Symantec™ IT Management Suite 7.6 powered by Altiris™ technology

QuickStart Upgrade Guide: 7.5 to 7.6

Introduction

Symantec™ IT Management Suite 7.6 powered by Altiris™ technology is all about IT flexibility and user freedom. It provides more flexibility than ever before while giving users more freedom to choose where and how they work. IT can now securely manage remote users, rapidly deploy and support new devices, platforms, and applications while also working smarter with simplified administration and reporting tools.

This QuickStart Upgrade Guide is designed for IT professionals to outline the steps required for successful upgrade to IT Management Suite version 7.6 from version 7.5.

Server OS Considerations

Windows Server 2012 R2 is the preferred host operating system. The process of moving to Windows Server 2012 R2 might vary greatly depending on the current operating system and the chosen upgrade pathway. Use the following link to determine the optimal upgrade path: https://technet.microsoft.com/en-us/library/dn303416.aspx

Hardware Considerations

It is important to review the hardware requirements for both the SMP server and SQL Server. It is recommended that organizations larger than 5,000 endpoints dedicate separate servers for SMP and SQL. Also note that while virtual environments are supported, the overall success and performance in virtual environments depends on proper management and resource allocation to the entire ITMS infrastructure – in particular the SMP and SQL Servers.

Additional Considerations

Changes in Symantec Installation Manager

The Symantec Installation Manager (SIM) is used to install the Symantec Management Platform and IT Management Suite solutions. During the installation process, the Symantec Installation Manager verifies hardware and software prerequisites. The new SIM will ensure the following prerequisites are met for a successful migration:

- Checks whether there is sufficient OS drive space on the server to store the logs and data that is posted by the agent or Notification Server.
- Checks the database collation during an upgrade that uses an existing database. The collation for the database server and the existing database need to match, otherwise the installation cannot continue.
- Integration of the KMS store utility with the SIM. This utility can restore backed-up cryptographic keys. The KMS restore utility: \Program Files\Altiris\Symantec Installation Manager\KMSRestoreUtility\ KMS_Utility
- Integration of IT Analytics, Report Server and Analysis Server configuration through SIM. Configuration is optional and can still be done later in the management console.
- New install readiness checks are added and upgraded for ASP.NET 4.5.1, SQL 2014, WCF4.5.1, Java 8, and Migration Wizard IRC.

For more information about Symantec Installation Manager, see the Symantec Installation Manager Getting Started Guide at the following URL: http://www.symantec.com/docs/DOC6717

Legacy Agent Communication

The Legacy Agent Communication (LAC) mode allows computers that use older versions of Symantec Management Agent to communicate with the upgraded 7.6 Notification Server. This option also allows agents to be updated in phases rather than updating all of them immediately after the upgrade of Notification Server. When performing an upgrade or re-direction of agents from a 7.5 system, enabling legacy agent communication mode is required. Depending on the installation method selected within the SIM, this functionality may need to be enabled *after* 7.6 is installed. If an upgrade installation is performed, legacy communication should be enabled by default.

Cloud-Enabled Management (CEM)

Cloud-enabled Management (CEM) allows for remote endpoint management when endpoints are not connected directly to the corporate network or through VPN. This functionality helps to improve inventory, software and patch deployment coverage of mobile workforces and telecommuting employees. CEM requires fully secure communication between roaming endpoints and Notification Server(s) on the internal network and supports most ITMS solutions. CEM is supported on Windows and Mac clients only.

Clients that utilize Cloud-enabled Management are required to use SSL. SSL communications are required between the SMP, the Internet Gateway and the CEM endpoint. This does not mean all clients are required to use SSL. While enabling all clients to utilize SSL may be easier, it may also increase processing of SSL based communications. It is possible to configure an explicit group of CEM clients for SSL while allowing others to communicate over regular http. This requires multiple client policies – at least one for CEM based endpoints requiring communications via https and one for non-CEM based endpoints allowing for http communications. To allow both http and https traffic to the SMP server, perform the install in SIM without the https/ssl required option.

Internet Gateway

Symantec recommends having at least two Internet gateways to provide failover options, load balancing, and to maintain communication continuity. Each Internet gateway can serve multiple Notification Servers. This configuration is supported even if Notification Servers are organized in a hierarchy. Each Internet gateway supports 1- 60,000 endpoints and 3,000 concurrent connections. Installing Internet Gateway on a virtual computer is not recommended. Running Internet gateway on virtual hardware can lower its scalability by up to 40%.

Site Server Services

Consider deployment locations for site server services. In ITMS 7.6 it is possible to install individual services, such as task, package and NetBoot service (NBS/PXE). A general recommendation is to consider concentrating task services in a central location while deploying package and NBS services to locations in closer proximity to managed endpoints. As an example, NBS services require traffic forwarded between subnets if the NBS services are not on the same network segment as the computer PXE booting.

Mac Management

In order to perform Mac management, OS X Server Tools as well as an OS X source computer are required to create NetBoot and NetInstall packages. Once these are created NBS services are utilized for imaging and installation tasks.

System Requirements

For complete details on platform and OS support, please review the Platform Support Matrix.

Management Server OS

Windows Server 2008 R2, 2008 R2 SP1
Windows Server 2012 R2
VMware ESX 3.5, 4.0, 5.0, 5.1, ESXi 5.5
Windows Hyper-V Server 2008 R2, 2012
Microsoft SQL Server 2008 SP2, 2008 SP3
Microsoft SQL Server 2008 R2, 2008 R2 SP1, 2008 R2 SP2
Microsoft SQL Server 2012
Microsoft SQL Server 2014

Management Server Software

- Microsoft IIS 7.5 (IIS 6 compatibility), Microsoft IIS 8.5 Native
- Java 8
- Microsoft Internet Explorer: 7, 8, 9, 10, 11
- Microsoft .NET Framework 4.5.1
- Microsoft Silverlight 5.0

Workflow Server

- Windows Server 2008 R2, 2008 R2 SP1 (64-bit only)
- Windows Server 2012 R2

Agents

The following applies to Client Management Suite and Server Management Suite. Asset Management Suite does not have an agent.

Windows Agent

- Windows 8, Windows 8.1
- Windows 7, Windows 7 SP1, Windows 7 Embedded SP1
- Windows Vista SP2
- Windows XP SP3 (x86), Windows XP SP2 (x64)

- Windows Server 2003 SP2 or later
- Windows Server 2008, 2008 R2, 2008 R2 SP1
- Windows Server 2012, 2012 R2
- Windows Hyper-V Server 2008
- Windows Small Business Server (SBS) 2003 R2, 2008

Mac Agent

- OS X 10.8, 10.9, 10.10
- OS X Server 10.9, 10.10

Linux Agent

- Red Hat Enterprise Linux Desktop: 5.10, 6-6.5, 7(partial)
- Red Hat Enterprise Linux Server: 5.10, 6-6.5, 7(partial)
- SUSE Linux Enterprise Desktop: 10, 11, 11 SP1, 11 SP2
- SUSE Linux Enterprise Server: 10, 11, 11 SP1, 11 SP2
- VMware ESX/ESXi (agentless): 3.5, 4.0, 4.1, 5.0, 5.1, 5.5

UNIX Agent

- IBM AIX 5.2, 5.3, 6.1, 7.1
- HP HP-UX 11i (PA-RISC), 11i v2 (PA-RISC), 11i v3 (PA-RISC /IA-64)
- Oracle Solaris 9 (SPARC), 10 (SPARC/x86/x64), 11 (SPARC/x86/x64)

Minimum Hardware Recommendations

Symantec Management Platform

SMP Hardware:

Component	Evaluation	100-1,000 endpoints	1,000 – 5,000	5,000 – 10,000	10,000 - 20,000
Processors	Two Cores\2.4 Ghz or more	Eight Cores\2.4 Ghz or more	Eight Cores\2.4 Ghz or more	Eight Cores\2.4 Ghz or more	8-12 Cores\2.4 Ghz or more
Disk Speed (in IOPS)	180 – C: OS, SMP	180 – C: OS, SMP	180 – C: OS, SMP	180 – C: OS 130 – D: SMP	180 – C: OS 130 – D:SMP 130 – E:Storage
Disk Capacity	80GB	80GB	200GB	400GB	600GB

SMP Hardware (continued):

Component	Evaluation	100-1,000 endpoints	1,000 – 5,000	5,000 – 10,000	10,000 - 20,000
RAM	4GB	8GB	16GB	16GB	16GB
Cache	6MB L2 or More				
Network	Dual Gigabit – Load Balanced				
OS	Windows Server 2012 R2 Enterprise				

SMP Server Software:

Component	
OS	Recommended: 2012 R2 Standard or Enterprise Alternative: 2008 R2 Standard or Enterprise (SP1 Supported)
IIS	On 2012 R2: 8.5 Native On 2008 R2: 7.0 + 6.0 compatibility
.NET	4.5.1
IE	Internet Explorer

Service Account:

Domain Account	Local Admin
Altiris Service Account	Local Admin on the Symantec Management Platform. It is also Beneficial for the account to be a Local Admin on site Servers, however that is not a Requirement.

SQL Hardware:

Processors	Evaluation	100 – 1,000 endpoints	1,000 – 5,000	5,000 – 10,000	10,000 – 20,000
Processors	Two Cores/2.4Ghz or More	Four Cores/2.4Ghz or More	Eight Cores/2.4Ghz or more	8-16 Cores/2.4Ghz or more	16 Plus Cores/2.4Ghz or more
Disk Speed (IOPS)	180 - C: OS, SMP 200 – D:SQL	180 - C: OS, SMP 200 – D:SQL	180 - C: OS, SQL App 300 - D: SQL DB 300 - E: Logs 200 - F: TempDB	180 - C: OS, SQL App 400 - D: SQL DB 400 - E: Logs 300 - F: TempDB	180 - C: OS, SQL App 600 - D: SQL DB 600 - E: Logs 400 - F: TempDB

SQL Hardware (Cont'd)

RAM	**Evaluation**	**100-1,000 endpoints**	**1,000 – 5,000**	**5,000 – 10,000**	**10,000 -20,000**
RAM (GB)	16 GB	16 GB	16+ GB	24+ GB	32+ GB
Drives	**Disk Configuration**	**IOPS**	**Write %**	**Read %**	**Drive Size**
Operating System Drive	RAID 1 (Mirrored)				
CMDB Drive	RAID 10 or RAID 0+1	250	98%	2%	=>5-8 MB Per Client
TempDB Drive	RAID 0 (Striped)	2	49%	51%	=>10% of CMDB
Transaction Log Drive	RAID 10 or RAID 0+1	600	100%	0%	=>10% of CMDB

SQL Software:

Evaluation	**100-1,000 endpoints**	**1,000 – 5,000**	**5,000 – 10,000**	**10,000 -20,000**
Microsoft SQL Server Express 2008 SP2 or higher, 2012, 2014.	Microsoft SQL Server 2008 SP2 or higher, 2012 or 2014 Standard or Enterprise. On-box SQL is supported; off-box SQL is recommended.		Microsoft SQL 2008 SP2 or higher, 2012 or 2014 Standard or Enterprise. Symantec recommends off-box SQL.	

Site Server – Package / Site / PXE

SS Hardware:

Component	**10-100 endpoints**	**100 – 1,000**	**1,000 – 5,000**	**5,000 - 7500**
Operating System	Desktop / Server OS	Server OS	Server OS	Server OS
Processors	One core	Two cores	Four cores	Four cores
Disk Capacity	100 GB – 250 GB	100 GB – 250 GB	100 GB – 250 GB	100 GB – 250 GB
RAM	4	4	4-6 GB	4-8 GB

SS Software:

Component	
OS	XP x86/x64 SP2 + Vista x86/x64 SP2 + Win 7 x86/x64 2008 SP1 +, 2008 R2 + 2012 R2
.NET	4.5.1
IIS	IIS 7 with IIS 6 compatibility components
IE	Internet Explorer

Internet Gateway:

Component	Requirement
OS	Windows 20012 R2 SP1
Processors	Dual Core CPU
RAM (GB)	8 GB
Disk Capacity	At least 40GB

Migration Paths

For more information about upgrade path requirements and the recommended upgrade paths visit:
http://www.symantec.com/docs/DOC7718

On-Box Upgrade

Notification Server must first be updated to the latest version including service packs and hot fixes. On-box upgrades require upgrading to ITMS 7.5 SP1 HF5 before upgrading to ITMS 7.6.

Off-Box Migration

Follow all recommendations and requirements to install IT Management Suite 7.6 on new server hardware or a new operating system. Then follow the migration steps to backup and restore the ITMS 7.5 data to the new server.

Migration Tips

Use a test environment

Before installing Symantec Management Platform 7.6 in a production environment, upgrade the test environment for evaluating and validating the entire installation and migration process. Symantec recommends maintaining a test environment for ongoing validation.

Naming the New Hardware

Symantec recommends using the same server name and IP address for the new server so clients can easily connect once the migration is complete.

Make note of all configuration settings before migrating

Examples to document before the migration process include:

- All Task Server settings
- All agent communication settings
- All policy refresh settings
- All membership update settings

After a successful migration use these settings to configure the new environment.

Ensure that Legacy Agent Communication (LAC) mode is enabled

To allow complete management of legacy agents when the upgrade is in progress, ensure that Legacy Agent Communication mode is enabled.

Manually Migrating Data

Always store backups in an accessible, secure location. Some data must be manually migrated for the following products:

- Inventory Solution
- Software Management Solution
- Barcode Solution
- Real-time System Management Solution
- Real-Time Console Infrastructure Solution

Migrate to New Hardware

Upgrading and/or Migrating to ITMS 7.6 provides an opportunity to upgrade server hardware and the operating system. If ITMS 7.5 is installed on hardware meeting ITMS 7.6 requirements, ITMS 7.6 can be installed on the same server. However, before installing the new operating system, important and specific migration steps must be completed. Consider new hardware to ensure current best practices are met and migration is successful.

Upgrading the Agent

After upgrade to Notification Server 7.6, upgrade the Symantec Management Agent (SMA) on the client computers to SMA 7.6. Also upgrade the solution plug-ins to the same version of the SMA. An older version of SMA can communicate with a latest version of SMP using the Legacy Agent Communication (LAC) mode, but Symantec recommends upgrading the SMA and the solution plug-ins to the latest version. Ensure that the SMA and solution plug-ins are always of the same release version for best results.

Hierarchy Migration

Before installing ITMS 7.6, verify the database collation on all the servers that might participate in Notification Server hierarchy. Hierarchy is not supported on the servers that have different database collation on parent Notification Server and child Notification Server.

Replication cannot be enabled during an upgrade. See the instructions in this article for details on disabling replication before continuing: http://www.symantec.com/docs/HOWTO44016

If migrating into a hierarchy, map out which clients will be managed by which SMP servers. In some environments it may be as simple as pointing one 7.5 Notification Server's clients to a specific 7.6 server. Additional logic and policies will be required to migrate clients to specific SMP servers. Typical scenarios include assigning a client's 7.6 SMP based on geographical proximity.

Symantec recommends upgrading the child Notification Servers first, and then upgrading the parent Notification Server. For information about upgrading Notification Servers in a hierarchy, see the knowledge base article: http://www.symantec.com/docs/HOWTO21657

Distributed Component Object Model (DCOM) service

Before beginning the upgrade process, ensure that the Distributed Component Object Model (DCOM) service is enabled on the computer. If the DCOM service is disabled, the Windows Management Instrumentation (WMI) connection fails on the server. If a version of pcAnywhere prior to version 7.1 SP2 is currently installed, the latest version will modify the registry disabling DCOM services. Therefore, the WMI connection fails on the server. For more information on disabling DCOM services visit: www.symantec.com/docs/TECH109673

IIS Application Pools

Ensure that all application pools that were separated in 7.5 for any solution is reverted back to its default configuration in IIS. For more information on reverting application pools visit: http://www.iis.net/configreference/system.applicationhost/applicationpools/applicationpooldefaults

Altiris Log Viewer & SMP Diag

Resolve any errors before upgrading to ITMS 7.6.
For more information on using Altiris Log viewer visit: http://www.symantec.com/docs/HOWTO75156
For more information on using SMP Diag visit: http://www.symantec.com/docs/TECH202997

ITMS 7.5 to ITMS 7.6 On-box Upgrade Steps

1. Back up the 7.5 Notification Server
2. Back up the 7.5 Notification Server Database (CMDB)
3. Click Start > All Programs > Accessories > System Tools > Task Scheduler > Microsoft. Select the task NS package refresh and click Run
4. Disable all agent and plugin installation and upgrade policies for Clients and Site Servers
5. Open the Symantec Installation Manager located in the Start menu under Symantec > Symantec Installation Manager
6. To upgrade installed products to the IT Management Suite 7.6, click Upgrade installed products
7. On the “Upgrade Installed Products” page, in the “Upgrade to product version” drop-down list, click 7.6, and then click Next
8. On the “End User License Agreement” page, check “I accept the terms in the license agreements,” and then click Next
9. On the “Contact Information” page, verify or modify the contact information, and then click Next
10. On the “Install Readiness Check” page, resolve the requirements that are marked with a red icon, and then click Next
11. Review the Installation Summary
12. Click Begin install to start the upgrade
13. (If applicable) Turn hierarchy and replication back on.
14. Click Start > All Programs > Symantec > Diagnostics > Altiris Log Viewer to open the Log Viewer. Check Symantec logs for errors or warnings and resolve them.
15. Perform a database defragmentation of the Symantec CMDB database
16. Update Site Server Agents and plugins.
    a. Enable SMA install and upgrade policies
    b. Enable all Site Server plugin install and upgrade policies
17. Update client Agents and plugins
    a. Clone Upgrade policies, agent and plugin, and enable them for a test group of machines
    b. Verify that test group has upgraded successfully
    c. Enable original upgrade polices for agents and plugins
    d. Enable agent install and upgrade policies.

Additional ITMS 7.5 to ITMS 7.6 Off-box Migration Steps

1. On the 7.5 ITMS server, open the Symantec Installation Manager located in the Start menu under Symantec > Symantec Installation Manager
2. Select Install optional components
3. Install and run the Migration Wizard Components option
4. Use the Migration Wizard to export the desired ITMS data
5. Install the Symantec Installation Manager, including the Migration Wizard, on the new ITMS 7.6 server
6. Restore the exported CMBD to a new SQL server if necessary
7. Import the exported ITMS data using the migration wizard
8. Manually copy any remaining solution data to the new ITMS server
9. Check the Agent Registration Status Report to ensure agents are communicating correctly with the new ITMS server

Migration Notes

Required version of Notification Server 7.5

Notification Server must be updated to 7.5 SP1 HF5 before migrating from ITMS 7.5 to ITMS 7.6. Upgrade to 7.5 SP1 HF5 prior to beginning 7.6 upgrade activities. For example, if 7.5 SP1 is installed, an upgrade to 7.5 SP1 HF5 is required before migrating to ITMS 7.6.

Database and server backup

Before beginning the migration, back up the 7.5 Notification Server Database (Symantec_CMDB) and the 7.5 Notification Server data to an accessible and secure location. If problems occur during the migration process, simply revert to these backups. Making backups before major migration steps provides more granular recovery options from any issues or unplanned outages that might occur during the migration process.

Product Parity

Before beginning the migration, create a list of the ITMS 7.5 products currently installed. When installing the ITMS 7.6 products, install at minimum the equivalent products installed on ITMS 7.5.
Warning: Failure to have minimum product parity can result in the inability to migrate 7.5 data to the 7.6 database.

Server name and IP address

Assign the same hostname and IP address to the ITMS 7.6 server when migrating to new server hardware.

Mixed mode

Symantec Management Platform 7.6 does not support mixed mode. A Symantec Management Platform 7.5 server cannot communicate with a Symantec Management Platform 7.6 server.

Gotchas

PXE (NBS)

PXE (NBS) service names changed in ITMS 7.5. Jobs to restart these services may need to be recreated.

Cloud Enabled Management

- (CEM) requires HTTPS and the use of SSL certificates. These can be self-signed, third-party commercial or internally issued using a Certificate Authority. In all cases the certificates must be trusted by all cloud-enabled endpoints for a successful CEM deployment.
- External remote package servers for CEM may require name changes to match the internal DNS names.
- The CEM Package Server publishes https codebases using the internal FQDN- http://www.symantec.com/
- Certificates can only be issued for publicly resolvable domains.

  Example, Company XYZ owns xyz.com, but uses xyz.local inside the corporate network. A certificate for cem.xyz.local cannot be purchased or issued as it will not be resolvable to the cloud-enabled agent.

Individual Solutions

When upgrading to ITMS 7.6, any solutions that has not yet released a new product version (i.e. - Mobile Management), will be uninstalled if the upgrade is allowed to proceed.

A warning message may appear in the SIM indicating a simultaneous upgrade of ServiceDesk is required. For more information visit: http://www.symantec.com/docs/TECH200807

Patch Management Import requires ICMP request to access solutionsam.com (if proxy being used). If ICMP traffic cannot reach solutionsam.com, Patch Management Import will fail.

Out of Band Management (OoB)

This product is no longer bundled with ITMS. The latest OoB component can be obtained directly from Intel at http://www.intel.com/go/scs. Although the OoB provisioning component is no longer bundled, existing RTSM features will continue to function on supported AMT computers. When upgrading from previous versions of ITMS, the OoBRemover utility performs a removal of OoB items from the Notification Server and Site Servers. The Intel SCS/RCS database will remain and provisioned computers will be unaffected by the OoBRemover utility. The Symantec OoB discovery tool can then be used to populate provisioned computers into the CMDB.

Helpful Links

- Symantec IT Management Suite 7.6 Documentation: http://www.symantec.com/docs/DOC8146
- IT Management Suite 7.6 Planning for Implementation Guide: http://www.symantec.com/docs/DOC8038
- IT Management Suite 7.6 Installation and Upgrade Guide: http://www.symantec.com/docs/DOC8039
- Symantec Connect page: http://www.symantec.com/connect/endpoint-management
- Knowledge Base: http://www.symantec.com/page.jsp?id=support-knowledgebase
- SQL 2008 Optimizing: http://www.symantec.com/business/support/index?page=content&id=HOWTO8589
- Software Replicator Tool: http://www.symantec.com/.../index?page=content&id=TECH166711
- Symantec Management Platform Support Matrix: http://www.symantec.com/docs/HOWTO9965