


# What's New in ITMS 7.6

This document highlights some of the most impactful features of Symantec™ IT Management Suite 7.6 powered by Altiris™ technology.



For more comprehensive information, please view the ITMS product page or refer to the release notes.

Confidence in a connected world.  **Symantec.**

This document is provided for informational purposes only. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice. Copyright © 2015 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, and the Checkmark Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners. 21355200 7/15

## Table of Contents

Introduction	1
General Enhancements and Improvements	3
Updated Operating System Version Support	3
Updated Database Version Support	3
Forward Servers List	4
Improvements to Internet Gateway	4
Supported Upgrade Paths to 7.6	5
Officially Supported Upgrade Paths	5
Navigation Paths	5
Improvements to the Symantec Installation Manager	6
SIM Installation Progress Bar	6
Upgrade Advisory Messages	6
Additional Installation Readiness Checks	7
Option to Configure IT Analytics	7
License Page Refresh	7
Cryptographic Key Restoration Utility	7
Improvements to Package Service	8
Support for HTTP and HTTPS Codebases on Same Package Server	8
Support for Two HTTPS Codebases on Same Package Server	9
Support for Up to Four Codebases	9
Improvements to Task Service	10
Default Timeout for Server Tasks	10
Server Tasks Can Run as Specified User	10
Advanced Task Server Settings	10
Encryption of All Task Output	10
Faster Reassignment of Agent to Different Task Server	11
New Features in Deployment Solution	12
Support for WinPE 5.1 and Multiple Versions of WinPE	12
Driver Tagging	13
Console for Automation Agent	14
Secure PXE Boot	14
Symantec Agent Communication Profiles	15
Improvements for UNIX and Linux Agents	17
Improvements for Mac Agent	17
CEM Support	17
Agent Localization	17
Signed Installers	18
Improved Pull Installation	18
Improvements for Windows Agent	19
New Agent UI	19
Agent Logs	19
Agent Health	19
Administrator Privileges	20

Console Enhancements for ITMS Management Views	22
Agent Health Tracking	22
Summary View of Agent Health	24
Target Folders	24
Enhancements to Filter Criteria Management	26
Custom Filter Reports	27
Enhancements to the Software Blade	29
Reporting Improvements	30
New Cube Browser in IT Analytics	30
Improvements in Standard Reporting	30
Workflow 7.6 Improvements	31
Active Directory Synchronization	31
Export/Importing of Configuration Items	31
REST API Generator	31

## Introduction

The purpose of this document is to introduce some of the new features and enhancements that are provided within IT Management Suite (ITMS) 7.6. While this document will focus on those features that will be of the most interest to the average ITMS administrator, a full listing of the features can be found in the official release notes.

Specifically, this document highlights the following topics:

- General Enhancements and Improvements
  - Updated Operating System Version Support
  - Updated Database Version Support
  - Forward Servers List
  - Improvements to Internet Gateway
- Supported Upgrade Paths to 7.6
  - Officially Supported Upgrade Paths
  - Navigation Paths
- Improvements to the Symantec Installation Manager
  - SIM Installation Progress Bar
  - Upgrade Advisory Messages
  - Additional Installation Readiness Checks
  - Option to Configure IT Analytics
  - License Page Refresh
  - Cryptographic Key Restoration Utility
- Improvements to Package Service
  - Support for HTTP and HTTPS Codebases on Same Package Server
  - Support for Two HTTPS Codebases on Same Package Server
  - Support for up to Four Codebases
- Improvements to Task Service
  - Default Timeout for Server Tasks
  - Server Tasks Can Run as Specified User
  - Advanced Task Server Settings
  - Encryption of All Task Output

- Faster Reassignment of Agent to Different Task Server
- New Features in Deployment Solution
  - Support for Multiple Versions of WinPE
  - Driver Tagging
  - Console for Automation Agent
- Symantec Agent Communication Profiles
- Improvements for Unix and Linux Agents
- Improvements for Mac Agent
  - CEM Support
  - Agent Localization
  - Signed Installers
  - Improved Pull Installation
- Improvements for Windows Agent
  - New Agent UI
  - Agent Logs
  - Agent Health
  - Administrator Privileges
- Console Enhancements for ITMS Management Views
  - Agent Health Tracking
  - Summary View of Agent Health
  - Target Folders
  - Enhancements to Filter Criteria Management
  - Custom Filter Reports
  - Enhancements to the Software Blade
- Reporting Improvements
  - New Cube Browser in IT Analytics
  - Improvements in Standard Reporting
- Workflow Improvements
  - Active Directory Synchronization
  - Export/Import of Configuration Items
  - REST API Generator

## General Enhancements and Improvements

IT Management Suite (ITMS) 7.6 includes many performance and stability improvements. Some technical features of note include:

- All ITMS components have been migrated to .NET 4.5.x
- Application pools associated with all ITMS web components are now configured with .NET CLR version 4.0 and are set to Integrated managed pipeline mode
- Handling of Active Directory imports has been vastly improved to increase performance of Delta membership updates
- Several database queries have been rewritten for better SQL performance
- New database views have been created for better console performance
- ActiveX controls have been removed for better console security and performance
- To improve security, ITMS can now send notification emails through SMTP servers that require SSL

## Updated Operating System Version Support

Support for the following operating systems has been added:

- RHEL 7 and 6.5
- SLES 11 SP3
- Solaris 11 (SPARC and Intel)
- OS X 10.10 Yosemite
- Windows 8.1 U1/U2

## Updated Database Version Support

The Symantec Management Platform has added support for the following versions of SQL:

- Microsoft SQL Server 2014
- Microsoft SQL Server 2014 Express

## **Forward Servers List**

Replication rules are a convenient feature in ITMS that allow an administrator to transfer data from one management server to another, with granular control of precisely what the data is, where it goes, and how often it is transmitted. Formerly, setting up replication rules required an administrator to repeat the communication configuration for the destination servers in each individual rule, which was a cumbersome process and made replication difficult to configure and maintain.

The 7.6 platform now supports a Forward Servers List, which makes actions such as inventory forwarding and other data replication easier to implement and maintain. After configuring server information once in the Forward Servers List, specific servers can be selected for each replication rule via a dropdown menu.

Note: servers in hierarchy will also appear in this dropdown and can be selected for standalone replication activities in addition to more typical hierarchy replication.

## **Improvements to Internet Gateway**

The Internet Gateway has received many improvements that provide enhanced support for Cloud-enabled Management (CEM). These enhancements include:

- Support for third-party certificates
- F5 load balancer support
- Upgraded Apache and OpenSSL
- Enhanced logging and reports

Note: Additional CEM enhancements in ITMS 7.6 include Agent Communication Profiles, Package Server improvements, and CEM support for Mac Agents. Those topics are covered in separate sections later in this document.

## Supported Upgrade Paths to 7.6

### Officially Supported Upgrade Paths

The following versions are the only officially supported direct upgrade paths:

- ITMS 7.1 SP2 MP1.1 to ITMS 7.6
- ITMS 7.1 SP2 MP1 Rollup v11 to ITMS 7.6
- ITMS 7.5 SP1 HF5 to ITMS 7.6

### Navigation Paths

For environments running alternate versions, the following are the recommended upgrade paths:

Currently Installed ITMS/SMP version	Recommended path to upgrade to ITMS 7.6
7.1	7.1 → 7.1 SP2 → 7.1 SP2 MP 1.1 → 7.6
7.1 SP1 b	7.1 SP 1 → 7.1 SP2 → 7.1 SP2 MP 1.1 → 7.6
7.1 SP2 b	7.1 SP2 → 7.1 SP2 MP 1.1 → 7.6
7.1 SP2 MP1	7.1 SP2 MP1 → 7.1 SP2 MP 1.1 → 7.6
7.5	7.5 → 7.5 HF6 → 7.5 SP1 → 7.5 SP1 HF5 → 7.6
7.5 HF6	7.5 HF6 → 7.5 SP1 → 7.5 SP1 HF5 → 7.6
7.5 SP1	7.5 SP1 → 7.5 SP1 HF5 → 7.6



## Improvements to the Symantec Installation Manager

The Symantec Installation Manager (SIM) has received many upgrades and enhancements improving performance and increasing usability. New features to highlight include:

- SIM installation progress bar
- Upgrade messages
- Additional Installation Readiness Checks
- Option to Configure IT Analytics
- License page refresh
- Cryptographic key restoration utility

### SIM Installation Progress Bar

A progress bar has been added to allow administrators to view SIM installation progress. Formerly,



progress information was only available for components the SIM was installing (such as ITMS), not for the installation of the SIM component itself.

### Upgrade Advisory Messages

When performing an upgrade to ITMS 7.6, it is very important that administrators close any ITMS management consoles currently open as well as the Altiris log viewer. Tests have found that the legacy (7.1) Altiris log viewer can cause a significant drag on the upgrade process, causing a 4-hour process to take 11 hours – nearly three times as long. To prevent this issue, the SIM will display an upgrade message to administrators, advising them to close the ITMS console, Altiris log viewer, and the Restore Notification Server Cryptographic keys utility before beginning the upgrade. Note: Upgrading with the 7.5 Altiris log viewer open should not be a problem.

Also, pcAnywhere is no longer supported in 7.6, so there is an upgrade message informing administrators that proceeding with the installation will remove the ability to manage pcAnywhere components. However, pcAnywhere can still be launched from the pcAnywhere Manager on the Notification Server and from Quick Connect. Host installations will remain with their current configurations. If you want to continue using pcAnywhere with the console, the following document describes how to reinstall console integration: <http://www.symantec.com/docs/HOWTO110286>.

### Additional Installation Readiness Checks

SIM has added the following Installation Readiness Checks (IRCs) to check for the following components prior to ITMS installation:

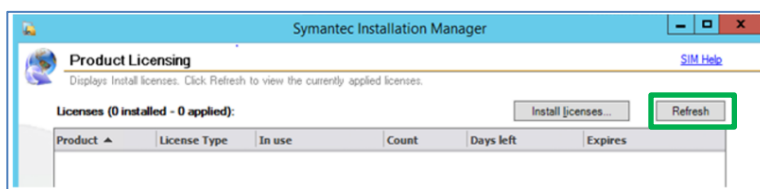
- ASP.NET 4.5.1
- WCF 4.5.1
- pcAnywhere EOL
- Migration wizard
- Supported upgrade path check

### Option to Configure IT Analytics

Formerly, IT Analytics (ITA) could be installed but not configured using the SIM; configuration could only be done through the ITMS management console. To make ITMS installation more comprehensive and convenient, SIM now presents the option to configure the ITA Analysis Server and Reporting Server as part of the ITMS configuration process. Analysis and Reporting Services must be installed on SQL Server before attempting ITA configuration, so this option can be skipped in SIM if those services are not yet installed. ITA configuration can always be performed later via the management console just as in previous versions.

### License Page Refresh

For enhanced performance, a Refresh button has been added to the Product Licensing page, so that administrators can control precisely when the license server is polled for information updates. This is much more efficient than the continuous polling behavior of previous versions.



### Cryptographic Key Restoration Utility

The KMS Restore Utility is now conveniently packaged with SIM and installed in the SIM installation folder. This utility allows the selection and restoration of previously back up cryptographic keys in disaster recovery situations. Symantec is also in the process of creating a Disaster Recovery Plan whitepaper.

## Improvements to Package Service

Package Service is an installed component that allows a system to act as a package server within an ITMS environment. It has been upgraded with the following highly requested features:

- Support for HTTP and HTTPS codebases on same package server
- Support for two HTTPS codebases on same package server

### Support for HTTP and HTTPS Codebases on Same Package Server

A codebase is an address or location of a file available on a package server. Symantec Management Agents use this codebase information when they need to download a specific file. A codebase can be a web address using HTTP or HTTPS, or it can be a UNC path.

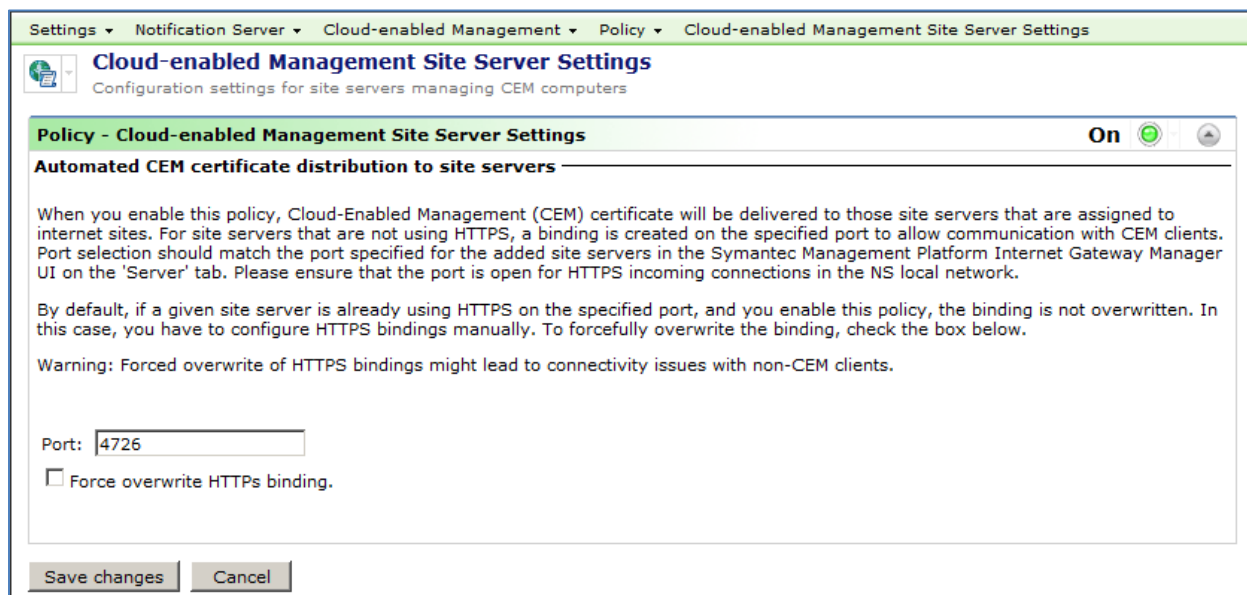
Prior to 7.6, a package server could publish combinations of codebases including a UNC and an HTTP codebase, or a UNC and an HTTPS codebase, but not an HTTP and an HTTPS codebase together. That made it very difficult for a single package server to provide package downloads to both CEM agents (client computers outside the corporate network) who require HTTPS connections for all downloads, and non-CEM agents (client computers on the internal corporate network) who can be configured to use either HTTP or HTTPS for downloads internally.

As a much requested feature, Package Service now supports providing both HTTP and HTTPS codebases at the same time. The webserver codebase configuration options that were formerly radio buttons are now checkboxes.

The screenshot displays the 'Package Service Settings' web interface. The breadcrumb trail at the top reads: Site Management > Site Server Settings > Package Service > Package Service Settings. The main heading is 'Package Service Settings' with a subtext 'View and edit global package service settings.' Below this is the 'Global Package Service Settings' section. Under 'Package File Settings', there are two options: 'Delete package files if they are unused for' (set to 1 Week) and 'Remove automatic site assignments if they are unused for' (set to 1 Month). Under 'Package Storage Settings', there are two checked options: 'Allow usage of all the fixed drives when the default storage location runs out of disk space' and 'Exclude the system drive'. Under 'Published Codebase Types', there are four checked options: 'Publish UNC codebase', 'Publish IIS hosted codebases (provided IIS is installed)', 'Publish HTTP codebase', and 'Publish HTTPS codebase (provided an SSL certificate is installed)'. A green rectangular box highlights the 'Publish IIS hosted codebases', 'Publish HTTP codebase', and 'Publish HTTPS codebase' options.

## Support for Two HTTPS Codebases on Same Package Server

In ITMS 7.6, Package Service now supports publishing two HTTPS codebases: one using the standard port assignment and a second using a custom port assignment. This feature allows a package server to provide downloads to internal clients using HTTPS as well as provide downloads to CEM agents, as long as CEM agents use HTTPS on a different port.



## Support for Up to Four Codebases

Combining the two new features presented above, a package server can now publish up to four codebases: UNC, HTTP, HTTPS (standard port), and HTTPS (custom port).

With these enhancements to Package Service, organizations now have a greater flexibility in how they utilize their package servers to provision client computers inside and outside their corporate networks. It is no longer necessary to dedicate a package server to an internal-only or an external (Internet) only site; a package server now has the capacity to serve both.

## Improvements to Task Service

Task Service has had many enhancements for security, reliability, and performance, including:

- Default timeout for server tasks
- Server tasks can run as specified user
- New advanced task server settings
- Encryption of all task output
- Faster reassignment of agent to different task server

### Default Timeout for Server Tasks

Formerly, server tasks did not time out, which meant that tasks could hang and build up on a server over time, eventually preventing any new tasks from launching. Now server tasks have a default timeout of 36 hours, and a custom timeout value can be assigned to any server task in the same manner as a client task.

### Server Tasks Can Run as Specified User

Server tasks can now be configured to run under a specific user rather than system, resolving problems sometimes encountered when task service requires access to secure storage. This problem has most frequently been encountered when customers upgraded from 7.1 to 7.5, because in 7.1 server tasks run as Application Identity but in 7.5 they run as system. Prior to 7.6 the workaround was to apply special scripts provided by Support.

### Advanced Task Server Settings

Advanced Task Server Settings have been added to the console, facilitating custom settings for load testing purposes and greater flexibility in troubleshooting.

### Encryption of All Task Output

Formerly, some items such as script output (if configured to be sent with task status), were not encrypted, causing a security concern for some organizations. Now all task output is encrypted between agent and task server, and between task server and Notification Server.

### **Faster Reassignment of Agent to Different Task Server**

Formerly, the assignment of an agent to a task server was verified every 24 hours, causing a significant delay if agents needed to be reassigned due to server maintenance. Now the assignment is checked every two hours by default.

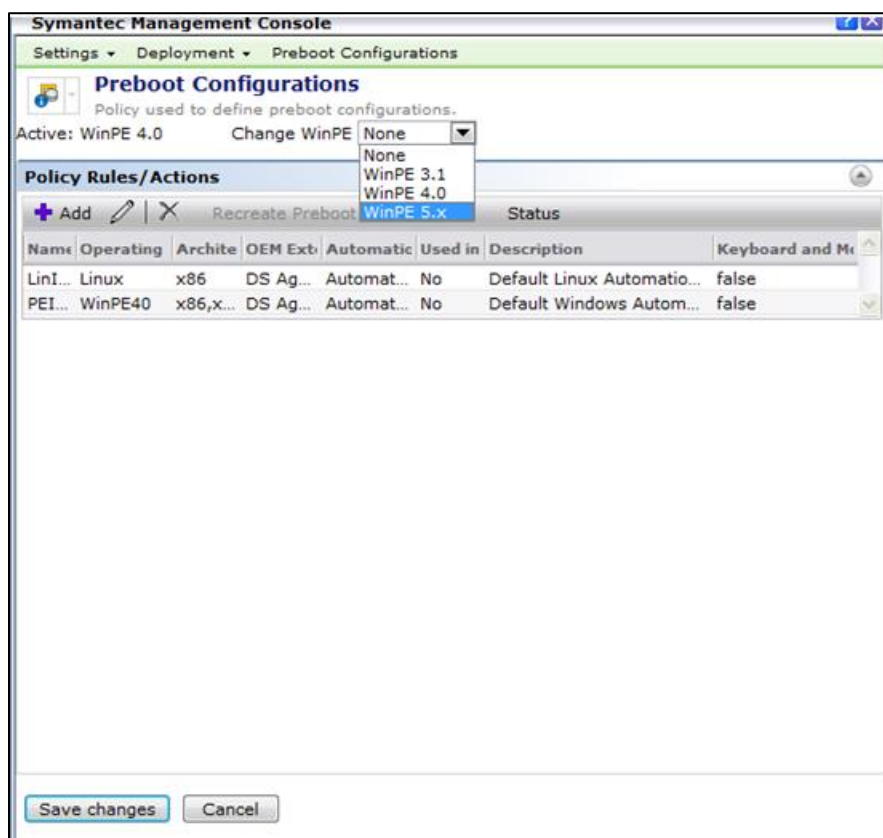
## New Features in Deployment Solution

Many enhancements have been added to Deployment Solution 7.6 to increase versatility and functionality. New features of note include:

- UEFI 32-bit support
- Support for WinPE 5.1 and multiple versions of WinPE
- Driver tagging
- Console for PECTAgent
- Secure PXE Boot

### Support for WinPE 5.1 and Multiple Versions of WinPE

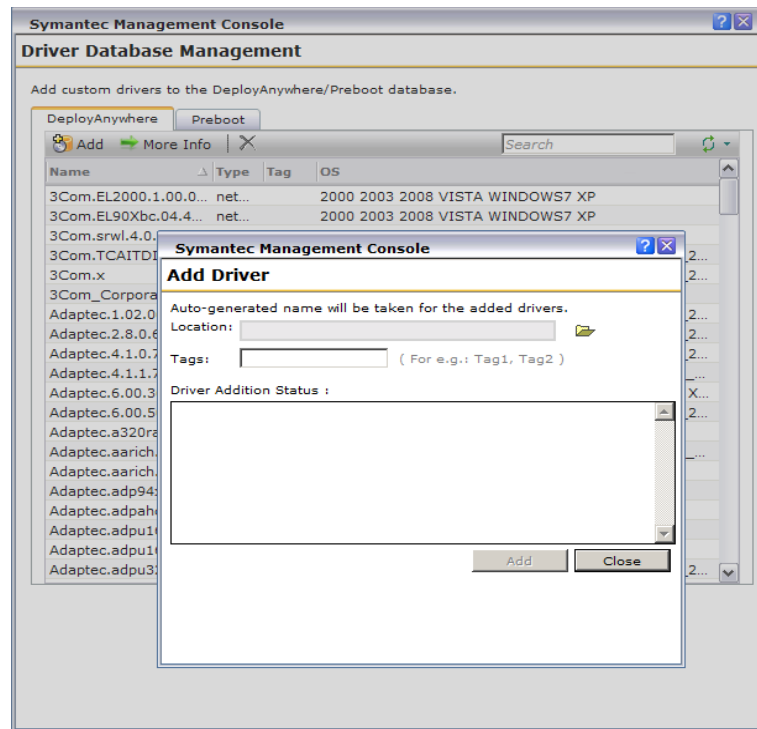
Previous releases of Deployment Solution supported only a single, specific version of WinPE. DS 7.5 SP1 only supported WinPE 4.0, for example. The 7.6 release now supports multiple versions of WinPE, including 3.1, 4.0, 5.0, and 5.1. The administrator has the flexibility of choosing a WinPE environment and setting it as the “active” WinPE for use in deployment tasks and jobs.



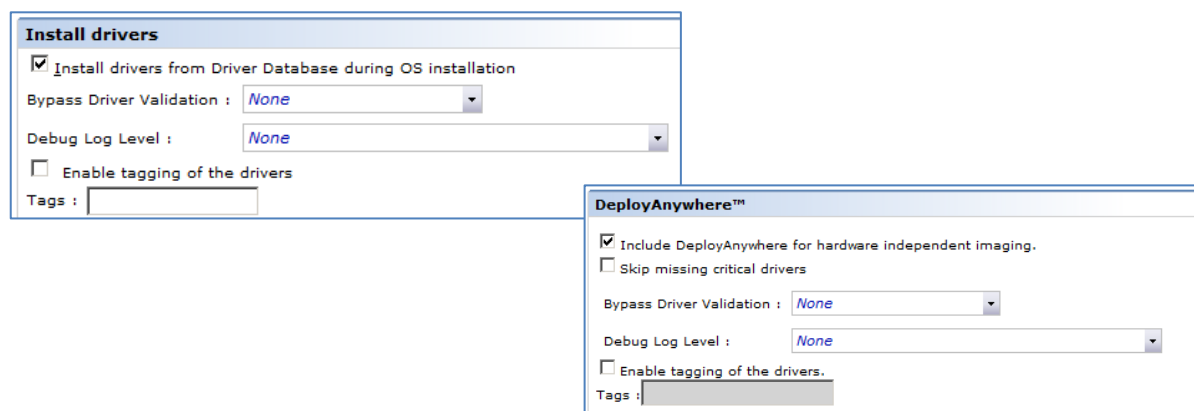
## Driver Tagging

In previous versions, DeployAnywhere took charge of targeting the best matching drivers during an image deployment or scripted operating system installation. Now in 7.6, the new feature of driver tagging allows an administrator to forcefully re-target desired drivers. This is particularly useful in situations where older hardware does not work well with the latest drivers, and specific older or generic drivers need to be targeted and installed instead of the latest matching driver available from a vendor.

Tags can be added when new drivers are added to the DeployAnywhere Driver Database and are displayed in a new Tag column.



Tags can then be enabled for use within a Scripted OS Install or within a Distribute Disk Image task.

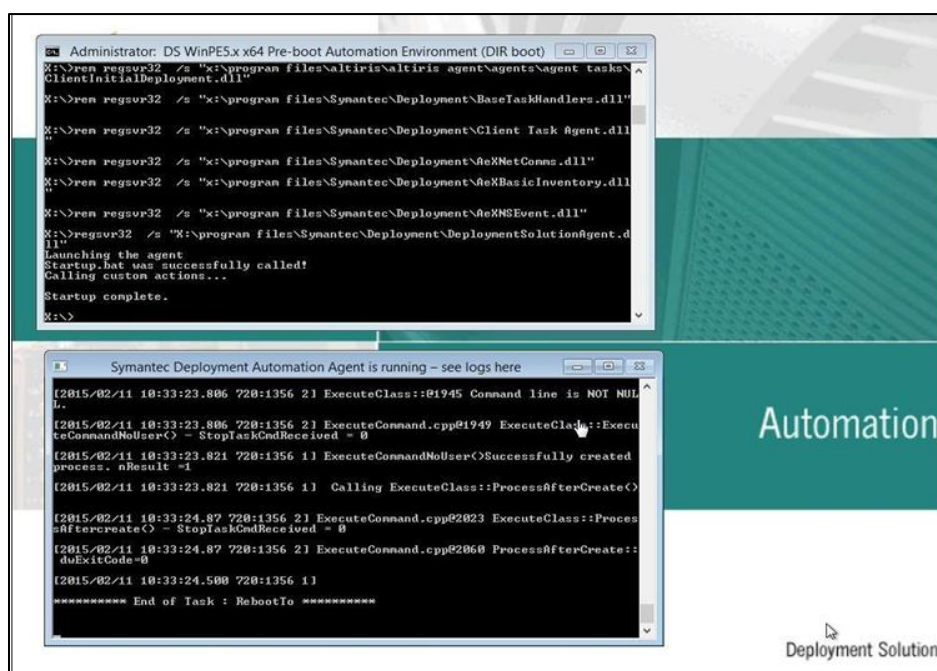




## Console for Automation Agent

All releases of Deployment Solution include specialized versions of deployment agents to run in the LinuxPE and WinPE automation operating system environments. These “automation agents” have different capabilities than the deployment agents that run in production operating systems like Windows 7. In ITMS 7.x, the deployment agent that runs in WinPE is called the PECTAgent (short for “PE Client Task Agent”), and it typically performs activities such as erasing hard drives or deploying an image.

Formerly there was no console for the PECTAgent, and it was difficult to view the agent's logs and troubleshoot any issues that might crop up. Now in the ITMS 7.6 release, when the PECTAgent starts up on a client computer, a command console also launches, enabling a technician to easily view the status of the PECTAgent and the operations it is performing.



## Secure PXE Boot

In the past, a UEFI-based computer was unable to boot to production when deploying a BIOS-based Windows 8 64-bit image. In Deployment Solution 7.6 the Secure PXE boot option allows you to boot into UEFI hardware.

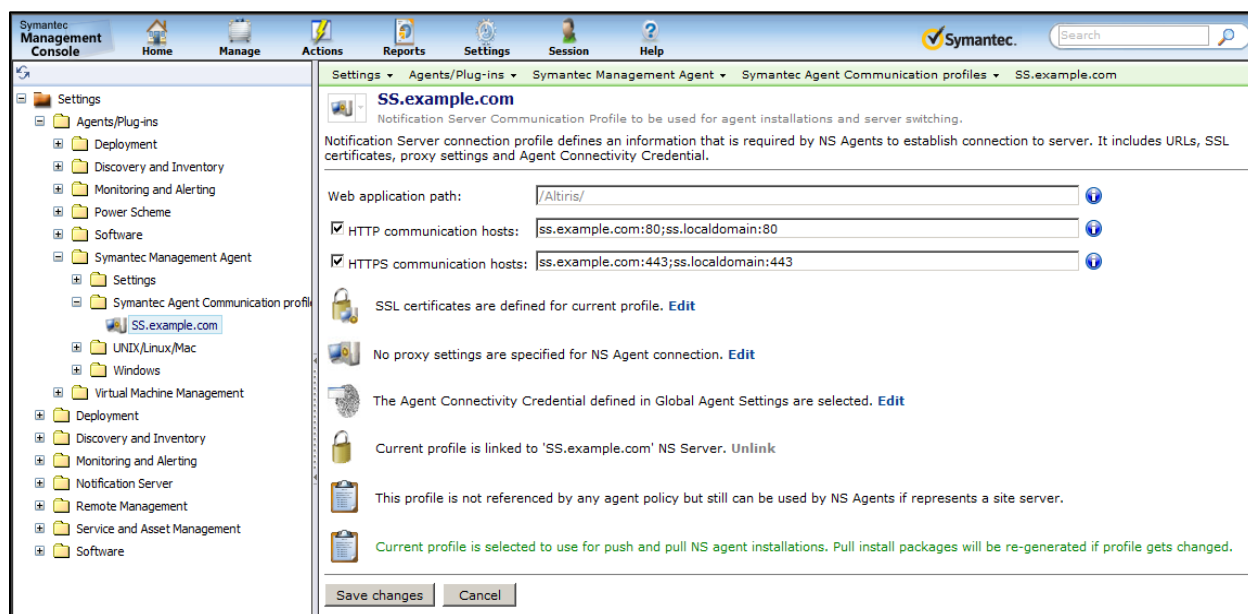
## Symantec Agent Communication Profiles

Formerly, a Symantec Management Agent could only be configured with communication information for a single Notification Server (NS). That caused problems in disaster recovery scenarios, when hardware failure on an NS could cause permanent loss of connectivity with agents, especially those in the cloud. Administrators doing off-box upgrades of Notification Server faced similar concerns.

ITMS 7.6 now includes Symantec Agent Communication Profiles, which provide an easier method of defining, storing, and assigning all the information that an agent needs in order to connect with Notification Servers and Package Servers. Multiple profiles can be created to suit a variety of use cases. Profiles are stored in the CMDB so they can be created, stored, inherited, exported, and assigned to agents as needs dictate.

Communication profiles include the web address, port, and SSL certificate necessary for agents to connect with each particular server. A single profile can contain addresses for multiple servers, which supports failover in disaster recovery and off-box upgrade scenarios.

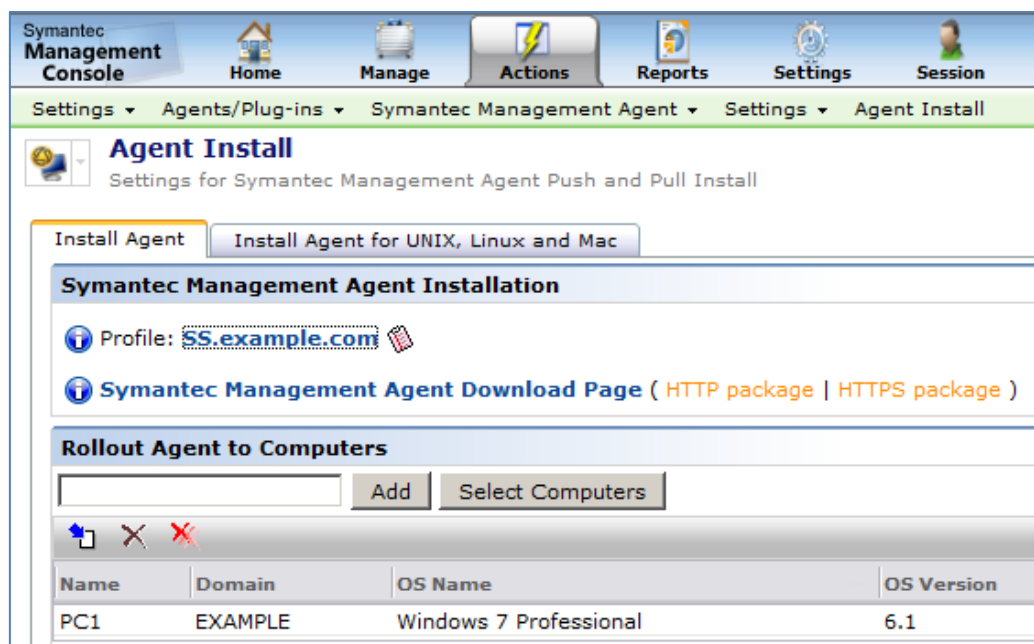
Profiles can also include proxy settings for the agent to use to connect with the server.



Communication Profiles are assignable to agents by direct import and through targeted agent settings policies, as in the screenshot below:



Communication Profiles are also included in agent installation packages, providing increased security to new agents, especially in the cloud. Formerly, an agent's initial registration request to a Notification Server was submitted in plain text, leaving client computers vulnerable to Man in the Middle attacks or spoofing. Now, the agent has the correct information to perform private, encrypted communication with the designated Notification Server from the very beginning.



## Improvements for UNIX and Linux Agents

Administrators can now perform push installs to UNIX or Linux computers using non-root accounts, a feature previously available only for the Mac agent. This is significant because default configurations of Solaris 11 (newly supported in 7.6) disallow root user installations across a network, and this security restriction is common to many enterprise environments that use UNIX or Linux.

## Improvements for Mac Agent

Improvements to the Mac Agent include the following important features:

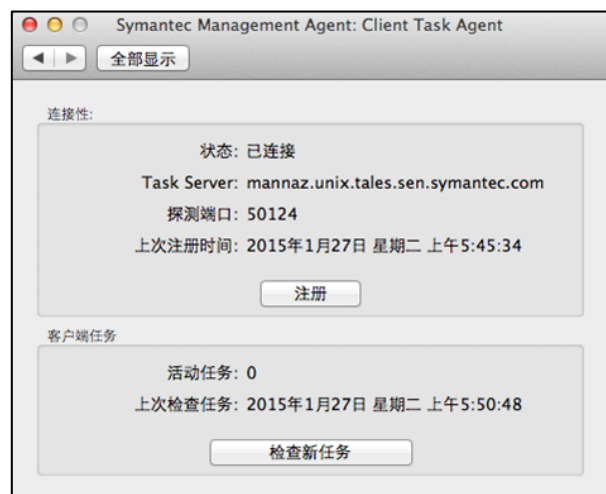
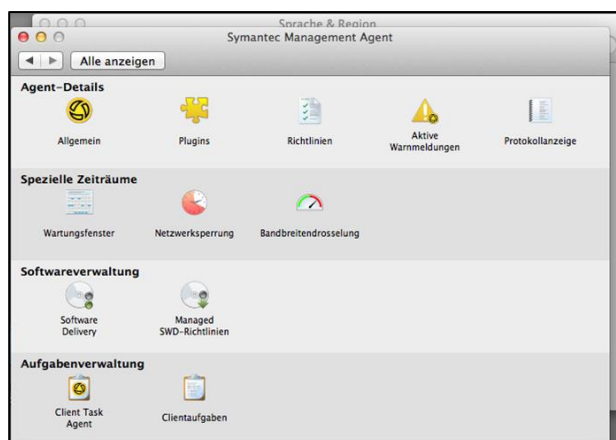
- CEM support
- Agent localization
- Signed installation files
- Improved pull installation

### CEM Support

The Symantec Management Agent for Mac now supports Cloud-enabled Management (CEM). Windows and Mac computers can now be managed equally in the cloud. This heterogeneous management of clients in the cloud was not available in previous versions.

### Agent Localization

The Mac Agent graphical UI now supports localization in 18 languages in addition to English.

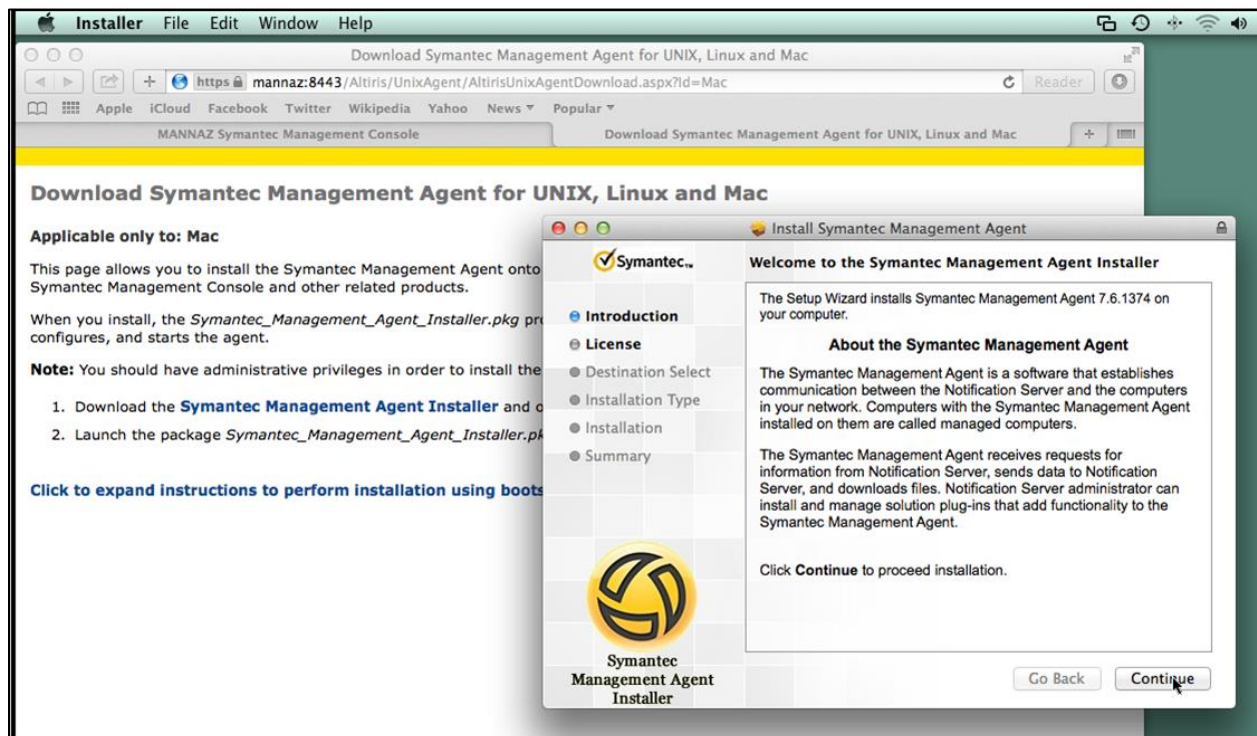


## Signed Installers

All agent software (for agent and plug-ins) is now signed with a Developer ID Installer certificate issued by Apple.

## Improved Pull Installation

Pull installations of the Symantec Management Agent for Mac no longer require using a terminal window and command line switches. In 7.6 agent installations can be performed conveniently through the graphical user interface in the same way as other Mac software.



## Improvements for Windows Agent

Many features and enhancements have been added to the Symantec Management Agent for Windows, including:

- New agent UI
- Agent logs
- Agent health
- Administrator privileges

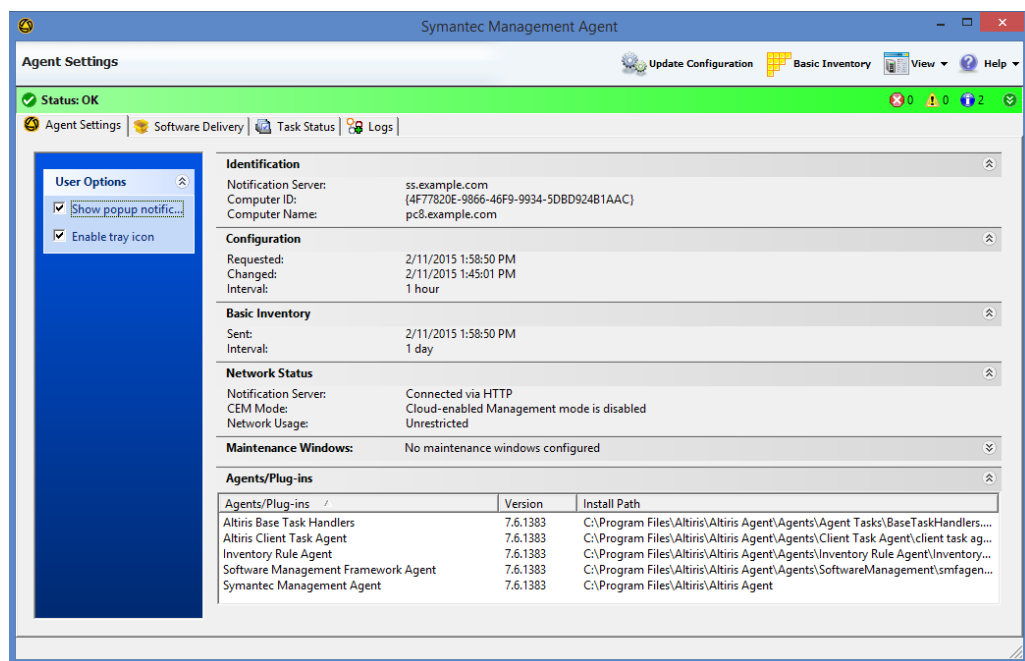
### New Agent UI

The graphical user interface has been completely redesigned for the Windows Agent. In particular, two windows that were formerly separate have been combined: the tabs and configuration options formerly available through the Settings window have now been integrated into the main agent UI, greatly

increasing  
convenience  
and usability.

### Agent Logs

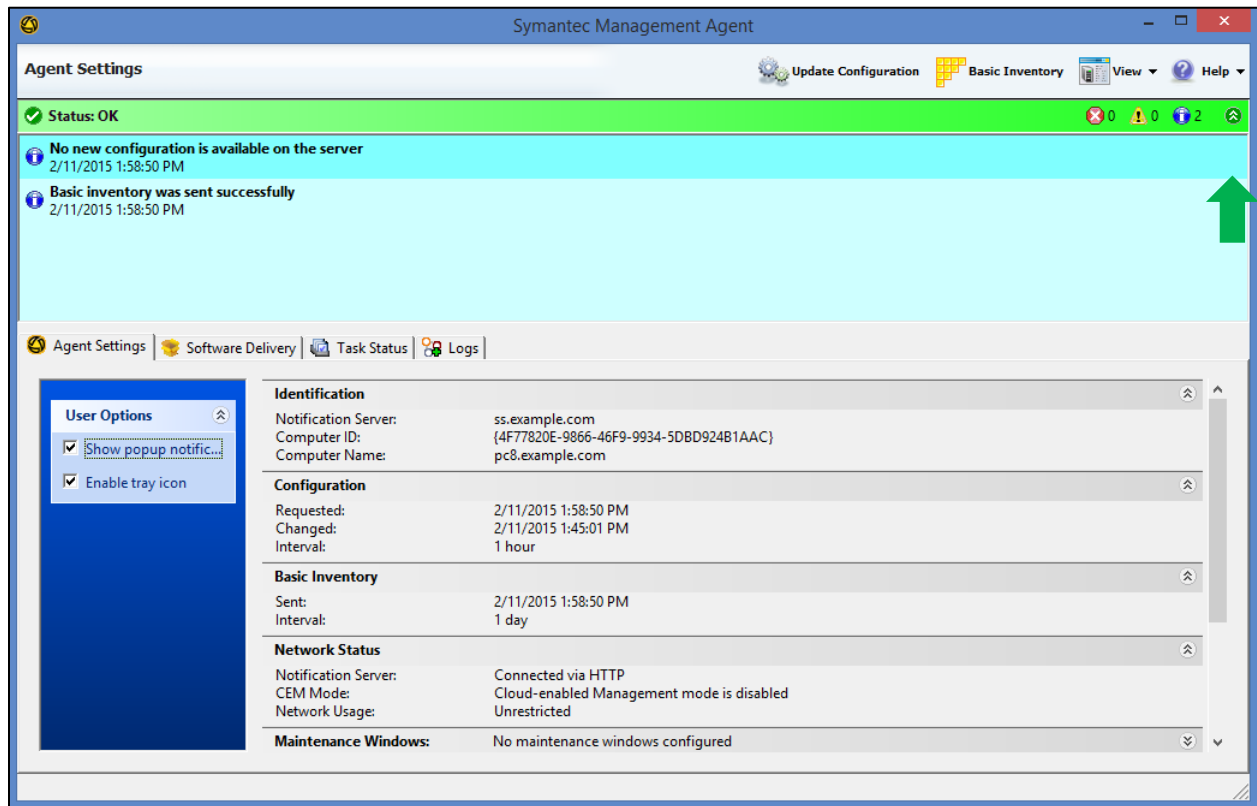
All users may  
now  
conveniently  
access the agent  
logs through the  
new Logs tab.



### Agent Health

At the top of the agent UI, the agent's health is now prominently displayed. The color bar along the top changes color based on current log entries: green indicates healthy, no warnings or errors in the logs, yellow indicates one or more warnings in the logs, and red indicates one or more errors in the logs.

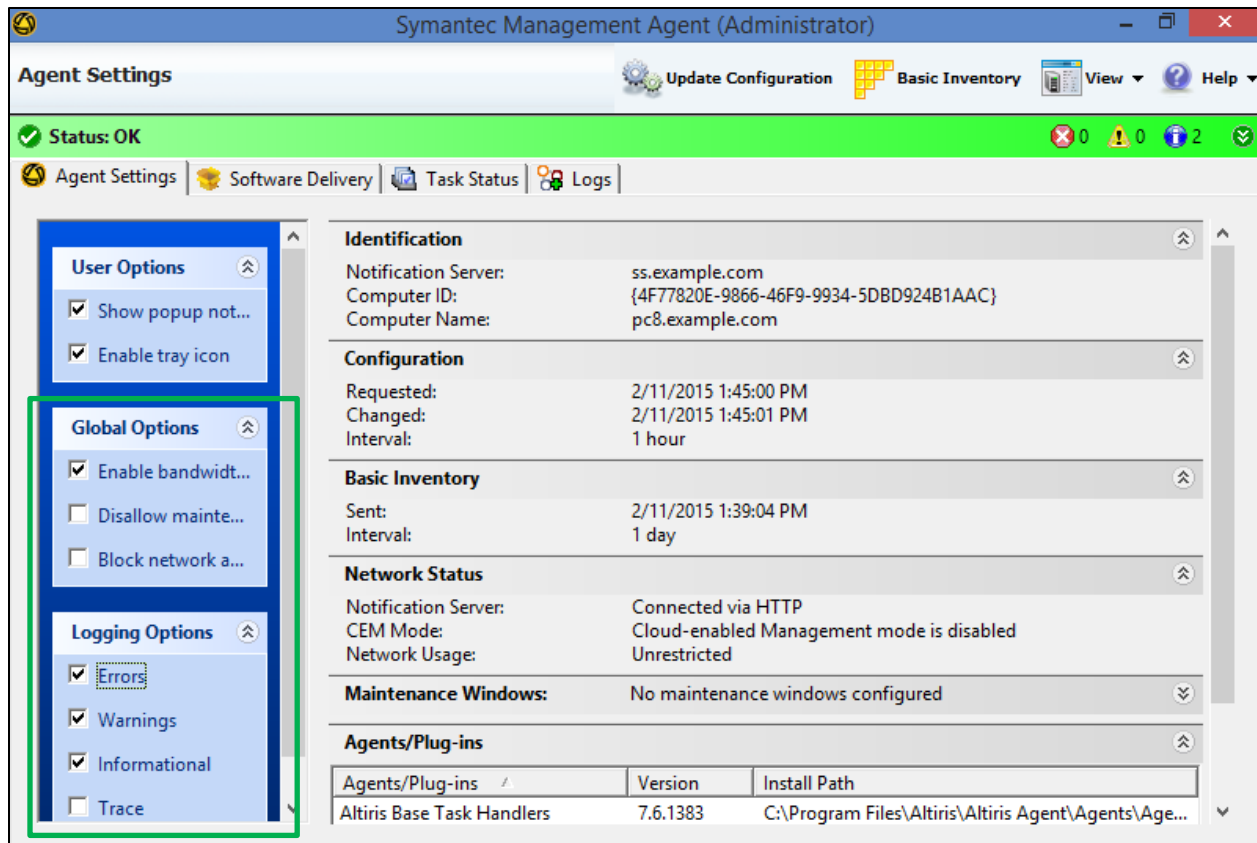
A double chevron gives access to more details regarding the agent health status.



### Administrator Privileges

If a user logs onto a client computer with a Windows administrator account, the user will see more information in the agent UI, especially if agent diagnostics are enabled, and will have more options to change the agent configuration than a standard user will. This allows technicians, for instance, to perform the following operations while preventing a standard user from doing the same:

- Enable bandwidth control
- Disallow maintenance tasks
- Block network activity
- Select the agent logging level: Errors, Warnings, Informational, and Trace



An administrator can view and modify these settings under Global Options and Logging Options. In contrast, a standard user can neither see nor make changes to them.




## Console Enhancements for ITMS Management Views

### Agent Health Tracking

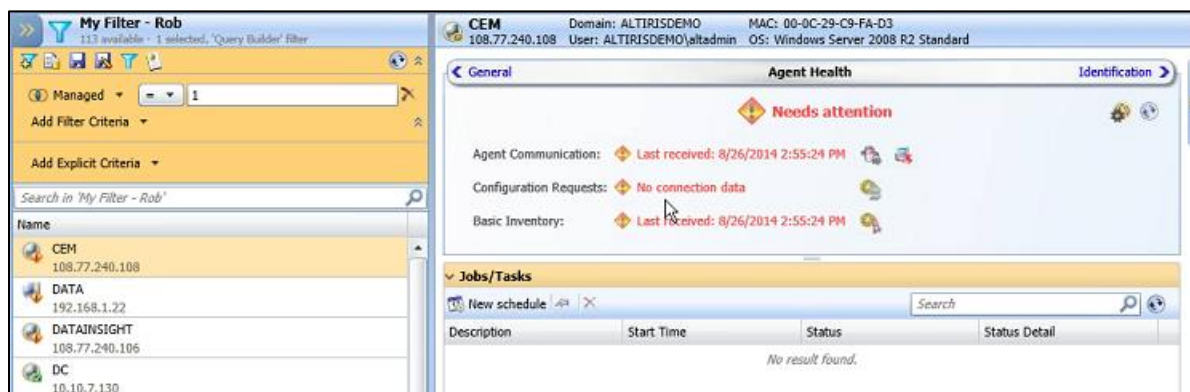
Agent health is now tracked in the console and viewable on the Manage > Computers page. Icons in the computer list indicate if an agent has a status of Healthy, Needs Attention, Untracked, or Unmanaged.

Here are examples of the Healthy and Needs Attention icons:

Healthy:  pc8  
10.10.2.100

Needs Attention:  PC1  
10.10.2.101

For each computer selected in the list, Agent Health details are viewable under a new flipbook link in the upper right-hand corner of the console.

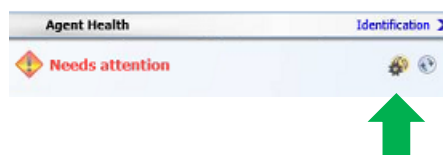


In the Symantec Management Console, agent health is calculated differently than it is in the agent UI, where health is evaluated by absence of warnings and errors in the agent logs. Within the management console, Notification Server uses three specific factors to calculate what status should be displayed for each client computer:

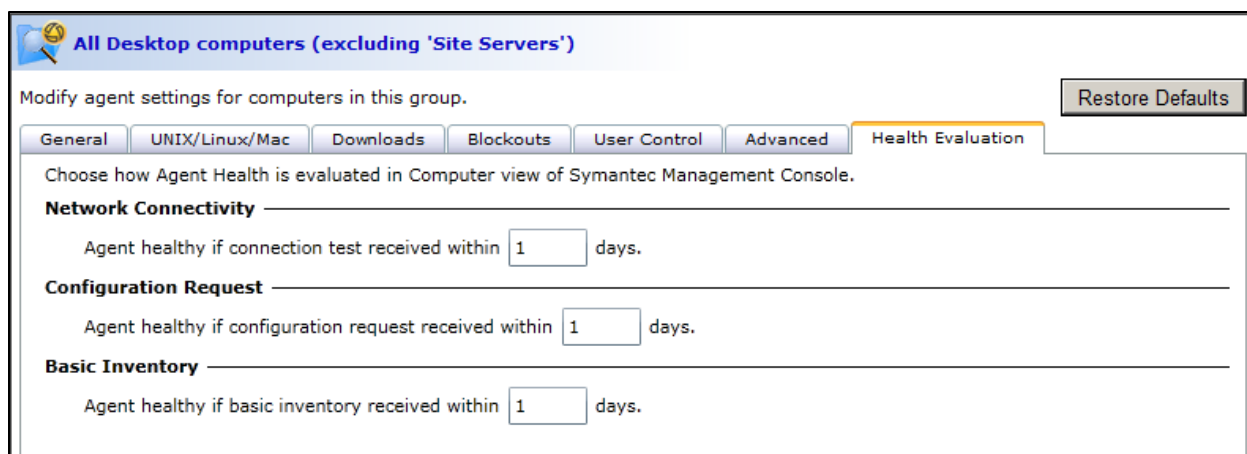
- Agent Communication
- Configuration Requests
- Basic Inventory

In the example above, the computer named “CEM” hasn’t checked in within the required interval, has failed to make a configuration request, and hasn’t sent up basic inventory within the required interval. Any one of these exceeded thresholds would generate the “Needs Attention” alert, much less all three.

Alert thresholds are set within the agent's assigned Targeted Agent Settings policy. To view these configurations conveniently, an icon has been added in the upper right corner of the Agent Health flipbook page:



When a console user clicks this icon, a separate window pops up with the Targeted Agent Settings policy for the selected agent. The policy contains a new tab for agent Health Evaluation, where an administrator can specify custom thresholds in numbers of days.



It is important to note that these thresholds are only used to calculate agent health on the management server and are not actually a setting received by the agent, unlike the other targeted agent settings. Also, because these policies are assigned to distinct groups of computers by type, different thresholds can be set for desktops versus laptops or servers. For instance, a laptop may be healthy if its agent has checked in within 5 days, where a desktop should check in every day or show an alert.

## Summary View of Agent Health

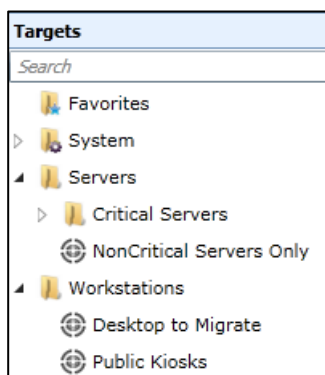
There is a new summary view for Agent Health (via the double chevrons in the center list of computers). Status types include: Healthy, Needs attention, Untracked, and Unmanaged. Clicking on any category or health status in the summary view will automatically modify the resulting computer list.



In the example above, the red portion of the Basic Inventory category of the summary view has been clicked, which caused the filter definition to change on the right, so that client computers with a status of Needs attention in the category of Basic Inventory Health are now the only computers listed in the computer list pane. Note: This is a temporary change. To modify a filter's definition permanently, the user would click the Save button.

## Target Folders

ITMS 7.5 SP1 introduced the ability to manage targets directly, in the Manage > Computers page. However, users could not create folders to help organize and manage their targets. To make target

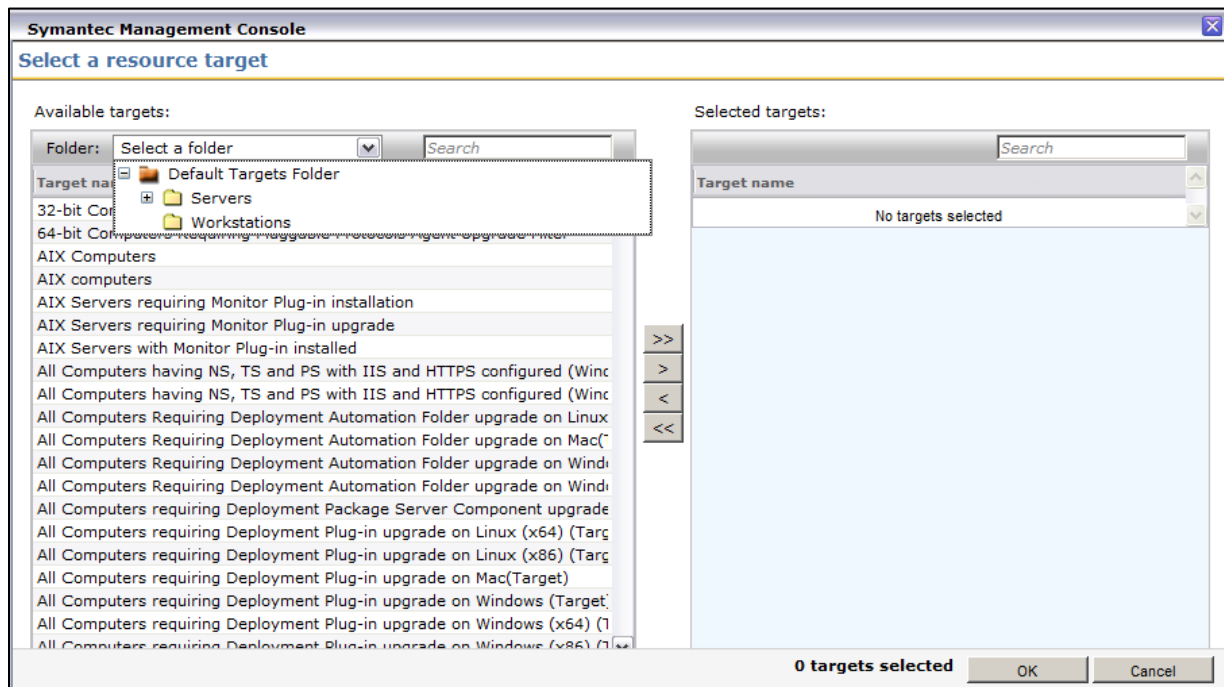


management more convenient, and to make targets vastly easier to re-use directly rather than constantly re-create, ITMS 7.6 now supports folders for targets.

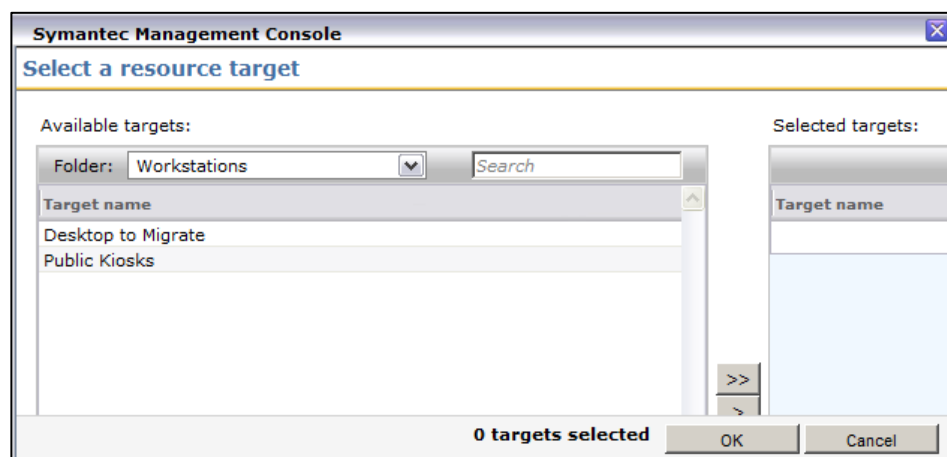
In the same way that console users can create folders and sub-folders to help secure and organize their custom filters, jobs, and tasks, users can now create folders and sub-folders to help secure and organize their targets. Target folder permissions are assigned to groups of console users

and are inherited just like other permissions in the console. Best practice is for the highest level of ITMS administrator to create target folders for general use, and lower level administrators should only create folders for personal or limited use.

In addition, a new feature has been added to the Quick Apply function for assigning policies, so that users can now browse and search for targets using the folder structure.



Using folders makes targets much easier to find and re-use.



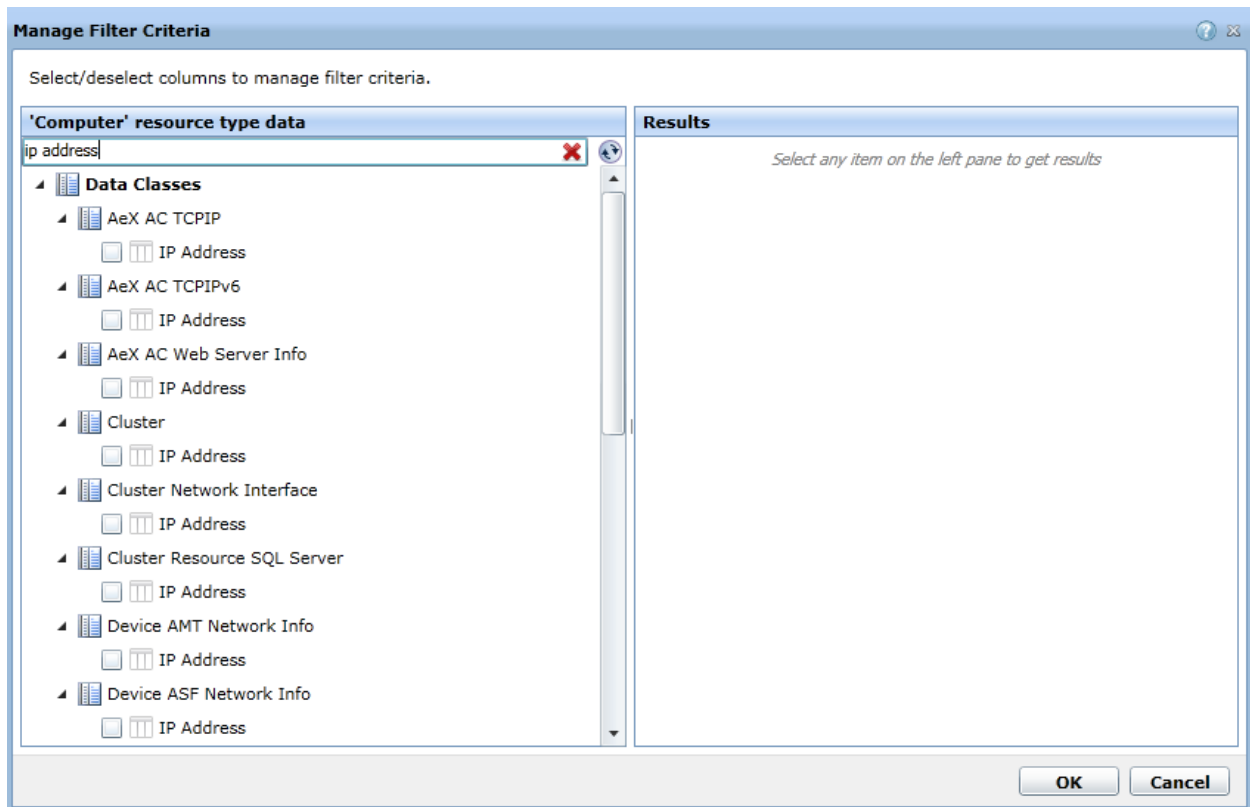
Note: the Quick Apply function for assigning targets to jobs and tasks still presents a flat list sorted alphabetically, but similar functionality for browsing target

folders is hoped to be included for jobs and tasks in a future release.

## Enhancements to Filter Criteria Management

Selecting the “Edit criteria list” link in the Filter builder of the ITMS Management Views will launch the newly enhanced Manage Filter Criteria utility. The tool includes two powerful search capabilities: one that searches by resource type (looking for a match in a data class attribute name), and one that searches for a match in data class results.

For example, a user can specify “IP address” in the search box on the left-hand side, and the search utility will recursively search all data classes and return all the classes that have “IP Address” as attributes.

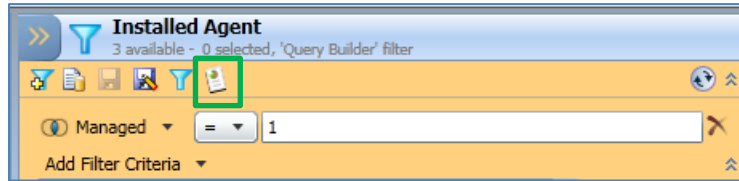


This is a significant enhancement because it means that no prior knowledge of data class names or structures is needed. A user can enter a descriptive name for the type of data desired and then use search result values on the right to help select the appropriate data class.

This utility makes it very simple for administrators to quickly validate potential filter results, and determine if a particular data class is in fact the one they want to add to the Filter Criteria list for easy usage in future filters.

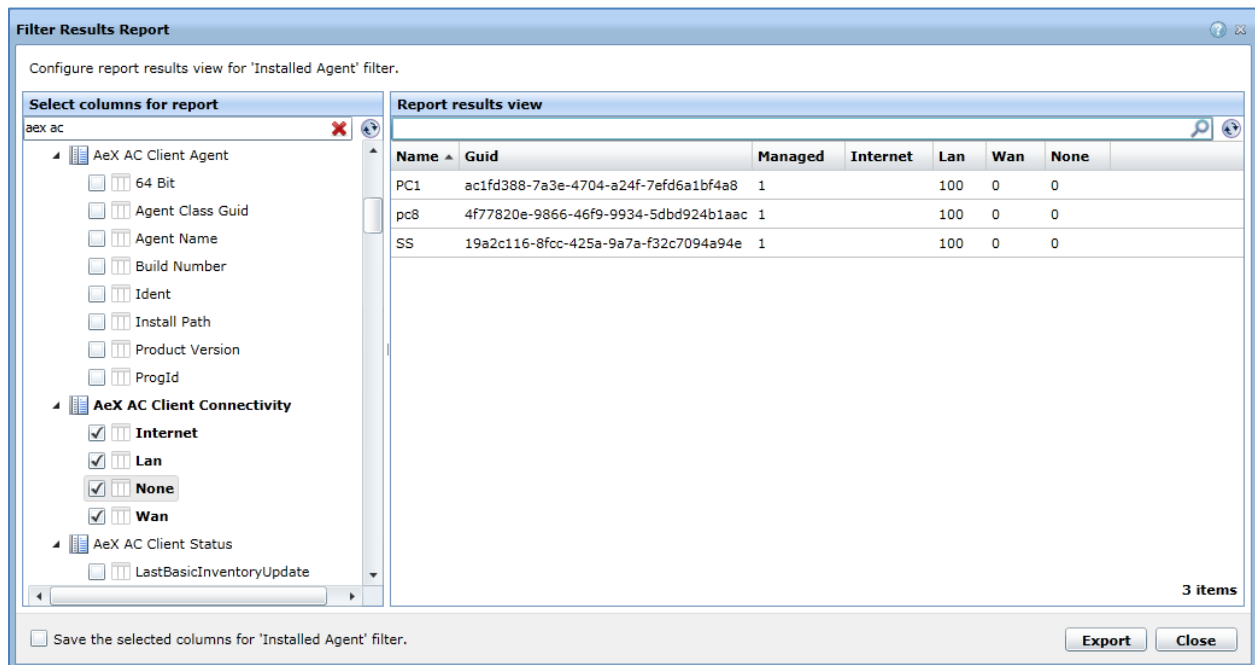
## Custom Filter Reports

The Custom Filter Reports Builder is accessed through the Manage > Computers interface via a new icon resembling a sheet of paper.



It should also be mentioned that the two Floppy disk icons represent “Save” and “Save As” functions that provides the user with consistency of functions between views, as ITMS 7.5 only had the “Save” function.

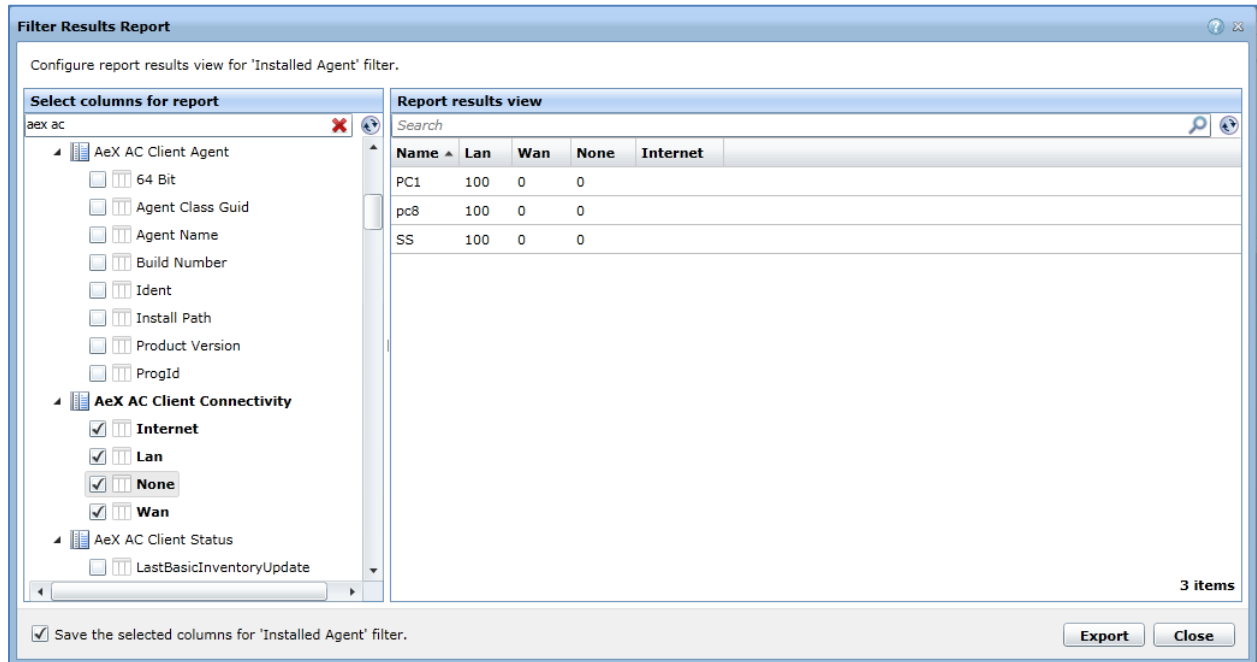
With the custom filter reports builder, a user can build out a report much more intuitively than with the standard report interface, so the builder is perfect for ad hoc data mining.



A user can drag and drop columns to change the layout, or right click a header to remove a column.

Name	Guid	Remove	Lan	Wan	None	Internet
PC1	ac1fd388-7a3e-4704-a24f-7efd6a1bf4a8		100	0	0	
pc8	4f77820e-9866-46f9-9934-5dbd924b1aac		100	0	0	
SS	19a2c116-8fcc-425a-9a7a-f32c7094a94e		100	0	0	

The results layout can be customized and saved per user.

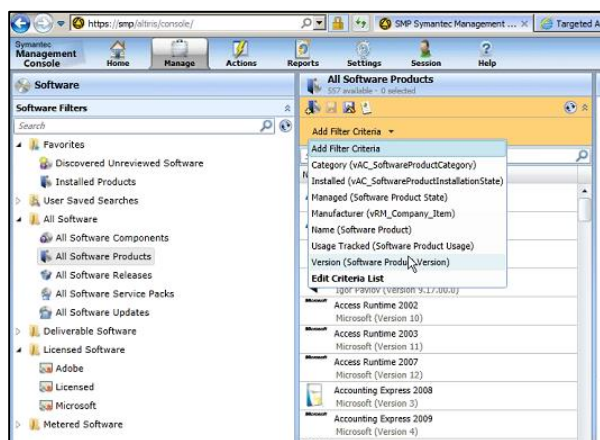
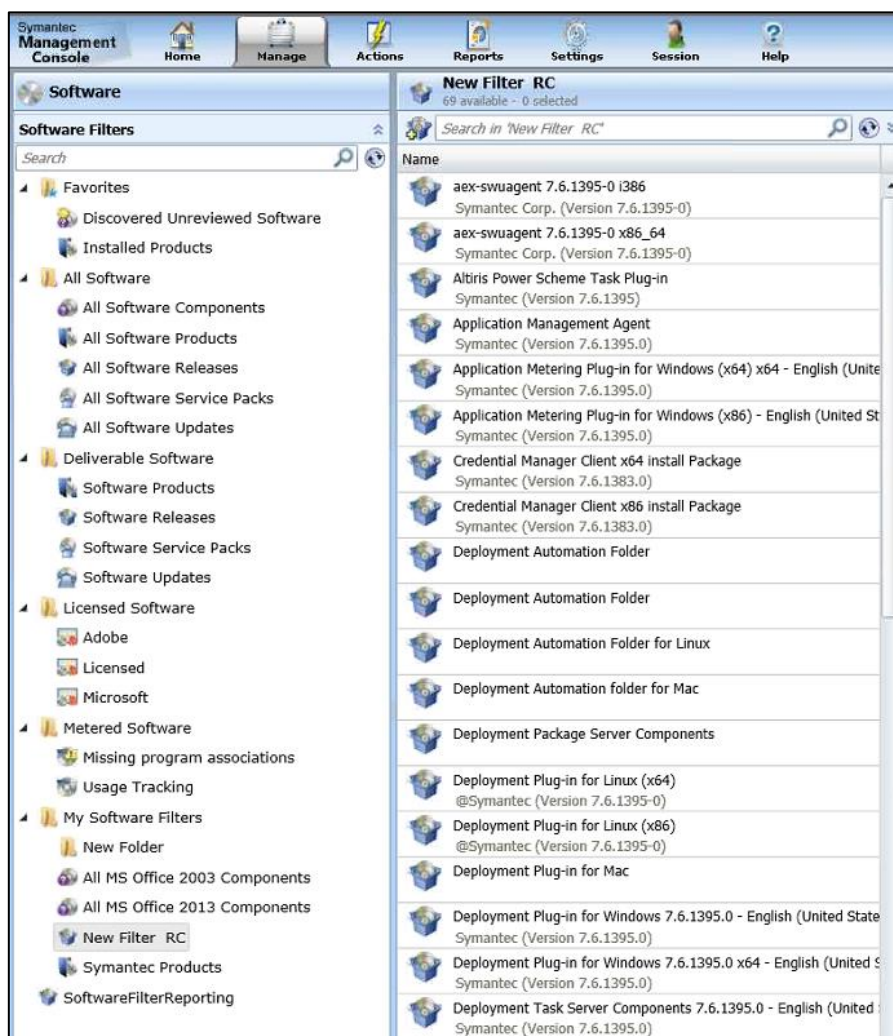


The results can also be exported to CSV and imported into a spreadsheet program for additional customization.

## Enhancements to the Software Blade

The Software blade of the 7.6 Console features many enhancements and improvements. One major change is that the left-hand side of the Software blade now presents a standard tree structure instead of the previous flat structure. Folders in the tree contain the filters that are used to organize the various types of software, such as All Software Products and All Software Releases. Administrators can create custom filters and add them to Favorites or their own custom folders.

In addition, the Software blade now has a full-featured filter builder very similar to the one in the Computers blade.



Depending on which software category is selected, the filter builder will present different options. For instance, a filter based on Software Products presents a different menu of default filter criteria from one based on Software Releases.

The Software blade also has a Filter Results Report builder, with capacity for customizing the layout and saving or exporting the results.



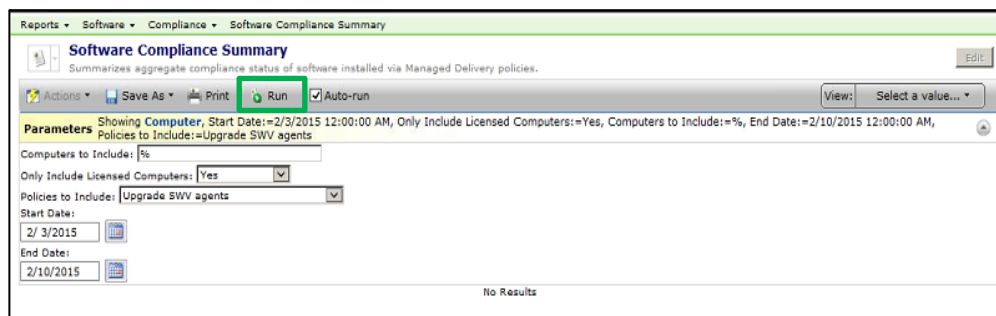
## Reporting Improvements

### New Cube Browser in IT Analytics

- Office Web Components no longer required (but still supported)
- Vastly improved performance
- Deeper drill-down capacity: go from big picture to specific detail with right click of a mouse!

### Improvements in Standard Reporting

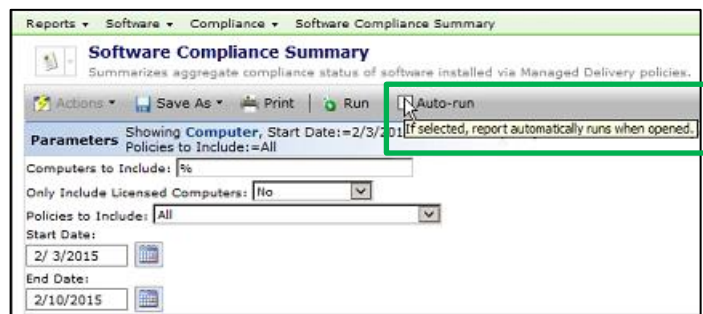
The standard report interface has a number of enhancements for better usability and performance. One new feature is that the name of the Refresh button has been changed to Run, to better inform the user what's actually happening. Also, when parameters are changed, the report will NOT automatically



refresh, but the parameters area will be highlighted in yellow to indicate that currently selected parameters are

out of synch with the currently displayed results. After Run has been clicked and the display has refreshed, this area returns to its normal blue color.

In addition, Auto Run is now a check box option at the top of every report. The default value is still set via Core Settings configuration, but can be overridden for individual reports.



Another new feature is that any editable report can now be edited by right-clicking the report name. Now users can skip executing a report, even if it is configured to Auto Run, and go straight to editing.

Lastly, the row count is now clearly visible at the bottom of the report, and much easier to view.

## Workflow 7.6 Improvements

### Active Directory Synchronization

You can connect Workflow with your entire Active Directory Forest using the '**Entire Forest**' synchronization option.

### Export/Importing of Configuration Items

Workflow 7.6 can now allow you to export and import the following items of an automation library service using Process Manager.

- [Rulesets](#)
- [SLA Levels](#)
- [Email Templates](#)

### REST API Generator

You can now generate Workflow components to call the **RE**presentational **St**ate **T**ransfer (REST) services and its methods. The new REST API generator has the following features:

- Provides HTTP header support.
- Functional HTTP methods GET, PUT, POST and DELETE that have components generated, including the ability to specify content that is sent to the server.
- Provides JavaScript Object Notation (JSON) support which lets you edit generated types

## About Symantec:

Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

Headquartered in Mountain View, Calif., Symantec has operations in 40 countries. More information is available at [www.symantec.com](http://www.symantec.com).

For specific country offices and contact numbers, please visit our Web site: **[www.symantec.com](http://www.symantec.com)**

Symantec Corporation  
World Headquarters  
350 Ellis Street  
Mountain View, CA 94043 USA  
+1 (650) 527 8000  
+1 (800) 721 3934

Copyright © 2015 Symantec Corporation. All rights reserved. Symantec and the Symantec logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners. 21355200 7/15