Symantec Corporation
IT Management Suite (ITMS)

Symantec ITMS 8.1
Upgrade Methodology

Document Control Page

Revision History

Version	Date	Changes	Author
1.0	05/04/17	Published Version	Symantec

Document Configuration

Title	Symantec ITMS 8.1 Upgrade Methodology
Author	Ian Atkin
Date of Creation	11/04/17
Owner	Ian Atkin
Distribution	Publicly Available

Related Documents

Name	Description	Version
ITMS Platform Support Matrix		
ITMS Planning for Implementation Guide		7.5 / 8.0

Table of contents

Introduction

This run book details the steps taken to fully upgrade a Symantec Management Platform implementation. The environment targeted for the upgrade was licenced for 5000 nodes and consisted of the following components:

1. One SMP Server
2. One back-end SQL Server
3. One Site Server
4. One Cloud Gateway

Upgrade Overview

Symantec's IT Management Suite (ITMS) is a highly functional endpoint management product. It possesses numerous infrastructure scaling features to assist organisations with complex network and use-case requirements. Using these however can be a double-edged sword. The more complex the configuration of your management components, the more necessarily complex your subsequent infrastructure upgrades will be. Upgrades should therefore be executed with a level of care that is appropriate to both your infrastructure complexity and the implementation's business criticality.

Our infrastructure configuration is not uncommon in the ITMS world; a few thousand nodes, a SMP (Symantec Management Platform), a site server and a cloud gateway. We are fairly mature ITMS customers and have over the years gained a lot of experience in what works well for our environment upgrades. To give you an idea of the time scales behind our SMP upgrades, we anticipate each major upgrade taking one Altiris Administrator a month. This breaks down as nearly 4 weeks of preparation, a day upgrading the live infrastructure, and a day of acceptance testing.

Like many enterprise customers, before any of our upgrades can be signed off from a change management perspective, we are required to put in place a robust 'rollback' plan. To facilitate this, the Altiris infrastructure is firewalled off from client access throughout most of the upgrade window. This keeps the upgrading environment encapsulated, permitting a seamless rollback in the unlikely event of unresolvable issues arising. As a side note, in the 6 or more years that we've had this style of upgrade plan in place, we've never had to rollback and reschedule an ITMS infrastructure upgrade.

Following the upgrade of our SMP infrastructure components, we execute acceptance testing plans. Should these pass, the firewalls on the SMP, Site Server and Internet Gateway are opened up in stages to allow communication with our client estate. From this point, agents and plugins will being their rollout. The client connection profile of our estate means that we expect 60% of clients to upgrade within the first 24hrs.

This article runs through our upgrade process, and hope this will assist other Altiris Administrators out there who are considering their upgrade plans. The key takeaway is that the bulk of our upgrade work is spent in preparation. This slashes the risk of unexpected events occurring on upgrade day, and assists a smooth upgrade execution. This upgrade methodology underpinned our 7.5SP1 to 8.0 upgrade (which we detailed on Symantec Connect[1]) as well as our more recent server management infrastructure upgrade of 8.0 to 8.1.

I find it useful to consider 3 distinct phases to *any* upgrade. For the ITMS this tends to looks like:

- Preparation (~1 month)
- Upgrade (1-2 days)
- Wash-up/Remediation (1 week)

The *preparation* phase is all about making sure we are satisfied that our current setup is well documented and upgrade-ready. Spending time here not only reduces the chances of things going awry on upgrade day, but it also reduces the issues to tackle in the final *wash-up*.

The thinking here is simple –spend resource in the first phase in a *planned* manner. This massively reduces the risk of us spending a lot of *unplanned* resource in the upgrade and remediation phases should things go awry.

Preparation

This is where most of the effort in an upgrade goes. And we do this because we want to minimise upgrade stress and the time spent in the post-upgrade wash-up. It's a pain to do, but, it is certainly worth it. The following sections cover the items we aim to accomplish before upgrading to a new ITMS release.

[1] http://www.symantec.com/connect/articles/upgrade-experience-itms-75sp1-80

1.1 Build new virtual server and install the target version of ITMS

When we plan to upgrade to the next version of ITMS, we want to play with that version in advance and check out its features. This is simplest to accomplish on a new virtual server. Once built, we complete the following tasks:

1. Check basic functionality of the server, check stability, confirm standard processes. We do lots of log checking here and are prepared to raise Symantec Support cases.
2. Check target version release notes – there might be "known issues" which are relevant to our environment.
3. Document changes that will occur in our environment as a result of the upgrade.

The objective here is to confirm that the target version works with our current processes. It's also useful as it helps familiarise ourselves with new features that could be leveraged following the upgrade.

1.2 Test the ITMS Upgrade

If the previous testing reveals no show stoppers, it's time to consider testing an upgrade on a server that *closely matches* our production environment.
The optimal way to test an upgrade is to see if we can recreate a true copy of our SMP infrastructure in a development environment. We can then execute the upgrade on a mirror copy of the SMP. This will likely draw out most of the upgrade challenges. It is especially important to execute those 'day-to-day' tasks that your common SMP roles undertake to ensure there are no upgrade surprises.

With the best will in the world though, we can't always create an exact copy of our infrastructure. If we happen to hit a perfect-storm regarding our virtual machine management, we proceed by building a fresh ITMS server that matches our *current* production version. We configure the core policies to mirror our production box, and then upgrade this implementation. Anything is better than nothing.

1.3 Other Preparation Tasks

In the weeks before the upgrade we also do the following:

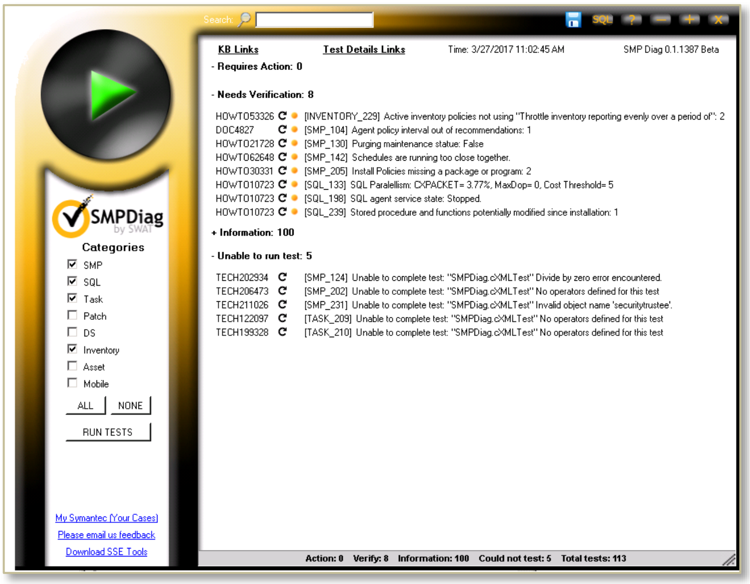
1. **Spend additional time attending to your *live SMP***

   We want to be happy with the state of the event logs (both the Windows logs and the Altiris Log Viewer). In general, we want to be confident with the current functioning of our server and client estate. When we upgrade the SMP, we want to ensure it's in *prime* condition.
   As the upgrade process will work the SMP quite hard we also consider at this stage if any hardware upgrades (CPU, RAM, disk) are appropriate and schedule these into the upgrade plan.

2. **Run *SMPDiag***

   This little utility can be downloaded from the Symantec support site. It will give useful tech note details for any items needing action. Make sure you resolve any items that "Require Action".

   https://support.symantec.com/en_US/article.TECH202997.html



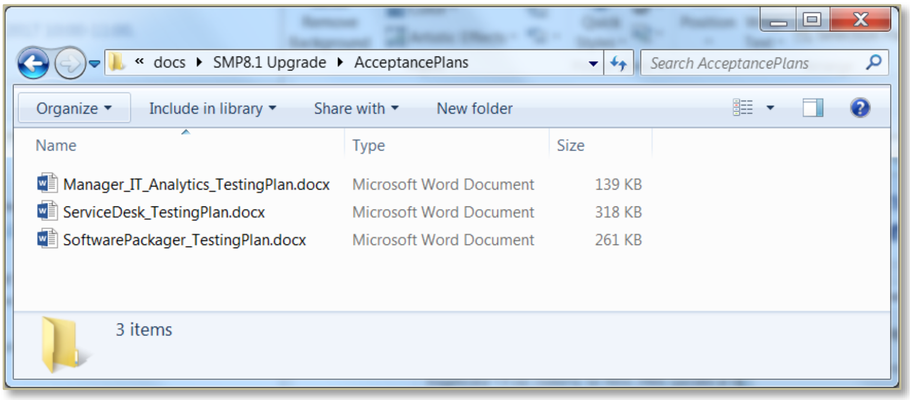
Categories

☑ SMP
☑ SQL
☑ Task
☐ Patch
☐ DS
☑ Inventory
☐ Asset
☐ Mobile

```
KB Links          Test Details Links          Time: 3/27/2017 11:02:45 AM          SMP Diag 0.1.1387 Beta
- Requires Action: 0

- Needs Verification: 8
 HOWTO53326  [INVENTORY_229] Active inventory policies not using "Throttle inventory reporting evenly over a period of": 2
 DOC4827     [SMP_104] Agent policy interval out of recommendations: 1
 HOWTO21728  [SMP_130] Purging maintenance statue: False
 HOWTO62648  [SMP_142] Schedules are running too close together.
 HOWTO30331  [SMP_205] Install Policies missing a package or program: 2
 HOWTO10723  [SQL_133] SQL Paralellism: CXPACKET= 3.77%, MaxDop= 0, Cost Threshold= 5
 HOWTO10723  [SQL_198] SQL agent service state: Stopped.
 HOWTO10723  [SQL_239] Stored procedure and functions potentially modified since installation: 1
+ Information: 100

- Unable to run test: 5
 TECH202934  [SMP_124] Unable to complete test: "SMPDiag.cXMLTest" Divide by zero error encountered.
 TECH206473  [SMP_202] Unable to complete test: "SMPDiag.cXMLTest" No operators defined for this test
 TECH211026  [SMP_231] Unable to complete test: "SMPDiag.cXMLTest" Invalid object name 'securitytrustee'.
 TECH122097  [TASK_209] Unable to complete test: "SMPDiag.cXMLTest" No operators defined for this test
 TECH199328  [TASK_210] Unable to complete test: "SMPDiag.cXMLTest" No operators defined for this test

Action: 0   Verify: 8   Information: 100   Could not test: 5   Total tests: 113
```

3. **Gather Testing Documentation**

   In our previous round of upgrades, we gathered "Acceptance Testing" documentation from the user groups that leverage the SMP console. We agreed which functions had to be operational immediately following the upgrade, and those which could fail as long as they were resolved within an agreed timespan. This is important as we needed to know what issues should trigger an infrastructure rollback should they not be operational by the end of the upgrade window.



Name	Type	Size
Manager_IT_Analytics_TestingPlan.docx	Microsoft Word Document	139 KB
ServiceDesk_TestingPlan.docx	Microsoft Word Document	318 KB
SoftwarePackager_TestingPlan.docx	Microsoft Word Document	261 KB

3 items

4. **Build the Upgrade Checklist**

   We don't 'wing it' on upgrade day. We build a checklist, and think about back out plans for each step that introduces a change. We create a simple spreadsheet of actions and have a column specifying where we’re at with each one. We update this as we proceed and this seems to serve us pretty well.

5. **Formally Schedule the Production Server Upgrade**

   We let people know we are planning the upgrade and inform them of the schedule and anticipated downtime. We point them to relevant documentation such as the back out plan, the changes, and give an indication of how long the client upgrade process will take (we aim for 75% coverage in 3 days). To simplify scheduling, we tend to plan our upgrades over a weekend to minimise customer impact.

Upgrade

On the morning of the upgrade, we confirm the *completeness* of our checklist one last time. We recheck the release notes for the version we are upgrading to (as they could have been updated). If all looks good, we take a breath and continue.

At a high level, our upgrade plan will follow these basic steps:

Step	Details
1. Quiesce infrastructure and snapshot the Environment	This puts the infrastructure in to a state that enables us to execute a rollback plan if required. This means firewalling off clients from the server, checking that the server has processed all outstanding events, and then taking virtual machine snapshots of all the infrastructure servers targeted by the upgrade
2. Upgrade the SMP server	We upgrade the core SMP services and confirm basic functionality with an appropriate testing plan
3. Upgrade site server	We rollout the upgraded agent to the site server which allows the SMP to offload package, task and boot services as required.
4. Upgrade a test client	By opening up the firewalls to a single client IP address we can test the upgrade process from the client perspective. We test the basic functionality of the client with an appropriate testing plan
5. Perform role testing plans	We confirm that each user role that logs into the server can perform their day-to-day tasks with an appropriate testing plan
6. Upgrade the Internet Gateway	The Internet Gateway expands management to internet-based clients. Once upgraded, open up firewall to single internet-based client and confirm agent upgrade process.
7. Engage full rollout	Finally, we open the firewalls to allow more clients to connect. Initially, open up a subnet at a time and monitor progress. If all goes well, we then open up the firewall to all our clients.

The main objective of the upgrade is to execute the upgrade in discrete steps using a phased and well-managed approach. This enables us to confirm that each step has been successful. We continue in this way until the upgrade is completed.

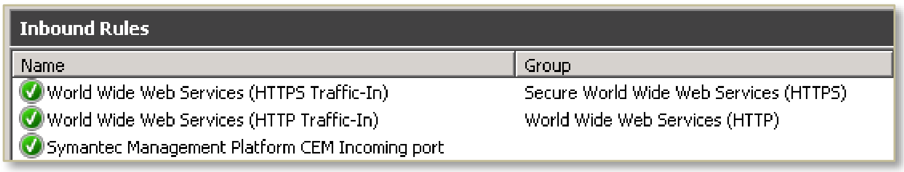
To help you understand this process a bit more fully, I'll now expand on the above points.

1.4 Quiesce the SMP Server

When executing SMP upgrades, there are a few steps we consider to minimise the risk of upgrade complications.

1. **Firewall off the SMP to Client Communications**.

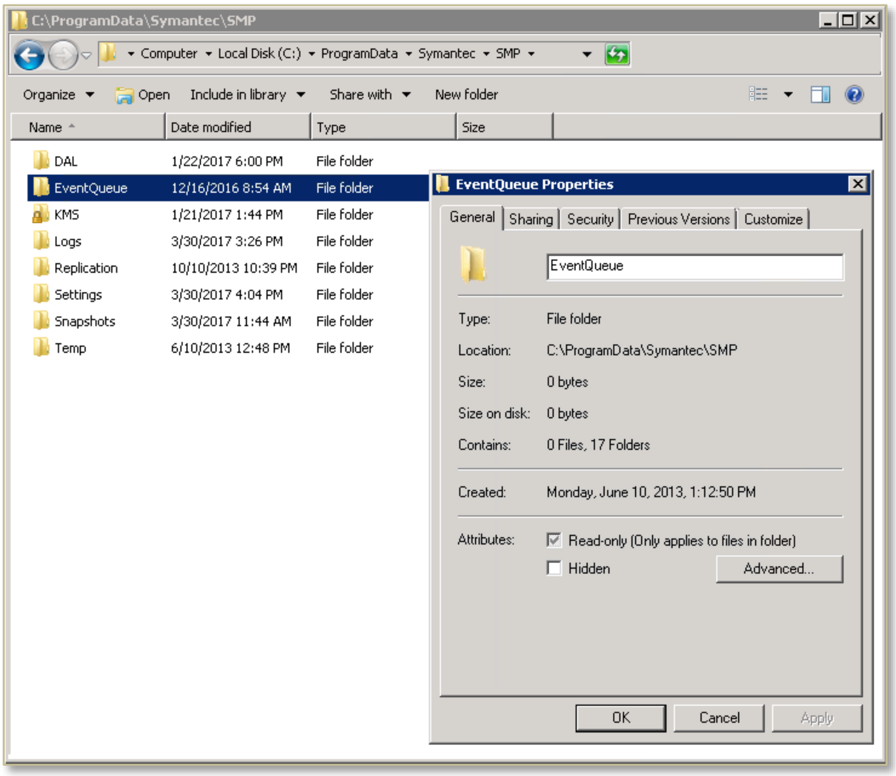
   Preventing your client base from communicating with the SMP does two things. First it helps to put the server into a peaceful trance. Secondly, the firewall helps later when trickling out the agent upgrade once the server upgrade is complete.
   The Windows firewall is quite granular and we find it sufficient for our needs here. When suitable firewall rules are in place, it is trivial to disable these to stop client communication on our SMP, Site Server and Cloud Gateway.



Inbound Rules

Name	Group
✓ World Wide Web Services (HTTPS Traffic-In)	Secure World Wide Web Services (HTTPS)
✓ World Wide Web Services (HTTP Traffic-In)	World Wide Web Services (HTTP)
✓ Symantec Management Platform CEM Incoming port	

2. Check that Event Queues are empty. Because the firewall has blocked client communications, this should naturally empty within a few minutes.



C:\ProgramData\Symantec\SMP

Computer ▸ Local Disk (C:) ▸ ProgramData ▸ Symantec ▸ SMP

Name	Date modified	Type	Size
DAL	1/22/2017 6:00 PM	File folder	
EventQueue	12/16/2016 8:54 AM	File folder	
KMS	1/21/2017 1:44 PM	File folder	
Logs	3/30/2017 3:26 PM	File folder	
Replication	10/10/2013 10:39 PM	File folder	
Settings	3/30/2017 4:04 PM	File folder	
Snapshots	3/30/2017 11:44 AM	File folder	
Temp	6/10/2013 12:48 PM	File folder	

EventQueue Properties

EventQueue

Type: File folder

Location: C:\ProgramData\Symantec\SMP

Size: 0 bytes

Size on disk: 0 bytes

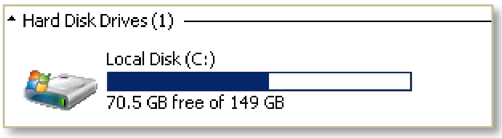
Contains: 0 Files, 17 Folders

Created: Monday, June 10, 2013, 1:12:50 PM

Attributes: ☑ Read-only (Only applies to files in folder)

□ Hidden

3. Check the Windows event logs and the SMP logs with the Altiris Log Viewer. Make sure all is well before the upgrade.
4. Confirm that there is adequate free disk space on SMP and SQL Server (We have an off-box SQL Server). Current ITMS implementation requirements mean you'll need *at least* 15GB free.

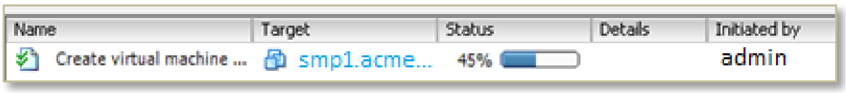


Hard Disk Drives (1)

Local Disk (C:)

70.5 GB free of 149 GB

5. Make sure file and database backups are current.
6. Reboot the SMP. This clears any ***PendingFileNameRename*** operations as well as simply being good basic hygiene for a Windows box.
7. Now Snapshot any virtual server the upgrade will touch. At the very least, we snapshot the SMP and SQL Server

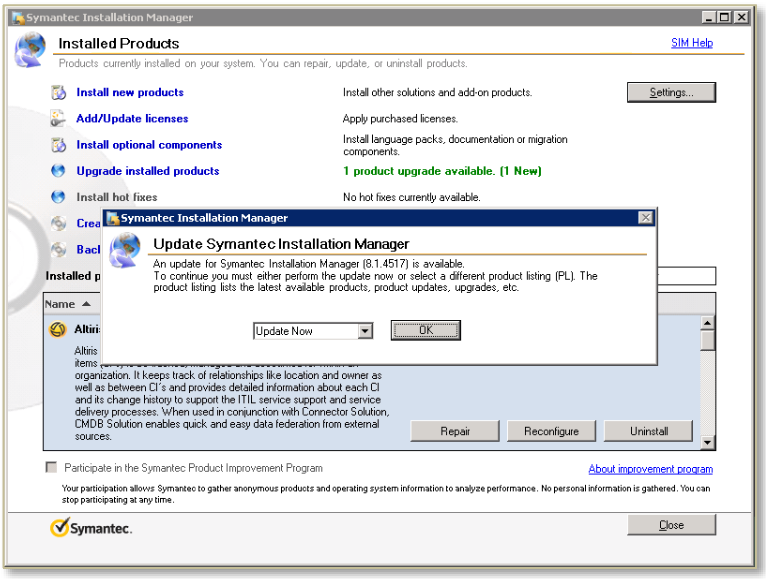


Name	Target	Status	Details	Initiated by
Create virtual machine ...	smp1.acme...	45%		admin

1.5 Execute the Upgrade of the SMP

1. **Install Upgrade prerequisites on SMP (if they exist)**
2. **Begin preparing the download of new SMP files in Symantec Installation Manager (SIM)**

When initiating our SMP upgrade, the first thing that usually needs to be done is to upgrade SIM. This is straight forward as once SIM sees that an upgrade is available, it will prompt you.



Products currently installed on your system. You can repair, update, or uninstall products.

Install other solutions and add-on products.

Apply purchased licenses.

Install language packs, documentation or migration components.

1 product upgrade available. (1 New)

No hot fixes currently available.

Altiris items organization. It keeps track of relationships like location and owner as well as between CI´s and provides detailed information about each CI and its change history to support the ITIL service support and service delivery processes. When used in conjunction with Connector Solution, CMDB Solution enables quick and easy data federation from external sources.

□ Participate in the Symantec Product Improvement Program

Your participation allows Symantec to gather anonymous products and operating system information to analyze performance. No personal information is gathered. You can stop participating at any time.

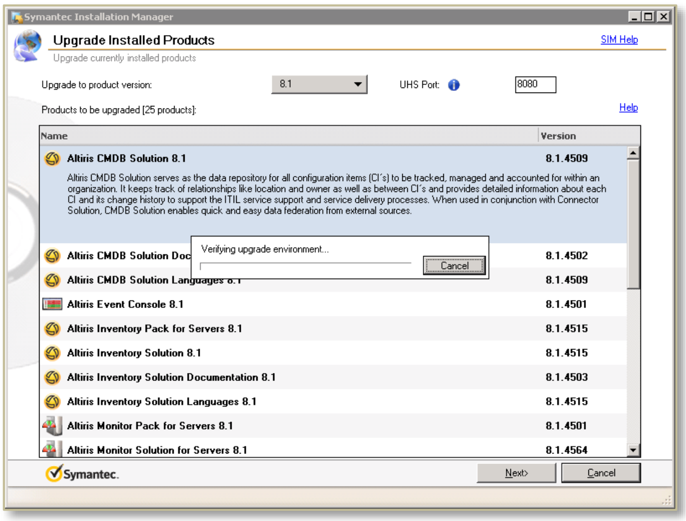
Symantec Installation Manager

Update Symantec Installation Manager

An update for Symantec Installation Manager (8.1.4517) is available.
To continue you must either perform the update now or select a different product listing (PL). The product listing lists the latest available products, product updates, upgrades, etc.

3. **Install the SIM Upgrade.** Once SIM has been upgraded, you'll be able to see the new SMP upgrade options.

4. **Select your upgrades and click Next to initiate the download process**.



Upgrade Installed Products

Upgrade currently installed products

Upgrade to product version: 8.1

UHS Port: 8080

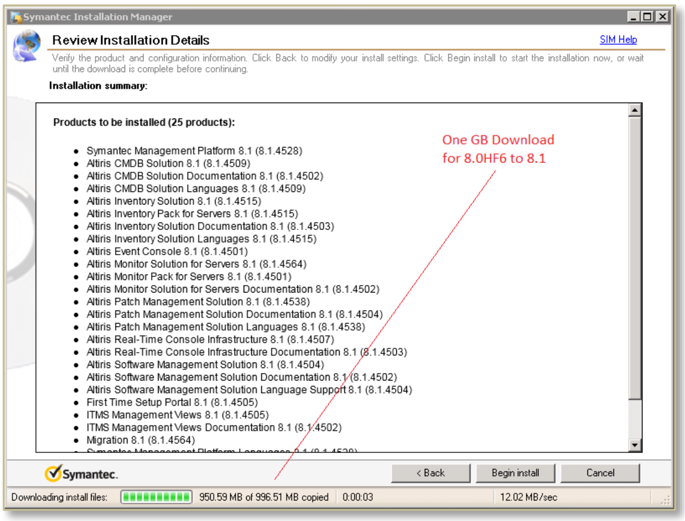
Products to be upgraded [25 products]:

Name	Version
Altiris CMDB Solution 8.1 Altiris CMDB Solution serves as the data repository for all configuration items (CI´s) to be tracked, managed and accounted for within an organization. It keeps track of relationships like location and owner as well as between CI´s and provides detailed information about each CI and its change history to support the ITIL service support and service delivery processes. When used in conjunction with Connector Solution, CMDB Solution enables quick and easy data federation from external sources.	8.1.4509
Altiris CMDB Solution Doc	8.1.4502
Altiris CMDB Solution Languages 8.1	8.1.4509
Altiris Event Console 8.1	8.1.4501
Altiris Inventory Pack for Servers 8.1	8.1.4515
Altiris Inventory Solution 8.1	8.1.4515
Altiris Inventory Solution Documentation 8.1	8.1.4503
Altiris Inventory Solution Languages 8.1	8.1.4515
Altiris Monitor Pack for Servers 8.1	8.1.4501
Altiris Monitor Solution for Servers 8.1	8.1.4564

Verifying upgrade environment...

Cancel

5. **Click the "Begin Install" button when it is offered.** This will ensure that when the download completes it will automatically commence the installation. Count on at least 90 mins for SIM to install, and a further 90 mins for SIM to configure the upgrades. Essentially, time this activity to coincide with a long lunch.



Review Installation Details

Verify the product and configuration information. Click Back to modify your install settings. Click Begin install to start the installation now, or wait until the download is complete before continuing.

Installation summary:

Products to be installed (25 products):

- Symantec Management Platform 8.1 (8.1.4528)
- Altiris CMDB Solution 8.1 (8.1.4509)
- Altiris CMDB Solution Documentation 8.1 (8.1.4502)
- Altiris CMDB Solution Languages 8.1 (8.1.4509)
- Altiris Inventory Solution 8.1 (8.1.4515)
- Altiris Inventory Pack for Servers 8.1 (8.1.4515)
- Altiris Inventory Solution Documentation 8.1 (8.1.4503)
- Altiris Inventory Solution Languages 8.1 (8.1.4515)
- Altiris Event Console 8.1 (8.1.4501)
- Altiris Monitor Solution for Servers 8.1 (8.1.4564)
- Altiris Monitor Pack for Servers 8.1 (8.1.4501)
- Altiris Monitor Solution for Servers Documentation 8.1 (8.1.4502)
- Altiris Patch Management Solution 8.1 (8.1.4538)
- Altiris Patch Management Solution Documentation 8.1 (8.1.4504)
- Altiris Patch Management Solution Languages 8.1 (8.1.4538)
- Altiris Real-Time Console Infrastructure 8.1 (8.1.4507)
- Altiris Real-Time Console Infrastructure Documentation 8.1 (8.1.4503)
- Altiris Software Management Solution 8.1 (8.1.4504)
- Altiris Software Management Solution Documentation 8.1 (8.1.4502)
- Altiris Software Management Solution Language Support 8.1 (8.1.4504)
- First Time Setup Portal 8.1 (8.1.4505)
- ITMS Management Views 8.1 (8.1.4505)
- ITMS Management Views Documentation 8.1 (8.1.4502)
- Migration 8.1 (8.1.4564)
- Symantec Management Platform Languages 8.1 (8.1.4528)

Downloading install files: 950.59 MB of 996.51 MB copied 0:00:03 12.02 MB/sec

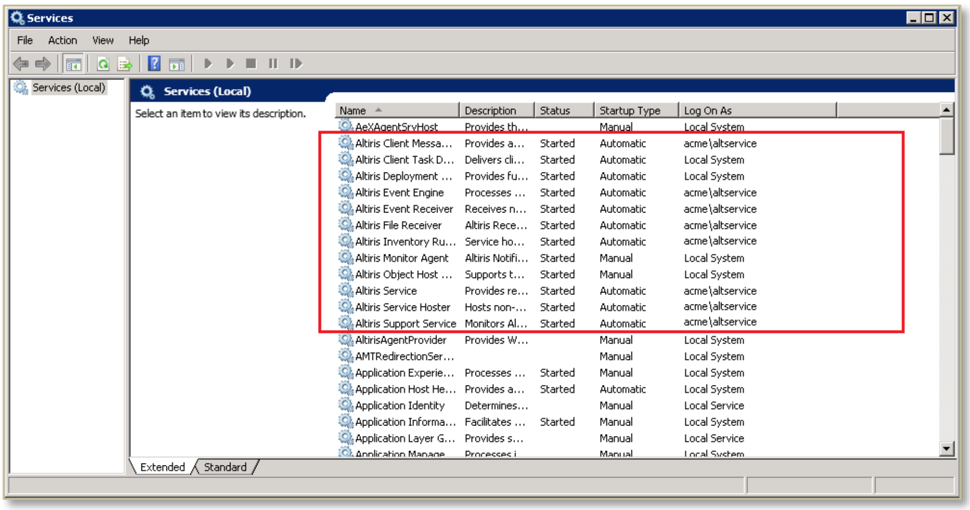
One GB Download
for 8.0HF6 to 8.1

6. **Reboot the SMP.**

   Once the install is complete, I like to reboot the server. This will ensure the SMP server has a clean slate. It is also advisable that you check the logs at this time.

7. **Check that there are no partial installs in SIM** (**CTRL+SHIFT+P**)

8. **Check that the SMP related services have started correctly**.

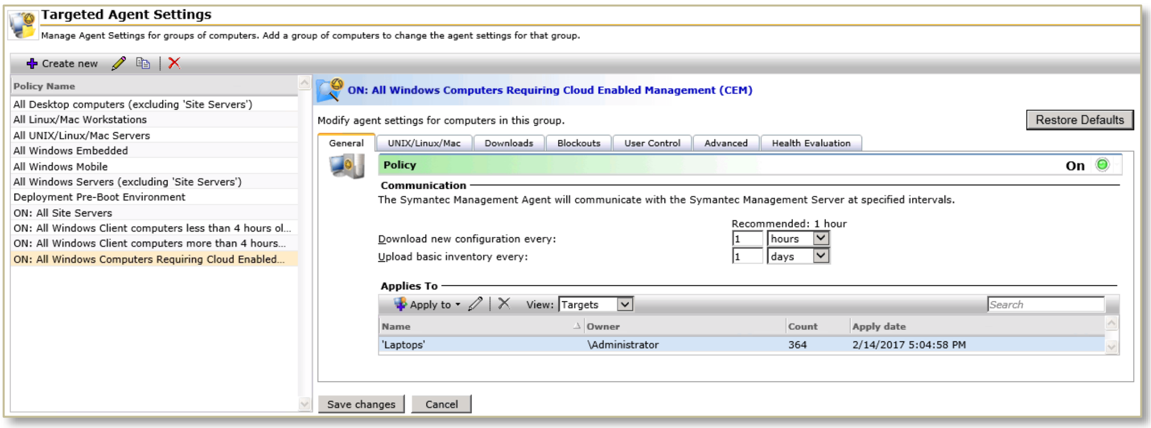


Select an item to view its description.

Name	Description	Status	Startup Type	Log On As
AeXAgentSrvHost	Provides th…		Manual	Local System
Altiris Client Messa…	Provides a…	Started	Automatic	acme\altservice
Altiris Client Task D…	Delivers cli…	Started	Automatic	Local System
Altiris Deployment …	Provides fu…	Started	Automatic	Local System
Altiris Event Engine	Processes …	Started	Automatic	acme\altservice
Altiris Event Receiver	Receives n…	Started	Automatic	acme\altservice
Altiris File Receiver	Altiris Rece…	Started	Automatic	acme\altservice
Altiris Inventory Ru…	Service ho…	Started	Automatic	acme\altservice
Altiris Monitor Agent	Altiris Notifi…	Started	Manual	Local System
Altiris Object Host …	Supports t…	Started	Manual	Local System
Altiris Service	Provides re…	Started	Automatic	acme\altservice
Altiris Service Hoster	Hosts non-…	Started	Automatic	acme\altservice
Altiris Support Service	Monitors Al…	Started	Automatic	acme\altservice
AltirisAgentProvider	Provides W…		Manual	Local System
AMTRedirectionSer…			Manual	Local System
Application Experie…	Processes …	Started	Manual	Local System
Application Host He…	Provides a…	Started	Automatic	Local System
Application Identity	Determines…		Manual	Local Service
Application Informa…	Facilitates …	Started	Manual	Local System
Application Layer G…	Provides s…		Manual	Local Service
Application Manage…	Processes i…		Manual	Local System

9. **Check the Targeted Agent Settings.** The targeted agent settings can sometimes see changes as a result of an SMP upgrade. Check that these are still sane before proceeding.

   Note: We rename our policy settings by prefixing them with **"ON:"** to indicate that they are enabled. This helps us locate the *active* policies faster for verifying those critical settings.



Targeted Agent Settings

Manage Agent Settings for groups of computers. Add a group of computers to change the agent settings for that group.

Policy Name
All Desktop computers (excluding 'Site Servers')
All Linux/Mac Workstations
All UNIX/Linux/Mac Servers
All Windows Embedded
All Windows Mobile
All Windows Servers (excluding 'Site Servers')
Deployment Pre-Boot Environment
ON: All Site Servers
ON: All Windows Client computers less than 4 hours ol…
ON: All Windows Client computers more than 4 hours…
ON: All Windows Computers Requiring Cloud Enabled…

ON: All Windows Computers Requiring Cloud Enabled Management (CEM)

Modify agent settings for computers in this group.

Policy On

Communication

The Symantec Management Agent will communicate with the Symantec Management Server at specified intervals.

Recommended: 1 hour

Download new configuration every: 1 hours

Upload basic inventory every: 1 days

Applies To

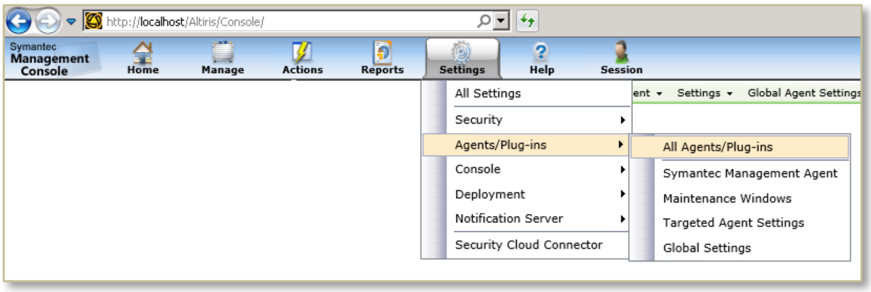
View: Targets

Name	Owner	Count	Apply date
'Laptops'	\Administrator	364	2/14/2017 5:04:58 PM

10. **Validate Agent Upgrade Policies**

    During the SMP upgrade, agent and plugin upgrade policies will be disabled by the installer. This is by design and sensible. This prevents the entire population of agents upgrading as soon as the SMP comes back online. Following an SMP upgrade, it is recommended you check all the plug-in policy settings -**targets** and **schedules** can be reset and may need attention before enabling again.

    Note: Although we check agent and plugin policies at this point, we do not enable them. We want to confirm the server is in basic working order before exposing our client base to the upgraded SMP.



11. **Refresh IT Analytics Credentials**

    If you use IT Analytics, this will likely be reset as part of the upgrade. Re-enter the credentials to resolve. https://support.symantec.com/en_US/article.TECH213502.html

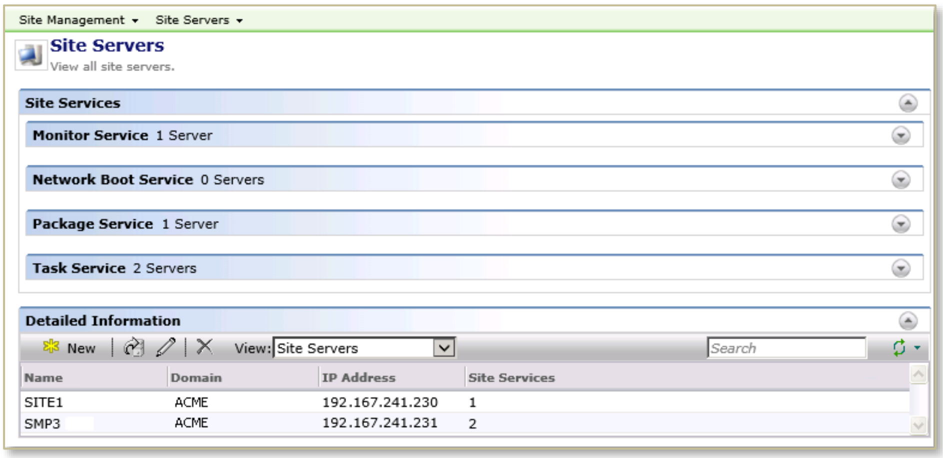
12. **Windows Event logs and SMP Logs (Altiris Log Viewer)**
    Yep –time to check those again.

13. **Execute Testing Plans**

    Now we begin testing the relevant portions of our "Acceptance Testing" plans (the sections specific to console use). We make sure at this point that we log into the Console as a user with the appropriate group rights

1.6 Execute Site Server Upgrade

1. **Ensure Site Server Upgrade pre-requisites are met** (.NET Framework 4.5.1)
2. **Enable Site Server agent upgrade policy and check that the site server exists in the policy target**
3. **Enable the Firewall rule to enable site server access to SMP**
4. **Check the logs**. Confirm Site Server upgrade in the SMP Console under
   Settings ->Notification Server-> Site Server Settings



Site Servers
View all site servers.

Site Services

Monitor Service 1 Server

Network Boot Service 0 Servers

Package Service 1 Server

Task Service 2 Servers

Detailed Information

View: Site Servers

Name	Domain	IP Address	Site Services
SITE1	ACME	192.167.241.230	1
SMP3	ACME	192.167.241.231	2

1.7 Single Client Testing

This is how far we've come in the outline plan we presented earlier:

Step	Completed?
1. Quiesce Infrastructure and Snapshot	Yes
2. Upgrade SMP server	Yes
3. Upgrade Site Server	Yes
4. Upgrade test client	No
5. Perform role testing plans	No
6. Upgrade Internet Gateway	No
7. Engage Full Rollout	No

So, we're at the point now where we are happy with the core SMP and its communication with the Site Server. It's now time to look at the clients. At this point, we begin exposing the upgraded server to our client estate by opening up the Windows firewall rules to specific client(s).

Note: In the past, we used to upgrade our client estate by amending the targets of our agent and plugin policies. However, this can be cumbersome as there are several targets to update. We found this approach to be a bit more work, not to mention more prone to error.

To adopt the Firewall method:

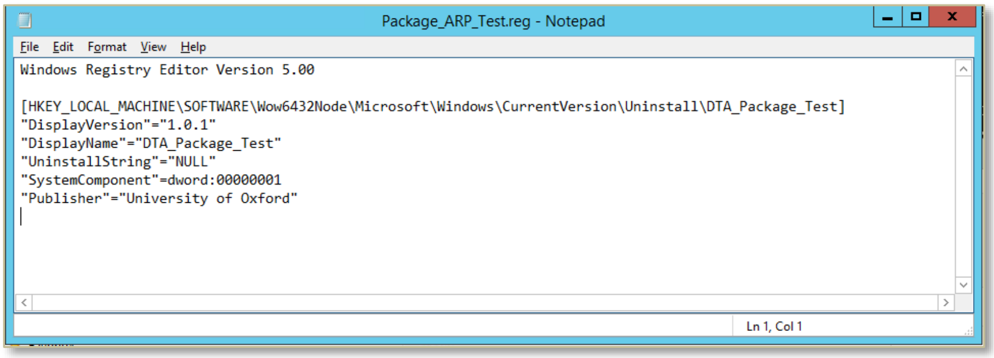
1. **Enable the Altiris agent upgrade and plugin policies**
2. **Create a HTTP/HTTPS Windows Firewall rule to enable *single-test* client access**
3. **Observe the client upgrade process.**

   Check that the plug-ins upgrade as expected. (The agent health flipbook is a nice way to confirm the progress of the plug-in upgrades)

4. **Confirm basic plugin functionality**

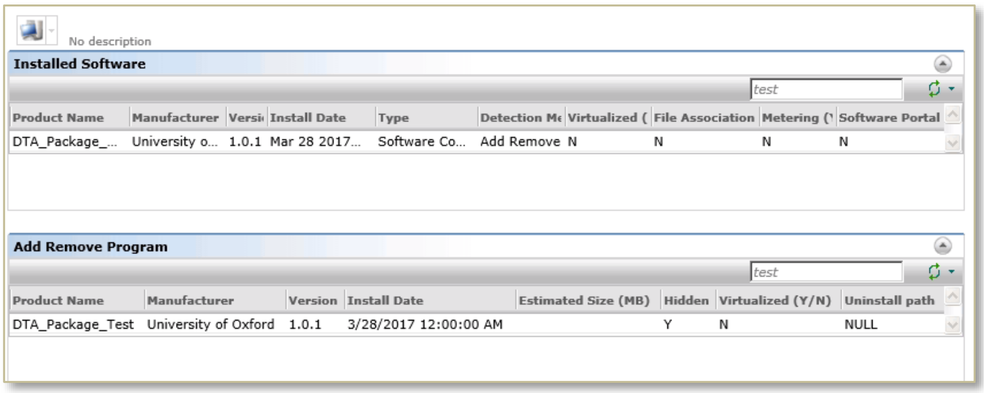
   To confirm the functionality of the plugins, you can execute some simple tests.

   a. **We confirm agent inventory functionality** by creating a dummy add-remove programs entry on the client machine. This is the script we use to add this dummy ARP entry:



```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall\DTA_Package_Test]
"DisplayVersion"="1.0.1"
"DisplayName"="DTA_Package_Test"
"UninstallString"="NULL"
"SystemComponent"=dword:00000001
"Publisher"="University of Oxford"
```

   b. **We then run a hardware inventory scan** (via a task which incidentally also confirms task server operation). Then you can see the correct entry in the client inventory on the server:



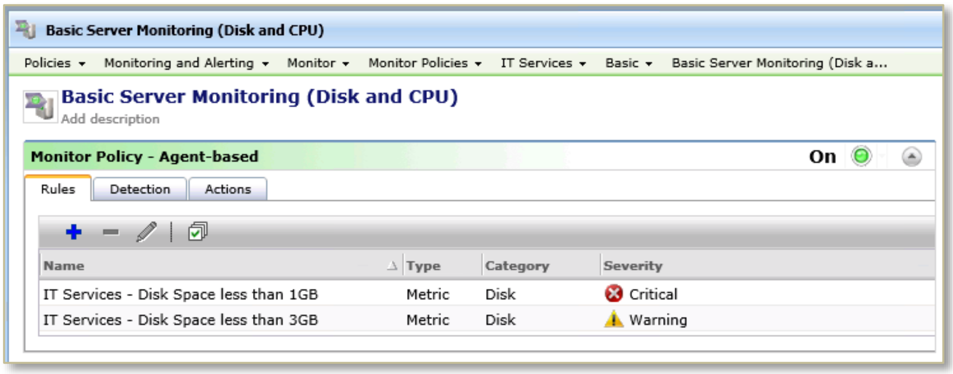
Installed Software

Product Name	Manufacturer	Versi	Install Date	Type	Detection Me	Virtualized (	File Association	Metering ('	Software Portal
DTA_Package_...	University o...	1.0.1	Mar 28 2017...	Software Co...	Add Remove	N	N	N	N

Add Remove Program

Product Name	Manufacturer	Version	Install Date	Estimated Size (MB)	Hidden	Virtualized (Y/N)	Uninstall path
DTA_Package_Test	University of Oxford	1.0.1	3/28/2017 12:00:00 AM		Y	N	NULL

Other solutions can be tested in similar ways. For example, we test Monitor Solution by filling up the client disk and seeing if a critical alert triggers. Then we clear the disk to confirm that the alert resets.



Basic Server Monitoring (Disk and CPU)
Policies ▾ Monitoring and Alerting ▾ Monitor ▾ Monitor Policies ▾ IT Services ▾ Basic ▾ Basic Server Monitoring (Disk a...
Basic Server Monitoring (Disk and CPU)
Add description
Monitor Policy - Agent-based
On
Rules
Detection
Actions

Name	Type	Category	Severity
IT Services - Disk Space less than 1GB	Metric	Disk	Critical
IT Services - Disk Space less than 3GB	Metric	Disk	Warning

The key takeaway here is to try to build your own testing steps which will give you confidence that at least the basics are working as expected following the upgrade.

5. **Execute relevant portions of your "Acceptance Testing" plan(s).**

   Log into the Console with the appropriate group rights for the plan you are testing. This for example might include the following:

   - Logging into the console as a manager and running reports
   - Logging in as a software packager to test the building of a new software package and deploying it to a client
   - Logging into a console as a helpdesk technician and executing remote control and Real-time functions as appropriate

1.8 Upgrade the Internet Gateway

The next step is to perform the Internet Gateway upgrade. Currently, as the upgrade plan stands, this should still be firewalled from remote client connections.

To Upgrade the Internet Gateway:

1. Enable Firewall on CEM gateway to click all clients
2. Install Server Prerequisites (.NET Framework 4.5.1)
3. Upgrade CEM Internet Gateway Package
4. Enable the Firewall rule to enable single client access (whatismyip.com is your friend here).
5. Observe client upgrade process
6. Confirm basic plugin functionality
7. Confirm cloud agent switching to and from cloud enabled mode. We use our enterprise VPN client to facilitate this, and of course add the client VPN address to the SMP/Site Server firewalls)
8. Execute relevant portions of "Acceptance Testing" plans for Cloud Clients.

1.9 Multiple Client Testing

1. Enable Firewall rule on the SMP and Site Server to enable *multiple test* client access
2. Observe client upgrade process
3. Confirm basic plugin functionality
4. Check logs

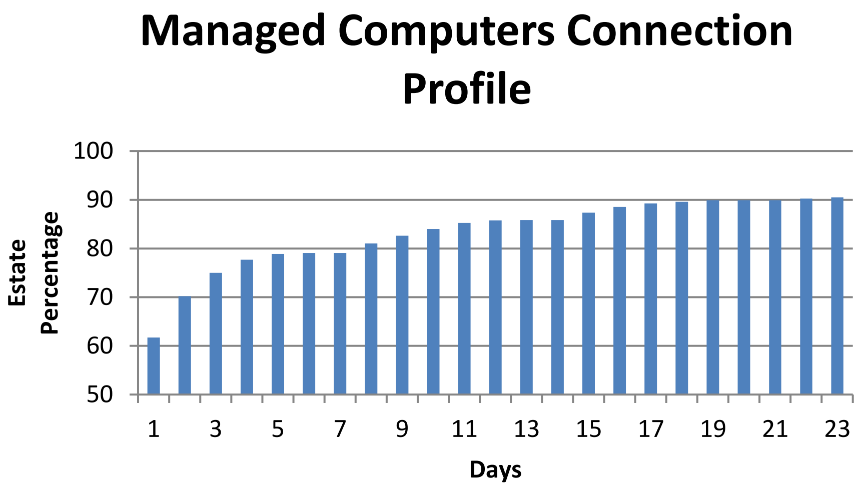
1.10 Go-Live State

1. Enable Firewall Rule for All Clients on SMP
2. Enable Firewall Rule for All Client on Cloud Gateway
3. Monitor logs
4. Commit Virtual Machine snapshots

For the ‘Go-Live’, we expect the agent upgrade to occur at the same speed as they habitually connect to the SMP. Employee working patterns, holidays, training, training room activity etc. mean that every machine across our estate will not be upgraded on day one.

Having analysed our client connection profile, we can reasonably expect about 80% of our managed machines to have connected (and therefore upgraded) in the first week.

Below is our connection profile -scavenged from the SMP database client connection table.



Wash-Up/Remediation

We are now at the point where the upgrade is complete, but sadly our work here is not yet done. Things will crop up, and in the week following the upgrade we can reasonably expect to see a few issues pop up. We categorise these as follows:

1. **Major Issues due to the Upgrade**
   With good preparation, this should not be a big list. Ideally it should really only contain issues that could not be reasonably expected to have been revealed in a pilot rollout scenario.

2. **Minor Issues**
   Console users will in general be aware that you have done an upgrade. As a result, they will likely be more alert in raising issues. It's a necessary evil to examine these and confirm whether or not they are related to the upgrade, whether they've always been there (so good to track and resolve anyhow) or whether they are simply part of the random IT noise.

3. **Communications Issues**
   With the best will in the world, people can miss the notification that a major upgrade was on the horizon. Have a pre-canned response email prepared to let users know of the communications undertaken, and a note of where they can find any console changes that have been agreed to.

In short –even if the upgrade is *perfect*, expect to get incidents raised against it.

And finally, expect the wash-up to last a week and try to be prepared for a *major* incident. Have the appropriate people assigned in advance to handle communications should an incident occur. Maybe even check with a Symantec partner what their availability might look like in wash-up week.

About Symantec

Symantec Corporation (NASDAQ: SYMC) is the global leader in cybersecurity. Operating one of the world’s largest cyber intelligence networks, we see more threats, and protect more customers from the next generation of attacks. We help companies, governments and individuals secure their most important data wherever it lives.