



# What's New in ITMS 8.5

## Deep Dive

**Brian Sheedy**

Sr. Principal TEC, Endpoint Management



# Agenda

**1** Core Platform Enhancements

**2** Product Integrations

**3** Solution Enhancements

---

# Core Platform Enhancements



## Platform Support

- **Additional SMP/CMDB Database Support:**

- **Windows Server 2016**
- Microsoft SQL Server® 2014 SP2
- Microsoft SQL Server 2016 SP1/SP2

- **Additional Site Server Support:**

- Windows 10 Redstone 3 (1703) , 4 (1803), 5 (1809)
- Windows Server 2016

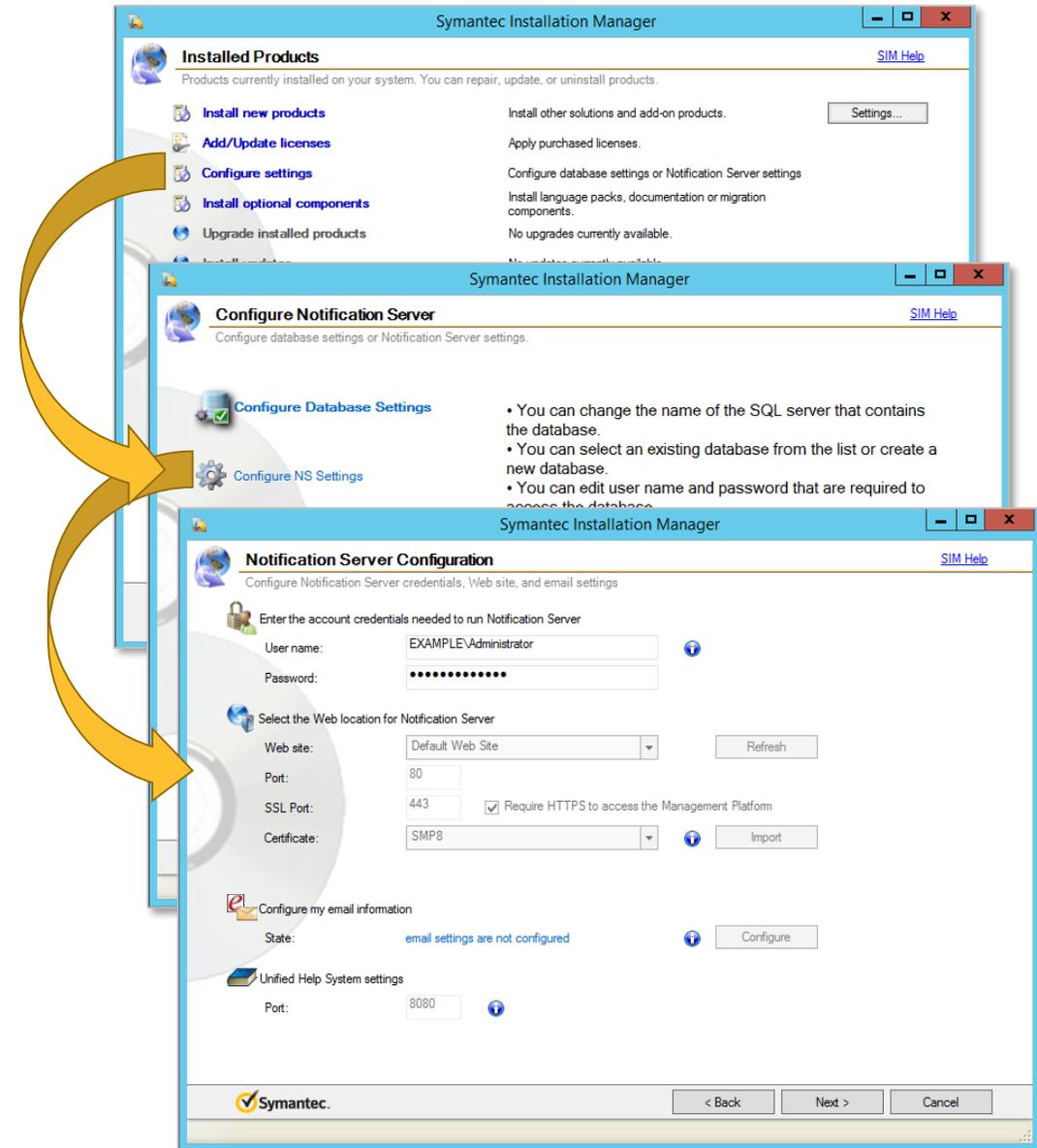
- **Additional Agent Support:**

- Windows 10 Redstone 3 (1703) , 4 (1803), 5 (1809)
- MacOS High Sierra (10.3), Mustang (10.4)
- RHEL 6.9, 7.3, 7.4, 7.5 (Partial)
- CentOS 6.9, 7.3, 7.4, 7.5
- SLES/SLED 12 SP3
- Ubuntu 14.04, 16.04, 18.04 (Partial - [HOWTO127014](#) )



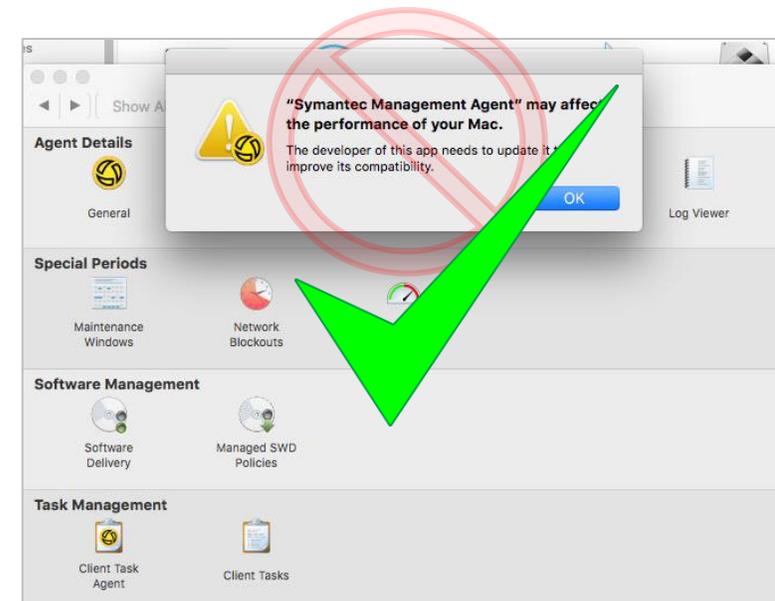
# Symantec Installation Manager

- **Switching Application Identity in SIM**
  - New **Configure NS Settings** option
    - Account must differ from existing
    - Added to Symantec Administrator role
    - Default owner changes to new account
- Release Updates are significantly faster
- Shows the installed products from all defined product listings.
  - Manage the products that belong to currently selected product listing.
- No longer possible to apply licenses that will be valid until applicable in the future.



# Symantec Management Agent

- **64 bit Mac Symantec Management Agent**
  - Apple officially announced that all applications must be converted to 64-bit
  - All Mac binaries were converted to 64-bit without impact to functionality
- **Apply Communication Profiles by CMD**
  - ***Using AeXNSAgent.EXE***
    - ***/importprofile:<path>***
      - lets you specify the path to XML file of the profile
    - ***/profilepwd:<pwd>***
      - lets you specify the decryption password



# Symantec Management Agent

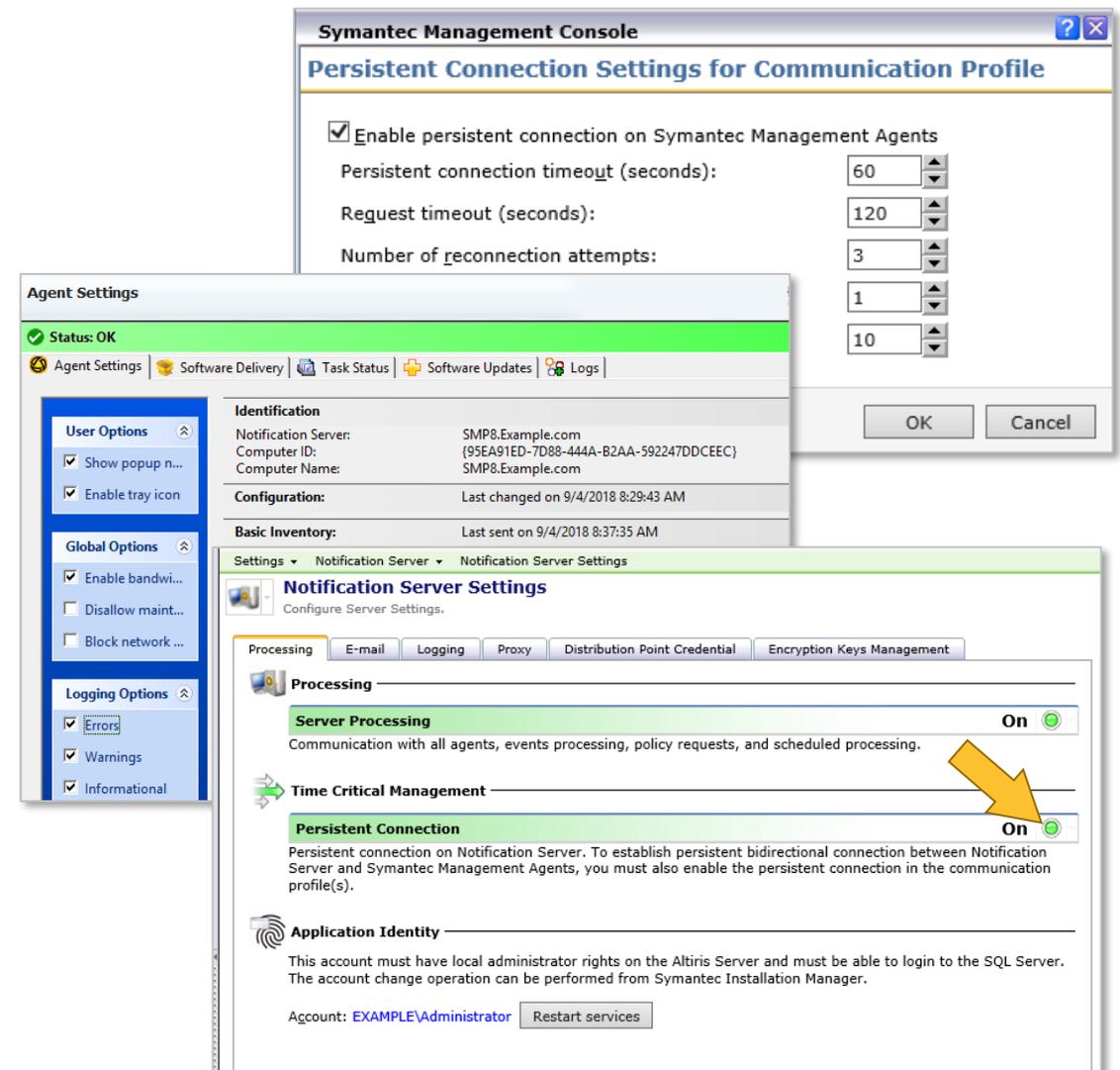
- **Initial Settings** Policy
  - In Targeted Agent Settings
    - Disabled by default
  - Sends initial settings to registered agents
    - To immediately connect to Task Servers
    - To enforce a configuration before admin
  - Applies standard TAS policy after connecting
  - Must be enabled for Deployment Solution



# Symantec Management Platform

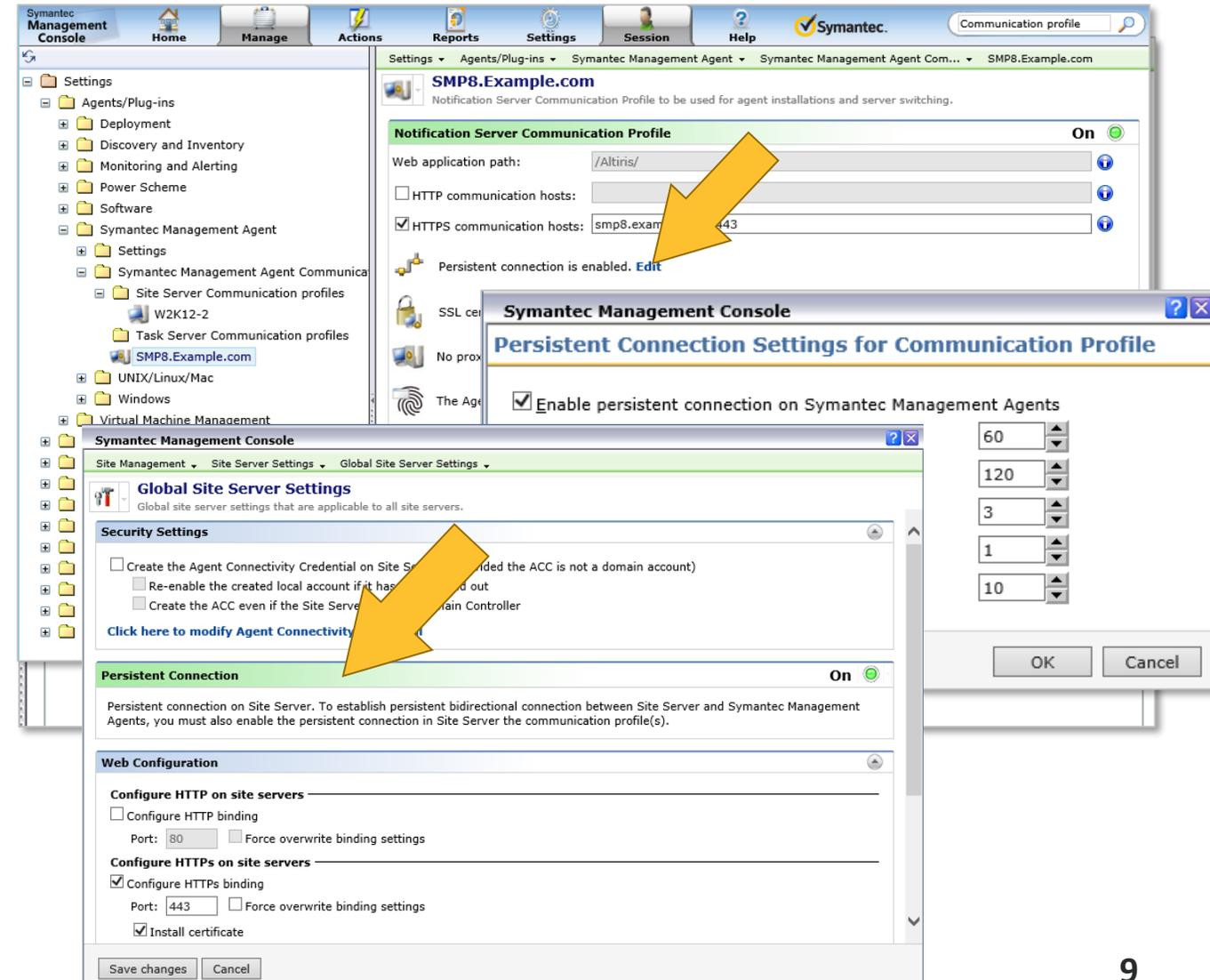
## ○ Persistent Connection

- Enables real time data transfer from and to Symantec Management Agent
- Uses **WebSocket** communication protocol
  - Operates over HTTPS on port 443
  - Does not require additional ports
  - Uses existing SSL Certificates
- Supports all settings in Communication Profiles
- All Infrastructure components supported
  - **CeM IG**, Task Servers, Win/Linux/Mac Agents
- **If Enabled on Clients:**
  - All LAN/WAN agents use it to connect to Notification/Task Servers
- **If Enabled on NS/Site Servers:**
  - Used for all management traffic (NSE, Policy, Task)
    - Not used for Package Downloads
- Reverts to standard HTTP/HTTPS if disabled



# Symantec Management Platform

- Persistent Connection
  - Must have HTTPS set up in your environment
  - Enabled in NS Configuration Settings
  - Configure for Agents and Site Servers
    - In the SMA communication profile(s)
    - In the Site Server communication profile(s)

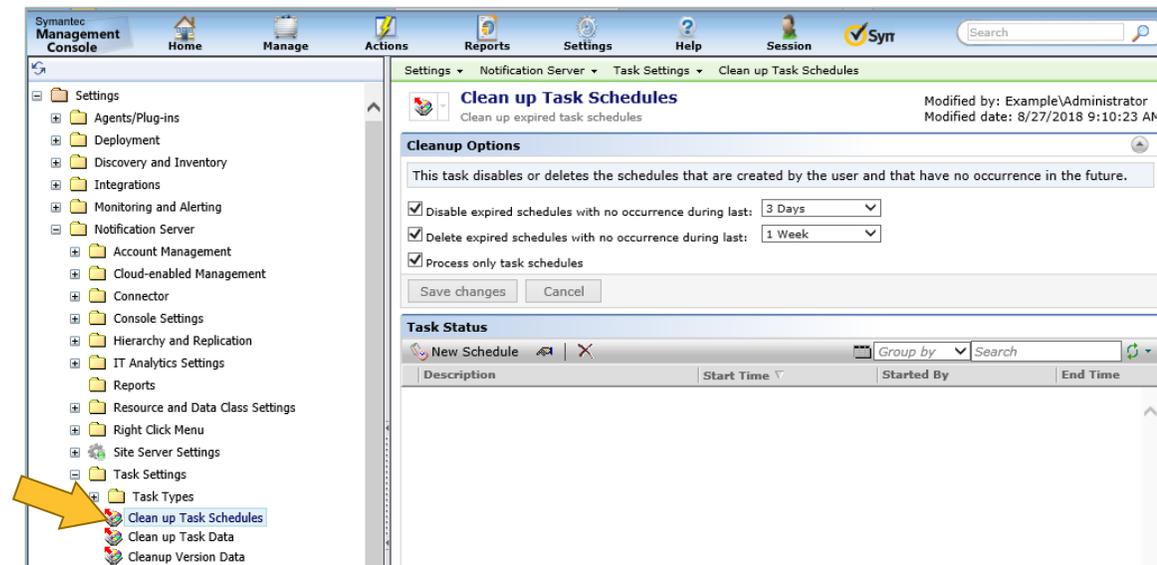


The screenshot displays the Symantec Management Console interface. The top window, titled 'SMP8.Example.com', shows the 'Notification Server Communication Profile' configuration. The 'HTTPS communication hosts' field is set to 'smp8.example.com:443', highlighted by a yellow arrow. Below it, the text 'Persistent connection is enabled. Edit' is visible. The bottom window, titled 'Symantec Management Console', shows the 'Persistent Connection Settings for Communication Profile' dialog. The checkbox 'Enable persistent connection on Symantec Management Agents' is checked, also highlighted by a yellow arrow. The background window shows 'Global Site Server Settings' with the 'Persistent Connection' status set to 'On'.

# Symantec Management Platform

- **Clean up Task Schedules**

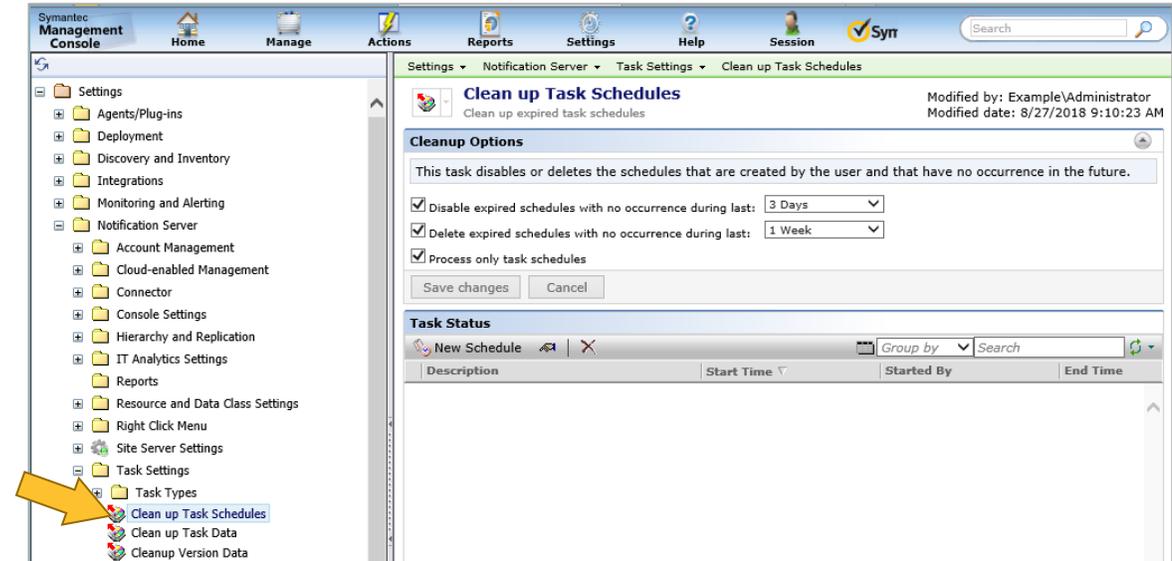
- Disables or deletes schedules that have no occurrence in the future.
- Removes these task schedules from the Windows Task Scheduler.
- **Settings > Notification Server > Task Settings.**



# Symantec Management Platform

## ○ Clean up Task Schedules

- Disables or deletes schedules that have no occurrence in the future.
- Removes these task schedules from the Windows Task Scheduler.
- **Settings > Notification Server > Task Settings.**



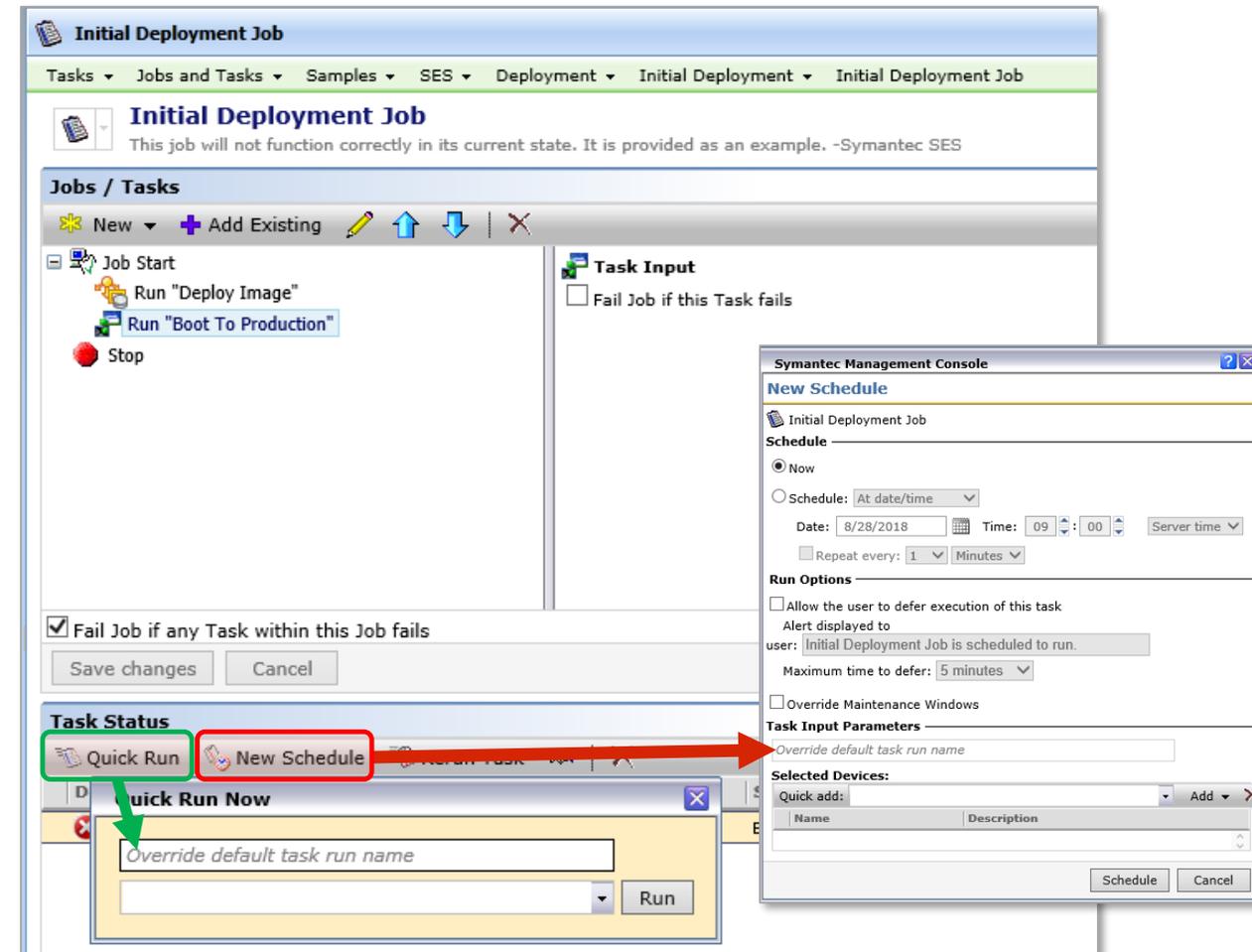
## ○ Console Notifications

- Product Listing updates are visible
  - Informational Only – Use SIM to Update
- Visually unified and don't overlap
- View can be controlled per Console user



# Symantec Management Platform

- **Task Instance Name**
  - Instance Name was based on Task Name
    - Difficult to distinguish within the console
  - Specify the task-run description
    - When launching from the "Quick Run"
    - In the "New Schedule" options
  - Makes it easily searchable



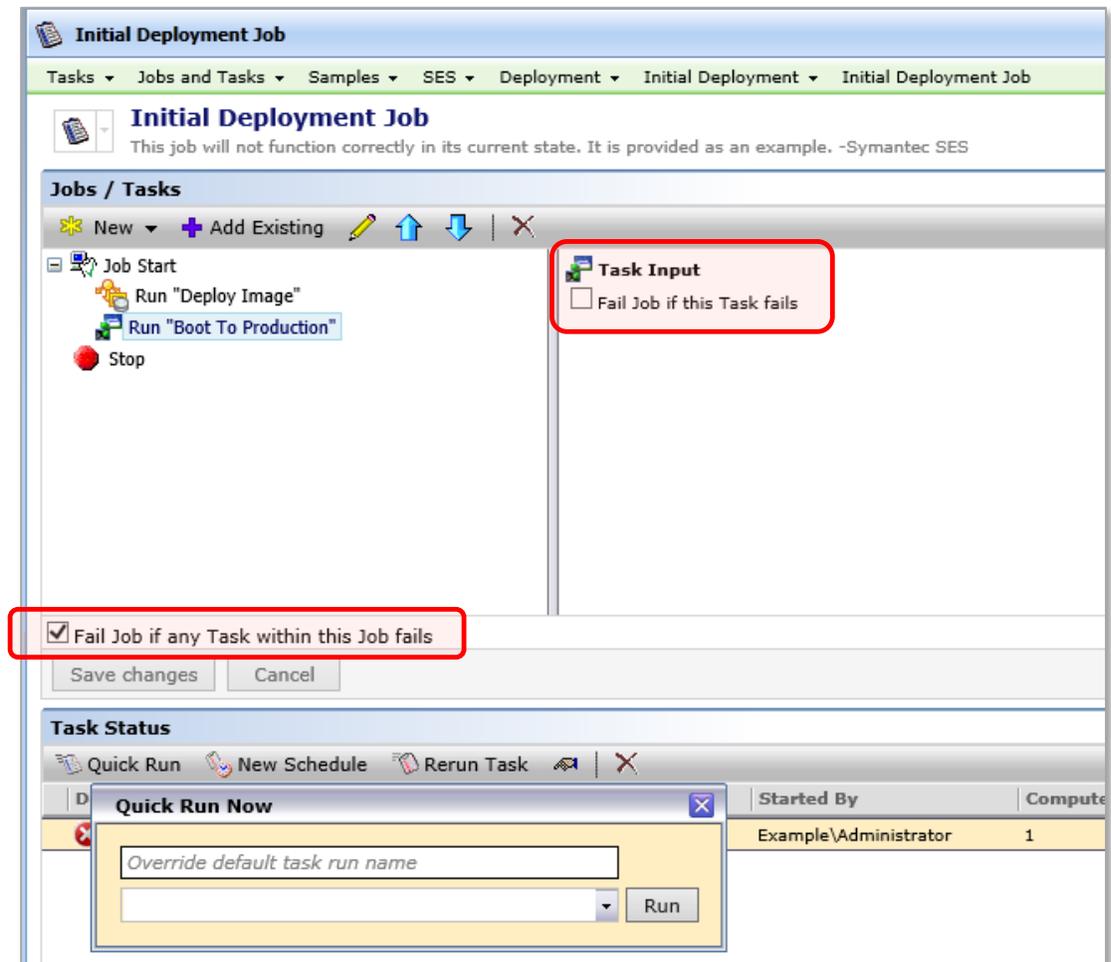
# Symantec Management Platform

## ○ Jobs/Tasks

- The logic to stop a Job was based on tasks failures being set and by building conditions based on different error codes

## ○ New Input Controls

- Each task has a “Fail job if this task fail”
- Controls what stops entire job or where failure is expected.
- Define each level as a critical task and stop execution at each failure.
- Saves time and provides proper visibility of Job failures



The screenshot displays the Symantec Management Platform interface for configuring an "Initial Deployment Job".

**Initial Deployment Job**  
 Tasks ▾ Jobs and Tasks ▾ Samples ▾ SES ▾ Deployment ▾ Initial Deployment ▾ Initial Deployment Job

**Initial Deployment Job**  
 This job will not function correctly in its current state. It is provided as an example. -Symantec SES

**Jobs / Tasks**

- New ▾ + Add Existing
- Job Start
  - Run "Deploy Image"
  - Run "Boot To Production"
  - Stop

**Task Input**

- Fail Job if this Task fails

Fail Job if any Task within this Job fails

Save changes Cancel

**Task Status**

Quick Run New Schedule Rerun Task

**Quick Run Now**

Override default task run name

Run

Started By	Compute
Example\Administrator	1

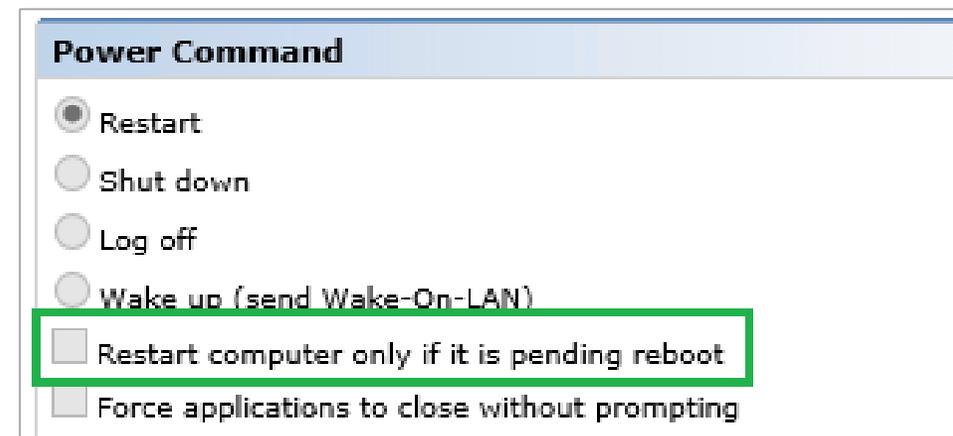
# Symantec Management Platform

## ○ Power Tasks

- Software Installations may fail if a machine has a reboot pending - Causing productivity and availability impacts
- Existing ways to solve the problem were unconditional reboot or complex registry checks.

## ○ New Reboot Option

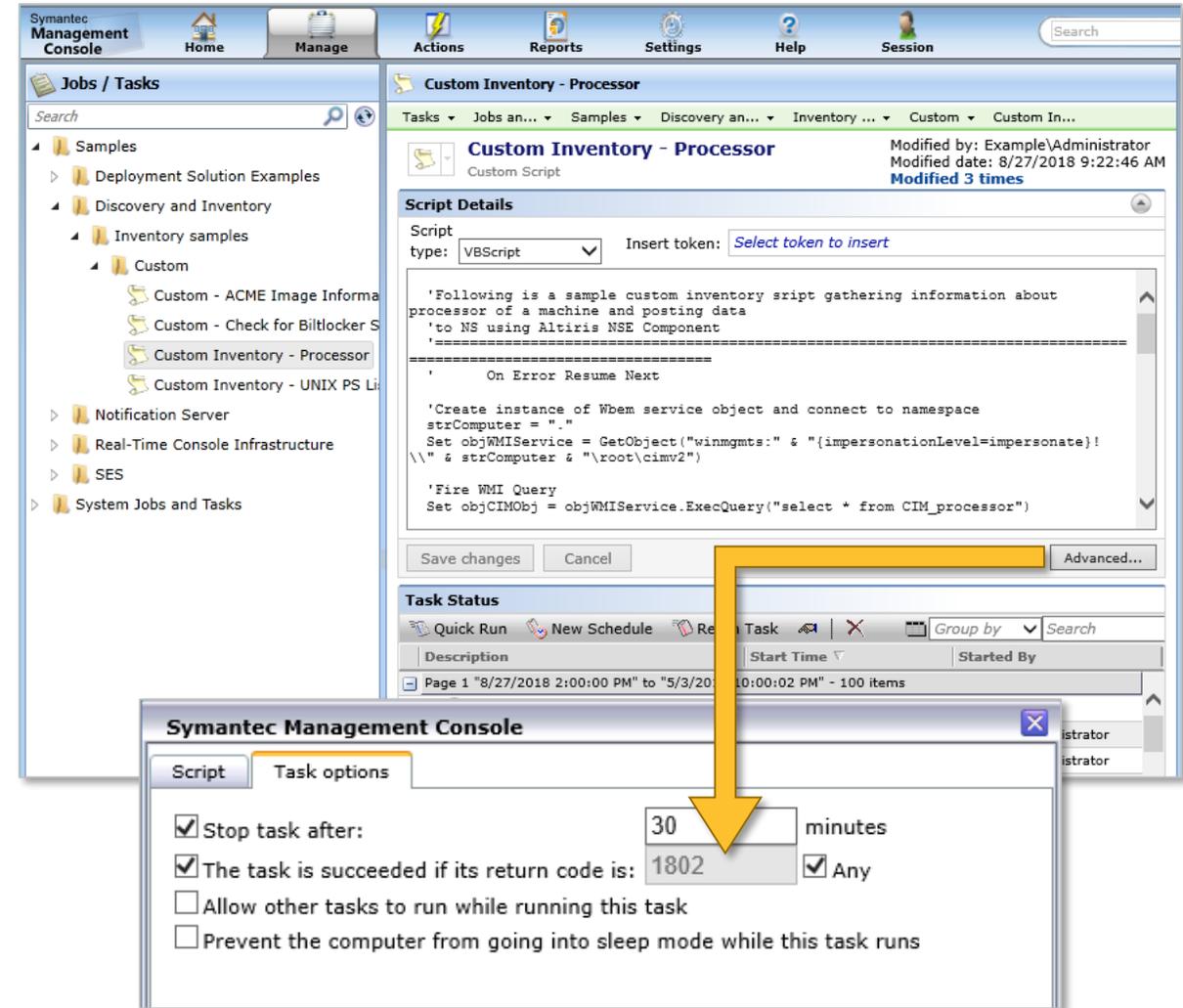
- Will only reboot machines that already in a “reboot pending” – reducing impact to productivity
- If checkbox selected, can be used in cases like:
  - In-use file rename
  - Computer rename
  - Computer role addition
  - Windows update



The screenshot shows a dialog box titled "Power Command" with a light blue header. It contains a list of radio button options: "Restart" (selected), "Shut down", "Log off", and "Wake up (send Wake-On-LAN)". Below these is a checkbox labeled "Restart computer only if it is pending reboot", which is highlighted with a green rectangular border. At the bottom is another checkbox labeled "Force applications to close without prompting".

# Symantec Management Platform

- **Custom Task Success/Failure codes**
  - Multiple values separated with commas.
  - Only available for script task types.

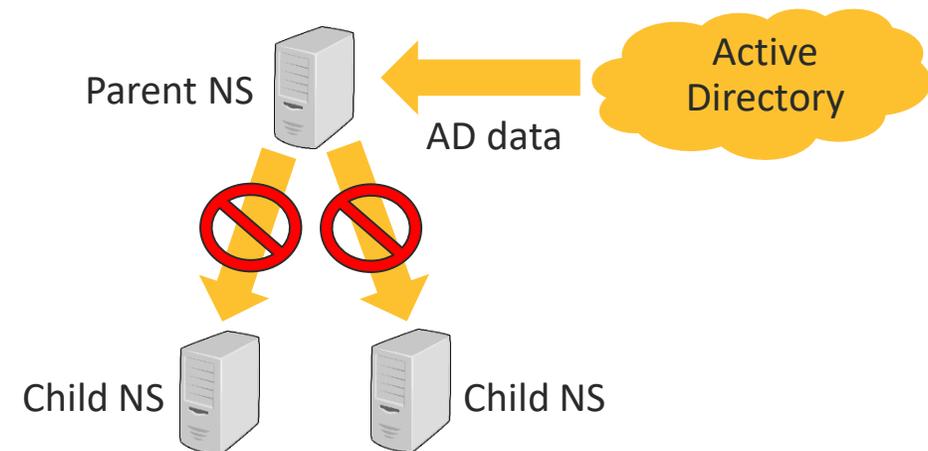


The screenshot displays the Symantec Management Console interface. The left pane shows a tree view under 'Jobs / Tasks' with 'Custom Inventory - Processor' selected. The main pane shows the configuration for this task, including a VBScript. A yellow arrow points from the 'Task Status' section to a 'Task options' dialog box. In the dialog, the 'Stop task after' checkbox is checked and set to 30 minutes. The 'The task is succeeded if its return code is' checkbox is also checked, with the value 1802 entered and the 'Any' checkbox checked. Other options like 'Allow other tasks to run while running this task' and 'Prevent the computer from going into sleep mode while this task runs' are unchecked.

# Symantec Management Platform

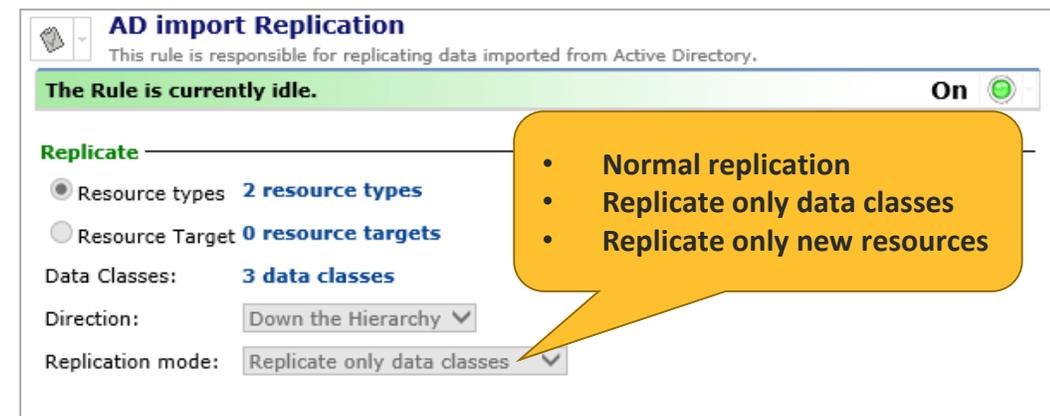
## ○ Legacy AD Management in a Hierarchy

- Active Directory data was not replicated down
- Mandatory AD import on Parent then Replicate
- If AD import on Child NS you could not manage Imported filters/Groups on the Parent
  - Caused mismatched GUID's and a massive merge process between Parent/Child NS's



## ○ Hierarchy Replication Options

- Replication rule added called **“AD import Replication”**
  - Replicates data for users and computers that are imported from Active Directory (Is Disabled)
- Allow configuration of hierarchy replication mode
  - Configures the type of data the hierarchy replication rule should replicate.



**AD import Replication**  
This rule is responsible for replicating data imported from Active Directory.

The Rule is currently idle. On

**Replicate**

- Resource types **2 resource types**
- Resource Target **0 resource targets**

Data Classes: **3 data classes**

Direction: Down the Hierarchy

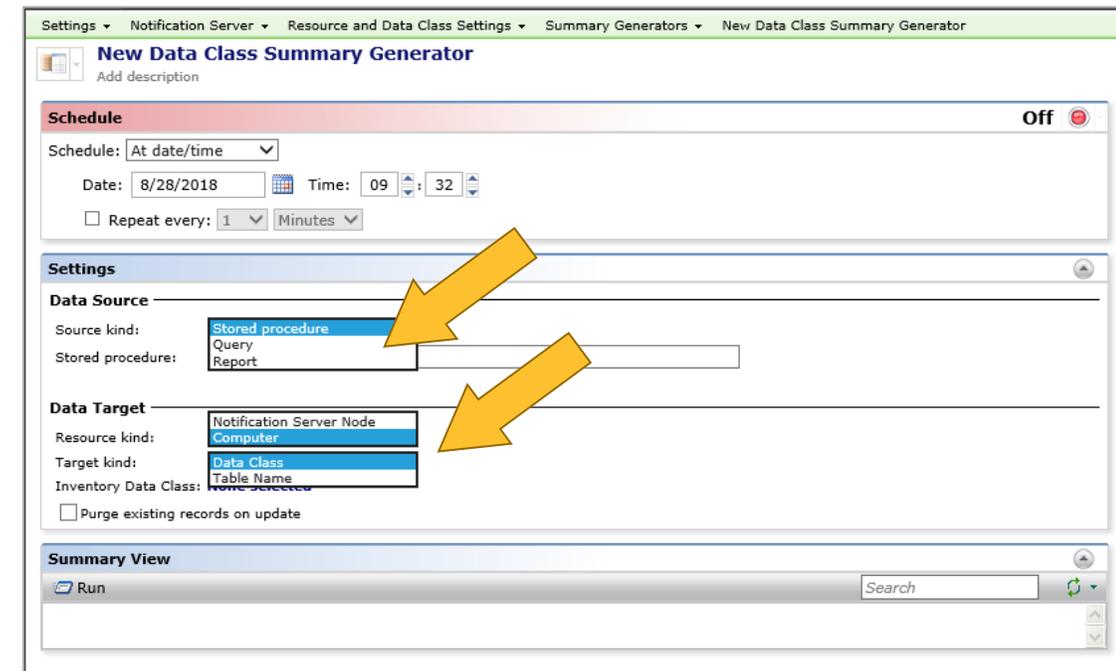
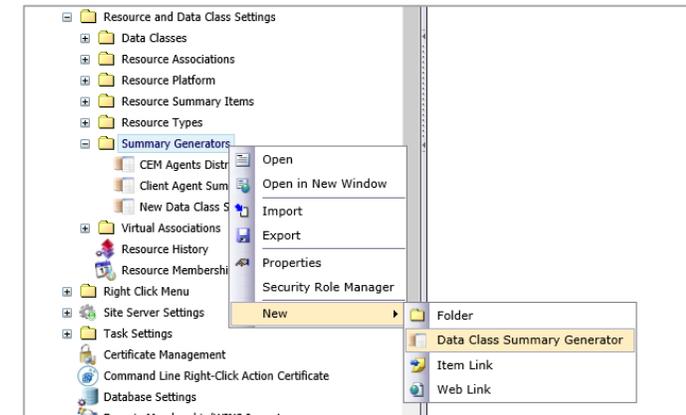
Replication mode: Replicate only data classes

- Normal replication
- Replicate only data classes
- Replicate only new resources

# Symantec Management Platform

## ○ Data Class Summary Generator

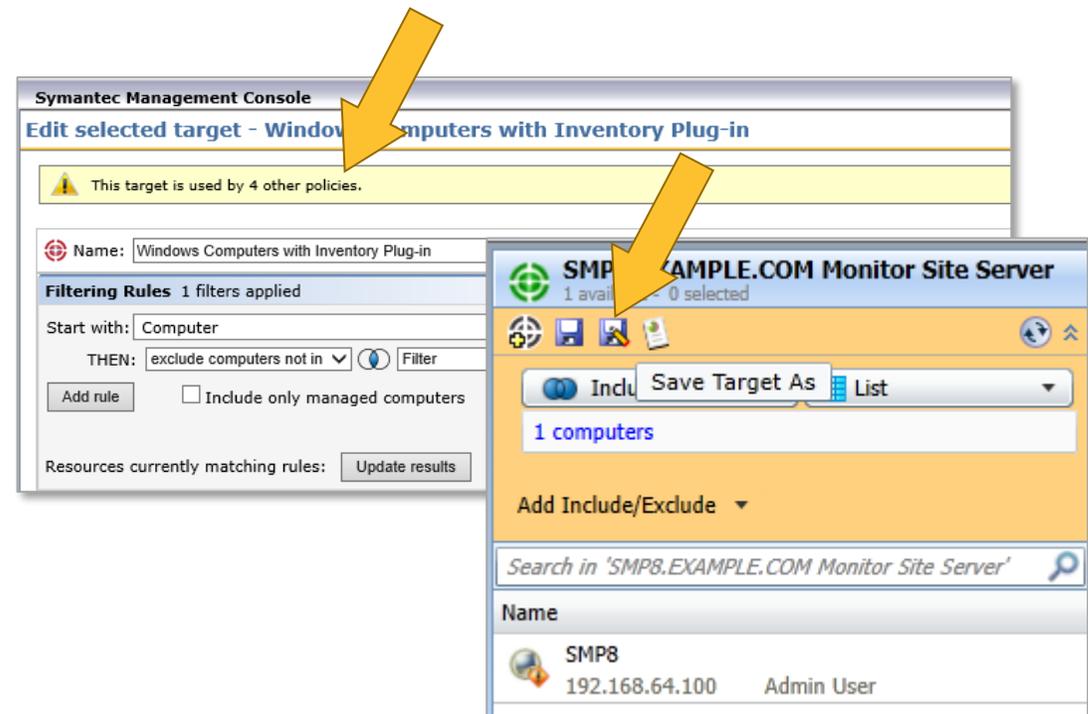
- Aggregates an extensive data set into a smaller data class content.
- Easier to replicate and use across multiple NS's
- Reports, queries or stored procedure can be used as data source
- Processes the Data Source and inserts the result into the Data Target data class.
- Data set can be managed using standard mechanisms, like Standalone Replication to reporting server
- Can use the Data Class Summary as a report



# Symantec Management Platform

## ○ Resource Target Modification

- Need to modify a shared Target for a Policy
- Warning appears “...Is used by *n* other Policies”
- **To change the Target:**
  - Close the Target window...
  - Find Target in Computer View...
  - Save the Target as something else...
  - Re-apply New Target in desired Policy.
- Within ITMS View, the targets section has a similar “Save As” option for an opened target



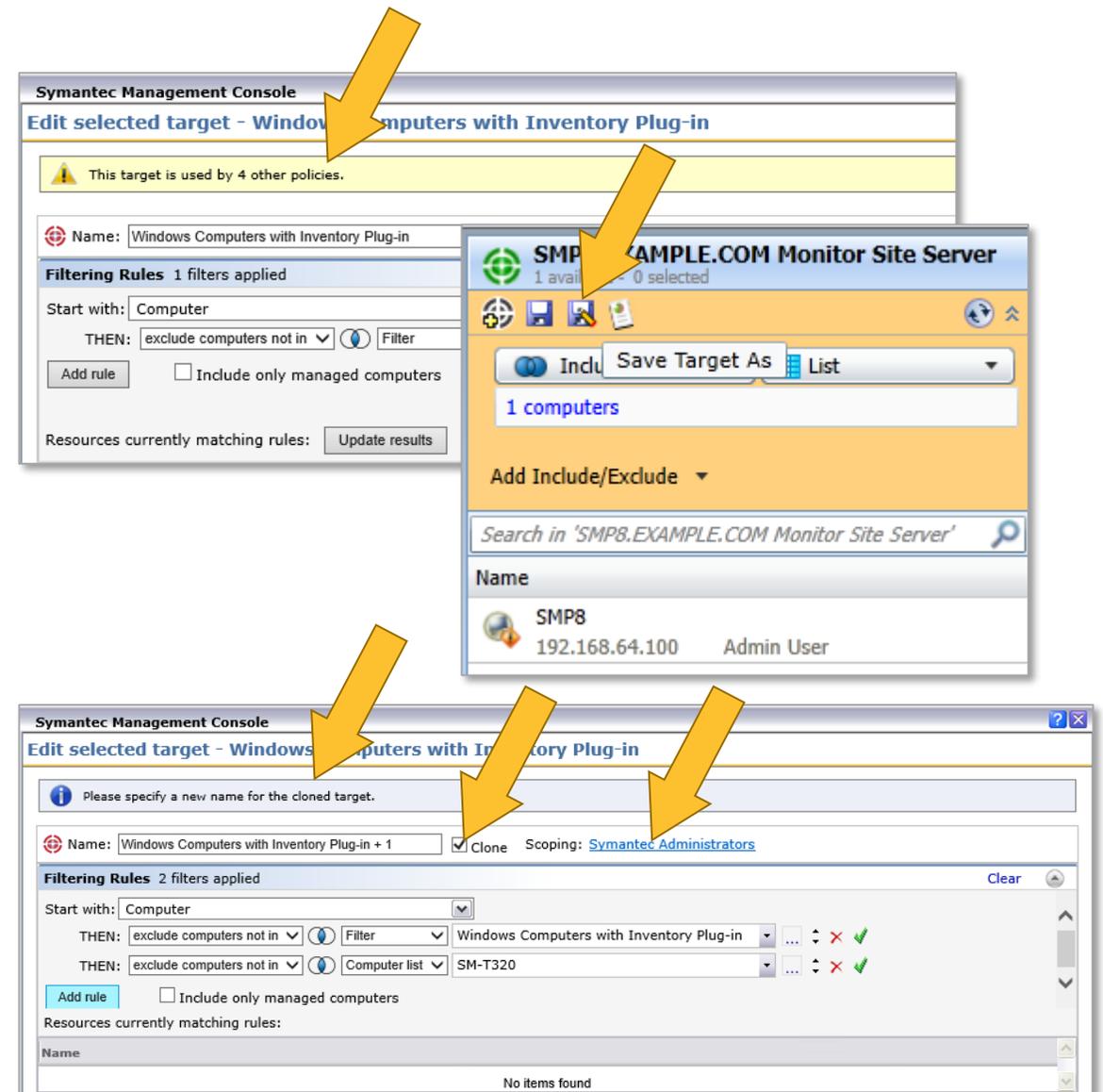
# Symantec Management Platform

## ○ Resource Target Modification

- Need to modify a shared Target for a Policy
- Warning appears “...Is used by *n* other Policies”
- To change the Target:
  - Close the Target window...
  - Find Target in Computer View...
  - Save the Target as something else...
  - Re-apply New Target in desired Policy.
- Within ITMS View, the targets section has a similar “Save As” option for an opened target

## ○ Resource Target Cloning

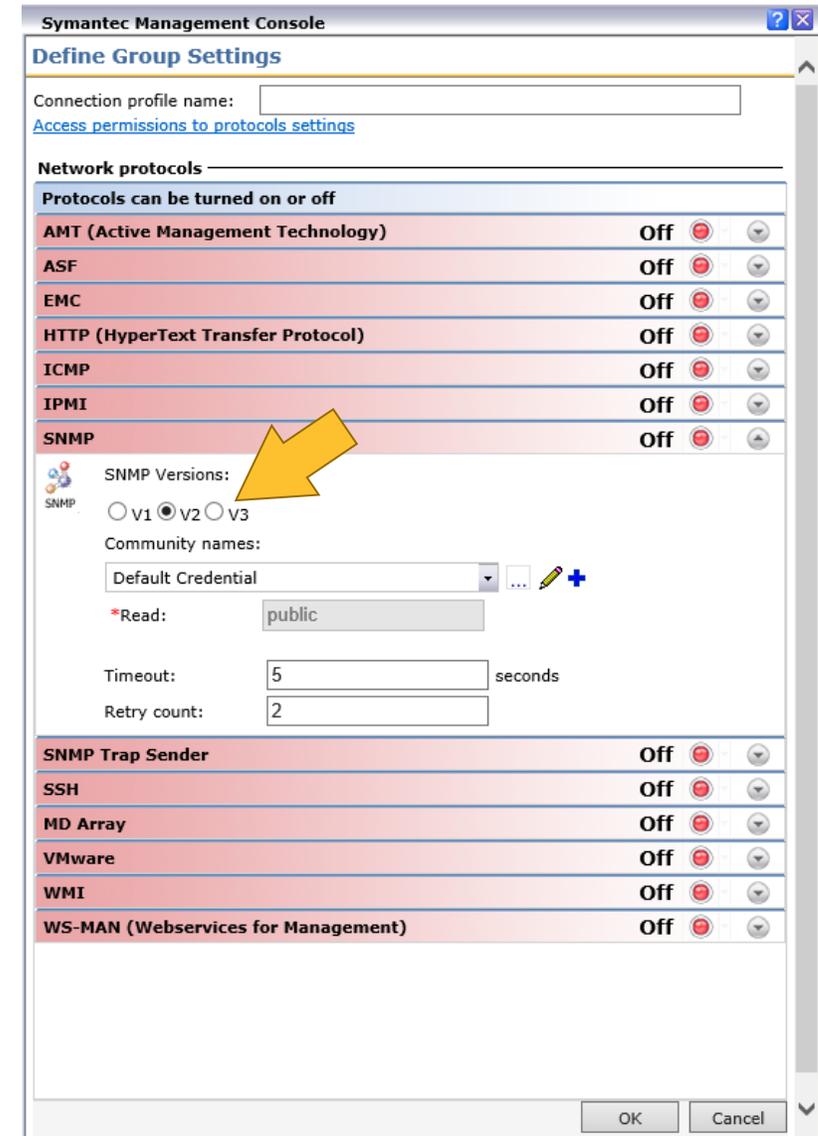
- “...Is used by...” Notification still exists
- Cloning check box added on Edit Target Page
- Scope is defined by security roles
- Lock icon on Target if insufficient rights



# Symantec Management Platform

## ○ SNMP v3 Support

- Protocol support on **Cisco** switches and the devices connected to them
  - I.e., Virtual Machines, Desktops, etc.
- Perform the following tasks
  - Discover the devices using Network Discovery.
  - Gather agentless inventory on the devices using Inventory for Network Devices.



Symantec Management Console

### Define Group Settings

Connection profile name:

[Access permissions to protocols settings](#)

**Network protocols**

Protocols can be turned on or off

Protocol	Status	Toggle
AMT (Active Management Technology)	Off	<input type="radio"/>
ASF	Off	<input type="radio"/>
EMC	Off	<input type="radio"/>
HTTP (HyperText Transfer Protocol)	Off	<input type="radio"/>
ICMP	Off	<input type="radio"/>
IPMI	Off	<input type="radio"/>
<b>SNMP</b>	Off	<input type="radio"/>
SNMP Trap Sender	Off	<input type="radio"/>
SSH	Off	<input type="radio"/>
MD Array	Off	<input type="radio"/>
VMware	Off	<input type="radio"/>
WMI	Off	<input type="radio"/>
WS-MAN (Webservices for Management)	Off	<input type="radio"/>

**SNMP Versions:**

V1  V2  V3

Community names:

Default Credential  ...

\*Read:

Timeout:  seconds

Retry count:

OK Cancel

# Symantec Management Platform

- **Schedule for SQL defragmentation**
  - **Database fragmentation causes massive impact to SQL operations**
  - Now Enabled by Default to run every Saturday
  - Should be Adjusted if a MS SQL Maintenance Plan is in place



**Shared Schedules**  
Manage shared schedules.

Shared Schedules are schedules which can be used by all managed tasks.

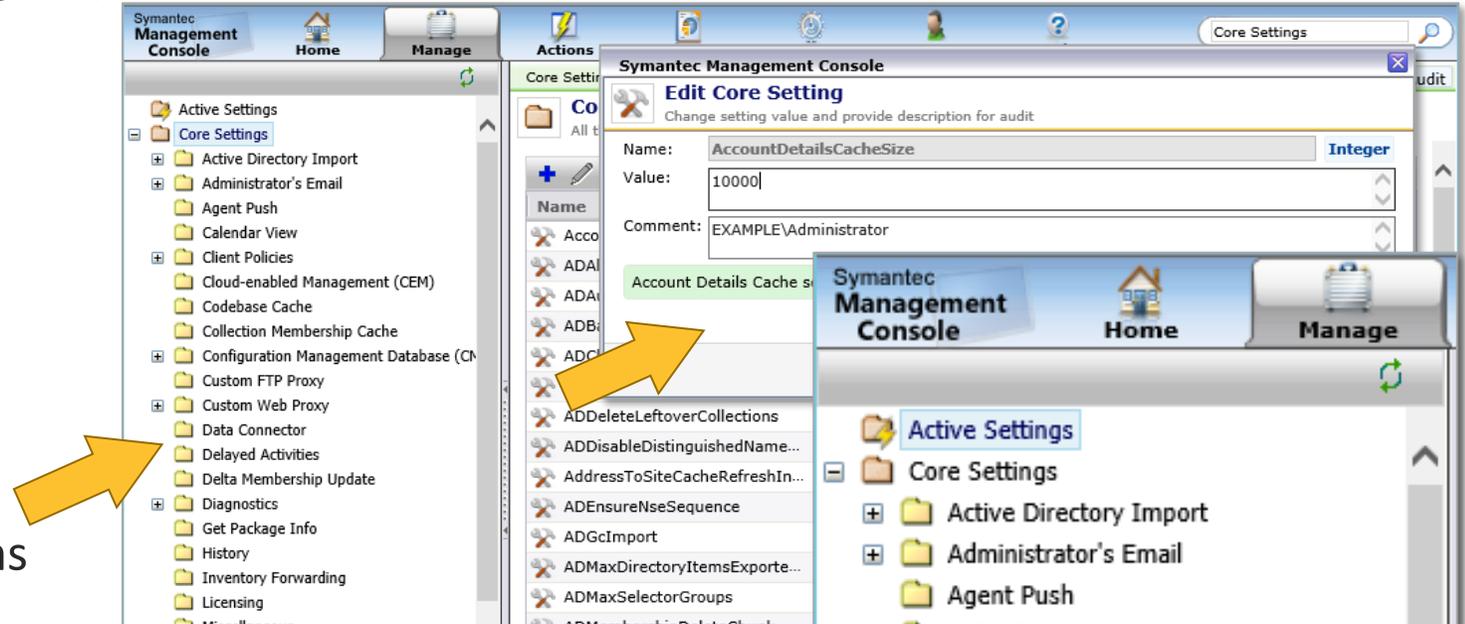
 Add Schedule    Resources

Enabled	Name	Description
<input checked="" type="checkbox"/>	Schedule to purge completed remediation tickets	At 10:00 AM every Sun of every 2 weeks, starting Saturday, January 1, 2005
<input checked="" type="checkbox"/> *	Restore Task Servers	At 12:00 AM on Monday, May 5, 1980
<input checked="" type="checkbox"/>	Purge Duplicate Inventory Rows	At 12:00 AM on Monday, May 5, 1980
<input checked="" type="checkbox"/>	<b>SQL defragmentation schedule</b>	At 12:00 PM every Sat of every 1 weeks, starting Monday, May 5, 1980
<input type="checkbox"/>	Schedule to pull remediation tickets	At 12:30 AM every 1 days, starting Saturday, January 1, 2005
<input checked="" type="checkbox"/>	Nightly schedule to associate Software compone...	At 12:30 AM every 1 days, starting Saturday, January 1, 2005
<input type="checkbox"/>	Detailed File Inventory Task schedule task	At 12:30 AM every Tue of every 1 weeks, starting Monday, May 26, 2008
<input checked="" type="checkbox"/>	SMP Statistic Uploader	At 2:00 AM every 1 days, starting Friday, January 1, 2010
<input checked="" type="checkbox"/>	Update Organizational Hierarchy	At 2:00 AM every 1 days, starting Wednesday, October 1, 2008
<input checked="" type="checkbox"/>	Complete Resource Membership Update	At 2:05 AM every 1 days, starting Saturday, January 1, 2005

# Symantec Management Platform

## ○ Core Settings Page

- Easy access to Core Settings
- Replaces NSConfigurator.exe
- All items are listed on the left pane
- Items are searchable
- Items can be edited easily
- Active Settings shows enabled items



## ○ Core Settings Audit Report

- Shows all changed core settings
- Shows From and To changes
- Shows User / Time of changes
- Allows you to edit the setting

Name	Time	User	From	To	Comment
MaxConcurrentMessageQueueThreadPoolSize	9/25/2018 7:41:43...	Example\Administrator	10	11	EXAMPLE\Administrator
MaxConcurrentCertificateRequests	9/25/2018 7:41:33...	Example\Administrator	600	700	EXAMPLE\Administrator
LoggingThreadPoolIdleMs	9/25/2018 7:41:22...	Example\Administrator	60000	50000	EXAMPLE\Administrator
ADPurgeIntermediateDays	9/25/2018 7:41:03...	Example\Administrator	30	30	EXAMPLE\Administrator
ADMaxSelectorGroups	9/25/2018 7:40:52...	Example\Administrator	200	202	EXAMPLE\Administrator
AccountDetailsCacheSize	9/25/2018 7:40:45...	Example\Administrator	10000	10001	EXAMPLE\Administrator
ADCrossDomainScanMode	9/25/2018 7:40:38...	Example\Administrator	3	3	EXAMPLE\Administrator

# Task/Package Server Infrastructure

## ○ New Site Based Reports

### ○ Subnet to Site Assignments

- lists the subnets and the sites to which they are assigned

### ○ Subnets with Affiliated Sites / by Computer

- Drill → View Computers in this Subnet

### ○ Packages Distribution by Download Type

- Package information and download count across all subnets or specific subnet.
- Drill → Exact source for package download along with transport used - HTTP, UNC, or P2P.

Reports ▾ Notification Server Management ▾ Server ▾ Subnet to Site assignments

**Subnet to Site assignments** Edit

Lists of Subnet to Site assignments including Encompassed subnets logic

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

Subnet	Site	Supernet
192.168.64.0/24	Corporate Site	-
10.104.198.0/24		
10.150.184.0/22		
10.16.0.0/24		
10.16.139.0/24		
10.16.232.0/24		

Reports ▾ Notification Server Management ▾ Server ▾ Subnets and Sites Info ▾ Subnets with Affiliated Sites

**Subnets with Affiliated Sites** Edit

List of subnets with affiliated Sites

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

Subnet	Formal Name	Subnet Mask	Assigned Site	Task Servers	Package Servers	Manually Assigned SS	Clients
192.168.64.0	192.168.64.0/24	255.255.255.0	Corporate Site	2	1	0	6
10.19.64.0	10.19.64.0/20	255.255.240.0		0	0	0	1
10.21.28.0	10.21.28.0/24	255.255.255.0		0	0	0	1

Rows: 3

Reports ▾ Notification Server Management ▾ Server ▾ Packages Distribution by Download Type

**Packages Distribution by Download Type** Edit

This report shows download types for each software package that client computers have downloaded within a specified timeframe. Additional i...

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

**Parameters** Subnet=, Package Name=%

Last N Days

Package Name

Subnet

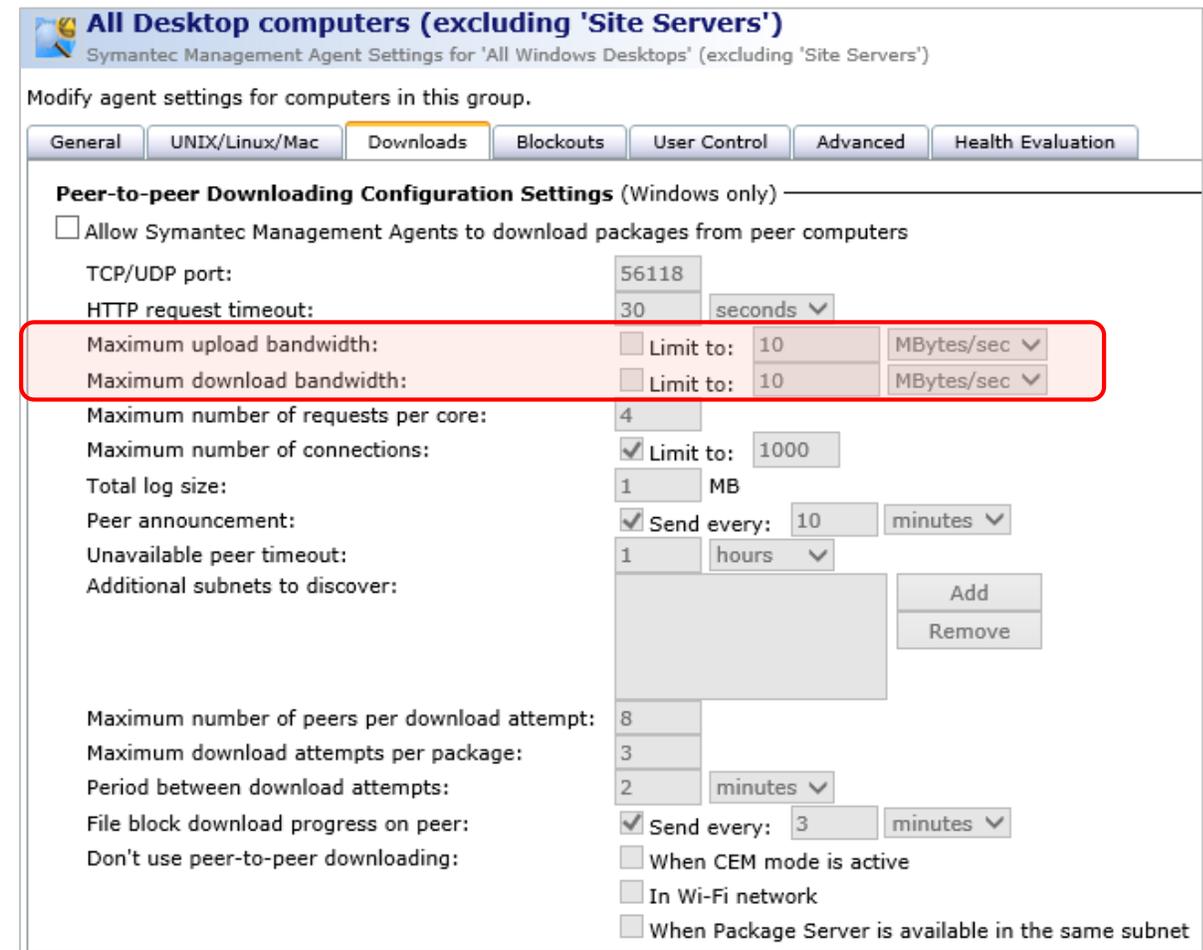
Package Name	Package Size (bytes)	Total Downloads	P2P (count)	P2P (%)	UNC (%)	HTTP (%)
No Results Returned						

Rows: 0

# Peer to Peer Infrastructure (P2P)

## ○ P2P Configuration Options

- *Maximum upload bandwidth and Maximum download bandwidth*
  - Replaces the **Maximum bandwidth** option
  - Independent from Throttling settings
  - Blockouts are Respected

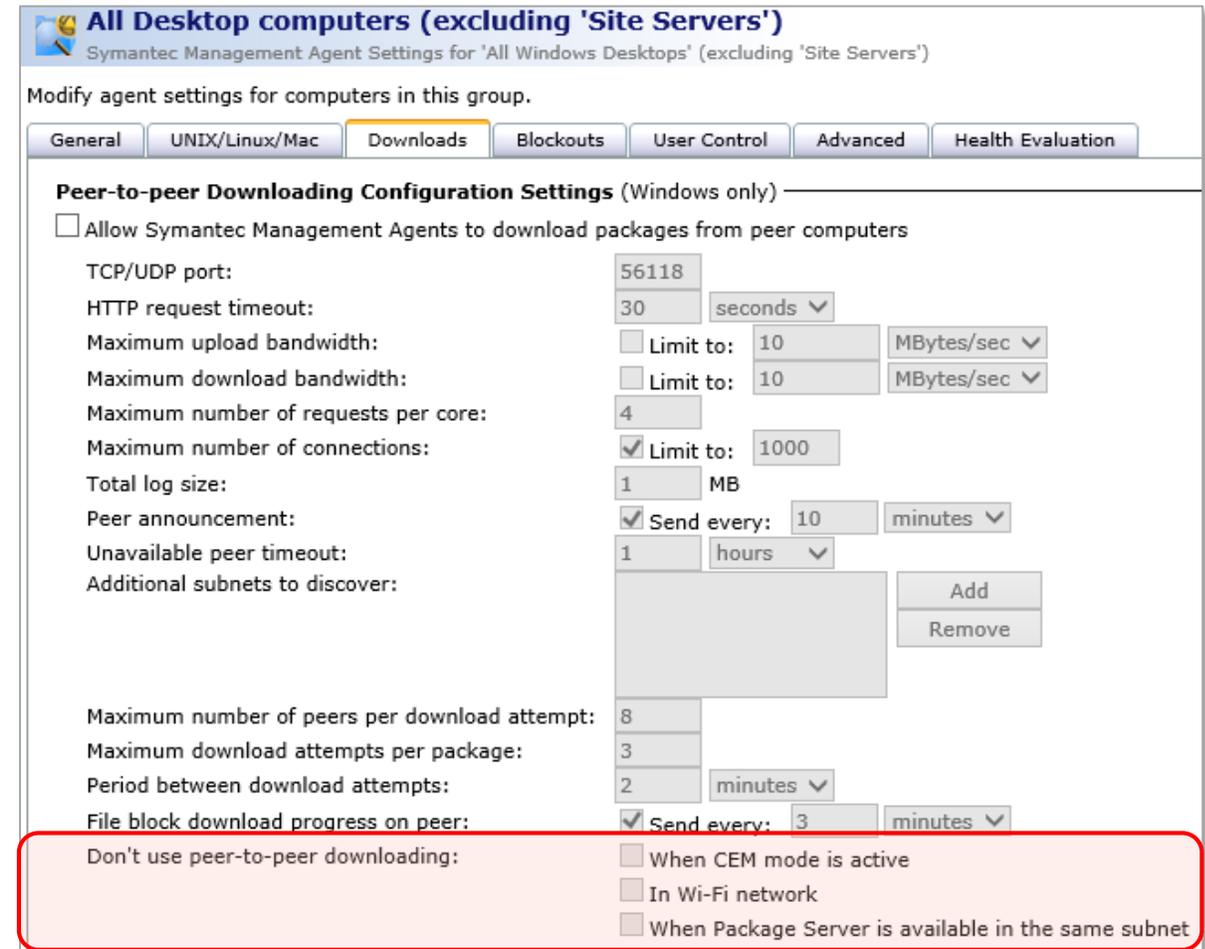


The screenshot displays the Symantec Management Agent Settings for 'All Desktop computers (excluding 'Site Servers')'. The 'Downloads' tab is selected, and the 'Peer-to-peer Downloading Configuration Settings (Windows only)' section is expanded. The 'Allow Symantec Management Agents to download packages from peer computers' checkbox is unchecked. The 'Maximum upload bandwidth' and 'Maximum download bandwidth' settings are highlighted with a red box, both set to 'Limit to: 10 MBytes/sec'. Other settings include TCP/UDP port (56118), HTTP request timeout (30 seconds), Maximum number of requests per core (4), Maximum number of connections (Limit to: 1000), Total log size (1 MB), Peer announcement (Send every: 10 minutes), Unavailable peer timeout (1 hours), and Maximum number of peers per download attempt (8).

# Peer to Peer Infrastructure (P2P)

## ○ P2P Configuration Options

- *Maximum upload bandwidth and Maximum download bandwidth*
  - Replaces the **Maximum bandwidth** option
  - Independent from Throttling settings
  - Blockouts are Respected
- **Don't use peer-to-peer downloading**
  - Disables P2P downloading in certain cases.
  - *When PS is available on same subnet*
    - Prevents P2P Downloading when codebases are received on the local subnet
  - *When CeM Mode is Enabled*
    - Disables P2P Downloading when CeM is enabled and resumes in Intranet mode
  - *When in Wi-Fi Network*
    - Disables P2P activity for local subnets connected through Wi-Fi adapters



**All Desktop computers (excluding 'Site Servers')**  
Symantec Management Agent Settings for 'All Windows Desktops' (excluding 'Site Servers')

Modify agent settings for computers in this group.

General UNIX/Linux/Mac Downloads Blockouts User Control Advanced Health Evaluation

**Peer-to-peer Downloading Configuration Settings (Windows only)**

Allow Symantec Management Agents to download packages from peer computers

TCP/UDP port: 56118

HTTP request timeout: 30 seconds

Maximum upload bandwidth:  Limit to: 10 MBytes/sec

Maximum download bandwidth:  Limit to: 10 MBytes/sec

Maximum number of requests per core: 4

Maximum number of connections:  Limit to: 1000

Total log size: 1 MB

Peer announcement:  Send every: 10 minutes

Unavailable peer timeout: 1 hours

Additional subnets to discover:  Add Remove

Maximum number of peers per download attempt: 8

Maximum download attempts per package: 3

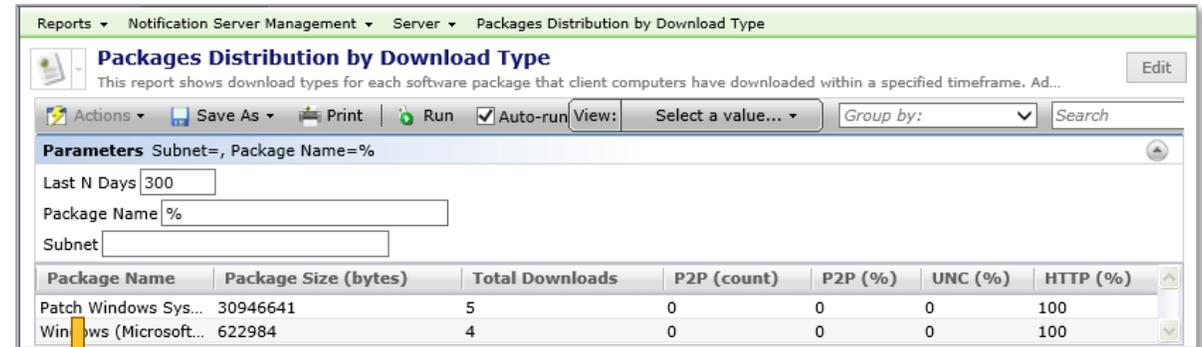
Period between download attempts: 2 minutes

File block download progress on peer:  Send every: 3 minutes

Don't use peer-to-peer downloading:  When CEM mode is active  
 In Wi-Fi network  
 When Package Server is available in the same subnet

# Peer to Peer Infrastructure (P2P)

- Improved Usability of P2P Reports
  - Packages Distribution by Download Type
    - *Drill Down* > Downloads by Computers and Download Types
      - *Drill Down* > Computers TCP/IP Info



Reports > Notification Server Management > Server > Packages Distribution by Download Type

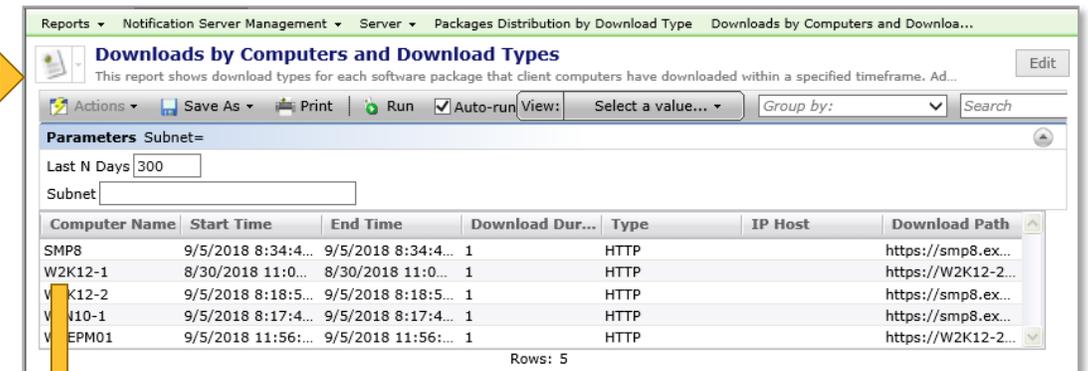
**Packages Distribution by Download Type**  
This report shows download types for each software package that client computers have downloaded within a specified timeframe. Ad...

Actions > Save As > Print > Run > Auto-run View: Select a value... Group by: Search

Parameters Subnet=, Package Name=%

Last N Days 300  
Package Name %  
Subnet

Package Name	Package Size (bytes)	Total Downloads	P2P (count)	P2P (%)	UNC (%)	HTTP (%)
Patch Windows Sys...	30946641	5	0	0	0	100
Windows (Microsoft...	622984	4	0	0	0	100



Reports > Notification Server Management > Server > Packages Distribution by Download Type > Downloads by Computers and Download Types

**Downloads by Computers and Download Types**  
This report shows download types for each software package that client computers have downloaded within a specified timeframe. Ad...

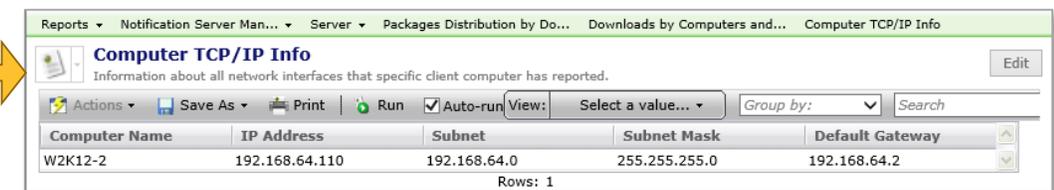
Actions > Save As > Print > Run > Auto-run View: Select a value... Group by: Search

Parameters Subnet=

Last N Days 300  
Subnet

Computer Name	Start Time	End Time	Download Dur...	Type	IP Host	Download Path
SMP8	9/5/2018 8:34:4...	9/5/2018 8:34:4...	1	HTTP		https://smp8.ex...
W2K12-1	8/30/2018 11:0...	8/30/2018 11:0...	1	HTTP		https://W2K12-2...
W2K12-2	9/5/2018 8:18:5...	9/5/2018 8:18:5...	1	HTTP		https://smp8.ex...
WIN10-1	9/5/2018 8:17:4...	9/5/2018 8:17:4...	1	HTTP		https://smp8.ex...
WEPM01	9/5/2018 11:56:...	9/5/2018 11:56:...	1	HTTP		https://W2K12-2...

Rows: 5



Reports > Notification Server Man... > Server > Packages Distribution by Do... > Downloads by Computers and... > Computer TCP/IP Info

**Computer TCP/IP Info**  
Information about all network interfaces that specific client computer has reported.

Actions > Save As > Print > Run > Auto-run View: Select a value... Group by: Search

Computer Name	IP Address	Subnet	Subnet Mask	Default Gateway
W2K12-2	192.168.64.110	192.168.64.0	255.255.255.0	192.168.64.2

Rows: 1

## Past Peer to Peer Infrastructure Challenges (P2P)



Existing Limitations Impacting Delivery Time

**Network instability**

Computers are elected as peer master and start downloading the same package again

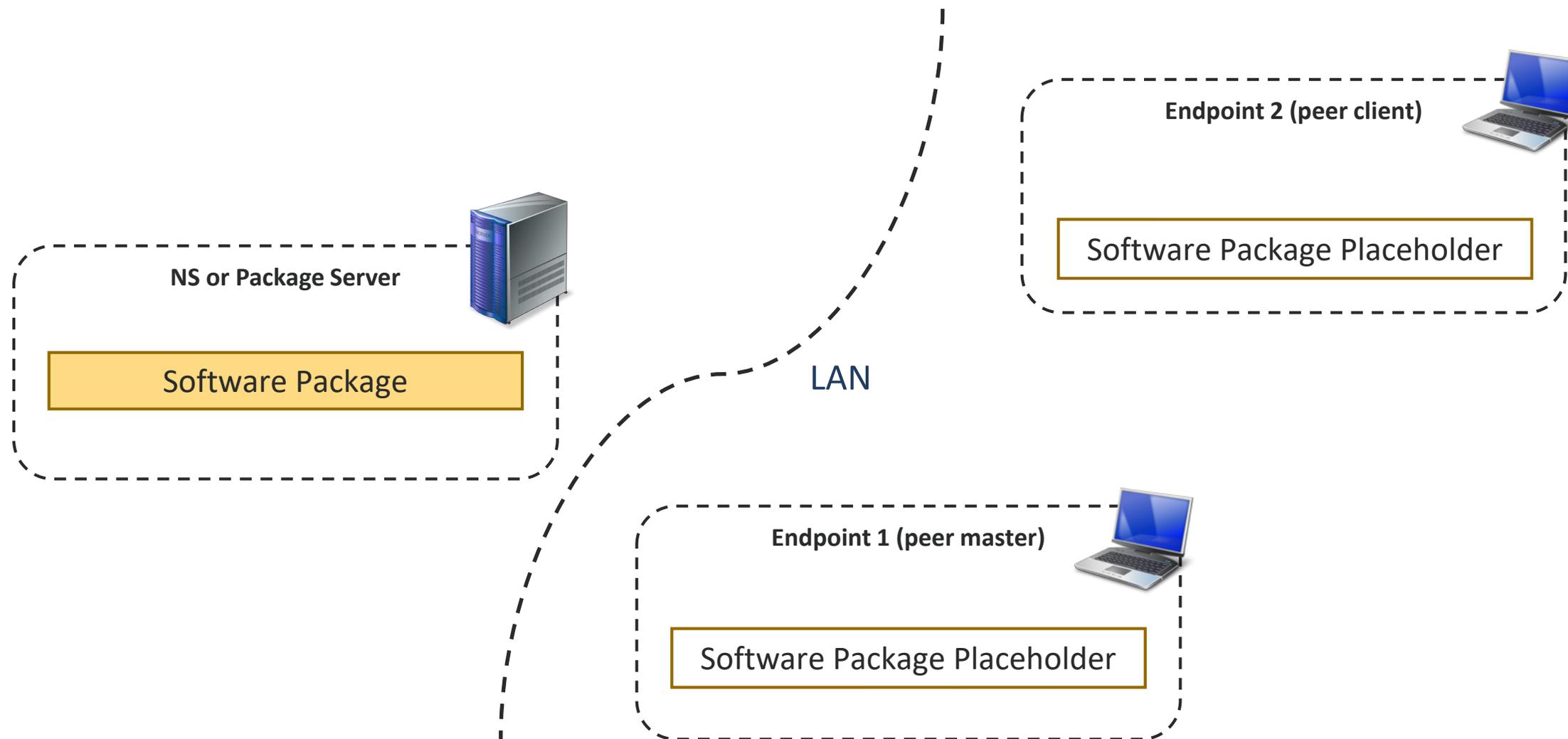
**Minor change in package content**

Entire file has to be re-downloaded as the hash will be different

**Late corruption detection**

Entire corrupted file needs to be re-downloaded

# New: File and Block Level Downloading in P2P

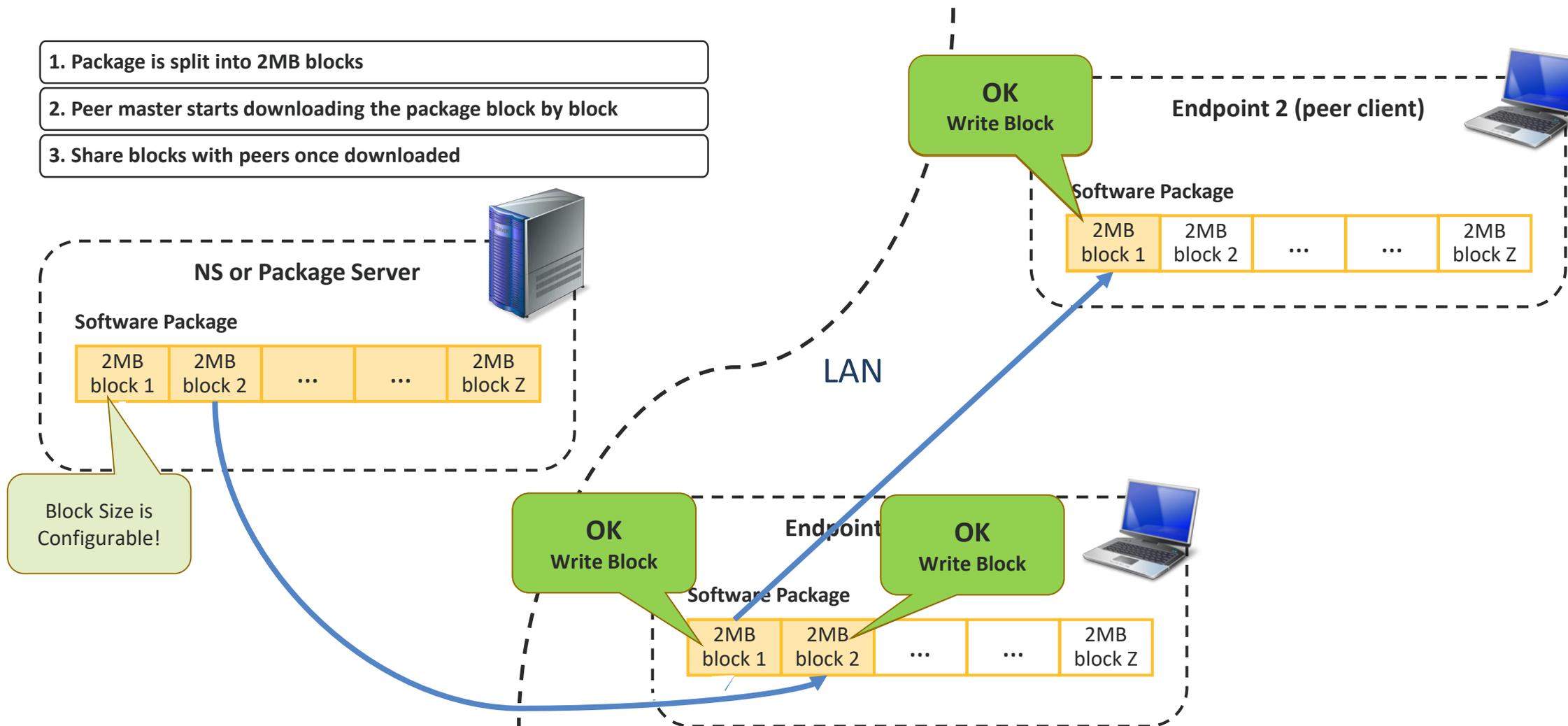


# File and Block Level Downloading

1. Package is split into 2MB blocks

2. Peer master starts downloading the package block by block

3. Share blocks with peers once downloaded



## Solution to Limitations in Package Delivery



Download blocks  
and share them  
immediately

**Network instability**



Transfer only  
changed block(s)

**Minor change in  
package content**



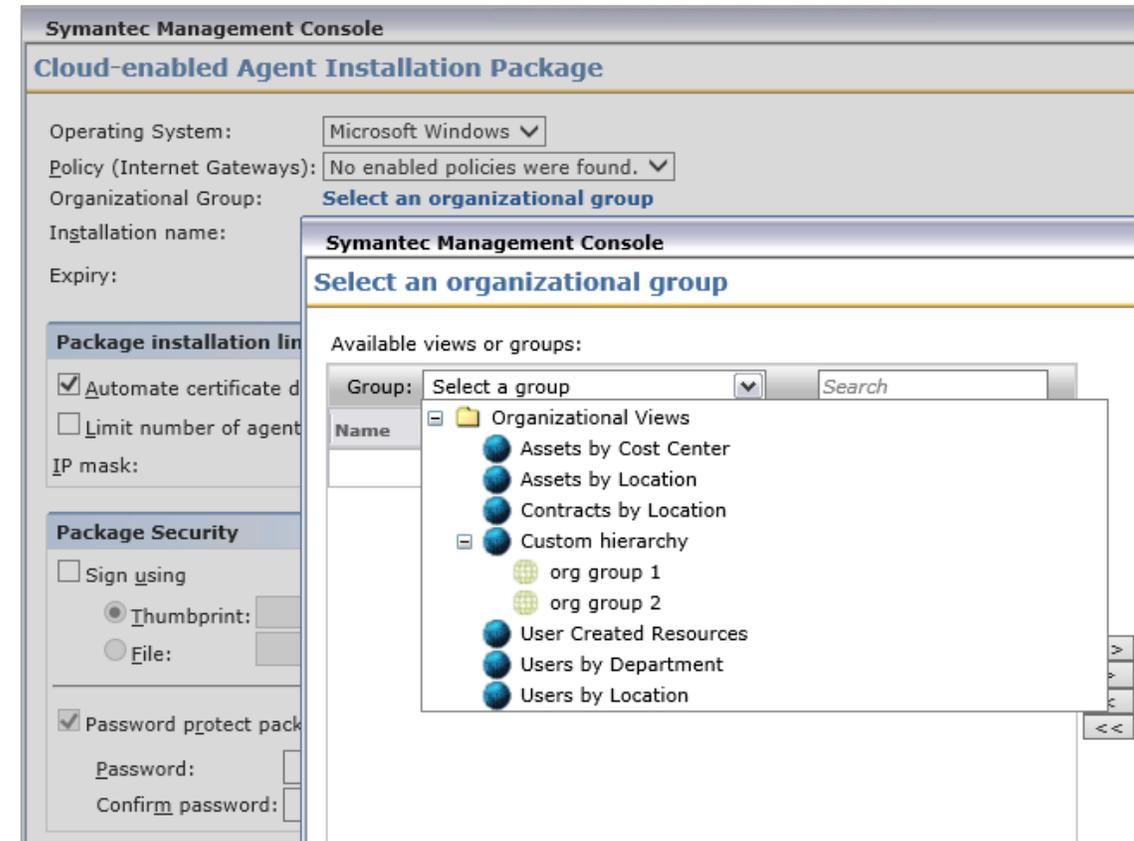
Re-download only  
damaged blocks

**Late corruption  
detection**

Existing Limitations Impacting Delivery Time

# Cloud Enabled Management

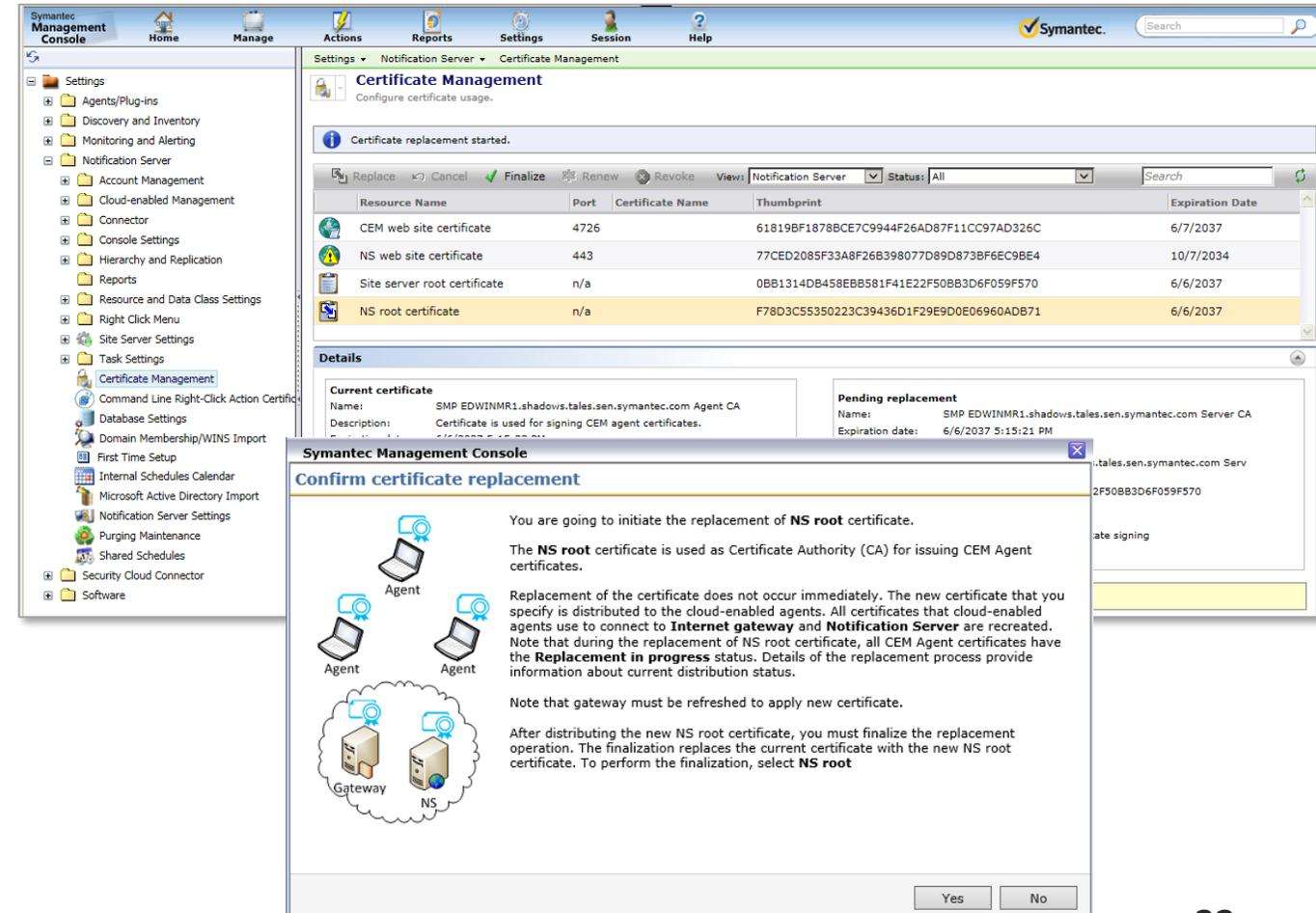
- **Cloud-enabled Agent Installation Package**
  - Select multiple Organizational Groups
  - When Running the Install Package:
    - The end user must select the group
    - The respective communication profile is applied.



# Certificate Management – In the Console

## ○ Certificate Management Page

- Located in *Settings > Notification Server > Certificate Management*
- Combines existing and new capabilities
  - Renewal of CEM agent certificates
  - Replacement of root certificate
  - Replacement of website certificates
- Guides you through the required replacement process.
- Easily see and fix the issues with current certificates.



The screenshot displays the Symantec Management Console interface. The left sidebar shows the navigation tree with 'Certificate Management' selected under 'Notification Server'. The main pane shows the 'Certificate Management' page with a table of certificates and a 'Details' section.

Resource Name	Port	Certificate Name	Thumbprint	Expiration Date
CEM web site certificate	4726		61819BF1878BCE7C9944F26AD87F11CC97AD326C	6/7/2037
NS web site certificate	443		77CED2085F33A8F26B398077D89D873BF6EC9BE4	10/7/2034
Site server root certificate	n/a		0BB1314DB458EBB581F41E22F50BB3D6F059F570	6/6/2037
NS root certificate	n/a		F78D3C55350223C39436D1F29E9D0E06960ADB71	6/6/2037

The 'Details' section shows the 'Current certificate' and 'Pending replacement' information. A 'Confirm certificate replacement' dialog box is overlaid, providing instructions for replacing the NS root certificate.

**Symantec Management Console**  
**Confirm certificate replacement**

You are going to initiate the replacement of **NS root** certificate.

The **NS root** certificate is used as Certificate Authority (CA) for issuing CEM Agent certificates.

Replacement of the certificate does not occur immediately. The new certificate that you specify is distributed to the cloud-enabled agents. All certificates that cloud-enabled agents use to connect to **Internet gateway** and **Notification Server** are recreated. Note that during the replacement of NS root certificate, all CEM Agent certificates have the **Replacement in progress** status. Details of the replacement process provide information about current distribution status.

Note that gateway must be refreshed to apply new certificate.

After distributing the new NS root certificate, you must finalize the replacement operation. The finalization replaces the current certificate with the new NS root certificate. To perform the finalization, select **NS root**.

Yes No

# Certificate Management

- **Certificate Status Report**
  - Shows the list of agents with/without certificate
  - On the **Certificate Management** page, under **Reports**
  - Also under **Reports > Notification Server Management > Agent**

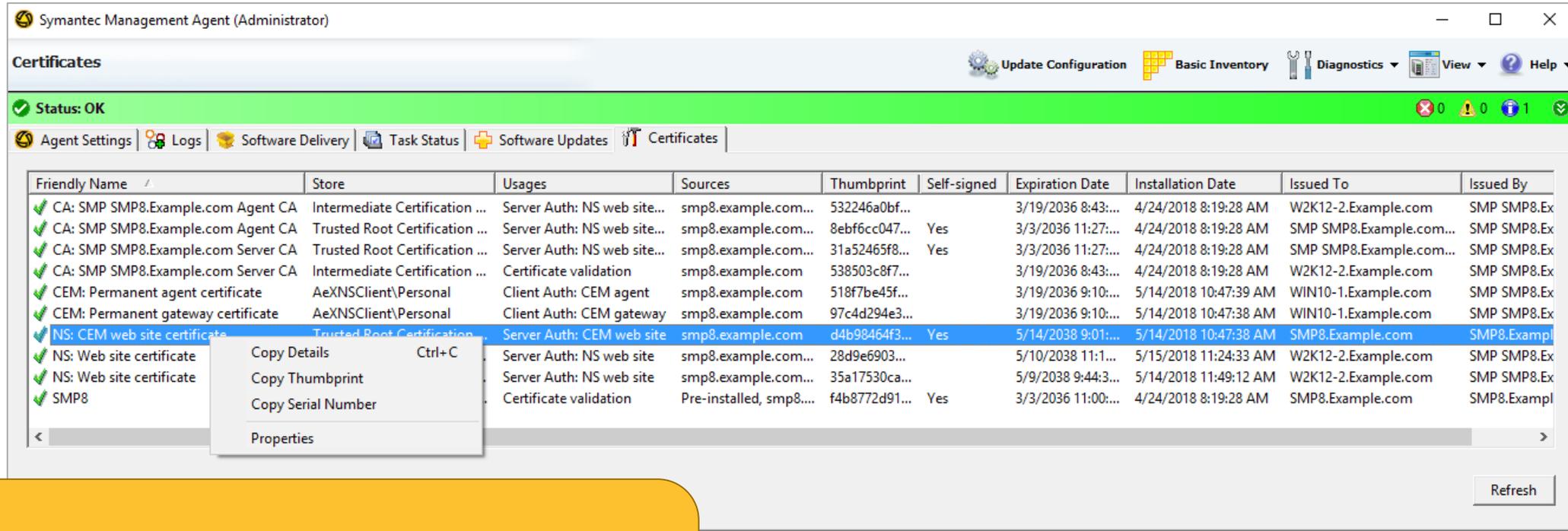
The screenshot displays the Symantec Certificate Management interface. The main window shows a list of certificates with columns for Resource Name, Port, and Certificate. The 'NS web site certificate' is highlighted. Below the list is a 'Details' section for the selected certificate, showing its name (DV16SQL16), description (NS web site certificate), expiration date (12/5/2037 3:43:30 PM), effective date (12/5/2017 3:43:30 PM), issued by (CN=DV16SQL16), thumbprint (E57F3455EA7FC8C910EFA5F4980), signature algorithm (sha256RSA), purpose, and status (Self-signed certificate).

On the right side, a report titled 'Computers having (or without) a Certificate' is displayed. The report parameters include 'Certificate Thumbprint=97A2933B5F317242D8F21CDD87E1523C69C14089, Show' and 'Number of computers to show 500'. The report table lists the following data:

Name	Doma	OS Name	Machine Guid	Server
DVParentSmoke	WO...	Windows Serv...	6fd15e66-afd3-414...	DV16SQL16
DV16NSSL	WO...	Windows Serv...	ae9b31fb-f184-482...	DV16SQL16
DV16SQL16	WO...	Windows Serv...	824acd66-7d1f-4fa...	DV16SQL16

A blue arrow points from the 'Reports' section in the bottom left of the main window to the report window. A yellow arrow points from the 'Reports' section in the bottom left of the report window to the 'Computers having (or without) a Certificate' report item in the navigation tree.

# Certificate Management – Agent UI



**Certificates**

Status: OK

Agent Settings | Logs | Software Delivery | Task Status | Software Updates | Certificates

Friendly Name	Store	Usages	Sources	Thumbprint	Self-signed	Expiration Date	Installation Date	Issued To	Issued By
CA: SMP SMP8.Example.com Agent CA	Intermediate Certification ...	Server Auth: NS web site...	smp8.example.com...	532246a0bf...		3/19/2036 8:43:...	4/24/2018 8:19:28 AM	W2K12-2.Example.com	SMP SMP8.Ex
CA: SMP SMP8.Example.com Agent CA	Trusted Root Certification ...	Server Auth: NS web site...	smp8.example.com...	8ebf6cc047...	Yes	3/3/2036 11:27:...	4/24/2018 8:19:28 AM	SMP SMP8.Example.com...	SMP SMP8.Ex
CA: SMP SMP8.Example.com Server CA	Trusted Root Certification ...	Server Auth: NS web site...	smp8.example.com...	31a52465f8...	Yes	3/3/2036 11:27:...	4/24/2018 8:19:28 AM	SMP SMP8.Example.com...	SMP SMP8.Ex
CA: SMP SMP8.Example.com Server CA	Intermediate Certification ...	Certificate validation	smp8.example.com	538503c8f7...		3/19/2036 8:43:...	4/24/2018 8:19:28 AM	W2K12-2.Example.com	SMP SMP8.Ex
CEM: Permanent agent certificate	AeXNSClient\Personal	Client Auth: CEM agent	smp8.example.com	518f7be45f...		3/19/2036 9:10:...	5/14/2018 10:47:39 AM	WIN10-1.Example.com	SMP SMP8.Ex
CEM: Permanent gateway certificate	AeXNSClient\Personal	Client Auth: CEM gateway	smp8.example.com	97c4d294e3...		3/19/2036 9:10:...	5/14/2018 10:47:38 AM	WIN10-1.Example.com	SMP SMP8.Ex
NS: CEM web site certificate	Trusted Root Certification ...	Server Auth: CEM web site	smp8.example.com	d4b98464f3...	Yes	5/14/2038 9:01:...	5/14/2018 10:47:38 AM	SMP8.Example.com	SMP8.Exampl
NS: Web site certificate		Server Auth: NS web site	smp8.example.com...	28d9e6903...		5/10/2038 11:1...	5/15/2018 11:24:33 AM	W2K12-2.Example.com	SMP SMP8.Ex
NS: Web site certificate		Server Auth: NS web site	smp8.example.com...	35a17530ca...		5/9/2038 9:44:3...	5/14/2018 11:49:12 AM	W2K12-2.Example.com	SMP SMP8.Ex
SMP8		Certificate validation	Pre-installed, smp8....	f4b8772d91...	Yes	3/3/2036 11:00:...	4/24/2018 8:19:28 AM	SMP8.Example.com	SMP8.Exampl

Refresh

Prior to **ITMS 8.1 RU2**, the Symantec Management Agent used Simple Certificate Management stored in **HKLM\SOFTWARE\Altiris\Communications\Certificates**

# Certificate Management – Agent UI

Extended certificate properties to store SMA related information

Friendly Name	Store	Usages	Sources	Thumbprint	Signed	Expiration Date	Installation Date	Issued To	Issued By
CA: SMP SMP8.Example.com Agent CA	Intermediate Certification ...	Server Auth: NS web site...	smp8.example.com...	532246a0bf...		3/19/2036 8:43:...	4/24/2018 8:19:28 AM	W2K12-2.Example.com	SMP SMP8.Ex
CA: SMP SMP8.Example.com Agent CA	Trusted Root Certification ...	Server Auth: NS web site...	smp8.example.com...	8ebf6cc047...	Yes	3/3/2036 11:27:...	4/24/2018 8:19:28 AM	SMP SMP8.Example.com...	SMP SMP8.Ex
CA: SMP SMP8.Example.com Server CA	Trusted Root Certification ...	Server Auth: NS web site...	smp8.example.com...	31a52465f8...	Yes	3/3/2036 11:27:...	4/24/2018 8:19:28 AM	SMP SMP8.Example.com...	SMP SMP8.Ex
CA: SMP SMP8.Example.com Server CA	Intermediate Certification ...	Certificate validation	smp8.example.com	538503c8f7...		3/19/2036 8:43:...	4/24/2018 8:19:28 AM	W2K12-2.Example.com	SMP SMP8.Ex
CEM: Permanent agent certificate	AeXNSClient\Personal	Client Auth: CEM agent	smp8.example.com	518f7be45f...		3/19/2036 9:10:...	5/14/2018 10:47:39 AM	WIN10-1.Example.com	SMP SMP8.Ex
CEM: Permanent gateway certificate	AeXNSClient\Personal	Client Auth: CEM gateway	smp8.example.com	97c4d294e3...		3/19/2036 9:10:...	5/14/2018 10:47:38 AM	WIN10-1.Example.com	SMP SMP8.Ex
NS: CEM web site certificate	Trusted Root Certification ...	Server Auth: CEM web site	smp8.example.com	d4b98464f3...	Yes	5/14/2038 9:01:...	5/14/2018 10:47:38 AM	SMP8.Example.com	SMP8.Exampl
NS: Web site certificate		Server Auth: NS web site	smp8.example.com...	28d9e6903...		5/10/2038 11:1...	5/15/2018 11:24:33 AM	W2K12-2.Example.com	SMP SMP8.Ex
NS: Web site certificate		Server Auth: NS web site	smp8.example.com...	35a17530ca...		5/9/2038 9:44:3...	5/14/2018 11:49:12 AM	W2K12-2.Example.com	SMP SMP8.Ex
SMP8		Certificate validation	Pre-installed, smp8....	f4b8772d91...	Yes	3/3/2036 11:00:...	4/24/2018 8:19:28 AM	SMP8.Example.com	SMP8.Exampl

New Certificate Management

Refresh

# Certificate Management – Agent UI

NEW Certificates UI Page when Diagnostics are Enabled

Status: OK

Agent Settings | Logs | Software Delivery | Task Status | Software Updates | Certificates

Friendly Name	Store	Usages	Sources	Thumbprint	Self-signed	Expiration Date	Installation Date	Issued To	Issued By
CA: SMP SMP8.Example.com Agent CA	Intermediate Certification ...	Server Auth: NS web site...	smp8.example.com...	532246a0bf...		3/19/2036 8:43:...	4/24/2018 8:19:28 AM	W2K12-2.Example.com	SMP SMP8.Ex
CA: SMP SMP8.Example.com Agent CA	Trusted Root Certification ...	Server Auth: NS web site...	smp8.example.com...	8ebf6cc047...	Yes	3/3/2036 11:27:...	4/24/2018 8:19:28 AM	SMP SMP8.Example.com...	SMP SMP8.Ex
CA: SMP SMP8.Example.com Server CA	Trusted Root Certification ...	Server Auth: NS web site...	smp8.example.com...	31a52465f8...	Yes	3/3/2036 11:27:...	4/24/2018 8:19:28 AM	SMP SMP8.Example.com...	SMP SMP8.Ex
CA: SMP SMP8.Example.com Server CA	Intermediate Certification ...	Certificate validation	smp8.example.com	538503c8f7...		3/19/2036 8:43:...	4/24/2018 8:19:28 AM	W2K12-2.Example.com	SMP SMP8.Ex
CEM: Permanent agent certificate	AeXNSClient\Personal	Client Auth: CEM agent	smp8.example.com	518f7be45f...		3/19/2036 9:10:...	5/14/2018 10:47:39 AM	WIN10-1.Example.com	SMP SMP8.Ex
CEM: Permanent gateway certificate	AeXNSClient\Personal	Client Auth: CEM gateway	smp8.example.com	97c4d294e3...		3/19/2036 9:10:...	5/14/2018 10:47:38 AM	WIN10-1.Example.com	SMP SMP8.Ex
NS: CEM web site certificate	Trusted Root Certification ...	Server Auth: CEM web site	smp8.example.com	d4b98464f3...	Yes	5/14/2038 9:01:...	5/14/2018 10:47:38 AM	SMP8.Example.com	SMP8.Exampl
NS: Web site certificate		Server Auth: NS web site	smp8.example.com...	28d9e6903...		5/10/2038 11:1...	5/15/2018 11:24:33 AM	W2K12-2.Example.com	SMP SMP8.Ex
NS: Web site certificate		Server Auth: NS web site	smp8.example.com...	35a17530ca...		5/9/2038 9:44:3...	5/14/2018 11:49:12 AM	W2K12-2.Example.com	SMP SMP8.Ex
SMP8		Certificate validation	Pre-installed, smp8....	f4b8772d91...	Yes	3/3/2036 11:00:...	4/24/2018 8:19:28 AM	SMP8.Example.com	SMP8.Exampl

Copy Details Ctrl+C  
Copy Thumbprint  
Copy Serial Number  
Properties

Refresh

Some Properties are not available in the Windows Certificate MMC

# Certificate Management – Agent UI

Friendly Names for Certificate Usage  
NS, CEM, CA...

Symantec Management Agent (Administrator)

**Certificates** Update Configuration Basic Inventory Diagnostics View Help

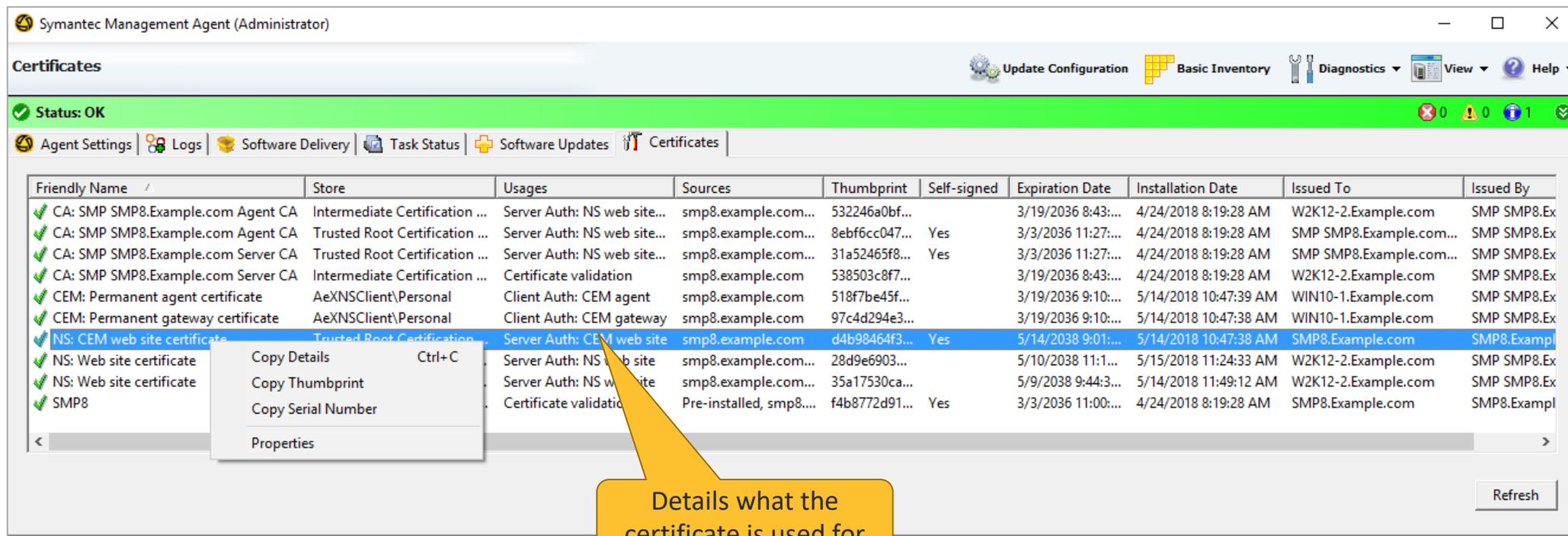
Status: OK

Agent Settings | Logs | Software Delivery | Task Status | Software Updates | Certificates

Friendly Name	Store	Usages	Sources	Thumbprint	Self-signed	Expiration Date	Installation Date	Issued To	Issued By
CA: SMP SMP8.Example.com Agent CA	Intermediate Certification ...	Server Auth: NS web site...	smp8.example.com...	532246a0bf...		3/19/2036 8:43:...	4/24/2018 8:19:28 AM	W2K12-2.Example.com	SMP SMP8.Ex
CA: SMP SMP8.Example.com Agent CA	Trusted Root Certification ...	Server Auth: NS web site...	smp8.example.com...	8ebf6cc047...	Yes	3/3/2036 11:27:...	4/24/2018 8:19:28 AM	SMP SMP8.Example.com...	SMP SMP8.Ex
CA: SMP SMP8.Example.com Server CA	Trusted Root Certification ...	Server Auth: NS web site...	smp8.example.com...	31a52465f8...	Yes	3/3/2036 11:27:...	4/24/2018 8:19:28 AM	SMP SMP8.Example.com...	SMP SMP8.Ex
CA: SMP SMP8.Example.com Server CA	Intermediate Certification ...	Certificate validation	smp8.example.com	538503c8f7...		3/19/2036 8:43:...	4/24/2018 8:19:28 AM	W2K12-2.Example.com	SMP SMP8.Ex
CEM: Permanent agent certificate	AeXNSClient\Personal	Client Auth: CEM agent	smp8.example.com	518f7be45f...		3/19/2036 9:10:...	5/14/2018 10:47:39 AM	WIN10-1.Example.com	SMP SMP8.Ex
CEM: Permanent gateway certificate	AeXNSClient\Personal	Client Auth: CEM gateway	smp8.example.com	97c4d294e3...		3/19/2036 9:10:...	5/14/2018 10:47:38 AM	WIN10-1.Example.com	SMP SMP8.Ex
NS: CEM web site certificate	Trusted Root Certification ...	Server Auth: CEM web site	smp8.example.com	d4b98464f3...	Yes	5/14/2038 9:01:...	5/14/2018 10:47:38 AM	SMP8.Example.com	SMP8.Exampl
NS: Web site certificate		Server Auth: NS web site	smp8.example.com...	28d9e6903...		5/10/2038 11:1...	5/15/2018 11:24:33 AM	W2K12-2.Example.com	SMP SMP8.Ex
NS: Web site certificate		Server Auth: NS web site	smp8.example.com...	35a17530ca...		5/9/2038 9:44:3...	5/14/2018 11:49:12 AM	W2K12-2.Example.com	SMP SMP8.Ex
SMP8		Certificate validation	Pre-installed, smp8....	f4b8772d91...	Yes	3/3/2036 11:00:...	4/24/2018 8:19:28 AM	SMP8.Example.com	SMP8.Exampl

Refresh

# Certificate Management – Agent UI



Symantec Management Agent (Administrator)

**Certificates** [Update Configuration] [Basic Inventory] [Diagnostics] [View] [Help]

Status: OK

Agent Settings | Logs | Software Delivery | Task Status | Software Updates | **Certificates**

Friendly Name	Store	Usages	Sources	Thumbprint	Self-signed	Expiration Date	Installation Date	Issued To	Issued By
CA: SMP SMP8.Example.com Agent CA	Intermediate Certification ...	Server Auth: NS web site...	smp8.example.com...	532246a0bf...		3/19/2036 8:43:...	4/24/2018 8:19:28 AM	W2K12-2.Example.com	SMP SMP8.Ex
CA: SMP SMP8.Example.com Agent CA	Trusted Root Certification ...	Server Auth: NS web site...	smp8.example.com...	8ebf6cc047...	Yes	3/3/2036 11:27:...	4/24/2018 8:19:28 AM	SMP SMP8.Example.com...	SMP SMP8.Ex
CA: SMP SMP8.Example.com Server CA	Trusted Root Certification ...	Server Auth: NS web site...	smp8.example.com...	31a52465f8...	Yes	3/3/2036 11:27:...	4/24/2018 8:19:28 AM	SMP SMP8.Example.com...	SMP SMP8.Ex
CA: SMP SMP8.Example.com Server CA	Intermediate Certification ...	Certificate validation	smp8.example.com	538503c8f7...		3/19/2036 8:43:...	4/24/2018 8:19:28 AM	W2K12-2.Example.com	SMP SMP8.Ex
CEM: Permanent agent certificate	AeXNSClient\Personal	Client Auth: CEM agent	smp8.example.com	518f7be45f...		3/19/2036 9:10:...	5/14/2018 10:47:39 AM	WIN10-1.Example.com	SMP SMP8.Ex
CEM: Permanent gateway certificate	AeXNSClient\Personal	Client Auth: CEM gateway	smp8.example.com	97c4d294e3...		3/19/2036 9:10:...	5/14/2018 10:47:38 AM	WIN10-1.Example.com	SMP SMP8.Ex
NS: CEM web site certificate	Trusted Root Certification ...	Server Auth: CEM web site	smp8.example.com	d4b98464f3...	Yes	5/14/2038 9:01:...	5/14/2018 10:47:38 AM	SMP8.Example.com	SMP8.Exampl
NS: Web site certificate		Server Auth: NS web site	smp8.example.com...	28d9e6903...		5/10/2038 11:1...	5/15/2018 11:24:33 AM	W2K12-2.Example.com	SMP SMP8.Ex
NS: Web site certificate		Server Auth: NS web site	smp8.example.com...	35a17530ca...		5/9/2038 9:44:3...	5/14/2018 11:49:12 AM	W2K12-2.Example.com	SMP SMP8.Ex
SMP8		Certificate validation	Pre-installed, smp8....	f4b8772d91...	Yes	3/3/2036 11:00:...	4/24/2018 8:19:28 AM	SMP8.Example.com	SMP8.Exampl

Refresh

Details what the certificate is used for

# Certificate Management – Agent UI

Symantec Management Agent (Administrator)

**Certificates** Update Configuration Basic Inventory Diagnostics View Help

**Status: OK** 0 1

Agent Settings | Logs | Software Delivery | Task Status | Software Updates | **Certificates**

Friendly Name	Store	Usages	Sources	Thumbprint	Self-signed	Expiration Date	Installation Date	Issued To	Issued By
CA: SMP SMP8.Example.com Agent CA	Intermediate Certification ...	Server Auth: NS web site...	smp8.example.com...	532246a0bf...		3/19/2036 8:43:...	4/24/2018 8:19:28 AM	W2K12-2.Example.com	SMP SMP8.Ex
CA: SMP SMP8.Example.com Agent CA	Trusted Root Certification ...	Server Auth: NS web site...	smp8.example.com...	8ebf6cc047...	Yes	3/3/2036 11:27:...	4/24/2018 8:19:28 AM	SMP SMP8.Example.com...	SMP SMP8.Ex
CA: SMP SMP8.Example.com Server CA	Trusted Root Certification ...	Server Auth: NS web site...	smp8.example.com...	31a52465f8...	Yes	3/3/2036 11:27:...	4/24/2018 8:19:28 AM	SMP SMP8.Example.com...	SMP SMP8.Ex
CA: SMP SMP8.Example.com Server CA	Intermediate Certification ...	Certificate validation	smp8.example.com	538503c8f7...		3/19/2036 8:43:...	4/24/2018 8:19:28 AM	W2K12-2.Example.com	SMP SMP8.Ex
CEM: Permanent agent certificate	AeXNSClient\Personal	Client Auth: CEM agent	smp8.example.com	518f7be45f...		3/19/2036 9:10:...	5/14/2018 10:47:39 AM	WIN10-1.Example.com	SMP SMP8.Ex
CEM: Permanent gateway certificate	AeXNSClient\Personal	Client Auth: CEM gateway	smp8.example.com	97c4d294e3...		3/19/2036 9:10:...	5/14/2018 10:47:38 AM	WIN10-1.Example.com	SMP SMP8.Ex
NS: CEM web site certificate	Trusted Root Certification ...	Server Auth: CEM web site	smp8.example.com	d4b98464f3...	Yes	5/14/2038 9:01:...	5/14/2018 10:47:38 AM	SMP8.Example.com	SMP8.Exampl
NS: Web site certificate		Server Auth: NS web site	smp8.example.com...	28d9e6903...		5/10/2038 11:1...	5/15/2018 11:24:33 AM	W2K12-2.Example.com	SMP SMP8.Ex
NS: Web site certificate		Server Auth: NS web site	smp8.example.com...	35a17530ca...		5/9/2038 9:44:3...	5/14/2018 11:49:12 AM	W2K12-2.Example.com	SMP SMP8.Ex
SMP8		Certificate validation	Pre-installed, smp8....	f4b8772d91...	Yes	3/3/2036 11:00:...	4/24/2018 8:19:28 AM	SMP8.Example.com	SMP8.Exampl

Copy Details Ctrl+C  
 Copy Thumbprint  
 Copy Serial Number  
**Properties**

Refresh

Easy to use Right Click Options

Certificate

General | Details | Certification Path

**Certificate Information**

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- All issuance policies

Issued to: SMP8.Example.com

Issued by: SMP8.Example.com

Valid from 5/14/2018 to 5/14/2038

Issuer Statement

OK

# Certificate Management – Agent UI

Symantec Management Agent (Administrator)

**Certificates** Update Configuration Basic Inventory Diagnostics View Help

Status: OK

Agent Settings | Logs | Software Delivery | Task Status | Software Updates | Certificates

Friendly Name	Store	Usages	Sources	Thumbprint	Self-signed	Expiration Date	Installation Date	Issued To	Issued By
CA: SMP SMP8.Example.com Agent CA	Intermediate Certification ...	Server Auth: NS web site...	smp8.example.com...	532246a0bf...		3/19/2036 8:43:...	4/24/2018 8:19:28 AM	W2K12-2.Example.com	SMP SMP8.Ex
CA: SMP SMP8.Example.com Agent CA	Trusted Root Certification ...	Server Auth: NS web site...	smp8.example.com...	8ebf6cc047...	Yes	3/3/2036 11:27:...	4/24/2018 8:19:28 AM	SMP SMP8.Example.com...	SMP SMP8.Ex
CA: SMP SMP8.Example.com Server CA	Trusted Root Certification ...	Server Auth: NS web site...	smp8.example.com...	31a52465f8...	Yes	3/3/2036 11:27:...	4/24/2018 8:19:28 AM	SMP SMP8.Example.com...	SMP SMP8.Ex
CA: SMP SMP8.Example.com Server CA	Intermediate Certification ...	Certificate validation	smp8.example.com	538503c8f7...		3/19/2036 8:43:...	4/24/2018 8:19:28 AM	W2K12-2.Example.com	SMP SMP8.Ex
CEM: Permanent agent certificate	AeXNSClient\Personal	Client Auth: CEM agent	smp8.example.com	518f7be45f...		3/19/2036 9:10:...	5/14/2018 10:47:39 AM	WIN10-1.Example.com	SMP SMP8.Ex
CEM: Permanent gateway certificate	AeXNSClient\Personal	Client Auth: CEM gateway	smp8.example.com	97c4d294e3...		3/19/2036 9:10:...	5/14/2018 10:47:38 AM	WIN10-1.Example.com	SMP SMP8.Ex
NS: CEM web site certificate	Trusted Root Certification ...	Server Auth: CEM web site	smp8.example.com	d4b98464f3...	Yes	5/14/2038 9:01:...	5/14/2018 10:47:38 AM	SMP8.Example.com	SMP8.Exampl
NS: Web site certificate		Server Auth: NS web site	smp8.example.com...	28d9e6903...		5/10/2038 11:1...	5/15/2018 11:24:33 AM	W2K12-2.Example.com	SMP SMP8.Ex
NS: Web site certificate		Server Auth: NS web site	smp8.example.com...	35a17530ca...		5/9/2038 9:44:3...	5/14/2018 11:49:12 AM	W2K12-2.Example.com	SMP SMP8.Ex
SMP8		Certificate validation	Pre-installed, smp8....	f4b8772d91...	Yes	3/3/2036 11:00:...	4/24/2018 8:19:28 AM	SMP8.Example.com	SMP8.Exampl

Context menu for selected row:

- Copy Details (Ctrl+C)
- Copy Thumbprint
- Copy Serial Number
- Properties

Refresh button

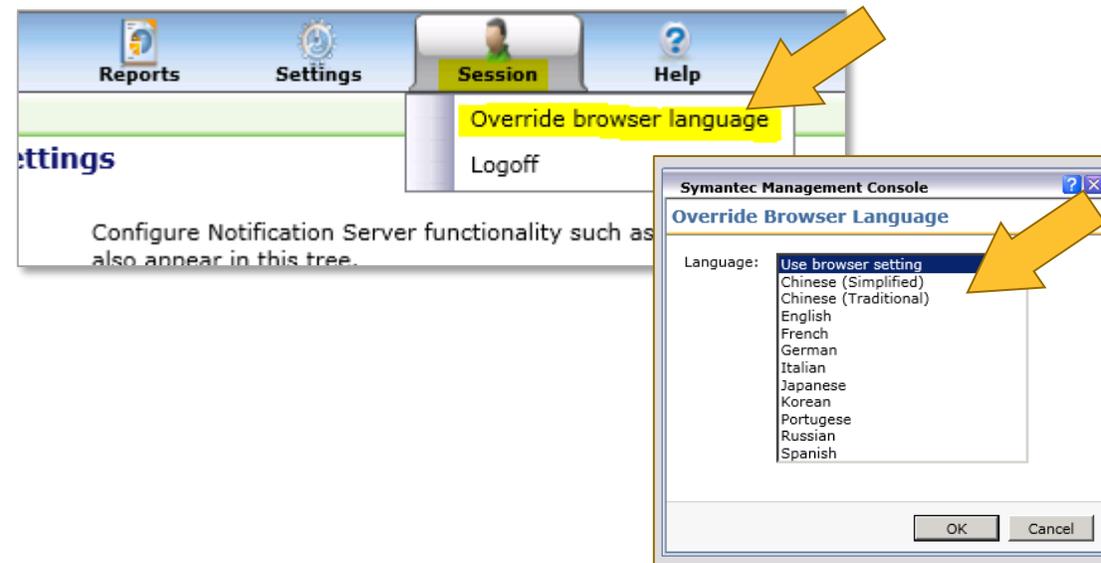
```

File Edit Format View Help
NS: CEM web site certificate
Trusted Root Certification Authorities
Server Auth: CEM web site
smp8.example.com
d4b98464f3c5b363cf1c789b5abe55c1534773eb
Yes
5/14/2038 9:01:03 AM
5/14/2018 10:47:38 AM
SMP8.Example.com
  
```

View is Not updated automatically

## Usability Enhancements

- **Change the Console Language**
  - Overrides the Browser Language
    - Session > Override Browser Language
  - Must have Language packs installed



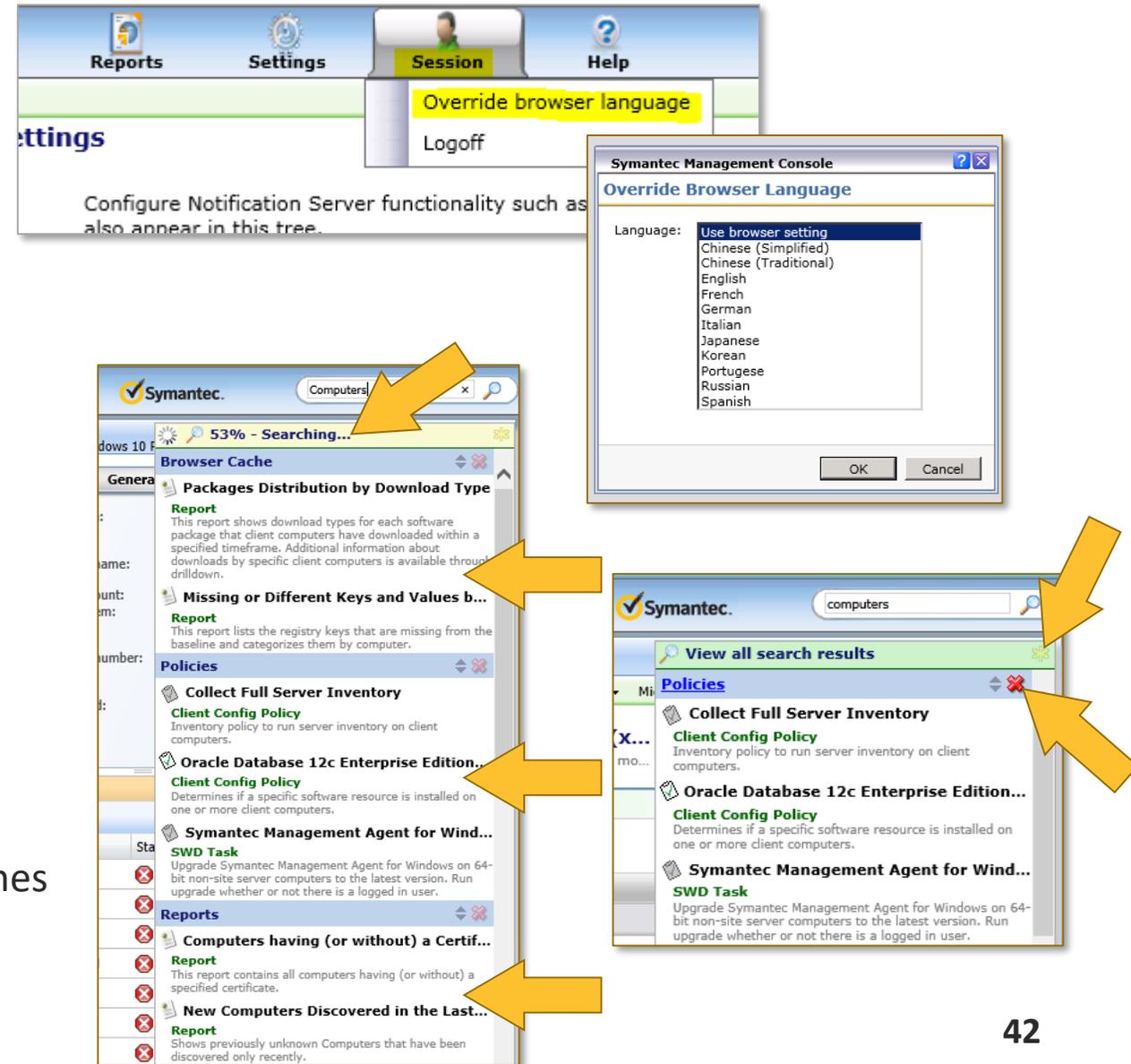
# Usability Enhancements

## ○ Change the Console Language

- Overrides the Browser Language
  - Session > Override Browser Language
- Must have Language packs installed

## ○ Improved Console Search

- Search progress is now displayed in Percent
  - Provides an estimate when it will be finished.
- Search results contain additional information
  - Divided by manageable sections
- Irrelevant search categories can be skipped
  - Improves Search time on large CMDB's
  - Sections are removed from subsequent searches
  - Can be reset to Full Scope if needed

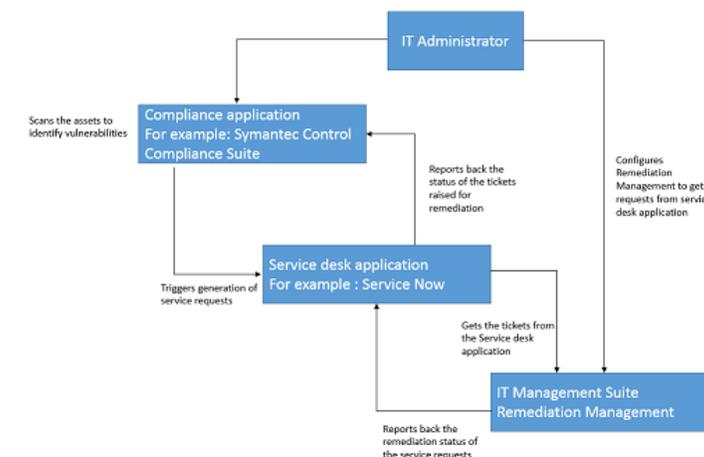
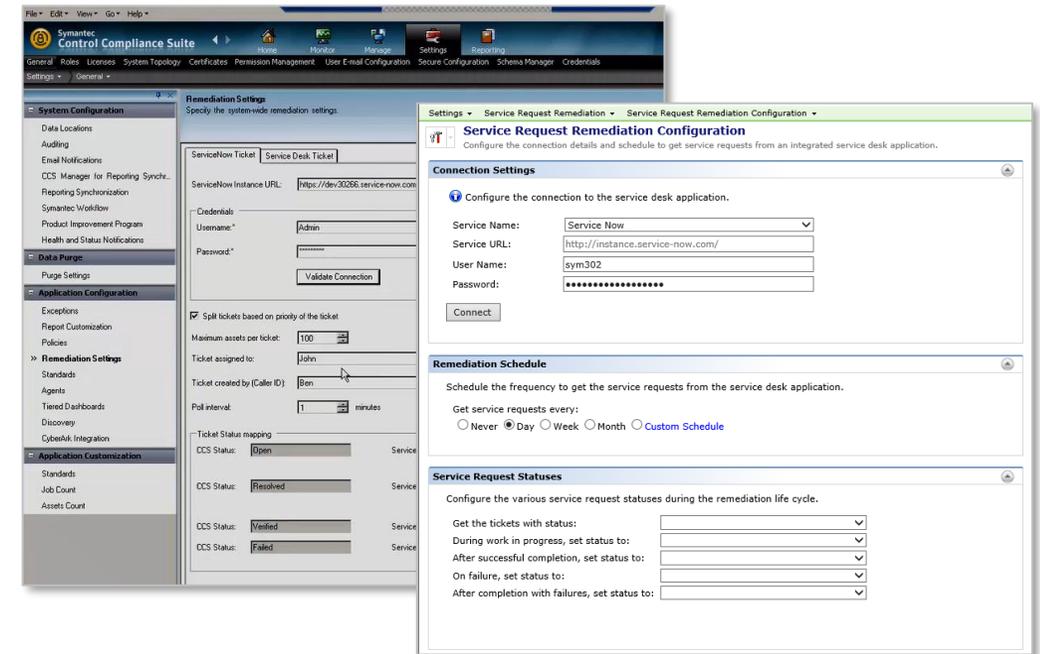


# Platform Integrations



# Control Compliance Suite Integration

- **Service Request Remediation**
  - Automates the remediation of compliance irregularities that are detected in the network
  - Works along with a service desk application and a compliance solution to complete the automated remediation of service requests
  - Integrates CCS and Patch Management Solution into a single flow and takes advantage of a 3rd-party ticketing system
  - Remediation of endpoint vulnerabilities identified by CCS-VM using Patch Management Solution
- For more information see: [DOC9752](#)



# Control Compliance Suite Integration

## CCS

- 1. Select a check:**
- 2. Run compliance scan**

Asset Name	Risk Score	Confidentiality	Integrity	Availability	Ticket ID	Ticket Status	Data Collection Date
CCSDEV\WIN2K12-CC53	7.5	High	High	High			09-02-2017 11:50:37
CCSDEV\WIN2K12-CC51	7.5	High	High	High			09-02-2017 11:50:37
ccsdev\WIN2K12-CC54	7.5	High	High	High			09-02-2017 11:50:37
- 3. Trigger CCS to Auto Log tickets**

Asset Name	Risk Score	Integrity	Availability	Ticket ID	Ticket Status	Data Collection Date
High (3)						
CCSDEV\WIN2K12-CC53	7.5	High	High			2017-11-30:37
CCSDEV\WIN2K12-CC51	7.5	High	High			2017-11-30:37
ccsdev\WIN2K12-CC54	7.5	High	High			08-02-2017 11:50:37

## ServiceNow

**CCS automatically logs tickets for vulnerable Assets**

## ITMS

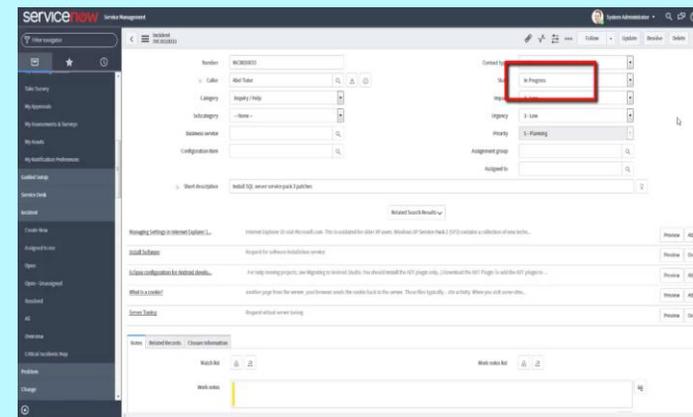
# Control Compliance Suite Integration

CCS

ServiceNow

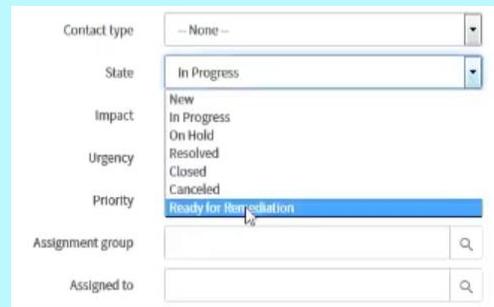
ITMS

4. Ticket is reviewed and approved



Ticket goes through approval flow and is set for remediation

5. Ticket placed in 'Ready for Remediation'



# Control Compliance Suite Integration

## CCS

**8. Automatically verifies compliance**

## ServiceNow

## ITMS

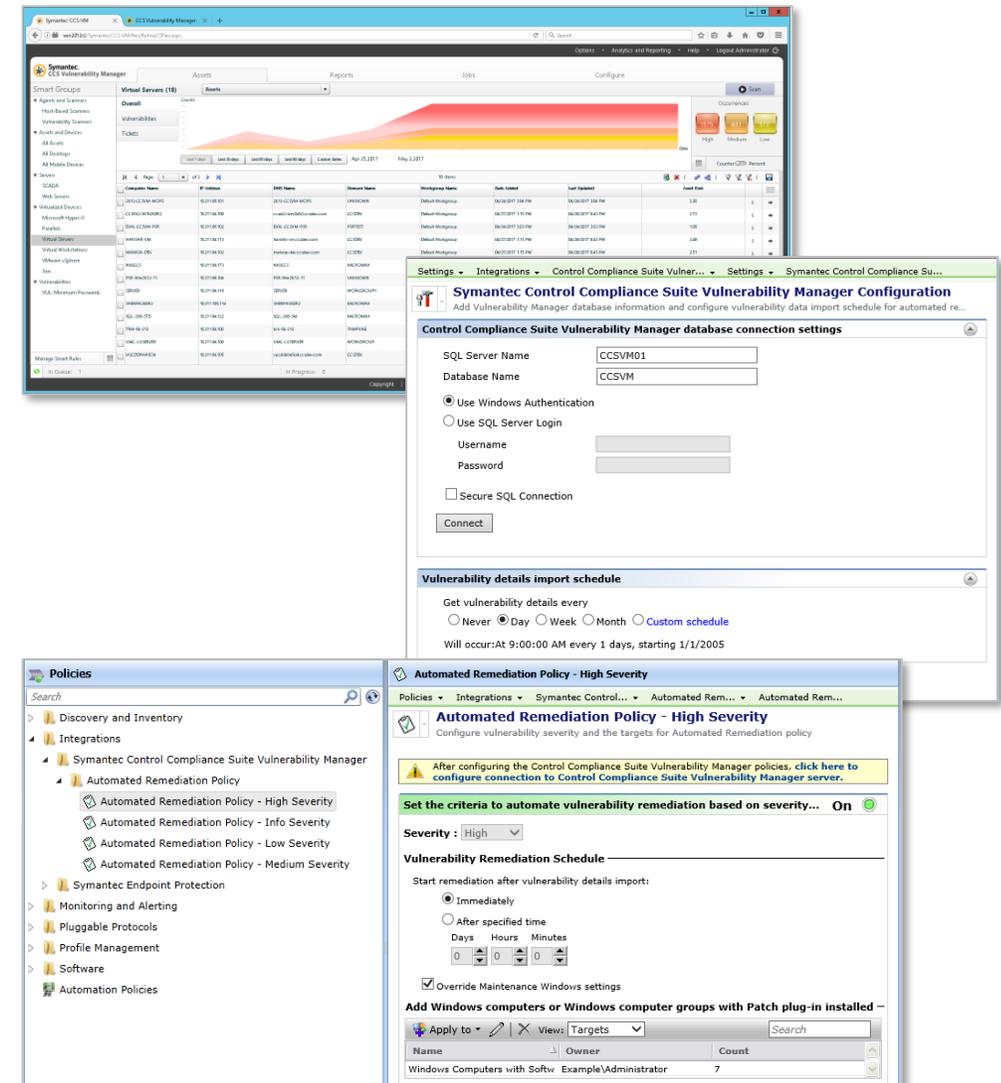
**6. Monitors tickets and executes remediation**

Policy	Computer	Bulletin	Status
INCO010033-06-02-17:14:45:0	KZ-win2k12-CC81	MS16-136	Installed
INCO010033-06-02-17:14:45:0	KZ-win2k12-CC83	MS16-136	Installed
INCO010033-06-02-17:14:45:0	KZ-win2k12-CC84	MS16-136	Installed

**7. Updates ticket status**

# Control Compliance Suite VM Integration

- **Automated Vulnerability Remediation**
  - Scans your environment for vulnerabilities and remediate Windows client computers automatically
    - **CCS Vulnerability Manager** provides an end-to-end discovery and vulnerability assessment
      - Determines Severity: High, Medium, Low, or Info.
    - **Patch Management Solution** leverages the vulnerability data provided by CCS-VM
      - Remediates vulnerabilities in your environment using the Automated Remediation Policies.
  - **Automated Vulnerability Remediation** provides four predefined Policies for different severity levels.
    - Apply these policies to different target computers
    - Create custom Automated Remediation Policies according to your organizations' requirements
- **MORE FROM ROB BARKER TODAY!**

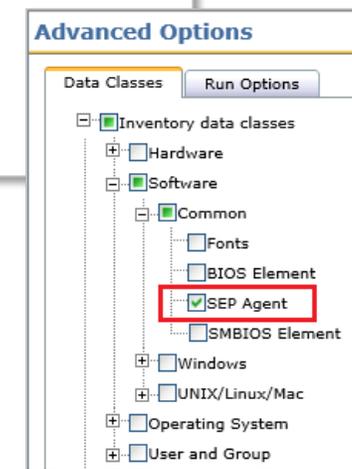


# Symantec Endpoint Protection Integration

## ○ SEP Health Information

- **Extended SEP Agent Health Information**
  - To better evaluate the SEP Health status
- In order for this data to be collected:
  - Inventory Plug-in should be installed and Inventory Solution licenses applied.
  - 'SEP Agent' checkbox should be selected
    - Can be accessed from **Advanced Options of Gather Inventory Task** or **Collect Full/Delta Inventory policy**

- SEP Agent Service Name
- Sep Agent Service State
- SEP Agent Service startup type
- Latest virus definition date
- Latest virus definition revision
- Last successful scan date/time
- AV running state
- Firewall running state **(Win Only)**
- Device infected or not
- SEPM Current Group
- SEPM Preferred Group



# SEP Agent Health Flipbooks

**hit-pc-000** 192.168.1.48 Domain: hitdom MAC: AA-BB-CC-00-00-30 User: hitdom\hitman OS: Microsoft Windows XP

SEP Agent Health

**Healthy**

- Infection Status:  Not infected
- Antivirus Status:  Enabled
- Firewall Status:  Enabled
- Last Antivirus Scan:  Thursday, March 29, 2018 3:58:13 PM
- SEP Agent Service State:  Running
- Virus Definitions Date:  Thursday, March 29, 2018
- Virus Definitions Revision: 20
- SEP Agent Version: 14.0.3876.1100
- SEP Manager Server: 10.36.101.21

Computer Details Flipbook

All Computers

SEP Agent Health

Overall SEP Agent Health

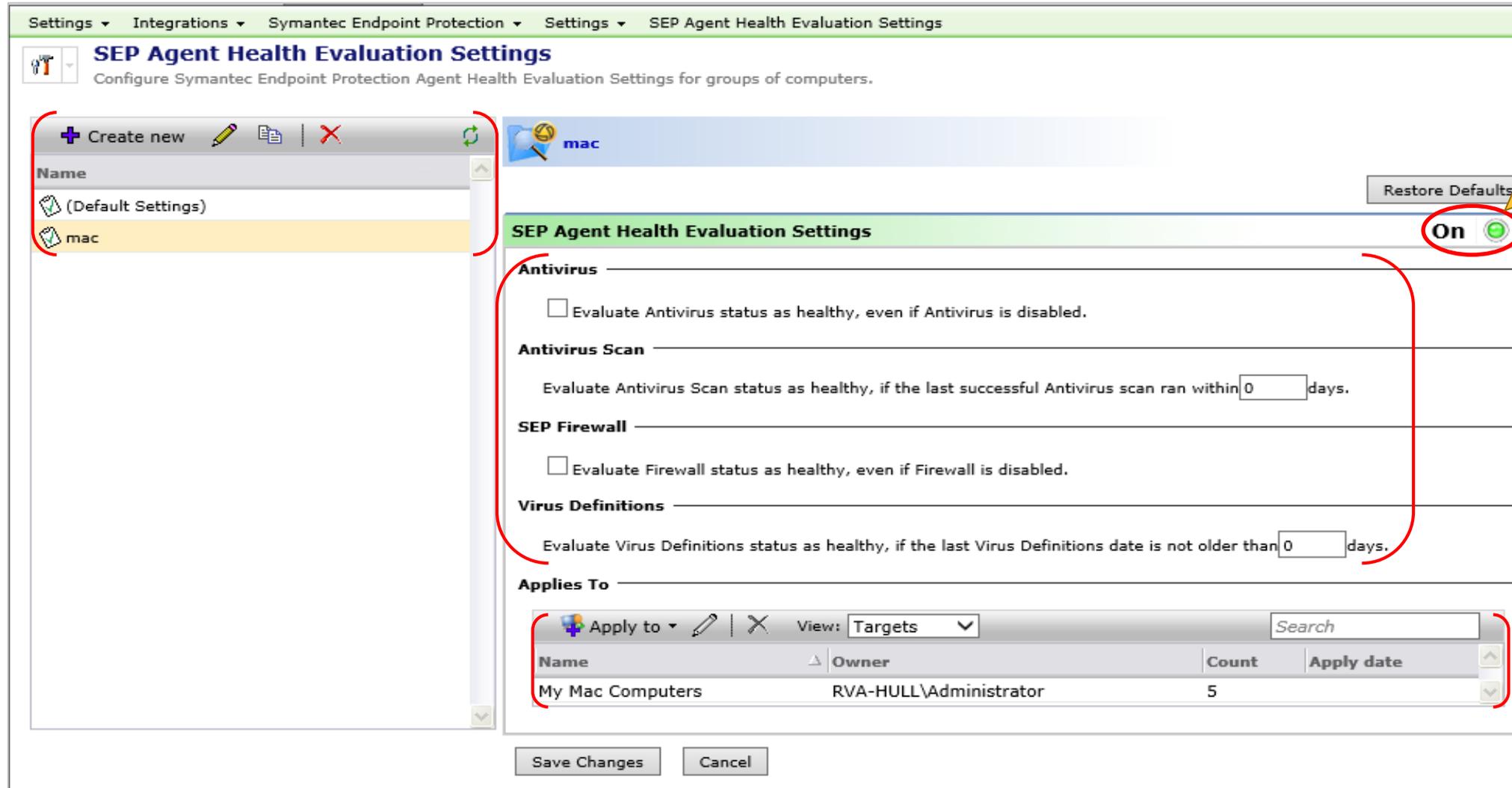
Health By Category

SEP Agent Service State:	84%
Infection Status:	59%
Antivirus Status:	61%
Firewall Status:	59%
Last Antivirus Scan:	58%
Virus Definitions Date:	82%

Healthy  
 Needs attention  
 Untracked

Computer Summary Flipbook

# SEP Agent Health Evaluation Settings



The screenshot shows the 'SEP Agent Health Evaluation Settings' configuration page. The breadcrumb trail at the top reads: Settings > Integrations > Symantec Endpoint Protection > Settings > SEP Agent Health Evaluation Settings. The page title is 'SEP Agent Health Evaluation Settings' with a subtitle 'Configure Symantec Endpoint Protection Agent Health Evaluation Settings for groups of computers.'

On the left, a sidebar lists settings for '(Default Settings)' and 'mac'. The 'mac' setting is selected and highlighted in yellow. A red circle highlights the 'Create new' button and the sidebar list.

The main content area shows the configuration for the 'mac' group. At the top right, there is a 'Restore Defaults' button and a status indicator 'On' with a green checkmark icon, which is circled in red and pointed to by a yellow arrow. Below this, several sections are visible, each with a red circle around its controls:

- Antivirus**: Includes a checkbox 'Evaluate Antivirus status as healthy, even if Antivirus is disabled.'
- Antivirus Scan**: Includes a text field 'Evaluate Antivirus Scan status as healthy, if the last successful Antivirus scan ran within 0 days.'
- SEP Firewall**: Includes a checkbox 'Evaluate Firewall status as healthy, even if Firewall is disabled.'
- Virus Definitions**: Includes a text field 'Evaluate Virus Definitions status as healthy, if the last Virus Definitions date is not older than 0 days.'

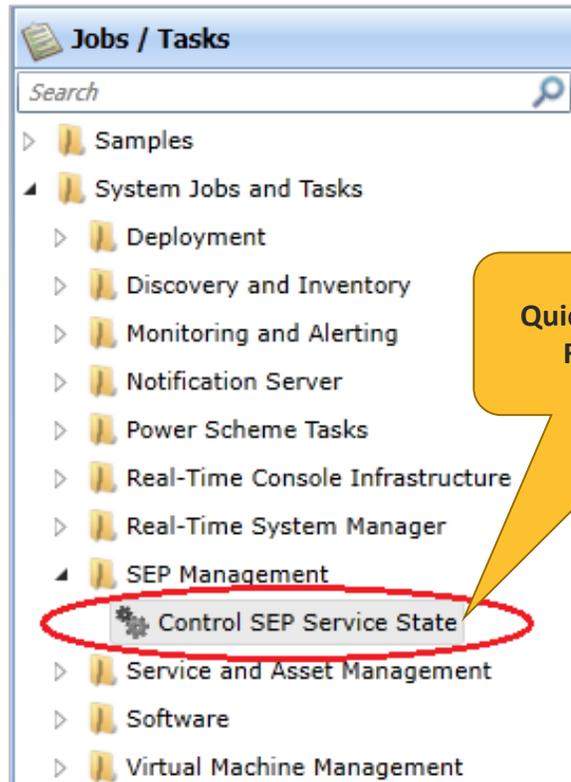
At the bottom, the 'Applies To' section features a table with columns for Name, Owner, Count, and Apply date. A red circle highlights the 'Apply to' button and the table.

Name	Owner	Count	Apply date
My Mac Computers	RVA-HULL\Administrator	5	

At the bottom of the page are 'Save Changes' and 'Cancel' buttons.

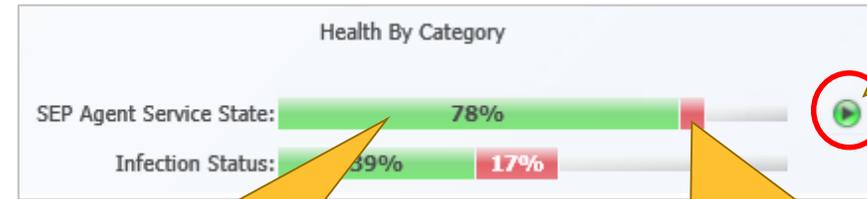
# Control SEP Service State Task

- Remediation action in case the SEP Agent service is in a stopped state



Quickly create a Job/Task to Restart the SEP Agent

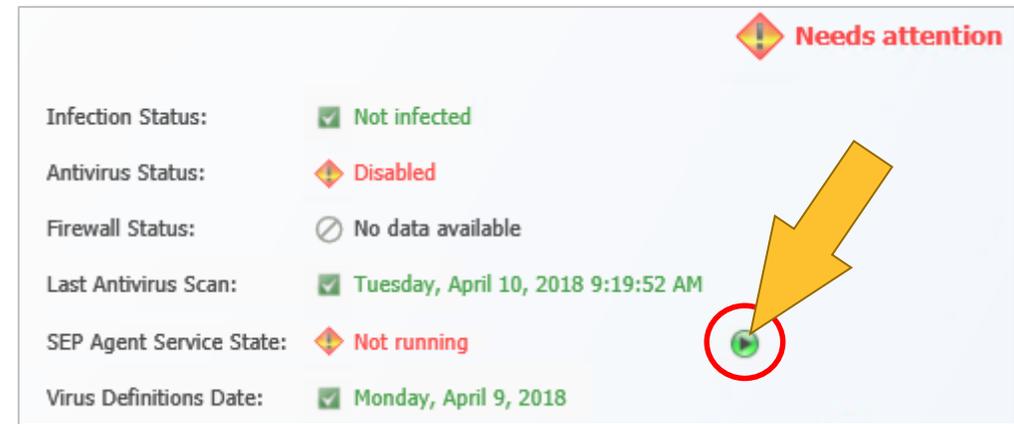
## Computer Summary flipbook



Number/Percentage of SEP Agents *installed* and *running*

Number/Percentage of SEP Agents *installed* and *NOT running*

## Computer Details flipbook



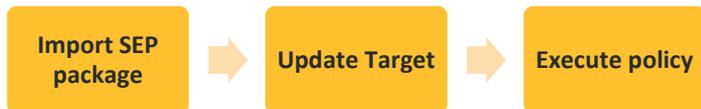
# SEP Agent Install/Upgrade

- **Symantec Endpoint Protection Agent Delivery**

- Easily create policies to install/upgrade SEP Agents
- **Import the SEP Installation Package**
  - Pulls metadata from the SEP Agent Package
  - Creates an entry in the Software Library
  - Packages appear in the console for distribution
  - Automatically created base Policy and Target

- **Distribute SEP Installation Package**

- Select the SEP Agent Entry
- Adjust Target for distribution
- Enable the policy to deploy the SEP Agent



The image displays two screenshots from the Symantec Management Console. The top screenshot shows the 'Symantec Endpoint Protection Agent Delivery' page with an 'Import installation package' button highlighted by a red arrow. The bottom screenshot shows the 'Symantec Endpoint Protection Agent Delivery' page with a red box around the 'SEP Delivery' configuration details. A yellow arrow points to the 'Symantec Endpoint Protection 14.0.3752.10' entries in the software library, and another yellow arrow points to the 'Applied to' target configuration.

**Symantec Management Console**

**Symantec Endpoint Protection Agent Delivery**

All Symantec Endpoint Protection delivery policies

**SEP Delivery**

Import a Symantec Endpoint Protection installation package to create and configure a new SEP Agent delivery policy.

Import installation package

**Symantec Endpoint Protection Agent Delivery**

All Symantec Endpoint Protection delivery policies

**SEP Delivery - Once at 00:00, Repeat daily at 02:00 (Agent Time)**

Package name: FeatureSet1 x86 14.0.3752.1000.exe

Company: Symantec

Version: 14.0.3752.1000

**Applied to - 0 resources**

Add computer groups or user groups to which the policy rules will be applied and enforced.

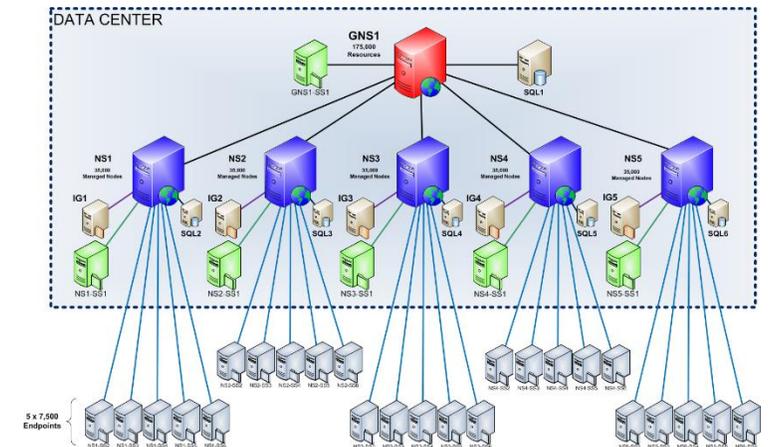
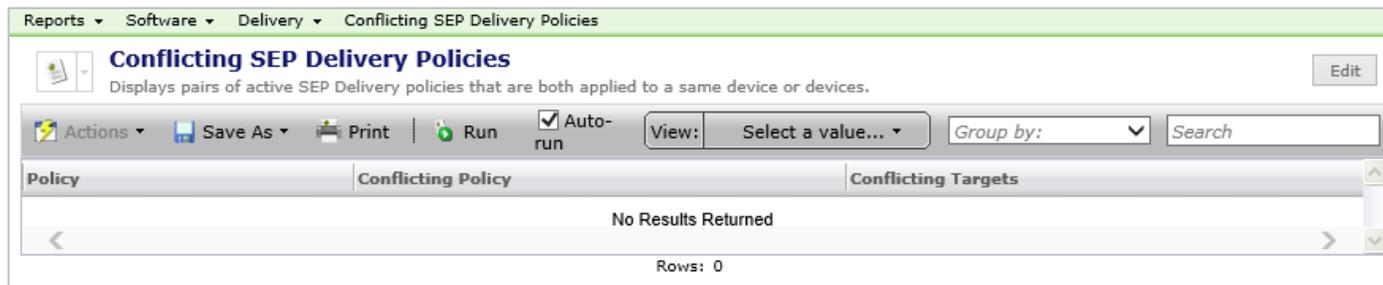
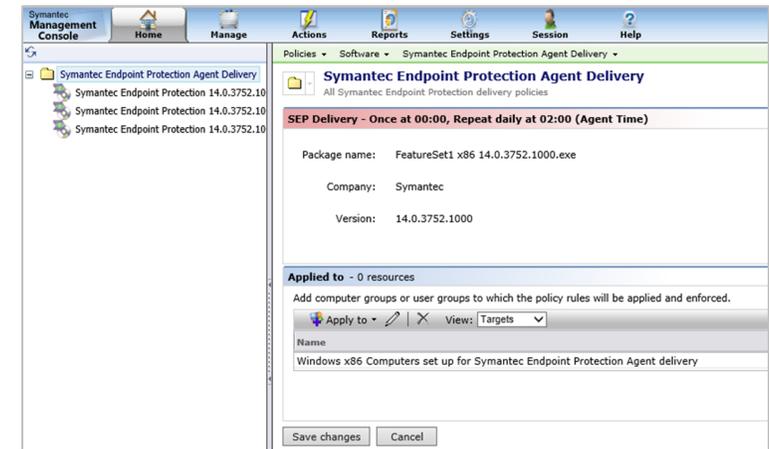
Apply to [icon] [icon] [icon] View: Targets

Name
Windows x86 Computers set up for Symantec Endpoint Protection Agent delivery

Save changes Cancel

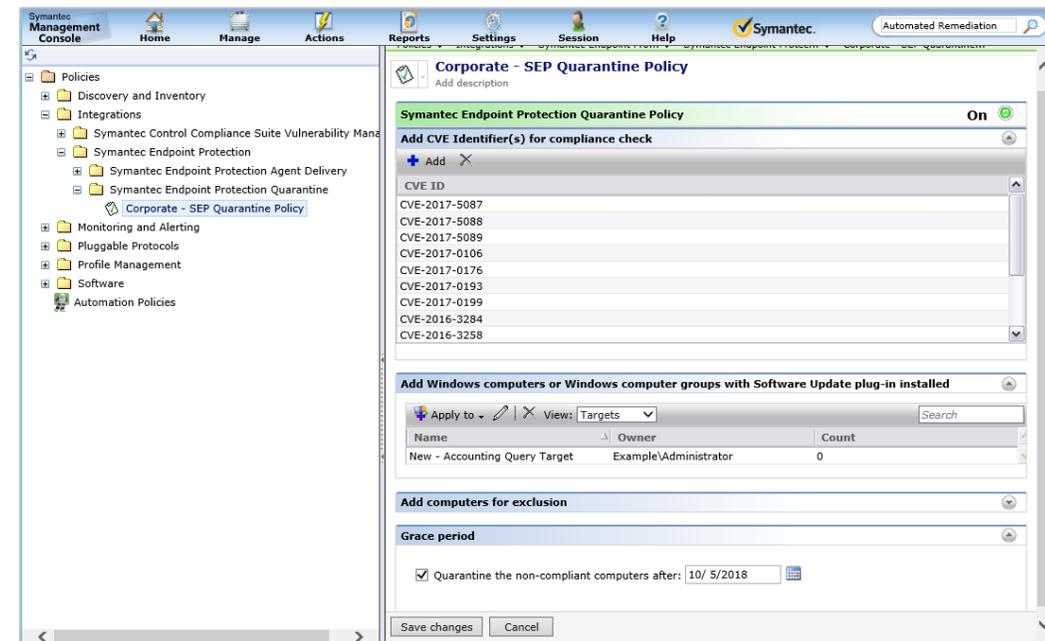
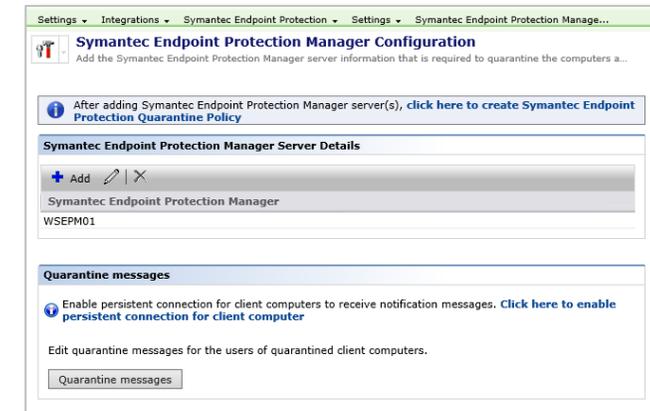
# SEP Agent Install/Upgrade

- **Advantages of ITMS SEP Agent Distribution:**
  - CeM feature enables the SEP agent to be installed/upgraded on devices on the WAN
  - P2P and checkpoint recovery significantly reduces the bandwidth used on delivering the SEP Agent
  - Infrastructure is highly scalable and distributed.
  - Out of the box reports that can be used to monitor the progress of a rollout to install/upgrade the SEP agent



# Symantec Endpoint Protection Integration

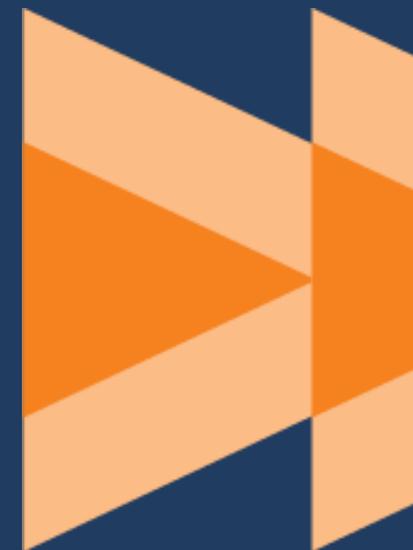
- **SEP Quarantine Enforcement**
  - Defines software updates that are **Mandatory** then **Enforces** quarantine from the network
  - **Once Configured...**
    - The **System Assessment Scan** results and **SEP Quarantine policy** settings are compared
    - ITMS sends information about quarantined computers to the SEP Manager
    - The SEP Manager Quarantines the computers
    - If the updates get applied during quarantine or the administrator excludes the endpoint from the policy, the quarantine will be reversed.
- **MORE FROM ROB BARKER LATER TODAY!**



END OF PART ONE



# Solution Enhancements

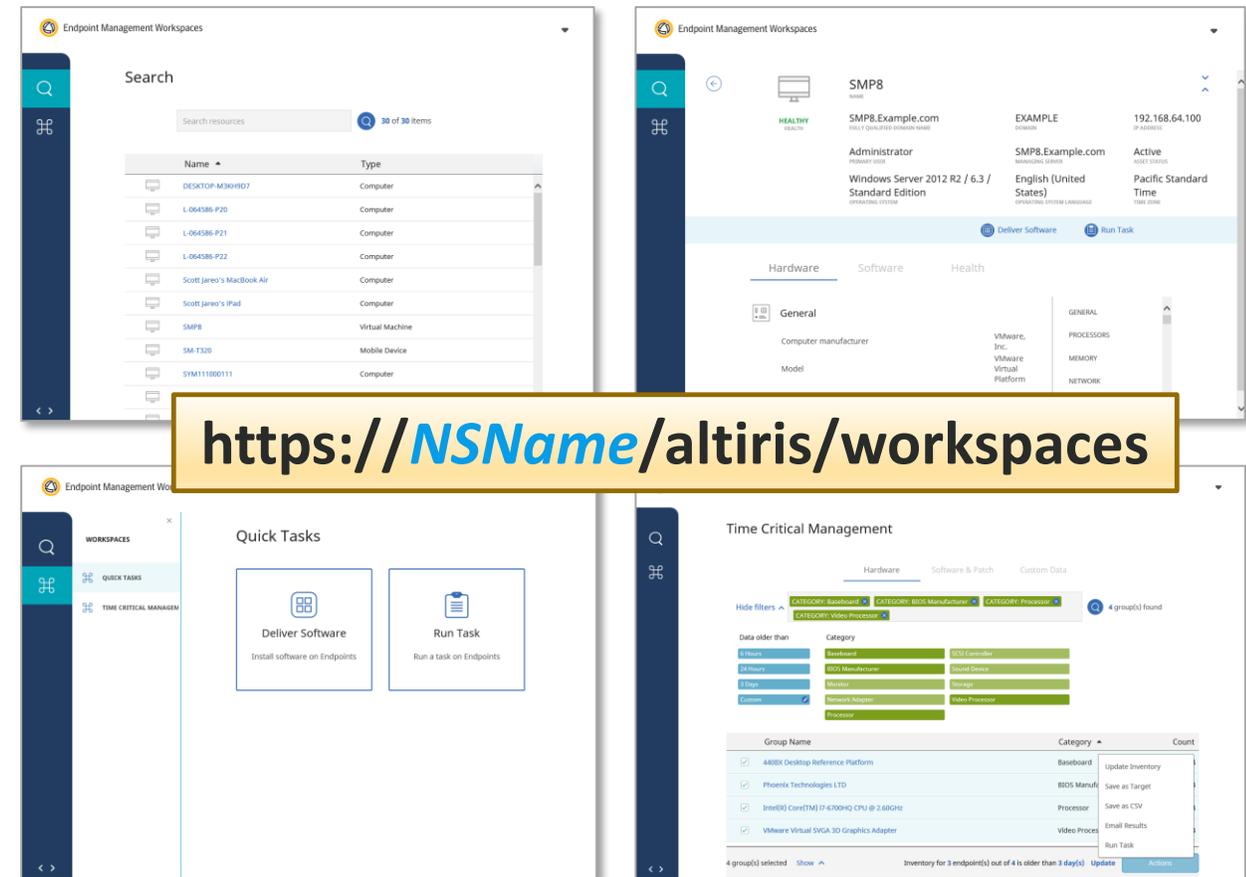


# Endpoint Management Workspaces

- **Web based console with dedicated workspaces and widgets**

- Speeds up day-to-day endpoint management jobs
- Depending on the permissions granted, you can perform the following tasks:
  - View inventory details for a selected endpoint.
  - Run tasks on one or more endpoints.
  - Deliver and install software on one or more endpoints.
  - Gather inventory in real time and perform Time Critical Management (TCM) tasks.

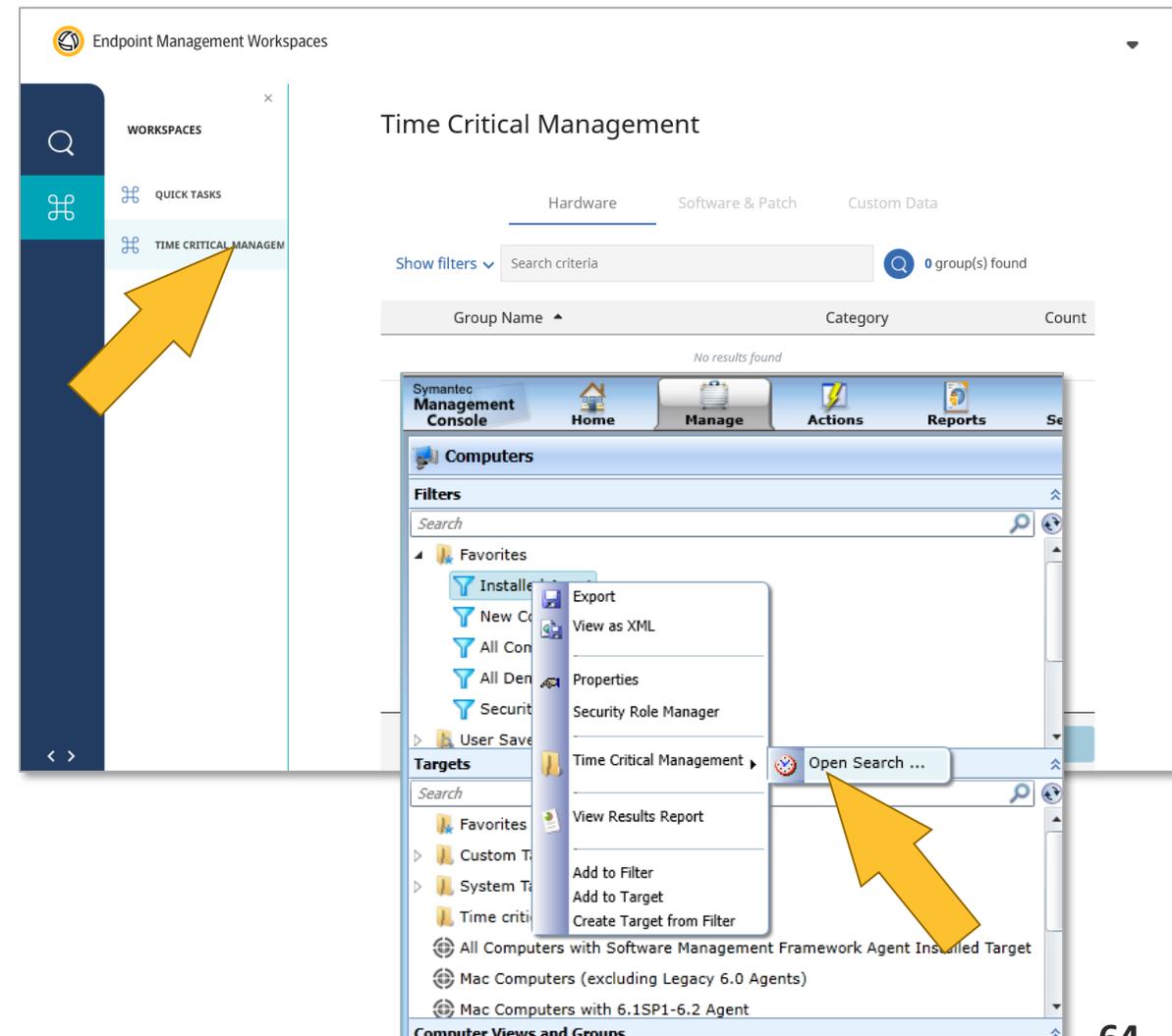
- **MORE FROM ROB LATER...**



# Endpoint Management Workspaces

## ○ Time Critical Management

- Gathers inventory in real time to perform immediate hardware and software state analysis
- Persistent Connection must be implemented
- Use the Time Critical Management portal or in the Symantec Management Console
  - <https://NSName/altiris/workspaces>
  - In the Right Click options of the Computer View
- Functions:
  - Verify that the inventory data is up-to-date.
  - Run tasks in real time.
  - Immediately push policies to the endpoints.



# Inventory Solution

## ○ Application Metering for MacOS

- Mac OS X 10.9 and above
- New data class: ***Product Monthly Summary***
- ***Resource Manger: View > Inventory***
- ***Software View: Product Summary Flipbook***

The screenshot displays the Symantec software management interface for 'Open Office.org 4'. It includes a configuration window for identifying inventory, a 'Policy Details' window showing general information and XML, and a 'Software Usage' window with a donut chart and a table of installed computers.

**Software Product Configuration:**

- Name: Open Office.org 4
- Company: OpenOffice.org
- Version: 4
- Category: Desktop Application

**Policy Details:**

- ID: {AD921BBB-9D65-4B0A-8A63-973D219E6561}
- Name: Application Metering Product-based Usage Tracking Policy
- Version: 8.1.5088.0
- Hash: 58E0A6A58613158ADF0ADD0190837708
- Applies to user: Everyone (host-based)
- Applies to class IDs: Altris.ProcessMonitor

**Policy XML:**

```
<Application>
  <MonitorItems>
    <product guid="48f13c18-aa4d-4a89-a4ed-877da9854718">
      <rule>
        <brackets op="Or">
          <openoffice-/exp>
          <e>openoffice-/exp>
        >4.</exp>
      </rule>
    </product>
  </MonitorItems>
</Application>
```

**Software Usage (2 installations in total):**

Usage Status	Percentage	Count
Unused	0%	0
Used	50%	1
No tracking data	50%	1

**Computers with software installed:**

Computer	User	Software Usage	Last Used	Install Date
Chere01	COV/PavelC	No tracking...		1/29/2019 12:00:00 AM
mac1011	mac1011.local\lus	Used	5/31/2019 1:47:10 PM	5/31/2019 12:07:03 PM

# Inventory Solution

## ○ Collect Time-Critical Inventory Policy

### ○ What it Collects:

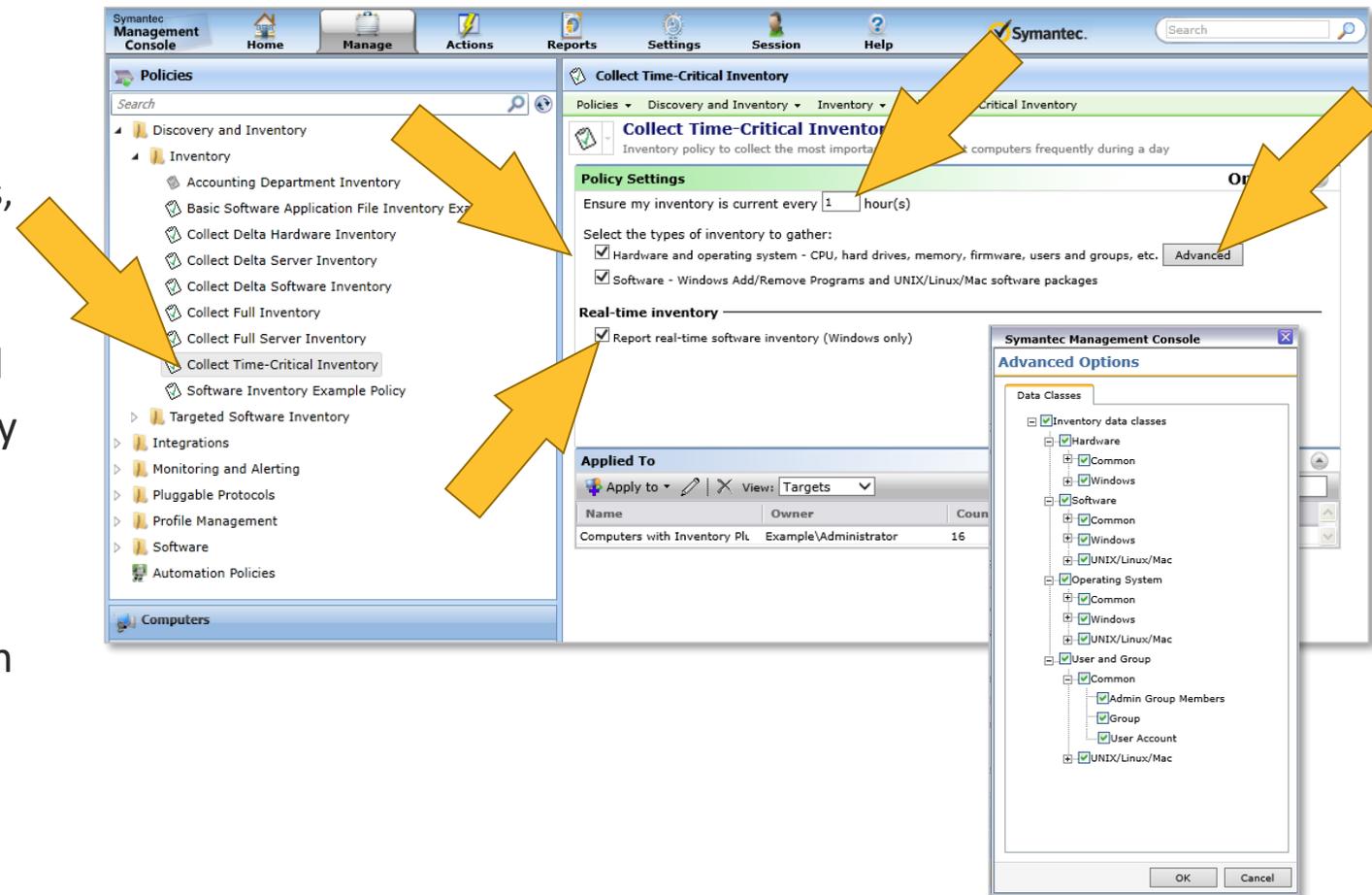
- Hardware & Software Data Classes
  - User selectable data classes
  - **Except** Data that is changing (Services, Ports, Plug & Play...)

### ○ When it Collects

- May be triggered by a defined interval
- Software Inventory can be triggered by a detected change in software (Windows only)

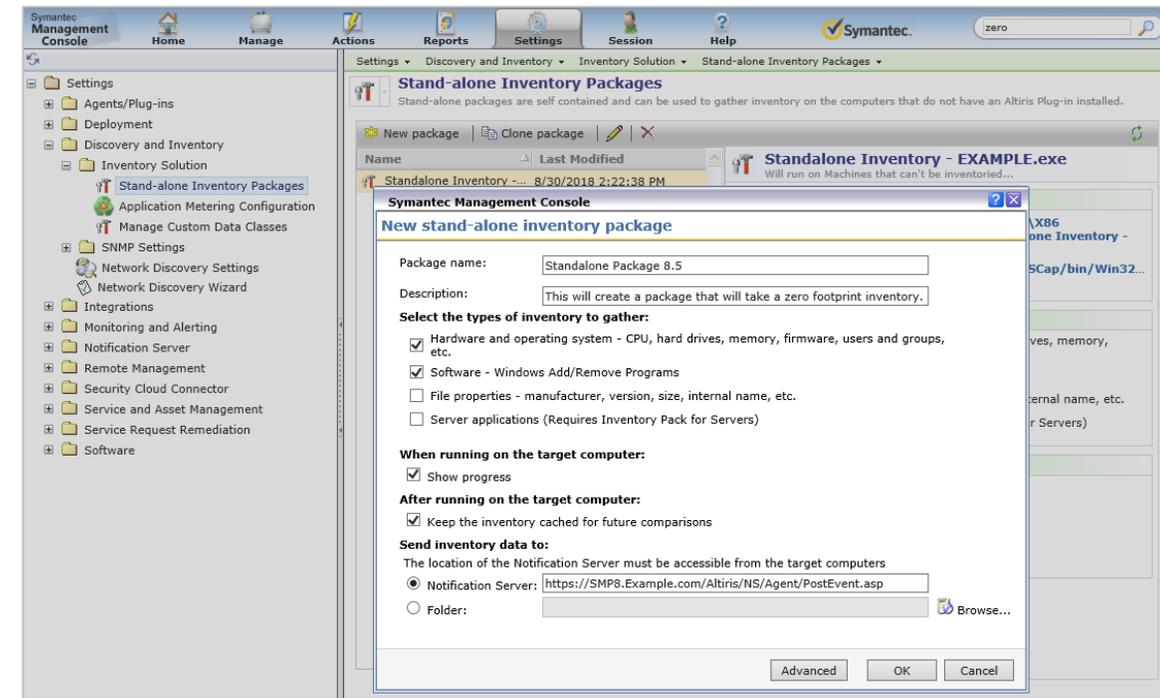
### ○ What it Reports:

- Collected Data reported since last scan
- Date/Time is recorded for each data class



# Inventory Solution

- **Zero footprint Standalone Inventory**
  - Reworked in order to use another technology which does not require DLL registration.
  - May be executed on managed client without impact of an installed SMA.
    - May also be useful for troubleshooting
  - May be executed on earlier environments (7.6, 8.0, 8.1) to collect inventory using the latest codebase.



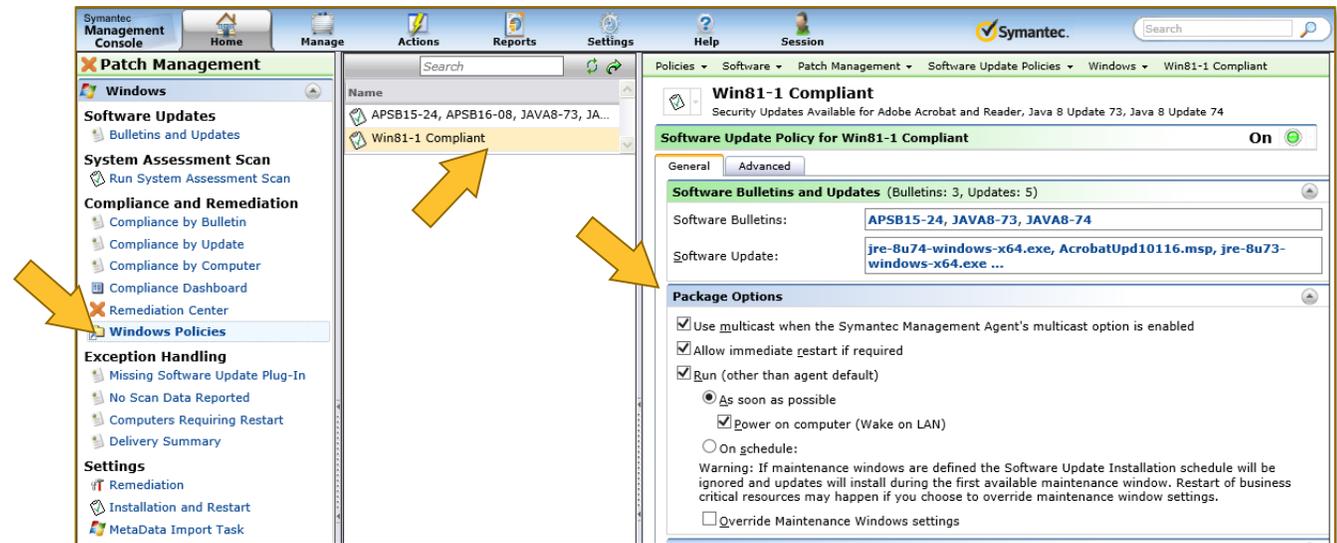
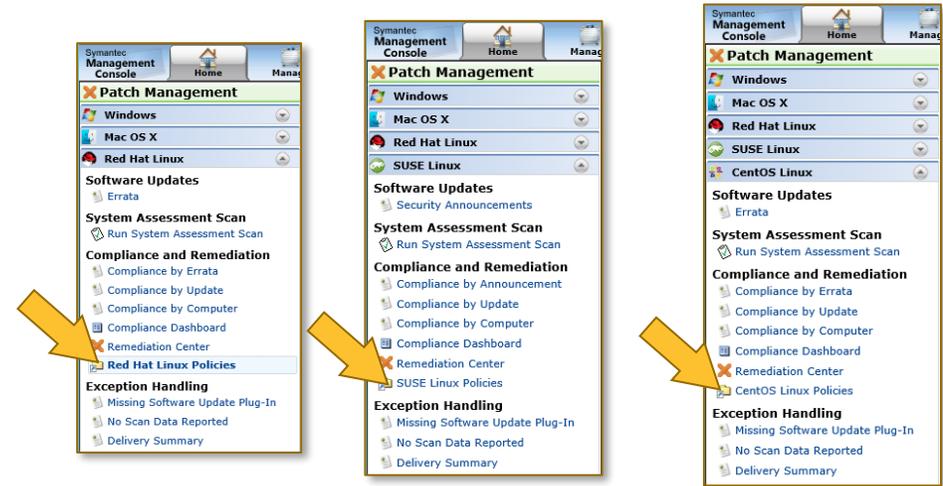
# Inventory Solution

- **Detection of new Windows application types**
  - Added support of **Windows Store Applications**
    - Windows 8, Windows 10
    - New detection method “AppX Scanner” (Source = 128) is shown in software summary report
  - Added support of **AppV Applications**
    - Windows 10
    - New detection method “AppV Scanner” (Source = 256) is shown in software summary report

Installed Software									
Product Name	Manufacturer	Version	Install Date	Type	Detection Me... $\Delta$	Virtualized (Y/...	File Associatio...	Metering (Y/N)	Software Porta...
Microsoft Visual C++ 2008 Redistributable - ...	Microsoft Corpora...	9.0.30729.4148	Oct 19 2017 12:...	Software Compo...	Add Remove And...	N	Y	N	N
Symantec Endpoint Protection 14.2.770.000...	Symantec Corpor...	14.2.770.0000	Sep 1 2018 12:0...	Software Compo...	Add Remove And...	N	Y	N	N
VMware Tools 10.1.10.6082533 English x64	VMware, Inc.	10.1.10.6082533	Mar 27 2018 12:...	Software Compo...	Add Remove And...	N	Y	N	N
NSFinCalculatorsXP 1.0.0.0	Nightshift Compu...	1.0.0.0	Sep 6 2018 12:0...	Software Release	Add Remove, Inv...	N	Y	N	N
Far Manager 3 English	Eugene Roshal &...	3.0.5000	Sep 15 2017 12:...	Software Compo...	AppV Scanner	Y	Y	N	N
InputApp 1000.17746.1000.0	Microsoft	1000.17746.100...		Software Compo...	AppX Scanner	N	Y	N	N
king.com.CandyCrushSodaSaga 1.118.400.0	king.com	1.118.400.0		Software Compo...	AppX Scanner	N	Y	N	N
Microsoft.AAD.BrokerPlugin 1000.17746.10...	Microsoft	1000.17746.100...		Software Compo...	AppX Scanner	N	Y	N	N
Microsoft.AccountsControl 10.0.17746.1000	Microsoft	10.0.17746.1000		Software Compo...	AppX Scanner	N	Y	N	N

# Patch Management Solution

- Patch Policy pages available on the Patch Management home page
  - Windows Policies
  - SUSE Linux Policies
  - Red Hat Linux Policies
  - CentOS Linux Policies
- Can select a policy from the list
  - View the details of the policy
  - Edit its settings if necessary



# Patch Management Solution

## ○ Microsoft Office 365 Channels Support

- Separate bulletin is available for each date when Microsoft Office 365 updates are released for a specific channel

- *MSYY-MM-0365* - < May 2018.
- *MSYY-MM-0365-CHANNEL\_NAME* - > May 2018

## ○ Metadata for PM for Windows will contain four O365 Products

1. Ensure that you have imported the latest patch management metadata for Windows
2. Ensure that they are selected in Vendors and SW **OR** Deselect “Microsoft Office Click to Run 2016” and select the appropriate Channel(s)

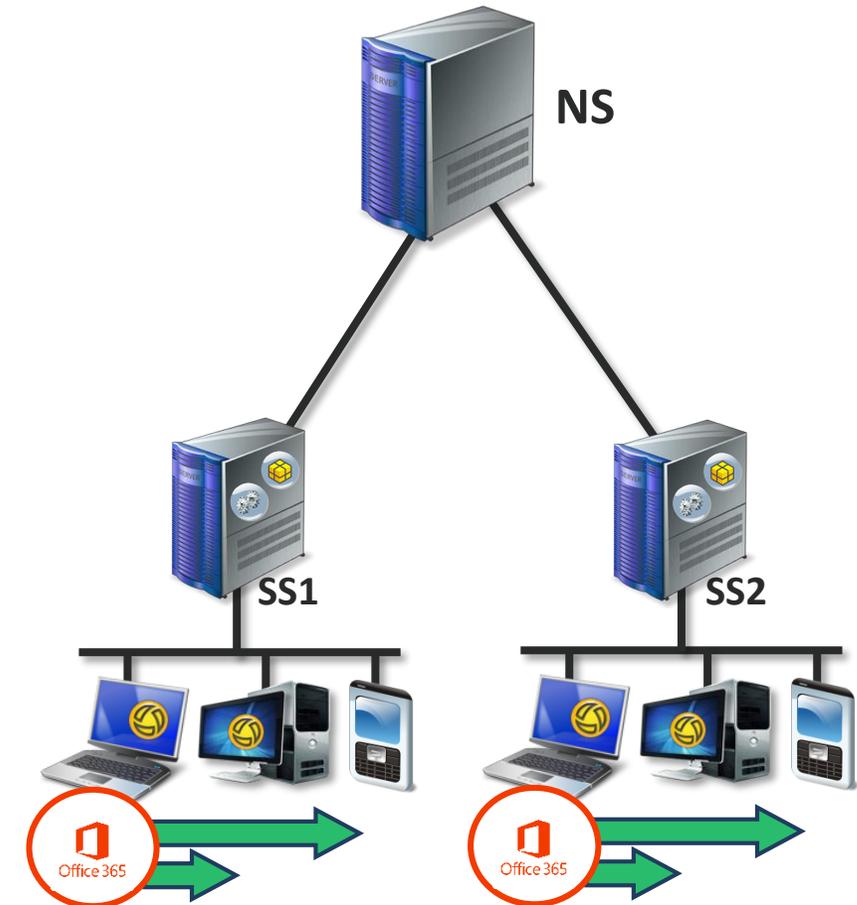
- For more information, see the following knowledge base article: [DOC9673](#)

The screenshot displays the Symantec Patch Management interface. At the top, a software bulletin for 'MS18-04-0365-SEMI-ANNUAL' (Office 365: April 10, 2018) is shown. Below it, the 'Import Patch Data for Windows' dialog box is open, showing 'Patch Management Import Settings' with 'Incremental import' and 'Delete previously downloaded data...' checked. The 'Vendors and Software' section shows a tree view with 'Microsoft' selected. A second dialog box is also open, showing the same settings and a list of products under 'Microsoft', including 'Microsoft Office Click to Run 2016' with various channels selected. A 'Warning' message states 'some nodes might be filtered out and not visible now.' Buttons for 'Save changes' and 'Cancel' are visible at the bottom of the dialog boxes.

# Patch Management Solution

## ○ P2P Support for Office 365 Updates

- Able to download O365 Updates from their peers using incremental differencing
  - Rather than each device downloading incremental differences from package servers or the NS
- Reduces WAN traffic
- Decreases update times

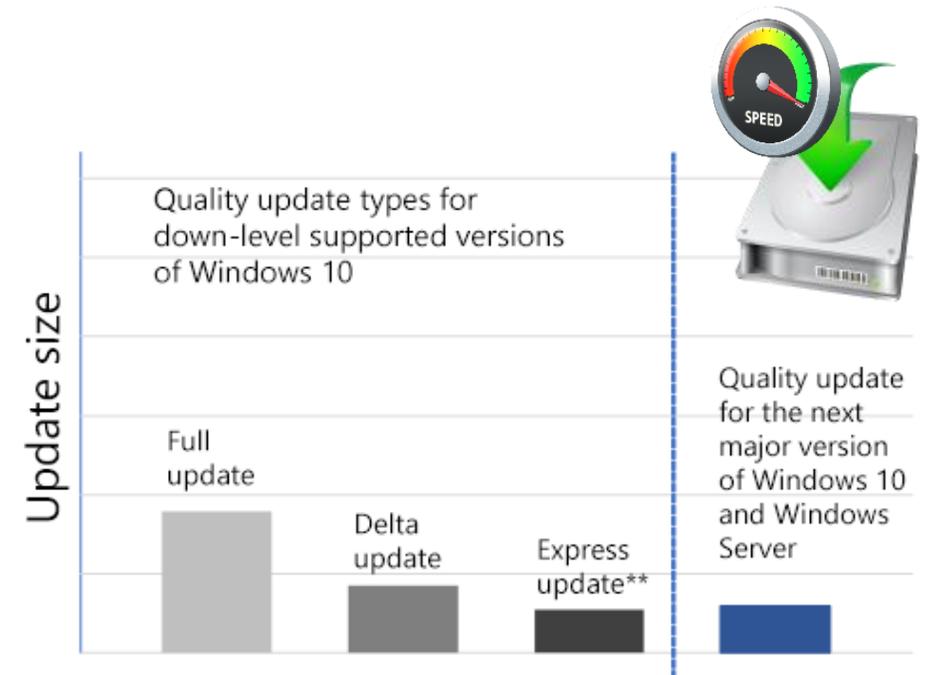


## Patch Management Solution

- **Natively Supports Microsoft “PSFX Updates”**
  - Windows 10 Redstone 5 – version 1809 and greater
- **Provides the benefit of reduced delivery time**
  - Delivers only delta changes to the latest Redstone release
  - Can utilize the Symantec P2P technology
    - Further reduces the download time
  - Quality updates also improve the overall install time
    - Compared to Express updates

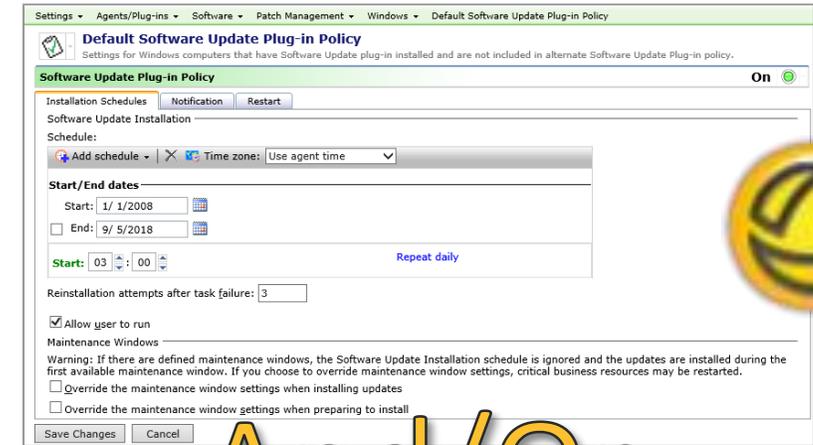
### Notes:

- “PSFX Update” is a work-in-progress name of the feature from MSFT
- Not available for Feature Updates (Express Updates are still the only traffic optimization option)
- Not available for Windows 10 versions earlier than 1809
  - (Microsoft still plans to build Express Updates for these versions, with delta updates discontinued in Feb 2019)

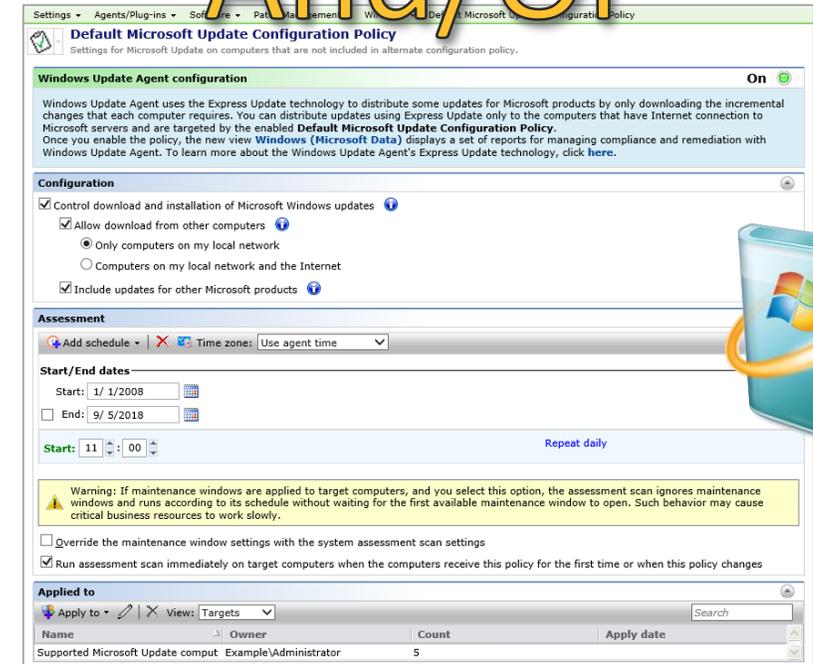


# Patch Management Solution

- Windows Update Service Integration
  - Choose PMS, WUS, or both methods
  - **Microsoft Express Update** technology can be used to distribute incremental changes for each client
    - Reduces bandwidth use and Latency in SW Updates
  - Distribute updates to clients that meet the following requirements:
    - Computers are ready for Patch Management
    - Computers can access Microsoft servers
    - Computers are targeted by the enabled **Default Microsoft Configuration Policy (DMCP)**.

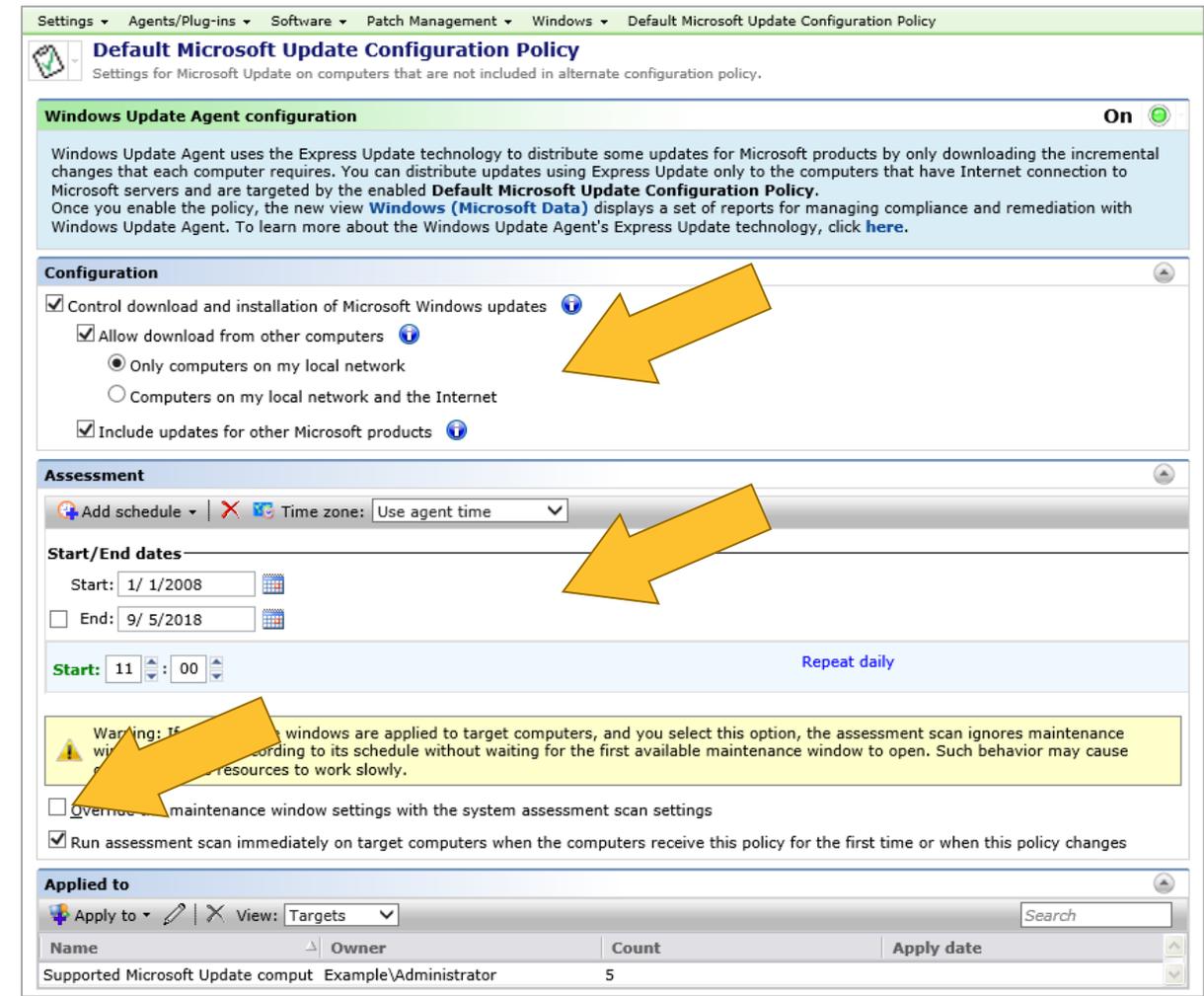


And/Or



# Patch Management Solution

- **Default Microsoft Configuration Policy**
  - Enables Windows update Assessment scan
  - Defines how often you want the scan to run
  - Can override maintenance window settings
  - Configures the Download/Install of Updates
    - Download from local/internet computers
      - Uses Delivery Optimization functionality from the Windows Update Agent
    - Can include other MS Updates
- **Assessment Scan:**
  - Inventories your managed computers for the software updates that they require
  - Targets for the software update policies are created automatically
  - Delta or Full Scans can be run
  - Also sends NSE's with Recency information



**Settings** ▾ Agents/Plug-ins ▾ Software ▾ Patch Management ▾ Windows ▾ Default Microsoft Update Configuration Policy

**Default Microsoft Update Configuration Policy**  
Settings for Microsoft Update on computers that are not included in alternate configuration policy.

**Windows Update Agent configuration** On 

Windows Update Agent uses the Express Update technology to distribute some updates for Microsoft products by only downloading the incremental changes that each computer requires. You can distribute updates using Express Update only to the computers that have Internet connection to Microsoft servers and are targeted by the enabled **Default Microsoft Update Configuration Policy**. Once you enable the policy, the new view **Windows (Microsoft Data)** displays a set of reports for managing compliance and remediation with Windows Update Agent. To learn more about the Windows Update Agent's Express Update technology, click [here](#).

**Configuration**

Control download and installation of Microsoft Windows updates 

Allow download from other computers 

Only computers on my local network

Computers on my local network and the Internet

Include updates for other Microsoft products 

**Assessment**

 Add schedule ▾   Time zone: Use agent time ▾

**Start/End dates**

Start: 1/ 1/2008 

End: 9/ 5/2018 

Start: 11 : 00 Repeat daily

 Warning: If maintenance windows are applied to target computers, and you select this option, the assessment scan ignores maintenance windows according to its schedule without waiting for the first available maintenance window to open. Such behavior may cause system resources to work slowly.

Override maintenance window settings with the system assessment scan settings

Run assessment scan immediately on target computers when the computers receive this policy for the first time or when this policy changes

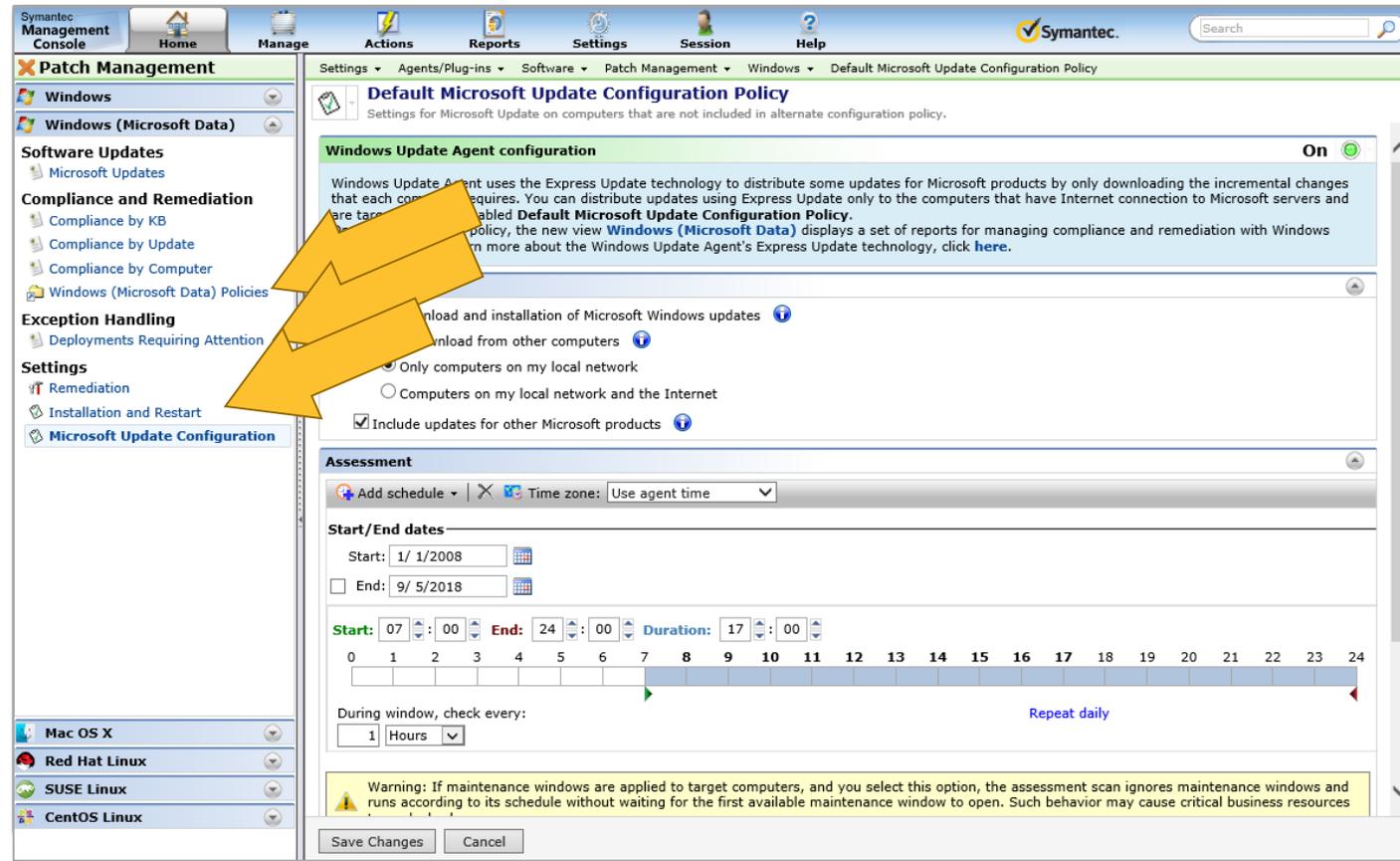
**Applied to**

 Apply to ▾   View: Targets ▾

Name	Owner	Count	Apply date
Supported Microsoft Update comput	Example\Administrator	5	

# Patch Management Solution

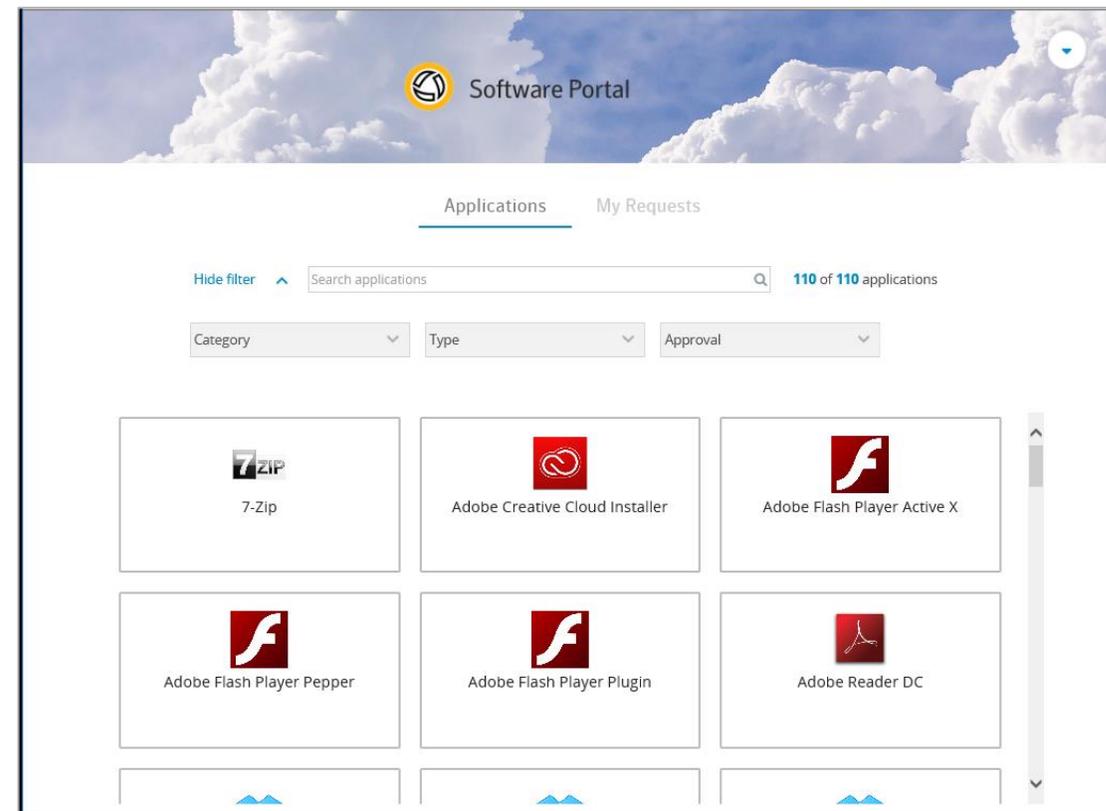
- Windows (Microsoft Data) Portal
  - Reports for managing compliance and remediation using the Windows Update Agent
    - Microsoft Updates
    - Compliance by KB
    - Compliance by Update
    - Compliance by Computer
  - Link to all Windows Update Policies
  - Exception Handling Report
  - Settings:
    - Remediation (Common)
    - Installation and Restart (Common)
    - **MS Update Configuration Policy**



# Software Management Solution

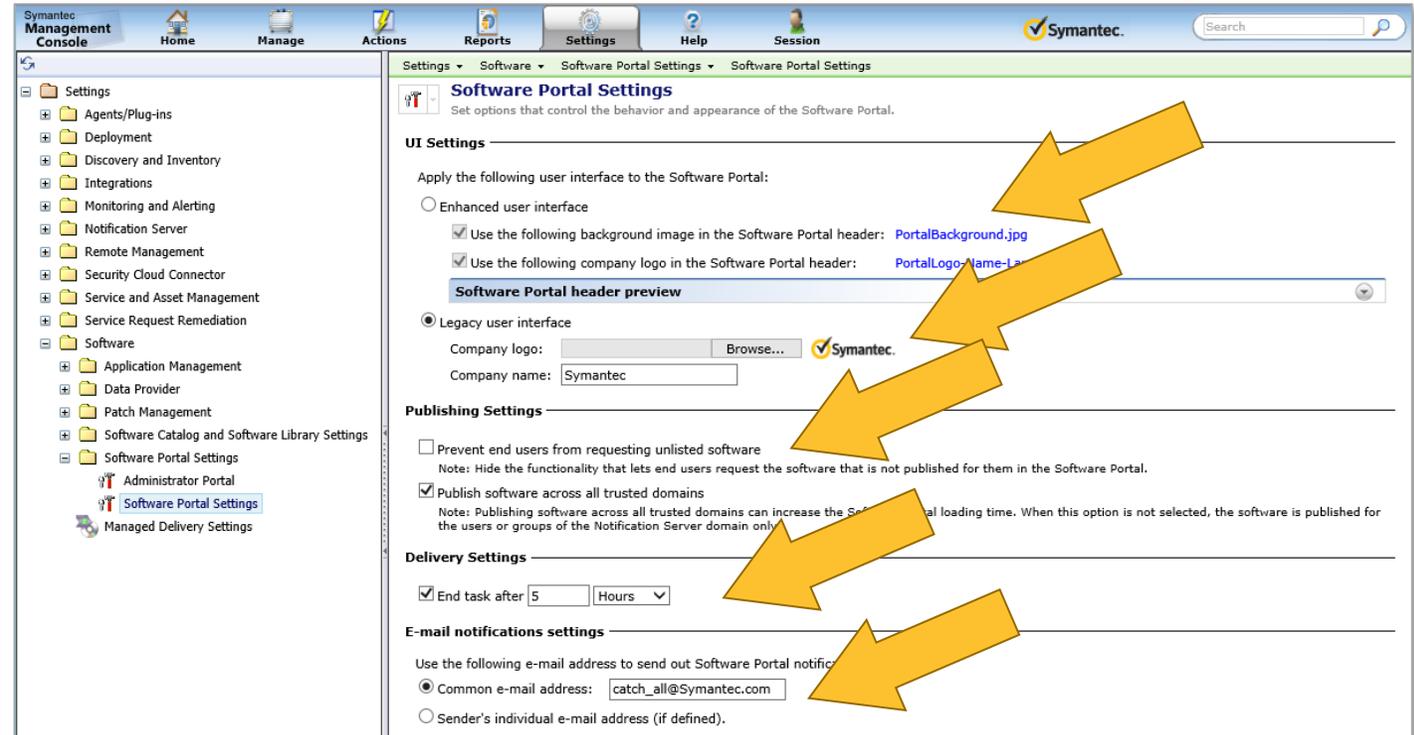
Available in ITMS 8.1 RU4+

- **Redeveloped Software Portal**
  - Submits requests and installs software through a Web-based interface with little or no administrator involvement
  - Reduces help desk calls and simplifies the process of SW Delivery
  - Uses predefined software information that automates delivery
  - Pre-Approved or Manager Approved Software Requests
  - Installed as part of the Symantec Management Agent
- SEE: [DOC9610](#) for SW Portal Guide



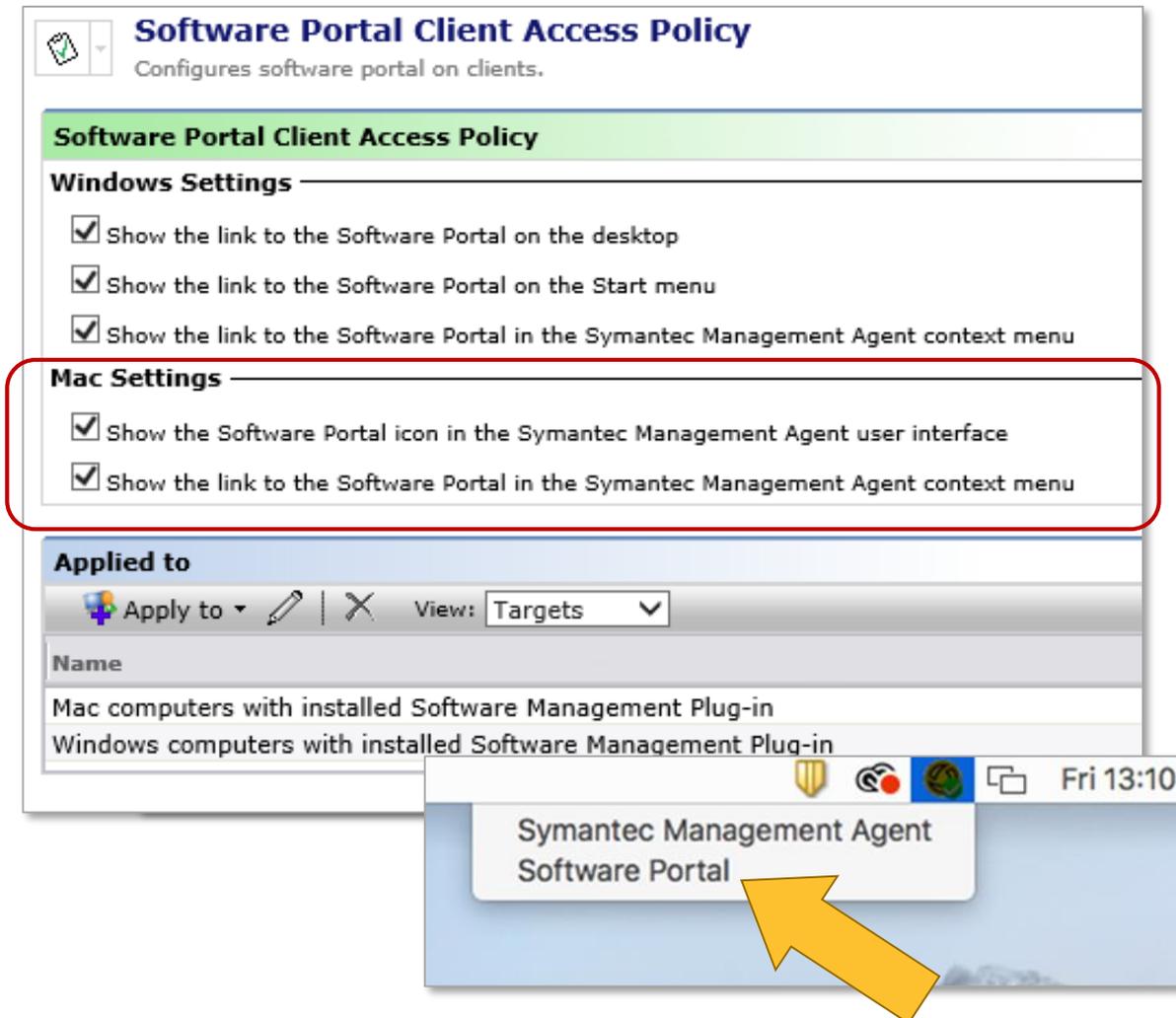
# Software Management Solution

- **Software Portal Settings**
  - Enhanced or Legacy Interface
  - Publishing
    - Prevent all Unlisted SW Requests
    - Publish across all Domains
  - Cancel delivery after n hours
  - Email notifications to common or user specific addresses



# Software Management Solution

- Software Portal Agent Settings
  - **SW Portal was inconvenient in MacOS**
  - **SW Portal Client Access Settings for Mac**
    - Can be set and applied to Mac machines
    - Will respect the new Mac-specific options
    - Policy was renamed to reflect its purpose more precisely
    - The Software Portal can be hidden or shown as specified in the policy
    - A Context menu item was also added



**Software Portal Client Access Policy**  
Configures software portal on clients.

**Software Portal Client Access Policy**

**Windows Settings**

- Show the link to the Software Portal on the desktop
- Show the link to the Software Portal on the Start menu
- Show the link to the Software Portal in the Symantec Management Agent context menu

**Mac Settings**

- Show the Software Portal icon in the Symantec Management Agent user interface
- Show the link to the Software Portal in the Symantec Management Agent context menu

**Applied to**

Apply to | X View: Targets

Name

- Mac computers with installed Software Management Plug-in
- Windows computers with installed Software Management Plug-in

Symantec Management Agent  
Software Portal

# Software Management Solution

## ○ Software Portal User Enhancements

○ *Legacy SW Portal showed all applications regardless of OS Type...*

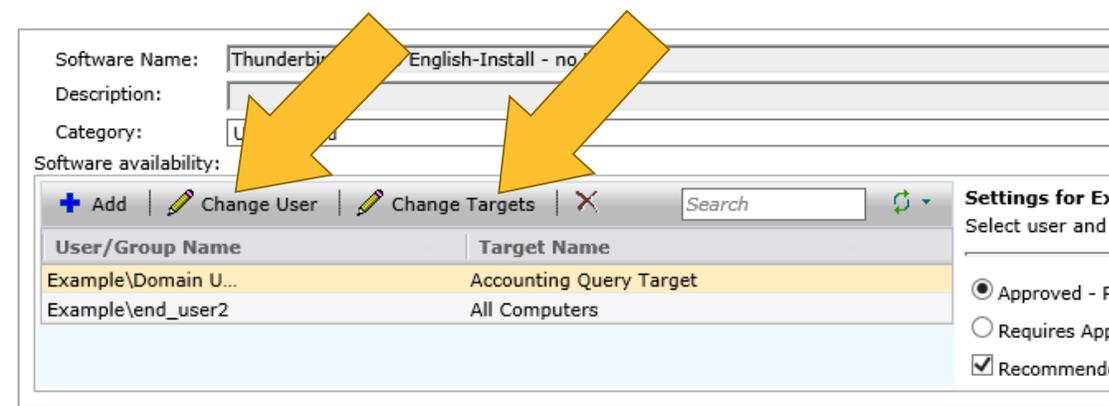
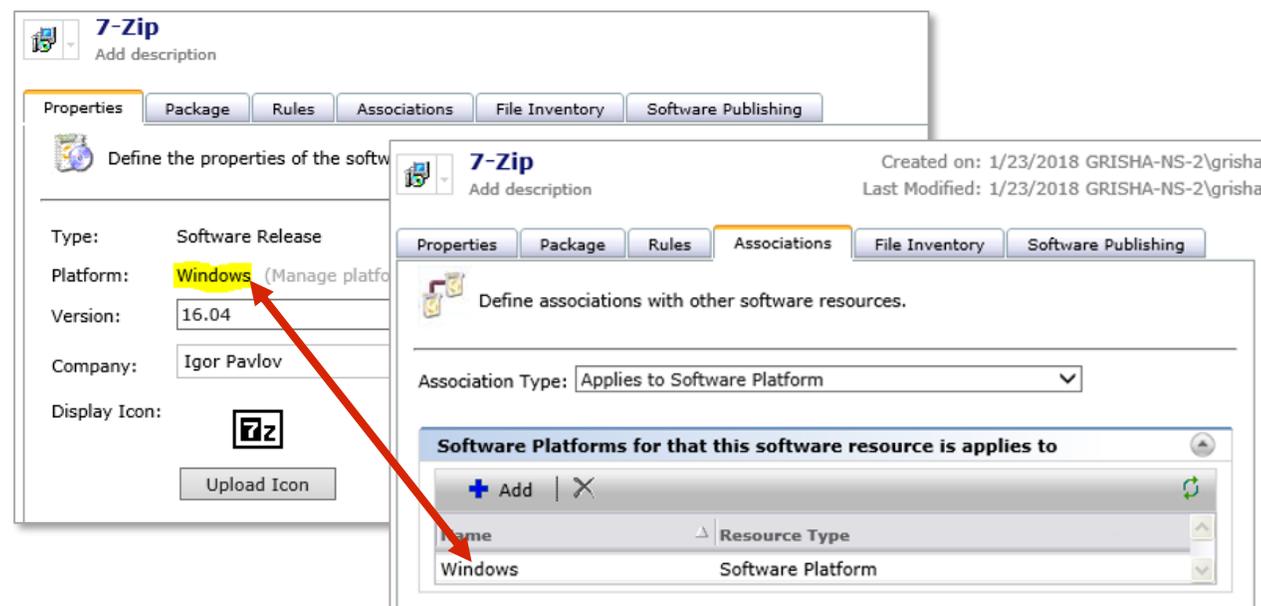
○ **Only Applications compatible with the requesting OS are now displayed**

- Solved by adding filtering “Applies to Software Platform” Association
- Filter works for all applications published
  - If at least one association is defined, the application will be shown.
  - If no associations exist, it is shown in the portal opened on any device.

○ These Associations are defined automatically during software component import

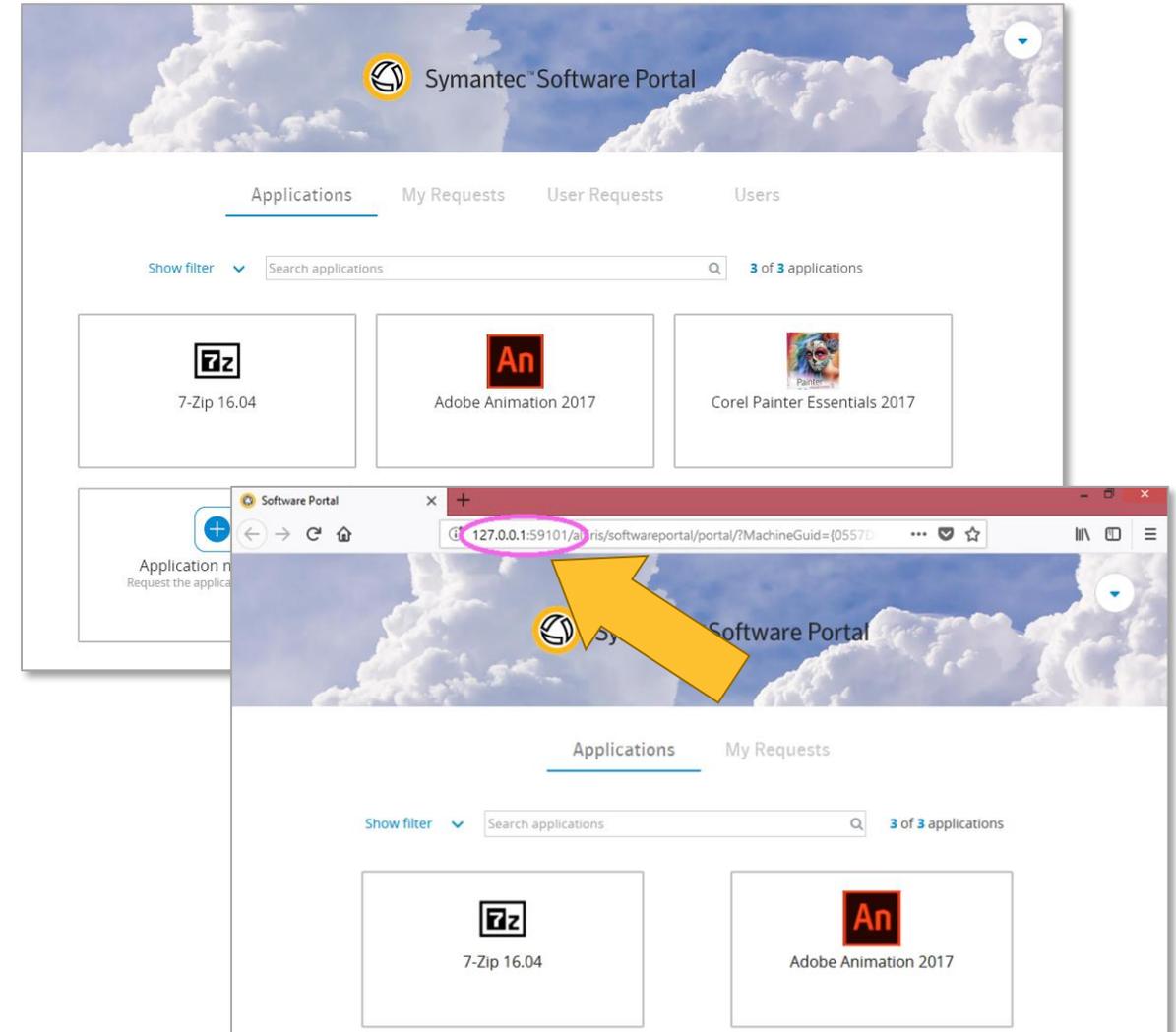
○ **Software can be published to groups of devices or combinations of users/devices**

- Prevents multiple device Installs from users



# Software Management Solution

- **Software Portal User Enhancements**
  - Users can open the Software Portal on **Cloud-enabled *Windows or Mac*** computers
  - SMA Implements a local Proxy Server
  - Browser Redirection in CeM Mode
  - Experience is the same!



# Software Management Solution

## ○ Software Portal Enhancements

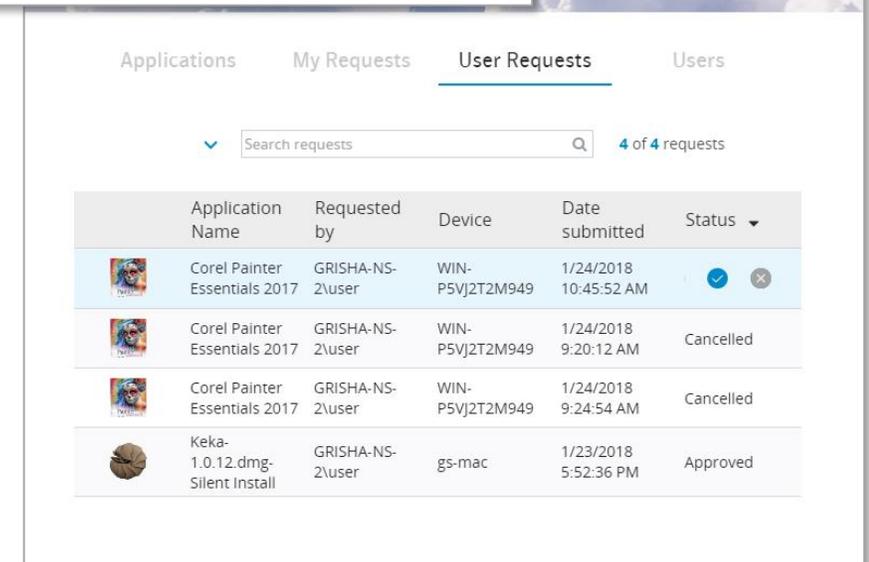
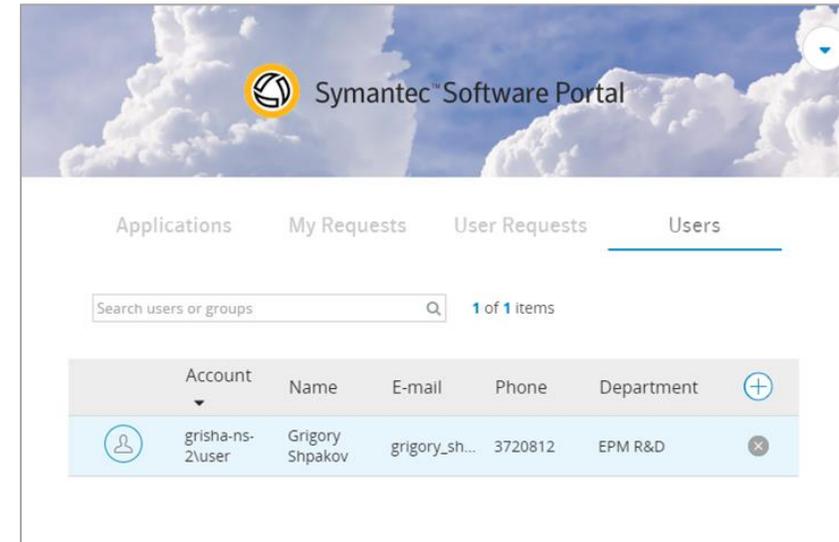
### ○ New Tabs for Managers

#### ○ Users Tab:

- Specify the list of users or groups whose requests need action taken
- View only the requests from the users who report directly to them

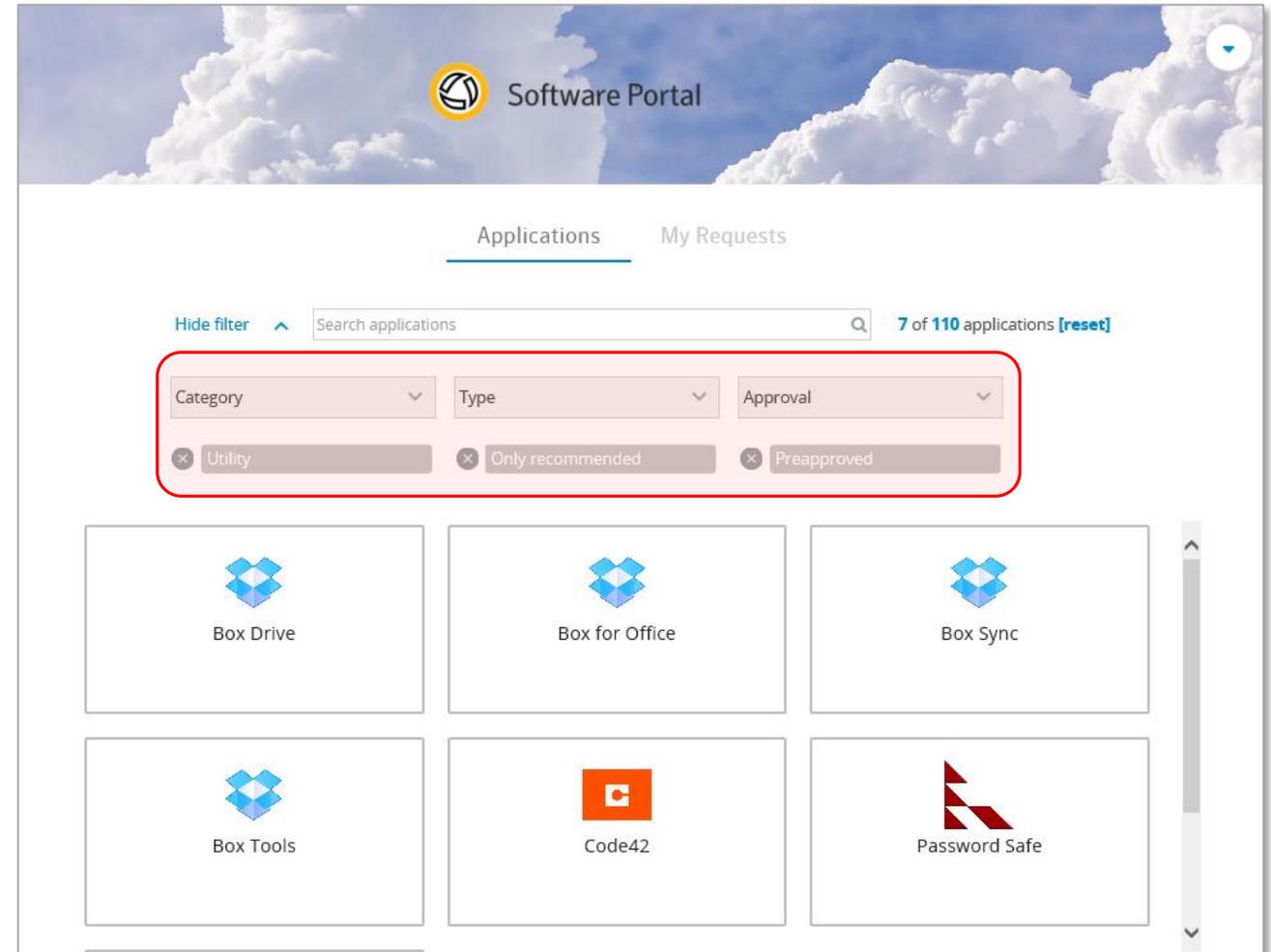
#### ○ User Requests:

- Review open requests
- Approve or deny requests
- Communicate with requesters
- Filter User requests by status/type



# Software Management Solution

- **Software Portal Enhancements**
  - **Application Filters**
    - Filters the applications list using:
      - Specific categories
      - Publishing Types
      - Approval types
    - Filters applied with the search option make finding the required application much easier



# Software Management Solution

- **Software Portal Enhancements**
  - **Request Unlisted Software**
    - Using this interface, end users will:
      - Specify **application name** in free form
      - Provide justification for the request
    - Request is handled in a similar way as requests for applications in the catalog

### Unlisted Application Request ✕

 Provide information about the application you need. If your request is approved, the software will be downloaded and installed on your device.

To receive email notifications about the changes related to your request, configure your user profile accordingly.

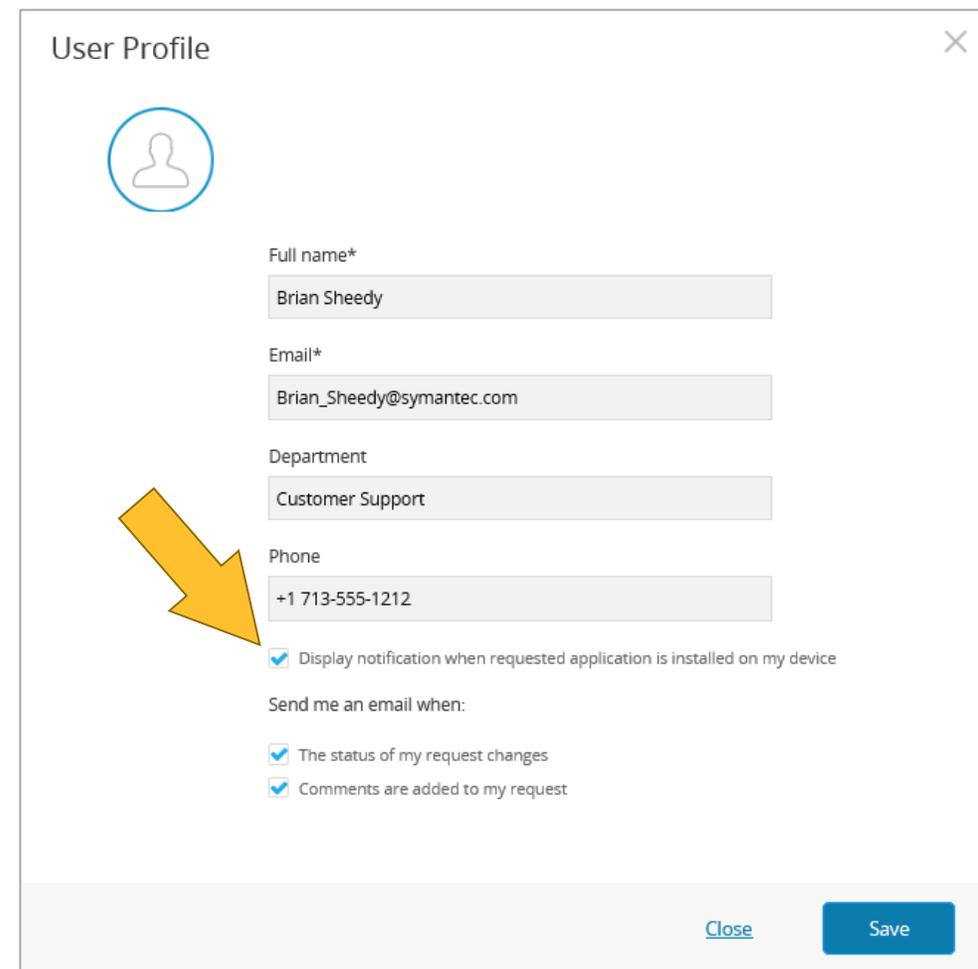
Application Name\*

Add justification\*

[Close](#)

# Software Management Solution

- **Software Portal Notification**
  - **Previous Releases:**
    - Delay before application is actually installed on the client machine
    - User is not Notified during the process
  - **SW Portal User Notifications in 8.5:**
    - Notification Options in the Portal
    - Receive emails when someone comments on or changes the status of the request
    - Email contains the link to the Software Portal where the user can manage the application request



User Profile



Full name\*  
Brian Sheedy

Email\*  
Brian\_Sheedy@symantec.com

Department  
Customer Support

Phone  
+1 713-555-1212

Display notification when requested application is installed on my device

Send me an email when:

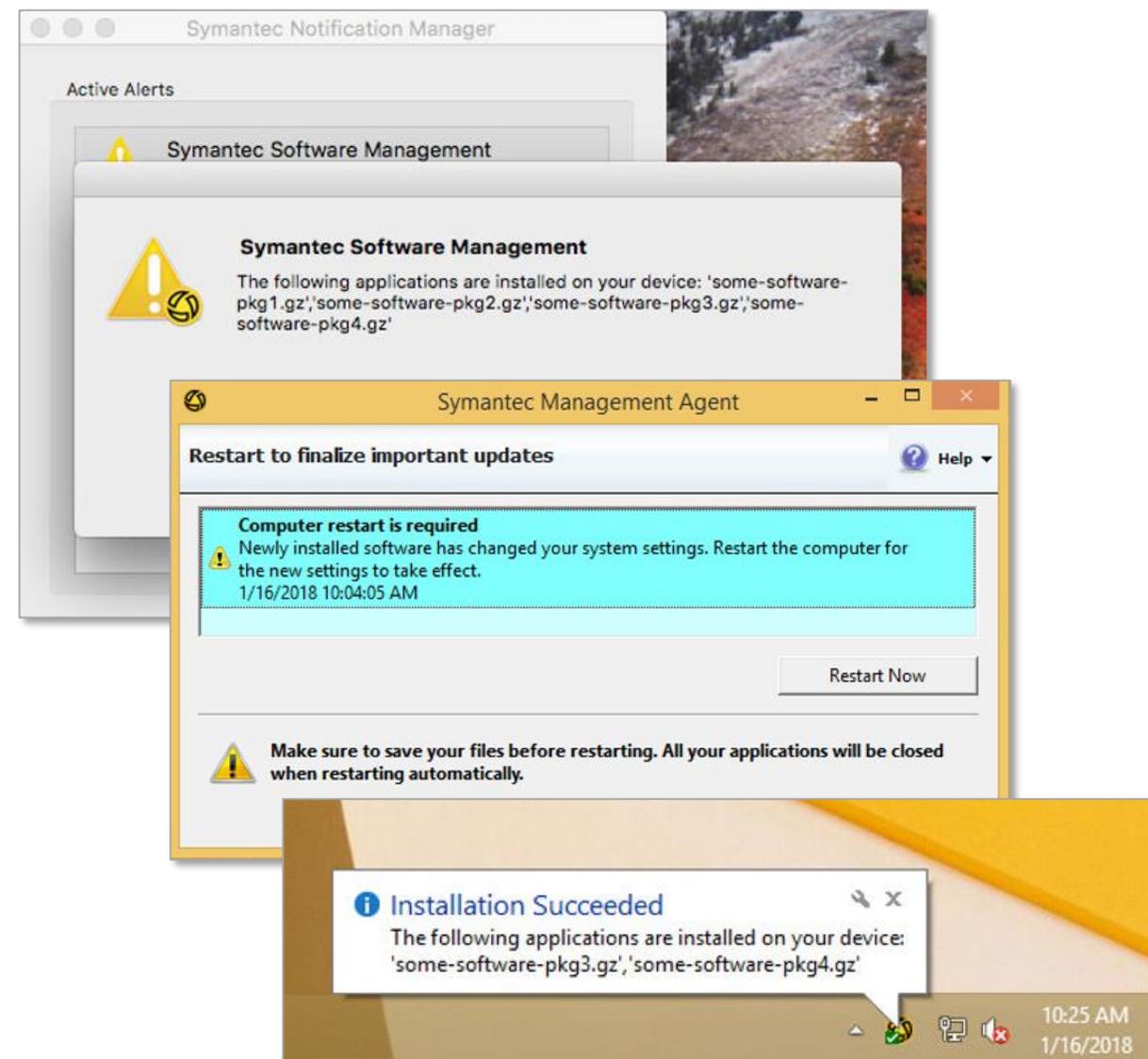
The status of my request changes

Comments are added to my request

[Close](#) [Save](#)

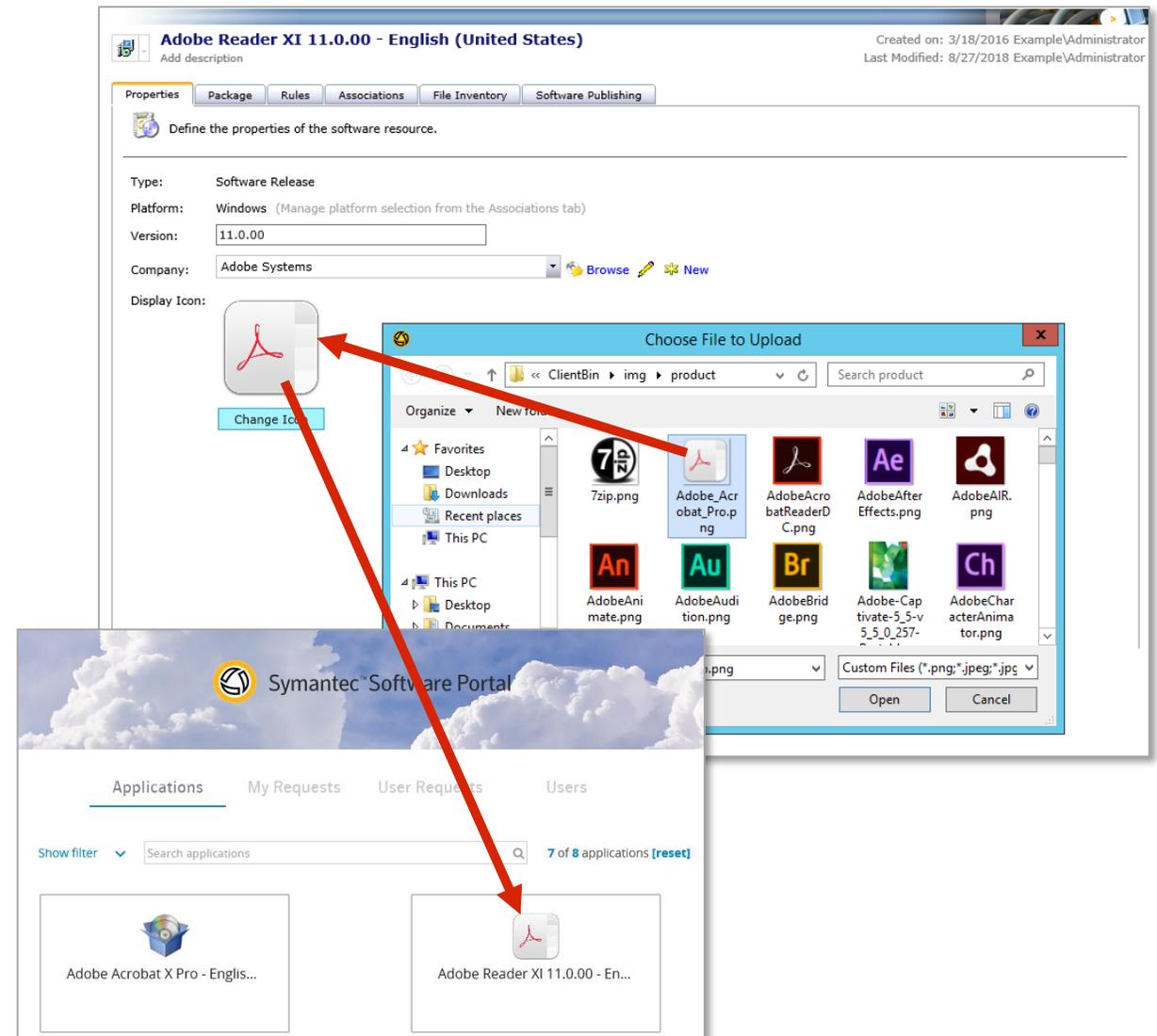
# Software Management Solution

- **Software Portal Notification**
  - **SW Portal User Notifications in 8.5:**
    - **Notification Options in the Portal**
      - Available to Windows/Mac clients
      - Appears if Portal User = Logged on User
      - Displays for 30 Seconds
      - Works for Portal Quick SWD & MSD Policies



# Software Management Solution

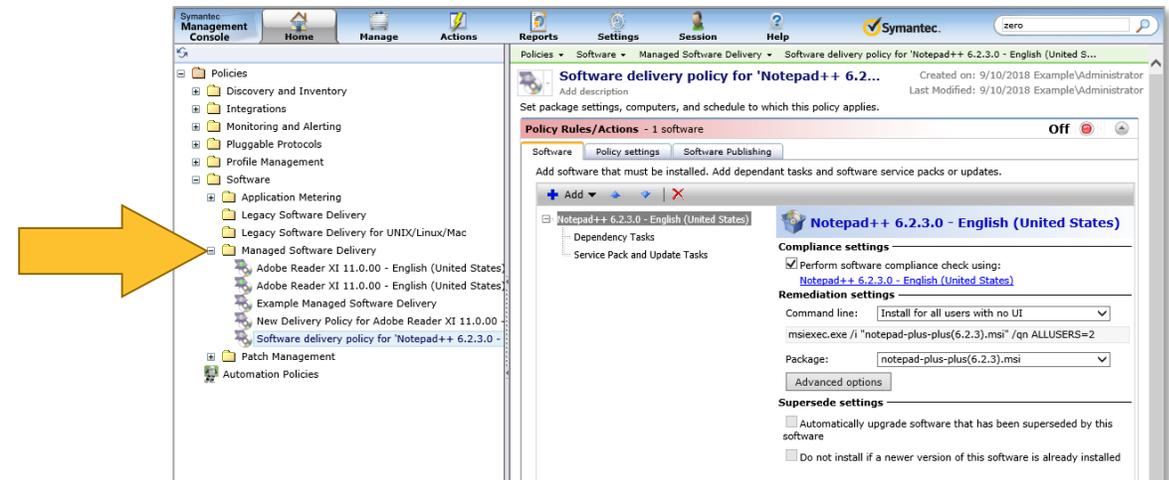
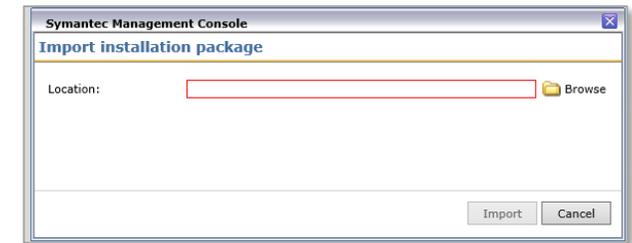
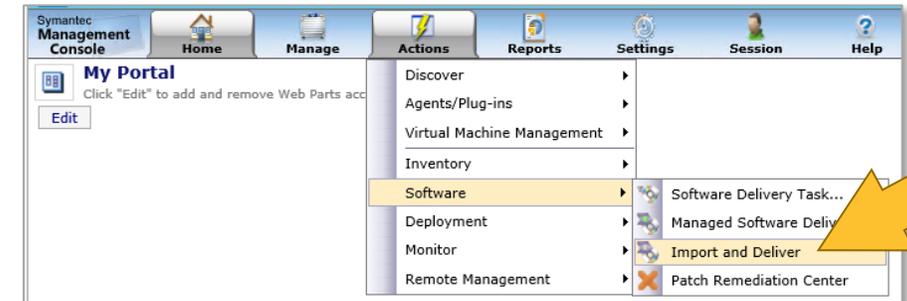
- **Software Resource Management**
  - Can add or edit a custom icon in the Software Catalog/Software Views
  - Will display Icon in the Software Portal



# Software Management Solution

- **Import and Deliver** action

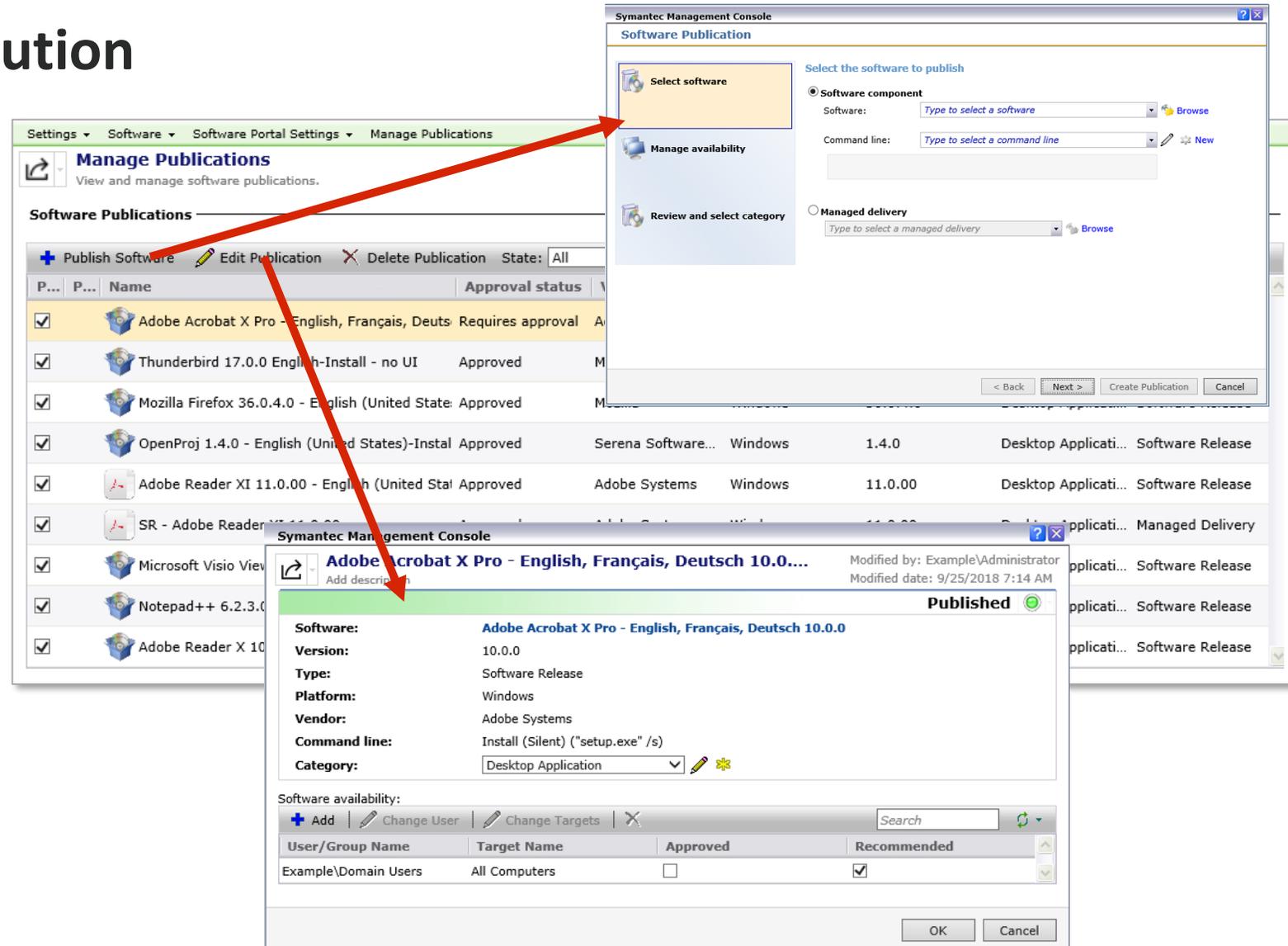
- Rapid creation of Managed Delivery Policies
- Accessible from **Actions>Software>Import and Deliver**
- Package is imported and included in a newly created *Managed SW Delivery Policy*
- Policy created in the *Managed Software Delivery* folder
- Created policy is opened automatically



# Software Management Solution

## ○ Manage Publications Page

- View, Edit, Delete
- Publish or Unpublish
- Create New Publications
  - Uses SW Wizard
- Fast and Convenient
  - No need to go to the Software Resource or Managed SWD Policy



The screenshot displays the Symantec Management Console interface. The main window shows the 'Manage Publications' page with a table of software publications. A red arrow points from the 'Publish Software' button to a 'Software Publication' wizard window. The wizard is titled 'Select the software to publish' and includes fields for 'Software component', 'Software', 'Command line', and 'Managed delivery'. Below the wizard, a detailed view of a specific publication for 'Adobe Acrobat X Pro - English, Français, Deutsch 10.0.0' is shown, including its version, type, platform, vendor, command line, and category. At the bottom, the 'Software availability' section shows a table with columns for 'User/Group Name', 'Target Name', 'Approved', and 'Recommended'.

Software	Version	Type	Platform	Vendor	Command line	Category
Adobe Acrobat X Pro - English, Français, Deuts	10.0.0	Software Release	Windows	Adobe Systems	Install (Silent) ("setup.exe" /s)	Desktop Application

User/Group Name	Target Name	Approved	Recommended
Example\Domain Users	All Computers	<input type="checkbox"/>	<input checked="" type="checkbox"/>

# Software Management Solution

## ○ Software Portal ASDK Enhancements

Modifying Software Portal Settings	
<i>Extended SetSoftwarePortalSetting()</i>	This API has been extended to set the software portal settings like CompanyLogo, PortalLogo and PortalBackground.
Setting Publishing Item Properties	
<i>SetPublishingItemProperty()</i>	This API has been newly created to set the application category.
<i>SetSoftwareComponentProperty()</i>	This API has been extended to add support for the property SoftwareIcon.
Add/Modify/Remove Users and Targets from Publishing items	
<i>ModifyUserAndTargetToPublishingItem()</i>	This API is newly created to modify the user and target in the publishing item.
<i>RemoveUserAndTargetToPublishingItem()</i>	This API is newly created to remove the user and target from the publishing item.
<i>AddUserAndTargetToPublishingItem()</i>	This API is newly created to add the user and target into the publishing item.
Modifying Software Product Properties	
<i>SetSoftwareProductProperty()</i>	This API has been newly created to allow user to modify the software product settings like Name, Description, Company, Version, NameFilterString, CompanyFilterString, VersionFilterString, IsManaged.

# Administrator Software Development Kit (ASDK)

## ○ Simplified Software Deployment API

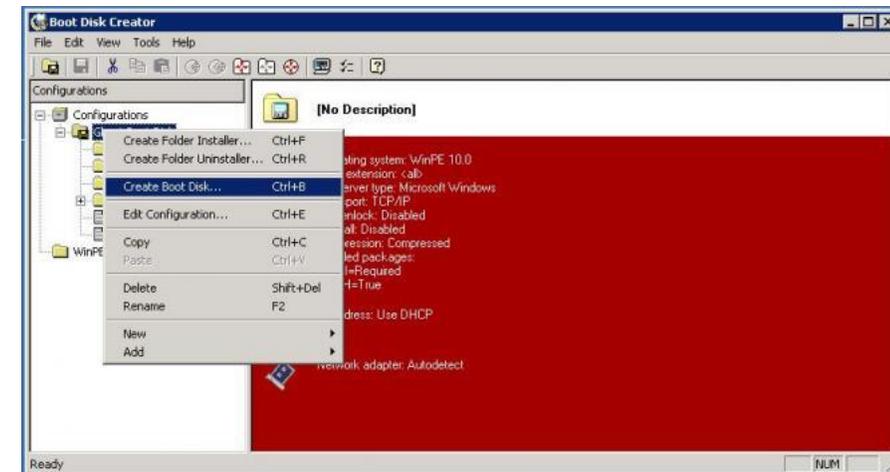
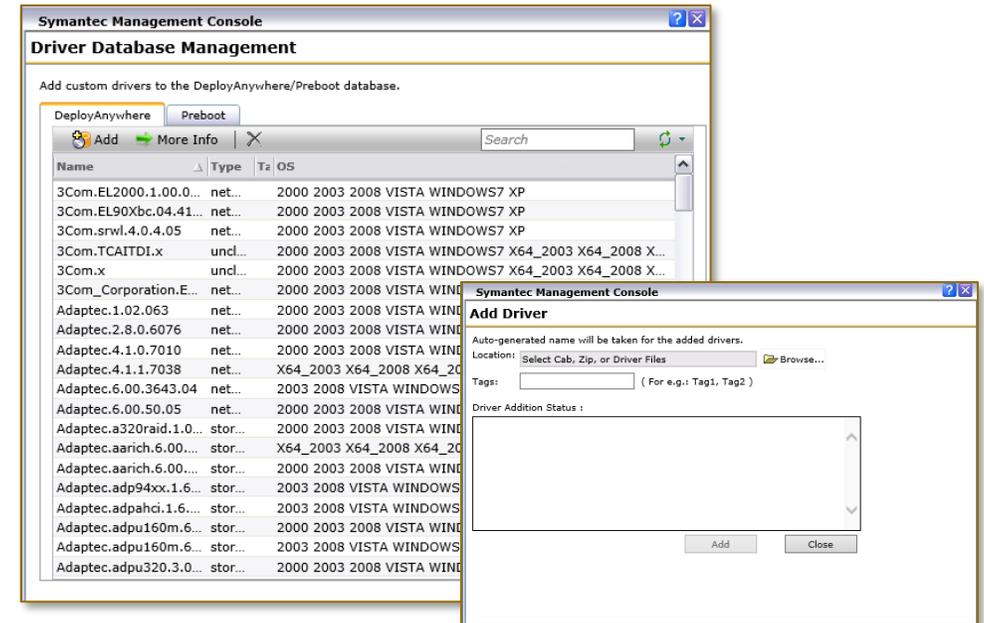
- With a single call to the *DeployPackageEx* method:
  - *Imports* a software package
  - *Creates* a software component
  - *Generates* an installation policy
- Supports the following types of installable packages:
  - Self-installable .exe packages
  - .msi packages
  - .rpm packages
  - non-DMG based .zip SEP packages for Mac
  - .exe (SFX) archive SEP packages for Windows
- **Method:**
  - *DeployPackageEx(string packageName, string parametersXML)*
- See: [DOC11040](#) for examples

Name	Description	Format
<b>packageName</b>	String that contains the path to a software installation file. The file may be located on the local NS or in the UNC directory.	Local NS path: "C:\installationFile.exe"  UNC path: "\\server\folder\installationFile.exe"
<b>parametersXML</b>	XML string with overridden parameters. If this parameter is empty string, the default parameters are used.	<parameters>

Name	Description
<b>RepositoryID</b>	<p>GUID of the repository for which the package will be imported. The following repositories are provided out of the box:</p> <ul style="list-style-type: none"> <li>• "Default smart repository" with the ID "{2406DBB0-613C-4BD6-9870-BCD49A6571D3}"</li> </ul> <p>When "Default smart repository" is used, the installation policies created with this method are located in the <b>Auto Deployment</b> folder that is not visible in the Symantec Management Console by default. To make the policy folder visible at <b>Manage &gt; Policies &gt; Software</b>, run the following SQL query:</p> <pre>Update Item SET Attributes = '22' Where Guid = '23d65059-752a-4aef-a6ab-aab902e3cdb5'</pre> <ul style="list-style-type: none"> <li>• "SEP repository" with the ID "E94719D0-D063-403F-BA60-68D5E2F2D9E3"</li> </ul> <p>When "SEP repository" is used, only SEP installation packages are supported for importing and Symantec Endpoint Protection Delivery policy is created at <b>Manage &gt; Policies &gt; Software Symantec Endpoint Protection Agent Delivery</b>.</p> <p>If this parameter is not specified, the default repository is used.</p>
<b>Targets</b>	Coma separated list of target GUIDs to be applied to the policy. If this parameter is not specified, no targets will be applied.
<b>Enabled</b>	False by default. True if the newly created policy should be enabled by default.
<b>DefaultCulture</b>	Culture to generate a localized policy name. English by default.

# Deployment Solution

- **Deployment Solution supports WinPE10**
  - Version 1607 and 1703 with some limitations.
  - See: [HOWTO126076](#)
- **Network Boot Service Supports W2K16**
  - See: [HOWTO125454](#)
- **Driver Management Enhancements**
  - Can Upload Drivers as .CAB files
- **Improved performance of Boot Disk Creator**
  - By reducing the time required to add preboot drivers and other packages while creating preboot packages for WinPE 5 and WinPE 10.



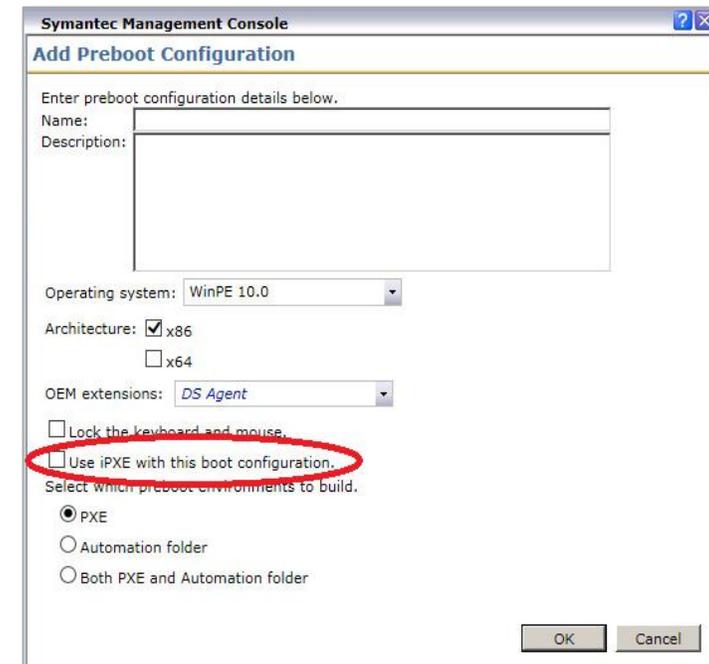
# Deployment Solution

## ○ iPXE Support

- Uses open source boot firmware of the iPXE project <https://ipxe.org/>
- Another PXE Option, Not a PXE replacement in DS 8.5!
- Existing Boot Loaders are still available and supported when creating PXE Boot Images

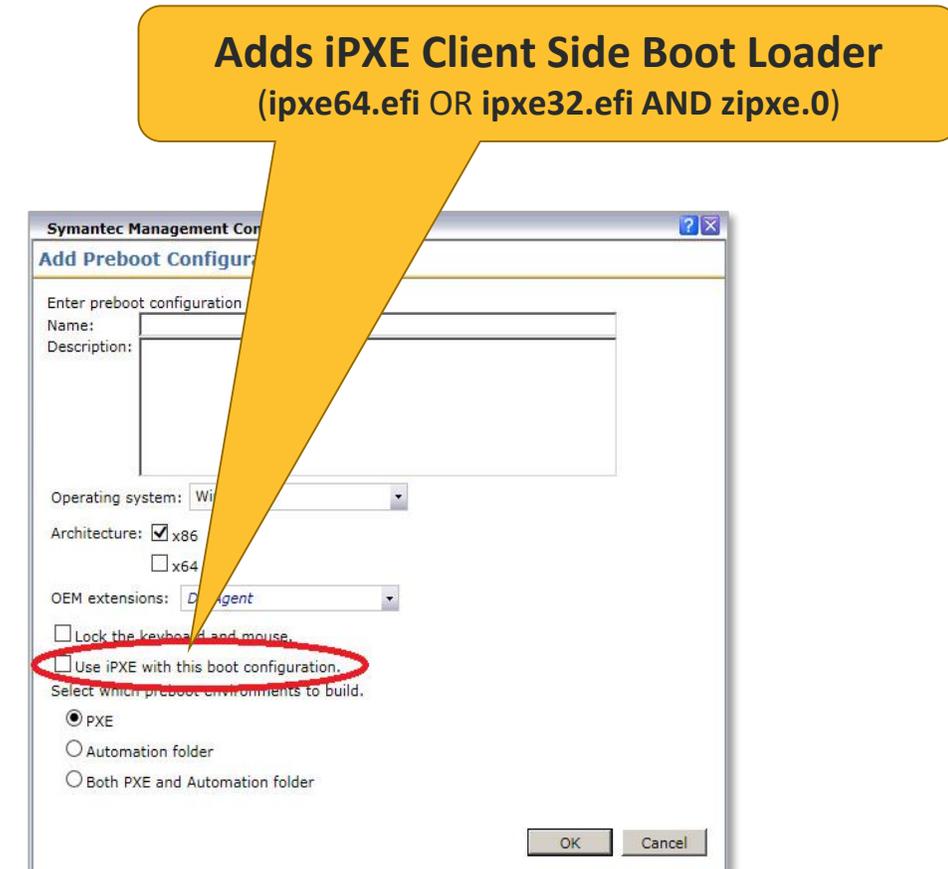
## ○ Benefits of iPXE:

- Increase download and boot up performance
- Lightweight boot loader with a full network stack
  - TFTP, SAN, HTTP – with multiple NIC Driver Support
- iPXE in DS 8.5 uses HTTP specifically:
  - Higher NW Performance than TFTP
  - Speeds up the DL and Boot of clients into PXE
- See: [TECH250831](#) for more information



# Deployment Solution

- **iPXE System Requirements:**
  - **IIS needs to be installed** on any system that will be acting as an iPXE Server
  - When the PXE server is installed or upgraded it will create a new website on **TCP port 4433**
    - This will be used for iPXE client/server communication.
    - Instructs PXE clients on how to act If a job is assigned
    - Provides access to the HTTP - PXE “Images” directory
  - ***If IIS is not available*** on Installation or upgrade:
    - Boot images with the iPXE boot loader will fail to boot from that server
    - Client systems will then boot to the next available device in the BIOS/UEFI boot order
  - Must Enable the **“Use iPXE with this boot configuration”** in the Preboot Configuration settings
  - See: [TECH250831](#) for more information



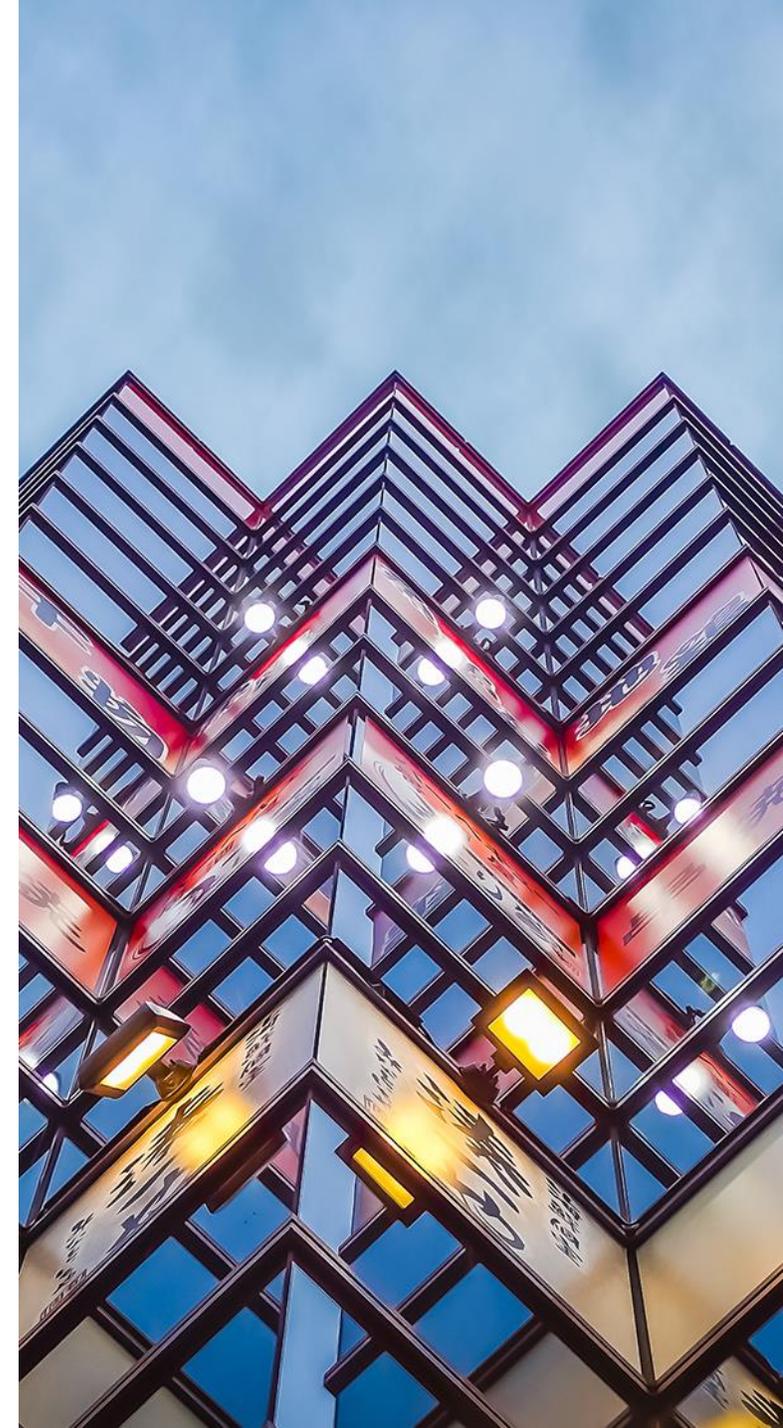
# Workflow Solution

- **Workflow support for SEP 14**
  - Customers want to be able to use previous **Workflow applications to automate their current SEP 14+ processes.**
  - **Workflow Components Library** has been developed for SEP 14 that covers:
    - Group Inquiries, Moves, Updates, and Quarantines are just a few...
    - For more information see: [DOC10748](#)
- Download and use the **ScreenCapture Utility** from a remote computer on which Workflow Solution is not installed. [DOC10956](#)
- The uninstallers for **Process Manager** and **Workflow Designer** are now localized.

SEP 14 Component name	SEP Component name	Description
Get Group List Component	Get All Group GUIDs	Gets a group list.
Get Group Computers Component	Get Client List	Gets the information about the computers in a specified domain and group
Run Command Update Content	Run Group Command Update Content & Run Client Command Update Content	Sends a command from SEPM to SEP endpoints to update content.
Get Command Status Details	Get Command Status Detail	Gets the details of a command status.
Get Admin Accounts List	Get Admin Account List	Gets the list of administrators for a
Move Computer Component	Mov	

SEP 14 Component name	Description
Run Command Baseline	Sends a command from Symantec Endpoint Protection Manager to Symantec Endpoint Protection endpoints to request that baseline application information be uploaded back to Symantec Endpoint Protection Manager.
Run Command Quarantine	Sends a command from Symantec Endpoint Protection Manager to (un)quarantine Symantec Endpoint Protection endpoints.
Get Admin Details	Gets the details of a single administrator.
Update Admin Details	Updates the details for a specified administrator.
Get Computer List Component	Gets the information about the computers in a specified domain.
Get Domains Component	Gets a list of all accessible domains.
Get Domain By Id Component	Gets the details for a specified domain
Update Domain Component	Updates an existing domain's information.

# Additional Information



# Symantec Education Services

*The confidence to own and solve IT security with Symantec technology and best practices*

## Instructor-Led Training

- Classroom or virtual
- Public or private
- Hands-on labs included

## Comprehensive E-Library

- Hundreds of regularly updated modules
- Self-paced, web-based

## Certification

- Symantec Certified Specialist (SCS) exams to validate technical knowledge and competency

## Security Awareness Service

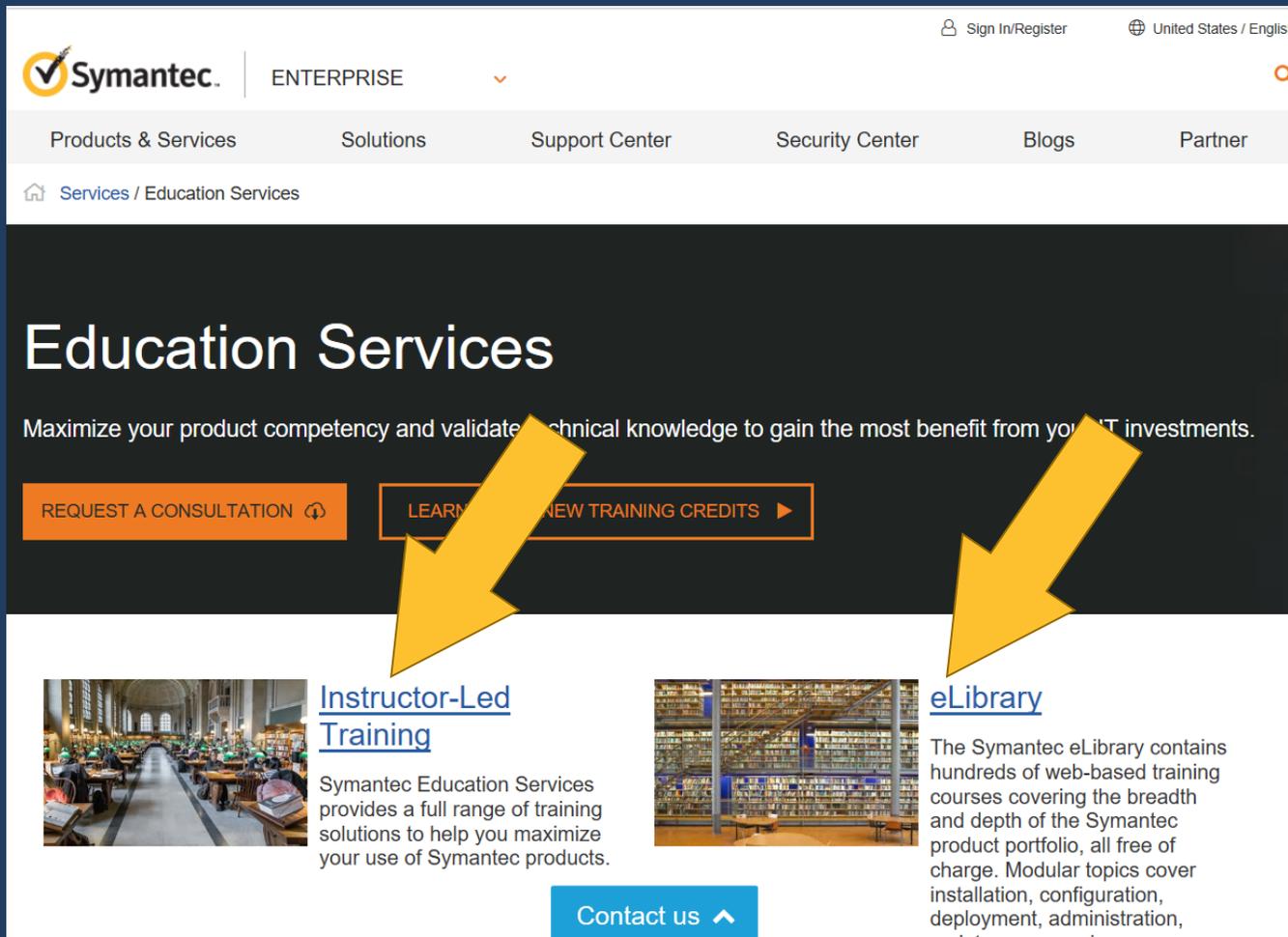
- Web-based, self-hosted
- Promotes proactive employee behavior to better protect information assets

[go.symantec.com/education](https://go.symantec.com/education)



# Symantec Education Services

GO TO: <https://go.symantec.com/education> and *Search* for:



Sign In/Register United States / English

Symantec ENTERPRISE

Products & Services Solutions Support Center Security Center Blogs Partner

Services / Education Services

## Education Services

Maximize your product competency and validate technical knowledge to gain the most benefit from your IT investments.

REQUEST A CONSULTATION LEARN MORE ABOUT NEW TRAINING CREDITS

**Instructor-Led Training**

Symantec Education Services provides a full range of training solutions to help you maximize your use of Symantec products.

**eLibrary**

The Symantec eLibrary contains hundreds of web-based training courses covering the breadth and depth of the Symantec product portfolio, all free of charge. Modular topics cover installation, configuration, deployment, administration,

Contact us

## Instructor/Virtual Courses

- ITMS 8.1 Administration
- ITMS 8.1 Diagnostics & Troubleshooting
- Client Management Suite 8.1
- Deployment Solution 8.1

## E-Library Courses

- ITMS 8.5 Differences
- ITMS 8.1 Administration
- ITMS 8.1 Diagnostics & Troubleshooting
- Deployment Solution 8.1



# Additional Resources and Summary

If you would like to know more about **IT Management Suite** please visit:

- **Product Overviews:** <https://www.symantec.com/products/it-management-suite>
- **Data Sheets:** <https://www.symantec.com/products/endpoint-management>
- **Community:** <http://www.symantec.com/connect/endpoint-management>
- **ITMS Documentation:** [https://support.symantec.com/en\\_US/article.DOC11076](https://support.symantec.com/en_US/article.DOC11076)
- **ITMS Help Center:** [https://help.symantec.com/home/ITMS8.5?locale=EN\\_US](https://help.symantec.com/home/ITMS8.5?locale=EN_US)
- **GSS Documentation:** <https://www.symantec.com/docs/DOC8558>
- **GSS Help Center:** [https://help.symantec.com/home/gss3.3?locale=EN\\_US&sku=GHOST\\_SOLUTION\\_SUITE\\_3\\_3](https://help.symantec.com/home/gss3.3?locale=EN_US&sku=GHOST_SOLUTION_SUITE_3_3)



# Thank You!

[brian\\_sheedy@Symantec.com](mailto:brian_sheedy@Symantec.com)

