this issue. The error is meaningless, and can be dismissed without concern – re-checking for updates will clear it from this interface. Patches that trigger this error will have been installed without issue.

Until Microsoft fix this issue, the error will be shown when endpoints look for it; we apologise for any inconvenience this may cause.