



Diagnosing and Troubleshooting IT Management Suite

Brian Sheedy

Sr. Principal TEC, Endpoint Management



Agenda



- 1 Troubleshooting Aids and Tools**
- 2 Resolving Common SMP Issues**
- 3 Resolving Common Site Issues**
- 4 Resolving Common Solution Issues**

Troubleshooting Aids and Tools

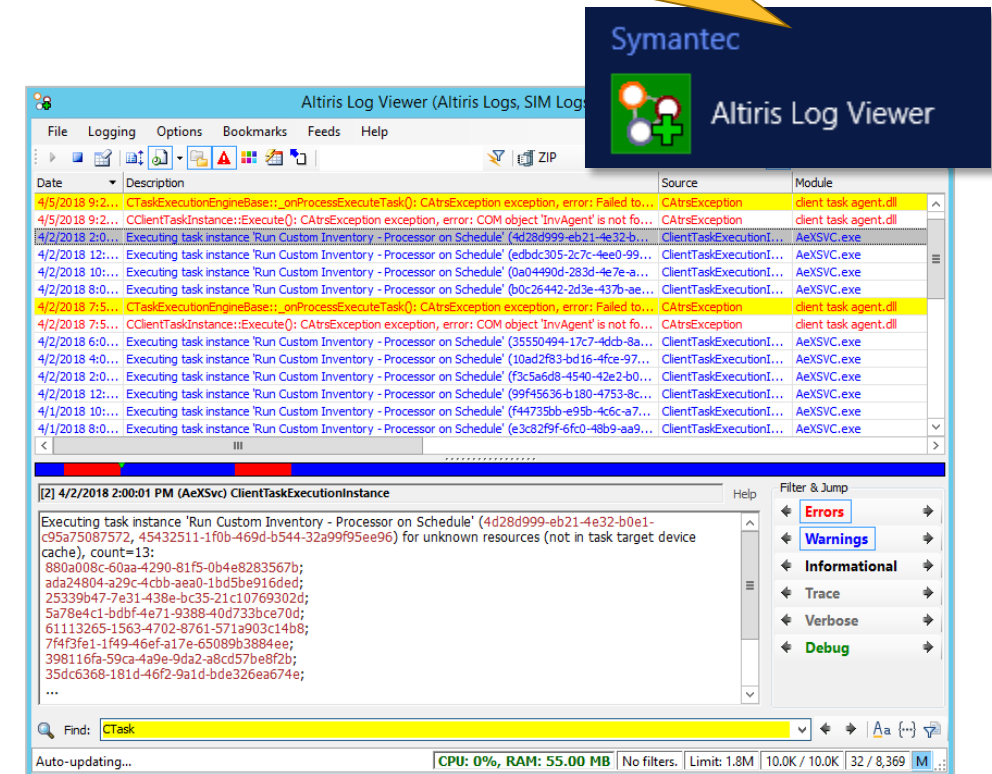


Altiris Log Viewer



- Tool Installed by default on the Notification Server
 - Displays a runtime view of errors, warning, information, and trace messages
 - Standalone tool that is SMP Version agnostic
 - Logs generated by the Notification Server, Solutions, or Agents can be viewed
- Complete record of what happens when you perform a particular action
 - Debugs issues that occur during the execution of solution-specific tasks or to check the accuracy of task execution.
 - Finds items that fail to execute, areas to debug, and the changes that are made in your endpoints
 - Use it to determine the problems and their cause.
 - Copy and paste errors to find solutions in KB Articles
- User Guide: [DOC8560](#)

`\\Program Files\\Altiris\\Diagnostics\\LogViewer2.exe`



SMP Log Files

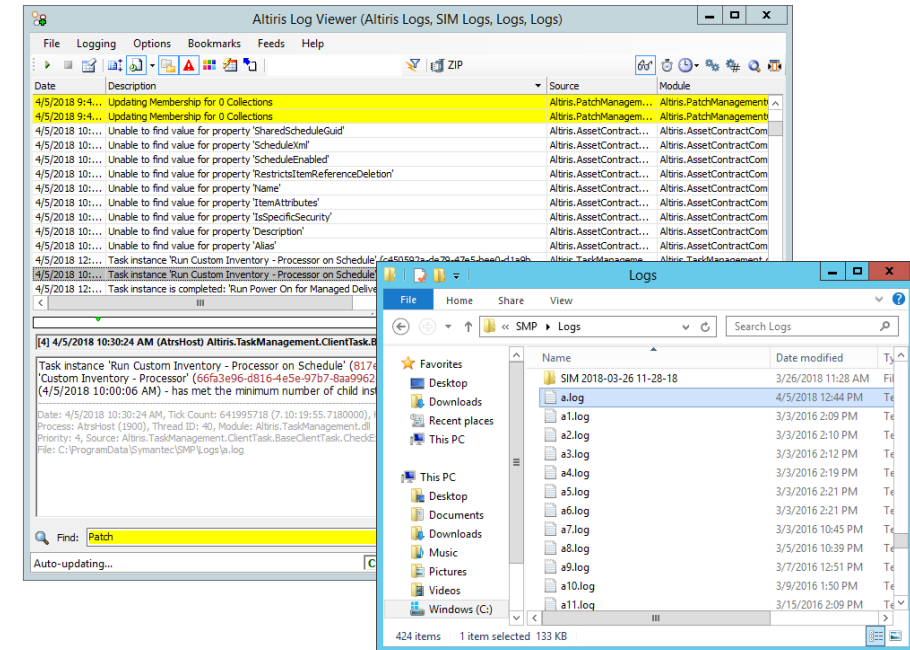


- Should be your first step in diagnosing SMP Server problems.
- Contains valuable information (and a lot of extraneous information)
- Below are a few details that you should become familiar with:
 - By default only Error, Warning and Information level events are captured.
 - Use the following switches with ***AeXNSAgent.exe*** command.
 - /nologging Disables the logging
 - /enablelogging:error Enables the error logging
 - /enablelogging:warning Enables the error and warning logging
 - /enablelogging:info Enables the error, warning and informational events logging
 - /enablelogging:debug Enables the error, warning, informational events and debug events logging
 - /enablelogging Enables the default logging
- NOTE: Verbose logging generates a lot of traffic, adding to the noise so remember to disable it when done

SMP Log File Locations



- Open with the Altiris Log Viewer for easy viewing
 - Drag and drop to the Log Viewer
- Server Logs: **A.log**
 - ...\\ProgramData\\Symantec\\SMP\\Logs
- Agent Logs: **Agent.log**
 - ...\\ProgramData\\Symantec\\Symantec Agent\\Logs
- Symantec Installation Manager (SIM) Logs: **A.log**
 - ...\\Users\\<user>\\AppData\\Local\\Temp\\SIM Logs\\
 - ...\\ProgramData\\Symantec\\SMP\\Logs\\SIM yyyy-mm-dd hh-mm-ss\\
 - ...\\ProgramData\\Symantec\\SMP\\Logs\\Install yyyy-mm-dd hh-mm-ss\\

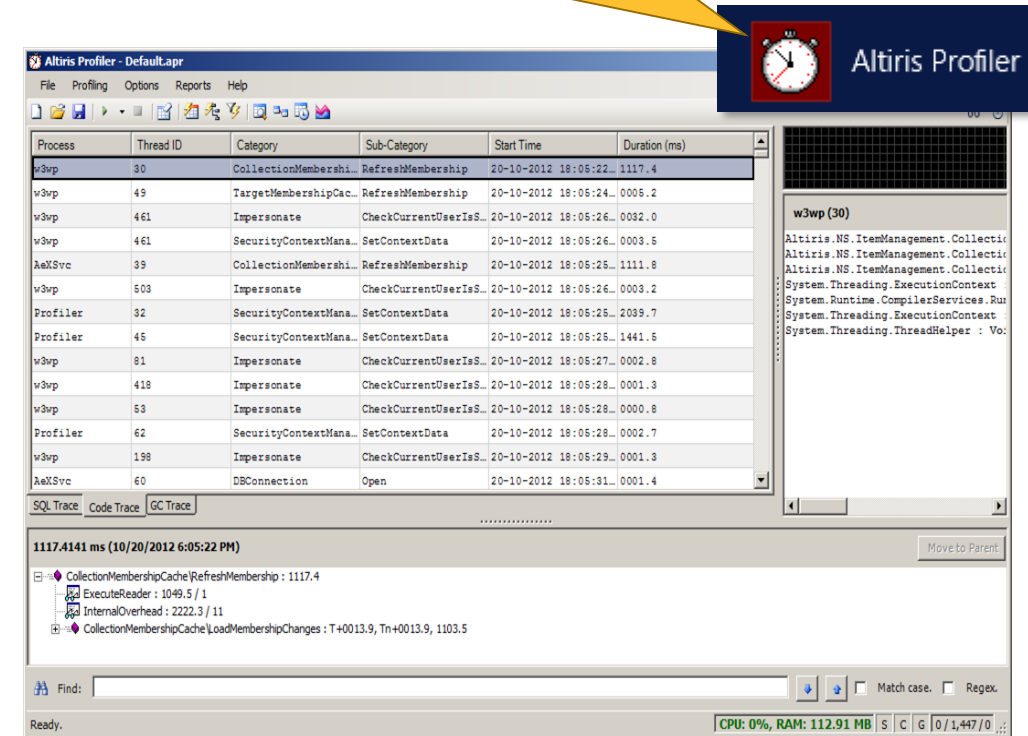


Altiris Profiler



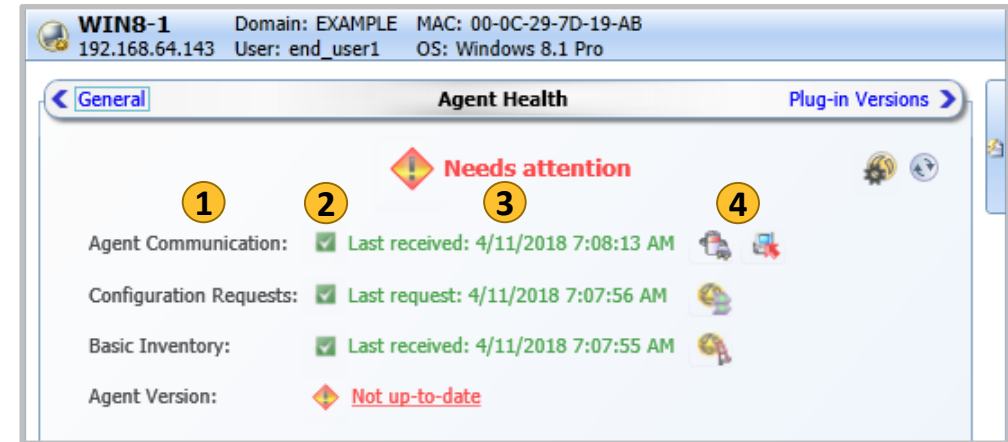
- Simple yet powerful tool for analyzing SQL queries and code executing on the NS and its associated processes.
 - See the .NET stack trace associated with database queries
 - Filter collected data based on timing constraints, or substring or regular expression matches
 - Copy and paste logged SQL straight into the Microsoft Query Analyzer, complete with pre-substituted command parameters
 - Track database errors as they occur with a live profile session
 - Set up a zero impact trace from Profiler to run on a schedule
 - Search your data with regular expressions and watch the results appear on your screen in real time
 - Profile executing queries without access to the SQL database
- User Guide: <http://www.symantec.com/docs/DOC8979>

\Program Files\Altiris\Diagnostics\Profiler.exe



Agent Health Status in the Console

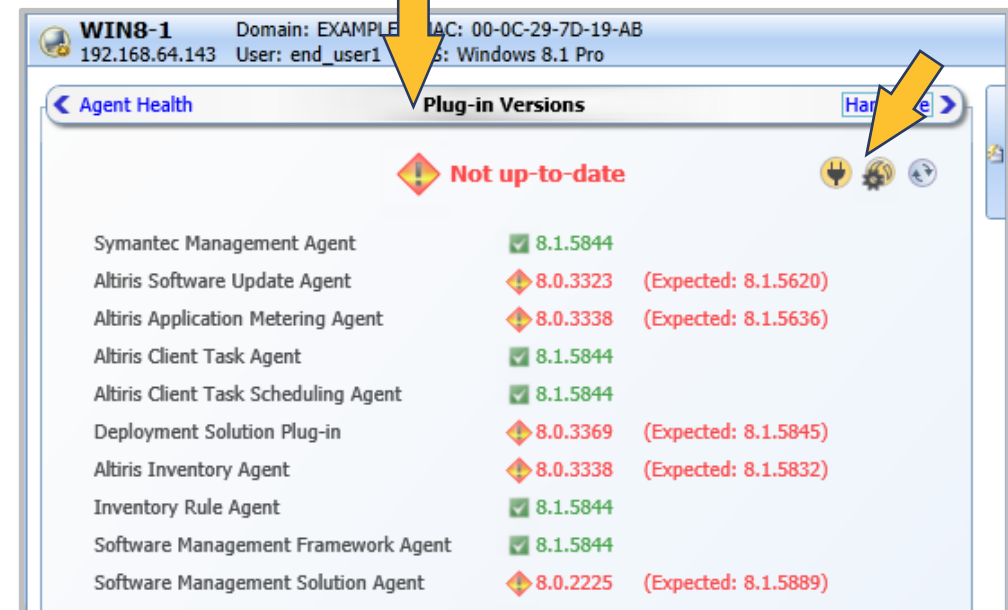
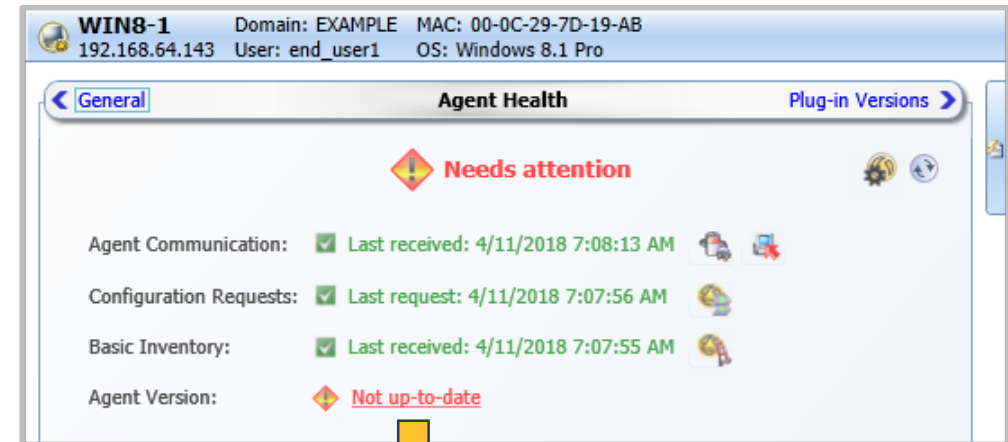
- Overall health indicator is on the top center
- If the agent health is needing attention:
 - Click on the health indicator
 - See more detailed information about agent health
 - See Problems and what actions to take
- **Agent Health flipbook is categorized by:**
 1. Agent health category status name
 2. Category agent health indicator
 3. Agent health category information message
 4. Action buttons to help to resolve the problem



Agent Health Status in the Console

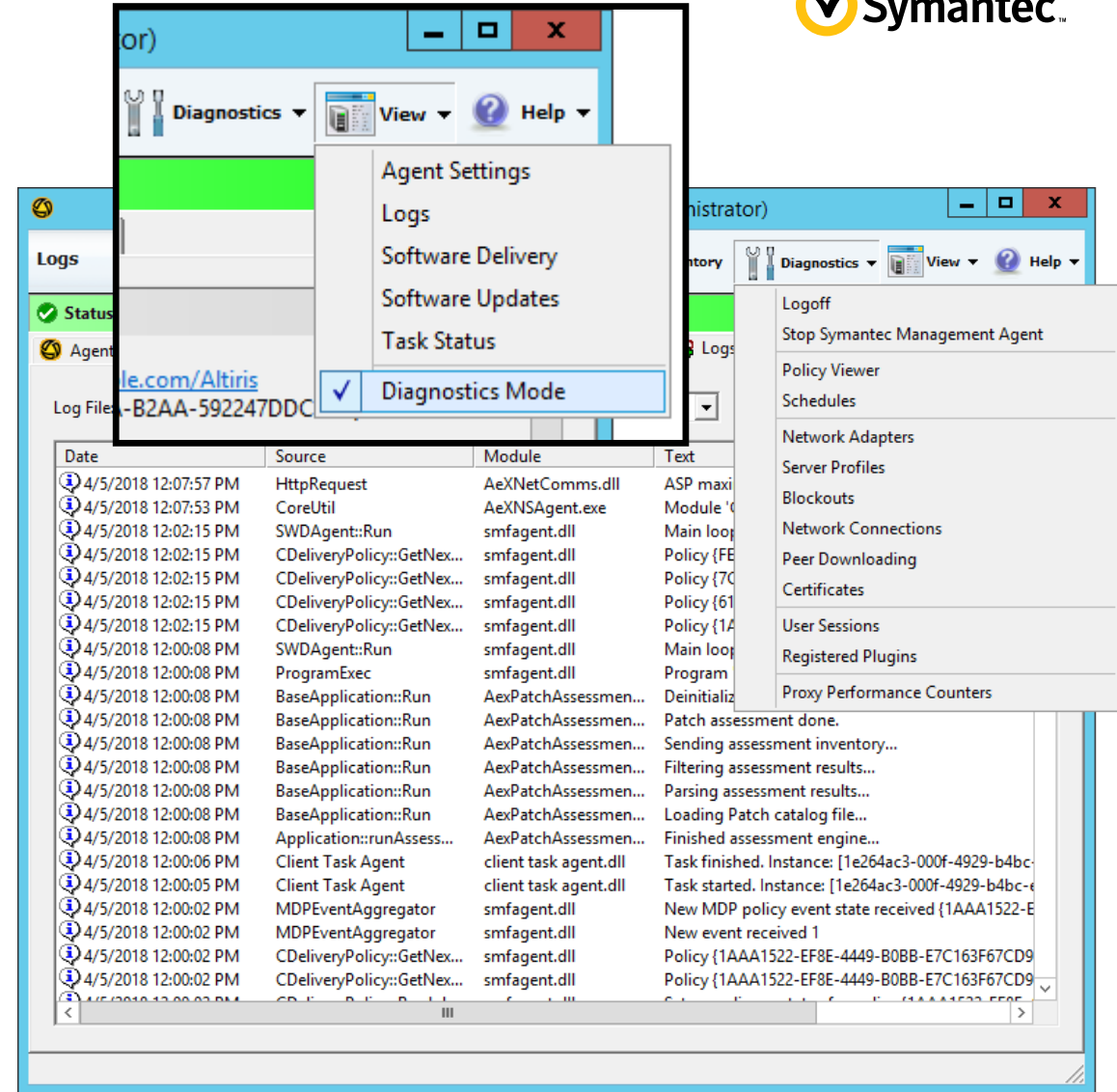


- Overall health indicator is on the top center
- If the agent health is needing attention:
 - Click on the health indicator
 - See more detailed information about agent health
 - See Problems and what actions to take
- Agent Health flipbook is categorized by:
 1. Agent health category status name
 2. Category agent health indicator
 3. Agent health category information message
 4. Action buttons to help to resolve the problem
- Plug-in Versions flipbook shows:
 - Name, version and status of the Agent or Plug-in
 - Links to the **All Agents Plug Ins** or **Targeted Agent Settings** pages



Agent Diagnostic Mode

- Allows you to work with the tools that help you troubleshoot the Symantec Management Agent.
 - Log in as an Administrator
 - Run ***Aexnsagent.exe /diags*** on the endpoint
- Under **View > Diagnostics** you will see:
 - Logoff and Shutdown SMA Service controls
 - Policies and Schedules
 - Network, Server, Blackouts and Connections
 - Peer Downloading
 - Certificates
 - User Sessions
 - Registered Plugins

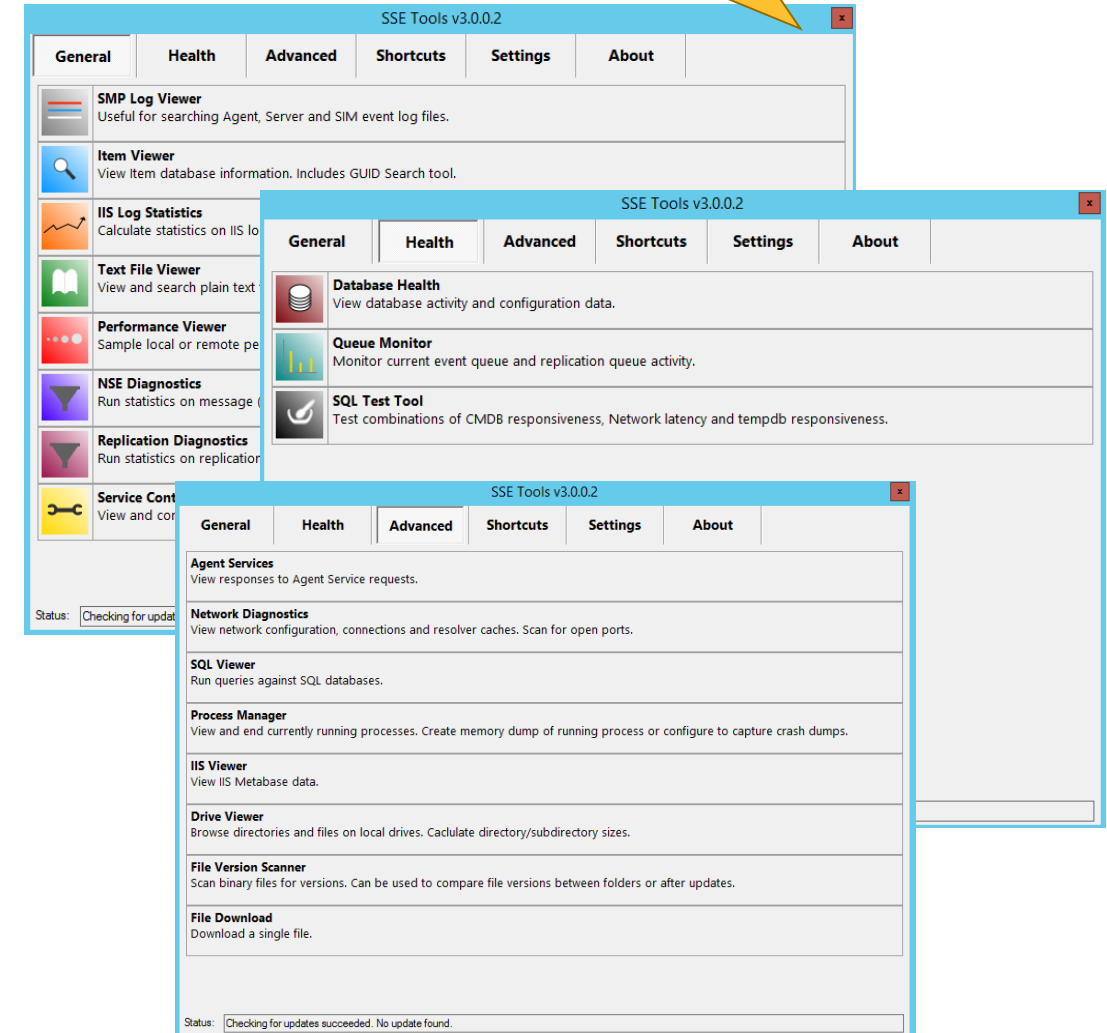


SSE Tools



INFO2568₆

- ITMS SSE Team at Symantec developed this as an aid in troubleshooting the SMP
- The SSE Tools primary objectives are:
 - Save time and efforts in identifying common issues.
 - Reduce the time required to troubleshoot issues
 - Create a platform for tool development and re-use
 - Improve both the quality and quantity of diagnostic information
- Very useful in identifying common areas that Symantec Support requires
 - SMP logs, IIS Logs, SQL Performance, Process Manager, Database and IIS Health, capture memory dumps.
- Provides Links commonly used Microsoft Tools:
 - IIS Manager, Services Console, Windbg, and additional tools from Sysinternals.



SSE Reports

HOWTO5298⁶

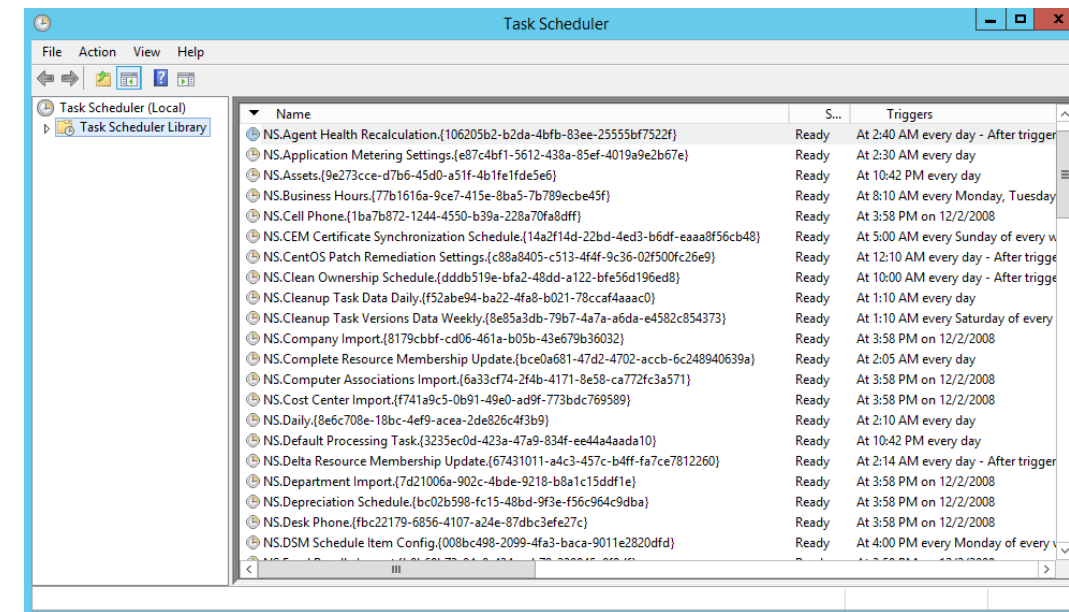


Report Name	Description	Useful For...
Daily Event Report	This report provides a summary of event processing per day.	Server Performance
Event History	This report lists event succeed/fail statistics over a given time period.	Server Performance
Event Queue Statistics	This report displays statistics for each event queue and the failed backup folder over the specified from-to range (last 7 days by default)	Server Performance
Event Trends Report	This report shows trends for the selected event.	Server Performance
Filter Update Duration	Lists the time taken for reports to update their membership, both by full update and delta update.	Server Performance
Package Server Account Creation Failure	Lists package servers which have failed to create ACC local accounts	Site Server TS, SWM TS, PMS TS, DS TS
Package Server Account Locked	Lists package servers which have ACC local accounts that have been locked out	Site Server TS, SWM TS, PMS TS, DS TS
Package Server DC Account Creation Failure	Lists package servers which are installed on a DC and cannot create ACC local accounts because the option is disabled	Site Server TS, SWM TS, PMS TS, DS TS
Package Server Password Expiry	Lists package servers with ACC local accounts that will expire within N days (14 days by default).	Site Server TS, SWM TS, PMS TS, DS TS
Resource Target Updates	Shows how long resource target updates are taking. Includes average, fastest and slowest times.	Server Performance
Scheduled Events	Lists the Scheduled Events run over a given period.	Server Performance
Scheduled Events Detail	Details instances of a Scheduled Event executed over a given period.	Server Performance
Site Report	This report lists configured site details.	Site Server TS, SWM TS, PMS TS, DS TS
Site Servers in Subnet Report	This report lists the configured site servers in the selected subnet.	Site Server TS, SWM TS, PMS TS, DS TS
Sites and Package Servers Report	Shows Sites with or without a particular type of Package Server.	Site Server TS, SWM TS, PMS TS, DS TS

SMP Scheduled Tasks (Windows Task Scheduler)



- Automates various activities within the Notification Server.
 - Filter and Target updating.
 - Distribution point updating.
 - General schedules for Hourly, Daily, Weekly...
- Managed by the Windows Task Scheduler.
 - May need to be adjusted to size of environment
 - If constantly in the 'Running' state reduce the repetition rate.
 - Hierarchy tasks can take considerable time to complete due to complexity and may appear as *always* running.



Other Important SMP Troubleshooting Tools



- **Wireshark**

- A free and open-source packet analyzer
- Used for network troubleshooting, analysis, software and communications protocol development, and education

- **WinDbg**

- A multipurpose debugger for Microsoft Windows
- Can be used to debug user mode applications, drivers, and the OS itself in kernel mode to inspect running processes.

- **Windows Performance Monitor**

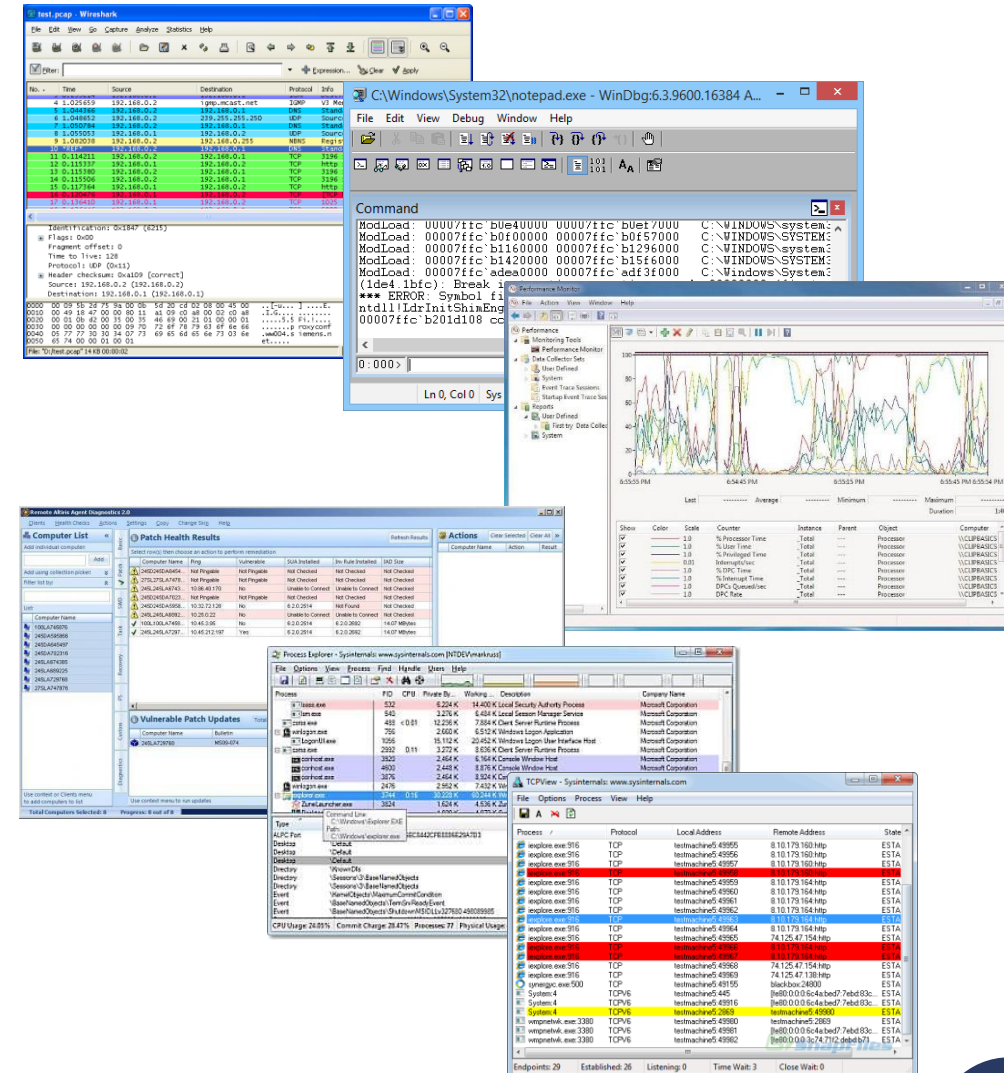
- Installed with the operating system.
- Very useful in determining benchmarks for server performance
- Monitors performance counters.

- **Remote Symantec Management Agent Diagnostics (RAAD)**

- Lets you remotely perform diagnostics of client computers, that have the SMA (Symantec Management Agent) installed.
- See HOWTO9637 and HOWTO21449

- **Microsoft Sysinternals Suite**

- **Process Explorer** shows you information about which handles and DLLs processes have opened or loaded.
- **TCPView** shows you detailed listings of all TCP and UDP endpoints on your system, including the local and remote addresses and state of TCP connections.



Common ITMS Troubleshooting Steps



ITMS Troubleshooting Overview



- **Identify the problem**
 - You are noticing slow console performance
 - Queries are taking too long to process
 - Agents are not responding to policies or tasks
- **Identify the cause**
 - Is it environmental? (firewalls, file system lockdown etc.)
 - Where is it failing? (w3wp.exe, sqlservr.exe, AeXSvc.exe etc.)
 - Which product is failing? (Core, Patch, Inventory etc.)
- **Remediation**
 - What can be done to get the system running again? (process restart, system reboot?)
 - Is this a short-term fix or can it be applied indefinitely?
- **Support Case**
 - What data needs to be gathered? (SMP version, Operating System info, stack traces, etc.)

ITMS Troubleshooting Overview



- **Non-invasive troubleshooting**
 - Inspecting aspects of the system without affecting it.
 - Reviewing log files.
 - Running various traces. (Altiris Profiler, SQL Server Profiler, Debug View)
 - Monitoring communications. (Web debugging proxies like Fiddler)
 - Running SQL Queries. (nolock hint, execution plans)
- **Invasive troubleshooting**
 - Diagnosing problems that may adversely affect the running system.
 - Attaching a debugger. (Visual Studio, WinDbg, MDbg, MSE)
 - Modifying the CMDB. (UPDATE/DELETE statements, altering stored procedures, views etc..)
 - Making changes to CoreSettings.config
 - Making changes to registry keys
- **Resources:**
 - The Symantec Connect Community (<https://www.symantec.com/connect/>)
 - The Symantec Support Site (<https://support.symantec.com>)
 - Symantec Management Console Help

ITMS Troubleshooting Overview



- **If you have resolved the issue:**
 - Communicate the result back to the impacted people
 - Add to the knowledge of problems and solutions
 - Internal Knowledgebase, support communities, forums.
- **If you have not resolved the issue:**
 - Record and contact Symantec Support if needed
 - Send pertinent information to help in resolving the problem
 - Definition of the problem
 - Diagnosis of the problem
 - Steps taken to solve the problem
 - Support may ask for log files, an Altiris Profiler trace or specific file dumps.

Resolving Common SMP Issues



Reduced Responsiveness in the Console

- **Symptoms:**
 - *Pages are taking too long to display (minutes instead of seconds)*
 - *Switching between views is slow and sometimes displays an error*
 - *Seeing Item Exception Errors, popups, blank screens*
- **Testing Approach:**
 - **Ensure that the SMP environment is sound**
 - Properly sized, configured and current health is good
 - **Check relevant Logs for errors or warnings**
 - Notification Server Logs with Altiris Log Viewer
 - **Check Processes and Scheduled items**
 - Check NS Services running, memory and resources used by them
 - Check MS Task Scheduler for long running processes
 - Altiris Profiler for long running processes
 - **Check IIS Web Services for optimal operation**
 - Check IIS Consistency and Performance
 - **Adjust depending on results**

Reduced Responsiveness in the Console

- **Ensure that the SMP environment is sound**
 - If the SMP and MS SQL environment is not sound
 - **Not Properly Sized** – adjust resources (RAM, CPU, Disk)
 - **Not Properly Configured** – adjust configuration to meet or exceed recommendations as indicated below to improve responsiveness:

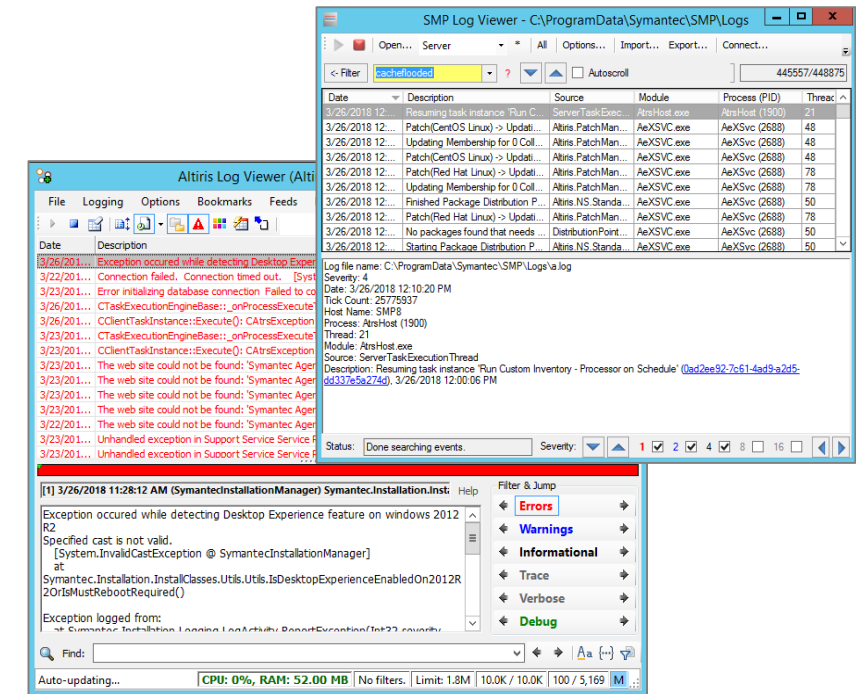
Setting	< 1000	1000 – 5000	5000 – 10,000	10,000 – 20,000	20,000 to 35,000
Agent Configuration Interval	Every 1 hour	Every 1 hour	Every 2 hours	Every 3 hours	Every 4 hours
Complete Resource Membership Update	Daily	Daily	Daily	Daily	Daily
Delta Resource Membership schedule	15 min	20 min	30 min	45 min	1 hr
Task Service task update interval	5 min	5 min	15 min	15 min	15 min
Policy Refresh schedule	5 min	10 min	15 min	15-20 min	15-20 min

- **Current Server Health Report indicates performance warnings** – follow advice from report
- **Know:**
 - Current Environment, Installed Products, versions, license state.
 - Location of Log Files, reports or applicable utilities
 - Historical operation, current state, recent changes.

Reduced Responsiveness in the Console



- Check relevant Logs and Events for errors or warnings
 - Use the Altiris Log Viewer or SSE Tools Log Viewer for NS Logs
 - Use the Windows Event Viewer for Application, System and OS errors
 - Look for errors that mention timeouts, item exceptions or 'unable to...'.
 - Errors/warnings regarding **AeXSVC.exe**
 - Errors/warnings **w3wp.exe**
 - Errors/warnings **Altiris.NS.dll**
- Search for and investigate relevant errors or warnings on the appropriate vendor sites.
 - Apply any suggested fixes to prove solutions



Reduced Responsiveness in the Console



- **Check Processes and Scheduled items**

- Use Windows Services.msc or SSE Tools to validate SMP Services
 - SSE Tools will filter the SMP Services
- Look for NS Services are using high memory and resources
 - Use is dependent on environment size – but 100% CPU is not normal
 - Investigate behavior on support pages or KB's
- Look at NS Task Schedules that seem to be stalled, have errors or run too often
 - Duration of some schedules are dependent on environment size
 - Running > 12 hours is not normal
 - Investigate behavior on support pages or KB's and apply solutions
- Use Altiris Profiler to investigate long running processes found
 - Apply any recommendations from the Altiris Profiler output

The image shows two overlapping windows from the Altiris console. The top window is 'Process Manager' and the bottom window is 'Service Controller'.

Process Manager Table:

Name	Id	CPU	Private KB	Working KB	Virtual KB	Threads	Se
AeXSMAAppDetector	10408	0	1,364	5,512	51,128	1	0
AeXSMAUpload	5588	0	1,256	5,336	51,204	1	0
AeXAgentUIHost	7504	0	4,140	13,512	120,520	4	1
ssetools	9876	0	37,564	47,304	671,772	15	1
ssetools	7436	0	27,396	43,648	652,660	6	1
AltirisSupportService	6552	0	46,752	59,904	657,304	34	0
w3wp	10748	0	320,164	142,724	18,327,656	51	0
w3wp	12976	0	704,628	569,696	18,938,560	197	0
AtrHost	1900	0	363,160	216,316	18,564,384	97	0
CTDataLoad	8924	0	49,288	63,224	663,832	35	0
inetinfo	11684	0	36,764	43,352	118,304	5	0
ScheduleProcessor	11600	0	20,468	18,248	550,548	6	0
AeXMetricProv	9880	0	63,736	83,808	723,704	41	0
Altiris.ServicesFramework.ServiceMonitor	1516	0	59,152	72,240	714,424	25	0

Service Controller Table:

Display Name	Status	Start Mode	Logon As	Path
AeXNSAgent	Stopped	Manual	LocalSystem	"C:\Program Files\Altiris\AeXNSAgent\AeXNSAgent.exe"
AeXAgentUIHost	Running	Automatic	EXAMPLE\Administrator	"C:\Program Files\Altiris\AeXAgentUIHost\AeXAgentUIHost.exe"
Altiris Client Task Data Loader	Running	Automatic	LocalSystem	"C:\Program Files\Altiris\Altiris\AltirisClientTaskDataLoader.exe"
Altiris Event Engine	Running	Automatic	EXAMPLE\Administrator	"C:\Program Files\Altiris\Altiris\AltirisEventEngine.exe"
Altiris Event Receiver	Running	Automatic	EXAMPLE\Administrator	"C:\Program Files\Altiris\Altiris\AltirisEventReceiver.exe"
Altiris File Receiver	Running	Automatic	EXAMPLE\Administrator	"C:\Program Files\Altiris\Altiris\AltirisFileReceiver.exe"
Altiris Inventory Rule Management Service	Running	Automatic	EXAMPLE\Administrator	"C:\Program Files\Altiris\Altiris\AltirisInventoryRuleManagementService.exe"
Altiris Monitor Agent	Running	Manual	LocalSystem	"C:\Program Files\Altiris\Altiris\AltirisMonitorAgent.exe"
Altiris Object Host Service	Running	Manual	LocalSystem	"C:\Program Files\Altiris\Altiris\AltirisObjectHostService.exe"
Altiris Service	Running	Automatic	EXAMPLE\Administrator	"C:\Program Files\Altiris\Altiris\AltirisService.exe"
Altiris Service Host	Running	Automatic	EXAMPLE\Administrator	"C:\Program Files\Altiris\Altiris\AltirisServiceHost.exe"
Altiris Support Service	Running	Automatic	EXAMPLE\Administrator	"C:\Program Files\Altiris\Altiris\AltirisSupportService.exe"
AltirisAgentProvider	Stopped	Manual	LocalSystem	"C:\Program Files\Altiris\Altiris\AltirisAgentProvider.exe"
AMTRedirectionService	Stopped	Manual	LocalSystem	"C:\Program Files\Altiris\Altiris\AltirisAMTRedirectionService.exe"
Symantec Deployment Solution - System Configuration	Stopped	Manual	LocalSystem	"C:\Program Files\Altiris\Altiris\AltirisDeploymentSolution\SystemConfiguration.exe"
Symantec Management Agent	Running	Automatic	LocalSystem	"C:\Program Files\Altiris\Altiris\AltirisManagementAgent.exe"
Symantec Workflow Server	Stopped	Automatic	LocalSystem	"C:\Program Files\Altiris\Altiris\AltirisWorkflowServer.exe"

Reduced Responsiveness in the Console



- **Check IIS Web Services for optimal operation**
 - Use Microsoft LogParser or SSE Tools
 - For IIS Logs %SystemDrive%\inetpub\logs\LogFiles
 - In SSE Tools, use IIS Log File Statistics feature or IIS Viewer
 - Review IIS Logs for heavy load or traffic
 - IP's Accessing a page more than 100 times in 8 hours indicates issues
 - Can be helpful in finding broken web services or misconfiguration of NS

Database Performance



Database Related Performance Issues



- Symptoms:
 - *Sluggish response to many processes in console, web, tasks and other operations*
 - *MS SQL Server Performance degraded with high use of resources, paging and other issues*
 - *Reports/Queries failing to display with timeout errors*
- Testing Approach:
 - **Ensure that the MS SQL and SMP environment is sound**
 - Properly sized, configured and current health is good
 - MS SQL Server Considerations are observed
 - **Eliminate Common MS SQL Server Misconfigurations**
 - MS SQL Settings: Memory, Growth, Permissions
 - SMP related CMDB Settings
 - **Perform Database Health and Performance Tests**
 - Index Fragmentation, Table Sizes, Network Performance
 - **Reduce CMDB Activity and Impact**
 - Examine SMP Configuration for opportunities to optimize performance
 - Adjust depending on results

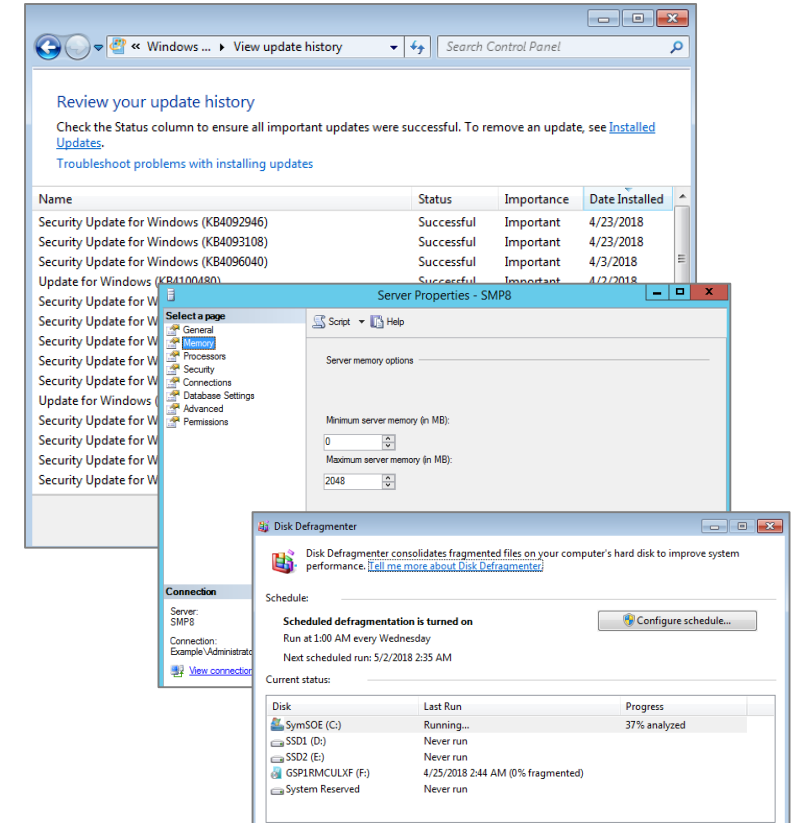
Database Related Performance Issues



- **Ensure that the MS SQL Server or SMP environment is sound**
 - Compare current implementation to Symantec and Microsoft SQL Server recommendations.
 - **Improperly sized MS SQL Server**
 - Upgrade the hardware associated with the bottleneck, e.g. adding more RAM, faster CPUs, more or faster Disks, etc..
 - **Improperly implemented SQL Server**
 - Observe and adjust configuration to adhere to recommended settings and considerations from Symantec and Microsoft.

Database Related Performance Issues

- **Eliminate Common MS SQL Server Misconfigurations**
 - **MS SQL and OS Updates**
 - Update to Highest level supported by your ITMS Implementation
 - Usually include performance fixes
 - **Memory Configuration**
 - Enable the **Optimize for Ad hoc Workloads** setting
 - Set a value in the **Maximum server memory** option
 - Reserve at least 4.5GB for OS/Apps
 - If SQL on-box, start out by setting SQL to a fixed memory value
 - **File Fragmentation**
 - Check and resolve with standard Defragmentation Tools
 - Defragment affected drives as needed



Database Related Performance Issues



- Eliminate Common MS SQL Server Misconfigurations
 - **MS SQL Server Maintenance Plans not configured**
 - **Will Most likely fix many SMP Performance issues**
 - Creates backups of databases
 - Reorganizes data and indexes
 - Checks database integrity
 - Resets statistics on the database
 - Can be created manually or from a Wizard
 - Wizard ensures that common features are taken care of
 - Not supported if using SQL Server Express
 - **Follow the Guide @ <http://www.symantec.com/docs/HOWTO8589>**
- If a Maintenance Plan resolves the performance issues, continue to Results phase

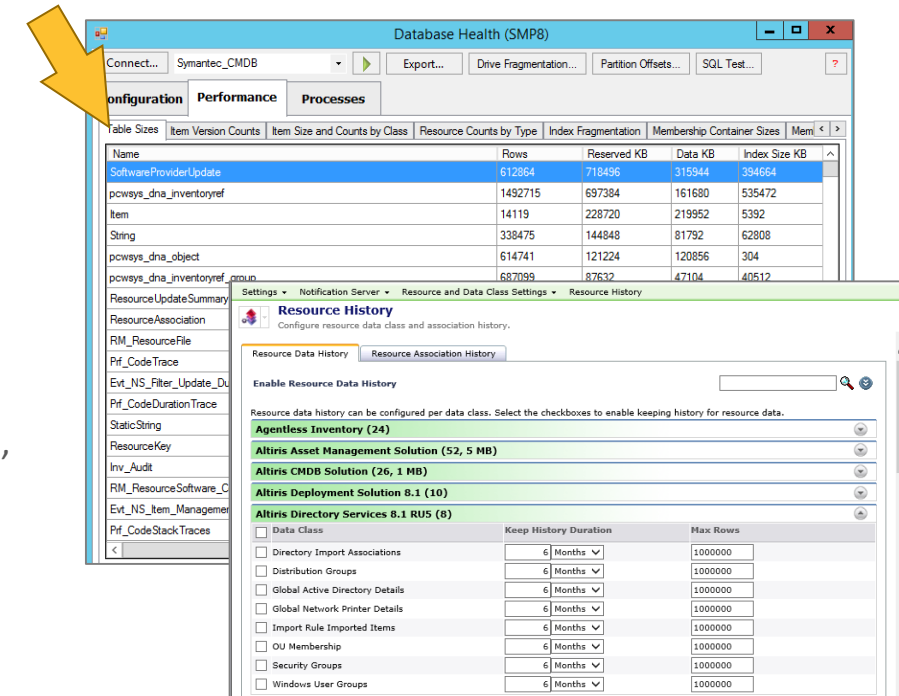
Database Related Performance Issues



- Perform Database Health and Performance Tests
 - Tests that will likely uncover performance issues:
 - Measure Table Sizes
 - Check Index Fragmentation
 - Measure Stored Procedure Duration
 - Perform a CMDB + Network Ping Test
 - Evaluate Basic SQL Performance Counters

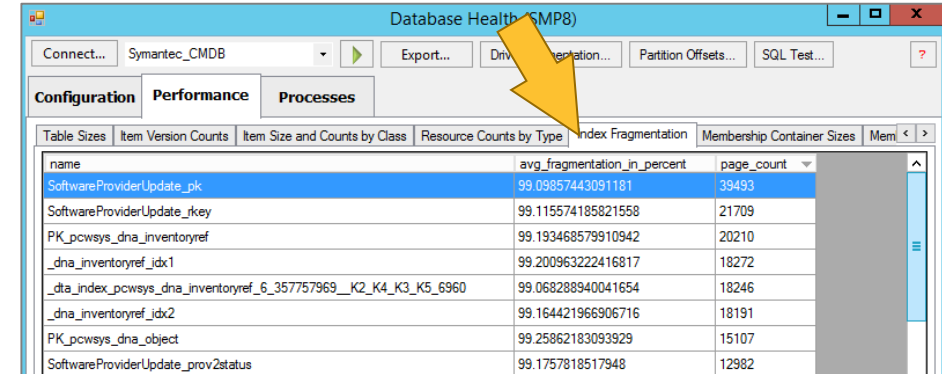
Database Related Performance Issues

- Perform Database Health and Performance Tests
 - **Measuring Table Sizes**
 - Use the **Database Health** function found in SSE Tools
 - From the “Performance” tab click the “Table Sizes” tab.
 - **PASS:** All tables should be < 2GB and No table should be two digits greater than any other table
- **Failure Remediation Steps:**
 - Creating a SQL Maintenance Plan is the easiest way (*HOWTO 8589*)
 - *Configure Purging Maintenance to reduce specific table sizes*
 - Check tables that relate to items in your console for unusually large sizes. I.e, Software view = Aex_SW...
 - Go to **Settings>Notification Server > Purging Maintenance** and **Settings>Notification Server > Resource History**
 - Set reasonable purging periods and row counts for events and resources.
 - Check that “**NS.Purging Maintenance....**” task is running on a regular basis – once per Day



Database Related Performance Issues

- Perform Database Health and Performance Tests
 - **Index Fragmentation**
 - Run the SSE Tools **Database Health** function
 - From the “Performance” tab click the “Index Fragmentation” tab
 - **PASS:** If entries are < 95%
 - **Failure Remediation Steps:**
 - *Check that “NS.SQL defragmentation schedule...” is running on a regular basis – once per Week*
 - **OR** *make sure you have a MS SQL Maintenance plan in place that will automatically defragment the indexes.*
 - *Run an Altiris Profiler SQL Trace to pinpoint issues if the above items do not improve performance.*

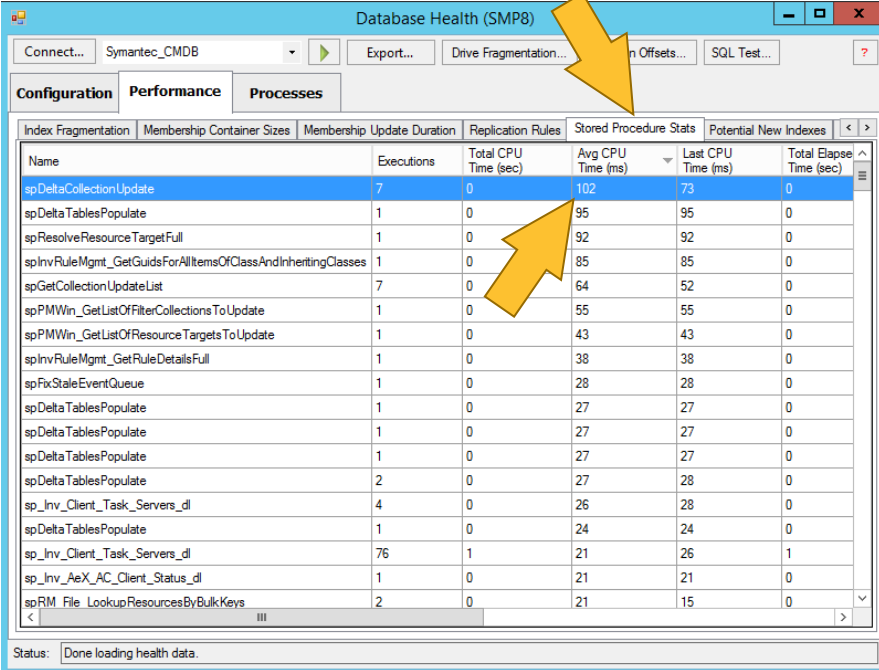


name	avg_fragmentation_in_percent	page_count
SoftwareProviderUpdate_pk	99.09857443091181	39493
SoftwareProviderUpdate_key	99.115574185821558	21709
PK_pcwsys_dna_inventoryref	99.193468579910942	20210
_dna_inventoryref_idx1	99.200963222416817	18272
_dna_index_pcwsys_dna_inventoryref_6_357757969__K2_K4_K3_K5_6960	99.068288940041654	18246
_dna_inventoryref_idx2	99.164421966906716	18191
PK_pcwsys_dna_object	99.25862183093929	15107
SoftwareProviderUpdate_prov2status	99.1757818517948	12982

Database Related Performance Issues



- Perform Database Health and Performance Tests
 - **Stored Procedure Duration:**
 - Run the SSE Tools **Database Health** function
 - Click the “Membership Update Duration” tab and the green arrow to start the test
 - **PASS:** No values returned or Avg. Duration (sec.) < 30s
 - **Failure Remediation Steps:**
 - Record the stored procedures taking longer than 30 seconds to run AND have an execution count greater than 40
 - Determine what part of the platform or solution they are associated with (The name provides a clue PM = Patch Management, SW = SW Management...)
 - Investigate the configuration of the associated platform or solution.
 - Research the problem on support resources.
 - Run the **Symantec Installation Manager** and determine if hotfixes, service packs or even license upgrades are required and apply if needed.

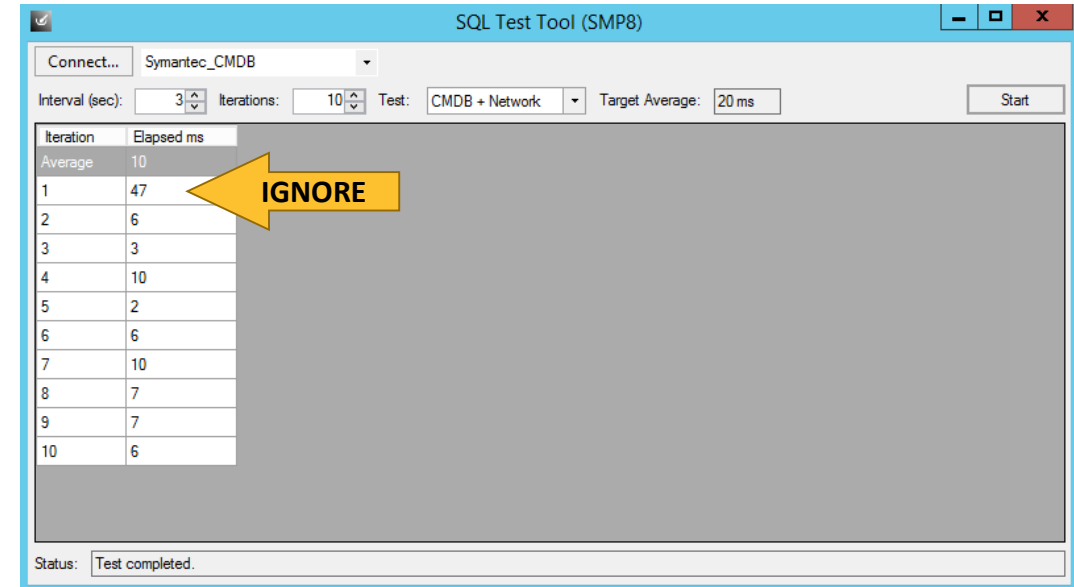


Database Health (SMP8)						
Connect... Symantec_CMDB Export... Drive Fragmentation... In Offsets... SQL Test...						
Configuration		Performance		Processes		
Index Fragmentation	Membership Container Sizes	Membership Update Duration	Replication Rules	Stored Procedure Stats	Potential New Indexes	
Name	Executions	Total CPU Time (sec)	Avg CPU Time (ms)	Last CPU Time (ms)	Total Elapse Time (sec)	
spDeltaCollectionUpdate	7	0	102	73	0	
spDeltaTablesPopulate	1	0	95	95	0	
spResolveResourceTargetFull	1	0	92	92	0	
spInvRuleMgmt_GetGuidsForAllItemsOfClassAndInheritingClasses	1	0	85	85	0	
spGetCollectionUpdateList	7	0	64	52	0	
spPMWin_GetListOfFilterCollectionsToUpdate	1	0	55	55	0	
spPMWin_GetListOfResourceTargetsToUpdate	1	0	43	43	0	
spInvRuleMgmt_GetRuleDetailsFull	1	0	38	38	0	
spFixStaleEventQueue	1	0	28	28	0	
spDeltaTablesPopulate	1	0	27	27	0	
spDeltaTablesPopulate	1	0	27	27	0	
spDeltaTablesPopulate	1	0	27	27	0	
spInv_Client_Task_Servers_dl	2	0	27	28	0	
spInv_Client_Task_Servers_dl	4	0	26	28	0	
spDeltaTablesPopulate	1	0	24	24	0	
spInv_Client_Task_Servers_dl	76	1	21	26	1	
spInv_AeX_AC_Client_Status_dl	1	0	21	21	0	
spRM_File_LookupResourcesByBulkKeys	2	0	21	15	0	

Status: Done loading health data.

Database Related Performance Issues

- Perform Database Health and Performance Tests
 - **Perform a CMDB + Network Ping Test**
 - Run the SSE Tools **Database Health** function
 - Click the “SQL Test” button, then Connect
 - Select “Symantec_CMDB” and change the “Test” option to CMDB + Network
 - Press Start
 - **PASS:** Target Average < 20ms
 - Ignore the 1st Value in the test
 - **Failure Remediation Steps:**
 - Verify a minimum 1GB connection from SMP to SQL Server.
 - May require network troubleshooting with utilities such as Wireshark to pinpoint latency issues.
 - Resolve Networking or Latency issues with the team responsible for network, security or server maintenance.

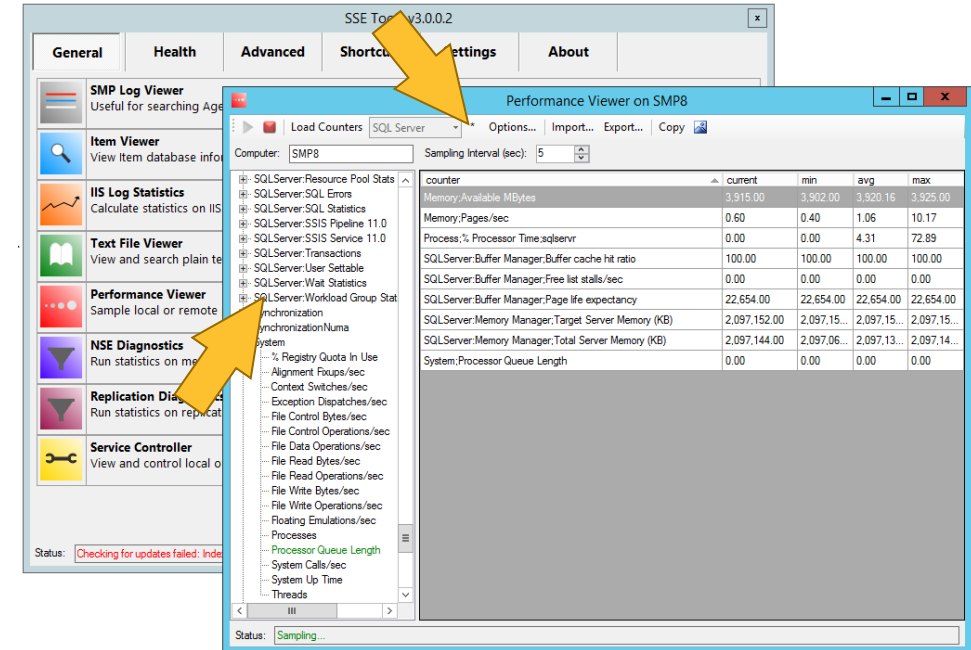


Iteration	Elapsed ms
Average	10
1	47
2	6
3	3
4	10
5	2
6	6
7	10
8	7
9	7
10	6

Status: Test completed.

Database Related Performance Issues

- Perform Database Health and Performance Tests
 - **Evaluate Basic SQL Performance Counters**
 - Run the SSE Tools **Performance Viewer** from the “General” tab
 - Select “SQL Server” and click “Load Counters”
 - **PASS:**
 - Current Physical Disk Queue Length ≤ 1 over sample duration
 - Current Logical Disk Queue Length ≤ 1 over sample duration
 - % Processor Time $< 50\%$ over duration or consistent 90% spike
 - Memory Available Mbytes 30% available as a % of total
 - **Failure Remediation Steps:**
 - Disk Queue Length Fail, Add IOPS, check disk I/O configuration
 - % Processor Fail, Add virtual/physical cores
 - Memory Available Mbytes Fail, Add physical Virtual memory
 - Note: Excessive CPU, Memory and Disk utilization may or may not be the result of hardware configuration. Misconfigured SMP, SQL, network configuration may be the root cause.



Database Related Performance Issues

- **Reduce CMDB Activity and Impact**

- Reduce the amount of load on SQL, where appropriate, by decreasing the frequency of the following Notification Server settings:

Setting	< 1000	1000 – 5000	5000 – 10,000	10,000 – 20,000	20,000 to 35,000
Agent Configuration Interval	Every 1 hour	Every 1 hour	Every 2 hours	Every 3 hours	Every 4 hours
Full inventory collection schedule	Monthly	Monthly	Monthly	Monthly	Monthly
Delta inventory collection schedule	Weekly	Weekly	Weekly	Weekly	Weekly
Complete Resource Membership Update	Daily	Daily	Daily	Daily	Daily
Delta Resource Membership schedule	15 min	20 min	30 min	45 min	1 hr
Task Service task update interval	5 min	5 min	15 min	15 min	15 min
Policy Refresh schedule	5 min	10 min	15 min	15-20 min	15-20 min

Symantec Management Agent



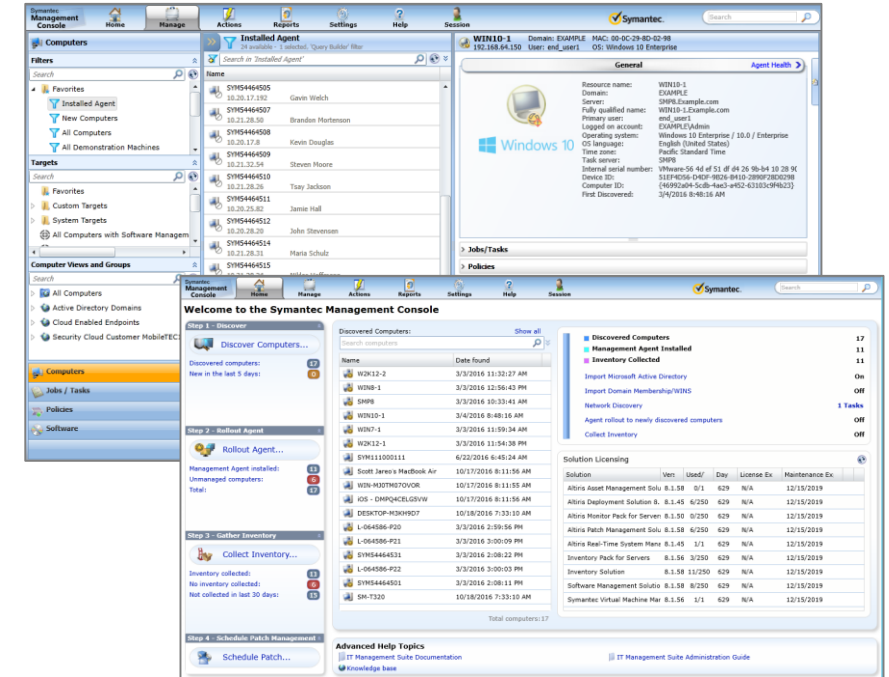
SMA Installation Issues



Symantec Management Agent Installation Issues

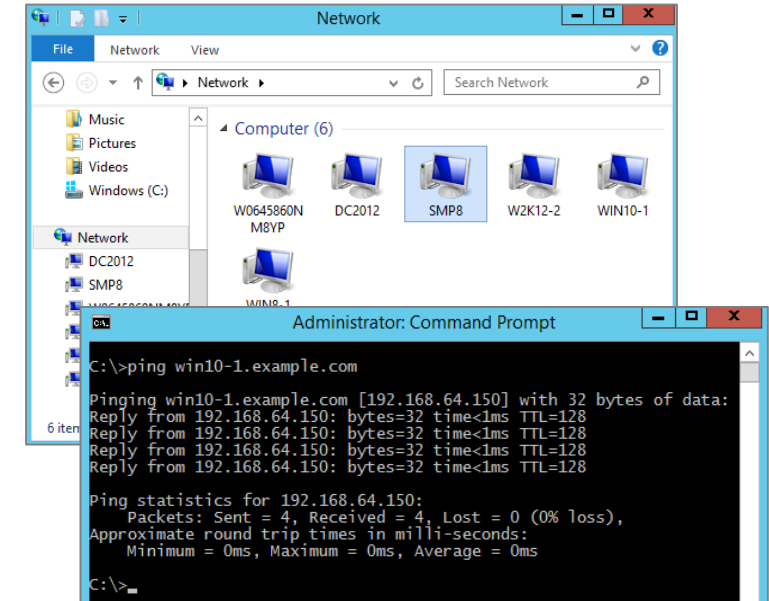


- Symptoms:
 - Determine if the problem is a result of an unsuccessful push, pull or direct execution of the agent installation.
 - Determine the state that the problem occurs – before, during or after an attempted agent installation
- Testing Approach:
 - Ensure that the Target Meets Prerequisites
 - Does the Notification Server have a direct connection to target machine?
 - Is the target endpoint 'hostname pingable'?
 - Is the credential used part of the target's "Administrators" group?
 - Is the credential used a valid account on the domain (or domains for cross-domain push)?
 - Is the target's Operating System supported by the Agent?
 - Is a proxy server being used to access the network?
 - Is the target machine's firewall turned off or configured properly for Agent install?
 - Are there errors when a Pull install is attempted?



SMA Installation Issues

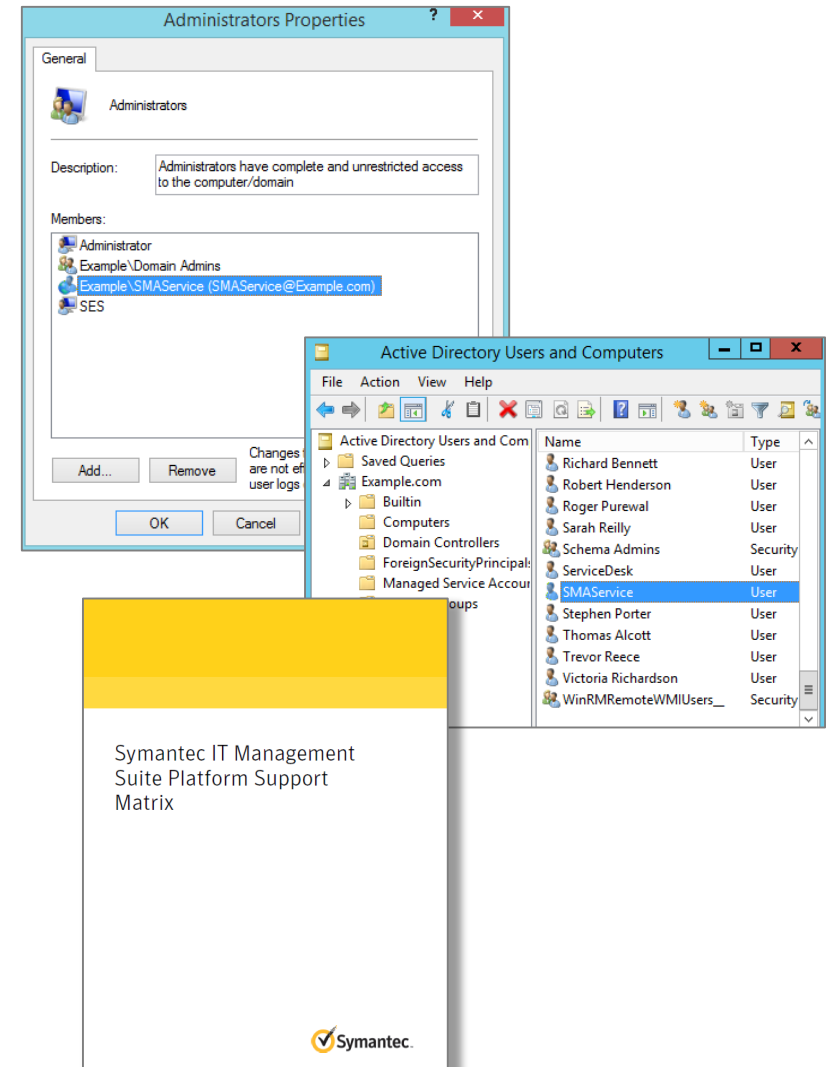
- Ensure that the Target Meets Prerequisites
 - **The current NS must have a direct connection to the target endpoint**
 - In file explorer, browse to [\\TargetName\c\\$](#) or other shares to determine if the NS has connectivity to the Target.
 - The target machine can be on the same or different domain than the NS.
 - **The target machine must be 'hostname pingable'**
 - Perform a simple Ping of the Target hostname, FQDN or IP
 - If this fails, move on to other solutions that refer to account or firewall issues



SMA Installation Issues



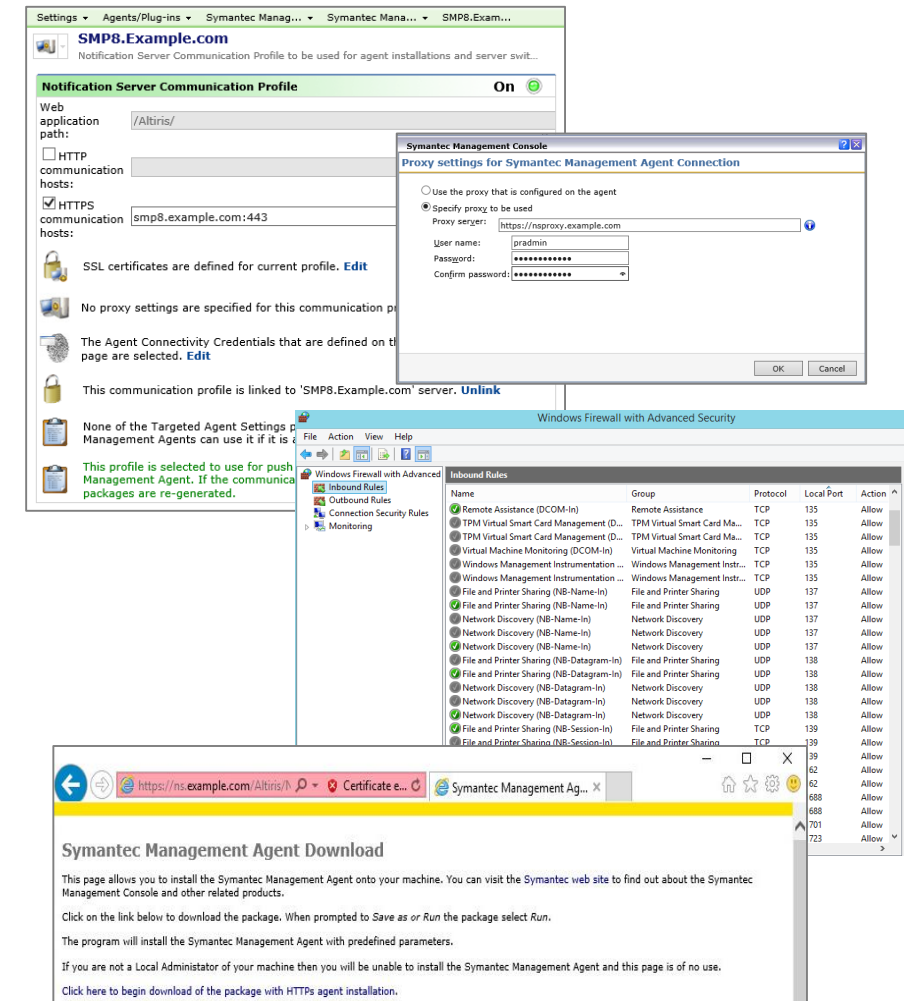
- **Ensure that the Target Meets Prerequisites**
 - **The credential used must be in the target's "Administrators" group.**
 - If it does not exist, either add the account or seek support from your network group to add it.
 - This is a very common solution to push/pull installation issues
 - **The credential used, must be valid on the domain**
 - Log into an endpoint that is a domain member or investigate the account
 - If it does not, use an appropriate account that was created for this purpose
 - **The target machine's OS) must be supported**
 - Check the **Platform Support Matrix** ([HOWTO9965](#) - 8.1)
 - If not supported, notations in the matrix might guide you to limitations or workarounds for the endpoint.



SMA Installation Issues



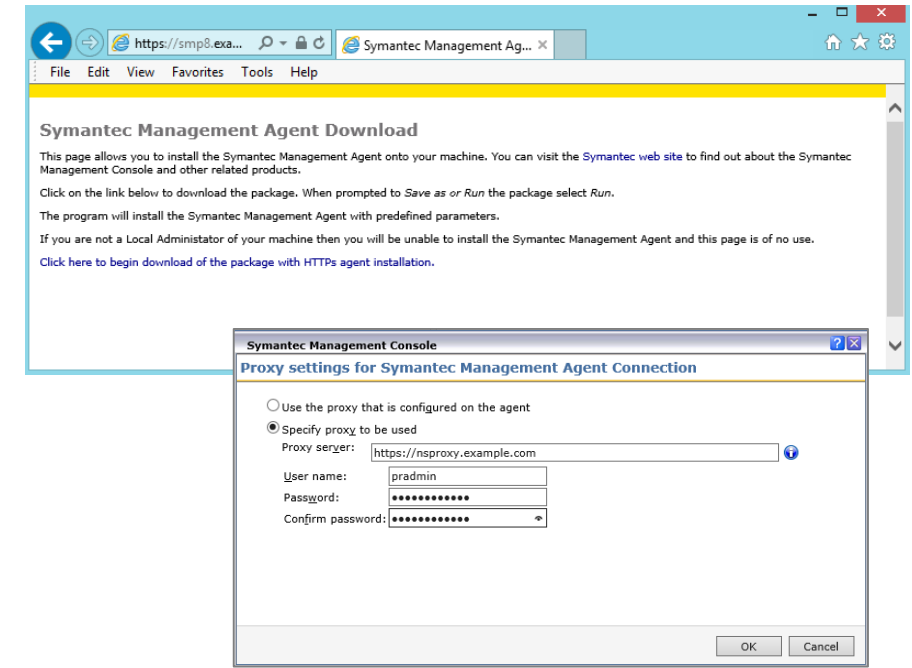
- Ensure that the Target Meets Prerequisites
 - Check that the proxy settings for the Server Communication Profile is valid
 - Incorrect Proxy settings can cause the console to reflect unsuccessful download or install errors
- The target machine's firewall should be configured properly
 - Configure the Firewall Rules to reflect these ports for initial installation and disable them after installation
 - File and Print Services ports: TCP 139, TCP 445 should work but UDP 137, UDP 138 may also be required
- If all methods have failed at this point, you can attempt a 'Pull' installation of the Agent



SMA Installation Issues



- **Ensure that the Target Meets Prerequisites**
 - **If a push installation fails, attempt a 'Pull' installation of the Agent**
 1. Log in to the target machine as an Administrator of the machine.
 2. Browse to the Agent Push URL
 3. Follow the instructions on the page to download and install the agent
- **Troubleshooting Failed Pull Installations:**
 - It is important to note that the proxy settings inside the agent push "Installation Settings" is also being used by the pull install.
 - Incorrect Proxy settings can cause the console to reflect unsuccessful download or install errors.



SMA Communication Issues



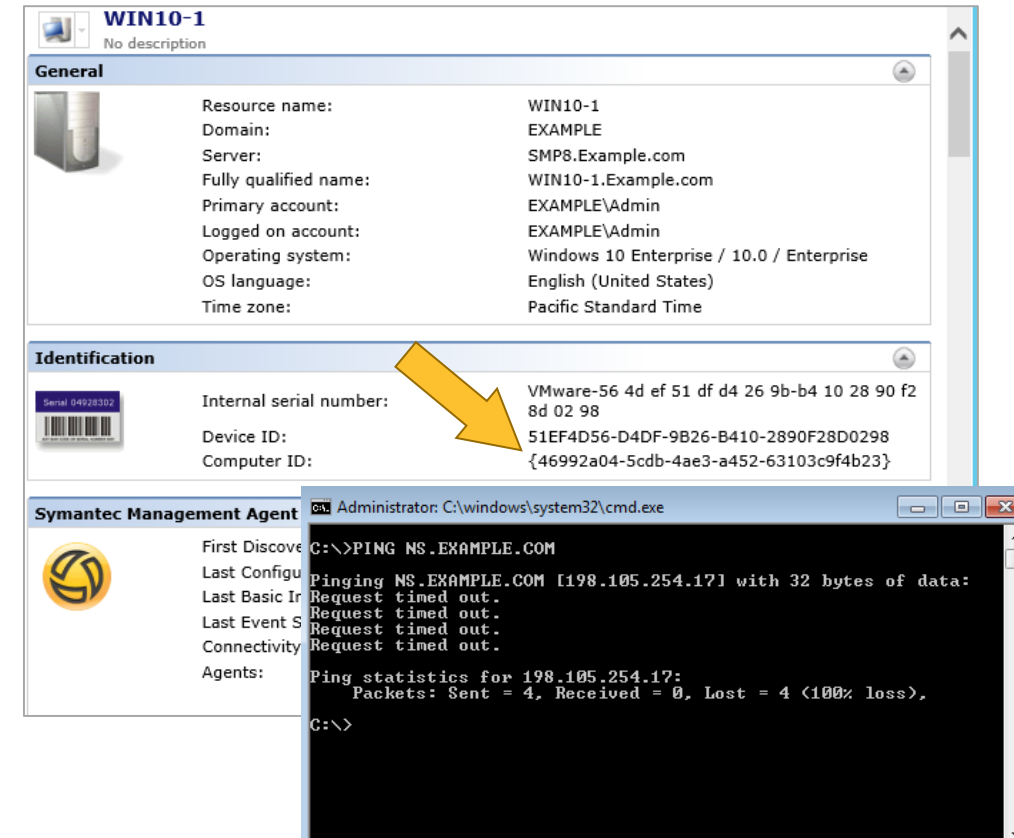
Symantec Management Agent Communication Issues



- **Symptoms:**
 - **Determine if the problem is related to the agent:**
 - **Not communicating with Notification Server**
 - **Not able to Download packages**
 - **Not able to receive or execute tasks**
- **Testing Approach:**
 - **Determine if Post-installation steps were successful**
 - **Determine if the Agent is 'Healthy'**
 - Are there warnings in the Agent Health/Plugin-Health panes?
 - Are there errors/warnings in the logs?
 - Adjust depending on results

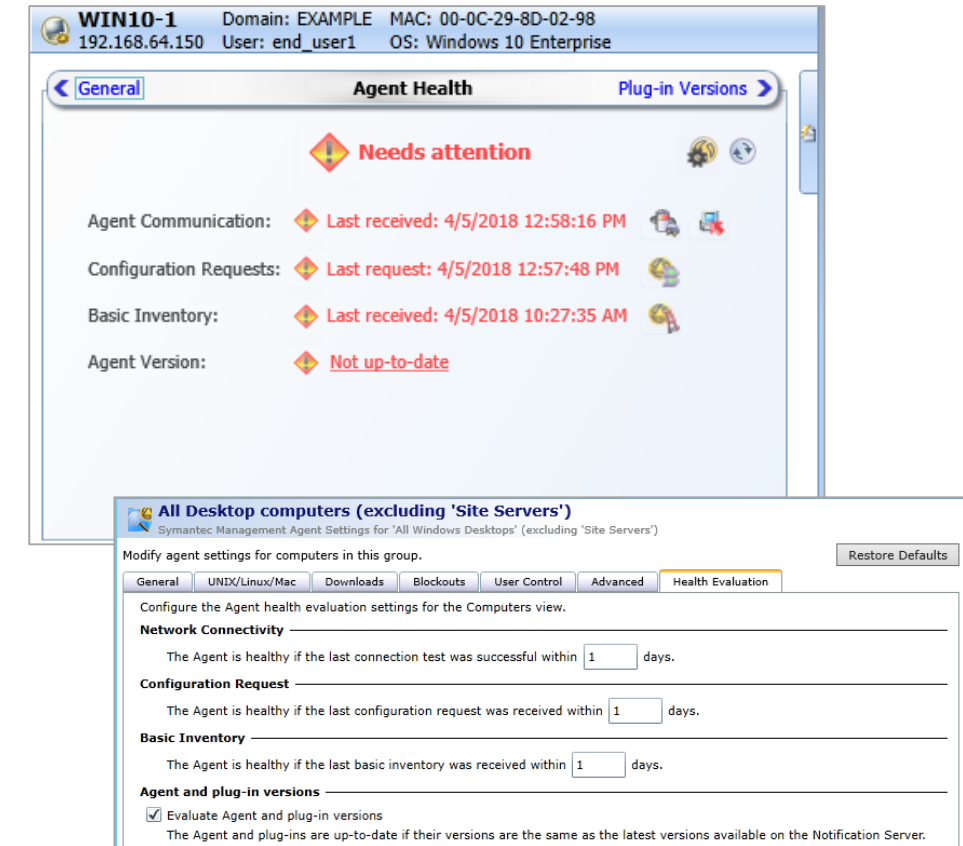
SMA Communication Issues

- **Determine if Post-installation actions were successful**
 - Check that the endpoint is present in the console
 - Open the Computer View and search for it
 - If present, go into the Resource Manager and ensure that it has a Resource GUID assigned
 - If the endpoint is not present in the console
 - From the NS - perform a simple Ping test of the Target hostname, FQDN or IP
 - From the endpoint
 - Perform a simple Ping test of the NS hostname, FQDN or IP
 - Check the agent logs for severity 1 errors & research
 - Check the Windows Event Viewer for errors
 - Perform standard network connection and account troubleshooting to resolve the communication issues



SMA Communication Issues

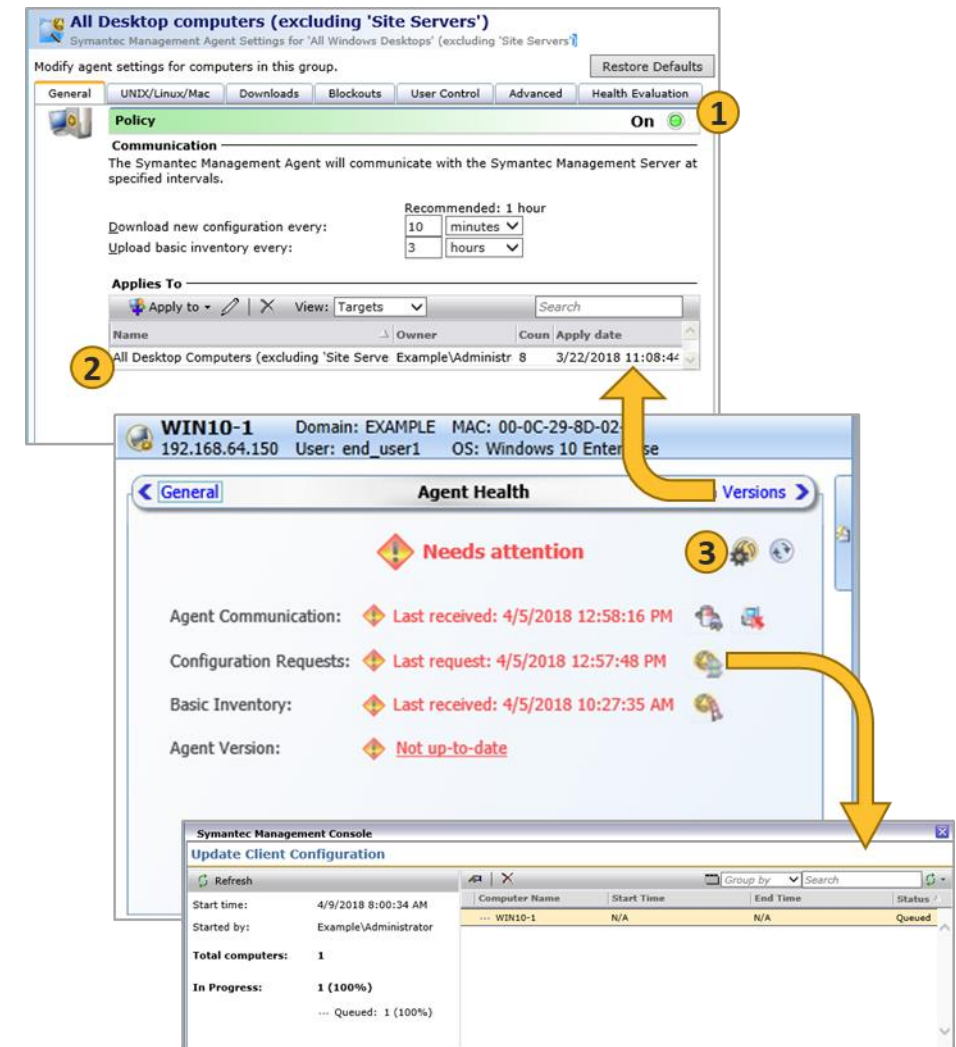
- **Determine if the Agent is 'Healthy'**
 - In the **Computer View**, Select the **Agent Health** Pane to begin troubleshooting
 - **Overall Status:** Indicates if the Agent is **Healthy** or **Needs Attention**
 - **Agent Communication:** The time of the last communication between the Agent and the server.
 - **Configuration Requests:** The time of the last configuration request received by Notification Server from the client computer.
 - **Basic Inventory:** The time of the last basic inventory received by Notification Server from the client computer.
 - **Agent Version:** The status of the current version of the Symantec Management Agent and plug-ins: up-to-date or not.
- For this section, we will assume that the above Health Evaluation periods are set to one day.



SMA Communication Issues

- **Agent Communication**

- If **Red**, it is indicating that there has been no communication in the last n days.
- The Icons next to the alert allow you to ping or traceroute the endpoint from the computer you are on.
- If ping or trace route are unsuccessful
 - Check the state of the client computer (power, network, etc..)
 - Perform standard network communication troubleshooting
 - Check the Targeted Agent Settings to ensure that the policy is enabled and that the endpoint is part of the Target (**1, & 2**)
 - Resolve any discrepancies and test
 - Check that the Endpoint has only one Targeted Agent Settings Policy assigned (**3**)
 - If the **Open Targeted Agent Settings** icon has an exclamation mark on it, hover over the icon and you can see which policies are in conflict.
 - Resolve the conflict and test
 - Check the Agent Logs and/or Notification Server Logs for errors, research and resolve



SMA Communication Issues



- **Configuration Requests**

- If **Red**, it is indicating that there has not been a configuration request from the Agent in the last **n** days.
- The Icon next to the alert allows you to send a task that will execute the “Configuration Request” on the target endpoint. This date/time will change if the task is successful.
- **If the date/time does not change**
 - Check the state of the client computer (power, network, etc..)
 - Check Targeted Agent Settings to ensure that the policy is enabled, the endpoint is part of the target and that configuration interval is correct for this implementation (**1, 2 & 3**).
 - Check that the Endpoint has only one Targeted Agent Settings Policy assigned (**3**)
 - If the **Open Targeted Agent Settings** icon has an exclamation mark, resolve the conflict and test
 - Check the Agent Logs and/or Notification Server Logs for errors, research and resolve

The image displays three screenshots from the Symantec Management Console illustrating configuration request issues.

Top Screenshot: Agent Settings
This window shows the configuration for 'All Desktop computers (excluding 'Site Servers')'. The 'Policy' tab is selected, showing the 'Communication' section. The 'Policy' is set to 'On'. The 'Download new configuration every' is set to 10 minutes, and the 'Upload basic inventory every' is set to 3 hours. The 'Applies To' section shows a table with one entry: 'All Desktop Computers (excluding 'Site Servers')' with a date of 3/22/2018 11:08:44. A yellow arrow points from the 'Configuration Requests' status in the bottom screenshot to this table.

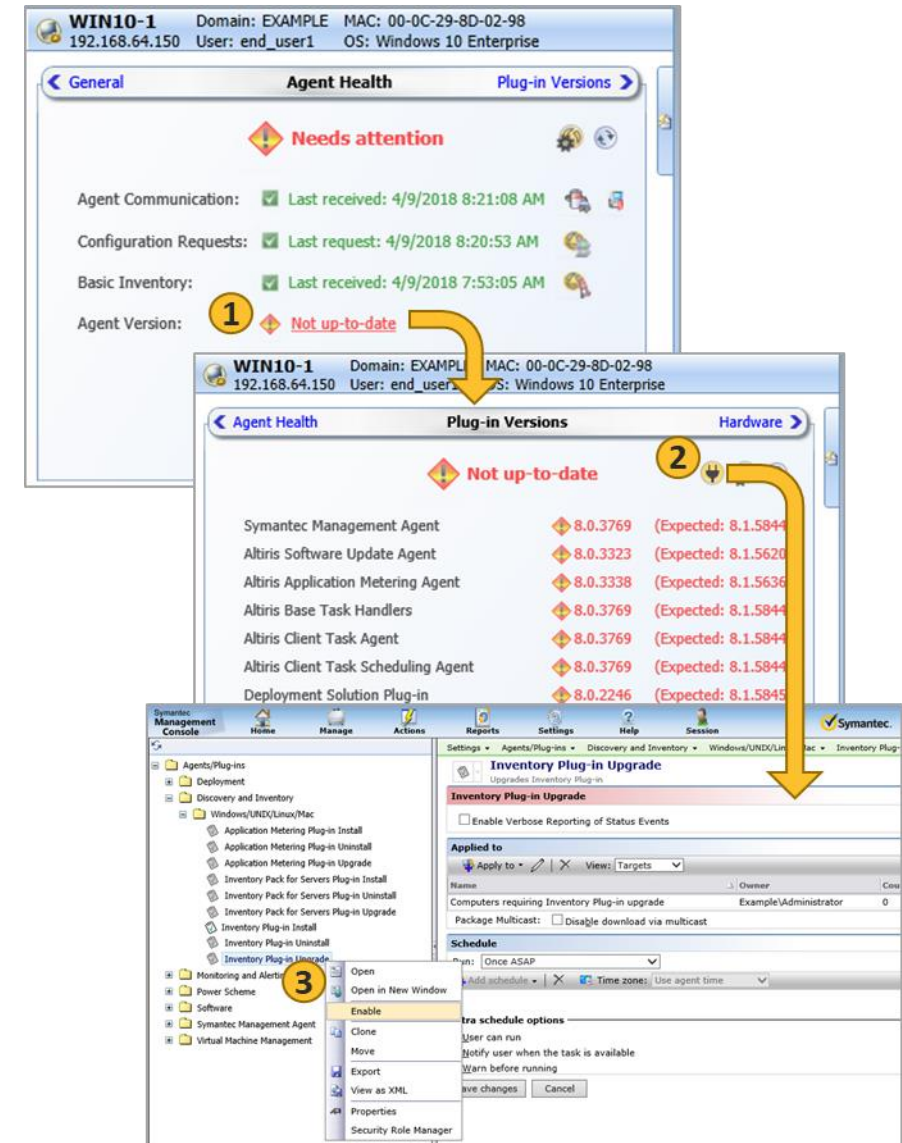
Middle Screenshot: Agent Health
This window shows the 'Agent Health' for a specific endpoint (WIN10-1). The status is 'Needs attention'. The 'Configuration Requests' status is 'Last request: 4/5/2018 12:57:48 PM'. A yellow arrow points from this status to the 'Update Client Configuration' window.

Bottom Screenshot: Update Client Configuration
This window shows the 'Update Client Configuration' progress. The 'Total computers' is 1, and 'In Progress' is 1 (100%). The 'Status' column shows 'Queued'.

SMA Communication Issues



- **Agent Version**
 - If **Red**, it is indicating that there are agent plug-ins that are out of date and need to be updated.
 - The Link of the alert allows you to go to the Plug-In Version flipbook to see the items needing an update
 - **Most likely cause:** A recent SMP update has disabled the 'upgrade' policies of certain agents/plug-ins to reduce load on the notification server
 - Once you review the plug-ins that need updating, press the **Open All Agents/Plug-ins** icon (2)
 - Update the affected Agent or Plug-in by enabling it (3)
 - If the Agent/Plug in does not update
 - Check the state of the client computer (power, network, etc..)
 - Check the Agent Logs and/or Notification Server Logs for errors related to agent or plug-in policies or communications, research and resolve
 - Check Notification Server task and package server state to ensure that actions and packages are able to be executed and distributed



SMA Communication Issues

- **Agent Command Line Options (AeXNSAgent.exe)**
 - Several SMA command line options that can be run on the endpoint to diagnose and resolve issues

Parameter	Description
<code>/? /h /help</code>	Shows this help
<code>/start OR /stop</code>	Starts OR Stops the Agent
<code>/restart</code>	Stops and starts the Agent
<code>/recover</code>	Stops the Agent and restarts it only if it stopped without crashing
<code>/sendbasicinventory</code>	Forces the Agent to send basic inventory
<code>/updateconfiguration</code>	Forces the Agent to update configuration
<code>/resetguid[:<delay sec>]</code>	Resets the Agent ID and forces the Agent to register on Notification Server after the optional delay
<code>/registerguid[:<delay sec>]</code>	Forces the Agent to register on Notification Server after the optional delay
<code>/diags /nodiags</code>	Enables or Disables the Agent diagnostics
<code>/uninstall /clean</code>	Uninstalls the Agent
<code>/uninstallagents</code>	Uninstalls all the installed plug-ins
<code>/registerclient</code>	Registers all COM objects of all *.dll files for Agent installation
<code>/nologging</code>	Disables the error logging
<code>/enablelogging</code>	Enables the default logging (Use <code>/enablelogging:error, warning, info</code> or <code>diags</code> for additional information)
<code>/server:<server> /ns:<server></code>	Switches the Agent to the new Notification Server specified by the host name <server>
<code>/web:<web> /nsweb:<web></code>	Switches the Agent to the new Notification Server specified by the URL <web>

**HOWTO
101012**

Resolving Common Site Infrastructure Issues



Resolving issues in Task Services



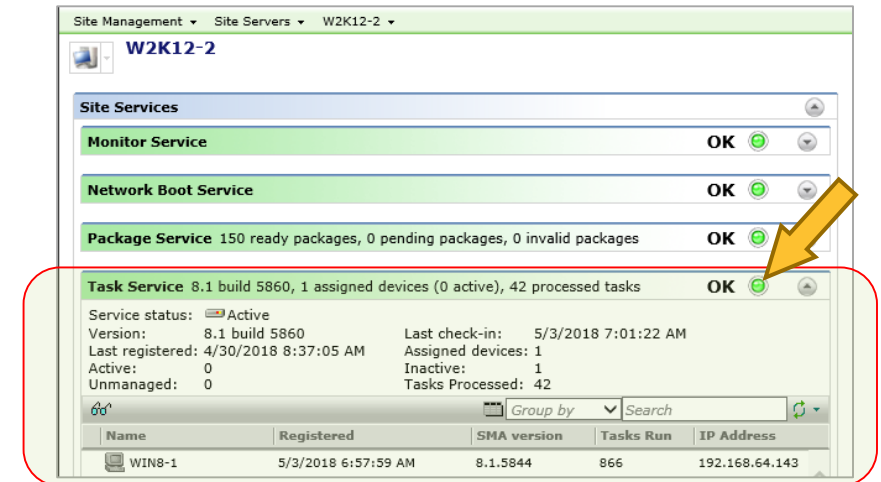
Task Service Registration and Execution Issues



- **Symptoms:**
 - Notification Server has been slow recently so Site Servers were implemented
 - Task Services have been installed on Site Server(s)
 - Some Agents cannot register with the Task Server
 - Tasks are not running on some of the endpoints
- **Testing Approach:**
 - **Ensure that the SMP environment is sound**
 - Properly sized, configured and current health is good
 - **Check Task Service Installation**
 - Are Site Server Logs, Task Services, IIS and other components problem free?
 - **Check Agent State on the Endpoint**
 - Is the Agent registered with a Task Server?
 - Are there task related errors in the Agent Logs?

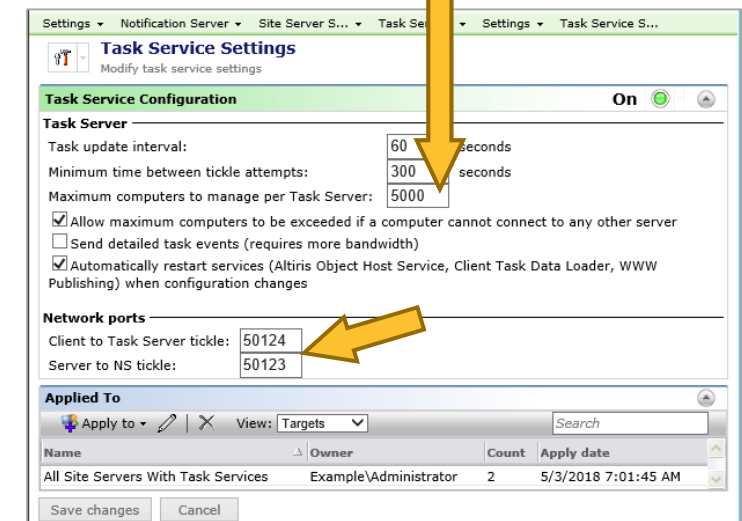
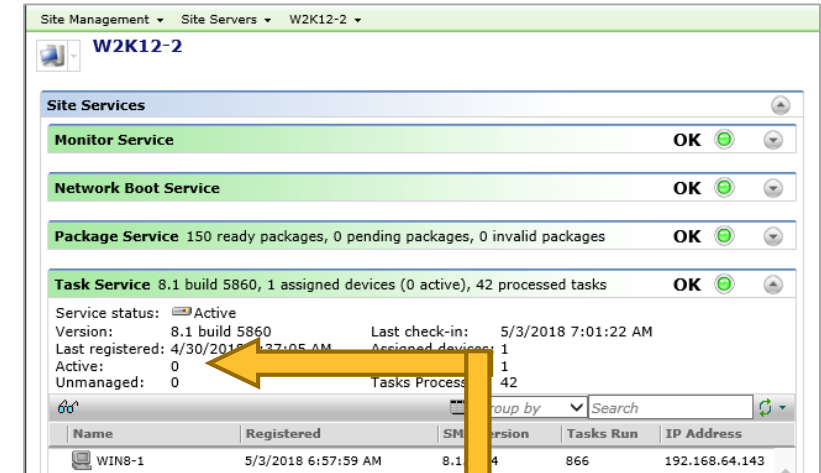
Task Service Registration and Execution Issues

- Check Task Service Installation
 - *On the Notification Server*, Open the Site Management View in the console.
 - Check the status of the Site Server and Task Service



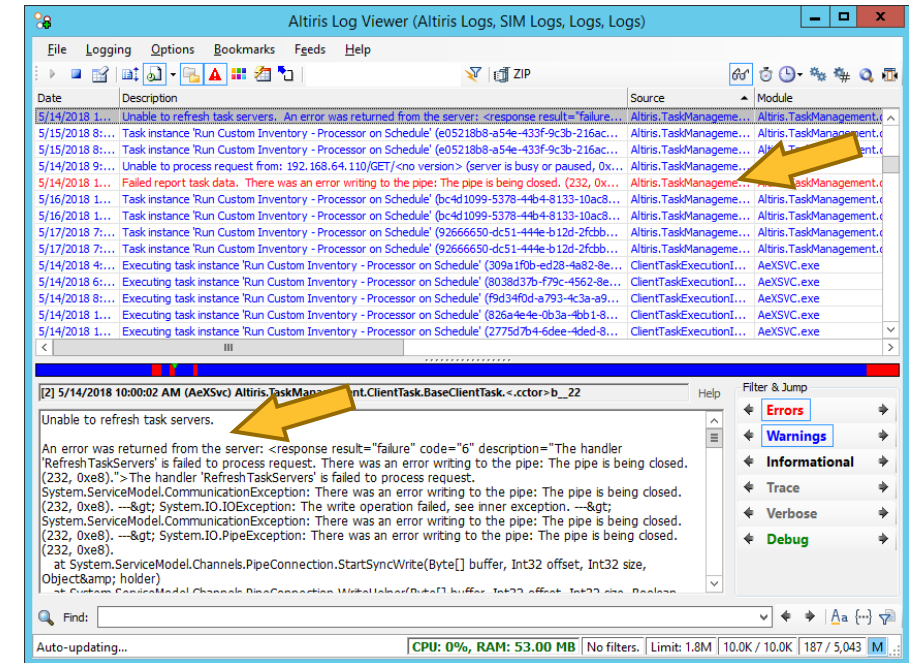
Task Service Registration and Execution Issues

- Check Task Service Installation
 - *On the Notification Server*, Open the Site Management View in the console.
 - Check the status of the Site Server and Task Service
 - Check the Global or Custom Task Server Settings:
 - Check it has not exceeded its maximum connection count
 - Take note of the maximum count and network ports
 - Ensure there are proper firewall rules in place to account for the Network Ports settings (50124 and 50123) within the network



Task Service Registration and Execution Issues

- Check Task Service Installation
 - *On the Notification Server*, Open the Site Management View in the console.
 - Check the status of the Site Server and Task Service
 - Check the Global or Custom Task Server Settings:
 - Check it has not exceeded its maximum connection count
 - Take note of the maximum count and network ports
 - Ensure there are proper firewall rules in place to account for the Network Ports settings (50124 and 50123) within the network
 - Check the NS logs for named Task Service entries
 - Can indicate the source of the issue (i.e., DNS, Services...)
 - Research these items by using the support resources and resolve by following the guidance that is found.



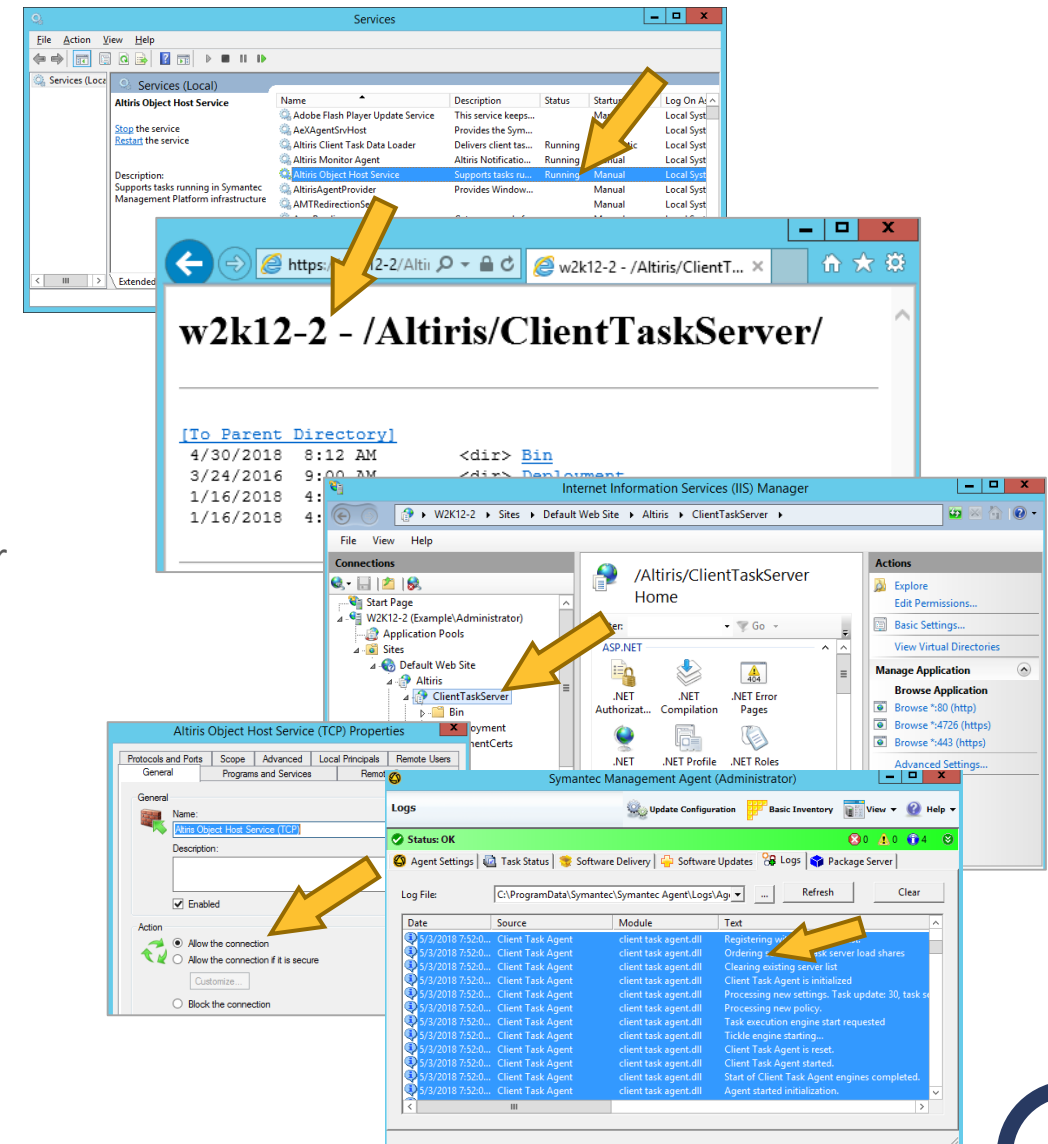
Task Service Registration and Execution Issues



- Check Task Service Installation

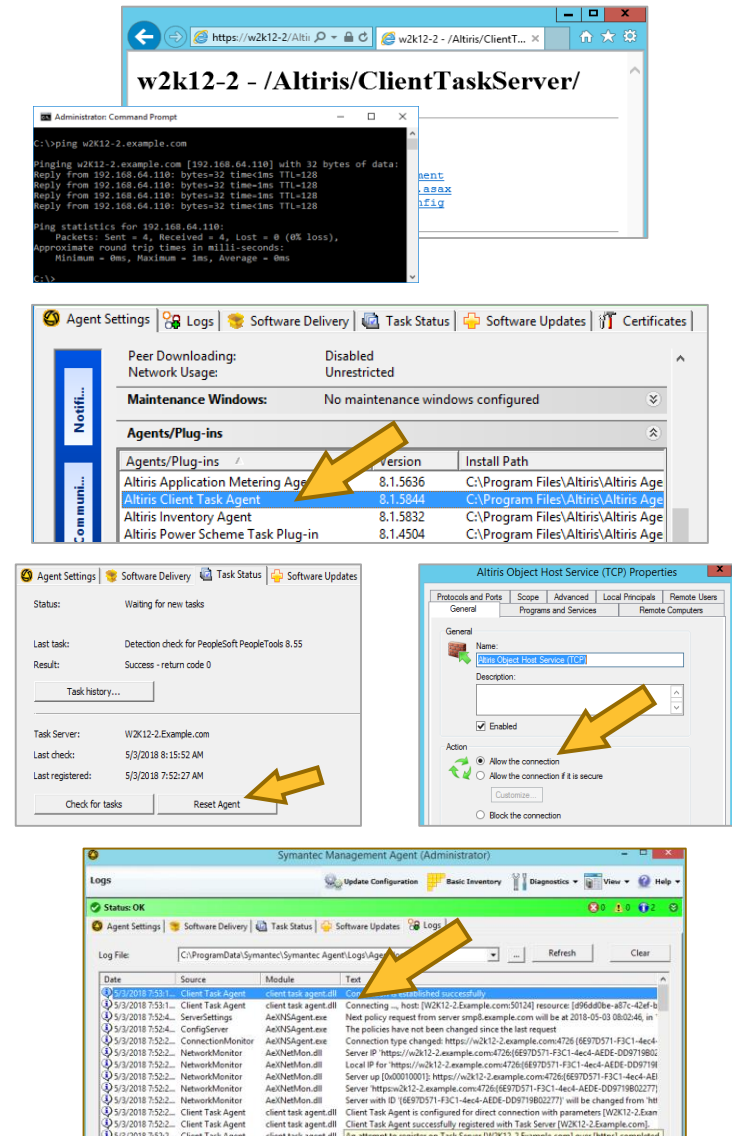
- *On the Site Server:*

- Check that Task Services are running
 - Altiris Object Host Service (AtrHost.exe)
- Check IIS by browsing to the Client Task Server website
 - https://SiteServer_FQDN/Altiris/ClientTaskServer/
 - Will indicate IIS misconfiguration or web service issues
 - May need to grant additional permissions to “Authenticated Users” in the **\Program Files\Altiris** folder
- Check Firewall for exceptions to the Task Service Ports
- Check the **taskmanagement.log** file and **Agent Logs**:
 - Task Service configuration or connection issues
 - Indicating that it has exceeded its maximum allowed connection count
 - That it is rejecting further registration attempts.



Task Service Registration and Execution Issues

- **Check Agent State on the Endpoint**
 - Check that the endpoint can resolve to the Site Server
 - By using Ping, NSLookup, etc.,
 - Browse to the Site Server task website
 - Ensure that the Client Task Plug-in is the latest version
 - Mismatches cause loss of connection or registration.
 - Check Firewall for exceptions to the Task Service Ports
 - Reset the Task Server registration on the Endpoint
 - **Reset Agent** in Agent UI can return it to a stable state
 - Check the Agent Logs for Client Task related errors
 - Provides insight into configuration or registration issues
 - Pay particular attention registration attempt and tasks
 - Research these items by using the support resources
 - Resolve by following the guidance that is found.



Resolving issues in Package Services



Package Service Operation & Distribution Issues



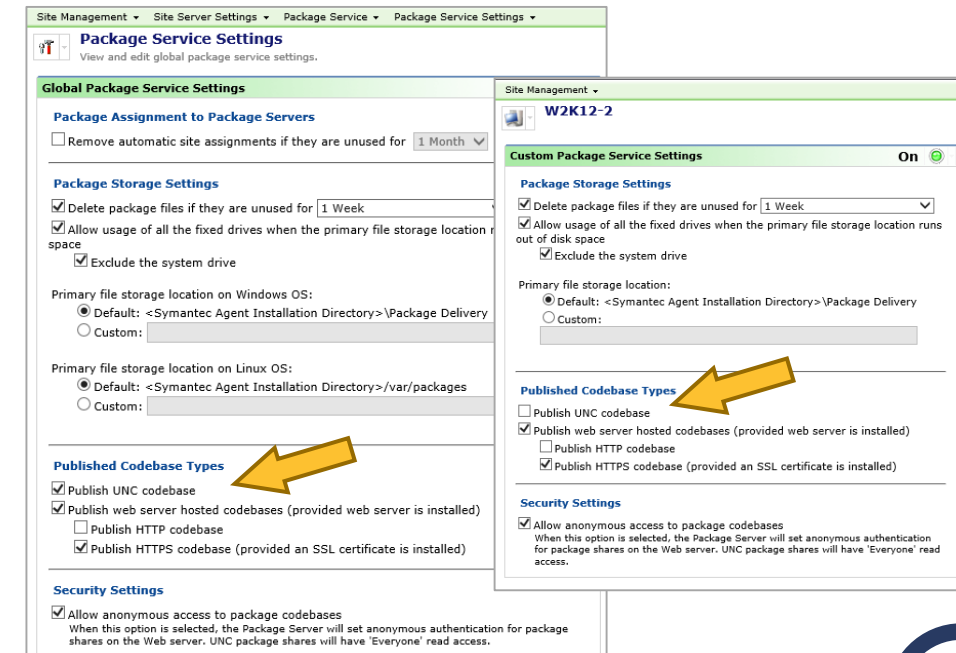
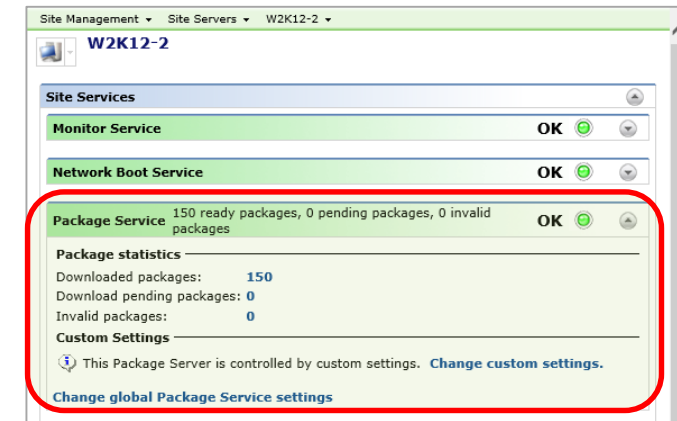
- **Symptoms:**
 - Bandwidth usage has increased so Site Servers were implemented
 - Package Services have been installed on Site Server(s)
 - Package Servers not populating or updating properly
 - Endpoints are not receiving packages
- **Testing Approach:**
 - **Ensure that the Site Server environment is sound**
 - Properly sized, configured and current health is good
 - **Validate Site Server Configuration**
 - Are Package Service Policies, IIS and other components problem free?
 - **Validate Package Services Operation**
 - Are the Package Statuses, Codebases, Synchronization and Share Permissions correct?

Package Service Operation & Distribution Issues



- **Validate Site Server Configuration**

- *On the Notification Server*, Check the status of the Site Server and Package Service
 - If **Download Pending Packages** are indicated:
 - Refresh the view and observe over time for a decrease
 - Continue to the steps in “**On the Site Server**” in this lesson
 - If **Invalid Packages** are indicated:
 - Check for sufficient storage space on the Site Server
 - Check the Global or Custom Package Service Settings:
 - Anonymous access to package codebases disabled OR the specified ACC cannot be applied to the downloaded file.
 - Check the SWD Package or Policy for improper settings



Package Service Operation & Distribution Issues



- **Validate Site Server Configuration**

- *On the Notification Server*, Check the status of the Site Server and Package Service
 - If **Download Pending Packages** are indicated:
 - Refresh the view and observe over time for a decrease
 - Continue to the steps in “**On the Site Server**” in this lesson
 - If **Invalid Packages** are indicated:
 - Check for sufficient storage space on the Site Server
 - Check the Global or Custom Package Service Settings:
 - Anonymous access to package codebases disabled OR the specified ACC cannot be applied to the downloaded file.
 - Check the SWD Package or Policy for improper settings
- Verify that the Resultant Policy matches the Site Server

The image displays three screenshots from the Symantec management console, illustrating the process of validating site server configuration for package services.

Top Screenshot: Site Services Overview
This view shows the status of various services for site W2K12-2. The **Package Service** is highlighted with a red box, indicating "150 ready packages, 0 pending packages, 0 invalid packages".

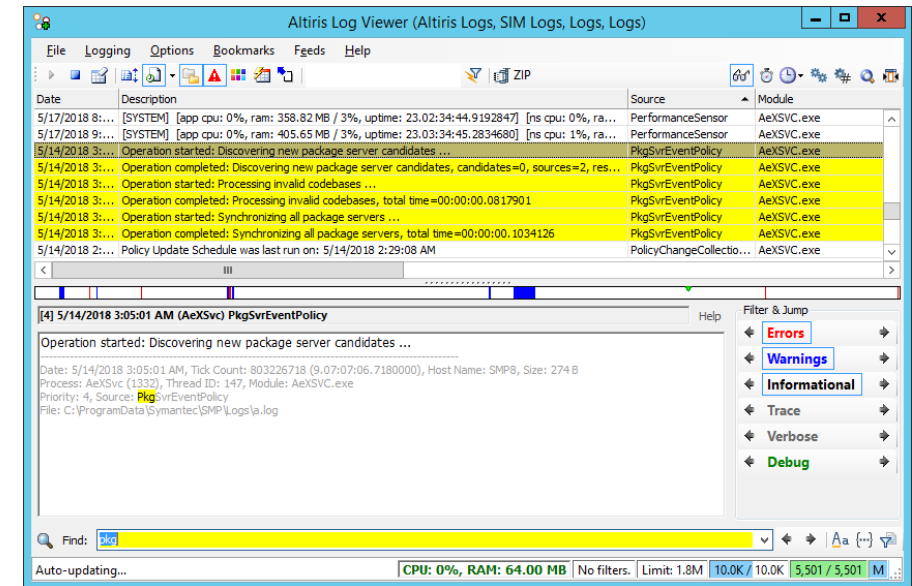
Middle Screenshot: Package Service Settings
This view shows the configuration for the Package Service. The **Package Statistics** section shows 150 downloaded packages, 0 pending packages, and 0 invalid packages. The **Custom Settings** section indicates that the Package Server is controlled by custom settings. A red box highlights the **Package Storage Settings** section, which includes options for deleting package files, allowing usage of all fixed drives, and excluding the system drive.

Bottom Screenshot: Global Package Service Settings
This view shows the global settings for the Package Service. The **Package Assignment to Package Servers** section shows that automatic site assignments are enabled. The **Package Storage Settings** section shows that package files are deleted if unused for 1 week, and that usage of all fixed drives is allowed. The **Published Codebase Types** section shows that UNC, HTTP, and HTTPS codebases are published. The **Security Settings** section shows that anonymous access to package codebases is allowed.

Package Service Operation & Distribution Issues

- **Validate Site Server Configuration**

- *On the Notification Server*, Check the status of the Site Server and Package Service
 - If **Download Pending Packages** are indicated:
 - Refresh the view and observe over time for a decrease
 - Continue to the steps in “**On the Site Server**” in this lesson
 - If **Invalid Packages** are indicated:
 - Check for sufficient storage space on the Site Server
 - Check the Global or Custom Package Service Settings:
 - Anonymous access to package codebases disabled OR the specified ACC cannot be applied to the downloaded file.
 - Check the SWD Package or Policy for improper settings
- Verify that the Resultant Policy matches the Site Server
- Check the NS logs for named Package Service entries
 - Confirm Issues then Research & Resolve using support resources

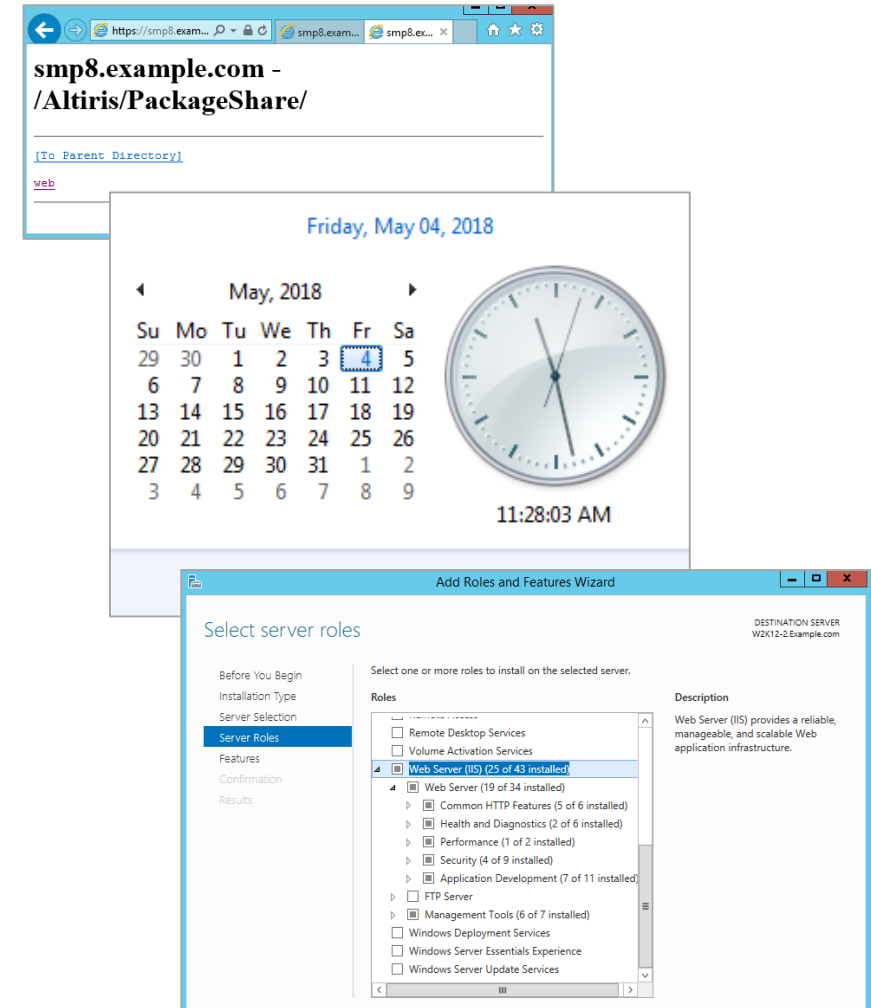


Package Service Operation & Distribution Issues



- **Validate Site Server Configuration**

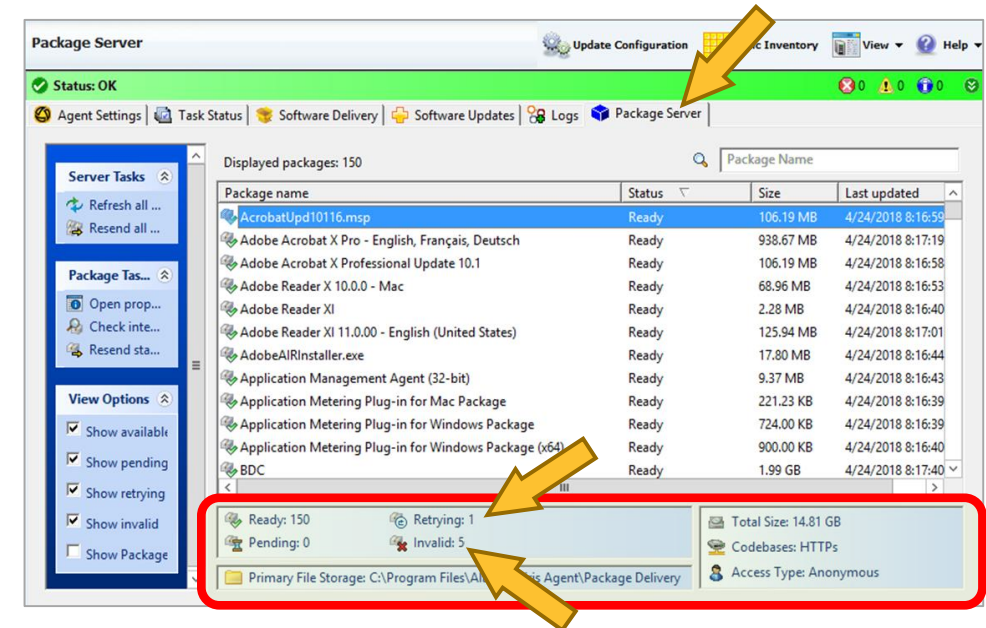
- *On the Site Server*
- Check that the endpoint can resolve to the Site Server
 - By using Ping, NSLookup, etc.,
 - Browse to the NS Package website
- Ensure that the Client Task Plug-in is the latest version
 - Mismatches cause validation and distribution issues.
- Ensure date/time are correct on the NS and Site Server.
- Ensure that the IIS configuration is sound for HTTP(S)
 - SEE: <http://www.symantec.com/docs/TECH240152>
- Check the Agent Logs for Package related errors
 - Provides insight into package distribution issues
 - Pay particular attention to Package Refresh/Status errors
 - Research these items by using the support resources
 - Resolve by following the guidance that is found.



Package Service Operation & Distribution Issues



- **Validate Package Services Operation**
- Check the status of the Site Server and Package Service
 - Open the Symantec Management Agent > Package Server tab.
 - If there are Packages in the **Pending**, **Invalid** or **Retrying** status then typical symptoms could include the following:
 - Stale Codebases
 - Invalid Packages
 - Packages won't download to clients
 - Packages Not Ready
 - Error while downloading package: Server is busy.
- Perform the following steps in order and test at each stage:
 1. Verify Package Status
 2. Recreate Codebases
 3. Perform a Manual Synchronization
 4. Check Share Permissions

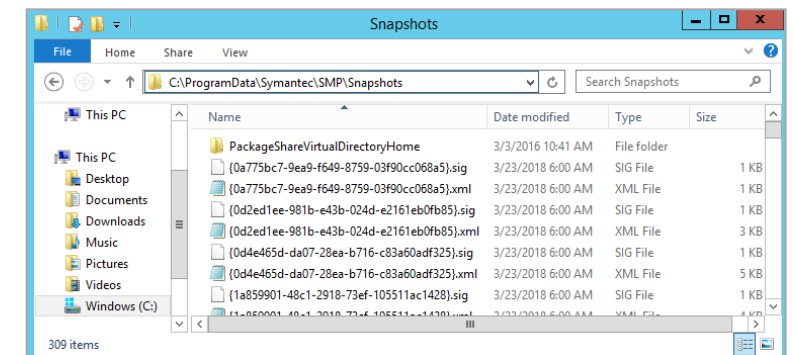
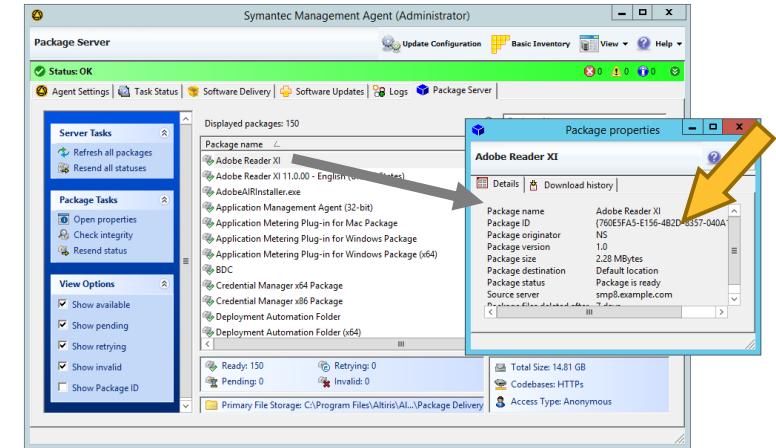


Package Service Operation & Distribution Issues



Step 1: Verify Package Status

- **On the Site Server:**
 - Gather the GUID of one or more affected packages on the Package Server
 - Double Click the affected package and review the Details Tab of the Properties page.
- **On the Notification Server:**
 - Open the Snapshots folder: `C:\ProgramData\Symantec\SMP\Snapshots\`
 - If the {GUID}.xml file(s) exists, move on to the next step in the process, as the Notification Server is properly creating the snapshot for the package.
 - If there is no snapshot.xml for a specific package found in the “.\Snapshots” folder then it means that the NS has not built or maintains the package.
 - **The path to the package could not be verified.** correct the problem by editing the package and pointing it to the correct path.
 - **The origination server of the package may be different than that of the local NS.** In this case you would have to investigate the origin of the package file and its Notification Server.

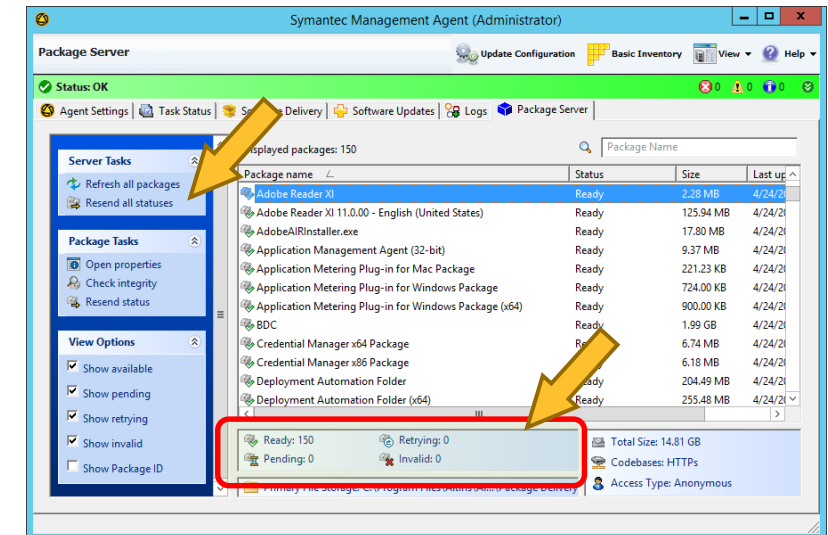
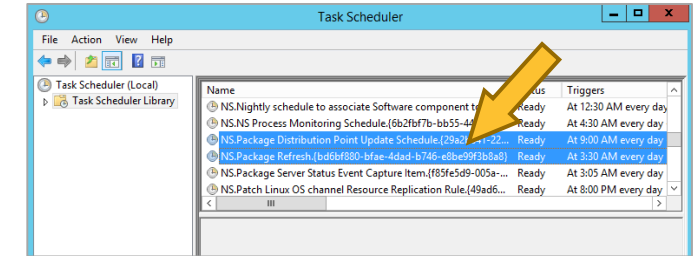


Package Service Operation & Distribution Issues



Step 2: Recreate Codebases

- **On the Notification Server:**
 - Run the following Windows Scheduled Tasks manually or wait for them to run on schedule overnight.
 - **NS.Package Distribution Point Update Schedule**
 - **NS.Package Refresh**
 - The Package Codebases are now rebuilt on the Notification Server.
 - NOTE: See article TECH26028 for more information if the tasks don't run
- **On the Site Server:**
 - Open the SMA and click on the "Refresh All Packages" and "Resend Package Status" tasks in order to refresh and update all package information.
 - Once this completes, the **SWDPackageCodebase** table on the NS will be completely rebuilt.
 - Review the status of the Package Server to see if it resolves the issues, if it doesn't, move on to the next troubleshooting step.



Package Service Operation & Distribution Issues



Step 3: Manual Synchronization

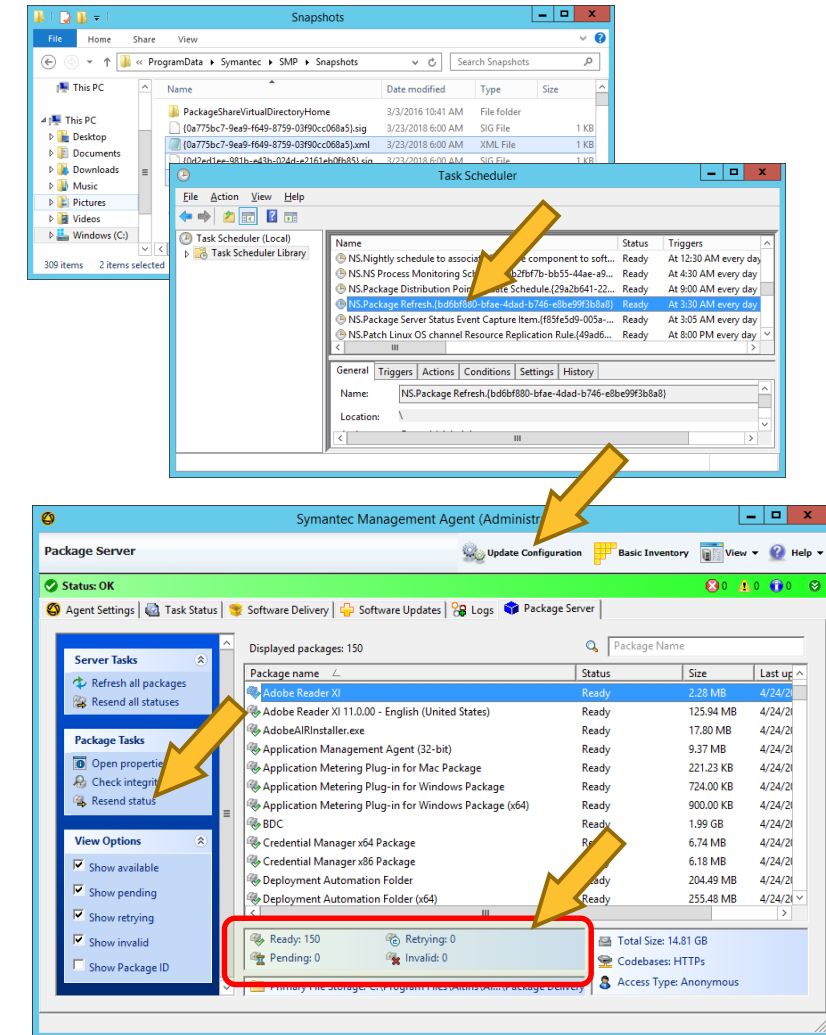
• On the Notification Server:

1. Take note of the GUIDs of the affected packages from Step 1.
2. Delete the affected snapshot(s) that are in the form **{GUID}.xml** found here: C:\ProgramData\Symantec\SMP\Snapshots
3. Run the Windows Scheduled task called **NS.Package Refresh.{GUID}**.
 - This will re-create the package snapshots on the server.
4. Make sure that the scheduled task does in fact start. If not see: **TECH26028**

• On the Site Server:

1. Delete the affected snapshot(s):
%ProgramFiles%\Altiris\Altiris Agent\Package Delivery\{GUID}\snapshot.xml
2. Delete the .xml file here: %ProgramFiles%\Altiris\Altiris Agent\Client Policies\<NS name>.xml
3. Open the SMA and click on Update Configuration.
4. Open the Package Server tab and click on the Resend Package Status button.
5. Review the status of the Package Server to see if it resolves the issues, if it doesn't, move on to the next troubleshooting step.

CAUTION: There are implications when taking this approach as all clients will download the new version. This will potentially generate a lot of IIS and Network traffic.



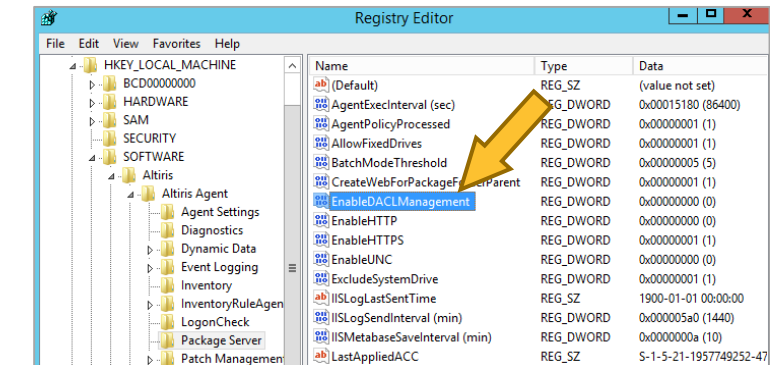
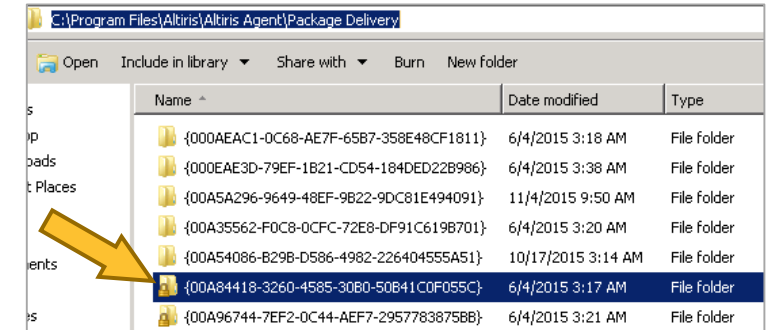
Package Service Operation & Distribution Issues



Step 4: Check Share Permissions on the Site Server

- Look for 'locked' folder icons under
...\\Program Files\\Altiris\\Altiris Agent\\Package Delivery
- If they have a lock:
 1. Check the registry for the "EnableDACLManagement" key under HKLM\\SOFTWARE\\Altiris\\Altiris Agent\\Package Server
 2. Stop the Symantec Management Agent and World Wide Web Publishing Services.
 3. Set the "EnableDACLManagement" DWORD registry key to '0'
 4. Run the following command against the affected directory:
`icacls "<Package GUID>" /t /reset`
 5. Start the Symantec Management Agent and World Wide Web Publishing Services.

This Package Server will now function as normal by applying and resetting permissions on package directories per Package Server Settings on the Notification Server.



Cloud Enabled Management Issues



Cloud Enabled Management Issues



- **Symptoms:**
 - **Organization wished to extend management reach so CeM infrastructure implemented**
 - CeM Site, Internet Gateways, Internet Site Servers and CeM Agents deployed
 - CeM Infrastructure is considered sound and operating as designed
 - **Some Agents cannot register with the Notification Server or Internet Gateway**
 - **Some Agents losing connection to the Notification Server or Internet Gateway**
- **Testing Approach:**
 - **Validate the CeM Infrastructure Implementation**
 - CeM Agent Site
 - Internet Gateway
 - Internet Site Servers
 - **Validate the CeM Agent Implementation**
 - Check CeM Settings Policies
 - Check CeM Installation Packages
 - **Adjust depending on results**

Cloud Enabled Management Issues



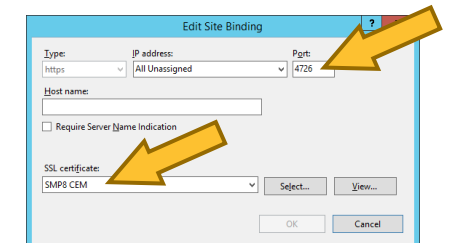
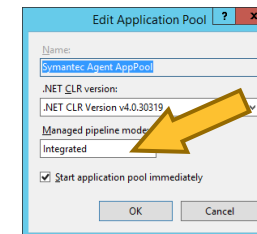
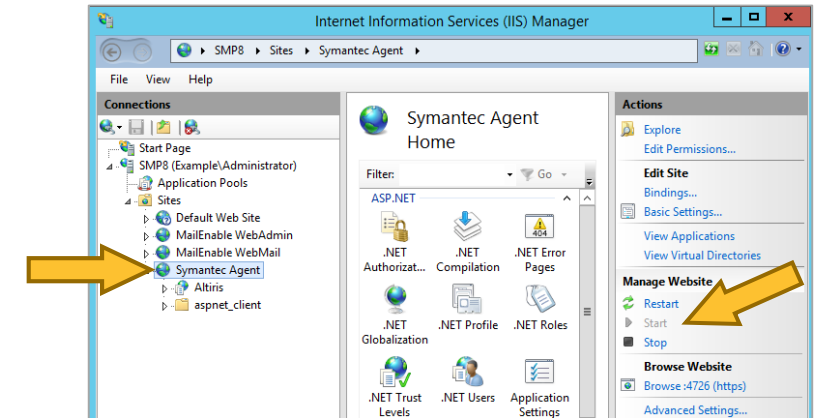
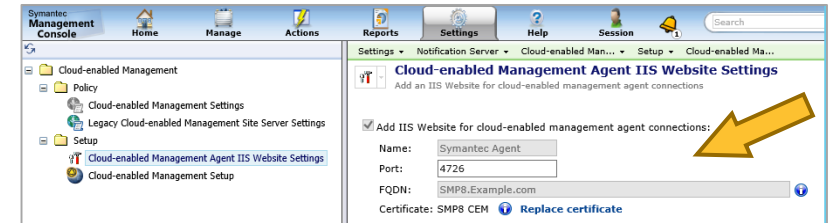
- In this phase we will assume the following:
 - **The CeM Infrastructure has been previously implemented:**
 - Agent Site, Internet Gateway and Internet Site Servers
 - **Self Signed Certificates have been used in all aspects of design**
 - 3rd Party, PKI and other methods not covered in this course
 - **CeM Infrastructure was installed using standard guidance**
 - CeM Whitepaper for ITMS 8.1 [DOC9321](#)
 - **This lesson will help you to quickly resolve most issues**
 - Over 90% of the issues that are seen in customer environments
 - **Take the time to understand certificate use** in the SMP, SMA, Site Server and CeM environments
 - Read the chapter “**About SSL certificates**” found in the CeM Whitepaper for ITMS 8.1 [DOC9321](#)

Cloud Enabled Management Issues



Validate the CeM Infrastructure Implementation

- Check the CeM Agent IIS Website (installation/Operation)
 - **CeM Agent IIS Website Settings:**
 - *Add IIS Website for...* is checked
 - Name/FQDN are greyed out
 - *Should not be set to Port: 443 – (4726 or custom port)*
 - **IIS Manager:**
 - Should exist and running as the “Name” you defined above
 - Should have the CeM Certificate binding to HTTPS on TCP Port 4726
 - Ensure the **Symantec Agent AppPool** is switched to Integrated Mode
 - **Windows Firewall:**
 - Exception - Inbound/Outbound on TCP port 4726



Cloud Enabled Management Issues



Validate the CeM Infrastructure Implementation

- Check the Internet Gateway Manager Configuration
 - **Under General:**
 - Internet Gateway Service should be running and at the latest version
 - Thumbprint shown should match your CeM Settings Policy
 - **Under Servers:**
 - All NS/SS in the “Internet Site” you define should be in the gateway
 - Servers should be in good status with proper DNS names indicated
 - All Servers should be configured for TCP port 4726 (or defined)
 - **Under Settings:**
 - Incoming TCP port set to 443 (or defined) from a **single** IP
 - **Under About:**
 - Look for any recent **Errors** or **Warnings** in the logs
 - Log Viewer configured to also show Apache service messages
 - Use Symantec Support, Symantec Connect to research and solve
 - Also consult the CeM Whitepaper for ITMS 8.1 [DOC9321](#)

The screenshots illustrate the configuration of Cloud-enabled Management Settings in the Symantec Management Console:

- Internet Gateway Setup:** Shows the 'General' tab with 'Port for incoming connections' set to 443 and 'Listen to IP addresses' set to 192.168.64.152.
- Internet Gateway Service:** Shows the 'General' tab with 'Service Status' as 'Stopped' and a 'Gateway Certificate Thumbprint' of d7 5b 96 eb 93 53 9c 0a bc 14 cf 3c 6f af 24 78 cb d8 90 54.
- Cloud-enabled Management Settings:** Shows the 'Policy - Cloud-enabled Management Settings' window with 'Gateways accepting external agent traffic' set to 'On'. A table lists the gateway configuration:

Gateway	Port	Thumbprint
W2K12-1.Example.com	443	d7 5b 96 eb 93 53 9c 0a bc 14 cf 3c 6f af 24 78 cb d8 90 54

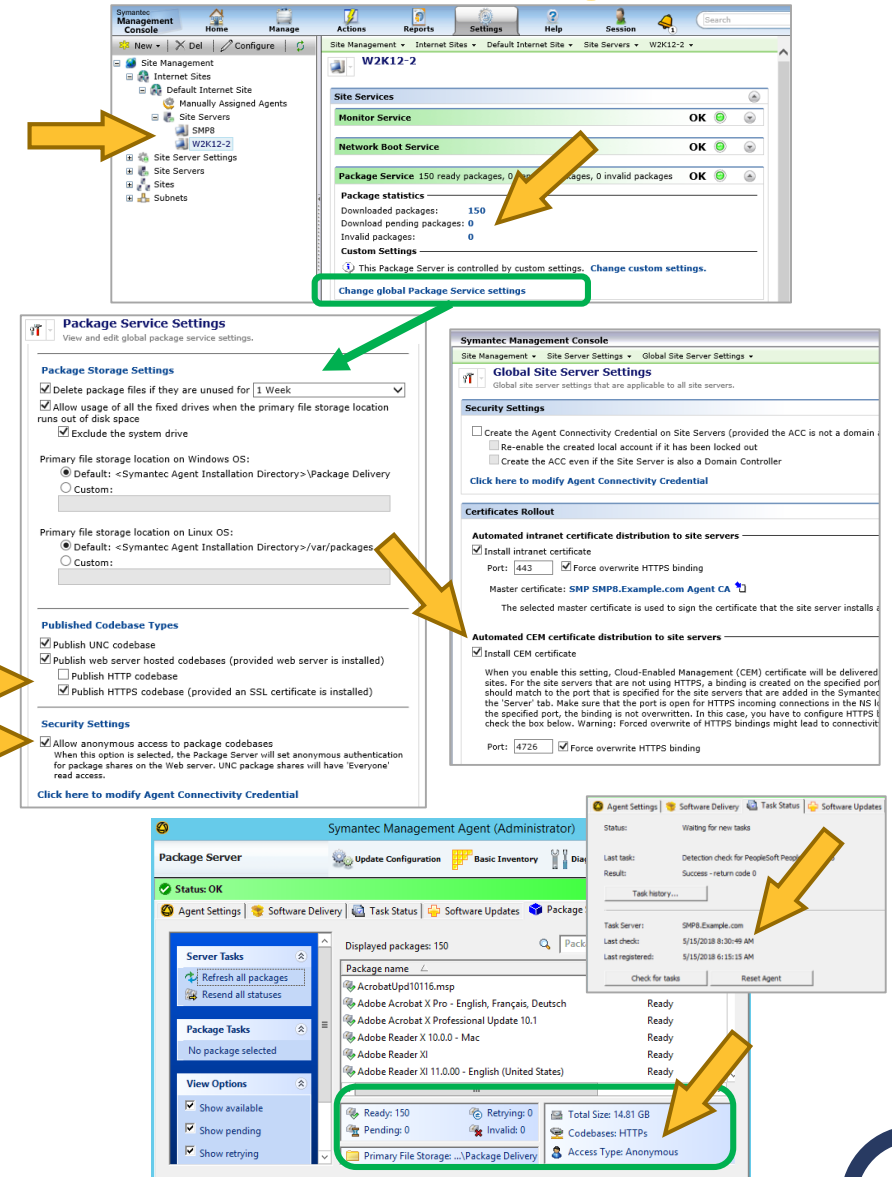
- Site Servers:** Shows the 'Site Servers' list with 'W2K12-2' selected.
- Site Server Settings:** Shows the 'General' tab for 'w2k12-2.example.com:4726' with 'Status report' set to 'Enabled'.
- Altrix Log Viewer:** Shows the 'Logs' tab with 'InternetGatewayStatus' selected, displaying logs for the 'Child process is running'.
- httpd.conf:** Shows the 'Global settings' section with 'ServerName localhost'.

Cloud Enabled Management Issues



Validate the CeM Infrastructure Implementation

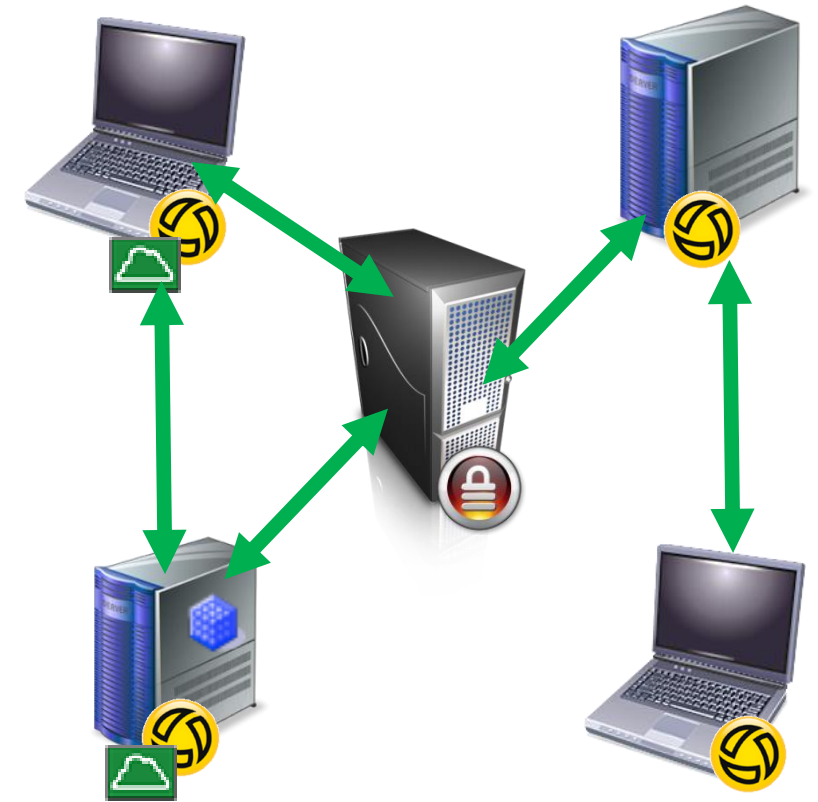
- Check the Internet Site Server configuration
 - **On the Console:**
 - Desired Site Servers are listed in the Default Internet Site
 - Site Servers have Package Services installed and functional
 - Site Server is configured properly to service CeM Endpoints
 - HTTPS Codebases enabled (Enable UNC and/or HTTP if used for Intranet Clients)
 - CeM Certificate Distribution enabled
 - “Force overwrite HTTPS binding” only if required
 - Anonymous or ACC set and tested
 - **On the Site Server:**
 - HTTPS codebases are enabled and reflects the Access Type
 - Packages are in a Ready state with no Invalid or Pending states
 - Site Server is registered to the Notification Server’s Task Service
 - Check the Agent Logs for any HTTP Connection, Network or Package Server errors
 - Research these errors on support resources and resolve as instructed.



Cloud Enabled Management Issues

Validate the CeM Infrastructure Implementation

- **Test All Communication Paths – Most Likely Cause**
- NS → IG, IG → NS, Agent → IG, Agent → Internet SS...
- 1. PING for name resolution (FQDN)
 - PING *NS_FQDN*
 - PING *SiteServer_FQDN*
 - PING *IG_FQDN* 4726 (FQDN listed in Certificate)
 - Resolve communication issues if errors present
- 2. NSLOOKUP for correct IP Addresses and DNS entries
 - NSLOOKUP *NS_FQDN*
 - NSLOOKUP *NS_IP_Address*
 - Resolve communication issues if errors present
- 3. TELNET for correct FQDN and Port numbers
 - TELNET *NS_FQDN* 443 on LAN or 4726 on WAN
 - TELNET *IG_FQDN* 4726 (FQDN listed in Certificate)
 - TELNET *SiteServer_FQDN* 443 on LAN or 4726 on WAN
 - Resolve communication issues if errors present



Cloud Enabled Management Issues



Validate the CeM Agent Implementation

- **Common areas to investigate:**
 - Ensure communication flow
 - Ping, Telnet (443) and NSLookup the FQDN of the IG
 - Browse to the NS or SS Website - ***https://FQDN/Altiris***
 - Check firewall rules, TCP Port 443 must be permitted
 - Check that the Endpoint Date/Time is correct
 - Check the Agent Settings
 - Defined NS is OK
 - Enabled for SSL – using proper port (443)
 - Check Network Status and Certificate Settings
 - Ensure that the CeM Mode matches the current state
 - Check the Agent Certificates for warnings
 - Check the Agent Log for Errors
 - Look for any HTTP Connection, Network or Certificate errors
 - Research these errors on support resources and resolve as instructed.
 - Check the CeM Settings Policy
 - Was it received?, is it the correct one?

The top screenshot shows the 'Agent Settings' window with the 'Identification' tab selected. The 'Notification Server' is set to 'smg8.example.com' and the 'Notification Server URL' is 'https://smg8.example.com:443/altiris'. The 'Computer ID' is '46992A04-5CDB-A4E3-A452-63103C9F4823' and the 'Computer Name' is 'WIN10-1.Example.com'. The 'Configuration' tab shows 'Last changed on 5/14/2018 1:09:00 PM'. The 'Basic Inventory' tab shows 'Last sent on 5/14/2018 12:19:12 PM'. The 'Network Status' tab shows 'Connected via internet gateway', 'Cryptographic protocol: TLS 1.2', 'Cipher suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384', and 'CEM Mode: Cloud-enabled Management mode is active'. The 'Peer Downloading' and 'Network Usage' are both 'Disabled' and 'Unrestricted' respectively.

The bottom screenshot shows the 'Certificates' window with a list of certificates. The 'Certificates' tab shows a list of certificates with columns for 'Friendly Name', 'Store', 'Usages', 'Sources', and 'Thumbprint'. The 'Logs' window shows a log entry for 'Validating certificate store: Trusted Root Certification Authorities' with a status of 'OK'. The 'Policies' window shows the 'Cloud-enabled Management Settings' policy.

Cloud Enabled Management Issues

Validate the CeM Agent Implementation

• Common CeM Agent Endpoint Issues:

1. Endpoint is connected to NS via IG but unable to register with NS

- **Cause:** User Added **NS_FQDN:443** on IG, instead of **NS_FQDN: 4726**
- **Solution:** Remove **NS_FQDN:443** on IG, and add **NS_FQDN: 4726**

2. Endpoint is unable to retrieve packages from Site Server in CeM Mode

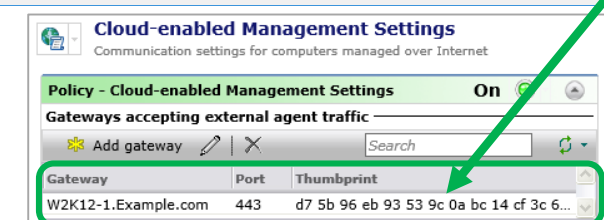
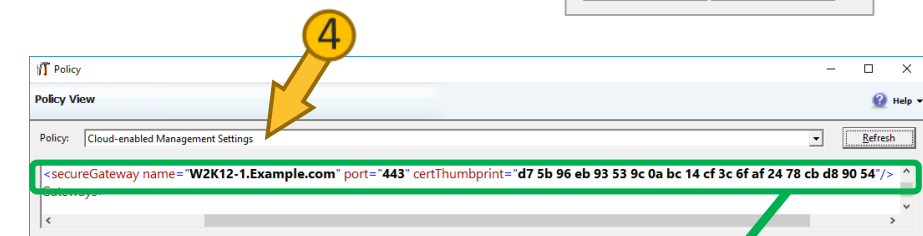
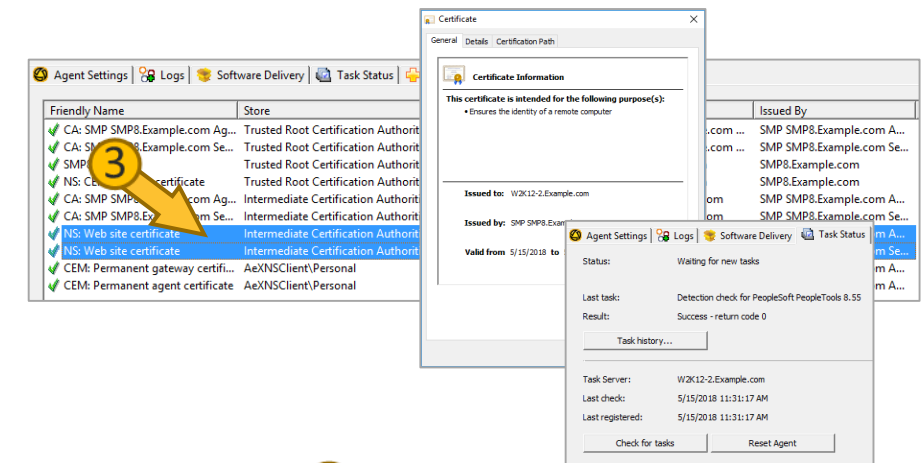
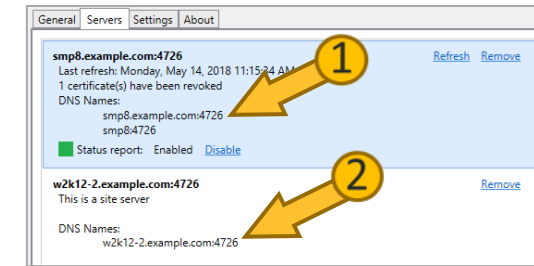
- **Cause:** User Added **SS_FQDN:443** on IG, instead of **SS_FQDN: 4726**
- **Solution:** Remove **SS_FQDN:443** on IG, and add **SS_FQDN: 4726** – This is the new port assigned to all Internet Site Servers since version 8.0.

3. Endpoint is unable to register with remote Task Server in CeM Mode

- **Cause:** Endpoint is missing the Site Server certificates
- **Solution:** Install Site Server's certificate in "Trusted Root Certification Authorities" on the Endpoint by CeM Certificate Policy or Manual means.

4. Unable to establish connection to IG or NS

- **Cause:** Network connection issues between Endpoint and Internet Gateway or invalid CeM Settings Policy
- **Solution:** Check that the IG and Endpoint resolve each other by Hostname/FQDN/IP, then check that the CeM Settings policy is set for the proper FQDN, Port (443) and Thumbprint.



Resolving Issues in Inventory Solution



Inventory Solution Issues

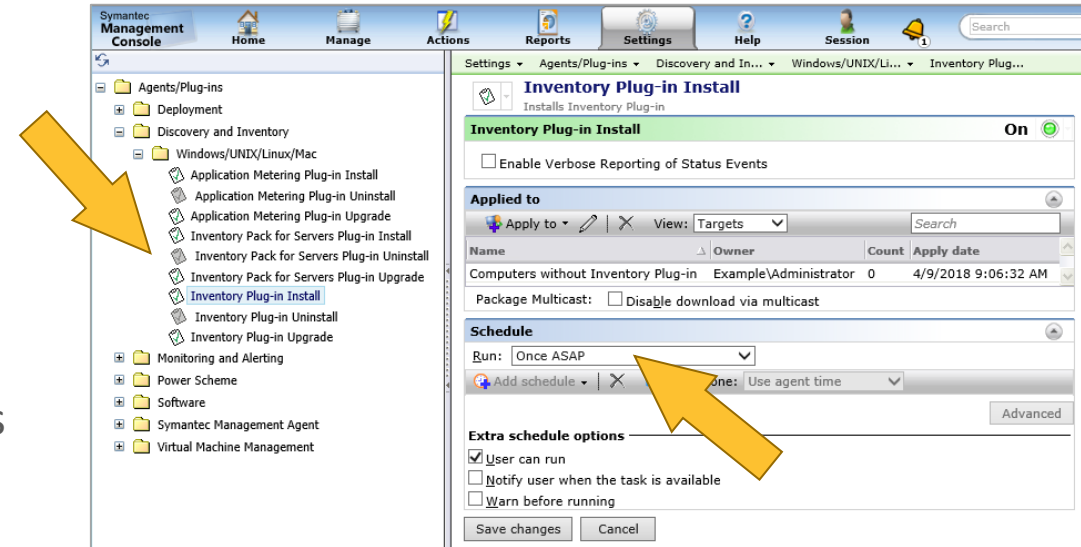


- **Symptoms:**
 - **Inventory Solution has been installed as a part of the ITMS implementation**
 - **Inventory Solution plug-ins have been deployed and policies created**
 - **Inventory information seems out of date in reports and console views**
 - **Inventory information seems to be missing for some endpoints**
- **Testing Approach:**
 - **Ensure the ITMS Implementation is sound**
 - Is the Overall SMP/Site Implementation sound?
 - Is the Database Implementation sound and Health?
 - Are the Event Queues Healthy
 - Are Inventory, Application Metering and even CMDB and Asset licenses valid?
 - **Validate Agent and Plug-in State**
 - Symantec Management Agent
 - Inventory, Application Metering Plug-ins
 - **Validate Inventory Solution Policies**
 - Are Inventory and Discovery Policies valid?
 - **Validate Endpoint and Server Inventory Processes**
 - Is the Inventory gathering and reporting process working as designed?

Inventory Solution Issues

Validate SMA and Inventory Plug-in State

- Check Agent and Plug-in Rollout
 - Verify the installation and upgrade policies are turned on and targeting machines as appropriate.
- To review the Policies:
 - **Settings > Agent / Plug-ins > All Agent / Plug-ins.**
 - Review the SMA / Inventory Plug-in policies.
 - Verify that the policies are enabled
 - Verify that the applied to section is targeting endpoints
 - If the “Run Once ASAP” option is selected with no schedule, it will only attempt to install/upgrade once.
 - If it has a schedule, check that the schedule includes a repeat to ensure the success of the install/upgrade.
 - In the schedule section, click the advanced button and verify that the settings are not interfering with the install/upgrade.

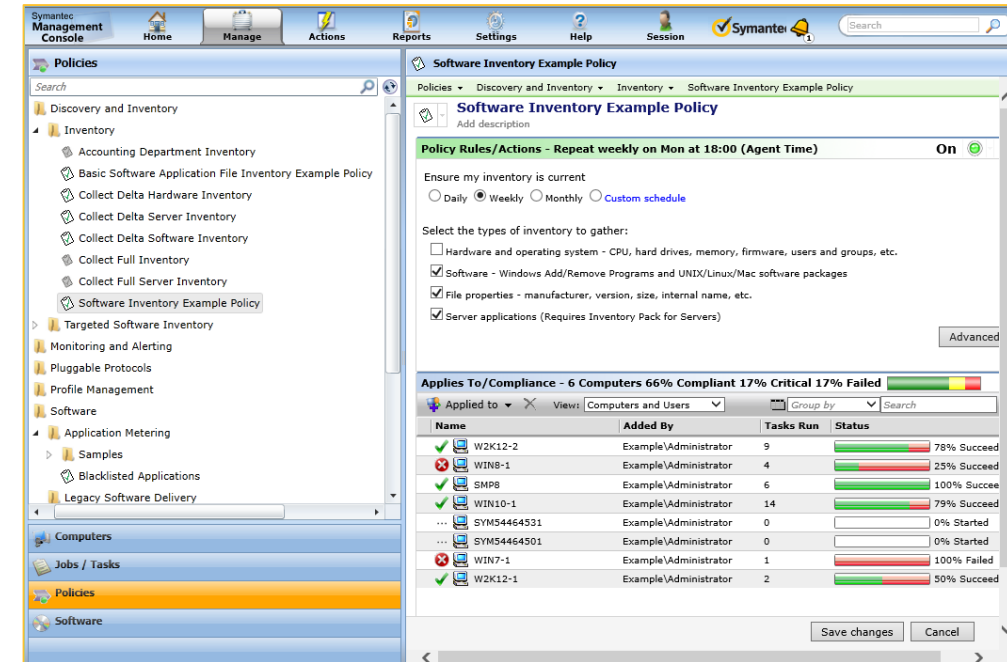


Inventory Solution Issues



Validate Inventory Solution Policies

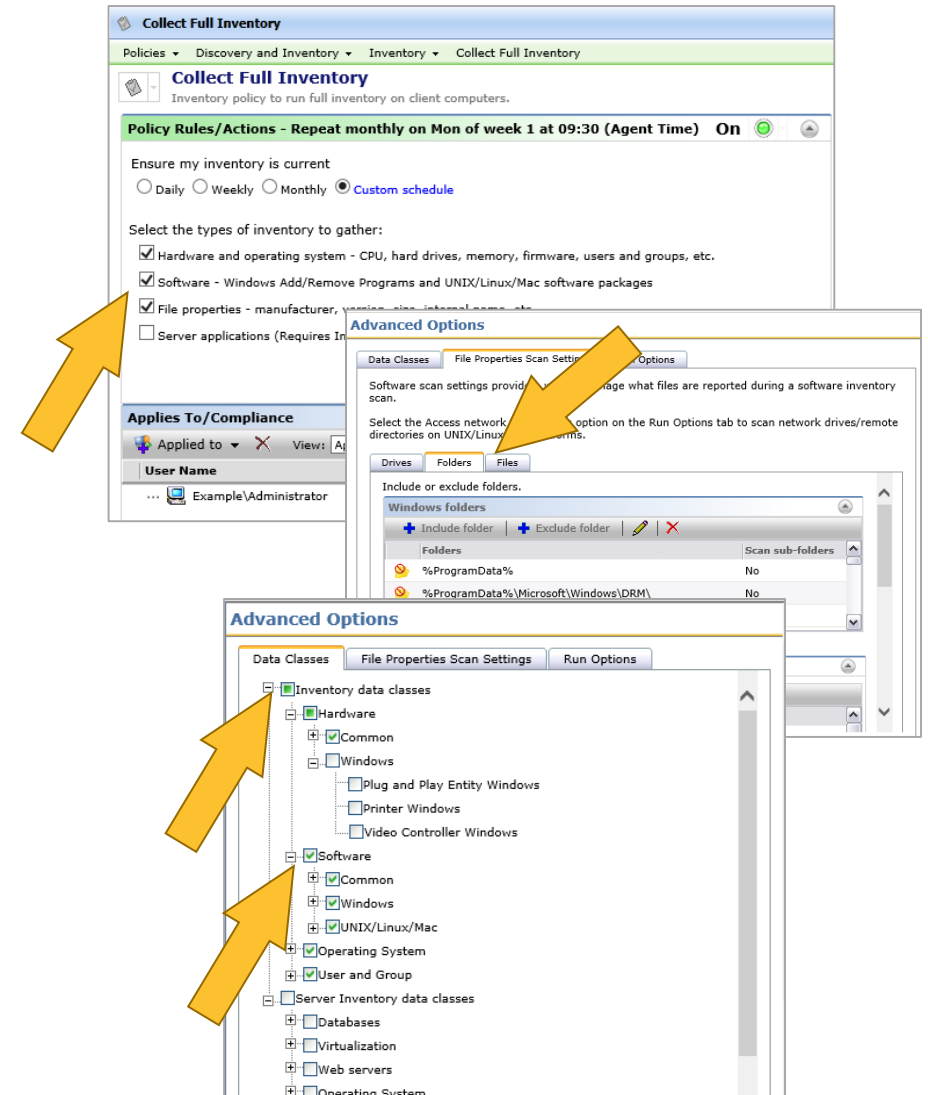
- Policies are instructions for the endpoints, telling them
 - What to inventory
 - When to run the inventory
 - Under what conditions to run the policy.
- A full inventory must be run once before delta inventories
- Policies must be enabled to function
- Policies must target the desired machines
 - By Default, Inventory policies target all machines with the Inventory Plug-in installed
- To review the Inventory Policies in the console:
 - Navigate to **Manage > Policies** in the main menu
 - Navigate to the **Discovery and Inventory > Inventory** folder
 - Select the Inventory Policy you wish to investigate



Inventory Solution Issues

Validate Inventory Solution Policies

- Confirm the types of inventory you wish to gather
 - Hardware, Operating System, and File Properties can be configured.
 - Confirm **File Properties** for individual files, types of files, and software executables not scanned by software inventory.
- Check for missing data class selections:
 - Under **Advanced > Data classes** tab, the Hardware is set to all by default.
 - If the box is empty or has a green dot instead of a green check mark, expand it and look for the missing data classes and check them
 - Check the top level Hardware box to change it to a check mark, which indicates all hardware data classes will be collected.



Inventory Solution Issues



Validate Inventory Solution Policies

- Check the Run Options
 - Under **Advanced**, check the **Run Options** tab.
 - For a full inventory, **Send inventory changes (deltas) only** must not be checked.
 - The **Run Inventory as** is set to System account by default;
 - Ensure credentials have the needed rights on the client to run the inventory.
- Check Throttling
 - Under **Advanced**, check the **Run Options** tab.
 - If a throttling period is not specified the NS EvtQueue folder can be overwhelmed by NSE files being sent from the clients at the same time.
 - If a throttling period extends after users typically shut down, many inventory tasks will fail as they missed their random start time within the throttling period.

Advanced Options

Data Classes **File Properties Scan Settings** **Run Options**

☐ Send inventory changes (deltas) only

☐ Enable verbose client logging

☐ Access network file systems (UNIX/Linux/Mac)

System resource usage: Low

Wind

☐ Throttle inventory scan evenly over a period of: 1 hours

Run Inventory as:

☒ System account

☐ Logged in user

☐ Specified user

User name: domain\user

Password:

UNIX

☒ Symantec Management Agent credentials

☐ Specified user

User name or ID:

Group name or ID:

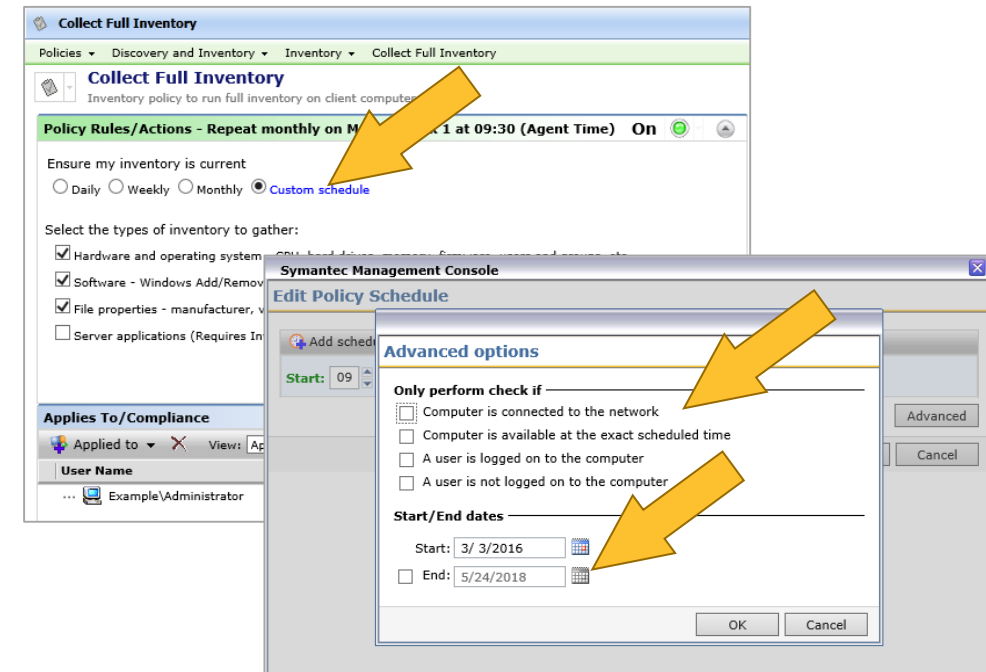
Mac

☒ Symantec Management Agent credentials

Inventory Solution Issues

Validate Inventory Solution Policies

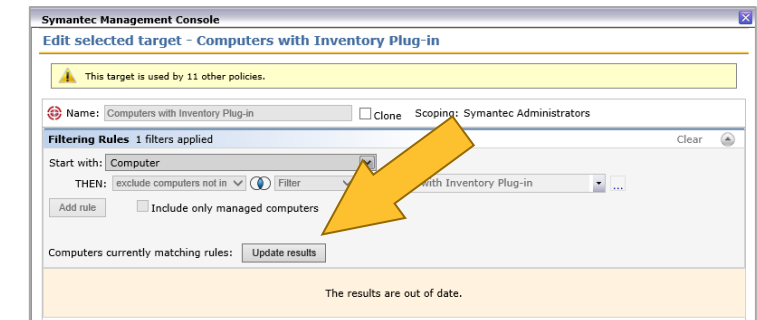
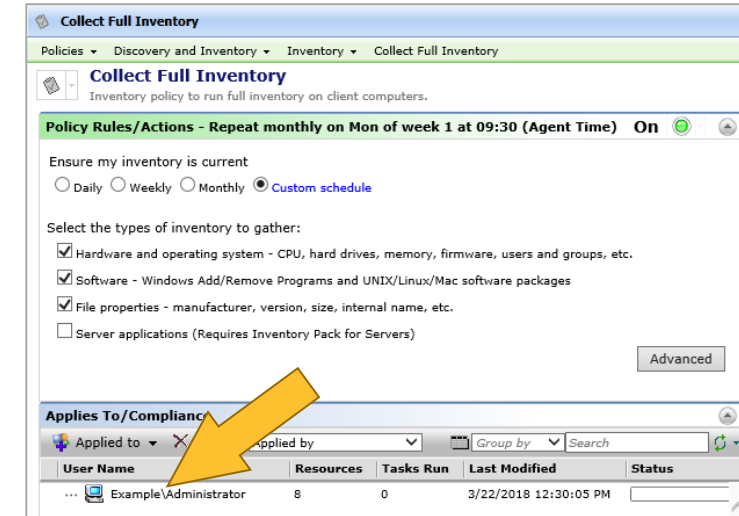
- Check for a Custom Schedule
 - If found, click the **Custom Schedule** link, go to **Advanced**, and review the **Only perform check if** section.
 - These options can limit when and if an inventory is performed by the client
 - Can cause missing hardware information from endpoints
 - Check that the End Date has not passed



Inventory Solution Issues

Validate Inventory Solution Policies

- Check for a Custom Schedule
 - If found, click the **Custom Schedule** link, go to **Advanced**, and review the **Only perform check if** section.
 - These options can limit when and if an inventory is performed by the client
 - Can cause missing hardware information from endpoints
 - Check that the End Date has not passed
- Check Applies To/Compliance
 - Ensure that the affected computers are included
 - Double Click the **Target** line
 - Click **Update Results**
 - You should see the affected endpoint in this list
 - If you do not, check the Target evaluation rule



Inventory Solution Issues



Validate Endpoint Inventory Processes

- Use the SMA to validate Inventory Operations
 - *Open the SMA with Diagnostics Mode Enabled*
 - **Task Status tab:**
 - Click Task History and verify that a full inventory has run and if there are any errors.
 - **Agent Settings tab:**
 - Check if any maintenance windows are in effect that might interfere with the inventories
 - Validate the SMA and Inventory Agent installations and versions
 - **Policies Tab:**
 - Verify that the endpoint received a specific Inventory Policy
 - Select **Diagnostics > Policy Viewer** and click the **Policies Tab**
 - Find the Inventory Policy under **Altiris Client Task Scheduling Agent** and double click on it
 - Validate the XML in the policy

The image displays three overlapping screenshots of the Symantec Management Agent (SMA) Administrator interface, illustrating the steps to validate inventory processes.

Top Screenshot: Task Status

The "Task Status" tab is selected. The "Task History" table shows a list of tasks with columns: Task, Description, Status, End time, Status, and Return code. The table lists several tasks, including "Custom Inventory - Processor", "Detection check for PeopleSoft P...", "Detection check for Oracle Datab...", "Detection check for Microsoft SQ...", "Collect Delta Software Inventory", "Basic Software Application File In...", "Software Inventory Example Policy", and "Collect Delta Hardware Inventory". The status for most tasks is "Succeeded".

Middle Screenshot: Agent Settings

The "Agent Settings" tab is selected. The "Status" is "OK". The "Basic Inventory" section shows "Last sent on 5/24/2018 7:54:57 AM". The "Network Status" section shows "Connected via HTTPS" and "Cryptographic protocol: TLS 1.2". The "CEM Mode" section shows "Cloud-enabled Management mode is enabled but inactive". The "Maintenance Windows" section shows "No maintenance windows configured".

Bottom Screenshot: Policy Viewer

The "Policy Viewer" tab is selected. The "Policy" dropdown is set to "Collect Full Inventory". The "Policy" section shows the XML configuration for the "Collect Full Inventory" policy, including the policy GUID, name, and schedule information.

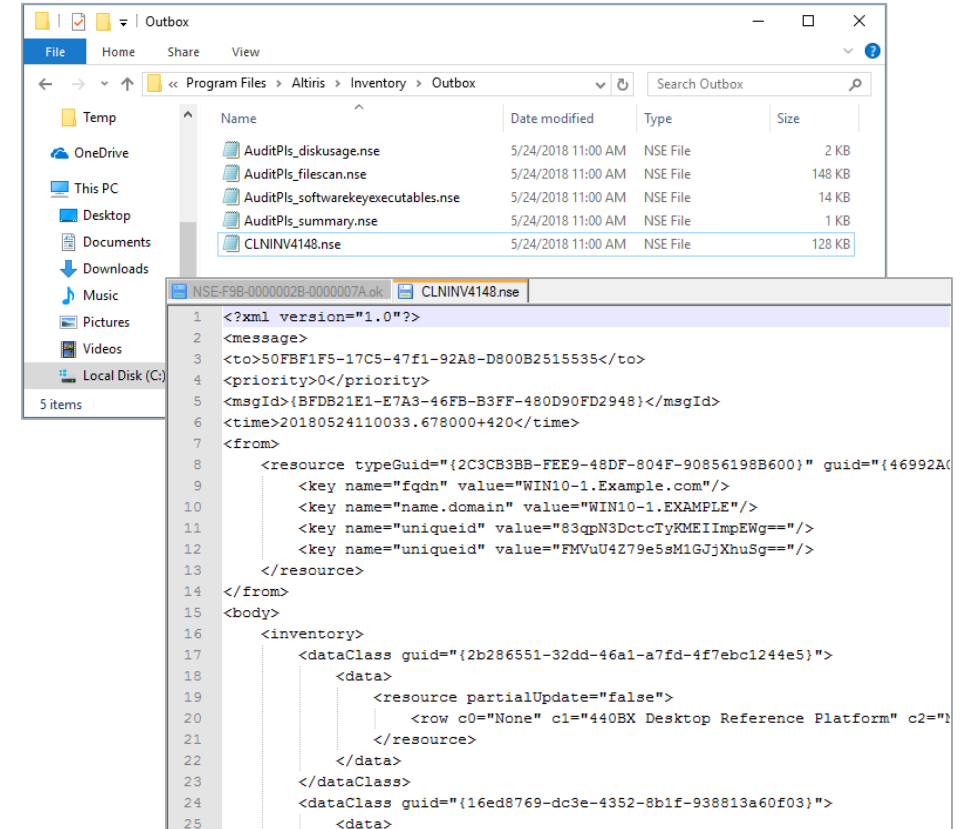
Orange arrows point from the "Task Status" screenshot to the "Agent Settings" screenshot, and from the "Agent Settings" screenshot to the "Policy Viewer" screenshot, indicating the sequence of steps.

Inventory Solution Issues



Validate Endpoint Inventory Processes

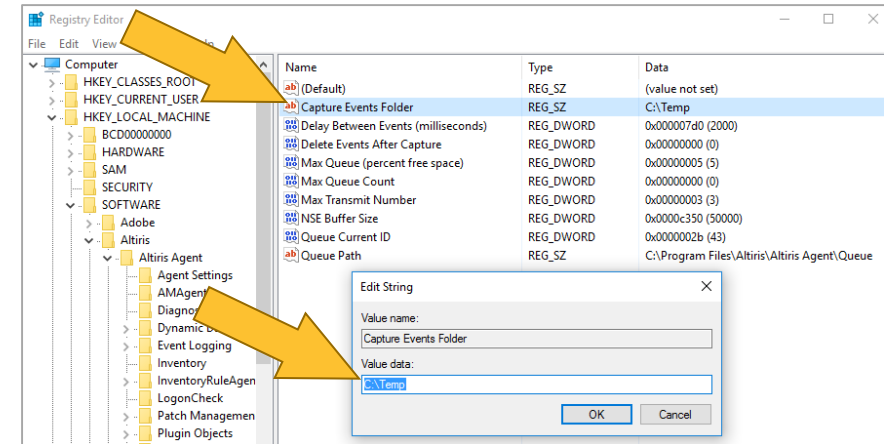
- Capture NSE Files on the Endpoint
 - NSE's may be captured from a machine missing inventory information.
 - If information is found in the NSE but it is incorrect, this is usually a problem relating to the operating system or related components
 - Software inventory is collected by scanning the registry in windows machines, RPM in Linux, and directory scans in Macs
 - E.g., Windows uses WMI, and if Data is returned as incorrect or blank, it may require seeking solutions outside of Symantec channels
- To gather additional client-side details about the inventory collection process, see: [HOWTO75160](#)



Inventory Solution Issues

Validate Endpoint Inventory Processes

- To Capture NSE Files on the Endpoint
 - Open the Registry Editor
 - Navigate *to HKLM\Software\Altiris\Altiris Agent\Transport*
 - Modify "Capture Events Folder" to a directory or path
 - Perform the actions to troubleshoot
 - Such as scheduling an Inventory Policy

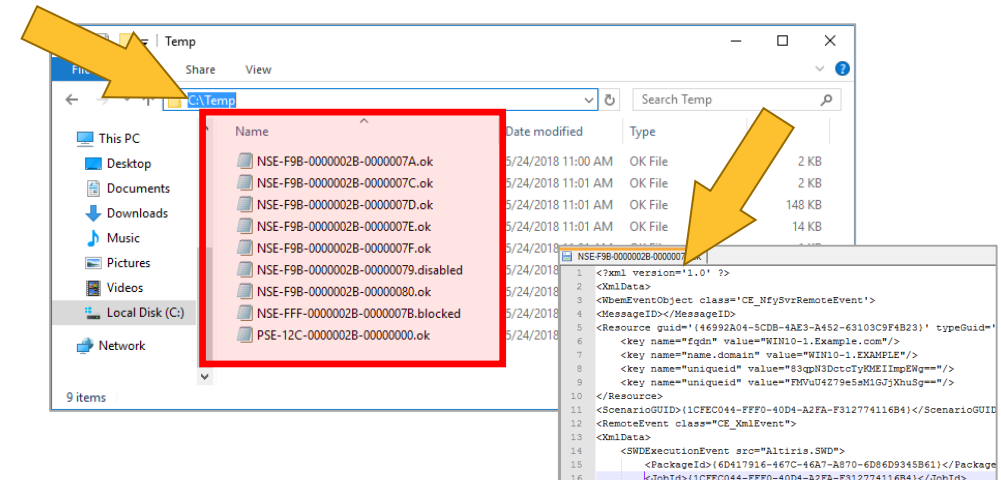
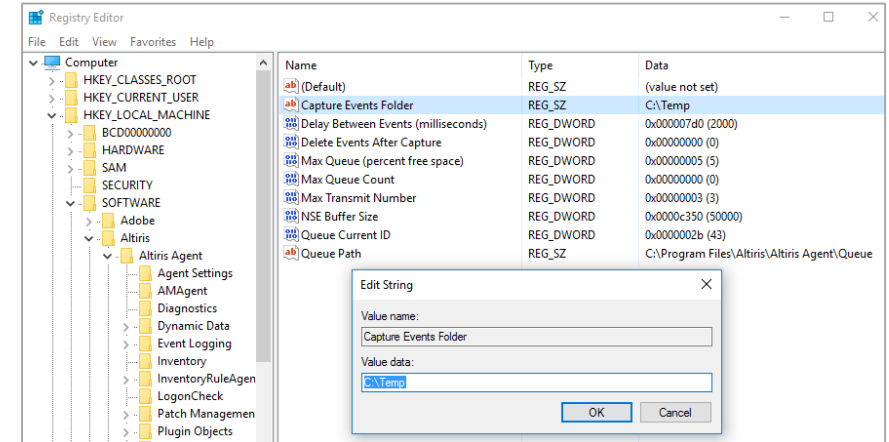


Inventory Solution Issues



Validate Endpoint Inventory Processes

- To Capture NSE Files on the Endpoint
 - Open the Registry Editor
 - Navigate *to HKLM\Software\Altiris\Altiris Agent\Transport*
 - Modify "Capture Events Folder" to a directory or path
 - Perform the actions to troubleshoot
 - Such as scheduling an Inventory Policy
 - Analyze what NSEs are being sent from this client machine.
 - NSE's saved in the Capture Folder use filenames that Indicate the method and result of transport to the NS
 - **NSE** - event was sent to the server directly
 - **PSE** - event was queued to the event queue on the agent
 - **.ok** - event was sent OK
 - **.blocked** - event wasn't sent because the agent is not registered
 - **.disabled** - the NSE's are disabled on the agent side
- **NOTE:** Be sure to remove the value from this registry entry after testing as it will eventually consume significant disk space.

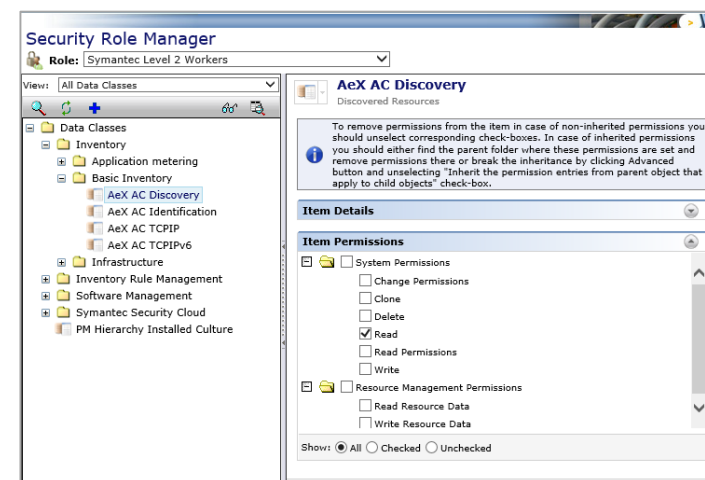
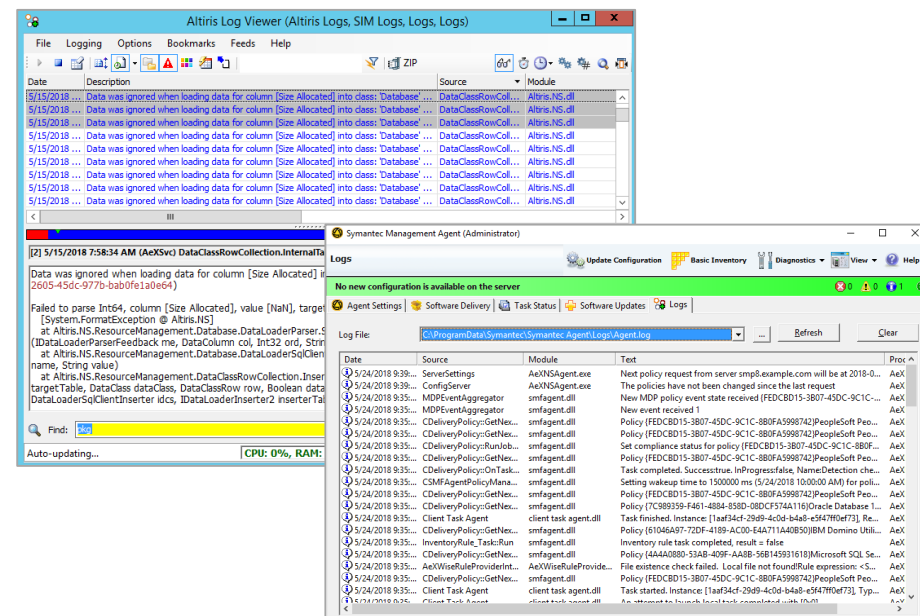


Inventory Solution Issues



Validate Endpoint and Server Inventory Processes

- Evaluate the NS Logs and Agent logs
 - Look for any errors or warnings relating to inventory, research using support resources and resolve as advised.
 - Extended information can be seen by
 - Configuring verbose logging in the inventory policies
 - Enabling verbose/trace logging in the Agent by running ***AeXNSAgent.exe /enablelogging:debug***
 - See [HOWTO75097](#) for information on capturing NSEs and configuring logs for verbose and/or trace messages
- Evaluate Security Roles/Permissions:
 - Look for Inventory items missing data or denied access messages in the console views
 - **Check the Security Role** - ensure it has at least read rights to the associated data classes, views and reports of the affected items



Resolving Issues in Software Management Solution



Software Management Solution Issues



- **Symptoms:**
 - **Software Management Solution has been installed as a part of the ITMS implementation**
 - **Software Management Solution plug-ins have been deployed and policies created**
 - **Software Delivery is not reporting true status or execution information**
 - **Software Delivery is not occurring for some endpoints**
 - **Certain Managed Software Delivery policies are not executing as expected**
- **Testing Approach:**
 - **Ensure the ITMS Implementation is sound**
 - Is the Overall SMP/Site Implementation sound?
 - Is the Software Library configuration sound and Healthy?
 - Are Software Management Solution licenses valid?
 - **Validate Agent and Software Management Plug-in State**
 - Symantec Management Agent
 - Software Management Solution and related Plug-ins
 - **Validate Software Delivery Processes**
 - Is the Software Delivery process working as designed on the endpoint?
 - Are Software Management processes functioning on the Notification Server?

Software Management Solution Issues



Validate Software Delivery Processes

Symptom: Endpoint Never Receives the MSD Policy

• Troubleshooting Steps:

1. Update Configuration and Check the Agent Log

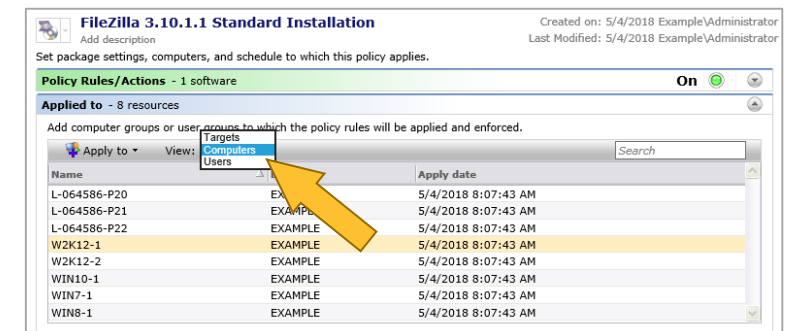
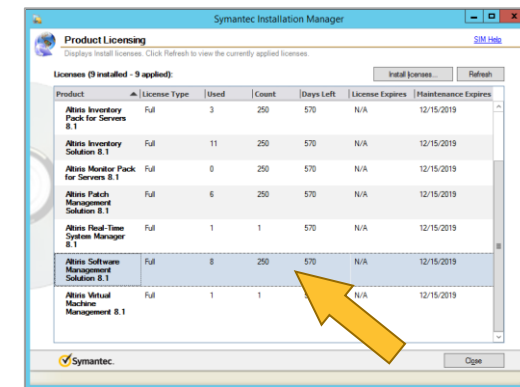
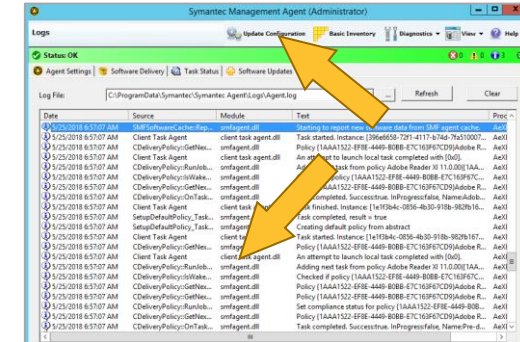
- If there is a policy related error, then investigate the policy settings
- Search support resources and follow solution guidance

2. Check Software Management Solution Licensing

- If you are at the limit this client did not receive a license
 - The MSD Policy is disallowed from executing on it
- Free up or obtain additional licenses

3. Validate Target on MSD Policy

- Change the targeting display to **computers**, you can search for the one that didn't receive the policy.
- Possible it is not applied due to filter criteria in the Target, or in the applied Filter.



Software Management Solution Issues



Validate Software Delivery Processes

Symptom: MSD Policy Never Finishes Running

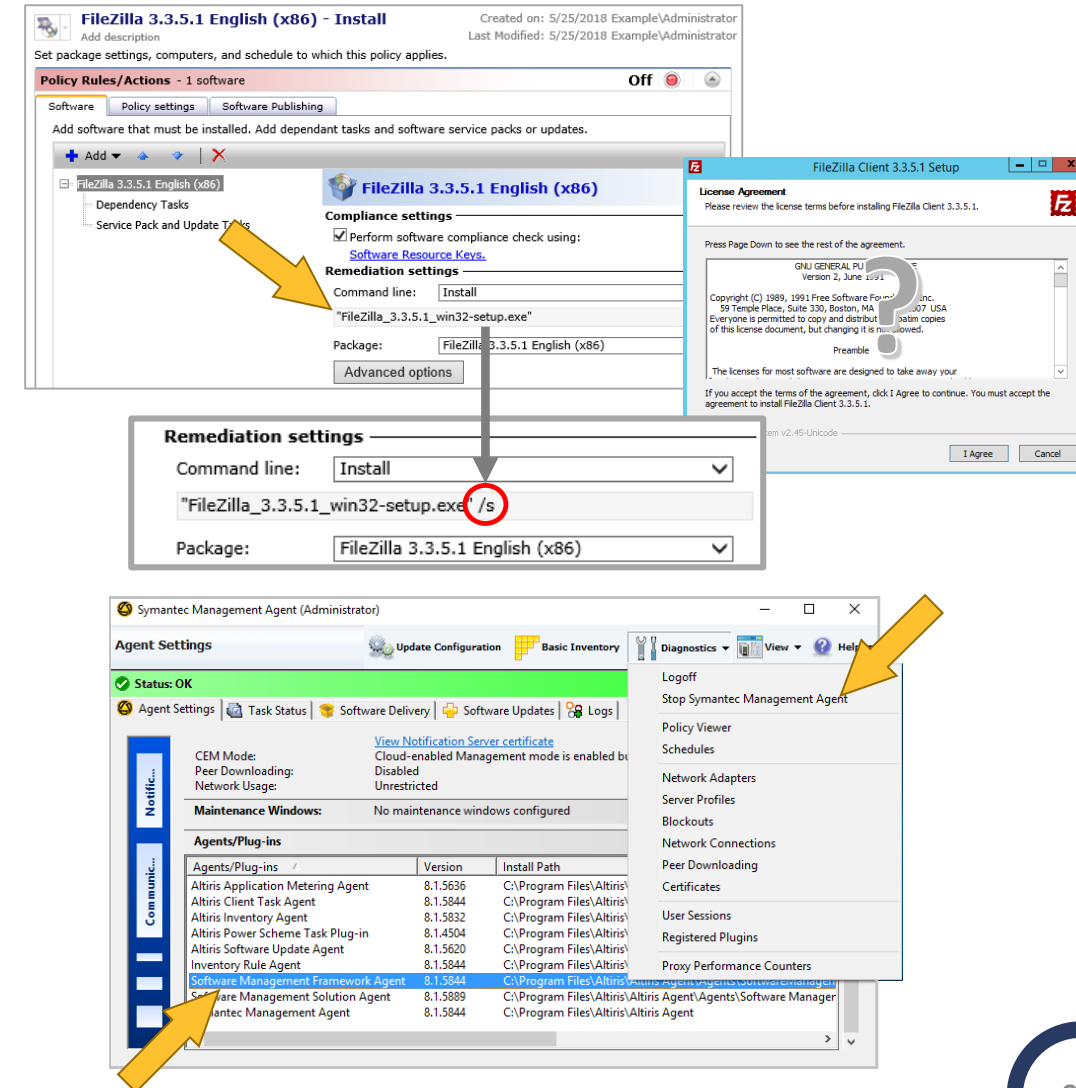
- Troubleshooting Steps:

1. Check the Command Line of the MSD Policy

- This is often caused by a prompt within the execution.
- Run the command-line outside of the process
 - Notice if you see any prompts that require user interaction
 - If so, make sure a silent switch or argument is added to the command-line of the MSD Policy.

2. Restart the Symantec Management Agent

- On rare occasions this is caused by a crash of the Software Management Framework Agent (SMF Agent).
- Try restarting the Symantec Management Agent and running the Policy again.



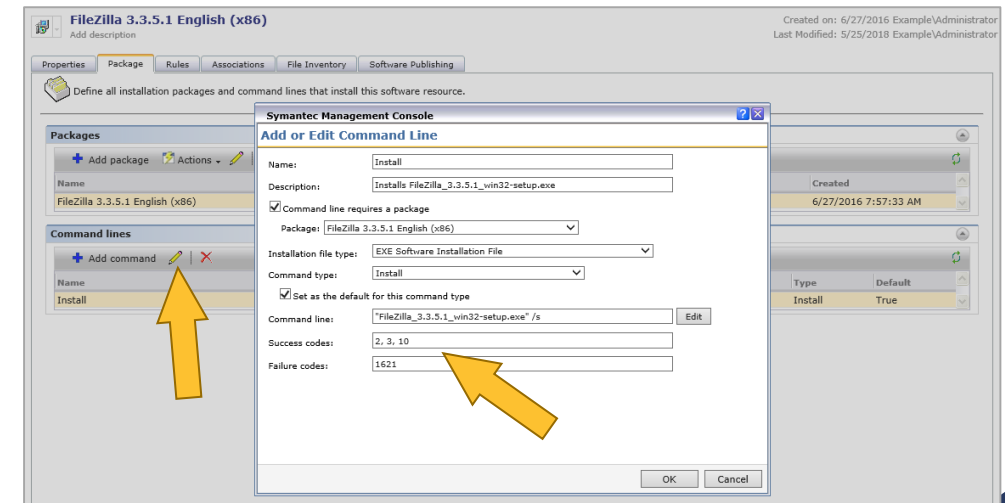
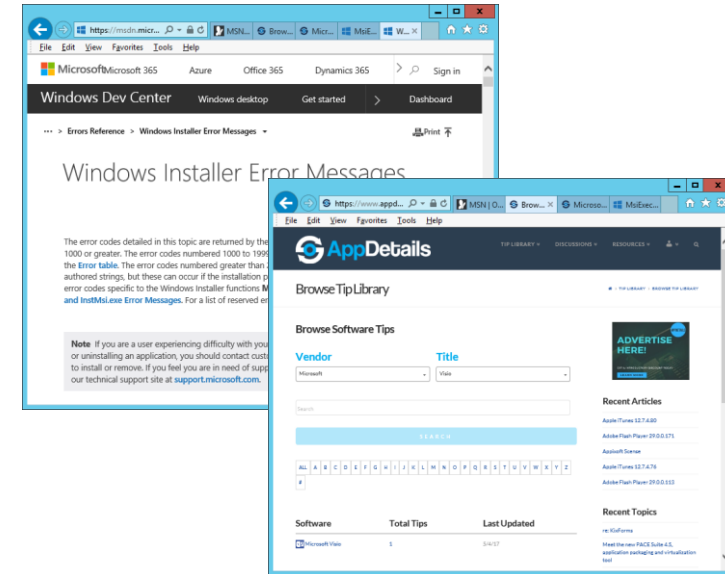
Software Management Solution Issues



Validate Software Delivery Processes

Symptom: MSD Policy Returns an Error

- Troubleshooting Steps:
 1. Run the Command-line outside of the process
 - If the same error occurs, this is an installer problem - Consult your Software or OS vendor
 2. Research the Exit Code.
 - Errors are passed back from the installer
 - Can be seen in the agent logs or in Software Delivery reports.
 - Run an internet search to see what the code means
 - Search Software Vendor/Application Deployment sites
 - Apply the resolution as applicable
 3. Add the Exit Code into the MSD Policy.
 - Some codes simply relay information that is considered a success
 - Add to the “Success Codes” section of the software package
 - Add them to the “Failure Codes” section to report a failure
 - Errors other than Status 0 or 1 will be considered a failure if left blank



Software Management Solution Issues



Validate Software Delivery Processes

Symptom: MSD Policy Scheduled but does not Execute

• Troubleshooting Steps:

1. Check if the schedule has been applied in the past

- Every schedule has a GUID and local clients store schedules by that GUID
- The SMA may think it's already run it, even if the schedule was modified.
- Delete and recreate the schedule in the policy to renew it.
- Test the Policy to confirm the solution

2. Check Advanced options in the MSD Policy

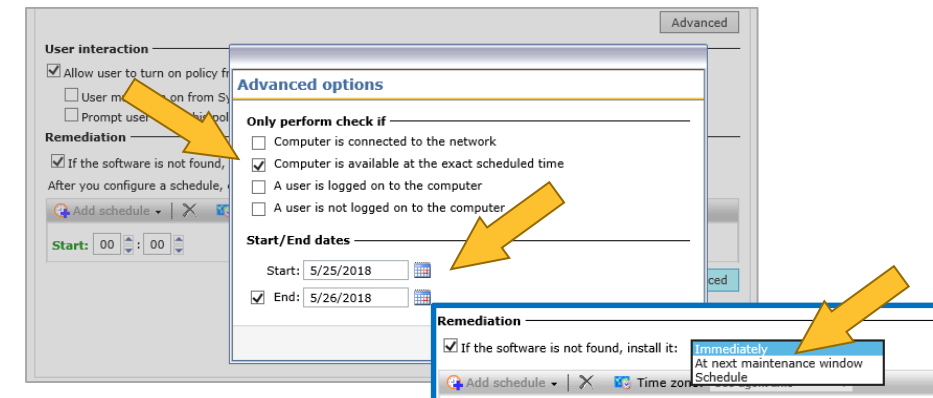
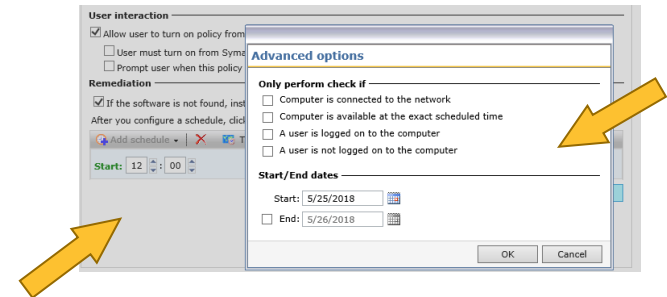
- Is it set for "Only run at the exact schedule time" or it has an End Date?
- If it misses this schedule, without a repeat, then it will never try again.
- Set a schedule that will try again like **Immediately** or **At next Maintenance**

3. Check if Other Policies are Queued up

- In the SMA under Software Delivery, check if there are Policies running, stuck at running, or waiting to run
- Wait for them to complete, and your policy will eventually run.
- If they don't, observe steps demonstrated in "MSD Policy Never Finishes Running"

Policy	Type	Status	Next Run
AcrobatUpd10116.msp for APSB15-24, APSB16-08, JAVAS-73...	Package Rol...	Disabled	Not scheduled
AcrobatUpd10116.msp for Win81-1 Compliant	Package Rol...	Disabled	Not scheduled
Application Metering Plug-in for Windows Install (x86)	Package Rol...	Disabled	Not scheduled
Application Metering Plug-in for Windows Upgrade (x86)	Package Rol...	Disabled	Not scheduled
Application Metering Plug-in for Windows Upgrade (x86)	Package Rol...	Disabled	Not scheduled
Deployment Plug-in for Windows (x86) - Upgrade	Package Rol...	Disabled	Not scheduled
Deployment Plug-in for Windows (x86) - Install	Package Rol...	Disabled	Not scheduled
FileZilla 3.3.5.1 English (x86) - Install	Package Rol...	Not compliant	Not scheduled
IBM Domino Utility Server 9.0.1 (P.VU) TSI	Package Rol...	Unknown or not st...	Not scheduled
Inventory Plug-in for Windows Install (x86)	Package Rol...	Disabled	Not scheduled

Task Name	Last Run	Last Status
Pre-download detection check for FileZilla 3.3.5.1 English (x86)	2018-05-25 09:30:36	Not detected
Downloading package for FileZilla 3.3.5.1 English (x86)	2018-05-25 09:30:36	Success
Execute install command for FileZilla 3.3.5.1 English (x86)	2018-05-25 09:31:20	Success



Software Management Solution Issues



Validate Software Delivery Processes

MSD Policy Never Executes due to Package Download Issues

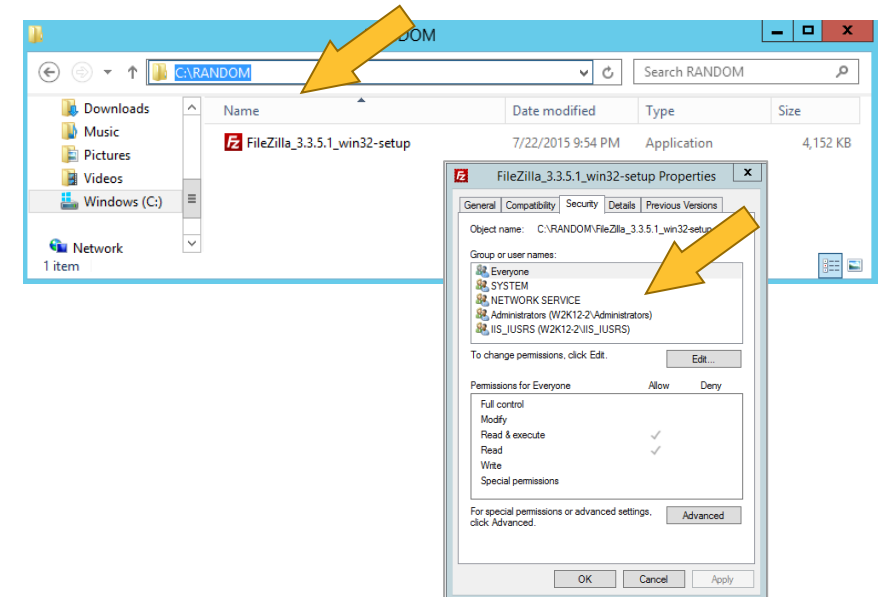
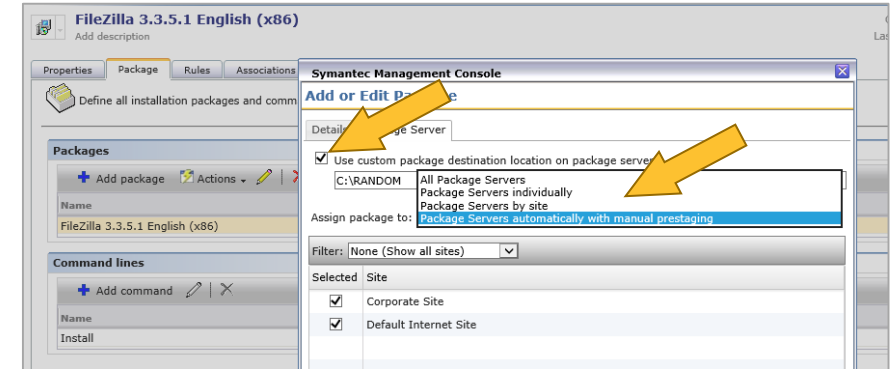
- Troubleshooting Steps:

1. Check the MSD Policy

- Review the Package Server tab in the software package
- Package Servers must be selected to download packages
 - **All Package Servers** is the easiest option since they will all host the package as soon as they know about it. This removes any potential for delay.
 - **All Package Servers with Manual Prestaging** will allow any PS to get the package, but only after a client requests it.
 - Adds potential delays to the download process and may explain why a client is not getting a valid codebase
 - **Package Servers Individually**, will allow any selected PS to host the files. If a PS is not selected for your site it may be the problem.

2. Check the Custom Package Destination setting:

- If defined check that the files physically exist on the Site Server in that directory and have proper rights.



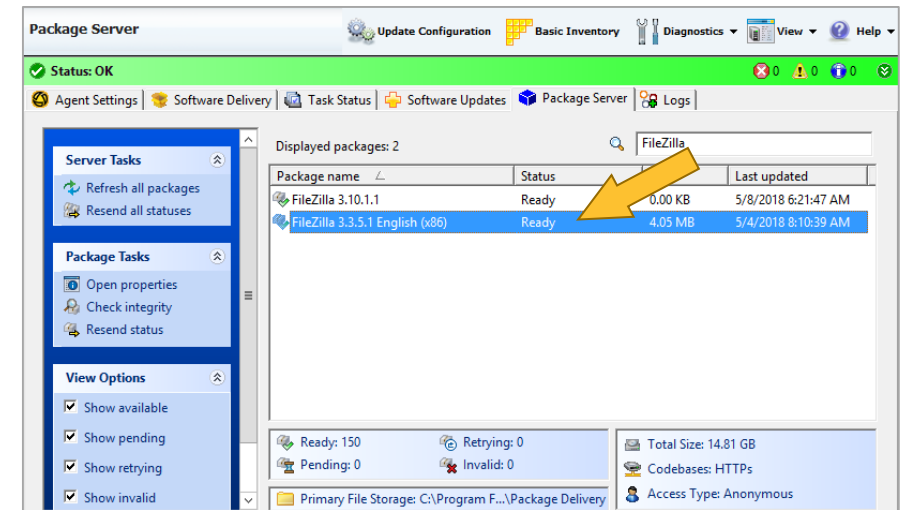
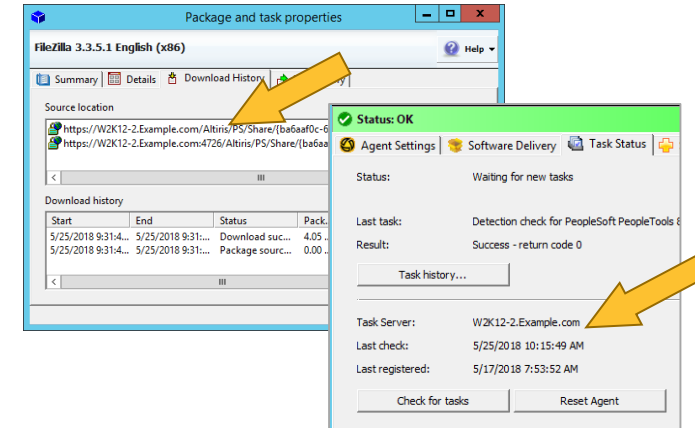
Software Management Solution Issues



Validate Software Delivery Processes

MSD Policy Never Executes due to Package Download Issues

- Troubleshooting Steps:
 3. Check the Package status on the Site Server
 - Open the Agent UI > **Task Status** tab or Software Delivery tab to find the name of the Site Server
 - Go to that Site Server and open the Agent UI.
 - Click on the **Package Server** tab to review the Status.
 - Check that the package is in a ready state



Software Management Solution Issues



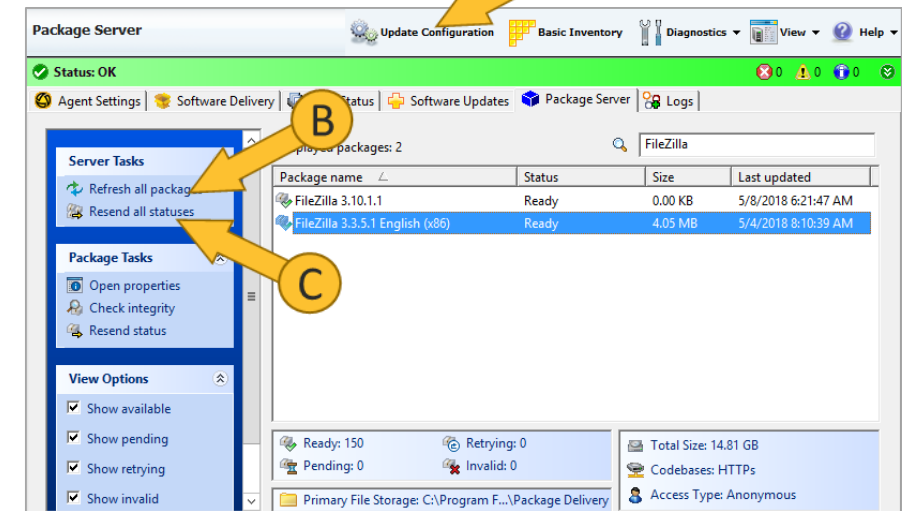
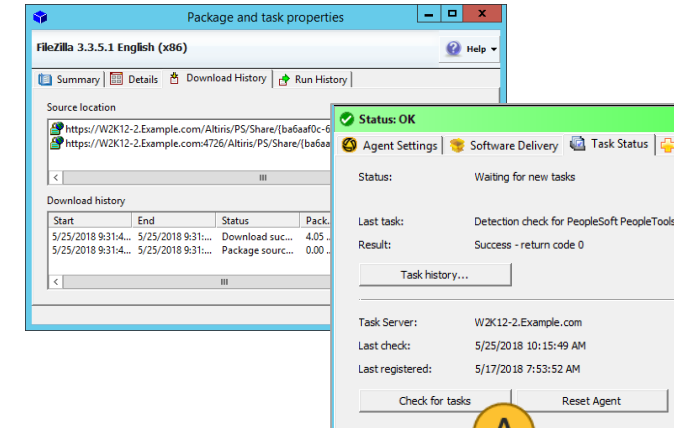
Validate Software Delivery Processes

MSD Policy Never Executes due to Package Download Issues

- Troubleshooting Steps:

- 3. Check the Package status on the Site Server

- Open the Agent UI > **Task Status** tab or Software Delivery tab to find the name of the Site Server
 - Go to that Site Server and open the Agent UI.
 - Click on the **Package Server** tab to review the Status.
 - Check that the package is in a ready state
 - **If it isn't in a ready state:**
 - A. Under Settings click *Update Configuration*.
 - B. Under the Package Server tab, click *Refresh all packages*
 - C. Under the Package Server tab, click *Resend all statuses*
 - Test the Policy to confirm the solution



Software Management Solution Issues



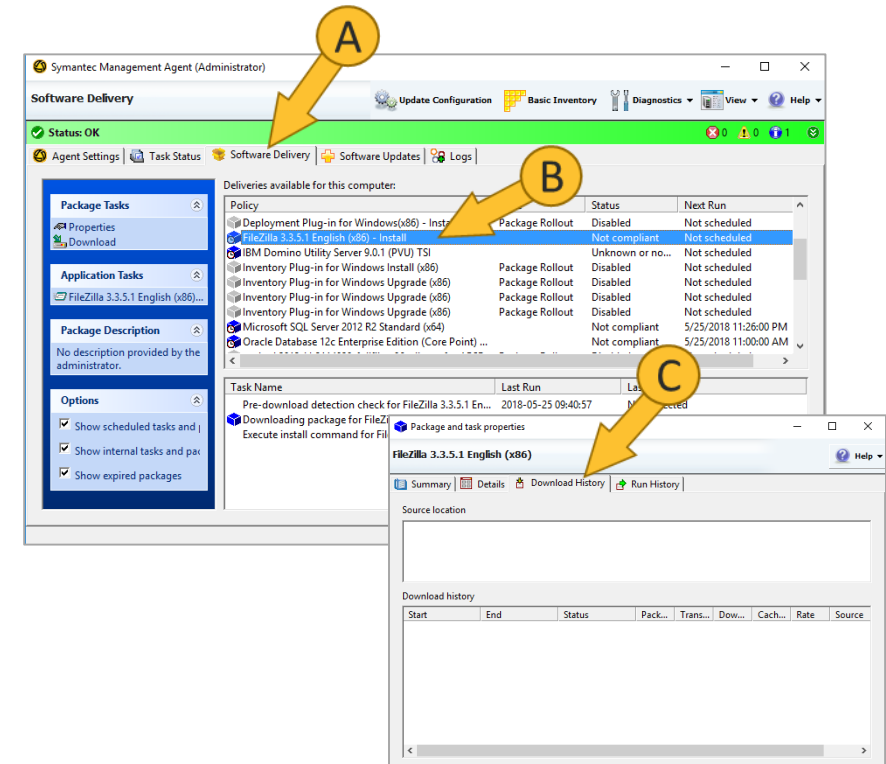
Validate Software Delivery Processes

MSD Policy Never Executes due to Package Download Issues

- Troubleshooting Steps:

4. Check the Agent for Codebases

- Determine if the client is getting the Code bases (links to download) from the Notification Server.
- On the affected client, bring up the agent user interface
 - A. Click on the **Software Delivery** tab.
 - B. Find the Policy that contains the package you need downloaded
 - Double-click on the package name in the page
 - C. Click on the **Download History** tab.
 - If no Source location is shown, you are dealing with an issue with the Site Server or Site Management settings.
 - It could stem from the client belonging to a site that does not have a Package Server assigned.
- These symptoms and solutions can be found in the “**Package Service Operation & Distribution Issues**” topics in the **Site Infrastructure Troubleshooting** lessons



Resolving Issues in Asset Management Solution



Asset Management Solution Issues



- **Symptoms:**
 - Asset Management Solution has been installed as a part of the ITMS implementation
 - Asset Management Solution has been configured using default settings and policies
 - Asset Administrators have been noticing the following behaviors:
 - Random assets suddenly disappear from the Symantec Management Console
 - Unable to find Assets when searching by certain attributes
 - Asset Status value unexpectedly changes
 - Asset's details are incorrect or missing
 - Duplicate assets are appearing in Reports
- **Testing Approach:**
 - **Ensure the Solution Implementation is sound**
 - Is the Overall ITMS Implementation sound?
 - Are Asset Management/CMDB Solution licenses valid?
 - Are the Asset Management Core settings configured properly?
 - **Validate Asset Management Processes**
 - Investigate Missing Assets from the CMDB
 - Investigate Asset picker reporting issues
 - Diagnose Asset Status change process
 - Investigate missing or incorrect Asset's details in the CMDB
 - Diagnose duplicate assets within the CMDB

Solving Asset Management Solution Issues



Validate Asset Management Operation

Symptoms: Random Assets Missing from Asset Reports/Views

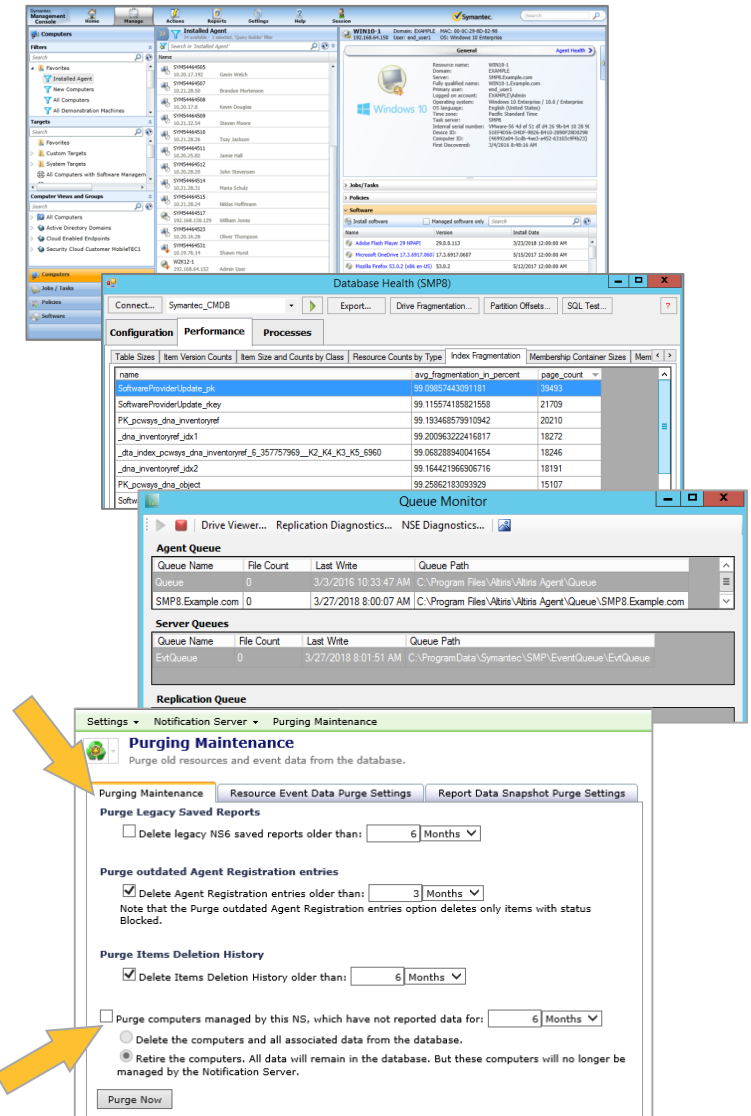
• Troubleshooting Steps:

1. Check For Data Loss Due to the Environment

- May occur if the NS / SQL Server are performing poorly
- Extreme situation to have an entire record or records vanish
- It may be advisable to check the following areas:
 - Check Notification Server Performance
 - Check Event Queue processing performance
 - Check MS SQL Performance and Operation
 - Create a maintenance plan on the SQL Server

2. Check Purging Maintenance

- If Purging Maintenance is set to delete computers, this will delete computers based on inactive endpoints
- Disable this option if it is enabled and test



Solving Asset Management Solution Issues



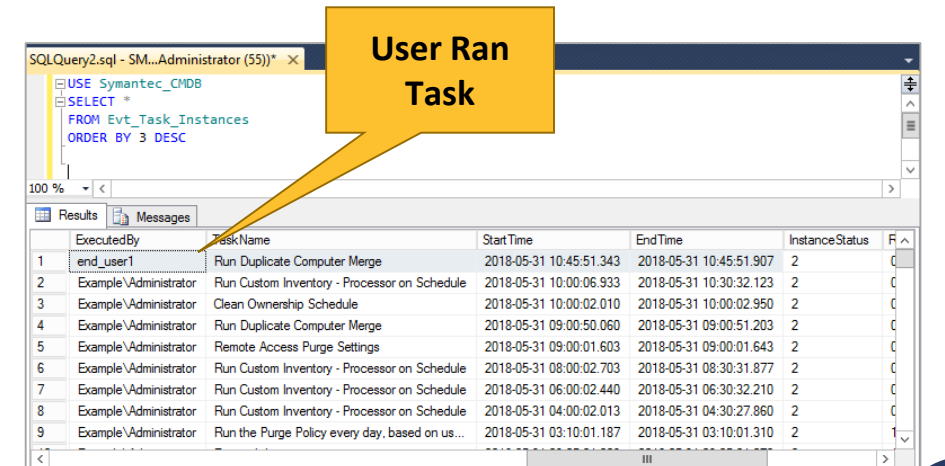
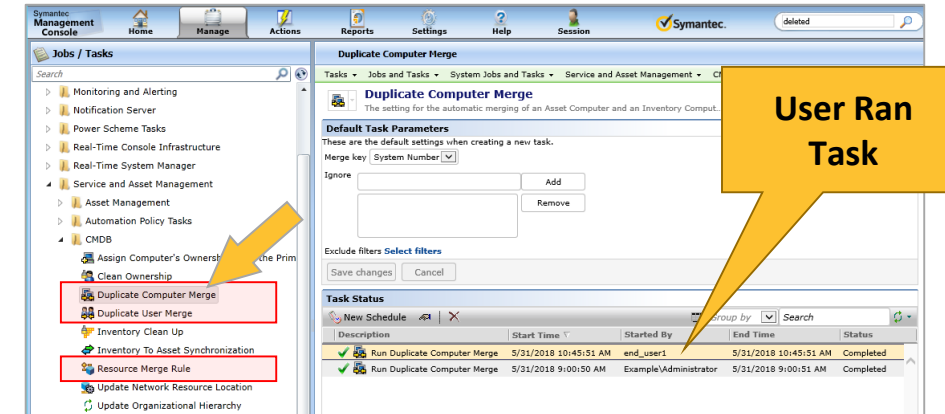
Validate Asset Management Operation

Symptoms: Random Assets Missing from Asset Reports/Views

- Troubleshooting Steps:

3. Check Resource Merge Rules

- If merge rules or manual merges have been performed, the result will be one final record with another now deleted.
- Cmdb merge rules can be checked and changed in Jobs/Tasks
 - Duplicate Computer Merge
 - Duplicate User Merge
 - Resource Merge Rule.
- Out of box, there are **no** merge rules enabled to run.
- Check who Ran the Task in the Job/Task
 - If users manually ran the task, then additional user training or removal of user's permissions would be required
 - If this was a scheduled task, remove or reschedule the task as necessary and test
 - **Evt_Task_Instances** view shows tasks that ran manually or scheduled.



Solving Asset Management Solution Issues



Validate Asset Management Operation

Symptoms: Random Assets Missing from Asset Reports/Views

- Troubleshooting Steps:

4. Check if a User Has Deleted Assets.

- ITMS Users that have permissions to delete assets may do so without further authorization.
- The Administrator should ensure that only those authorized to delete assets are set to do so.
- The *Evt_NS_Item_Management* table can be checked for assets that Altiris users deleted.
 - If a user has deleted an asset, additional training or removal of delete permissions would need to be completed.
 - If the user account is the Application Identity:
 - Someone is logging in as that and performing the action, or a task or policy is doing so on behalf of the App ID.

The image contains two screenshots from the Symantec Management Console. The top screenshot shows the 'Accounts' management page. A yellow arrow points to the 'end_user1' account in the list, which is marked as 'Enable'. A yellow callout bubble next to it says 'User has rights to Delete Assets'. The bottom screenshot shows a SQL query window with the following query:

```
USE Symantec_CMDB
SELECT *
FROM Evt_NS_Item_Management
WHERE Action = 'Delete'
ORDER BY 3 Desc
```

A yellow arrow points from the 'end_user1' account in the top screenshot to the 'end_user1' user in the bottom screenshot's results table. A yellow callout bubble next to the 'end_user1' user in the results table says 'User Deleted this Asset'.

ItemGUID	_eventTime	ItemName	User	Action
44744669-ADAA-4031-926A-F804FE74CAB8	2018-05-31 10:30:26.687	SYM04464523	end_user1	Delete
98F8B437-B84D-4198-96B4-555F67AA72DC	2018-05-31 10:30:26.687	All Computers	end_user1	Delete
7B8BAFEC-423F-4C46-AB09-ADB543D6F7A7	2018-05-31 10:29:46.683	All Computers	end_user1	Delete
5746FCA1-EF3E-4E3F-861E-DE5598494683	2018-05-31 10:29:36.700	Security Cloud Customer MobileTEC1	end_user1	Delete
4EC71A57-2DEE-45C6-86F3-D2BE92073195	2018-05-31 10:29:26.683	All Computers	end_user1	Delete
8503438B-78E7-4DDF-AD74-5CFB8F0FCAF53	2018-05-31 10:29:26.683	Cloud Enabled Endpoints	end_user1	Delete
FAEF85B6-38FB-4A8C-AFFD-7411E1307A4E	2018-05-31 10:15:09.183	Urgent replication for 'Custom Invent...	Example\Administrator	Delete
C75864C9-ADAD-4BD9-903B-4DC2091FBE68	2018-05-31 09:30:56.567	All Computers	end_user1	Delete
1D76AAAA-FB00-4C20-8E20-F8B2D231A2A	2018-05-31 09:02:02.742		Example\Administrator	Delete

Solving Asset Management Solution Issues



Validate Asset Management Operation

Symptom: An Asset's Status Value Unexpectedly Changes to Active

- Troubleshooting Steps:

1. Check if the Computer exists and is Online:

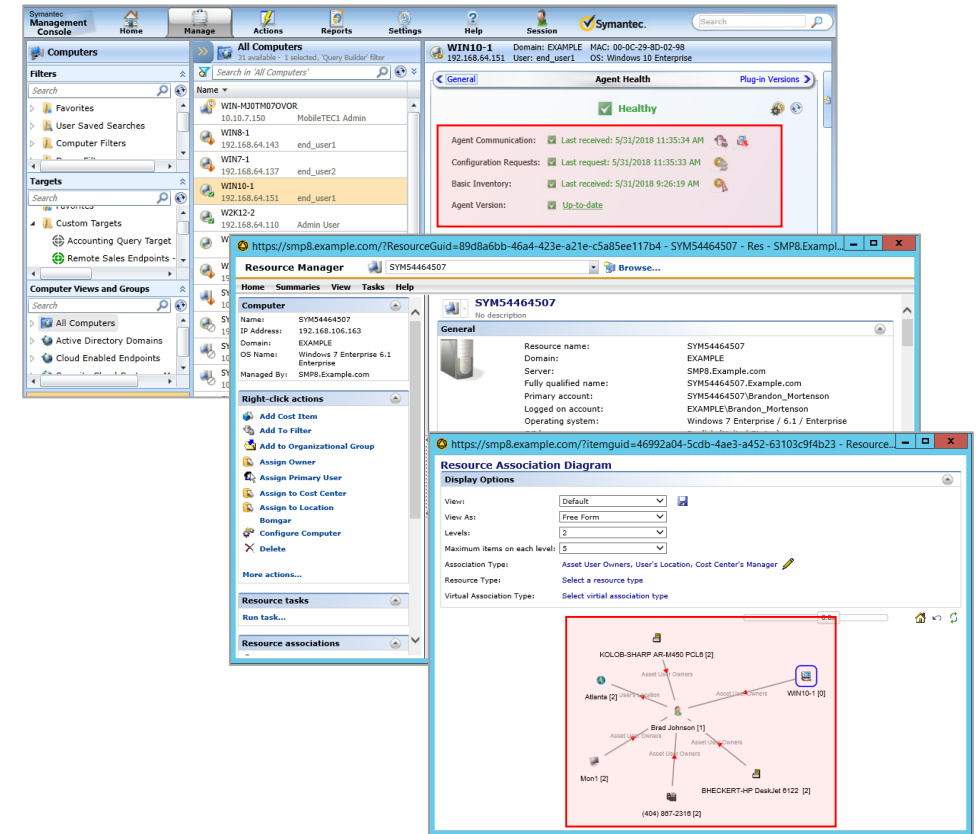
- Most likely being managed by a SMA and it checked in, which automatically changes the computer's Status to Active.
- A SMA will always change the computer's Status to Active, even if the user doesn't wish this to change.

2. Check the Console to Confirm

- **Agent Health:** Current Agent, Inventory and Configuration events?
- **Resource Manager:** Make, Model, User, IP Address
- **Asset:** Location, Cost Center, Department

3. Prevent the Status Change

- Through the Uninstall of the Symantec Management Agent.
- If Retired, should be part of a retirement process.
- How to retire a computer: [HOWTO95111](#)



Solving Asset Management Solution Issues



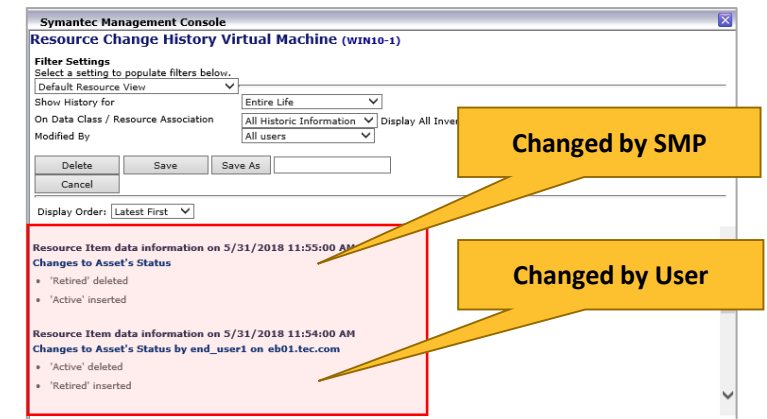
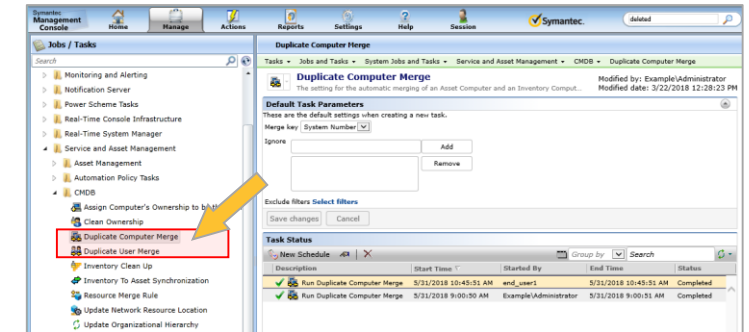
Validate Asset Management Operation

Symptom: An Asset's Status Value Unexpectedly Changes to Active

- Troubleshooting Steps:

4. Check if Computers were Merged Improperly

- Computer may be merged with other computers that had been active.
 - If a computer merge occurred and the Status of the other computer was kept and it was Active, then the affected computer retains this and it becomes active.
- Check **Duplicate Computer Merge** and **Resource Merge Rule**
 - If either are enabled, these could have been the cause.
- Check an affected computer's **Resource Change History**
 - In the history list, look for entries that refer to the Asset's Status.
 - Includes user account along with the date and time the change occurred on.
- Check the **Evt_NS_Item_Management** table for Status changes.
 - May not be very clear on what happened, but it will show changes that occurred that can be tracked down.



Solving Asset Management Solution Issues



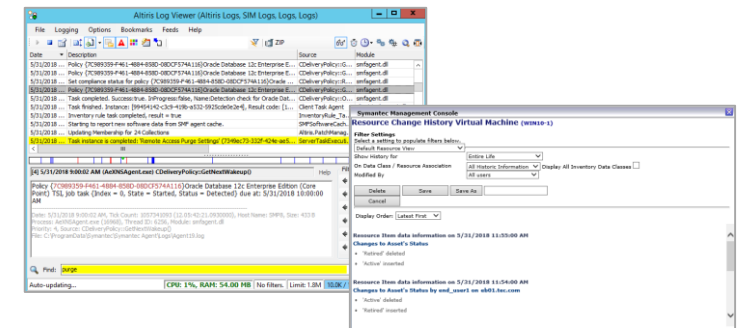
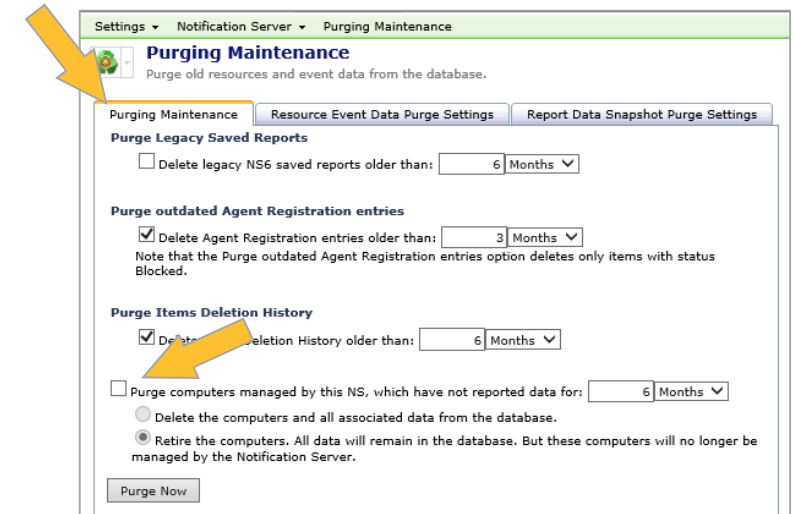
Validate Asset Management Operation

Symptoms: An Asset's Status Value Unexpectedly Changes to Retired

• Troubleshooting Steps:

1. Check Purging Maintenance

- Purging Maintenance is the only out of box process that can set a computer's Status to Retired if enabled
 - This task is normally the cause of unexpected Status changes
 - Can retire or even delete computers when they don't check in
 - if Computers check in, but no data is received, this can still result in the computer's being processed and retired.
- If this is configured to retire computers, disable that function temporarily to verify if this was the cause.
- The Server logs can also be checked to see when this was ran
 - Compare the date and time with the computer's Status change



Solving Asset Management Solution Issues



Validate Asset Management Operation

Symptoms: An Asset's Status Value Unexpectedly Changes to Retired

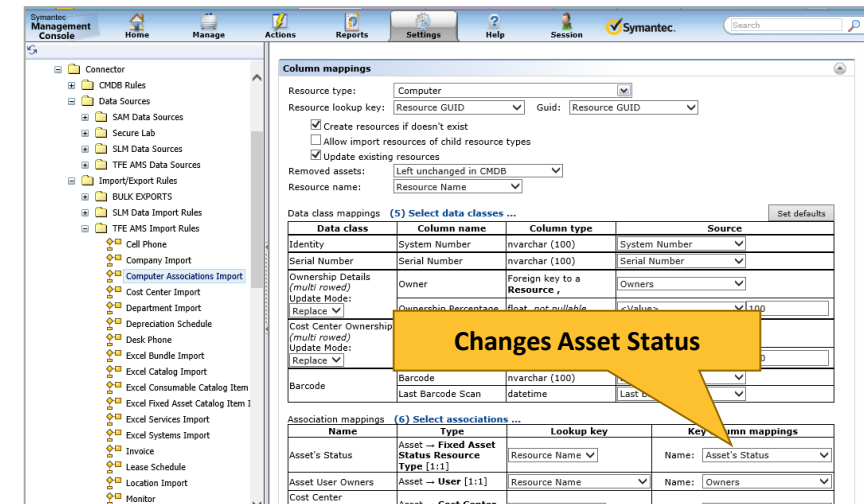
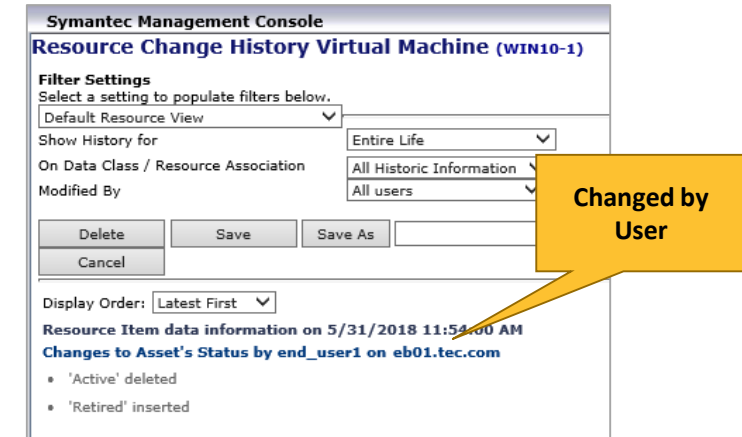
• Troubleshooting Steps:

2. Check if a user manually changed the Status to Retired.

- The Symantec Administrator should check with their Asset users to verify who may be changing computer Status values.
- It may be that one or more users are doing this as part of their normal job but this was unexpected to the Symantec Administrator.

3. Check the Data Connector import rules or CMDb rules

- Harder to track down as they could include a lot of areas to check
- Verify if any are changing the Status by reviewing all rules



Solving Asset Management Solution Issues



Validate Asset Management Operation

Symptoms: Asset Details are Missing or Incorrect

- Troubleshooting Steps:

1. Check for a Physical Change in Hardware

- Hardware, such as a motherboard, might have been replaced
 - Inventory Solution has updated its hardware data classes
 - Older CMDB data classes still show the older hardware values.
- Check the **Inventory to Asset Synchronization** Task
 - This task is normally be used to copy Inventory's Manufacturer, Model, Serial Number and System Number to CMDB Solution's counterpart data classes.
- If CMDB's counterpart data classes have any non-empty values
 - The task will not overwrite the old values
 - The user must find a way to clear out the CMDB Solution's counterpart data classes so that the Inventory to Asset Synchronization can be used properly

Manufacturer

Manufacturer: Dell

Model: OptiPlex 745

Hardware

Computer manufacturer: HP

Model: HP Z230

Processor count: 2

Processor: Intel(R) Xeon(R) CPU 511

RAM: 6144 MB

Symantec Management Console

Home Manage Actions Reports Settings Help Session

Jobs / Tasks

Inventory To Asset Synchronization

Tasks: Jobs and Tasks, System Jobs and..., Service and Asset..., CMDB, Inventory To Asset...

Inventory To Asset Synchronization

The settings to control the synchronization of inventory and asset...

Default Task Parameters

These are the default settings when creating a new task.

Include filters: Windows Computers

Exclude filters: Select filters

Save changes Cancel

Task Status

New Schedule

Description	Start Time	Started By	End Time
Run Inventory To Asset Synchronization on 5/6/1/2018 2:10:00 AM			N/A
Run Inventory To Asset Synchronization	5/31/2018 12:53:57 PM	Example\Administrator	5/31/2018
Run Inventory To Asset Synchronization	5/31/2018 12:51:51 PM	Example\Administrator	5/31/2018

Symantec Management Console

Resource Change History Computer (SYM54464501)

Filter Settings

Select a setting to populate filters below.

Default Resource View

Show History for: Entire Life

On Data Class / Resource Association: All Historic Information

Modified By: All users

Display All Inventory Data Classes: ☒

Delete Save Save As Cancel

Display Order: Latest First

Changes to Serial Number by Example\Administrator on SMP8.Example.com

Changes to Serial Number

Row modified

- "Serial Number" set to Q807011899

Changes to Manufacturer

Row modified

- "Model" set to OptiPlex 960

Changes to Manufacturer

Row modified

- "Manufacturer" set to Dell Inc.

Solving Asset Management Solution Issues

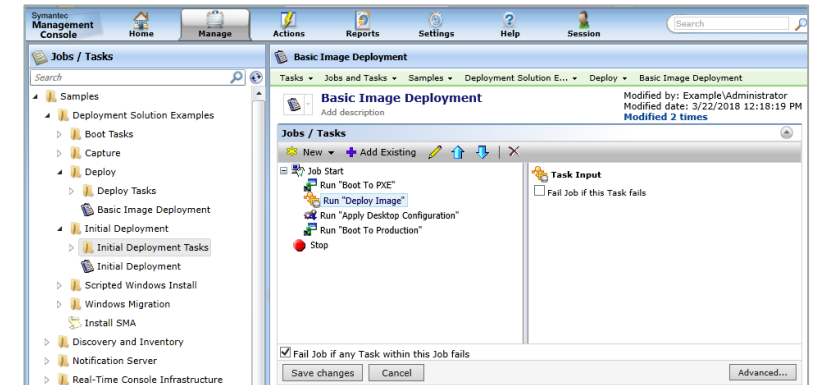
Validate Asset Management Operation

Symptoms: Asset Details are Missing or Incorrect

- Troubleshooting Steps:

2. Check Deployment Processes

- Computer was Reimaged and its name reused **OR** images with the SMA that have an existing GUID are being deployed
 - Results in Inventory Solution data being matched up against the older computer record, even if it was deleted in the Console.
 - This can result in duplicate IP addresses or MAC addresses, among other duplicate issues.
 - Can also occur by deploying an image from a process set to use a specific MAC address



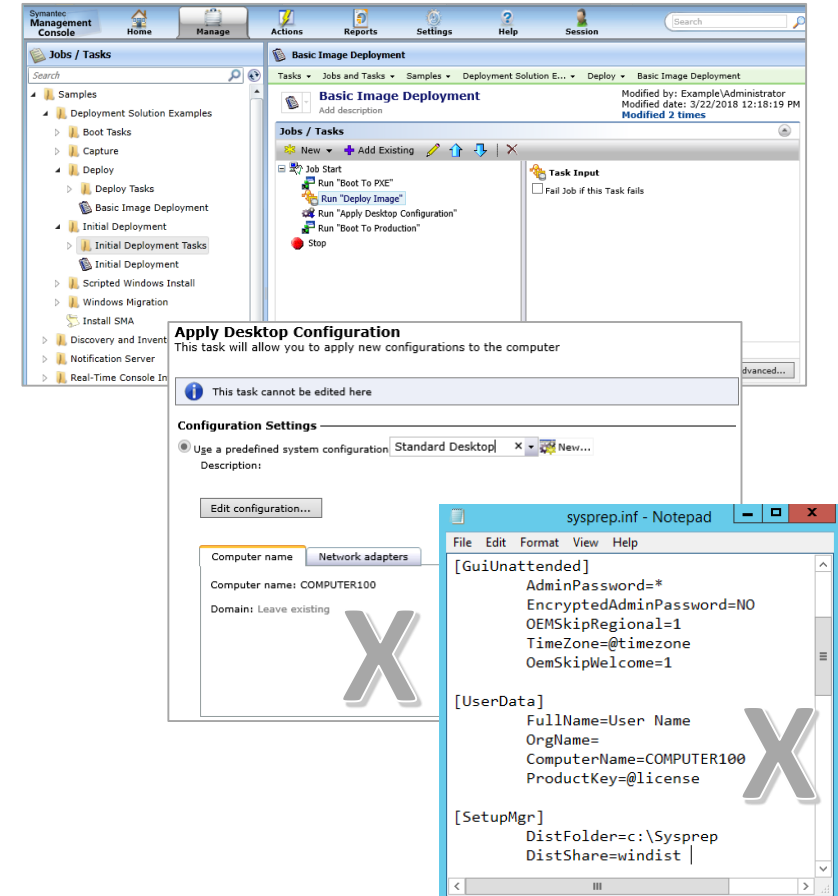
Solving Asset Management Solution Issues



Validate Asset Management Operation

Symptoms: Asset Details are Missing or Incorrect

- Troubleshooting Steps:
 2. Check Deployment Processes
 - Computer was Reimaged and its name reused **OR** images with the SMA that have an existing GUID are being deployed
 - Results in Inventory Solution data being matched up against the older computer record, even if it was deleted in the Console.
 - This can result in duplicate IP addresses or MAC addresses, among other duplicate issues.
 - Can also occur by deploying an image from a process set to use a specific MAC address
 - Symantec **does not** support reusing computers or their names
 - This can result in duplicate or shared GUIDs and/or corrupted inventory and asset data.
 - The **correct** way to edit the name of an Active, managed computer is to do so directly on the computer, then the SMA will update the record's name



Solving Asset Management Solution Issues



Validate Asset Management Operation

Symptoms: Asset Details are Missing or Incorrect

- Troubleshooting Steps:

3. Check Data Connector Processes

- CMDB data may have been imported via Data Connector or manually entered into computers.
- When the Inventory to Asset Synchronization runs, it fails to copy over Inventory Solution's counterpart data.
- **Validate Data Connector Import Methods**
 - If the CMDB's data classes already contain values, the sync will not overwrite these.
 - If these values are incorrect, the user can change the method of import to reflect the correct values then reimport the computers.
 - This will update them (not create duplicates) with their correct Manufacturer, Model, Serial Number or System Number, depending on which ones the customer imported previously.

Manufacturer
Manufacturer: Dell
Model: OptiPlex 745

Hardware
Computer manufacturer: HP
Model: HP Z230
Processor count: 2
Processor: Intel(R) Xeon(R) CPU 511
RAM: 6144 MB

Computer Associations Import
Add description

This rule has never been run.

Resource import/export rule configuration

Data source: Excel Computer Associations
Replication direction: Import
Data filter:
Refresh Data Source
Show data ...

Column mappings

Resource type: Computer
Resource lookup key: Resource GUID
Guid: Resource GUID
☒ Create resources if doesn't exist
☐ Allow import resources of child resource types
☒ Update existing resources
Removed assets: Left unchanged in CMDB
Resource name: Resource Name

Data class mappings (3) Select data classes ...

Data class	Column name	Column type	Source
Identity	System Number	nvarchar (100)	System Number
Serial Number	Serial Number	nvarchar (100)	Serial Number
Chassis (multi rowed)	Audible Alarm	bit	
	Chassis Package Type	int	
	Lock Present	bit	
	Part Number	nvarchar (256)	
	Security Breach	int	
	Serial Number	nvarchar (256)	Serial Number
	Security Status	int	<Value>
	Device ID	Key, nvarchar (256), not nullable	
Tag	nvarchar (256)	System Number	

Update Mode: Replace

Solving Asset Management Solution Issues



Validate Asset Management Operation

Symptoms: Duplicate Assets Appear in Reports/Views

- *What are they and what causes them?:*
 - **Duplicate Assets** refers to when two or more asset records share at least one data class value between them
 - Asset records may or may not refer to the same physical asset - this refers to one of the following:
 - A CMDB Solution record has a duplicate value to another CMDB Solution record, such as a duplicate serial number.
 - A CMDB Solution record has a duplicate value to an Inventory Solution record, such as a duplicate system number.
 - Duplicate assets can be any asset type but are most often associated with duplicate computer records.
 - Depending on how the computers and their data classes were brought into the CMDB often determines how the duplicates were caused.

Solving Asset Management Solution Issues



Validate Asset Management Operation

Symptoms: Duplicate Assets Appear in Reports/Views

- **Scenario 1: Duplicate Computer Names**
 - Not considered to be an issue because the resource name data class *by itself* is not required to be unique.
 - Can be created in a variety of ways:
 - Computers were received by a Purchase Order, twenty may all be named "Dell Inspiron 15".
 - Computers were imported by a Data Connector, fifteen may be named "New Computer".
- **Solve these by:**
 - Entering the proper Computer Names or other attributes as they are being received into the procurement process
 - Ensure Data Connector rules import data that has unique Computer names Or at least one unique attribute per row - even if the Resource Name is the same for all rows

Solving Asset Management Solution Issues

Validate Asset Management Operation

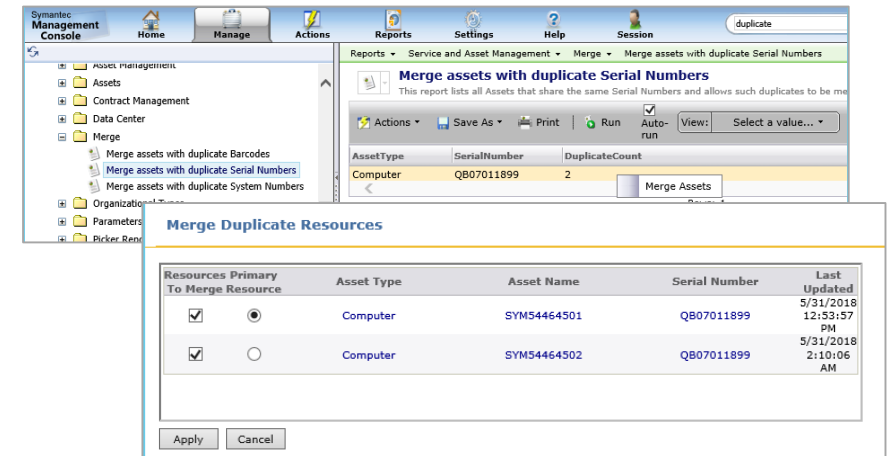
Symptoms: Duplicate Assets Appear in Reports/Views

- **Scenario 2: Duplicate Computers + Inventory to Asset Sync task**

- A common business practice is to create unmanaged "staging" computers
- Later, physical computers with a SMA and create managed computer records.
 - Results in an unmanaged and managed computer referring to the same computer
- Lastly, the Inventory to Asset Synchronization task is ran.
 - Since Unmanaged S/N are the same, Managed S/N are now the same.
- *End Result:* Duplicates with same attributes and serial numbers

- **Solve these by:**

- **Creating staging records with serial number and/or the system number included.**
 - Once the computer checks in, a merge task can easily then combine the records
 - Without these merge keys, it can be difficult if not impossible to match records
- **Validating/Resolving Inventory Solution duplicate values**
 - The end result and symptoms are usually first detected when using Asset products, but The root cause is usually caused by a different product



Resolving Issues in Patch Management Solution



Defining Patch Management Solution Issues



- **Symptoms:**
 - Patch Management Solution has been installed as a part of the ITMS implementation
 - Software Update plug-ins have been deployed and policies created
 - Software Update policies are not received or applied on some endpoints
 - Some Updates fail to download or install on some endpoints and we are missing SLA's
 - Compliance and Vulnerability assessment reports are not accurate
- **Testing Approach:**
 - **Ensure the Solution Implementation is sound**
 - Is the Overall ITMS/Site Implementation sound?
 - Are the Patch Management Core settings configured properly?
 - Are the SMA and Software Update plug-ins and components installed?
 - Are Patch Management Solution licenses valid?
 - **Validate Software Update Processes**
 - *Is the endpoint:*
 - Receiving Software Update policies?
 - Downloading and executing software updates?
 - Sending proper status updates to the Notification Server?
 - Rebooting at the wrong time?

Solving Patch Management Solution Issues

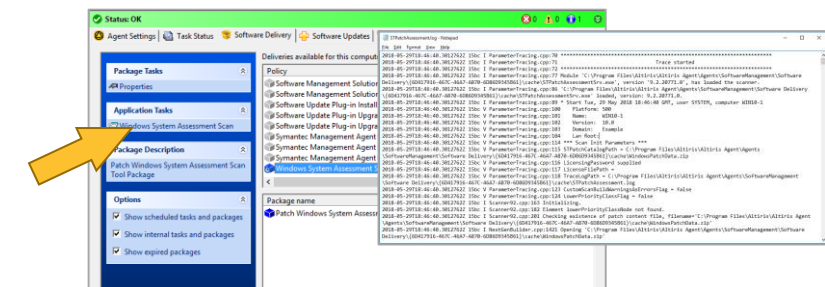
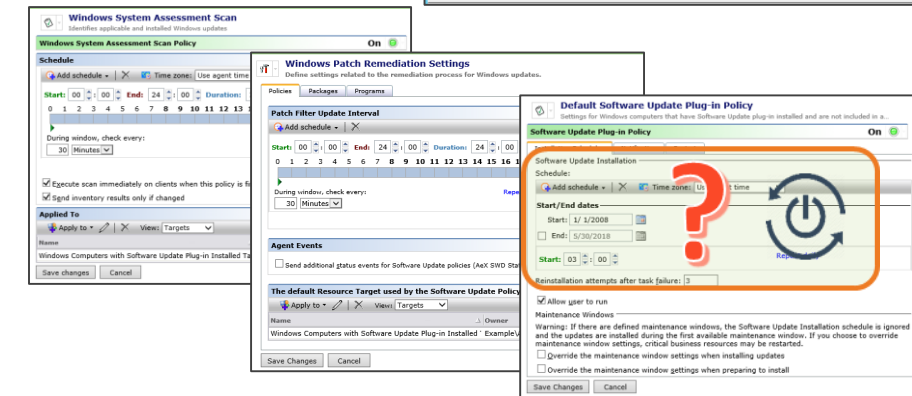
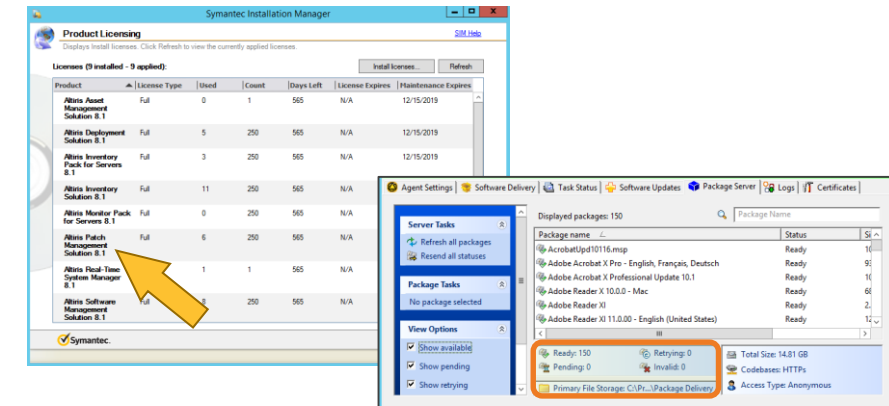


Validate Software Update Processes

Symptom: Displays Updates Stuck in a 'Pending' Status

- Troubleshooting Steps:

1. **Check Licensing:** The current Licenses may be expired, exceeded or the AUP (Annual Upgrade Protection) time has elapsed.
2. **Check Download:** Troubleshoot Agent to Site Server communications
 - Check that Package servers have the package available.
 - Check that the endpoint has more than 500 Mb of free space on the Agent Installation drive
3. **Check the Base PM Policies:** Check that the endpoint is targeted by Policies required for the Software Update Plug-in to function correctly
4. **Check if endpoint is Ignoring update schedule:** Updates cannot be applied while in this state – Reboot endpoint and test
5. **Check if Endpoint is Missing Patch inventory:**
 - Force a scan of the Patch Management Inventories (Windows System Assessment Scan) and test
 - Check the STPatchAssessment.log on the endpoint for errors in communication or process



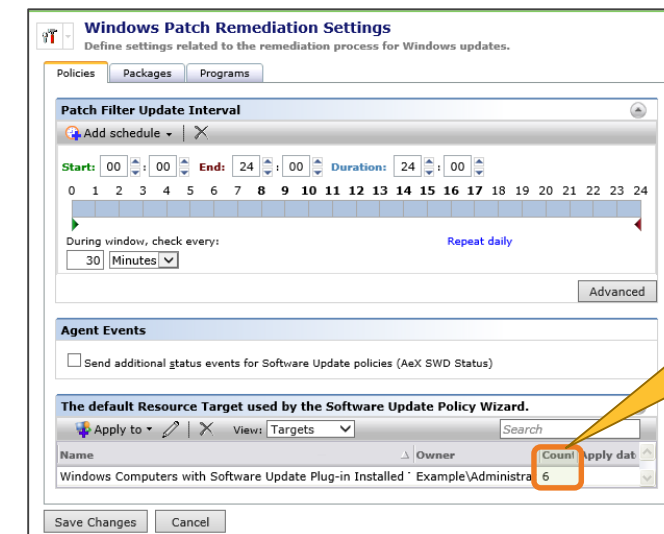
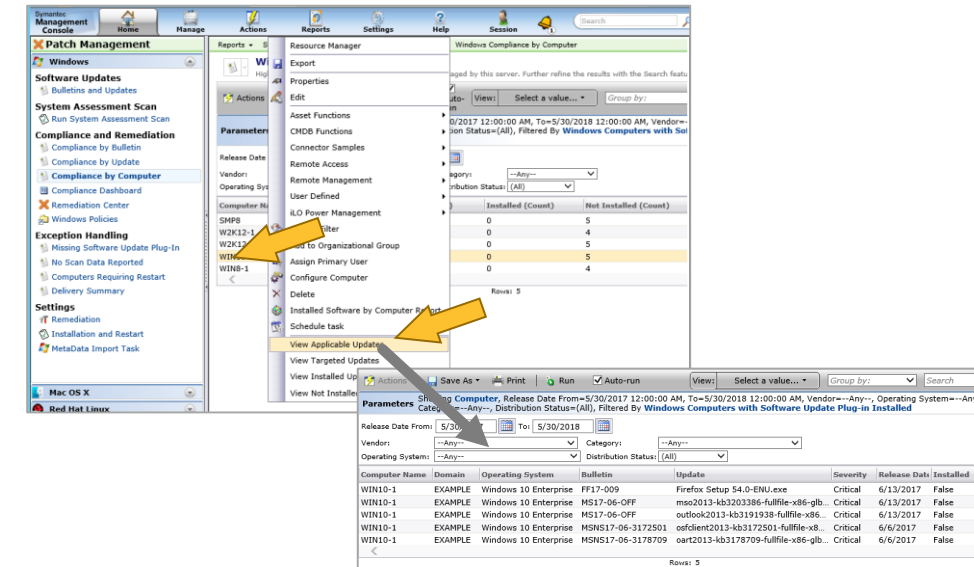
Solving Patch Management Solution Issues



Validate Software Update Processes

Symptoms: Endpoint Fails to be targeted by the SU Policy

- Troubleshooting Steps:
 1. Ensure the client is vulnerable to the Updates in the policy
 - Review the Compliance Reports (By Bulletin, By Update or By Computer)
 - These reports will show if the computer is targeted by the update's 'IsApplicable' rule.
 - Right Click on the item and choose "View Applicable..."
 2. Check that *Windows Patch Remediation Settings* has at least one client targeted.
 - Ensure at least one client or filter is targeted by this policy at all times before creating Policies and rolling out updates
 - This is critical for the process to complete, without it, the process to build resource associations will not always be successful



At least 1
Targeted
Endpoint

Solving Patch Management Solution Issues



Validate Software Update Processes

Symptoms: Patch Agent fails to download Software Updates

- Troubleshooting Steps:

1. Troubleshoot Agent to Site Server communications

- DNS, NSLookup, Ping... as taught in previous lessons

2. Check Windows Patch Remediation Settings policy

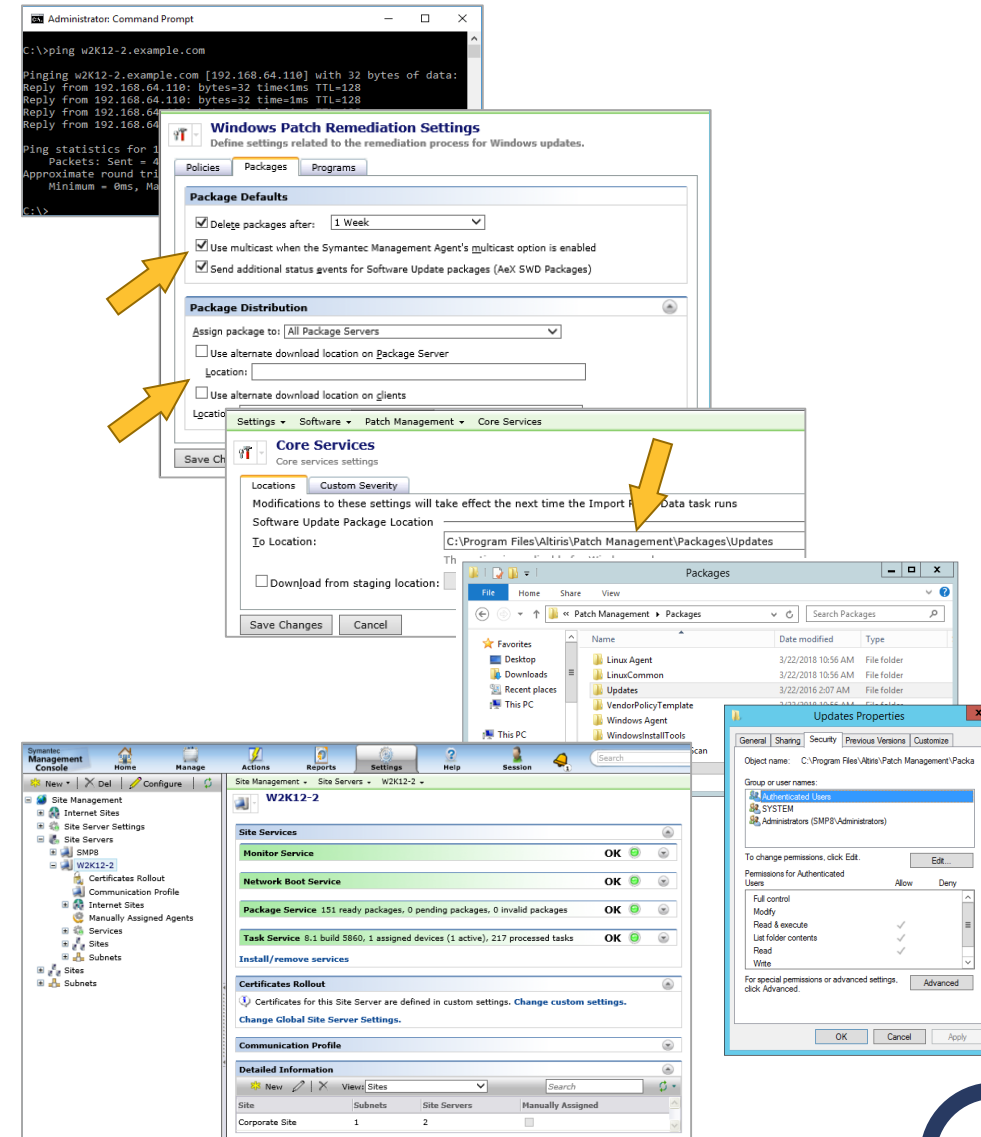
- Ensure the Delete package after setting isn't set to 0 days
- Ensure the Package Distribution settings are in order
 - Set to All Package Servers or the Package Servers individually configurations to test that communications and package integrity is maintained

3. Ensure the download location for Patch Packages is accessible

- Found on the Console under Patch Management > Core Services
- Ensure that the 'To Location' is a valid path that is accessible and the path has proper permissions in place to ensure the NTFS permissions allow all Solution Agents and Software Update Packages (See [TECH233964](#))

4. Ensure Site Management is in order:

- Subnets are targeted appropriately
- Constrained settings are in order, for there has to be at least one unconstrained Package Server per subnet.
- No Pending status count for packages



Solving Patch Management Solution Issues

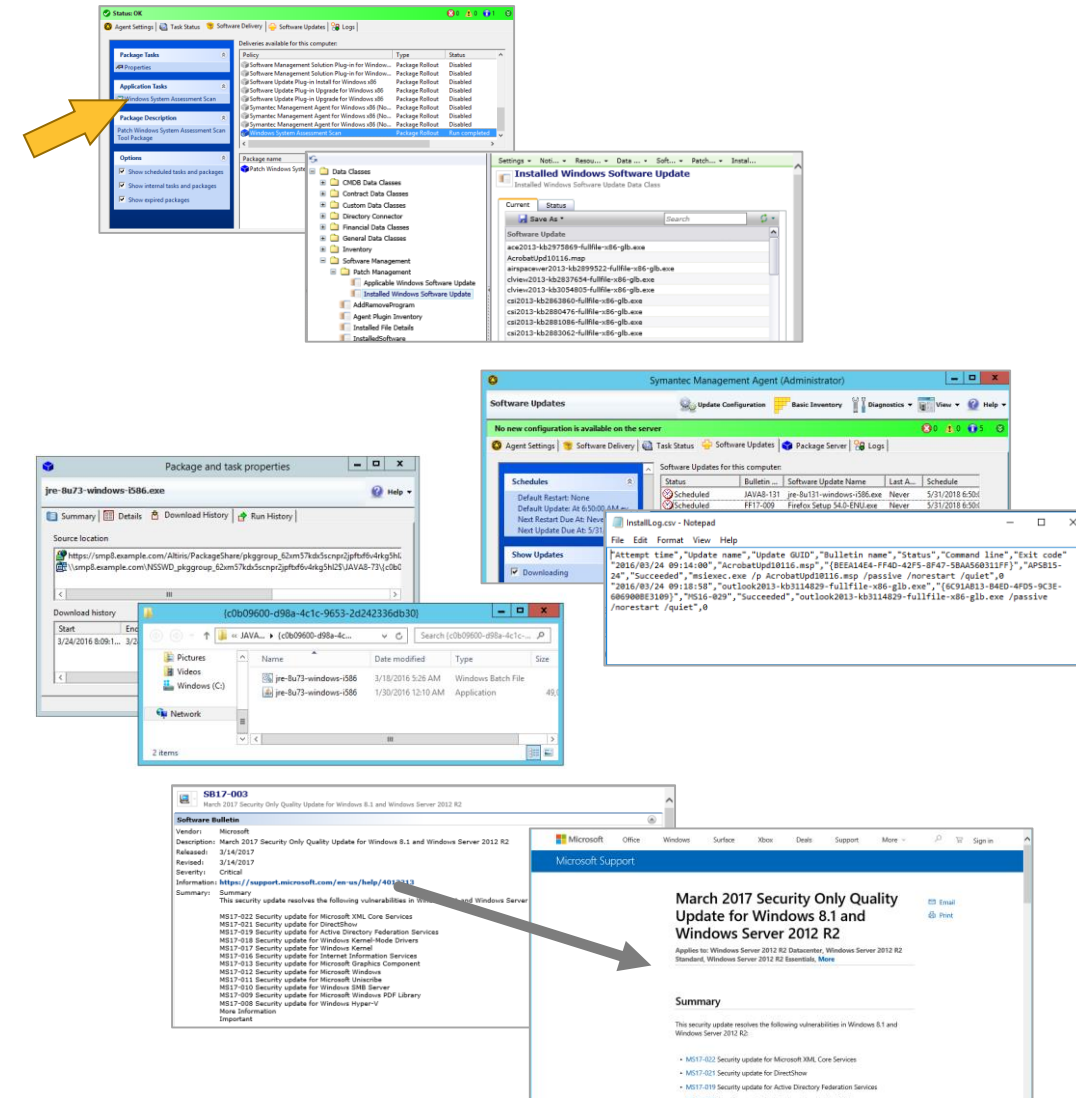


Validate Software Update Processes

Symptoms: Software Update fails to install on the endpoint

• Troubleshooting Steps:

1. **Ensure the issue is not something simple:** Like Patch Inventory failing to return Scan Inventory
2. **Find the Exit code in the Agent GUI or InstallLog.csv file and research.**
 - Exit codes will show what the issue is regarding the install process
 - Exit codes detail individual issues; where some are 'client needs reboot' and others outlined 'update is already installed.'
3. **Check if the Update is failing due to 'Rules Issue'**
 - If an update is failing to install; run it manually from the URL link provided in the Download History of that update and review results
 - If an update is failing to target; check Vendor's Web site for the update and ensure that the update is actually supposed to be targeting the client.
 - Check if the dll, or target file, is the version that is to be updated
 - Often the rule issue is a problem with how the update is confirming **IsInstalled=TRUE**, or the file is current and the OS is at fault for failing to provide the proper Add/Remove Listings.
4. **Contact Symantec Support if it continues to fail**
 - Document these checks/results in the Support Case
 - Gather all the data from **HOWTO60789** in a single compressed folder.



Solving Patch Management Solution Issues



Validate Software Update Processes

Symptom: Clients Are Compliant, but Reporting Says Vulnerable

• Troubleshooting Steps:

1. Check the Windows Patch Remediation Settings

- Check that 'Send additional status events for Software Update policies (Aex SWD Status)' is enabled
- Will resolve most discrepancies in Patch reporting if enabled

2. Check the Client's Registry to see if a reboot is required

- Check for HKLM\SOFTWARE\Altiris\Altiris Agent\Patch Management - 'RebootRequired' with a value of (1):
- Reboot the client and allow for time to gather the event files

3. Compare Resource Manager with Compliance Report

- Open **"Installed Windows Software Update"** Data Class from endpoint's Resource Manager
- Open **Compliance by Computer** report and look at installed updates
- Match the installed list with the report to see what is conflicting
 - You will see a discrepancy if there is a delay in reporting Patch events
 - Wait for the Software Update Cycle to execute on the client

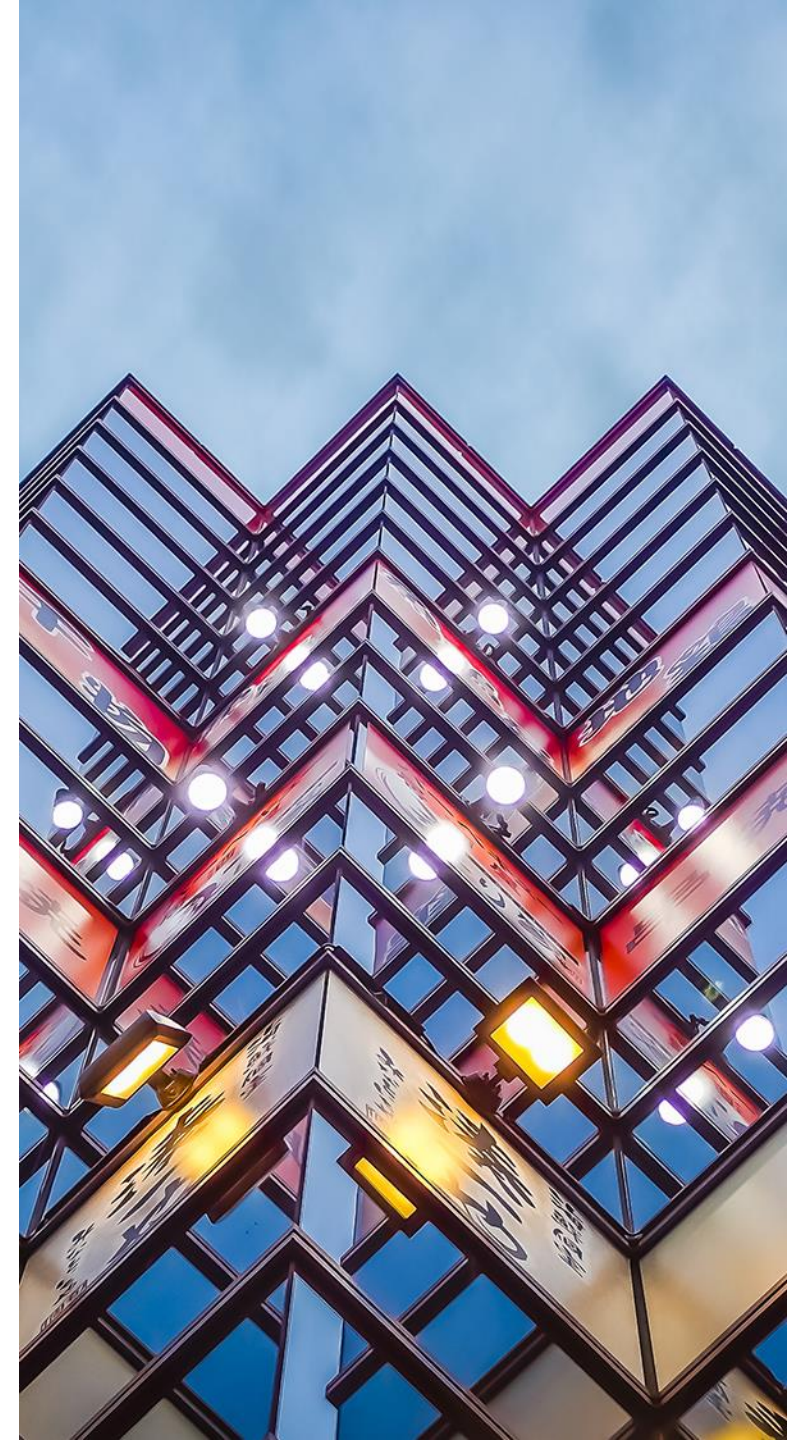
The image displays three screenshots related to Windows patch management troubleshooting.

The top screenshot shows the **Windows Patch Remediation Settings** window. The **Patch Filter Update Interval** is set to 24 hours. The **Agent Events** section has **Send additional status events for Software Update policies (Aex SWD Status)** checked. The **The default Resource Target used by the Software Update Policy Wizard** is set to **Windows Computer**.

The middle screenshot shows the **Registry Editor** window. The left pane shows the tree structure expanded to **Computer > HKEY_LOCAL_MACHINE > SOFTWARE > Altiris > Altiris Agent > Patch Management**. The right pane shows the **RebootRequired** value, which is a **REG_SZ** type with a data value of **(1)**.

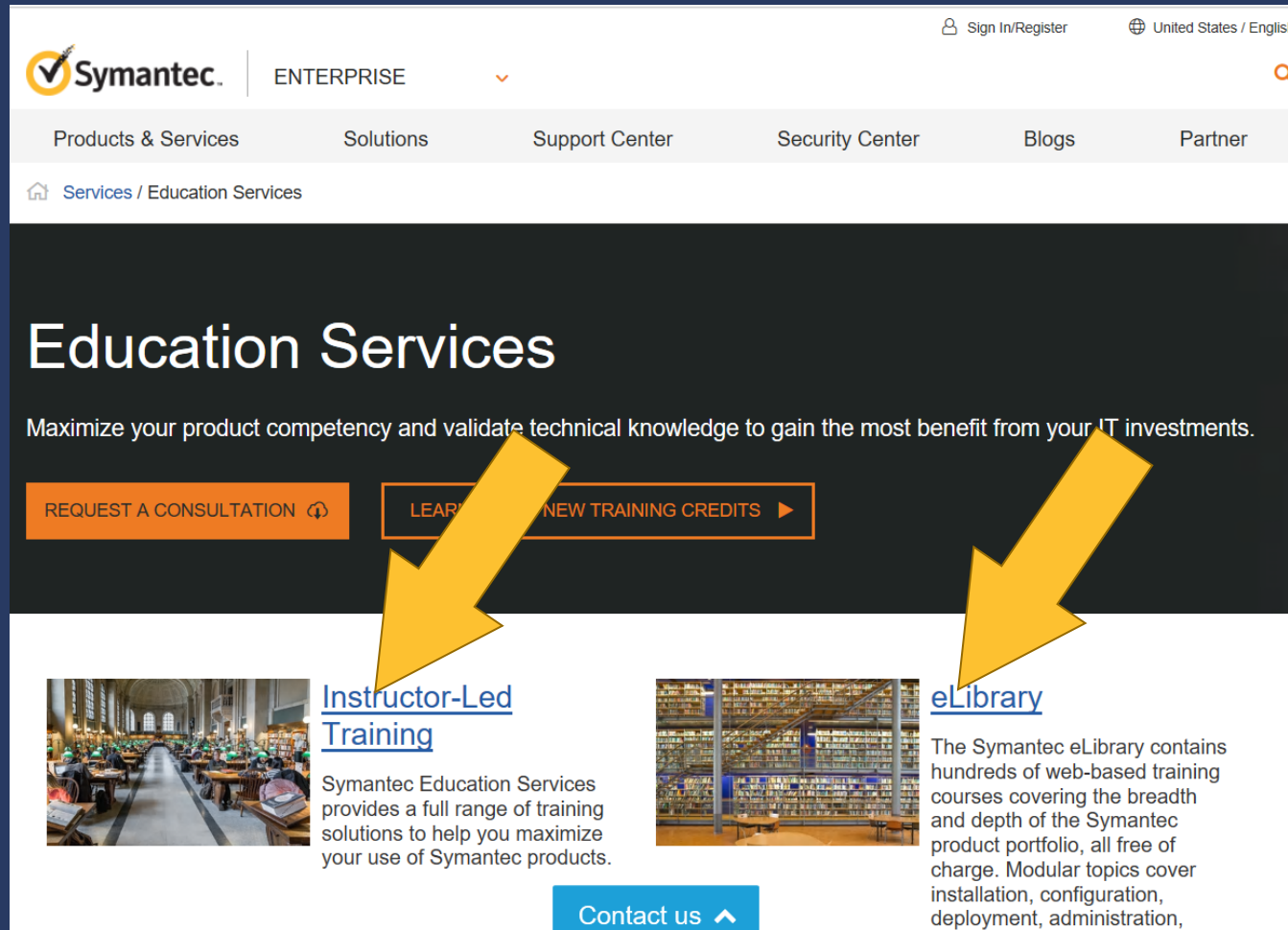
The bottom screenshot shows the **Installed Updates** window. The **Parameters** section shows **Release Date From: 5/30/2014** and **To: 5/30/2018**. The **Operating System** is set to **Windows 10**. The **Category** is set to **Software Updates**. The **Installed Updates** list shows various updates, including **Windows 10 KB4013147** and **Windows 10 KB4013148**.

Additional Information



ITMS 8.x Diagnostics & Troubleshooting Course

GO TO: <https://go.symantec.com/education>



The screenshot shows the Symantec Education Services website. At the top, there's a navigation bar with the Symantec logo, 'ENTERPRISE' dropdown, and links for 'Sign In/Register', 'United States / English', and a search icon. Below this is a secondary navigation bar with links for 'Products & Services', 'Solutions', 'Support Center', 'Security Center', 'Blogs', and 'Partner'. A breadcrumb trail shows 'Services / Education Services'. The main heading is 'Education Services' with a subtext: 'Maximize your product competency and validate technical knowledge to gain the most benefit from your IT investments.' Below this are two orange buttons: 'REQUEST A CONSULTATION' and 'LEARN MORE ABOUT NEW TRAINING CREDITS'. Two large yellow arrows point from these buttons to the 'Instructor-Led Training' and 'eLibrary' sections respectively. The 'Instructor-Led Training' section features an image of a classroom and text stating that Symantec Education Services provides a full range of training solutions. The 'eLibrary' section features an image of a library and text stating that the Symantec eLibrary contains hundreds of web-based training courses. A 'Contact us' button is at the bottom.

Education Services

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

[REQUEST A CONSULTATION](#) [LEARN MORE ABOUT NEW TRAINING CREDITS](#)

Instructor-Led Training

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

eLibrary

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

[Contact us](#)

Course is Available:

- **Instructor Led / Virtual Class**
 - 4 Lessons – 2 Day Course
- **Symantec eLibrary**
 - 4 Lessons – 6 Hours of Videos!

Additional Resources and Summary



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

- **Product Overviews:** <https://www.symantec.com/products/it-management-suite>
- **Data Sheets:** <https://www.symantec.com/products/endpoint-management>
- **Community:** <http://www.symantec.com/connect/endpoint-management>
- **ITMS Documentation:** https://support.symantec.com/en_US/article.DOC11076
- **ITMS Help Center:** https://help.symantec.com/home/ITMS8.5?locale=EN_US
- **GSS Documentation:** <https://www.symantec.com/docs/DOC8558>
- **GSS Help Center:** https://help.symantec.com/home/gss3.3?locale=EN_US&sku=GHOST_SOLUTION_SUITE_3_3



Q&A





Thank You!

brian_sheedy@Symantec.com
+1 713 309 5742

