



Symantec Endpoint Management Office Hours

August 10, 2022



What are Office Hours?

- Calls hosted by the extended Endpoint Management (EPM) product team designed to facilitate regular communication and open dialog with customers and partners
 - Modeled after sessions hosted by Layer 7 team
 - Typically 30-60 minutes in duration
- First part of session usually devoted to information shared by members of EPM product team (presentation, demo, etc.,)
- Second part of session devoted to open discussion to enable customers and partners to ask questions and provide feedback
 - Not intended to be used as a substitute for technical support calls, means for reporting potential defects, etc.,

Housekeeping

- An updated Cloud Enabled Management white paper has been published and is available here:
- https://techdocs.broadcom.com/content/dam/broadcom/techdocs/us/en/dita/symantec-security-software/endpoint-security-and-management/it-management-suite/generated-pdfs/cloud_enabled_management_for_itms.pdf
 - Short URL: shorturl.at/bcklr
- Modern Device Management (MDM) support for Windows is expected to be a part of our first ITMS release in 2023.
 - If you are interested in participating providing feedback regarding that functionality as part of a technical preview, please reach out to me through our online community

Agenda

1

What's New in ITMS 8.6 RU3?

- A. Symantec Installation Manager
- B. O/S Support
- C. Patch Management Solution
- D. Deployment Solution
- E. Symantec Management Agent
- F. Symantec Management Platform/Console
- G. Task Management

2

Open Discussion: Questions and Answers



What's New in ITMS 8.6 RU3?

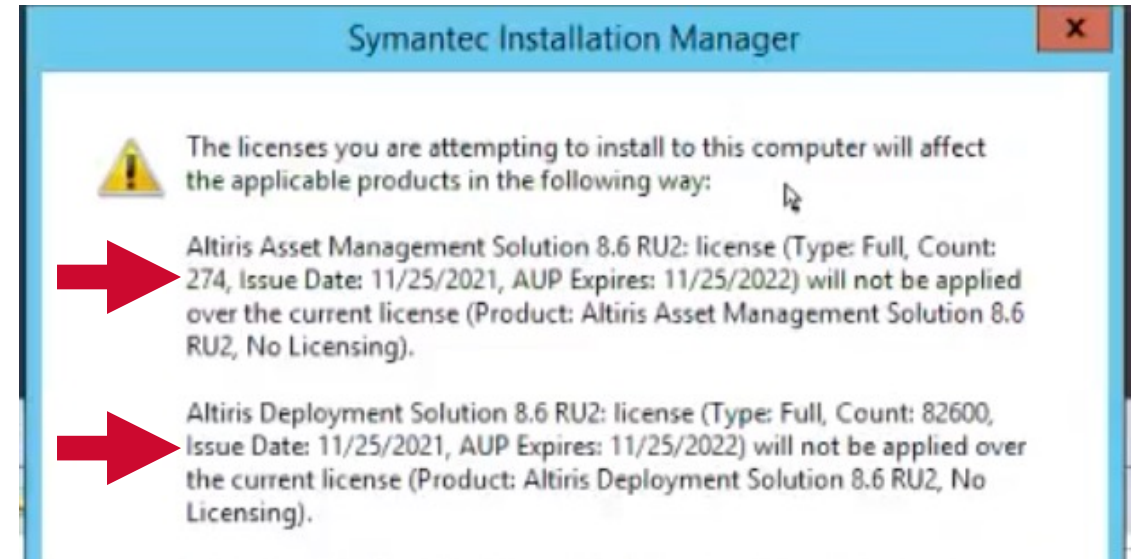


Symantec Installation Manager: License Files with Future Start Dates

Use case: As an ITMS customer, I need to apply license files with future start dates, so that I can load such license files when I receive them rather than waiting until the start date

- When attempting to load license files with future start dates, users previously received a message that such licenses cannot be applied

Prior to changes to SIM

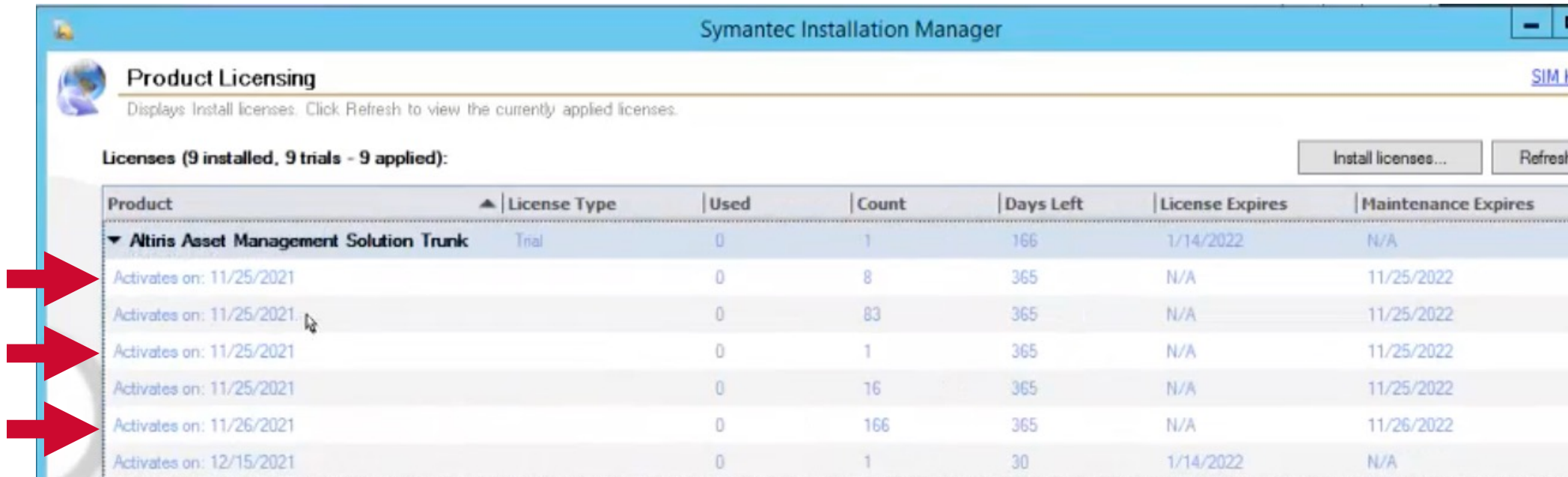


Note: Screenshot was taken on 11/15/21 when attempting to load a license file with start date of 11/25/21

Symantec Installation Manager: License Files with Future Start Dates

- License files with future start dates can now be loaded, but do not become active until the start date
- The date on which a license file becomes active is displayed

After changes to SIM



Symantec Installation Manager

Product Licensing
Displays Install licenses. Click Refresh to view the currently applied licenses.

Licenses (9 installed, 9 trials - 9 applied):

Install licenses... Refresh

Product	License Type	Used	Count	Days Left	License Expires	Maintenance Expires
▼ Altiris Asset Management Solution Trunk	Trial	0	1	166	1/14/2022	N/A
Activates on: 11/25/2021		0	8	365	N/A	11/25/2022
Activates on: 11/25/2021		0	83	365	N/A	11/25/2022
Activates on: 11/25/2021		0	1	365	N/A	11/25/2022
Activates on: 11/25/2021		0	16	365	N/A	11/25/2022
Activates on: 11/26/2021		0	166	365	N/A	11/26/2022
Activates on: 12/15/2021		0	1	30	1/14/2022	N/A

Note: Screenshot was taken on 11/15/21 after loading license files with start dates of 11/25/21, 11/26/21 and 12/15/21

Operating System Support

- **Expanded agent and platform support**
 - Red Hat Enterprise Linux 8.5 and Oracle Linux 8.5
 - Red Hat Enterprise Linux 8.6 and Oracle Linux 8.6
 - Red Hat Enterprise Linux 9
 - SUSE 12 SP5
 - Ubuntu 22.04 LTS
 - Windows Server 2022 support for Notification Server



Patch Management – Compliance by Computer Report

Use case: As an ITMS administrator, I need to filter the Compliance by Computer report by Severity Level, so that I can report on the compliance rate with respect to other those bulletins/updates associated with vulnerabilities of that Severity Level

- The Compliance by Computer report shows the compliance rate for all applicable updates, regardless of the severity level of the associated vulnerability (if any)
- Some customers only care about the compliance rate with respect to bulletins/updates associated with Critical vulnerabilities
- Beginning with ITMS 8.6 RU3, users can filter the Compliance by Computer report by Severity Level or Custom Severity

Patch Management – Compliance by Computer Report

No filters applied – showing compliance based on all applicable updates

Reports ▾ Software ▾ Patch Management ▾ Compliance ▾ Windows ▾ Windows Compliance by Computer

Windows Compliance by Computer

High-level compliance view of Windows computers managed by this server. Further refine the results with the Search feature. Right-click a particular resource view more detailed information.

Actions ▾ Save As ▾ Print | Run ☒ Auto-run View: Select a value... ▾ Group by: ▾

Parameters Showing **Computer**, To=22/07/2022 00:00:00, Release Date From=22/07/2021 00:00:00, Severity=--Any--, Vendor=--Any--, Supersede Status=Not Superseded, Custom Se Distribution Status=(All), Operating System=--Any--, Filtered By **Windows Computers with Software Update Plug-in Installed**

Release Date From: 22/07/2021 To: 22/07/2022

Vendor: --Any-- Operating System: --Any--

Category: --Any-- Distribution Status: (All) Supersede Status: Not Superseded ▾

Severity: --Any-- Custom Severity: --Any--

Computer Name	Compliance	Applicable (Count)	Installed (Count)	Not Installed (Count)
Igrp12Camngr	75.68%	37	28	9

Filtered to show compliance based only on updates with associated severity of "Important"

Reports ▾ Software ▾ Patch Management ▾ Compliance ▾ Windows ▾ Windows Compliance by Computer

Windows Compliance by Computer

High-level compliance view of Windows computers managed by this server. Further refine the results with the Search feature. Right-click a particular resource view more detailed information.

Actions ▾ Save As ▾ Print | Run ☒ Auto-run View: Select a value... ▾ Group by: ▾

Parameters Showing **Computer**, To=22/07/2022 00:00:00, Release Date From=22/07/2021 00:00:00, Severity=Important, Vendor=--Any--, Supersede Status=Not Superseded, Distribution Status=(All), Operating System=--Any--, Filtered By **Windows Computers with Software Update Plug-in Installed**

Release Date From: 22/07/2021 To: 22/07/2022

Vendor: --Any-- Operating System: --Any--

Category: --Any-- Distribution Status: (All) Supersede Status: Not Superseded ▾


Severity: Important Custom Severity: --Any--

Computer Name	Compliance	Applicable (Count)	Installed (Count)	Not Installed (Count)
Igrp12Camngr	85.71%	7	6	1

Patch Management – Compliance by CVE-ID Report

- **Use case:** As an IT administrator, I need to filter the Compliance by CVE-ID report to only display those CVE-IDs for vulnerabilities with CVSS scores of certain level, because my organization is only interested in compliance with respect to such CVE-IDs.
 - The Compliance by CVE-ID report previously showed the compliance rate for all CVE-IDs, regardless of the CVSS score assigned to the associated vulnerability
 - Some customers only care about the compliance rate with respect to CVE-IDs associated with vulnerabilities with CVSS scores of a certain level
 - Beginning with ITMS 8.6 RU3, users can filter the Compliance by CVE-ID report by the CVSS v.2 or CVSS v.3 score assigned to the vulnerability associated with the CVE-ID
 - This feature involves a change to the product and a change to the Windows patch data feed
 - Product change included in ITMS 8.6 RU3
 - Change to data feed expected to be made within the next month
 - Once change to data feed is made, you can use new feature

Patch Management – Compliance by CVE-ID Report

 **CVE-2022-30136**
Windows Network File System Remote Code Execution Vulnerability.


CVE ID





Description: Windows Network File System Remote Code Execution Vulnerability.

CVSS v2 base score: 10 (High)

CVSS v3 base score: 9.8 (Critical)



 **Windows Compliance by CVE ID**
High-level compliance view of CVE ID resources for Windows computers managed by this server. Further refine the results with the Search feature. Right-click a particular resource

 Actions ▾  Save As ▾  Print |  Run ☒ Auto-run

Parameters Showing Computer, Supersede Status=Not Superseded, Operating System=--Any--, Vendor=--Any--, CVSS version 3=High (7.0-8.9), CVSS version 2=Status=(All)

Year:

Vendor: Operating System: CVSS v2 base score:

Distribution Status: Supersede Status: CVSS v3 base score:

CVE ID	Compliance	Applicable (Count)	Installed (Count)	Not Installed (Count)	CVSS v2	CVSS v3	Description
CVE-2022-30220	100.00%	1	1	0	7.2	7.8	Windows Co
CVE-2022-30206	100.00%	1	1	0	7.2	7.8	Windows Pr
CVE-2022-30190	100.00%	1	1	0	9.3	7.8	Microsoft W
CVE-2022-30136	100.00%	1	1	0	10.0	9.8	Windows N



Patch Management – Updates that cannot be automatically downloaded

Use case: As an IT administrator, I need an easy way to manage software updates that cannot be downloaded automatically to the Notification Server, so that I can use the Patch Management Solution to install such updates and report on compliance regarding same.

- Why can't some software updates be downloaded in an automated manner?
 - Some software updates are only available to registered users
 - Some require the acceptance of a EULA online before downloading
 - Some require an active subscription
 - Others can no longer be downloaded from the vendor because the the product has been EOL'd or because the vendor always uses the same URL for the latest update and doesn't make previous updates available once a new update is released
- Examples include Oracle Java, Google Chrome and Windows O/S images that are part of enterprise agreements
- In the past, such updates were generally filtered out of the Windows patch data feed
 - Two exceptions: Oracle Java updates and Windows feature updates were included in the data feed, but required workaround in which customers had to manually download the updates and put them in a particular location

Patch Management – Updates that cannot be automatically downloaded

- If updates are not included in the data feed, Patch Management Solution cannot be used to install them or report on compliance
- In cases where software update was included in data feed and later removed from data feed, existing policies referencing those updates were deleted
- This posed a challenge for customers
 - Some customers have long testing cycles and don't finish testing an update before the vendor releases a new update
 - In the case of applications such as Google Chrome, this meant, for example, that Google Chrome 99 would be removed from the data feed when Google Chrome 100 was released since Google re-used the download URL for Google Chrome 99 for Google Chrome 100
 - The end result was that policies that included Chrome 99 got deleted once Google Chrome 100 was released and customer imported updated data feed (which no longer included Google Chrome 99)
 - This also posed a challenge regarding Compliance by CVE-ID report added in 8.6 RU2
 - If customer installed Google Chrome 99 on all applicable computers to address a particular vulnerability, Compliance by CVE-ID report would show 100% compliance for CVE-ID associated with that vulnerability
 - When Google Chrome 100 was released, Google Chrome 99 was removed from data feed and Compliance by CVE-ID report would show 0% compliance because Google Chrome 100 had not yet been distributed (Environment was actually in 100% compliance, but report showed 0% compliance because it was not aware of Google Chrome 99)


Patch Management – Updates that cannot be automatically downloaded

- Moving forward, updates that cannot be automatically downloaded will be kept in data feed
 - Such updates will be visible in ITMS 8.6 RU3 and above, but will be hidden in previous versions of ITMS
 - Versions of ITMS prior to 8.6 RU3 will continue to delete policies that include updates that can't be automatically downloaded
 - ITMS 8.6 RU3 will not delete policies that include updates that could previously be automatically downloaded, but can no longer be downloaded in such manner
 - This change to the Windows patch data feed is expected to be implemented a few weeks after the ITMS 8.6 RU3 release, so that it does not interfere with Patch Tuesday (August 9)

Patch Management – Updates that cannot be automatically downloaded

- Manual Download column has been added to Software Bulletin Details report to identify updates that need to be manually downloaded

Reports ▾ Software ▾ Patch Management ▾ Software Bulletins ▾ Software Bulletin Details

 **Software Bulletin Details**
Detailed Software Bulletin information for computers managed by this server.

Actions ▾ Save As ▾ Print | Run ☒ Auto-run

Parameters Showing Computer, Supersede Status=(All), Platform=Windows, Distribution Status=(All)

Platform: Windows ▾ Vendor: Microsoft ▾

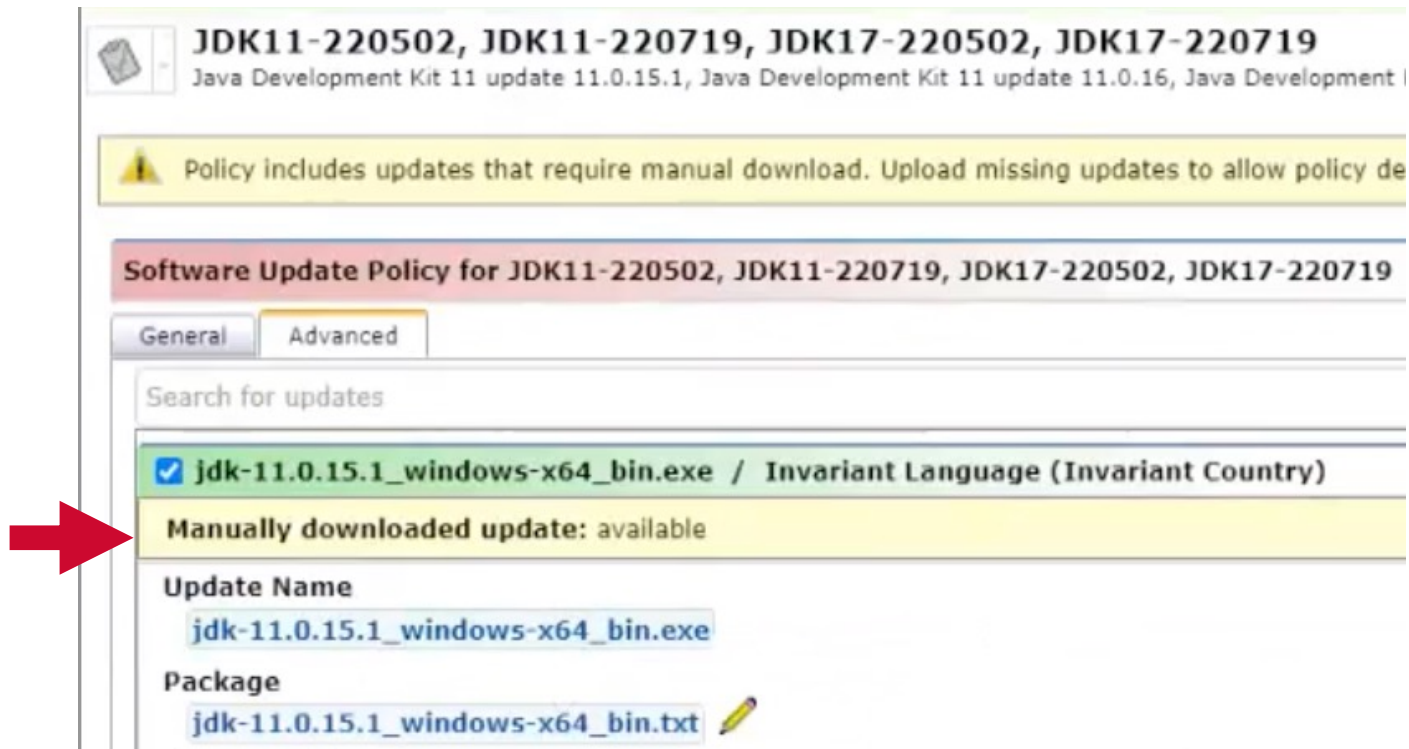
Distribution Status: (All) ▾

Supersede Status: (All) ▾

Bulletin	Severity	Custom Sever...	Manual Dow...
MSWU-092	Unclassified	Not Set	Yes
MSWU-083	Unclassified	Not Set	Yes
MS05-038	Critical	Not Set	Yes
MS03-005	Important	Not Set	Yes
MS02-053	Critical	Not Set	Yes
MSNS22-07-MRNET-5015733	Unclassified	Not Set	

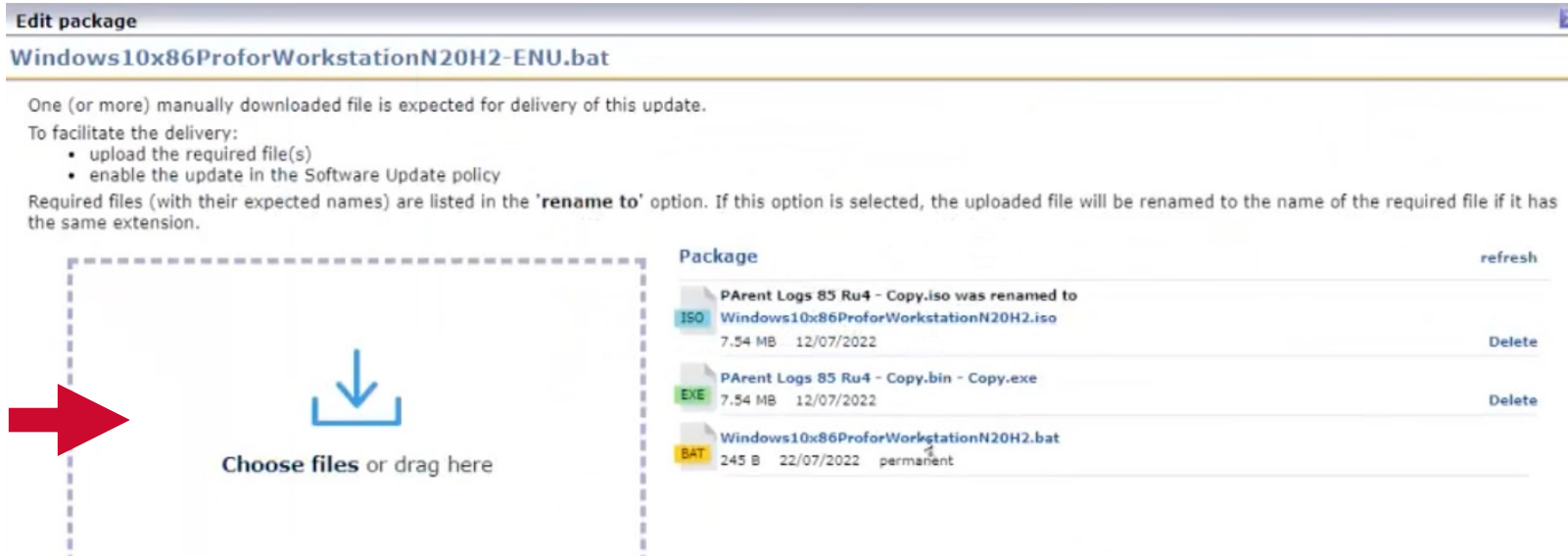
Patch Management – Updates that cannot be automatically downloaded

- When creating Software Update policy with updates that need to be manually downloaded, you will see a message indicating that the update needs to be manually downloaded



Patch Management – Updates that cannot be automatically downloaded

- You can then browse to the package file(s) and the utility will create a folder of the appropriate name and in the expected location to store the file(s)

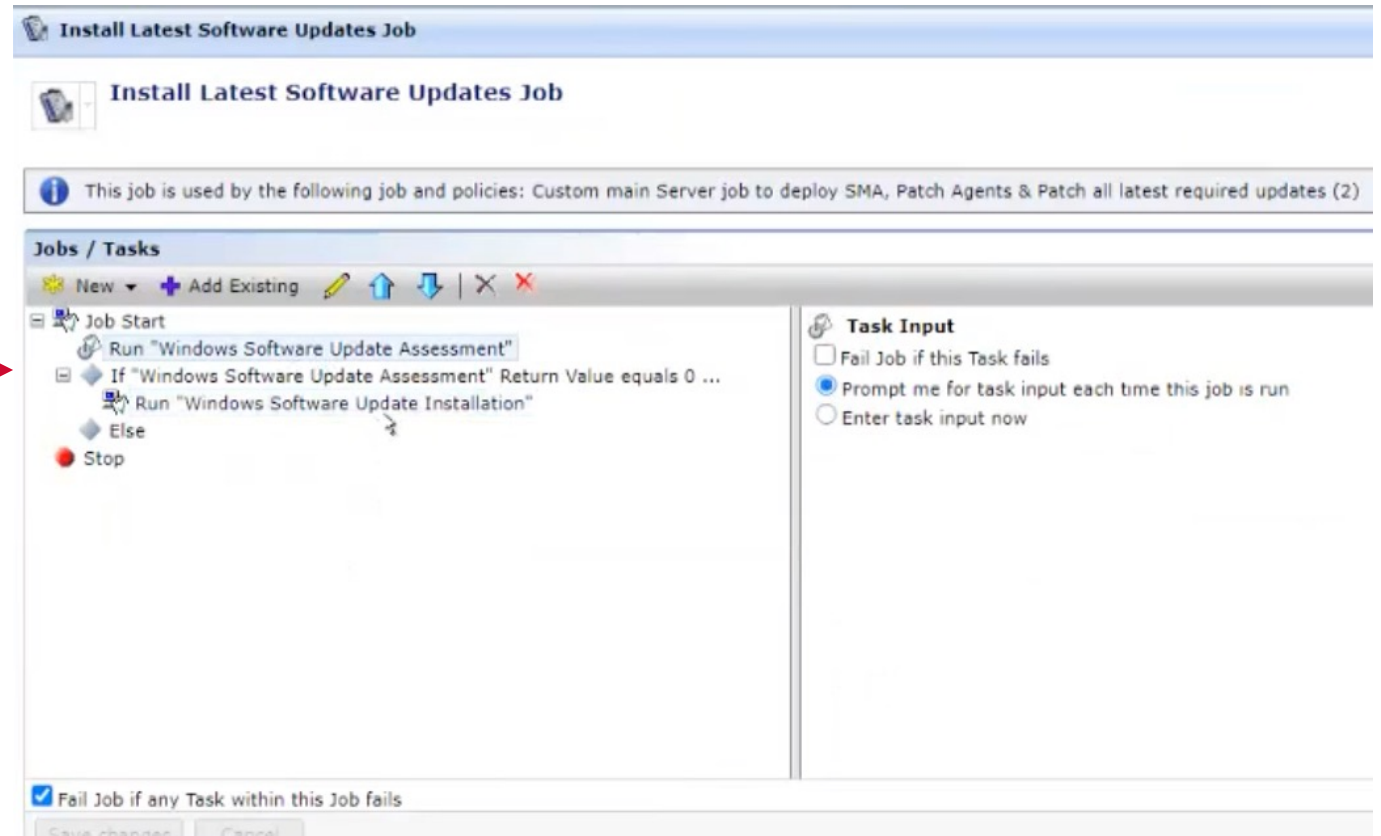


- ITMS expects installation files to have specific names; the utility will rename the selected file to the expected name if it has the same extension as the expected file name
- You can upload multiple files to the folder that will be created; some customers include additional files to maintain configuration settings that get overwritten by updates
- Software Update packages are generally not replicated down a hierarchy, but will be in the case of manually download updates in most cases

Patch Management: Install Updates During Provisioning/Imaging

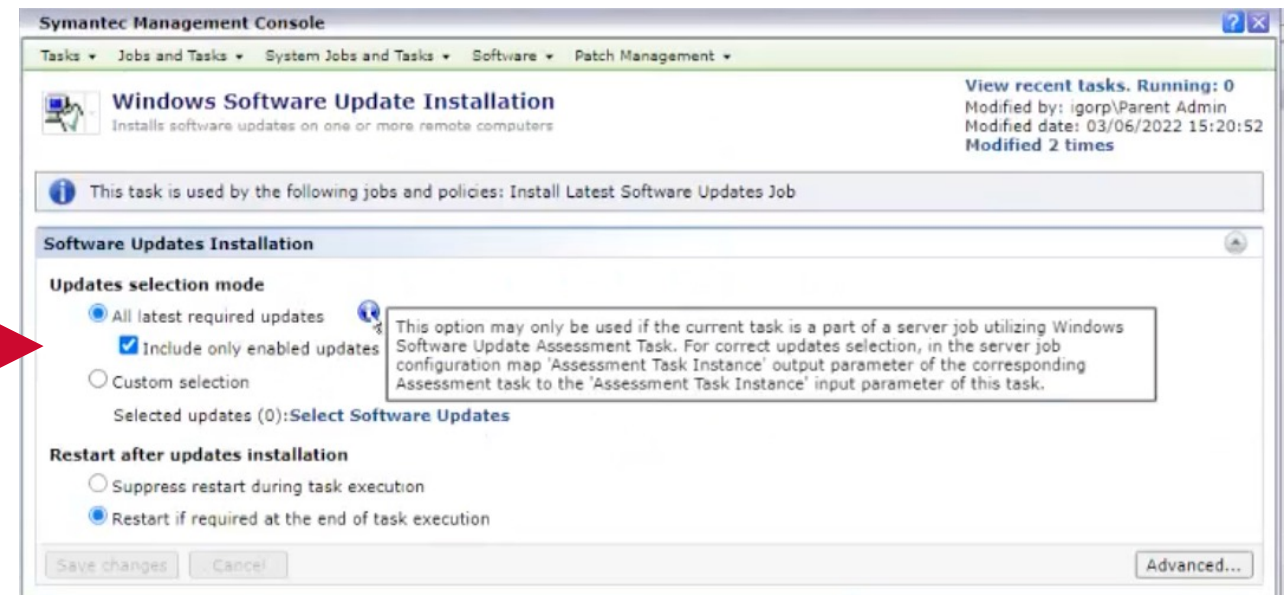
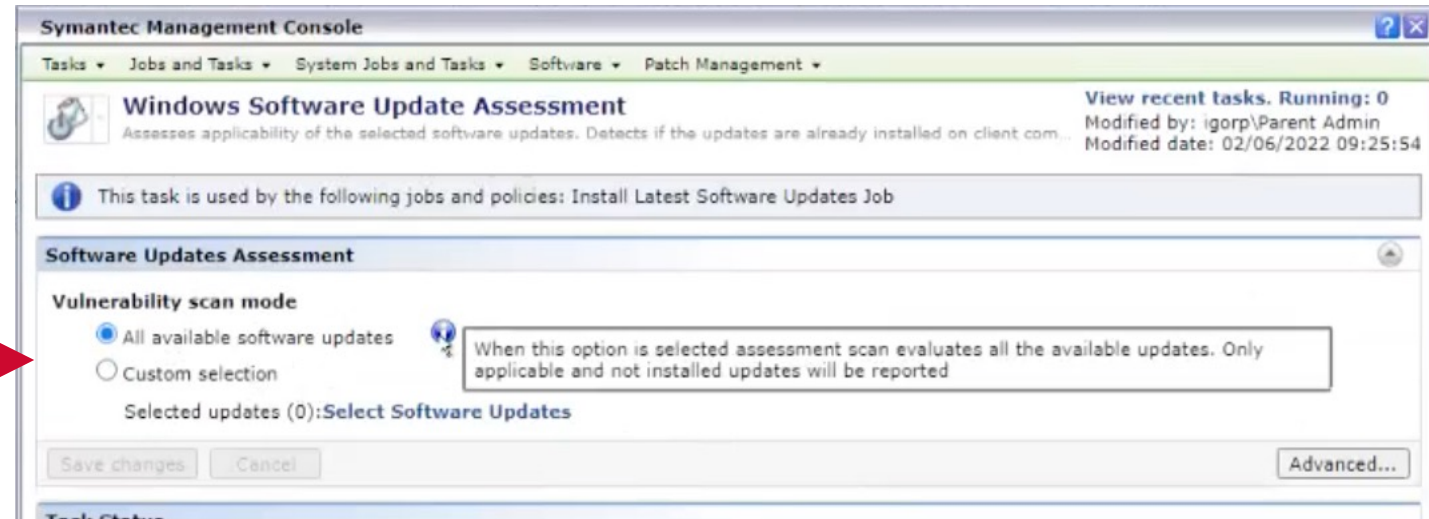
Use case: As an IT administrator, I need to be able to install applicable patches on machines as part of the provisioning process, so that newly provisioned devices are not vulnerable as soon as they come online.

- Prior to 8.6 RU3, server tasks did not support use of the software update assessment and software update installation tasks
- In 8.6 RU3, default “Install Latest Software Updates” **server job** added with software update assessment and software update installation tasks
 - Job can be cloned and settings changed



Patch Management: Install Updates During Provisioning/Imaging

- **Windows Software Update Assessment** task can now scan for all available software updates (new) or just select software updates
- **Windows Software Update Installation** task can now install all latest updates (new), only latest updates that are enabled (new), or just select software updates
 - “**Latest**” - in the case of updates that are part of supersedence chain, only latest update will be installed
 - “**Enabled**” – update is included in existing software update policy that is enabled and update itself is enabled within policy



Patch Management: Install Updates During Provisioning/Imaging

- If provisioning job targets multiple machines and tasks fails on some machines, it is possible for job to proceed to next task on other machines

Install Latest Software Updates Job

This job is used by the following job and policies: Custom main Server job to deploy SMA, Patch Agents & Patch all latest required updates (2)

Jobs / Tasks

- New
- Add Existing
- Job Start
 - Run "Windows Software Update Assessment"
 - If "Windows Software Update Assessment" Return Value equals 0 ...
 - Run "Windows Software Update Installation"
 - Else
 - Stop

Task Input

- ☐ Fail Job if this Task fails
- ☐ Prompt me for task input each time this job is run
- ☒ Enter task input now

For Selected Devices: prompt at run time

For Assessment Task Instance: use output from a previous task
Windows Software Update Assessment - Assessment Task Instance

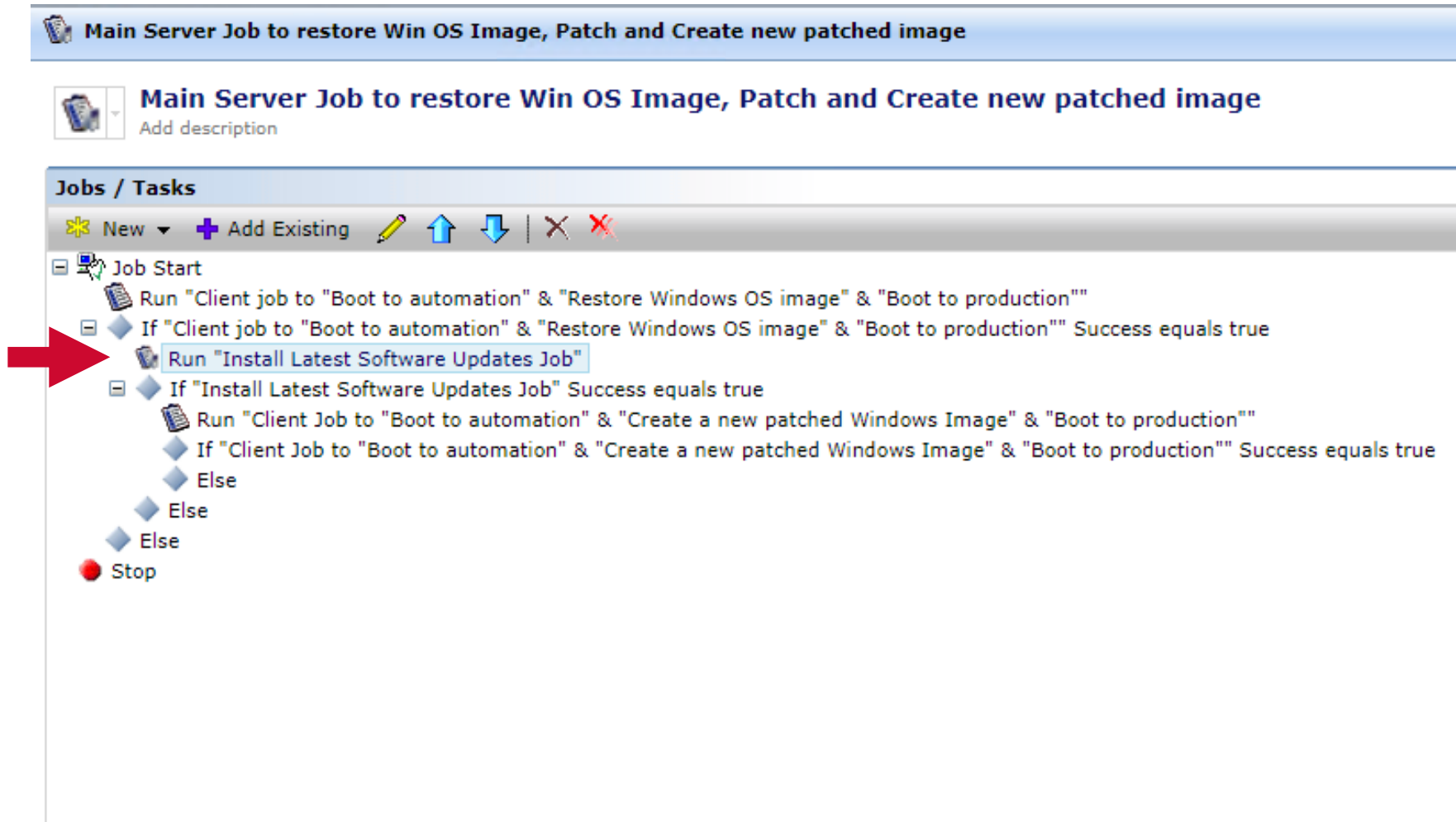
Completion Requirements:

Proceed to the next task:
After 60 Minutes if 95 % of computers have completed

Fail and move on:
After 90 Minutes

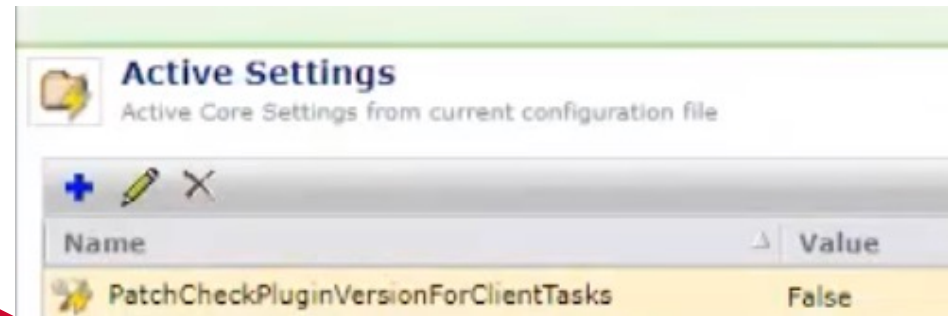
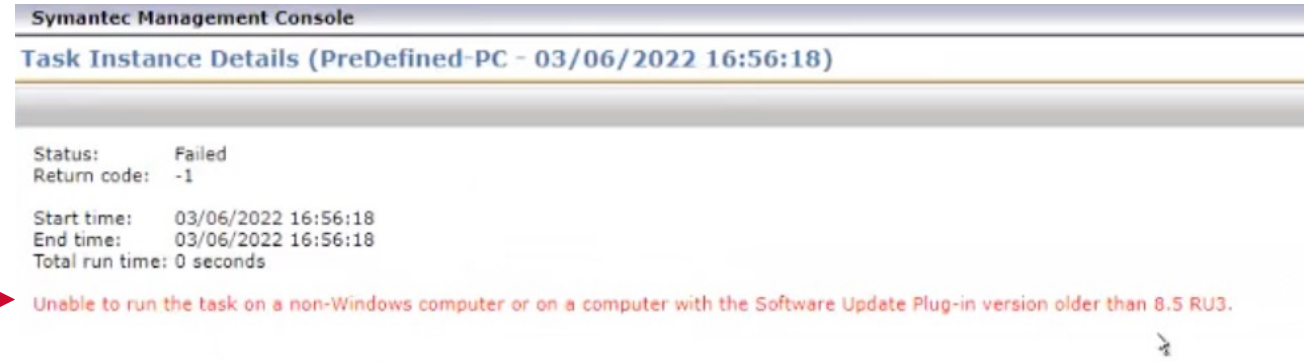
Patch Management: Install Updates During Provisioning/Imaging

- If imaging/provisioning is typically done as part of a client job, new job can be created that combines Install Latest Software Updates job with client job



Deployment Solution: Install Patches on Pre-Defined Computers

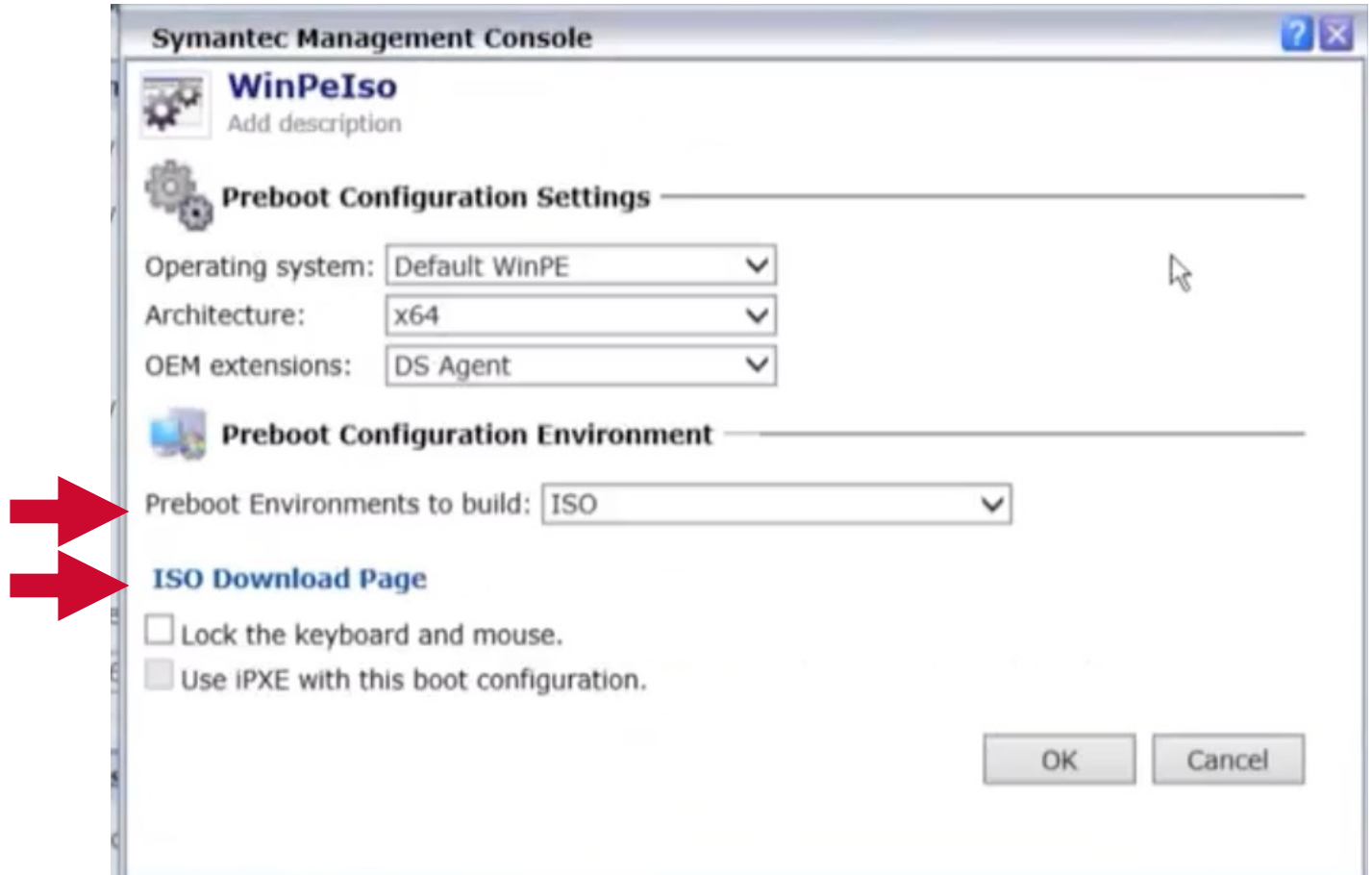
- Prior to 8.6 RU3, it was not possible to run the Software Update Assessment or Software Update Installation tasks on Pre-Defined computers as part of the deployment process
- Doing so would result in an error message regarding the version of the Software Update plug-in, regardless of which version (if any) was actually installed
- In 8.6 RU3, it is now possible to run the Software Update Assessment and Software Update Installation tasks on Pre-Defined computers by setting the value of the new PatchCheckPluginVersionForClientTasks setting to “False”



Deployment Solution: Preboot Support for Remote Imaging

Use case: As a remote user or technician out in the field, I need to locally boot into a preboot environment when remotely imaging a computer using Cloud Enabled Management

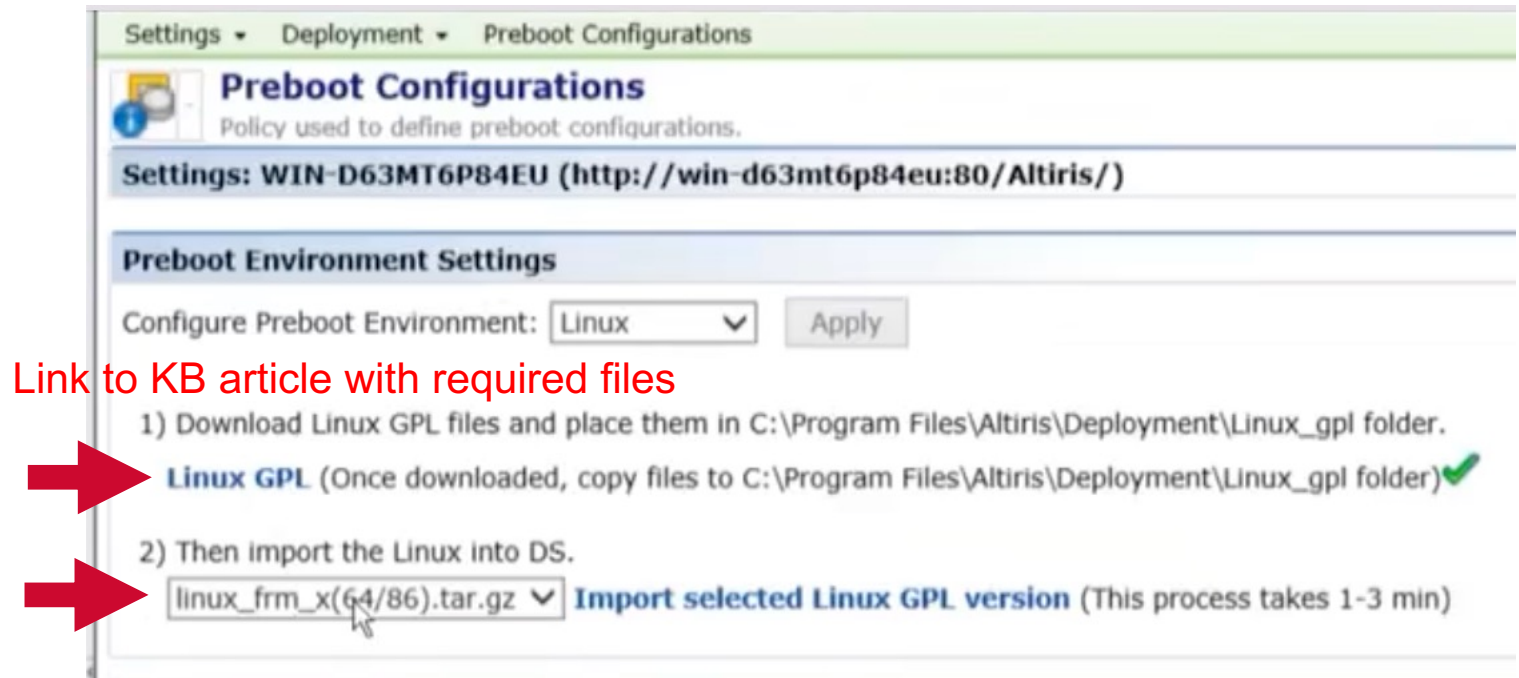
- ITMS 8.6 RU3 enables administrators to create an .ISO file containing WinPE or Linux PE
- The .ISO file gets saved to the Notification Server
- The .ISO file can be used to create a bootable disk from a USB drive, CD or DVD
- The .ISO can also be published to a web page from which it can be downloaded



Deployment Solution: Download/Import Linux PE

Use case: As an IT administrator, I need to download the Linux PE files and import them into Deployment Solution because such files can no longer be re-distributed and installed as part of the Deployment Solution

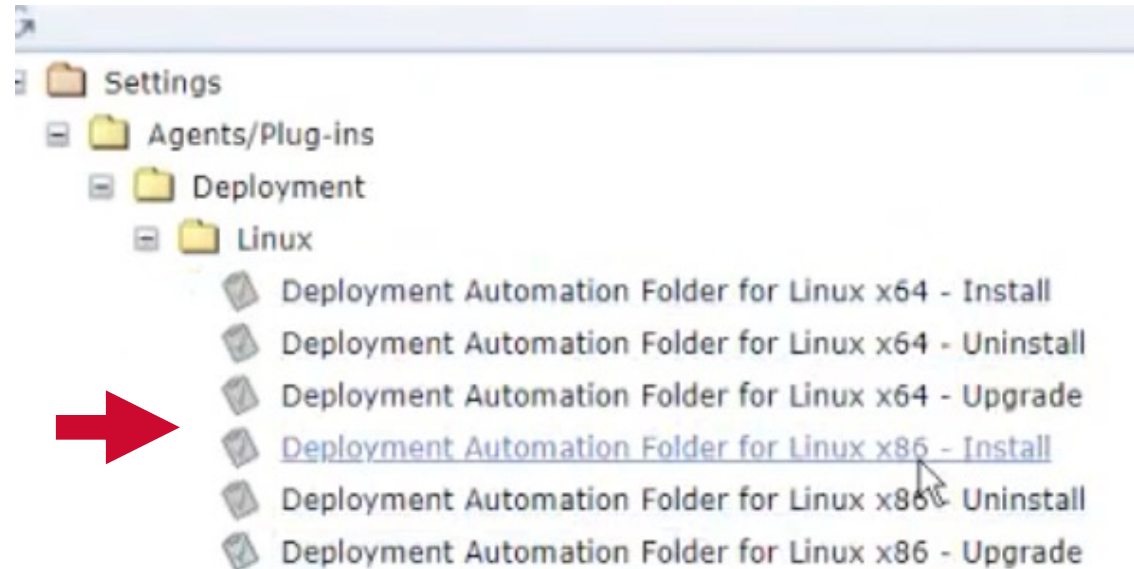
- As was previously the case regarding WinPE, Linux PE is no longer re-distributed as part of the DS
- Linux PE must now be downloaded and imported within the Symantec Management Console
- Linux PE files can be downloaded from KB article (link appears in console)



Deployment Solution: Linux 64-bit support

Use case: As an IT administrator, I need ITMS to support the capture and deployment of 64-bit Linux images, so that I do not need another tool for that purpose.

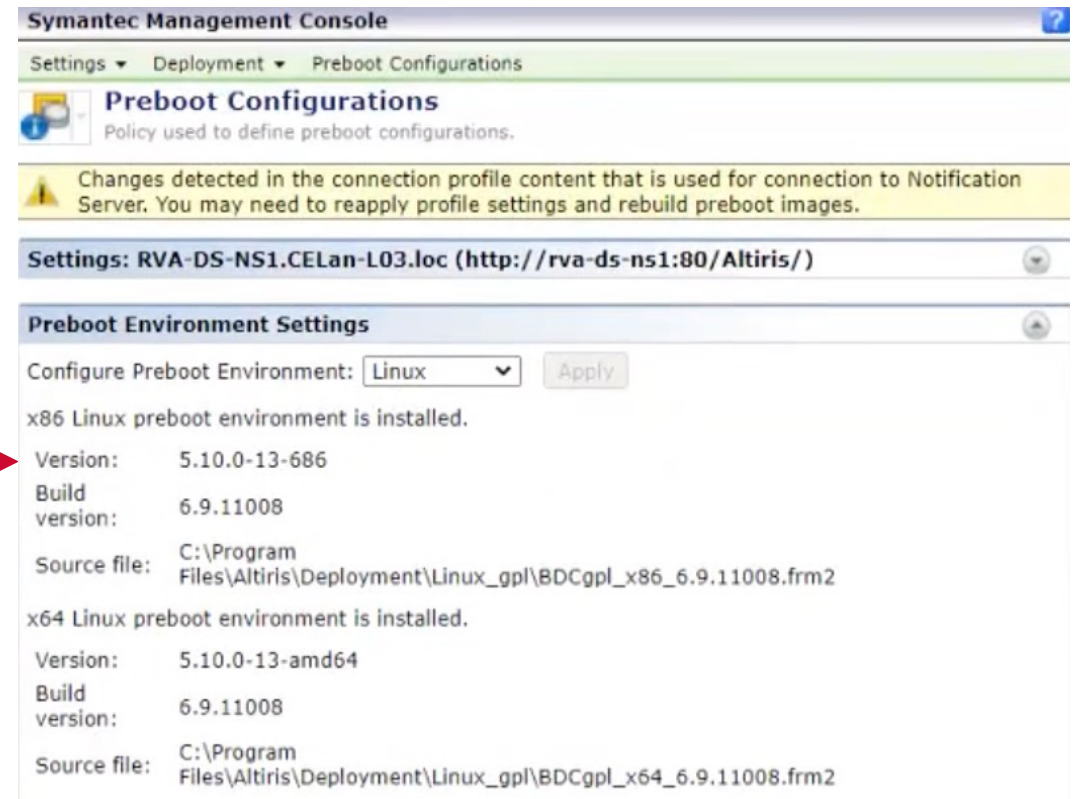
- The 32-bit version of Linux PE was previously included in the Deployment Solution installation
- Deployment Solution was previously not able to use the 64-bit version of Linux PE
- Deployment Solution now supports the 32-bit and 64-bit versions of Linux PE (both can be downloaded and imported)
- There are now separate policies to install, uninstall and upgrade automation folders for the 32-bit and 64-bit versions of Linux PE



Deployment Solution: Linux UEFI support

Use case: As an IT administrator, I need Deployment Solution to capture and deploy Linux images with UEFI partitions, so that I am not required to use another tool for that purpose.

- No changes to console UI
- Changes in scripts and other internals to enable Linux images with UEFI partitions to be captured and deployed
 - Automation folder can now be installed to UEFI partition
 - Scripted OS Install templates are now universal and can be used for machines with BIOS or UEFI
- Linux PE files updated to version 5.10 of the kernel
- Secure Boot not supported on Linux



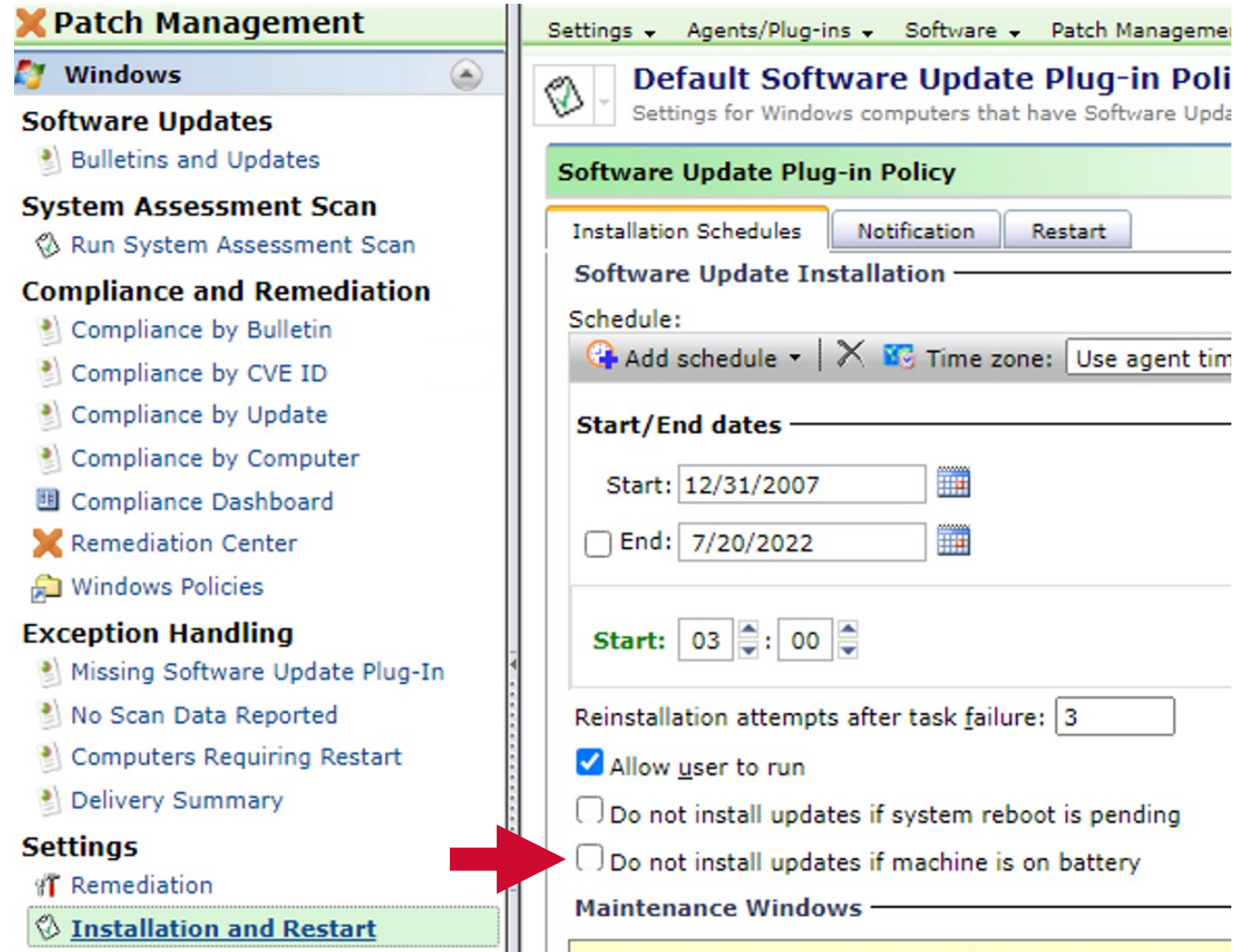
Symantec Management Agent: Option to not install if computer running on battery power

Use case: As an IT administrator, I need to have an option for the installation of software and patches to be suspended in cases where a device is running on battery power, so I can ensure the device will not run out of power before the installation completes.

- Applies to Software Update policies and Managed Software Delivery policies
- Does not apply to Software Update installation tasks or Quick Delivery task
- If computer is detected to be running on battery power, software or software update will not be installed
- Message displayed in Agent UI indicating that installation did not proceed due to computer running on battery power
- Reports reflect that installation did not proceed due to computer running on battery power
- When computer is plugged back in, software or software update will then get installed on schedule

Symantec Management Agent: Option to not install if computer running on battery power (Software Update Policies)

- Global option that applies to all Software Update policies
- Cannot be overridden within individual Software Update policy



Symantec Management Agent: Option to not install if computer running on battery power

- Message displayed in Agent UI


The screenshot shows the Symantec Management Agent 8.6.4077 (Administrator) interface. A yellow banner at the top reads "Machine is on battery". Below it, a light blue message box contains the text: "Machine is on battery", "Software Update Plug-in configuration policy does not allow installation of software updates while machine is on battery", and "4/1/2022 4:08:01 PM". A red arrow points to this message box. At the bottom, a blue sidebar shows "Schedules" and "Status" sections. A red arrow points to the "Default Update: At 3:00:00 AM every day," line in the "Schedules" section. To the right, a table titled "Software Updates for this computer:" lists updates with their status, bulletin names, and software update names.

Status	Bulletin Name	Software Update Name
Requires A/C power to install	7ZIP-211228	7z2107_21.07_x64.msi
Requires A/C power to install	TB-220309	Thunderbird Setup 91.7.0_x64-ENU.exe
Requires A/C power to install	NPPP-220315	npp.8.3.3.Installer.x86.exe
Requires reboot to install	FF-220323	Firefox Setup 98.0.2_x64-ENU.msi

Symantec Management Agent: Option to not install if computer running on battery power

- Reports reflect software and software updates that did not install due to computers running on battery power

Reports ▾ Software ▾ Patch Management ▾ Remediation Status ▾ Policy Execution by Computer

 **Policy Execution by Computer**
Recent software update installation activity. The report lets you see which updates have installed successfully and which have failed.


Actions ▾ Save As ▾ Print | Run ☒ Auto-run

Parameters Showing Computer, Filtered By Windows Computers with Software Update Plug-in Installed

Computer Name	Software Bulletin	Software Update	Policy Name	Package Status	Status
DESKTOP-6NFO8R2	TB-220309	Thunderbird Setup 91....	TB-220309 (no power?)	n/a	Requires A/C power to install

Row 1

Reports ▾ Software ▾ Compliance ▾ Software Compliance Detailed Summary

 **Software Compliance Detailed Summary**
Displays compliance status with respect to each computer for software installed via Managed Delivery policies.


Actions ▾ Save As ▾ Print | Run ☒ Auto-run View: Select a va


Parameters Only Include Licensed Computers: =No, Showing Computer, Start Date: =3/25/2022 12:00:00 AM, Maximum Number of Results to Include: =50, Applied, End Date: =4/1/2022 12:00:00 AM, Policies to Include: =All

Computers to Include: %

Only Include Licensed Computers: No ▾

Policies to Include: All ▾

Start Date: 3/25/2022 

End Date: 4/1/2022 

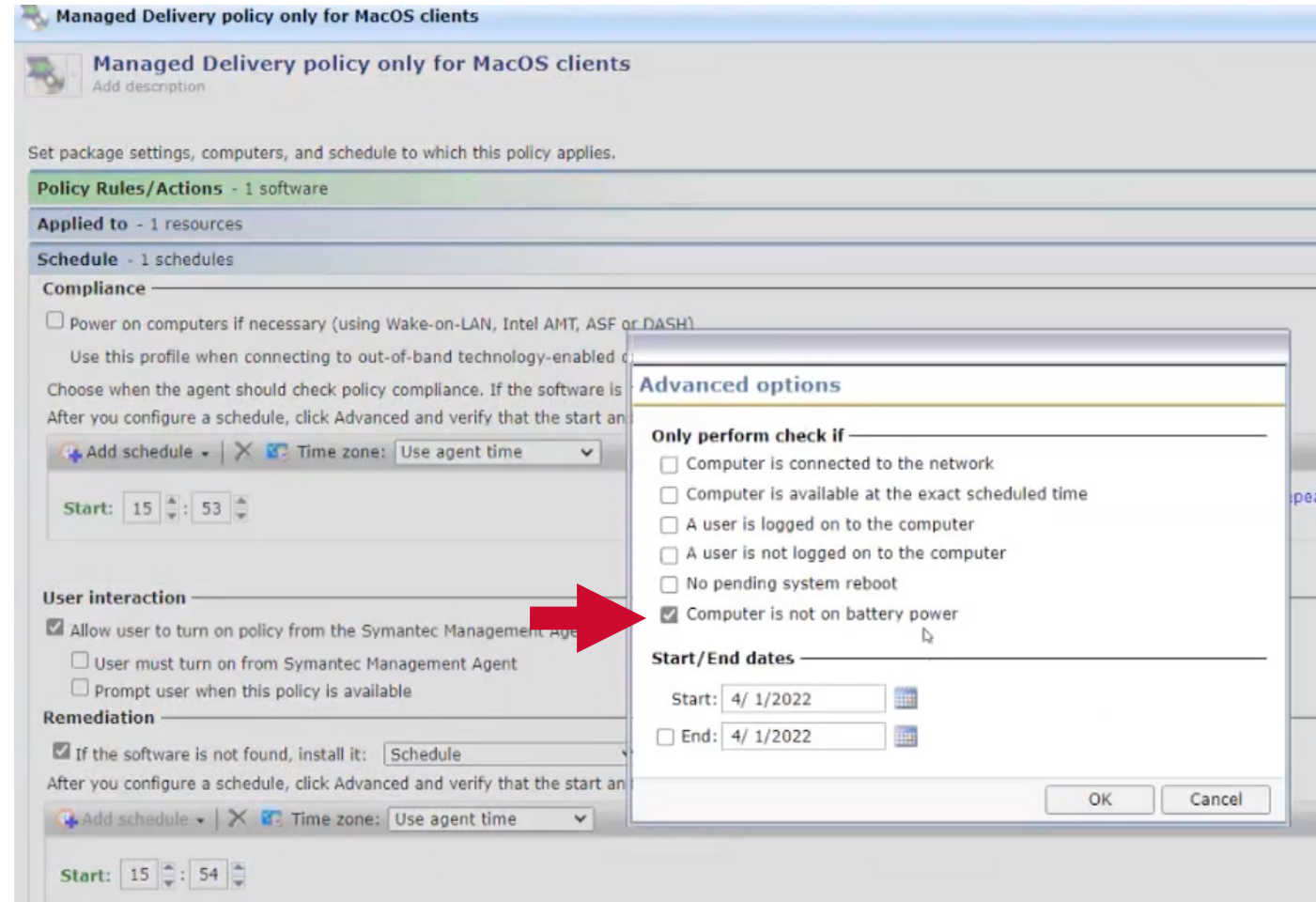
Compliance Status: Not Applied ▾

Maximum Number of Results to Include: 50

Computer Name	Policy Name	Status	Details
ulm-macos11h	Managed Delivery policy only for MacOS clients	Not Applied	Pending A/C Power Connection
DESKTOP-6NFO8R2	Managed Delivery policy - Deployment Agent x64	Not Applied	Pending A/C Power Connection

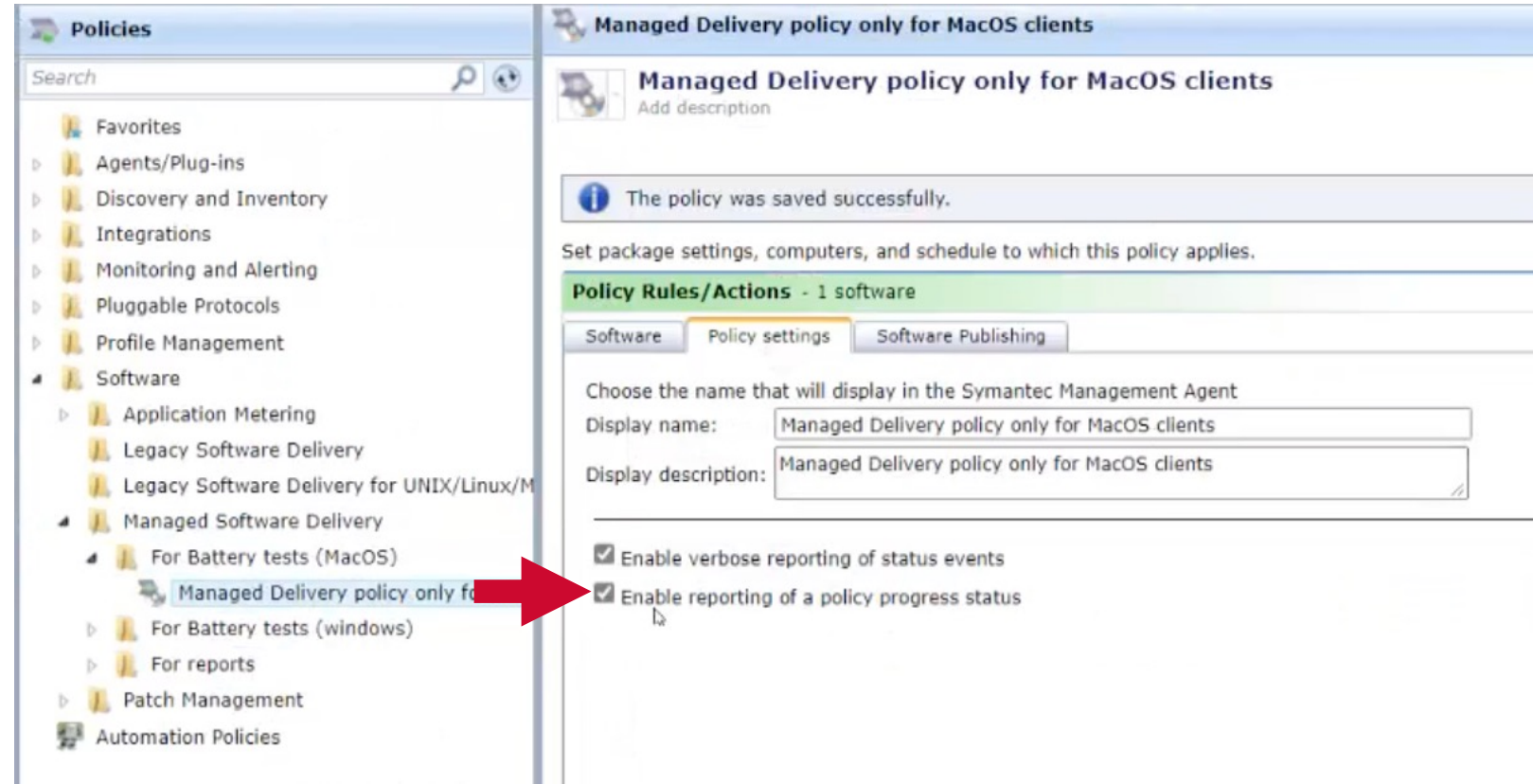
Symantec Management Agent: Option to not install if computer running on battery power (Managed Software Delivery Policies)

- Setting that can be defined within individual policies
- Separate settings for compliance and remediation checks
- Available for MSD policies targeting either Windows or Mac computers



Symantec Management Agent: Option to not install if computer running on battery power (Managed Software Delivery Policies)

- **REMINDER:** To report on why MSD policy is not in compliance, “Enable reporting of policy progress status” setting must be checked within policy
- By default, this setting is not checked



Symantec Management Agent: Identifying RHEV and GCE virtual machines

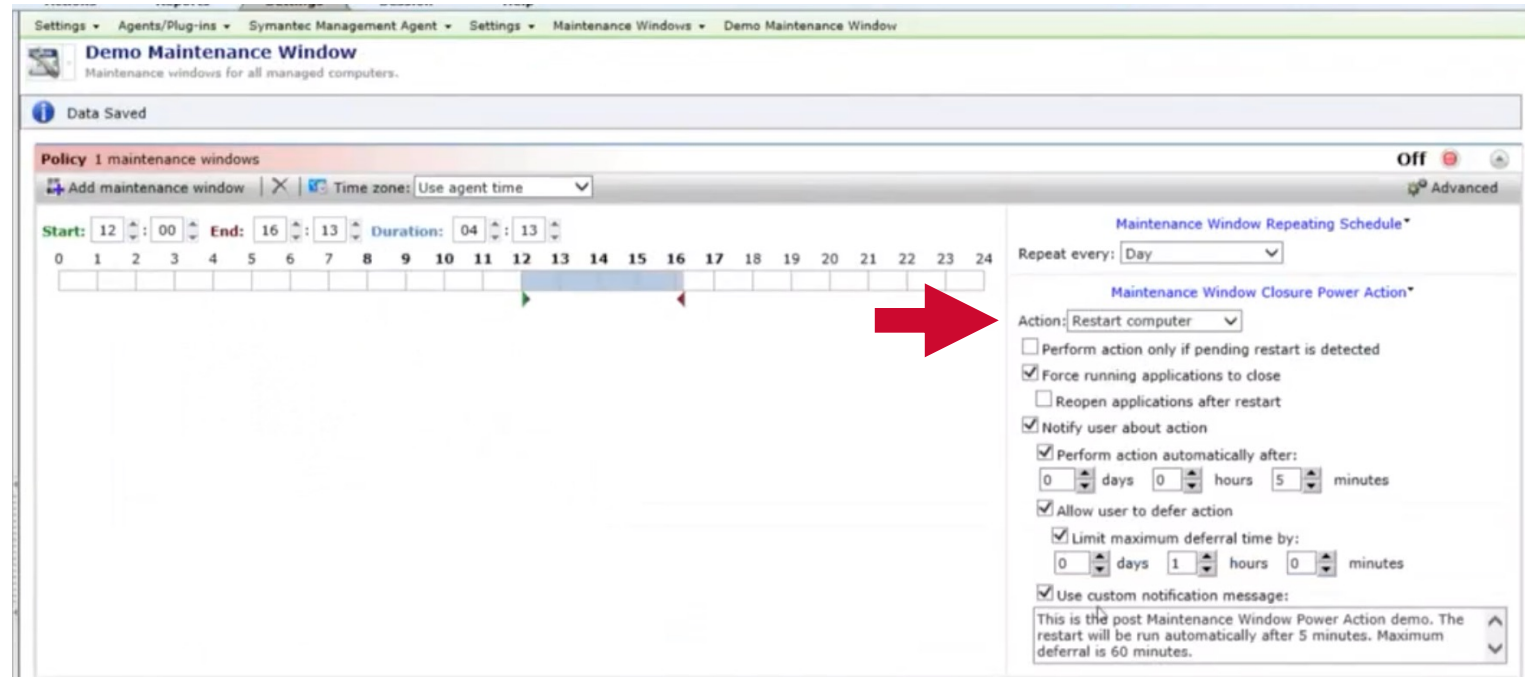
Use case: As an IT administrator, I need machines running under the Red Hat Enterprise Virtualization (RHEV) and Google Compute Engine (GCE) hypervisors to be identified as virtual machines, so that I can properly manage them.

- Prior to 8.6 RU3, machines running under the RHEV and GCE hypervisors were identified as physical machines because RHEV and GCE were not supported
- Beginning with 8.6 RU3, Basic Inventory will identify machines running under the RHEV and GCE hypervisors as virtual machines.

Symantec Management Agent (ULM): Power Control, System Restarts and Maintenance Windows

Use case: As an IT administrator, I need to perform a system restart as the last action within a maintenance window closes so that I can ensure that the computer will return to a working state regardless of how many tasks, jobs and policies in the queue are executed during the maintenance window.

- ITMS 8.6 RU2 included a feature that executes the power scheme task as the last action within a maintenance window on Windows computers
- ITMS 8.6 RU3 extends that feature to Mac and Linux computers
 - Mac and Linux now respect all settings within the Power Scheme task except re-opening applications after system restart and only restarting system if pending reboot detected



Symantec Management Console: Maintenance Window Information

Use case: As an IT administrator, I need to be able to quickly and easily see whether a computer currently has an active maintenance window, so that I can determine if it is possible to execute a task on that computer now.

- Computer view now shows whether there is currently an active maintenance window on Windows computers
 - Active
 - Not Active
 - Not Defined
- Computer view shows “Not Defined” if no maintenance windows are defined on a Windows computer (and for all Mac and Linux computers)
- Clicking on “Not Defined” link will display list of all maintenance window policies and allow you to add **computer to policy**



Symantec Management Console: Maintenance Window Information

- If one or more active maintenance windows, status = "Active"
 - Clicking on "Active" link will display information related to maintenance window that is currently active
- If one or more maintenance windows but not them are active, status = "Not Active"
 - Clicking on "Not Active" link will display a list of all maintenance window policies
- Maintenance windows defined by maintenance window policies, but can be turned off on Windows computers in agent UI
 - Maintenance Window status displayed reflects data collected from computers, not information from policies



The screenshot displays two entries in the Symantec Management Console. Each entry shows a server icon, the operating system name, and a table of system details. A red arrow points from the 'Maintenance Window' status to the 'Active' or 'Not Active' link.

Operating System	Maintenance Window Status
Windows Server 2016	Active
Windows 10	Not Active

Windows Server 2016 Details:

- Resource name: Igorp-CAMngr
- Domain: IGORP
- Server: Igorp-CAMngr.igorp.ad.local
- Fully qualified name: Igorp-CAMngr.igorp.ad.local
- Primary user: Child Admin CA, Perevoz
- Logged on account: IGORP\Child Admin
- Operating system: Windows Server 2016 (1607) / 10.0 / Standard Edition
- OS language: English (United States)
- Time zone: Pacific Standard Time
- Server connection: Persistent
- Task server: Igorp-CAMngr
- First Discovered: 28/04/2022 09:15:38
- Internal serial number: BB9C9B93-656F-404A-A1AB-7357C69CDFB8
- Device ID: BB9C9B93-656F-404A-A1AB-7357C69CDFB8
- Computer ID: {cf986bc9-b53c-4c34-aafe-a6a016a5bb1d}

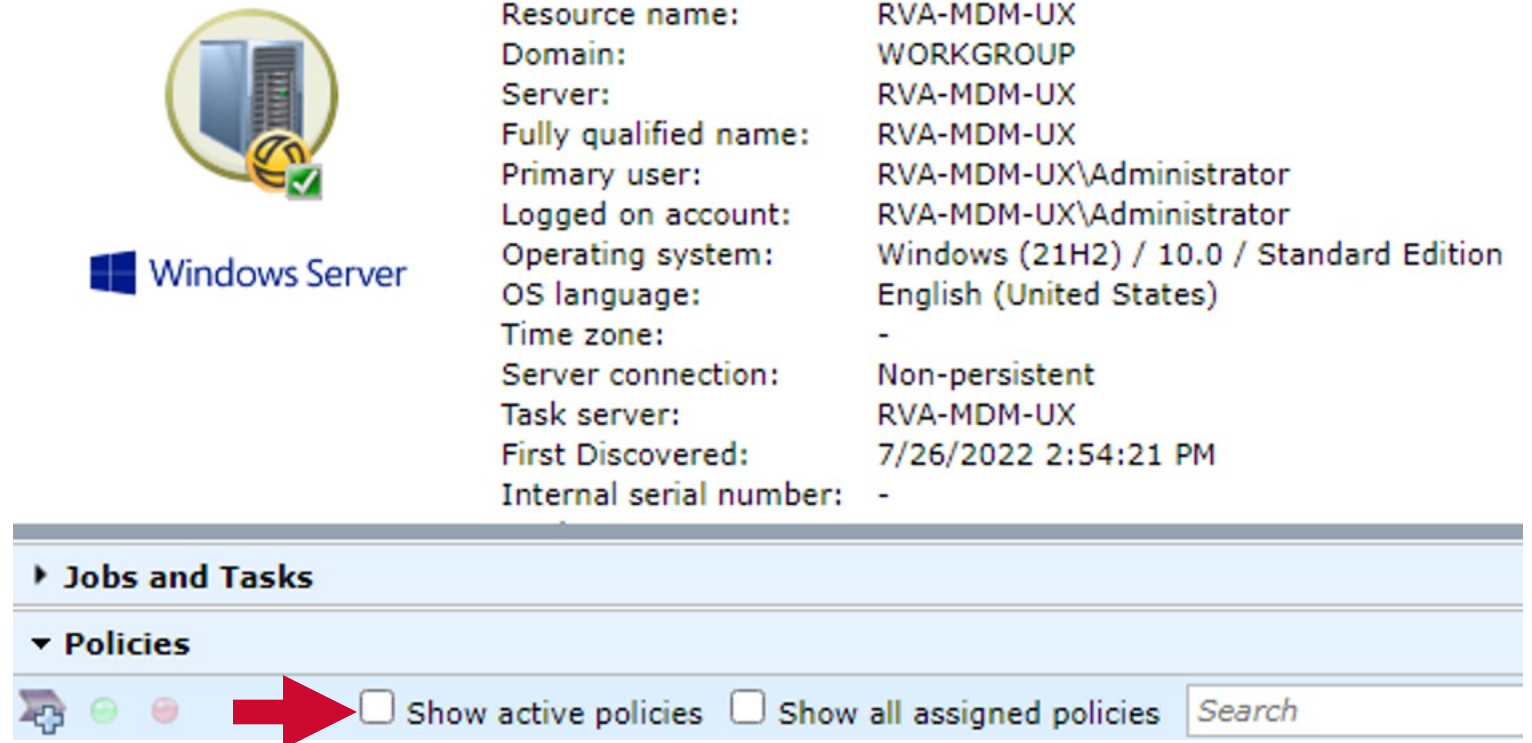
Windows 10 Details:

- Resource name: Igr-Ger10-64Ent
- Domain: WORKGROUP
- Server: Igrp12Camngr.igorp.ad.local
- Fully qualified name: Igr-Ger10-64Ent
- Primary user: IGR-GER10-64ENT\Administrator
- Logged on account: IGR-GER10-64ENT\Administrator
- Operating system: Windows 10 (21H1) / 10.0 / Enterprise
- OS language: German (Germany)
- Time zone: Mitteleuropäische Zeit
- Server connection: Persistent
- Task server: Igrp12Camngr
- First Discovered: 02/06/2022 11:01:18
- Internal serial number: 04583479-97FD-4A10-B904-49210661A133
- Device ID: 04583479-97FD-4A10-B904-49210661A133
- Computer ID: {f8fcfd0-d620-4ae4-8c6a-081fedc67c78}

Symantec Management Console: Active Policies

Use case: As an IT administrator, I need to quickly and easily see a list of active policies associated with a given computer, so that I am not required to browse through a list of all policies assigned to the computer and open each policy to determine if it is active.

- Computer view now includes “Show Active Policies” option to filter out policies that are no longer active



The screenshot displays the Symantec Management Console interface. On the left, a computer icon is shown with the text "Windows Server" below it. To the right, a list of system properties is displayed:

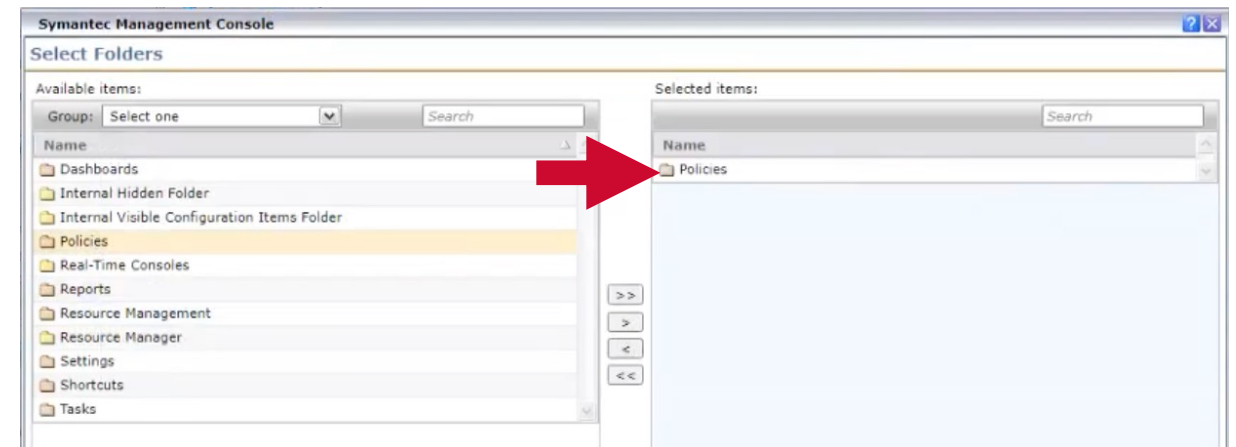
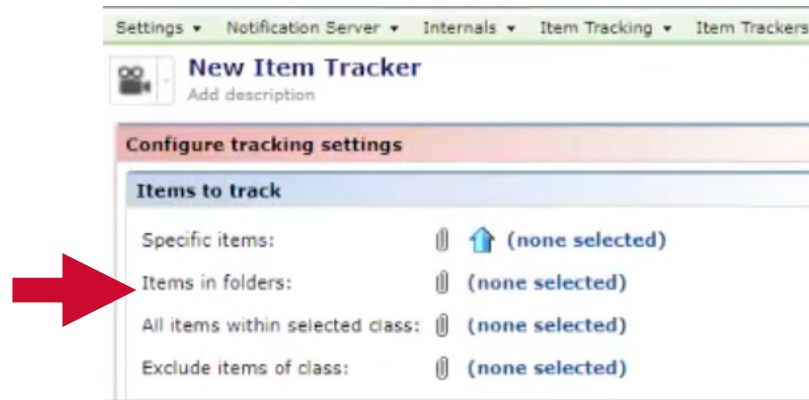
Resource name:	RVA-MDM-UX
Domain:	WORKGROUP
Server:	RVA-MDM-UX
Fully qualified name:	RVA-MDM-UX
Primary user:	RVA-MDM-UX\Administrator
Logged on account:	RVA-MDM-UX\Administrator
Operating system:	Windows (21H2) / 10.0 / Standard Edition
OS language:	English (United States)
Time zone:	-
Server connection:	Non-persistent
Task server:	RVA-MDM-UX
First Discovered:	7/26/2022 2:54:21 PM
Internal serial number:	-

Below the system properties, there are two expandable sections: "Jobs and Tasks" and "Policies". The "Policies" section is expanded, showing a list of policies. A red arrow points to the "Show active policies" checkbox, which is currently unchecked. Next to it is the "Show all assigned policies" checkbox, which is also unchecked. A search bar is located to the right of these checkboxes.

Symantec Management Console – Track All Changes Under Specified Folder

Use case: As an ITMS administrator, I need to track all changes under a specified folder within the console for audit purposes (including new objects), so that which ITMS users (non-admin roles) made changes impacting devices

- Prior to 8.6 RU3, changes to specified items within a folder could be tracked, but changes could not be tracked at the folder level (e.g. Creation of new item within a folder)
- ITMS 8.6 RU3 provides the ability to track all changes within a specified folder, including newly created objects




Symantec Management Console: Tasks/policies executed under context of specified account

Use case: As an IT administrator, I need to identify tasks and policies executed using custom credentials (other than the system account or the account of the logged on user), so that I can determine the cause of authentication failures (inactive accounts or accounts with password changes)

- Such tasks and policies could previously only be identified by individually reviewing each task or policy
- Reports have been added to help identify such cases
 - Collect Inventory with Specific User
 - Directory Import with Specific User (AD Import)
 - Managed Delivery with Specific User (Each package can be installed with different credentials)
 - Software Delivery with Specific User (Quick Delivery tasks)
 - Task with Specific User (Script tasks)
- Intended to provide greater visibility into custom configuration settings used by customers and speed up troubleshooting in situations where account locking issues are encountered

Symantec Management Console: Tasks/policies executed under context of specified account

Reports ▾ Notification Server Management ▾ Server ▾ Account Management ▾ Collect Inventory with Specific User

 **Collect Inventory with Specific User**
Add description


Actions ▾ Save As ▾ Print | Run ☒ Auto-run

Parameters

User name:

Name	Platform	Version	Username
Gather Inventory Win, Unix, Mac	windows	1	WINDOMAIN\WindowsUser1
Gather Inventory Win, Unix, Mac	UNIX	1	UnixUser
Gather Inventory Win, Unix, Mac	mac	1	MacUser

Reports ▾ Notification Server Management ▾ Server ▾ Account Management ▾ Directory Import with Specific User


 **Directory Import with Specific User**
Add description

Actions ▾ Save As ▾ Print | Run ☒ Auto-run View: Select a value... ▾

Parameters

User name:

Name	Username
Import Computer resources from 10.127.156.128 starting from BuiltIn and using the default column mappings. Import all computers on the specified schedules	igorpadmin
Import User resources from 10.127.156.128 starting from IP ORG UNIT1, IP ORG UNIT2 and using the default column mappings and these resource associations.	igorpadmin2

 **Managed Delivery with Specific User**
Add description

Actions ▾ Save As ▾ Print | Run ☒ Auto-run


Parameters

User name:

Name	Domain	Username
Managed Delivery policy with 3 different Software pac...	1stSWDomain	1stSWUsername
Managed Delivery policy with 3 different Software pac...	3rdSWDomain	3rdSWUsername
Managed Delivery policy with 3 different Software pac...	2ndSWDomain	2ndSWUsername

Symantec Management Console: Tasks/policies executed under context of specified account

Reports ▾ Notification Server Management ▾ Server ▾ Account Management ▾ Software Delivery with Specific User

 **Software Delivery with Specific User**
Add description


Actions ▾ Save As ▾ Print | Run ☒ Auto-run

Parameters

User name:

Name	Version	Domain	Username
Package Delivery	1	igordomain	igorpadmin
Quick Delivery task	1	.	LocalUser1

Reports ▾ Notification Server Management ▾ Server ▾ Account Management ▾ Task with Specific User

 **Task with Specific User**
Add description

Actions ▾ Save As ▾ Print | Run ☒ Auto-run

Parameters

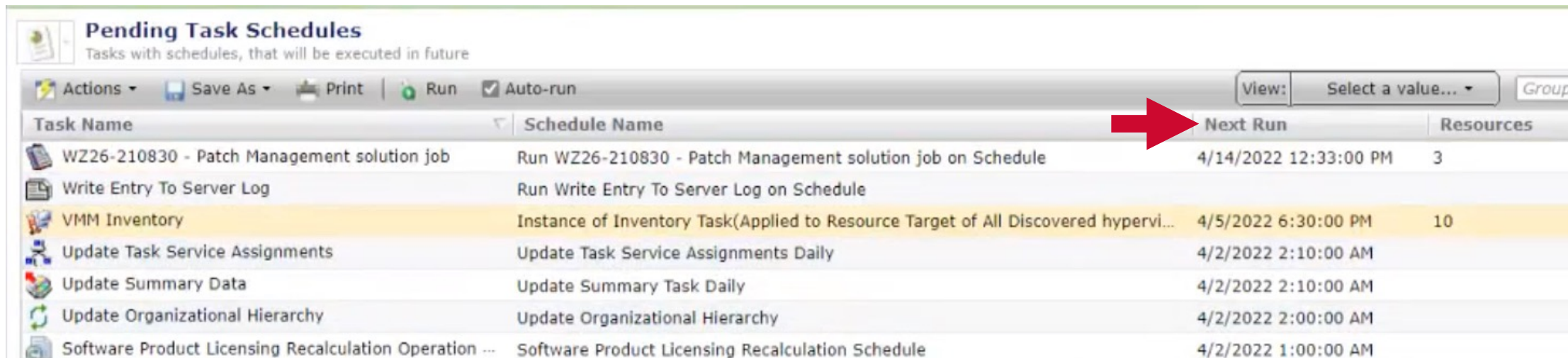
User name:

Name	Version	Username
Run Script task #2 with custom credentials	1	localhost\LocalAdmin
Run Script task #3 with custom credentials	1	localhost\LocalAdmin3
Run Script task #3 with custom credentials	1	localhost\LocalAdmin2

Symantec Management Console: Overview of tasks scheduled to be executed in the future

Use case: As an IT administrator, I need to be able to identify all tasks that have a pending schedule to identify and review for deprecated/obsolete tasks to avoid potential issues on targeted computers

- IT administrators previously had to review each task individually to determine when they would be executed
- New Pending Task Schedules report provides an overview of all tasks with Next Run date/time



Pending Task Schedules
Tasks with schedules, that will be executed in future

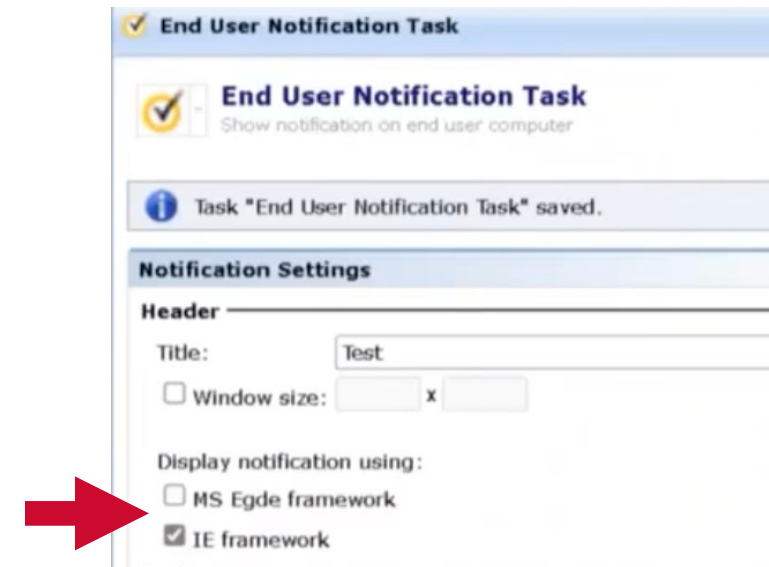
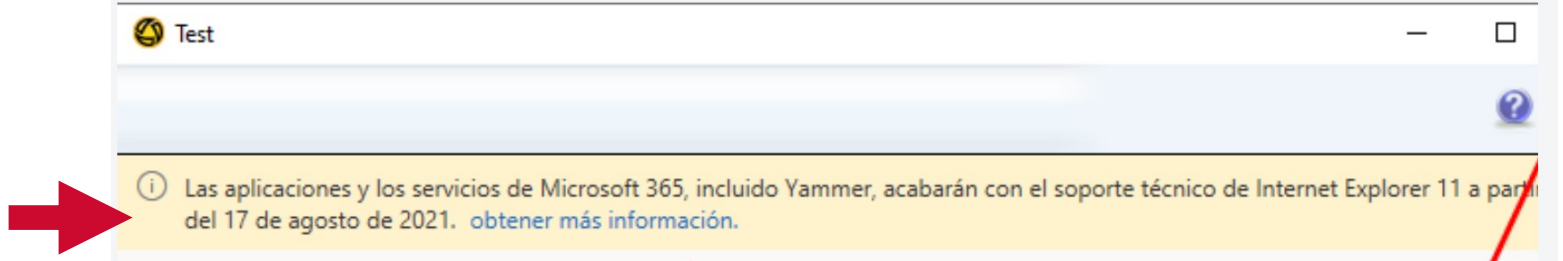
Actions ▾ Save As ▾ Print Run Auto-run View: Select a value... ▾ Group

Task Name	Schedule Name	Next Run	Resources
WZ26-210830 - Patch Management solution job	Run WZ26-210830 - Patch Management solution job on Schedule	4/14/2022 12:33:00 PM	3
Write Entry To Server Log	Run Write Entry To Server Log on Schedule		
VMM Inventory	Instance of Inventory Task(Applied to Resource Target of All Discovered hypervi...	4/5/2022 6:30:00 PM	10
Update Task Service Assignments	Update Task Service Assignments Daily	4/2/2022 2:10:00 AM	
Update Summary Data	Update Summary Task Daily	4/2/2022 2:10:00 AM	
Update Organizational Hierarchy	Update Organizational Hierarchy	4/2/2022 2:00:00 AM	
Software Product Licensing Recalculation Operation ...	Software Product Licensing Recalculation Schedule	4/2/2022 1:00:00 AM	

Symantec Management Platform: End User Notification Tasks

Use case: As an IT administrator, I need end user notifications to be displayed by a framework that is not part of the Internet Explorer framework, so that end users do not get confused by a warning message that Internet Explorer will be (or has been) EOL'd

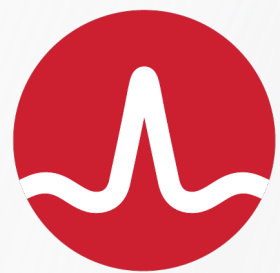
- Prior to 8.6 RU3, end user notifications were displayed using ActiveX (IE framework)
- When viewing such notifications, end users were warned that Internet Explorer was being EOL'd
- Notifications can now be displayed using WebView2 (Chromium-based Edge framework)
 - Installed as part of Edge
 - Can be installed independently of Edge





Open Discussion: Questions and Answers





BROADCOM[®]

SOFTWARE