

# SOFTWARE UPDATES MANAGEMENT IN CONFIGURATION MANAGER

Vinay Pamnani

SR. SUPPORT ESCALATION ENGINEER, MICROSOFT CORPORATION

Contributors: Mike Johnson and Meghan Stewart

NOTE: This document was originally written for Configuration Manager 2012 R2, but most of the concepts explained are also applicable to Configuration Manager Current Branch.

Introduction to Software Updates Management .....	4
Installation & Configuration.....	5
Prerequisites & Requirements.....	5
Software Updates.....	5
Endpoint Protection .....	5
Installation & Configuration .....	5
Software Update Point Role.....	5
Endpoint Protection Role .....	5
Configuring Client Settings .....	6
Configuring Client Settings for Software Updates.....	6
Configuring Client Settings for Endpoint Protection .....	6
Other Relevant Client Settings .....	7
Deployment.....	8
Client Requirements .....	8
Update Groups .....	8
Deployment Packages .....	8
Deployments .....	8
Maintenance Windows.....	9
Maintenance .....	9
Expired Updates .....	9
Content Cleanup.....	9
WSUS Server Maintenance.....	10
How it works .....	12
Software Update Point Installation .....	12
WSUS Configuration Manager.....	13
Synchronization .....	15
On Central Administration Site or Standalone Primary Site .....	15
On Child Primary Site and Secondary Sites .....	19
Compliance .....	21
Software Update Scan Policy .....	22
WSUS Server Location .....	24
Software Update Scan on Clients .....	27
State Message Processing Flow .....	32
Software Update Summarization.....	35
Software Update Switching (SP1 and R2 only).....	36
Deployment .....	36
Creating a Software Update Group.....	36
manually Creating a Deployment for Software Update Group.....	38

Creating a Deployment using an Automatic Deployment Rule.....	43
Deployment Evaluation and Update Installation on Clients .....	48
State Message Reporting .....	56
End User Experience .....	57
Scenario 1 – Suppress Restart Disabled .....	57
Scenario 2 – Suppress Restart Enabled .....	59
Scenario 3 – Override Maintenance Window without suppressing reboot.....	61
Best Practices .....	64
Troubleshooting.....	64
Synchronization .....	64
Relevant Data .....	64
Synchronization fails with “WSUS server not configured” .....	64
Synchronization fails Because of issues with THE EULA.....	66
Synchronization fails because of errors communicating with Microsoft Update .....	66
WSUS Control Manager (WSUSCtrl) reports an error .....	66
Compliance .....	67
Relevant Data .....	67
Scan Failures.....	67
Group Policy overrides WSUS Server .....	68
Compliance results Unknown .....	69
Clients are unable to find the WSUS Source Location.....	69
Deployment .....	69
Relevant Data .....	69
Updates fail to get downloaded.....	69
Update installation fails .....	70
Unexpected Reboots OR Updates are Installed outside OF A Maintenance Window .....	70
Procedures .....	71
A. Logging .....	71
How to enable Verbose & Debug Logging on the Configuration Manager Client & Management Point .....	71
How to enable Verbose Logging for State System component on the Site Server .....	71
How to enable Verbose Logging for WSUS Synchronization Manager (WSyncMgr) .....	71
How to enable SQL Tracing for Configuration Manager Logs .....	72
How to enable verbose logging for Windows Update Agent.....	72
How to configure SQL Profiler to troubleshoot WSUS Location Request Issues.....	72
How to configure SQL Profiler to see State Message processing.....	73
B. Synchronization .....	74
How to Configure Proxy Settings for the Software Update Point .....	74
How to Check Proxy Configuration on a computer.....	75
How to Configure WSUS Server Connection Account for the Software Update Point .....	75
How to Determine the Port Settings Used by WSUS .....	76

Verify Anonymous Access is Enabled on the DssAuthWebService Virtual Directory.....	76
Check Permissions on the ApiRemoting30 Virtual Directory .....	76
Check the Update Source Settings in WSUS.....	77
How to test Connectivity from Site Server to WSUS.....	78
How to check WSUS Server Version.....	78
Configure Software Update Point for Secure Sockets Layer (SSL) .....	78
C. Compliance .....	79
How to check Proxy Settings on a Client .....	79
How to check if WSUS Server Ports are accessible from the client .....	80
How to verify connectivity on a client against the WSUS (Software Update Point) Server .....	80
How to reset the Windows Update Agent Data Store .....	81
How to use Windows Update Troubleshooter and update the Windows Update Agent to the latest version.....	81
D. Deployment.....	82
How to review ServiceWindowManager.log.....	82
How to review the Audit Status messages to find if a Deployment was modified .....	83
ADDITIONAL RESOURCES .....	83
How many clients can the Software Update Point support? .....	83
What's the maximum number of updates you can have in a Deployment? .....	83
Can I manage software updates for clients in an untrusted forest? .....	83

Software Update Management in System Center 2012 Configuration Manager provides a set of tools and resources that help manage the complex task of tracking and applying software updates to client computers in the enterprise. An effective software update management process is necessary to maintain operational efficiency, overcome security issues, and maintain the stability of the network infrastructure. However, because of the changing nature of technology and the continual appearance of new security threats, effective software update management requires consistent and continual attention.

Configuration Manager synchronizes Software Updates from the Microsoft Update Catalog to retrieve software update metadata, and then it makes them available in the Configuration Manager console. To do this, Configuration Manager requires a Windows Server Update Services (WSUS) computer that has the Software Update Point role installed. After synchronization is completed, a site-wide policy is created that provides the location of the Software Update Point to the client computers. After receiving this policy, clients scan for software update compliance against the WSUS computer (Software Update Point) and report the results to the management point, which then sends that information to the Configuration Manager site server. This allows an administrator to determine which updates are required on the clients so that updates can be deployed to the clients efficiently. After the updates are deployed, clients install the updates and send updated compliance results back which can then be used for compliance reporting.

As such, Software Update Management can be broken down in to four main components:

- Synchronization
- Compliance
- Deployment
- Reporting

## INSTALLATION & CONFIGURATION

### PREREQUISITES & REQUIREMENTS

---

#### SOFTWARE UPDATES

Prerequisites for Software Updates in Configuration Manager are documented here:

<http://technet.microsoft.com/en-us/library/hh237372.aspx>

Requirements for the Site System that will host the Software Update Point role are documented here:

[http://technet.microsoft.com/en-us/library/c1e93ef9-761f-4f60-8372-df9bf5009be0#BKMK\\_SupConfigSiteSystemReq](http://technet.microsoft.com/en-us/library/c1e93ef9-761f-4f60-8372-df9bf5009be0#BKMK_SupConfigSiteSystemReq)

[http://technet.microsoft.com/en-us/library/gg712696.aspx#BKMK\\_SUPInstallation](http://technet.microsoft.com/en-us/library/gg712696.aspx#BKMK_SUPInstallation)

---

#### ENDPOINT PROTECTION

Prerequisites for Endpoint Protection in Configuration Manager are documented here:

<http://technet.microsoft.com/en-us/library/hh508780.aspx>

Requirements for the Site System that will host the Endpoint Protection role are documented here:

[http://technet.microsoft.com/en-us/library/c1e93ef9-761f-4f60-8372-df9bf5009be0#BKMK\\_SupConfigSiteSystemReq](http://technet.microsoft.com/en-us/library/c1e93ef9-761f-4f60-8372-df9bf5009be0#BKMK_SupConfigSiteSystemReq)

### INSTALLATION & CONFIGURATION

How to install a Site System Role in Configuration Manager:

[http://technet.microsoft.com/en-us/library/5c669a3c-404f-4a5d-88f0-bc40443ebaae#BKMK\\_HowtoInstallSiteSystems](http://technet.microsoft.com/en-us/library/5c669a3c-404f-4a5d-88f0-bc40443ebaae#BKMK_HowtoInstallSiteSystems)

---

#### SOFTWARE UPDATE POINT ROLE

Installation and Configuration of Software Update Point Role:

[http://technet.microsoft.com/en-us/library/912bfec1-fd19-4f56-a840-4ecd643c541b#BKMK\\_InstallSUP](http://technet.microsoft.com/en-us/library/912bfec1-fd19-4f56-a840-4ecd643c541b#BKMK_InstallSUP)

Synchronize Software Updates:

[http://technet.microsoft.com/en-us/library/912bfec1-fd19-4f56-a840-4ecd643c541b#BKMK\\_SUMSync](http://technet.microsoft.com/en-us/library/912bfec1-fd19-4f56-a840-4ecd643c541b#BKMK_SUMSync)

Configure Classifications and Products to Synchronize:

[http://technet.microsoft.com/en-us/library/912bfec1-fd19-4f56-a840-4ecd643c541b#BKMK\\_ConfigureClassesProducts](http://technet.microsoft.com/en-us/library/912bfec1-fd19-4f56-a840-4ecd643c541b#BKMK_ConfigureClassesProducts)

---

#### ENDPOINT PROTECTION ROLE

Steps to Configure Endpoint Protection in Configuration Manager:

<http://technet.microsoft.com/en-us/library/hh508770.aspx>

Installation of the Endpoint Protection Point Role:

[http://technet.microsoft.com/en-us/library/hh508770.aspx#BKMK\\_Step1](http://technet.microsoft.com/en-us/library/hh508770.aspx#BKMK_Step1)

Configure Alerts for Endpoint Protection in Configuration Manager:

<http://technet.microsoft.com/en-us/library/hh508782.aspx>

Configure Definition Updates for Endpoint Protection in Configuration Manager:

<http://technet.microsoft.com/en-us/library/jj822983.aspx>

Create and Deploy Antimalware Policies for Endpoint Protection in Configuration Manager:

<http://technet.microsoft.com/en-us/library/hh508785.aspx>

Configuring products and classifications required for Endpoint Protection for Software Update Point:

- 1) In the **Configuration Manager Console**:
  - a) Go to the Administration pane, expand **Site Configuration**, and then click **Sites**.
  - b) Right-click the Central Administration or Standalone Primary Site.
  - c) Select **Configure Site Components**, and then click **Software Update Point**.
- 2) On the **Classifications** tab, make sure that the **Definition Updates** check box and the **Updates** check box are selected.
- 3) On the **Products** tab, make sure that the **Forefront Endpoint Protection 2010** check box is selected, and then click **OK**.

## CONFIGURING CLIENT SETTINGS

How to create and configure Client Settings in Configuration Manager:

<http://technet.microsoft.com/en-us/library/gg682109>

About Client Settings in Configuration Manager

<http://technet.microsoft.com/en-us/library/gg682067.aspx>

---

## CONFIGURING CLIENT SETTINGS FOR SOFTWARE UPDATES

Information about Software Update Client Settings:

[http://technet.microsoft.com/en-us/library/gg682067.aspx#BKMK\\_SoftwareUpdatesDeviceSetting](http://technet.microsoft.com/en-us/library/gg682067.aspx#BKMK_SoftwareUpdatesDeviceSetting)

Planning for Settings associated with Software Updates:

[http://technet.microsoft.com/en-us/library/gg712696.aspx#BKMK\\_Settings](http://technet.microsoft.com/en-us/library/gg712696.aspx#BKMK_Settings)

[http://technet.microsoft.com/en-us/library/912bfec1-fd19-4f56-a840-4ecd643c541b#BKMK\\_AssociatedSettings](http://technet.microsoft.com/en-us/library/912bfec1-fd19-4f56-a840-4ecd643c541b#BKMK_AssociatedSettings)

---

## CONFIGURING CLIENT SETTINGS FOR ENDPOINT PROTECTION

Information about Endpoint Protection Client Settings:

[http://technet.microsoft.com/en-us/library/gg682067.aspx#BKMK\\_EndpointProtectionDeviceSettings](http://technet.microsoft.com/en-us/library/gg682067.aspx#BKMK_EndpointProtectionDeviceSettings)

Configuring Client Settings for Endpoint Protection:

[http://technet.microsoft.com/en-us/library/hh508770.aspx#BKMK\\_Step2](http://technet.microsoft.com/en-us/library/hh508770.aspx#BKMK_Step2)

---

## OTHER RELEVANT CLIENT SETTINGS

### **Background Intelligent Transfer:**

[http://technet.microsoft.com/en-us/library/gg682067.aspx#BKMK\\_BITS](http://technet.microsoft.com/en-us/library/gg682067.aspx#BKMK_BITS)

### **Client Policy:**

[http://technet.microsoft.com/en-us/library/gg682067.aspx#BKMK\\_ClientPolicyDeviceSettings](http://technet.microsoft.com/en-us/library/gg682067.aspx#BKMK_ClientPolicyDeviceSettings)

### **Computer Agent:**

[http://technet.microsoft.com/en-us/library/gg682067.aspx#BKMK\\_ComputerAgentDeviceSettings](http://technet.microsoft.com/en-us/library/gg682067.aspx#BKMK_ComputerAgentDeviceSettings)

### **Computer Restart:**

[http://technet.microsoft.com/en-us/library/gg682067.aspx#BKMK\\_ComputerRestartDeviceSettings](http://technet.microsoft.com/en-us/library/gg682067.aspx#BKMK_ComputerRestartDeviceSettings)

### **Network Access Protection (NAP):**

[http://technet.microsoft.com/en-us/library/gg682067.aspx#BKMK\\_NAPDeviceSettings](http://technet.microsoft.com/en-us/library/gg682067.aspx#BKMK_NAPDeviceSettings)

### **State Messaging:**

State Message Reporting Cycle (minutes) - Default value is 15 minutes



## DEPLOYMENT

### CLIENT REQUIREMENTS

Windows Update Agent 3.0 or later.

### UPDATE GROUPS

Software update groups provide you with an effective method to organize software updates in your environment. For steps on adding updates to an update group, refer to the following:

[http://technet.microsoft.com/en-us/library/gg712304.aspx#BKMK\\_AddUpdatesToGroup](http://technet.microsoft.com/en-us/library/gg712304.aspx#BKMK_AddUpdatesToGroup)

### DEPLOYMENT PACKAGES

Planning for Content Management:

<http://technet.microsoft.com/en-us/library/gg712321.aspx>

Downloading updates to Deployment Package:

[http://technet.microsoft.com/en-us/library/gg712304.aspx#BKMK\\_DownloadUpdates](http://technet.microsoft.com/en-us/library/gg712304.aspx#BKMK_DownloadUpdates)

Distributing Deployment Package to the Distribution Points:

[http://technet.microsoft.com/en-us/library/gg712694.aspx#BKMK\\_DistributeContent](http://technet.microsoft.com/en-us/library/gg712694.aspx#BKMK_DistributeContent)

Monitoring Content:

[http://technet.microsoft.com/en-us/library/gg712694.aspx#BKMK\\_MonitorContent](http://technet.microsoft.com/en-us/library/gg712694.aspx#BKMK_MonitorContent)

### DEPLOYMENTS

Deploying Software Updates

[http://technet.microsoft.com/en-us/library/gg712304.aspx#BKMK\\_SUMDeploy](http://technet.microsoft.com/en-us/library/gg712304.aspx#BKMK_SUMDeploy)

Example Scenario for Deploying Security Software Updates released monthly:

<http://technet.microsoft.com/en-us/library/jj134348.aspx>

Manual Deployment

[http://technet.microsoft.com/en-us/library/gg712304.aspx#BKMK\\_ManualDeploy](http://technet.microsoft.com/en-us/library/gg712304.aspx#BKMK_ManualDeploy)

Automatic Deployment Rules (ADR)

[http://technet.microsoft.com/en-us/library/gg712304.aspx#BKMK\\_AutoDeploy](http://technet.microsoft.com/en-us/library/gg712304.aspx#BKMK_AutoDeploy)

Deploying Definition Updates for Endpoint Protection

See “Using Configuration Manager Software Updates to Deliver Definition Updates” section on the following TechNet website:

<http://technet.microsoft.com/en-us/library/jj822983.aspx>

## MAINTENANCE WINDOWS

### Maintenance Windows

<http://technet.microsoft.com/en-us/library/hh508762.aspx>

### Maintenance Windows vs. Business Hours:

<http://blogs.technet.com/b/server-cloud/archive/2012/03/28/business-hours-vs-maintenance-windows-with-system-center-2012-configuration-manager.aspx>

## MAINTENANCE

### EXPIRED UPDATES

As part of the ongoing update revision process, some updates in the Microsoft Update Catalog are expired. This typically occurs when there is a newer version of the update available. However, in rare cases, Microsoft may discover a problem with an update and expire it for that reason as well. During software update synchronization, these expired updates are marked as *Expired* in the Configuration Manger console. This expired status is indicated by a gray icon next to the update. These expired updates are automatically cleaned up from the Configuration Manager database on a regular schedule.

Removal of expired updates is performed by the WSUS Synchronization Manager component, and these updates are removed only if the following conditions are true:

- The update is not referenced in an Update Assignment.
- The update is older than the value of Updates Cleanup Age (seven days, by default).

WSUS Synchronization Manager at the top-level Configuration Manger site checks every hour for updates that need to be removed, and it removes expired updates if they match the criteria in the preceding bulleted list. When WSUS Synchronization Manager deletes expired updates, the following entries can be seen in the WSyncMgr.log:

```
Deleting old expired updates... SMS_WSUS_SYNC_MANAGER
Deleted 100 expired updates   SMS_WSUS_SYNC_MANAGER
...
...
Deleted 2995 expired updates total   SMS_WSUS_SYNC_MANAGER
```

### CONTENT CLEANUP

As expired updates are removed, content for those expired updates may become orphaned. WSUS Synchronization Manager also cleans up this orphaned content. As part of the content clean up, WSUS Synchronization Manager analyzes the packages that are owned by the current site, finds content that is no longer referenced, and then removes the content from the package source directory. Content is removed only if it has been orphaned for more than one day (by default).

If any content is removed, the cleanup process also refreshes the package so that the updated content is sent to the distribution points (DPs). When WSUS Synchronization Manager removes orphaned content, the following entries can be seen in the WSyncMgr.log:

```
Deleting orphaned content for package CS100006 (EPDefinitions) from source <PackageSource>
SMS_WSUS_SYNC_MANAGER
Deleting orphaned content folder \\<PackageSource>\51b6db15-6938-4b37-9fa8-caf513e13930...
SMS_WSUS_SYNC_MANAGER
.
.
Deleting orphaned content folder \\<PackageSource>\526b6a85-a62c-4d54-bc0d-b3409223b0df...
SMS_WSUS_SYNC_MANAGER
Deleted 12 orphaned content folders in package CS100006 (EPDefinitions) SMS_WSUS_SYNC_MANAGER
Refreshing package CS100006 (EPDefinitions) SMS_WSUS_SYNC_MANAGER
```

For more information about cleanup of expired updates and content, see the following blog post:

<http://blogs.technet.com/b/configmgrteam/archive/2012/04/12/software-update-content-cleanup-in-system-center-2012-configuration-manager.aspx>

## WSUS SERVER MAINTENANCE

To maintain optimal performance of the WSUS database, we recommend that you routinely perform the WSUS Cleanup Wizard tasks on the WSUS database (SUSDB) as well as re-index the WSUS database on each WSUS computer that is hosting a Software Update Point role in the Configuration Manager environment. When you perform WSUS Cleanup Wizard actions in a multi-level hierarchy, make sure that you run the cleanup process on the lowest tier of WSUS server chain first, then move up to the next tier to run the Cleanup Wizard tasks, and continue on up the hierarchy until you reach the top-tier WSUS server. This WSUS maintenance can be performed simultaneously on multiple servers in the same tier. And although the re-indexing can be performed in any order on any WSUS server's SUSDB, we recommend that you perform the cleanup and re-indexing on each WSUS server, running the re-indexing first, followed by the Cleanup Wizard tasks. By tuning the performance of the SUSDB first through re-indexing, the Cleanup Wizard tasks are completed more quickly.

### Re-indexing the WSUS database (SUSDB):

You can re-index the WSUS database (SUSDB) by using the script in the following TechNet resource:

<http://gallery.technet.microsoft.com/scriptcenter/6f8cde49-5c52-4abd-9820-f1d270ddea61>

**If WSUS Database is installed on SQL Server**, use SQL Server Management Studio to connect to the database server and to run the database maintenance script.

**If WSUS Database is installed on Windows Internal Database**, you can use either SQL Management Studio Express or the `sqlcmd` utility.

1. To use SQL Management Studio Express:
  - a. Start SQL Management Studio Express, and then connect to the database server.  
For Server 2012 or Server 2012 R2, Server Name would be: `\\.\pipe\MICROSOFT##WID\tsql\query`  
For older operating systems, Server Name would be: `\\.\pipe\MSSQL$MICROSOFT##SSEE\sql\query`
  - b. Click **New Query**, paste the contents of the Database maintenance script, and then click **Execute**.

2. To use **sqlcmd** utility, open a command prompt with Administrator privileges, and then run the following command.

For Server 2012 or Server 2012 R2:

```
sqlcmd -S \\.\pipe\MICROSOFT##WID\tsql\query -i <scriptLocation>\WsusDBMaintenance.sql
```

For older operating systems:

```
sqlcmd -S \\.\pipe\MSSQL$MICROSOFT##SSEE\sql\query -i <scriptLocation>\WsusDBMaintenance.sql
```

**TIP:**

If you are not sure whether the WSUS database is hosted on SQL Server or Windows Internal Database, you can verify by checking the following registry key on the WSUS server:

```
HKLM\Software\Microsoft\Update Services\Server\Setup\SQLServerName
```

If you see just the ServerName or Server\Instance, you are using SQL Server. If you see something that has the ##SSEE or ##WID string in it, the WSUS database is installed on the Windows Internal Database.

**TIP:**

To determine the version of SQL Server Management Studio Express to install:

- 1) For Windows Server 2012 or Windows Server 2012 R2, go to C:\Windows\WID\Log, and then open the latest ErrorLog in Notepad.
- 2) For Windows Server 2008 R2 or earlier, go to C:\Windows\SYSTEM32\SSEE\MSSQL.2005\MSSQL\LOG, and then open the latest ErrorLog in Notepad.

At the very top of the ErrorLog file, you will find the version number (for example, 9.00.4035.00 x64). Look up the version number here at <http://www.sqlteam.com/article/sql-server-versions> and locate the service pack level it's running. Use the version number and service pack level to search the [Download Center](#) for SQL Management Studio Express.

## Performing a WSUS Server cleanup:

The WSUS Server Cleanup Wizard can be run from the WSUS Console -> Options. We recommend that WSUS Maintenance be run once a month. If cleanup has never been run and the WSUS computer has been in production for a long time, it is possible that the cleanup may time out and fail. If this occurs, run the cleanup with only the **Unused updates and updates revisions** check box selected (the top check box). Then, wait for the process to finish before you run the cleanup again with the next check box selected. Keep in mind that this may require several passes to complete the cleanup process. Lastly, run cleanup with all the options selected.

You can find more information about the WSUS Server Cleanup Wizard here:

[http://technet.microsoft.com/en-us/library/dd939856\(v=ws.10\)](http://technet.microsoft.com/en-us/library/dd939856(v=ws.10))

**NOTE:**

All log excerpts in this section are from a System Center 2012 R2 Configuration Manager (ConfigMgr 2012 R2) environment with Verbose & Debug Logging enabled. For information about how to enable Verbose & Debug Logging see [How to enable Verbose & Debug Logging](#).

In order to see some of the SQL queries being executed in the logs on the Configuration Manager Site Server, SQL Tracing must be enabled. For information about how to do this please see [How to enable SQL Tracing for Configuration Manager Logs](#).

SOFTWARE UPDATE POINT INSTALLATION

Installation of a Software Update Point is initiated by adding the Software Update Point role. When the Software Update Point role is installed, an instance of *SMS\_SCI\_SysResUse* class is created, and entries that resemble the following are logged in SMSProv.log.

**SMSProv.log:**

```
PutInstanceAsync SMS_SCI_SysResUse SMS Provider 2/9/2014 10:53:16 PM 5804 (0x16AC)
CExtProviderClassObject::DoPutInstanceInstance SMS Provider 2/9/2014 10:53:16 PM 5804 (0x16AC)
INFO: 'PR1SITE.CONTOSO.COM' is a valid FQDN. SMS Provider 2/9/2014 10:53:16 PM 5804 (0x16AC)
```

Site Component Manager then detects the change in site control information and initiates the installation of the Software Update Point role. When this occurs, entries that resemble the following are logged in SiteComp.log.

**SiteComp.log:**

```
Parsed the master site control file, serial number 3559422579. SMS_SITE_COMPONENT_MANAGER 2/9/2014
10:53:23 PM 4460 (0x116C)
Synchronizing server table and polling servers as needed... SMS_SITE_COMPONENT_MANAGER 2/9/2014
10:53:23 PM 4460 (0x116C)
Synchronizing component server PR1SITE.CONTOSO.COM... SMS_SITE_COMPONENT_MANAGER 2/9/2014
10:53:23 PM 4460 (0x116C)
Installing component SMS_WSUS_CONTROL_MANAGER... SMS_SITE_COMPONENT_MANAGER 2/9/2014
10:53:23 PM 6040 (0x1798)
INFO: 'PR1SITE.CONTOSO.COM' is a valid FQDN. SMS_SITE_COMPONENT_MANAGER 2/9/2014 10:53:23 PM 6040
(0x1798)
Creating registry keys Operations Management\SMS Server Role\SMS Software Update Point on server
PR1SITE.CONTOSO.COM. SMS_SITE_COMPONENT_MANAGER 2/9/2014 10:53:23 PM 6040 (0x1798)
Updated WSUS Configuration for PR1SITE.CONTOSO.COM. SMS_SITE_COMPONENT_MANAGER 2/9/2014
10:53:23 PM 6040 (0x1798)
The component is being installed on the site server, no files need to be installed in the "E:\ConfigMgr" directory because the
files are already there. SMS_SITE_COMPONENT_MANAGER 2/9/2014 10:53:23 PM 6040 (0x1798)
All files installed. SMS_SITE_COMPONENT_MANAGER 2/9/2014 10:53:23 PM 6040 (0x1798)
Starting bootstrap operations... SMS_SITE_COMPONENT_MANAGER 2/9/2014 10:53:23 PM 6040 (0x1798)
Installed service SMS_SERVER_BOOTSTRAP_PR1SITE.SMS_SITE_COMPONENT_MANAGER 2/9/2014 10:53:23 PM
6040 (0x1798)
Starting service SMS_SERVER_BOOTSTRAP_PR1SITE with command-line arguments "PR1 E:\ConfigMgr /install
E:\ConfigMgr\bin\x64\rolesetup.exe SMSWSUS "... SMS_SITE_COMPONENT_MANAGER 2/9/2014 10:53:23 PM
6040 (0x1798)
```

Once the role installation is started by Site Component Manager, SUPSetup.log is created, and this file contains information about the role installation, as in the following log sample.

**SUPSetup.log:**

```
<02/09/14 22:53:28> =====
<02/09/14 22:53:28> SMSWSUS Setup Started...
<02/09/14 22:53:28> Parameters: E:\ConfigMgr\bin\x64\rolesetup.exe /install /siteserver:PR1SITE SMSWSUS 0
<02/09/14 22:53:28> Installing Pre Reqs for SMSWSUS
<02/09/14 22:53:28>      ===== Installing Pre Reqs for Role SMSWSUS =====
<02/09/14 22:53:28> Found 1 Pre Reqs for Role SMSWSUS
<02/09/14 22:53:28> Pre Req SqlNativeClient found.
<02/09/14 22:53:28> SqlNativeClient already installed (Product Code: {D411E9C9-CE62-4DBF-9D92-4CB22B750ED5}). Would not
install again.
<02/09/14 22:53:28> Pre Req SqlNativeClient is already installed. Skipping it.
<02/09/14 22:53:28>      ===== Completed Installation of Pre Reqs for Role SMSWSUS =====
<02/09/14 22:53:28> Installing the SMSWSUS
<02/09/14 22:53:28> Checking for supported version of WSUS (min WSUS 3.0 SP2 + KB2720211 + KB2734608)
<02/09/14 22:53:28> Checking runtime v2.0.50727...
<02/09/14 22:53:28> Did not find supported version of assembly Microsoft.UpdateServices.Administration.
<02/09/14 22:53:28> Checking runtime v4.0.30319...
<02/09/14 22:53:28> Found supported assembly Microsoft.UpdateServices.Administration version 4.0.0.0, file version
6.2.9200.16384
<02/09/14 22:53:28> Found supported assembly Microsoft.UpdateServices.BaseApi version 4.0.0.0, file version 6.2.9200.16384
<02/09/14 22:53:28> Supported WSUS version found
<02/09/14 22:53:28> Supported WSUS Server version (6.2.9200.16384) is installed.
<02/09/14 22:53:28> CTool::RegisterManagedBinary: run command line:
"C:\Windows\Microsoft.NET\Framework64\v2.0.50727\RegAsm.exe" "E:\ConfigMgr\bin\x64\wsusmsp.dll"
<02/09/14 22:53:44> CTool::RegisterManagedBinary: Registered E:\ConfigMgr\bin\x64\wsusmsp.dll successfully
<02/09/14 22:53:44> Registered DLL E:\ConfigMgr\bin\x64\wsusmsp.dll
<02/09/14 22:53:44> Installation was successful.
<02/09/14 22:53:44> ~RoleSetup().
```

After the role is installed, Site Component Manager removes the bootstrap service that is created to perform the installation, as in the following log sample.

**SiteComp.log:**

```
"E:\ConfigMgr\bin\x64\rolesetup.exe /install /siteserver:PR1SITE.CONTOSO.COM" executed successfully on server
PR1SITE.CONTOSO.COM.      SMS_SITE_COMPONENT_MANAGER      2/9/2014 10:53:46 PM      6040 (0x1798)
  Bootstrap operation successful.      SMS_SITE_COMPONENT_MANAGER      2/9/2014 10:53:46 PM      6040 (0x1798)
  Deinstalled service SMS_SERVER_BOOTSTRAP_PR1SITE.      SMS_SITE_COMPONENT_MANAGER      2/9/2014
10:53:46 PM 6040 (0x1798)
  Bootstrap operations completed.      SMS_SITE_COMPONENT_MANAGER      2/9/2014 10:53:46 PM      6040 (0x1798)
```

## WSUS CONFIGURATION MANAGER

WSUS Configuration Manager connects to the WSUS computer once every hour and configures the WSUS computer with the settings that are defined for the Software Update Point in the Configuration Manager console. WSUS Configuration Manager uses the WSUS APIs to connect to the WSUS computer, and this is why the WSUS Administration Console must be installed on the Configuration Manager Site Server (i.e., the WSUS Administration Console installs the APIs that are used to connect to the WSUS computer). The WSUS Administration Console must also have [KB2734608](#) installed, as this is a prerequisite for the Software Update Point role.

**WCM.log:**

```

Checking for supported version of WSUS (min WSUS 3.0 SP2 + KB2720211 + KB2734608)
SMS_WSUS_CONFIGURATION_MANAGER
Checking runtime v2.0.50727... SMS_WSUS_CONFIGURATION_MANAGER
Did not find supported version of assembly Microsoft.UpdateServices.Administration.
SMS_WSUS_CONFIGURATION_MANAGER
Checking runtime v4.0.30319... SMS_WSUS_CONFIGURATION_MANAGER
Found supported assembly Microsoft.UpdateServices.Administration version 4.0.0.0, file version 6.2.9200.16384
SMS_WSUS_CONFIGURATION_MANAGER
Found supported assembly Microsoft.UpdateServices.BaseApi version 4.0.0.0, file version 6.2.9200.16384
SMS_WSUS_CONFIGURATION_MANAGER
Supported WSUS version found SMS_WSUS_CONFIGURATION_MANAGER

```

If the products or classifications defined for the Software Update Point are modified, SMS Provider makes changes in the appropriate *CI\_* tables in the database. For example, when a product is selected for synchronization, SMS Provider updates rows in the *CI\_CategoryInstances* and *CI\_UpdateCategorySubscription* tables. SMS Database Monitor monitors these tables, and after detecting an update it drops a CSB file in the *WSUSMgr.box* folder, notifying WCM to update the WSUS Server Configuration as follows.

**SMSDBMon.log:**

```

RCV: UPDATE on CI_CategoryInstances for CategoryNotify_iud [177 ][14252] SMS_DATABASE_NOTIFICATION_MONITOR
2/9/2014 6:21:50 PM 3472 (0x0D90)
RCV: UPDATE on CI_UpdateCategorySubscription for SubNotify_iu_WCM [177 ][14253]
SMS_DATABASE_NOTIFICATION_MONITOR 2/9/2014 6:21:50 PM 3472 (0x0D90)
SND: Dropped E:\ConfigMgr\inboxes\objmgr.box\177.CTN [14252] SMS_DATABASE_NOTIFICATION_MONITOR
2/9/2014 6:21:50 PM 3472 (0x0D90)
SND: Dropped E:\ConfigMgr\inboxes\WSUSMgr.box\177.CSB [14253] SMS_DATABASE_NOTIFICATION_MONITOR
2/9/2014 6:21:51 PM 3472 (0x0D90)

```

WCM then wakes up after being notified and connects to the WSUS computer to make sure that it is configured with the options defined in the Configuration Manager console.

**WCM.log:**

```

File notification triggered WCM Inbox. SMS_WSUS_CONFIGURATION_MANAGER
Setting new configuration state to 4 (WSUS_CONFIG_SUBSCRIPTION_PENDING) SMS_WSUS_CONFIGURATION_MANAGER
Attempting connection to WSUS server: CE1SITE.CONTOSO.COM, port: 8530, useSSL: False
SMS_WSUS_CONFIGURATION_MANAGER
Successfully connected to server: CE1SITE.CONTOSO.COM, port: 8530, useSSL: False SMS_WSUS_CONFIGURATION_MANAGER
Subscribed Update Categories <?xml version="1.0" ?>~<Categories>~<Category Id="Product:a105a108-7c9b-4518-bbbe-73f0fe30012b"><![CDATA[Windows Server 2012]]></Category>~<Category Id="Product:fdfe8200-9d98-44ba-a12a-772282bf60ef"><![CDATA[Windows Server 2008 R2]]></Category>~<Category Id="UpdateClassification:0fa1201d-4330-4fa8-8ae9-b877473b6441"><![CDATA[Security Updates]]></Category>~<Category Id="UpdateClassification:28bc880e-0592-4cbf-8f95-c79b17911d5f"><![CDATA[Update Rollups]]></Category>~<Category Id="UpdateClassification:cd5ffd1e-e932-4e3a-bf74-18bf0b1bbd83"><![CDATA[Updates]]></Category>~<Category Id="UpdateClassification:e6cf1350-c01b-414d-a61f-263d14d133b4"><![CDATA[Critical Updates]]></Category>~</Categories> SMS_WSUS_CONFIGURATION_MANAGER
Configuration successful. Will wait for 1 minute for any subscription or proxy changes
SMS_WSUS_CONFIGURATION_MANAGER
Setting new configuration state to 2 (WSUS_CONFIG_SUCCESS) SMS_WSUS_CONFIGURATION_MANAGER

```

Using WSUS APIs to connect to the WSUS computer works by connecting to the *ApiRemoting30* virtual directory on the WSUS website. Therefore, it is important that you specify the correct port configuration when you install the Software Update Point role.

## ON CENTRAL ADMINISTRATION SITE OR STANDALONE PRIMARY SITE

The software updates synchronization process at the top-level site contacts Microsoft Update and retrieves software update metadata that meets the criteria specified in the Software Update Point Component properties. This criteria is specified only at the top-level site. Beginning with System Center 2012 Configuration Manager Service Pack 1 (SP1), at the top-level site you can specify a synchronization source other than Microsoft Update, such as an existing WSUS computer that is not in the Configuration Manager hierarchy.

The synchronization process at the top-level site performs the following steps:

1. [Software updates synchronization starts](#). Synchronization can be initiated either manually or on a schedule.
2. [WSUS Synchronization Manager sends a request to WSUS running on the software update point to start synchronization with Microsoft Update](#).
3. [WSUS synchronizes software updates metadata from Microsoft Update](#). Any changes are inserted or updated in the WSUS database.
4. [WSUS Synchronization Manager synchronizes the software updates metadata](#). This is done from the WSUS database to the Configuration Manager database, and any changes after the last synchronization are inserted or updated in the site database. The software updates metadata is stored in the site database as a configuration item.
5. For a stand-alone Primary site running System Center 2012 Configuration Manager SP1 or R2 only: [WSUS Synchronization Manager sends a request one at a time to WSUS running on other software update points at the site](#).
6. [WSUS Synchronization Manager sends a synchronization request to all child sites](#).
7. [The software updates configuration items are sent to child sites by using database replication](#).

**Software updates synchronization starts.** Synchronization can be initiated either manually or on a schedule.

When synchronization is initiated on a schedule, WSUS Synchronization Manager (**WSyncMgr**) wakes up on the configured schedule and initiates synchronization:

**WSyncMgr.log:**

```
Wakeup for scheduled regular sync      SMS_WSUS_SYNC_MANAGER      1/16/2014 2:25:00 PM
Starting Sync SMS_WSUS_SYNC_MANAGER    1/16/2014 2:25:00 PM
Performing sync on regular schedule    SMS_WSUS_SYNC_MANAGER      1/16/2014 2:25:00 PM
```

When synchronization is initiated manually from the console, WSyncMgr is notified to initiate a sync by executing the **SyncNow** method in the **SMS\_SoftwareUpdate** WMI class. This method updates the Update\_SyncStatus table in the Site database and sets the value of **SyncNow** to SELF. This triggers SMS Database Notification Monitor (SMSDBMON) to place a SELF.SYN file in WSyncMgr.box, and this awakens WSyncMgr and initiates synchronization.

**SMSProv.log:**

```
ExecMethodAsync : SMS_SoftwareUpdate::SyncNow      SMS Provider      1/16/2014 2:19:38 PM      3248 (0x0CB0)
```

**SQL Profiler Trace:**

```
update Update_SyncStatus set SyncNow = 'SELF' where SiteCode = dbo.fnGetSiteCode()
update Update_SyncStatus set SyncNow = null where SiteCode = dbo.fnGetSiteCode()
```

**SMSDBMON.log:**



```
RCV: UPDATE on Update_SyncStatus for SyncNotif_WSyncMgr [SELF ][47788] SMS_DATABASE_NOTIFICATION_MONITOR
1/16/2014 2:19:44 PM
SND: Dropped E:\ConfigMgr\inboxes\WSyncMgr.box\SELF.SYN [47788] SMS_DATABASE_NOTIFICATION_MONITOR
1/16/2014 2:19:44 PM
```

**WSyncMgr.log:**

```
Wakeup by inbox drop SMS_WSUS_SYNC_MANAGER 1/16/2014 2:19:44 PM
Found local sync request file SMS_WSUS_SYNC_MANAGER 1/16/2014 2:19:49 PM
Starting Sync SMS_WSUS_SYNC_MANAGER 1/16/2014 2:19:49 PM
Performing sync on local request SMS_WSUS_SYNC_MANAGER 1/16/2014 2:19:49 PM
```

WSyncMgr then reads the list of Software Update Points (SUPs) from the Site Control File (SCF). WSyncMgr first synchronizes the SUP that was installed as the first SUP in the site and then synchronizes the remaining SUPs. All additional SUPs are configured as replicas of the first SUP.

**WsyncMgr.log:**

```
Read SUPs from SCF for CS1SITE.CONTOSO.COM SMS_WSUS_SYNC_MANAGER 1/16/2014 2:19:49 PM
Found 1 SUPs SMS_WSUS_SYNC_MANAGER 1/16/2014 2:19:49 PM
Found active SUP CS1SITE.CONTOSO.COM from SCF File. SMS_WSUS_SYNC_MANAGER 1/16/2014 2:19:49 PM
```

When synchronization starts (either on schedule or manually), WSyncMgr creates Status Message ID 6701 to indicate that the WSUS synchronization has started.

```
STATMSG: ID=6701 SEV=I LEV=M SOURCE="SMS Server" COMP="SMS_WSUS_SYNC_MANAGER" SYS=<SERVERFQDN> SITE=CS1
PID=432 TID=3404 GMTDATE=Thu Jan 16 18:53:52.608 2014 ISTR0="" ISTR1="" ISTR2="" ISTR3="" ISTR4="" ISTR5="" ISTR6=""
ISTR7="" ISTR8="" ISTR9="" NUMATTRS=0 SMS_WSUS_SYNC_MANAGER 1/16/2014 1:53:52 PM 3404 (0x0D4C)
```

**TIP:**

To manually initiate the sync, you can also create a 0-KB file named SELF.SYN in the WSyncMgr.box directory on the CAS or Standalone Primary Site Server.

**WSUS Synchronization Manager sends a request to WSUS running on the software update point to start synchronization with Microsoft Update.**

The first phase of the synchronization process is to synchronize the WSUS server with Microsoft Update. WSyncMgr instructs the WSUS computer to start a synchronization with Microsoft Update and creates Status Message ID 6704 (WSUS Synchronization in progress. Current phase: Synchronizing WSUS Server).

**WSyncMgr.log:**

```
STATMSG: ID=6704 SEV=I LEV=M SOURCE="SMS Server" COMP="SMS_WSUS_SYNC_MANAGER" SYS=<SERVERFQDN> SITE=CS1
PID=432 TID=3404 GMTDATE=Thu Jan 16 18:53:53.698 2014 ISTR0="" ISTR1="" ISTR2="" ISTR3="" ISTR4="" ISTR5="" ISTR6=""
ISTR7="" ISTR8="" ISTR9="" NUMATTRS=0 SMS_WSUS_SYNC_MANAGER 1/16/2014 1:53:53 PM 3404 (0x0D4C)
Synchronizing WSUS server cs1site.contoso.com ... SMS_WSUS_SYNC_MANAGER 1/16/2014 1:53:53 PM
sync: Starting WSUS synchronization SMS_WSUS_SYNC_MANAGER 1/16/2014 1:53:53 PM
```

**SoftwareDistribution.log:**

```
2014-01-16 18:53:54.231 UTC Change w3wp.58 AdminDataAccess.StartSubscriptionManually Synchronization
manually started
2014-01-16 18:53:56.168 UTC Info WsusService.15 EventLogEventReporter.ReportEvent
EventId=382,Type=Information,Category=Synchronization,Message=A manual synchronization was started.
```

**WSUS synchronizes software update metadata from Microsoft Update.** Any changes are inserted or updated in the WSUS database.

WSUS starts synchronizing with Microsoft Update, and WSyncMgr begins monitoring synchronization progress.

**WSyncMgr.log:**

```
sync: WSUS synchronizing categories SMS_WSUS_SYNC_MANAGER 1/16/2014 1:53:58 PM
sync: WSUS synchronizing updates SMS_WSUS_SYNC_MANAGER 1/16/2014 1:54:00 PM
sync: WSUS synchronizing updates, processed 122 out of 130 items (93%), ETA in 00:00:03 SMS_WSUS_SYNC_MANAGER
1/16/2014 1:55:01 PM
sync: WSUS synchronizing updates, processed 130 out of 130 items (100%) SMS_WSUS_SYNC_MANAGER 1/16/2014
1:55:04 PM
sync: WSUS synchronizing updates, processed 130 out of 130 items (100%) SMS_WSUS_SYNC_MANAGER 1/16/2014
1:55:08 PM
```

The following entries in the log files indicate that WSUS has finished synchronizing with Microsoft Update.

**SoftwareDistribution.log:**

```
2014-01-16 18:55:05.166 UTC Info WsusService.15 EventLogEventReporter.ReportEvent
EventId=384,Type=Information,Category=Synchronization,Message=Synchronization completed successfully.
2014-01-16 18:55:06.307 UTC Info WsusService.31 CatalogSyncAgent.SetSubscriptionStateWithRetry Firing event
SyncFinish...
```

**WSyncMgr.log:**

```
Done synchronizing WSUS Server <SERVERFQDN> SMS_WSUS_SYNC_MANAGER 1/16/2014 1:55:08 PM
Sleeping 2 more minutes for WSUS server sync results to become available SMS_WSUS_SYNC_MANAGER 1/16/2014
1:55:08 PM
Set content version of update source {C2D17964-BBDD-4339-B9F3-12D7205B39CC} for site CS1 to 33
SMS_WSUS_SYNC_MANAGER 1/16/2014 1:57:09 PM
```

**After WSUS has finished synchronization, WSUS Synchronization Manager synchronizes the software updates metadata.** This is done from the WSUS database to the Configuration Manager database, and any changes after the last synchronization are inserted or updated in the site database. The software updates metadata is stored in the site database as a configuration item.

The second phase of the synchronization process is to synchronize the software update metadata from the WSUS database to the Configuration Manager database. At this point, WSyncMgr creates Status Message ID 6705 (WSUS Synchronization in progress. Current phase: Synchronizing site database)

**WSyncMgr.log:**

```
STATMSG: ID=6705 SEV=I LEV=M SOURCE="SMS Server" COMP="SMS_WSUS_SYNC_MANAGER" SYS=<SERVERFQDN> SITE=CS1
PID=432 TID=3404 GMTDATE=Thu Jan 16 18:57:09.156 2014 ISTR0="" ISTR1="" ISTR2="" ISTR3="" ISTR4="" ISTR5="" ISTR6=""
ISTR7="" ISTR8="" ISTR9="" NUMATTRS=0 SMS_WSUS_SYNC_MANAGER 1/16/2014 1:57:09 PM
Synchronizing SMS database with WSUS server <SERVERFQDN> ... SMS_WSUS_SYNC_MANAGER 1/16/2014 1:57:09 PM
```

WSyncMgr reads categories and updates from the WSUS database and inserts or updates the Configuration Manager database. Software Update metadata for each update is stored in the site database as a Configuration Item (CI).

**WSyncMgr.log:**

```
sync: SMS synchronizing categories SMS_WSUS_SYNC_MANAGER 1/16/2014 1:57:09 PM
...<log entries truncated>...
```

```

sync: SMS synchronizing categories, processed 223 out of 223 items (100%) SMS_WSUS_SYNC_MANAGER 1/16/2014
1:57:10 PM
sync: SMS synchronizing updates SMS_WSUS_SYNC_MANAGER 1/16/2014 1:57:10 PM
...<log entries truncated>...
Synchronizing update af5eb87e-cdd6-40bf-984f-5d0630406de8 - Definition Update for Microsoft Endpoint Protection -
KB2461484 (Definition 1.165.1945.0) SMS_WSUS_SYNC_MANAGER 1/16/2014 1:57:12 PM
...<log entries truncated>...
sync: SMS synchronizing updates, processed 5 out of 5 items (100%) SMS_WSUS_SYNC_MANAGER 1/16/2014
1:57:39 PM
...<log entries truncated>...
Done synchronizing SMS with WSUS Server cs1site.contoso.com SMS_WSUS_SYNC_MANAGER 1/16/2014 1:57:46 PM
Set content version of update source {C2D17964-BBDD-4339-B9F3-12D7205B39CC} for site CS1 to 34
SMS_WSUS_SYNC_MANAGER 1/16/2014 1:57:46 PM

```

After synchronization of the site database is complete, if any changes were made to the site database, the content version of the update source is updated in the database. After synchronization finishes successfully, WSyncMgr creates Status Message ID 6702 (WSUS Synchronization done).

```

WSyncMgr.log:
STATMSG: ID=6702 SEV=I LEV=M SOURCE="SMS Server" COMP="SMS_WSUS_SYNC_MANAGER" SYS=<SERVEFRFQDN> SITE=CS1
PID=432 TID=3404 GMTDATE=Thu Jan 16 18:57:46.304 2014 ISTR0="" ISTR1="" ISTR2="" ISTR3="" ISTR4="" ISTR5="" ISTR6=""
ISTR7="" ISTR8="" ISTR9="" NUMATTRS=0 SMS_WSUS_SYNC_MANAGER 1/16/2014 1:57:46 PM
Sync succeeded. Setting sync alert to canceled state on site CS1 SMS_WSUS_SYNC_MANAGER 1/16/2014 1:57:46 PM
Updated 130 items in SMS database, new update source content version is 34 SMS_WSUS_SYNC_MANAGER
1/16/2014 1:57:46 PM
Sync time: 0d00h03m53s SMS_WSUS_SYNC_MANAGER 1/16/2014 1:57:46 PM

```

**For a stand-alone Primary site running System Center 2012 Configuration Manager SP1 or System Center 2012 R2 Configuration Manager only: WSUS Synchronization Manager sends requests one at a time to the WSUS component running on other Software Update Points on the site.**

The WSUS computers on the other Software Update Points are configured as replicas of the WSUS installation running on the default Software Update Point for the site.

```

WSyncMgr.log:
Synchronizing replica WSUS servers SMS_WSUS_SYNC_MANAGER
STATMSG: ID=6706 SEV=I LEV=M SOURCE="SMS Server" COMP="SMS_WSUS_SYNC_MANAGER" SYS=PS1SITE.CONTOSO.COM
SITE=PS1 PID=1840 TID=2832 GMTDATE=Thu Jan 16 19:17:13.575 2014 ISTR0="" ISTR1="" ISTR2="" ISTR3="" ISTR4="" ISTR5=""
ISTR6="" ISTR7="" ISTR8="" ISTR9="" NUMATTRS=0 SMS_WSUS_SYNC_MANAGER
Synchronizing WSUS server ps1sys.contoso.com ... SMS_WSUS_SYNC_MANAGER
sync: Starting Replica WSUS synchronization SMS_WSUS_SYNC_MANAGER
sync: Replica WSUS synchronizing other items SMS_WSUS_SYNC_MANAGER
sync: Replica WSUS synchronizing other items, processed 4 out of 4 items (100%) SMS_WSUS_SYNC_MANAGER
Done synchronizing WSUS Server ps1sys.contoso.com SMS_WSUS_SYNC_MANAGER

```

**WSUS Synchronization Manager sends a synchronization request to all child sites.**

Sync notifications are sent to all child sites to instruct them to start synchronization. These notifications are sent via file replication and not database replication.

```

WSyncMgr.log:
Sending sync notification to child site(s): PS1, PS2 SMS_WSUS_SYNC_MANAGER

```

SQL Replication type has not been set for E:\ConfigMgr\inboxes\WSyncMgr.box\outbox\CS1.SYN, replicating to (PS1, PS2),  
inbox: E:\ConfigMgr\inboxes\replmgr.box SMS\_WSUS\_SYNC\_MANAGER

## The software updates configuration items are sent to child sites by using database replication.

### ON CHILD PRIMARY SITE AND SECONDARY SITES

During the software update synchronization process on the top-level site, the software update configuration items are replicated to child sites by using database replication. At the end of the process, the top-level site sends a synchronization request to the child site, and the child site then starts the WSUS synchronization process. Because the software update metadata (Configuration Items) from the Site Database is replicated to the Primary sites via database replication, the synchronization process on the Child Primary and Secondary sites consists of only the WSUS synchronization phase.

The synchronization process on a child primary site or secondary site performs the following steps:

1. [WSUS Synchronization Manager receives a synchronization request from the top-level site.](#)
2. [Software updates synchronization starts.](#)
3. [WSUS Synchronization Manager makes a request to WSUS running on the first software update point to start synchronization.](#)
4. [WSUS running on the Software Update Point on the child site synchronizes software updates metadata from WSUS running on the Software Update Point on the parent site.](#)
5. For Configuration Manager with no service pack only: [When there is a remote Internet-based software update point, WSUS Synchronization Manager starts the synchronization process for WSUS running on the remote site system.](#)
6. For System Center 2012 Configuration Manager SP1 and System Center 2012 R2 Configuration Manager only: [WSUS Synchronization Manager sends a request one at a time to WSUS running on other software update points \(including Internet facing SUPs\) at the site.](#)
7. [When synchronization has finished successfully, WSUS Synchronization Manager creates status message 6702.](#)
8. [From a primary site, WSUS Synchronization Manager sends a synchronization request to any child secondary sites.](#)  
The secondary site starts the software updates synchronization with the parent primary site. The secondary site's SUP is configured as a replica of WSUS running on the parent site.

### WSUS Synchronization Manager receives a synchronization request from the top-level site.

When the sync notification that's sent by the parent site arrives in the \WSyncMgr.box folder via file replication, WSyncMgr wakes up and starts synchronization.

#### WSyncMgr.log:

```
Wakeup by inbox drop      SMS_WSUS_SYNC_MANAGER    1/16/2014 1:58:32 PM    2832 (0x0B10)
Found parent sync notification file CS1.SYN.  SMS_WSUS_SYNC_MANAGER    1/16/2014 1:58:37 PM    2832 (0x0B10)
Starting Sync SMS_WSUS_SYNC_MANAGER    1/16/2014 1:58:37 PM    2832 (0x0B10)
Performing sync on parent request  SMS_WSUS_SYNC_MANAGER    1/16/2014 1:58:37 PM    2832 (0x0B10)
```

WSyncMgr then reads the list of Software Update Points from the Site Control File (SCF). WSyncMgr will first synchronize the SUP that was installed as the first SUP in the site and then synchronize all remaining SUPs. All additional SUPs are configured as replicas of the first SUP.

#### WSyncMgr.log:

```
Read SUPs from SCF for PS1SITE.CONTOSO.COM SMS_WSUS_SYNC_MANAGER    1/16/2014 1:58:37 PM
Found 2 SUPs      SMS_WSUS_SYNC_MANAGER    1/16/2014 1:58:37 PM
```

Found active SUP PS1SITE.CONTOSO.COM from SCF File.	SMS_WSUS_SYNC_MANAGER	1/16/2014 1:58:37 PM
Found active SUP PS1SYS.CONTOSO.COM from SCF File.	SMS_WSUS_SYNC_MANAGER	1/16/2014 1:58:37 PM

### Software updates synchronization begins.

```

WSyncMgr.log:
STATMSG: ID=6701 SEV=I LEV=M SOURCE="SMS Server" COMP="SMS_WSUS_SYNC_MANAGER" SYS=PS1SITE.CONTOSO.COM
SITE=PS1 PID=1840 TID=2832 GMTDATE=Thu Jan 16 18:58:37.599 2014 ISTR0="" ISTR1="" ISTR2="" ISTR3="" ISTR4="" ISTR5=""
ISTR6="" ISTR7="" ISTR8="" ISTR9="" NUMATTRS=0      SMS_WSUS_SYNC_MANAGER      1/16/2014 1:58:37 PM      2832
(0x0B10)
Synchronizing WSUS server PS1SITE.CONTOSO.COM      SMS_WSUS_SYNC_MANAGER      1/16/2014 1:58:38 PM      2832
(0x0B10)

```

### WSUS Synchronization Manager makes a request to WSUS running on the first Software Update Point to start synchronization.

```

WSyncMgr.log:
STATMSG: ID=6704 SEV=I LEV=M SOURCE="SMS Server" COMP="SMS_WSUS_SYNC_MANAGER" SYS=PS1SITE.CONTOSO.COM
SITE=PS1 PID=1840 TID=2832 GMTDATE=Thu Jan 16 18:58:38.909 2014 ISTR0="" ISTR1="" ISTR2="" ISTR3="" ISTR4="" ISTR5=""
ISTR6="" ISTR7="" ISTR8="" ISTR9="" NUMATTRS=0      SMS_WSUS_SYNC_MANAGER      1/16/2014 1:58:38 PM      2832
(0x0B10)
Synchronizing WSUS server ps1site.contoso.com ...  SMS_WSUS_SYNC_MANAGER      1/16/2014 1:58:39 PM      3412
(0x0D54)

```

### WSUS running on the Software Update Point on the child site synchronizes software updates metadata from WSUS running on the Software Update Point on the parent site.

```

WSyncMgr.log:
sync: Starting WSUS synchronization      SMS_WSUS_SYNC_MANAGER      1/16/2014 1:58:39 PM      3412 (0x0D54)
sync: WSUS synchronizing categories      SMS_WSUS_SYNC_MANAGER      1/16/2014 1:58:46 PM      3412 (0x0D54)
sync: WSUS synchronizing updates        SMS_WSUS_SYNC_MANAGER      1/16/2014 1:58:47 PM      3412 (0x0D54)
sync: WSUS synchronizing updates, processed 130 out of 130 items (100%) SMS_WSUS_SYNC_MANAGER      1/16/2014
1:59:05 PM      3412 (0x0D54)
Done synchronizing WSUS Server ps1site.contoso.com  SMS_WSUS_SYNC_MANAGER      1/16/2014 1:59:05 PM      3412
(0x0D54)
Sleeping 2 more minutes for WSUS server sync results to become available SMS_WSUS_SYNC_MANAGER      1/16/2014
1:59:05 PM      3412 (0x0D54)
Set content version of update source {C2D17964-BBDD-4339-B9F3-12D7205B39CC} for site PS1 to 34
SMS_WSUS_SYNC_MANAGER      1/16/2014 2:01:05 PM      2832 (0x0B10)

```

### For Configuration Manager with no service pack only:

When there is a remote Internet-based Software Update Point, WSUS Synchronization Manager starts the synchronization process for WSUS running on the remote site system.

### For System Center 2012 Configuration Manager SP1 and System Center 2012 R2 Configuration Manager only:

WSUS Synchronization Manager sends requests one at a time to WSUS running on other Software Update Points (including Internet-facing SUPs) at the site. The WSUS servers on the other Software Update Points are configured as replicas of WSUS running on the default Software Update Point at the site. WSyncMgr then creates Status Message ID

6706 (WSUS Synchronization in progress. Current phase: Synchronizing Internet-facing WSUS server). Even though the SUP may not be Internet-facing, the Status Message will still be 6706.

**WsyncMgr.log:**

```
Synchronizing replica WSUS servers      SMS_WSUS_SYNC_MANAGER
STATMSG: ID=6706 SEV=I LEV=M SOURCE="SMS Server" COMP="SMS_WSUS_SYNC_MANAGER" SYS=PS1SITE.CONTOSO.COM
SITE=PS1 PID=1840 TID=2832 GMTDATE=Thu Jan 16 19:17:13.575 2014 ISTR0="" ISTR1="" ISTR2="" ISTR3="" ISTR4="" ISTR5=""
ISTR6="" ISTR7="" ISTR8="" ISTR9="" NUMATTRS=0      SMS_WSUS_SYNC_MANAGER
Synchronizing WSUS server ps1sys.contoso.com ...      SMS_WSUS_SYNC_MANAGER
sync: Starting Replica WSUS synchronization      SMS_WSUS_SYNC_MANAGER
sync: Replica WSUS synchronizing other items      SMS_WSUS_SYNC_MANAGER
sync: Replica WSUS synchronizing other items, processed 4 out of 4 items (100%)      SMS_WSUS_SYNC_MANAGER
Done synchronizing WSUS Server ps1sys.contoso.com      SMS_WSUS_SYNC_MANAGER
```

**When synchronization has finished successfully, WSUS Synchronization Manager creates status message 6702.**

**WSyncMgr.log:**

```
STATMSG: ID=6702 SEV=I LEV=M SOURCE="SMS Server" COMP="SMS_WSUS_SYNC_MANAGER" SYS=PS1SITE.CONTOSO.COM
SITE=PS1 PID=1840 TID=2832 GMTDATE=Thu Jan 16 19:01:35.117 2014 ISTR0="" ISTR1="" ISTR2="" ISTR3="" ISTR4="" ISTR5=""
ISTR6="" ISTR7="" ISTR8="" ISTR9="" NUMATTRS=0      SMS_WSUS_SYNC_MANAGER      1/16/2014 2:01:35 PM      2832
(0x0B10)
Sync succeeded. Setting sync alert to canceled state on site PS1      SMS_WSUS_SYNC_MANAGER      1/16/2014 2:01:35 PM
2832 (0x0B10)
Successfully synced site with parent CS1, version 34      SMS_WSUS_SYNC_MANAGER      1/16/2014 2:01:35 PM      2832
(0x0B10)
Sync time: 0d00h02m57s      SMS_WSUS_SYNC_MANAGER      1/16/2014 2:01:35 PM      2832 (0x0B10)
```

**From a primary site, WSUS Synchronization Manager sends a synchronization request to any child secondary sites. The secondary site starts the software updates synchronization with the parent primary site. The secondary site's SUP is configured as a replica of WSUS running on the parent site.**

**WSyncMgr.log:**

```
Sending sync notification to child site(s): SS1      SMS_WSUS_SYNC_MANAGER
```

## COMPLIANCE

Before you can deploy software updates to clients, the clients must run a Software Update scan. We recommend that you allow enough time for clients to complete a Software Update scan and report compliance results so that you can review the compliance results and deploy only the updates that are required on the clients.

When the Software Update Point is installed and synchronized, a site-wide machine policy is created that informs client computers that Configuration Manager Software Updates was enabled for the site. When a client receives the machine policy, a compliance assessment scan is scheduled to start randomly within the next two hours. When the scan is started, a Software Updates Client Agent process clears the scan history, submits a request to find the WSUS server that should be used for the scan, and updates the local Group Policy with the WSUS location.

For an overview of the Compliance assessment process, see the following TechNet website:

[http://technet.microsoft.com/en-us/library/gg682168.aspx#BKMK\\_SUMCompliance](http://technet.microsoft.com/en-us/library/gg682168.aspx#BKMK_SUMCompliance)

Before a client can try to scan for updates, it needs the Update Source policy. This policy is created on the Site Server after a successful synchronization of the Software Update Point. This section discusses how this policy is created by the following process:

1. [After successful sync, WSyncMgr updates the Content Version and Last Sync Time in the database.](#)
2. [SMSDBMON gets triggered and drops an .STN file in Policypv.box.](#)
3. [Policy Provider creates or updates the UpdateSource Policy in the database.](#)
4. [Policy is downloaded and evaluated on the client during the next Policy Evaluation cycle.](#)
5. [Scan Agent is notified that the UpdateSource Policy is updated.](#)

#### **After successful sync, WSyncMgr updates the Content Version and Last Sync Time in the database.**

After a successful synchronization on a Primary Site, WSyncMgr updates *Last Sync Time* and *Content Version* in the database for the Software Update Point. This is done by executing the *spProcessSUMSyncStateMessage* stored procedure. In the example below, this stored procedure is being executed to update the content version to 36.

#### **SQL Profiler:**

```
declare @Error int; exec spProcessSUMSyncStateMessage N'2014-01-17 17:59:54', N'PS1', N'{C2D17964-BBDD-4339-B9F3-12D7205B39CC}', 1, 0, '36', @Error output, N'PS1SITE.CONTOSO.COM'
```

#### **SMSDBMON gets triggered and drops a .STN file in policypv.box.**

*spProcessSUMSyncStateMessage* updates the *Update\_SyncStatus* table with the new *Content Version* and *Sync Time*. This insertion/update to the *Update\_SyncStatus* table triggers SMSDBMON to drop a <UpdateSource\_UniqueID>.STN file (STN stands for Scan Tool Notification) in policypv.box to indicate a change in the scan tool definition.

#### **SMSDBMON.log:**

```
RCV: UPDATE on Update_SyncStatus for UpdSyncStatus_iu [{C2D17964-BBDD-4339-B9F3-12D7205B39CC} ] [46680]
      SMS_DATABASE_NOTIFICATION_MONITOR 1/17/2014 1:00:00 PM 2944 (0x0B80)
SND: Dropped E:\ConfigMgr\inboxes\policypv.box\{C2D17964-BBDD-4339-B9F3-12D7205B39CC}.STN (non-zero) [46680]
      SMS_DATABASE_NOTIFICATION_MONITOR 1/17/2014 1:00:00 PM 2944 (0x0B80)
```

#### **Policy Provider creates or updates the UpdateSource Policy in the database.**

The <UpdateSource\_UniqueID>.STN file notifies Policy Provider that it should wake up and update the UpdateSource policy in the database.

#### **PolicyPv.log:**

```
Found {C2D17964-BBDD-4339-B9F3-12D7205B39CC}.STN SMS_POLICY_PROVIDER 1/17/2014 1:00:05 PM 2372 (0x0944)
Added Scan Tool ID {C2D17964-BBDD-4339-B9F3-12D7205B39CC} SMS_POLICY_PROVIDER 1/17/2014 1:00:05 PM 2372
(0x0944)
Adding to delete list: E:\ConfigMgr\inboxes\policypv.box\{C2D17964-BBDD-4339-B9F3-12D7205B39CC}.STN
SMS_POLICY_PROVIDER 1/17/2014 1:00:05 PM 2372 (0x0944)
```

#### **SQL Profiler Trace:**

```
select PolicyID, PolicyAssignmentID, SourceCRC, PADBID from SettingsPolicy where SourceID = N'PS1' and SourceType = N'UpdateSource'
```

```
select Version from Policy where PolicyID = N'{d0855677-b0a6-4e33-9bd5-7b0d06f0a2be}'
```

```
IF EXISTS (select PolicyID from Policy where PolicyID = N'{d0855677-b0a6-4e33-9bd5-7b0d06f0a2be}') update Policy set Version = N'40.00' where PolicyID = N'{d0855677-b0a6-4e33-9bd5-7b0d06f0a2be}' ELSE insert Policy (PolicyID, Version) values (N'{d0855677-b0a6-4e33-9bd5-7b0d06f0a2be}', N'40.00')
```

```
exec sp_describe_undeclared_parameters N'UPDATE Policy SET Body = @P1 where PolicyID = N'{d0855677-b0a6-4e33-9bd5-7b0d06f0a2be}'
```

```
IF EXISTS (select PADBID from PolicyAssignment where PADBID = 16777218) update PolicyAssignment set Version = N'40.00', InProcess = 1, BodyHash = null where PADBID = 16777218 ELSE insert PolicyAssignment (PolicyAssignmentID, PADBID, Version, PolicyID) values (N'{375c8020-3cae-4736-89ca-ccf1ce6e3709}', 16777218, N'40.00', N'{d0855677-b0a6-4e33-9bd5-7b0d06f0a2be}')
```

```
exec sp_describe_undeclared_parameters N'UPDATE PolicyAssignment SET Body = @P1 where PADBID = 16777218'
```

```
update PolicyAssignment set InProcess = 0, BodySignature = N'<BodySignatureTruncated', TombstoneBodySignature = N'<TombstoneBodySignatureTruncated>', HashAlgOID = N'1.2.840.113549.1.1.11', HashAlgId = 32780, BodyHash = N'<BodyHashTruncated', TombstoneBodyHash = N'<TombstoneBodyHashTruncated' where PADBID = 16777218
```

**TIP:**

To see this policy in the database, run the following query:

```
SELECT CONVERT(XML, Body, 1), * FROM Policy WHERE PolicyID = (SELECT PolicyID FROM SettingsPolicy WHERE SourceType = 'UpdateSource')
```

This policy contains the content version of the update server which is used to find the location of the WSUS computer that the client can scan against. After this policy is created or updated in the database, the clients get the new or updated Update Source policy during the next policy evaluation cycle.

**Policy is downloaded and evaluated on the client.**

**PolicyAgent.log on Client:**

```
Successfully initiated download of policy 'CCM_Policy_Policy5.PolicyID="{d0855677-b0a6-4e33-9bd5-7b0d06f0a2be}",PolicySource="SMS:PS1",PolicyVersion="40.00" PolicyAgent_ReplyAssignments 1/17/2014 1:57:39 PM  
Policy 'CCM_Policy_Policy5.PolicyID="{d0855677-b0a6-4e33-9bd5-7b0d06f0a2be}",PolicyVersion="40.00",PolicySource="SMS:PS1"  
successfully compiled PolicyAgent_PolicyDownload 1/17/2014 1:57:41 PM
```

**PolicyEvaluator.log on Client:**

```
Updating policy CCM_Policy_Policy5.PolicyID="{d0855677-b0a6-4e33-9bd5-7b0d06f0a2be}",PolicySource="SMS:PS1",PolicyVersion="40.00" PolicyAgent_PolicyEvaluator  
Applied policy CCM_Policy_Policy5.PolicyID="{d0855677-b0a6-4e33-9bd5-7b0d06f0a2be}",PolicySource="SMS:PS1",PolicyVersion="40.00" PolicyAgent_PolicyEvaluator  
Policy state for [CCM_Policy_Policy5.PolicyID="{d0855677-b0a6-4e33-9bd5-7b0d06f0a2be}",PolicyVersion="40.00",PolicySource="SMS:PS1"] is currently [Active] PolicyAgent_PolicyEvaluator
```

To find the PolicyID of the Update Source policy on a client, run the following WQL query:

**Namespace:** *ROOT\ccm\Policy\Machine\RequestedConfig*

**Query:** *SELECT \* FROM CCM\_Policy\_Policy5 WHERE PolicyCategory = 'UpdateSource'*



Once this policy is compiled on the client, the Update Source information is stored in the following WMI Class:

**Namespace:** ROOT\ccm\Policy\Machine\ActualConfig

**Class:** CCM\_UpdateSource

**TIP:**

If you compare the instance of CCM\_UpdateSource class on the client with the XML Body retrieved from the Policy table, you will notice that the content of the XML looks identical to the instance.

**Scan Agent is notified that the UpdateSource policy is updated.**

**ScanAgent.log on Client:**

```
Inside CScanAgent::Notify()      ScanAgent      1/17/2014 1:57:42 PM      2996 (0x0BB4)
CScanAgent::OnPolicyChange- Policy __InstanceModificationEvent notification received ScanAgent      1/17/2014 1:57:42 PM
2996 (0x0BB4)
```

---

## WSUS SERVER LOCATION

After the client receives the Update Source policy, it is now ready to run a scan for Software Updates Compliance. At this point, the client locate the WSUS computer with the content version specified in the policy. This process is very similar to the way client finds the location of a Distribution Point for a specific package and version.

1. [Scan Agent creates a scan request based on the available policy.](#)
2. [Scan Agent sends a request for the WSUS location to Location Services.](#)
3. [Location Services sends the location request to the management point.](#)
4. [CCM Messaging sends the location request message to the management point.](#)
5. [The management point parses the request, gets the WSUS location from the database, and sends a response back.](#)
6. [CCM Messaging receives the response and sends it back to Location Services.](#)
7. [Location Services parses the response and sends the location back to Scan Agent.](#)
8. [Scan Agent notifies WUAHandler to add the Update Source to registry.](#)
9. [Scan Agent initiates the scan.](#)

**Scan Agent creates a scan request based on the available policy.**

**ScanAgent.log:**

```
CScanAgent::ScanByUpdates- Policy available for UpdateSourceID={C2D17964-BBDD-4339-B9F3-12D7205B39CC} ContentVersion=38
ScanAgent      1/20/2014 11:59:52 AM
CScanAgent::ScanByUpdates- Added Policy to final ScanRequest List UpdateSourceID={C2D17964-BBDD-4339-B9F3-12D7205B39CC},
Policy-ContentVersion=38, Required-ContentVersion=38      ScanAgent      1/20/2014 11:59:56 AM
```

**Scan Agent sends a request for the WSUS location to Location Services.**

Scan Agent now requests the WSUS location from Location Services and waits for a response. In this example, the Location Request ID is {C2BB9710-C548-49D0-9DF8-5F9CFC5F3862}.

**ScanAgent.log:**

```

Inside CScanAgent::ProcessScanRequest() ScanAgent 1/20/2014 12:18:09 PM
CScanJobManager::Scan- entered ScanAgent 1/20/2014 12:18:09 PM
ScanJob({4CD06388-D509-46E4-8C00-75909EDD9EE8}): CScanJob::Initialize- entered ScanAgent 1/20/2014 12:18:09 PM
ScanJob({4CD06388-D509-46E4-8C00-75909EDD9EE8}): CScanJob::Scan- entered ScanAgent 1/20/2014 12:18:09 PM
ScanJob({4CD06388-D509-46E4-8C00-75909EDD9EE8}): CScanJob::RequestLocations- entered ScanAgent 1/20/2014
12:18:09 PM
-----Requesting WSUS Server Locations from LS for {C2D17964-BBDD-4339-B9F3-12D7205B39CC} version 38 ScanAgent
1/20/2014 12:18:09 PM
-----Location Request ID = {C2BB9710-C548-49D0-9DF8-5F9CFC5F3862} ScanAgent 1/20/2014 12:18:09 PM
CScanAgentCache::PersistInstanceInCache- Persisted Instance CCM_ScanJobInstance ScanAgent 1/20/2014 12:18:09 PM
ScanJob({4CD06388-D509-46E4-8C00-75909EDD9EE8}): -----Locations requested for ScanJobID={4CD06388-D509-46E4-8C00-
75909EDD9EE8} (LocationRequestID={C2BB9710-C548-49D0-9DF8-5F9CFC5F3862}), will process the scan request once locations are
available. ScanAgent 1/20/2014 12:18:09 PM

```

Each scan job is stored in WMI in the *CCM\_ScanJobInstance* class:

**Namespace:** root\CCM\ScanAgent

**Class:** CCM\_ScanJobInstance

**Location Services sends the location request to the management point.**

Location Services creates a Location Request and sends it to the management point. The package ID for a WSUS location request is the Update Source Unique ID.

**LocationServices.log:**

```

CCCMWSUSLocation::GetLocationsAsyncEx LocationServices 1/20/2014 12:18:09 PM
Attempting to persist WSUS location request for ContentID='{C2D17964-BBDD-4339-B9F3-12D7205B39CC}' and ContentVersion='38'
LocationServices 1/20/2014 12:18:09 PM
Persisted WSUS location request LocationServices 1/20/2014 12:18:09 PM 1596 (0x063C)
Attempting to send WSUS Location Request for ContentID='{C2D17964-BBDD-4339-B9F3-12D7205B39CC}'LocationServices
1/20/2014 12:18:09 PM
WSUSLocationRequest : <WSUSLocationRequest SchemaVersion="1.00"><Content ID="{C2D17964-BBDD-4339-B9F3-
12D7205B39CC}" Version="38"/><AssignedSite SiteCode="PS1"/><ClientLocationInfo OnInternet="0"><ADSite Name="CM12-R2-
PS1"/><Forest Name="CONTOSO.COM"/><Domain Name="CONTOSO.COM"/><IPAddresses><IPAddress
SubnetAddress="192.168.2.0" Address="192.168.2.62"/></IPAddresses></ClientLocationInfo></WSUSLocationRequest>
LocationServices 1/20/2014 12:18:09 PM
Created and Sent Location Request '{C2BB9710-C548-49D0-9DF8-5F9CFC5F3862}' for package {C2D17964-BBDD-4339-B9F3-
12D7205B39CC} LocationServices 1/20/2014 12:18:09 PM

```

**CCM Messaging sends the location request message to the management point.**

**CcmMessaging.log:**

```

Sending async message '{76453CC6-76BA-4B68-BE30-BA70754570BB}' to outgoing queue 'mp:[http]mp_locationmanager'
CcmMessaging 1/20/2014 12:18:09 PM 1596 (0x063C)
Sending outgoing message '{76453CC6-76BA-4B68-BE30-BA70754570BB}'. Flags 0x200, sender account empty CcmMessaging
1/20/2014 12:18:09 PM 2520 (0x09D8)

```

**The management point parses the request, obtains the WSUS location from the database, and sends a response.**

The management point parses this request and calls the *MP\_GetWSUSServerLocations* stored procedure to get the WSUS locations from the database:

**MP\_Location.log:**

```
MP LM: Message Body : <WSUSLocationRequest SchemaVersion="1.00"><Content ID="{C2D17964-BBDD-4339-B9F3-12D7205B39CC}" Version="38"/><AssignedSite SiteCode="PS1"/><ClientLocationInfo OnInternet="0"><ADSite Name="CM12-R2-PS1"/><Forest Name="CONTOSO.COM"/><Domain Name="CONTOSO.COM"/><IPAddresses><IPAddress SubnetAddress="192.168.2.0" Address="192.168.2.62"/></IPAddresses></ClientLocationInfo></WSUSLocationRequest>
MP_LocationManager 1/20/2014 12:18:09 PM 548 (0x0224)
MP LM: calling MP_GetWSUSServerLocations MP_LocationManager 1/20/2014 12:18:09 PM 548 (0x0224)
```

#### SQL Profiler:

```
exec MP_GetMPSitesFromAssignedSite N'PS1'
exec MP_GetSiteInfoUnified N'<ClientLocationInfo OnInternet="0"><ADSite Name="CM12-R2-PS1"/><Forest Name="CONTOSO.COM"/><Domain Name="CONTOSO.COM"/><IPAddresses><IPAddress SubnetAddress="192.168.2.0" Address="192.168.2.62"/></IPAddresses></ClientLocationInfo>'
exec MP_GetWSUSServerLocations N'{C2D17964-BBDD-4339-B9F3-12D7205B39CC}',N'38',N'PS1',N'PS1',N'0',N'CONTOSO.COM'
```

After getting the results from the stored procedure, the management point sends a response to the client.

#### MP\_Location.log:

```
MP LM: Reply message body:
<WSUSLocationReply SchemaVersion="1.00"><Sites><Site><MPSite SiteCode="PS1"/><LocationRecords><LocationRecord WSUSURL="http://PS1SITE.CONTOSO.COM:8530" ServerName="PS1SITE.CONTOSO.COM" Version="38"/><LocationRecord WSUSURL="https://PS1SYS.CONTOSO.COM:8531" ServerName="PS1SYS.CONTOSO.COM" Version="38"/></LocationRecords></Site></Sites></WSUSLocationReply>
MP_LocationManager 1/20/2014 12:18:09 PM
```

#### CCM Messaging receives the response and sends it back to Location Services.

The CcmMessaging.log file on the client shows that a reply was received. This message was delivered to Location Services.

#### CcmMessaging.log:

```
Message '{76453CC6-76BA-4B68-BE30-BA70754570BB}' got reply '{8E6D05EF-B77F-4AD0-AF64-1C6F3069A29C}' to local endpoint queue 'LS_ReplyLocations' CcmMessaging 1/20/2014 12:18:09 PM 2520 (0x09D8)
OutgoingMessage(Queue='mp_[http]mp_locationmanager', ID='{76453CC6-76BA-4B68-BE30-BA70754570BB}'): Delivered successfully to host 'PS1SYS.CONTOSO.COM'. CcmMessaging 1/20/2014 12:18:09 PM 2520 (0x09D8)
Message '{8E6D05EF-B77F-4AD0-AF64-1C6F3069A29C}' delivered to endpoint 'LS_ReplyLocations' CcmMessaging 1/20/2014 12:18:09 PM 3680 (0x0E60)
```

#### Location Services parses the response and sends the location back to Scan Agent.

#### LocationServices.log:

```
Processing Location reply message LocationServices 1/20/2014 12:18:09 PM
WSUSLocationReply : <WSUSLocationReply SchemaVersion="1.00"><Sites><Site><MPSite SiteCode="PS1"/><LocationRecords><LocationRecord WSUSURL="http://PS1SITE.CONTOSO.COM:8530" ServerName="PS1SITE.CONTOSO.COM" Version="38"/><LocationRecord WSUSURL="https://PS1SYS.CONTOSO.COM:8531" ServerName="PS1SYS.CONTOSO.COM" Version="38"/></LocationRecords></Site></Sites></WSUSLocationReply> LocationServices 1/20/2014 12:18:09 PM
Calling back with the following WSUS locations LocationServices 1/20/2014 12:18:09 PM 3680 (0x0E60)
WSUS Path='http://PS1SITE.CONTOSO.COM:8530', Server='PS1SITE.CONTOSO.COM', Version='38' LocationServices 1/20/2014 12:18:09 PM
WSUS Path='https://PS1SYS.CONTOSO.COM:8531', Server='PS1SYS.CONTOSO.COM', Version='38' LocationServices 1/20/2014 12:18:09 PM
Calling back with locations for WSUS request {C2BB9710-C548-49D0-9DF8-5F9CFC5F3862} LocationServices 1/20/2014 12:18:09 PM
```

## Scan Agent notifies WUAHandler to add the Update Source to the registry.

Scan Agent now has the policy and the update source location with the appropriate content version. Scan Agent notifies WUAHandler to add the update source. WUAHandler adds the update source to the registry and initiates a Group Policy refresh (if the client is in domain) to see whether Group Policy overrides the update server that we just added.

### ScanAgent.log:

```
*****WSUSLocationUpdate received for location request guid={C2BB9710-C548-49D0-9DF8-5F9CFC5F3862} ScanAgent
1/20/2014 12:18:09 PM
ScanJob({4CD06388-D509-46E4-8C00-75909EDD9EE8}): CScanJob::OnLocationUpdate- Received
Location=http://PS1SITE.CONTOSO.COM:8530, Version=38 ScanAgent 1/20/2014 12:18:09 PM
ScanJob({4CD06388-D509-46E4-8C00-75909EDD9EE8}): CScanJob::Execute- Adding UpdateSource={C2D17964-BBDD-4339-B9F3-12D7205B39CC}, ContentType=2, ContentLocation=http://PS1SITE.CONTOSO.COM:8530, ContentVersion=38 ScanAgent
1/20/2014 12:18:09 PM
```

### WUAHandler.log on a New Client showing new Update Source being added:

```
Its a WSUS Update Source type ({C2D17964-BBDD-4339-B9F3-12D7205B39CC}), adding it. WUAHandler 1/20/2014
12:18:09 PM
Its a completely new WSUS Update Source. WUAHandler 1/20/2014 12:18:09 PM 1800 (0x0708)
Enabling WUA Managed server policy to use server: http://PS1SITE.CONTOSO.COM:8530 WUAHandler 1/20/2014
12:18:09 PM
Policy refresh forced. WUAHandler 1/20/2014 12:18:09 PM
Waiting for 2 mins for Group Policy to notify of WUA policy change... WUAHandler 1/20/2014 12:18:09 PM
Waiting for 30 secs for policy to take effect on WU Agent. WUAHandler 1/20/2014 12:18:11 PM
Added Update Source ({C2D17964-BBDD-4339-B9F3-12D7205B39CC}) of content type: 2 WUAHandler 1/20/2014 12:18:41 PM
```

### WindowsUpdate.log:

```
2014-01-20 12:18:11:520 968 9d0 Agent * WSUS server: http://PS1SITE.CONTOSO.COM:8530 (Changed)
2014-01-20 12:18:11:520 968 9d0 Agent * WSUS status server: http://PS1SITE.CONTOSO.COM:8530 (Changed)
2014-01-20 12:18:11:520 968 9d0 AU Sus server changed through policy.
```

### WUAHandler.log on existing client showing content version getting incremented:

```
Its a WSUS Update Source type ({C2D17964-BBDD-4339-B9F3-12D7205B39CC}), adding it. WUAHandler
WSUS update source already exists, it has increased version to 38. WUAHandler
```

## Scan Agent initiates the scan.

After the update source is successfully added, Scan Agent raises a State Message and initiates the scan.

### ScanAgent.log:

```
ScanJob({4CD06388-D509-46E4-8C00-75909EDD9EE8}): Raised UpdateSource ({C2D17964-BBDD-4339-B9F3-12D7205B39CC}) state
message successfully. StateId = 2 ScanAgent 1/20/2014 12:18:42 PM
ScanJob({4CD06388-D509-46E4-8C00-75909EDD9EE8}): CScanJob::Execute - successfully requested Scan, ScanType=1
ScanAgent 1/20/2014 12:18:42 PM
```

After the Update Source policy and the Update Source location is available, Scan Agent initiates the scan. Software Update Scan is actually performed by the Windows Update Agent. However, the Configuration Manager client interacts with the Windows Update Agent to perform a scan and obtain the scan results. This interaction is handled by the Windows Update Agent Handler (WUAHandler) component, which communicates with the Windows Update Agent.

1. [Scan Agent requests the scan, and WUAHandler initiates the scan.](#)
2. [Windows Update Agent \(WUA\) starts the scan against WSUS Server.](#)
3. [WUAHandler receives results from Windows Update Agent.](#)
4. [WUAHandler parses the scan results.](#)
5. [Update Store records the status and raises a State Message for each update in WMI.](#)
6. [State Messages are sent to the management point.](#)

### Scan Agent requests the scan and WUAHandler initiates the scan.

Scan Agent requests the scan from WUAHandler, which uses the Windows Update Agent API to request a Software Update Scan from the Windows Update Agent.

#### ScanAgent.log:

```
ScanJob({4CD06388-D509-46E4-8C00-75909EDD9EE8}): CScanJob::Execute - successfully requested Scan, ScanType=1
ScanAgent      1/20/2014 12:18:42 PM
```

#### WUAHandler.log:

Scan results will include superseded updates only when they are superseded by service packs and definition updates.

```
WUAHandler      1/20/2014 12:18:42 PM
```

```
Search Criteria is (DeploymentAction=* AND Type='Software') OR (DeploymentAction=* AND Type='Driver')      WUAHandler
1/20/2014 12:18:42 PM
```

```
Running single-call scan of updates.      WUAHandler      1/20/2014 12:18:42 PM
```

```
Async searching of updates using WUAgent started. WUAHandler      1/20/2014 12:18:42 PM
```

### Windows Update Agent (WUA) starts the scan against the WSUS computer.

Windows Update Agent starts a scan after receiving a request from the Configuration Manager client (CcmExec). Because the Windows Update Server value was already set to the Software Update Point server, this scan is performed against the WSUS server that has the SUP role installed.

#### WindowsUpdate.log:

```
2014-01-20 12:18:42:694 3856 708 COMAPI -- START -- COMAPI: Search [ClientId = CcmExec]
2014-01-20 12:18:42:752 3856 708 COMAPI <<-- SUBMITTED -- COMAPI: Search [ClientId = CcmExec]
2014-01-20 12:18:47:511 968 f58 PT + ServiceId = {3DA21691-E39D-4DA6-8A4B-B43877BCB1B7}, Server
URL = http://PS1SITE.CONTOSO.COM:8530/ClientWebService/client.asmx
2014-01-20 12:18:48:662 968 f58 Agent ** START ** Agent: Finding updates [CallerId = CcmExec]
2014-01-20 12:18:48:662 968 f58 Agent * Include potentially superseded updates
2014-01-20 12:18:48:662 968 f58 Agent * Online = Yes; Ignore download priority = Yes
2014-01-20 12:18:48:662 968 f58 Agent * Criteria = "(DeploymentAction=* AND Type='Software') OR
(DeploymentAction=* AND Type='Driver')"
2014-01-20 12:18:48:662 968 f58 Agent * ServiceID = {3DA21691-E39D-4DA6-8A4B-B43877BCB1B7} Managed
2014-01-20 12:18:48:662 968 f58 Agent * Search Scope = {Machine}
```

Windows Update Agent now scans against the WSUS server and reports the results to CcmExec (specifically WUAHandler).

**WindowsUpdate.log:**

```

2014-01-20 12:18:49:175 968 f58 PT + ServiceId = {3DA21691-E39D-4DA6-8A4B-B43877BCB1B7}, Server
URL = http://PS1SITE.CONTOSO.COM:8530/ClientWebService/client.asmx
2014-01-20 12:18:52:680 968 f58 Agent * Added update {4AE85C00-0EAA-4BE0-B81B-DBD7053D5FAE}.104 to
search result
.
.
2014-01-20 12:18:52:683 968 f58 Agent * Added update {57260DFE-227C-45E3-9FFC-2FC77A67F95A}.104 to
search result
2014-01-20 12:18:52:694 968 f58 Agent * Found 163 updates and 70 categories in search; evaluated appl.
rules of 622 out of 1150 deployed entities
2014-01-20 12:18:52:745 968 f58 Agent ** END ** Agent: Finding updates [CallerId = CcmExec]
2014-01-20 12:18:52:755 3856 708 COMAPI >>-- RESUMED -- COMAPI: Search [ClientId = CcmExec]
2014-01-20 12:18:53:137 3856 708 COMAPI - Updates found = 163
2014-01-20 12:18:53:137 3856 708 COMAPI -- END -- COMAPI: Search [ClientId = CcmExec]

```

**WUAHandler receives the results from the Windows Update Agent and marks the scan as complete.****WUAHandler.log:**

```

Async searching completed. WUAHandler 1/20/2014 12:18:53 PM 3548 (0x0DDC)
Finished searching for everything in single call. WUAHandler 1/20/2014 12:18:53 PM 1800 (0x0708)

```

**WUAHandler parses the scan results.**

WUAHandler then parses the results, which include the applicability state for each update. As part of this process, superseded updates are pruned out.

**WUAHandler.log:**

```

Pruning: update id (70f4f236-0248-4e84-b472-292913576fa1) is superseded by (726b7201-862a-4fde-9b12-f36b38323a6f).
WUAHandler 1/20/2014 12:18:53 PM 1800 (0x0708)
.
.
Update (Installed): Security Update for Windows 7 for x64-based Systems (KB2584146) (4ae85c00-0eaa-4be0-b81b-dbd7053d5fae,
104) WUAHandler 1/20/2014 12:18:53 PM 1800 (0x0708)
Update (Missing): Security Update for Windows 7 for x64-based Systems (KB2862152) (505fda07-b4f3-45fb-83d9-8642554e2773,
200) WUAHandler 1/20/2014 12:18:53 PM 1800 (0x0708)
.
.
Successfully completed scan. WUAHandler 1/20/2014 12:18:54 PM 1800 (0x0708)

```

**Update Store records the status and raises a State Message for each update in WMI.**

Once the scan results are available, these results are stored in the Updates Store. Update Store records the current state of each update and creates a State Message for each update. These State Messages are forwarded to the Site Server in bulk at the end of the Status Message Reporting cycle (which is minutes, by default).

**UpdateStore.log showing state for Missing Update (KB2862152) being recorded and a State Message being raised:**

```

Processing update status from update (505fda07-b4f3-45fb-83d9-8642554e2773) with ProductID = 0fa1201d-4330-4fa8-8ae9-
b877473b6441 UpdatesStore 1/20/2014 12:18:55 PM 1800 (0x0708)
Update status from update (505fda07-b4f3-45fb-83d9-8642554e2773) hasn't been reported before, creating new instance.
UpdatesStore 1/20/2014 12:18:55 PM 1800 (0x0708)
Successfully raised state message for update (505fda07-b4f3-45fb-83d9-8642554e2773) with state (Missing). UpdatesStore
1/20/2014 12:18:55 PM 1800 (0x0708)

```

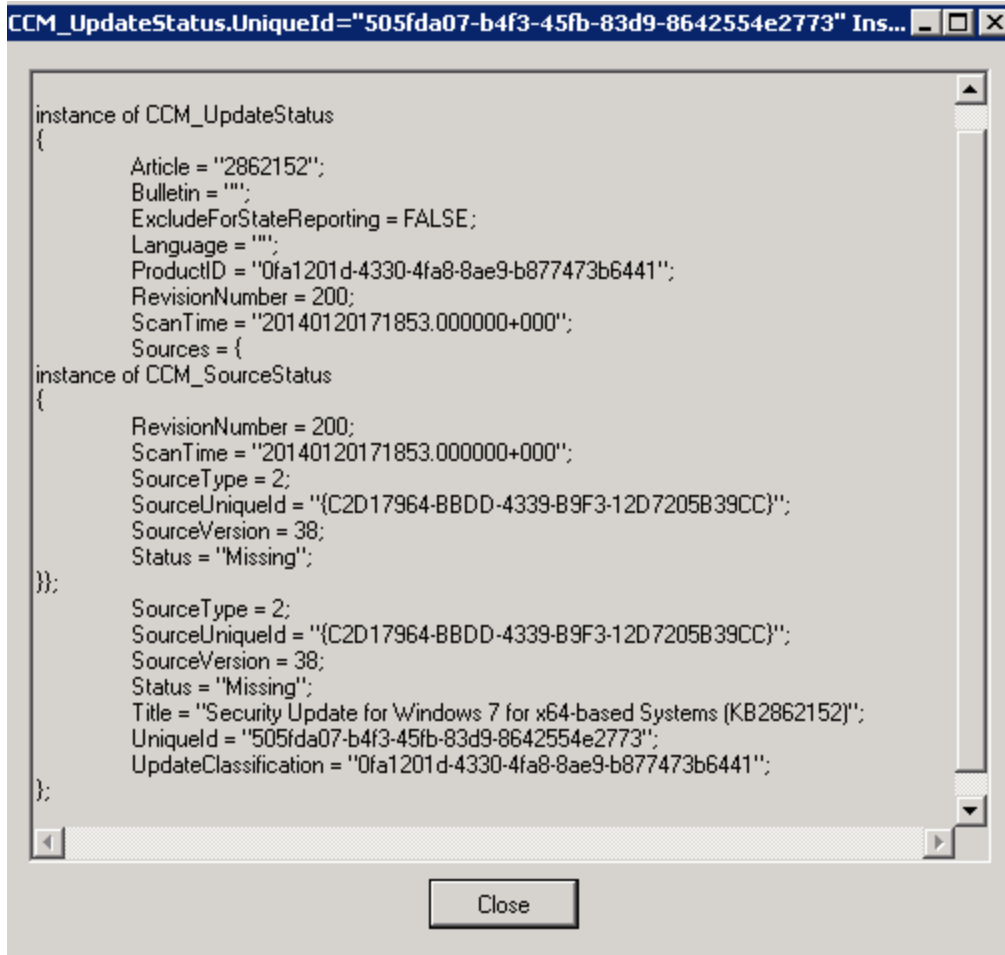
Successfully added WMI instance of update status (505fda07-b4f3-45fb-83d9-8642554e2773). UpdatesStore 1/20/2014  
12:18:55 PM 1800 (0x0708)

**StateMessage.log showing state messaged being recorded with State ID 2 (Missing):**

Adding message with TopicType 500 and TopicId 505fda07-b4f3-45fb-83d9-8642554e2773 to WMI StateMessage  
1/20/2014 12:18:55 PM 1800 (0x0708)

State message(State ID : 2) with TopicType 500 and TopicId 505fda07-b4f3-45fb-83d9-8642554e2773 has been recorded for SYSTEM  
StateMessage 1/20/2014 12:18:55 PM 1800 (0x0708)

For each update, an instance of the **CCM\_UpdateStatus** class is created or updated, and this stores the current status of the update. The **CCM\_UpdateStatus** class is located in the ROOT\CCM\SoftwareUpdates\UpdatesStore namespace.

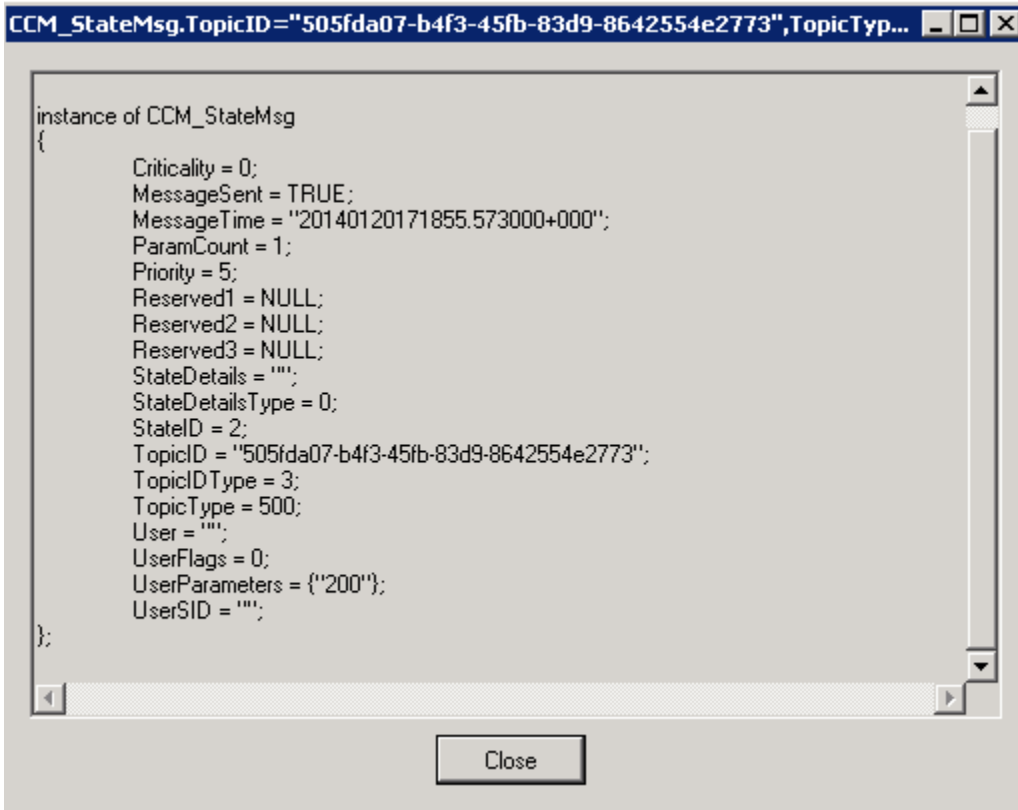


The screenshot shows a window titled "CCM\_UpdateStatus.UniqueId='505fda07-b4f3-45fb-83d9-8642554e2773' Ins...". The window contains a list of properties for an instance of the CCM\_UpdateStatus class. The properties are as follows:

```
instance of CCM_UpdateStatus
{
    Article = "2862152";
    Bulletin = "";
    ExcludeForStateReporting = FALSE;
    Language = "";
    ProductID = "0fa1201d-4330-4fa8-8ae9-b877473b6441";
    RevisionNumber = 200;
    ScanTime = "20140120171853.000000+000";
    Sources = {
instance of CCM_SourceStatus
{
    RevisionNumber = 200;
    ScanTime = "20140120171853.000000+000";
    SourceType = 2;
    SourceUniqueId = "{C2D17964-BBDD-4339-B9F3-12D7205B39CC}";
    SourceVersion = 38;
    Status = "Missing";
}};
    SourceType = 2;
    SourceUniqueId = "{C2D17964-BBDD-4339-B9F3-12D7205B39CC}";
    SourceVersion = 38;
    Status = "Missing";
    Title = "Security Update for Windows 7 for x64-based Systems (KB2862152)";
    UniqueId = "505fda07-b4f3-45fb-83d9-8642554e2773";
    UpdateClassification = "0fa1201d-4330-4fa8-8ae9-b877473b6441";
};
```

A "Close" button is visible at the bottom of the window.

Similarly, an instance of the **CCM\_StateMsg** class is created or updated, and this stores the current state of the update. The **CCM\_StateMsg** class is located in the ROOT\CCM\StateMsg namespace.



**State messages are sent to the management point.**

As mentioned earlier, state messages are sent to the management point based on the State Message reporting cycle schedule, which is configured to 15 minutes by default. Once a state message is sent to the management point, the **MessageSent** property for the State Message instance in the **CCM\_StateMsg** class is set to True.

**StateMessage.log:**

StateMessage body: <XML Report Body Truncated> StateMessage  
 Successfully forwarded State Messages to the MP StateMessage 1/20/2014 12:32:01 PM

Here’s how the State Message Body looks for our update. Normally this XML body is too large for the log and is truncated in CMTrace. However, you can see the whole body in Notepad.

**StateMessage.log:**

StateMessage body: <?xml version="1.0" encoding="UTF-16"?>  
 <Report><ReportHeader><Identification><Machine><ClientInstalled>1</ClientInstalled><ClientType>1</ClientType><ClientID>GUID:  
 A1006D0E-CF56-41D1-A006-  
 6330EFC39381</ClientID><ClientVersion>5.00.7958.1000</ClientVersion><NetBIOSName>PS1WIN7X64</NetBIOSName><CodePage  
 >437</CodePage><SystemDefaultLCID>1033</SystemDefaultLCID><Priority>5</Priority></Machine></Identification><ReportDetails  
 ><ReportContent>State Message  
 Data</ReportContent><ReportType>Full</ReportType><Date>20140120194656.903000+000</Date><Version>1.0</Version><Forma  
 t>1.0</Format></ReportDetails></ReportHeader><ReportBody><StateMessage MessageTime="20140120171855.573000+000"  
 SerialNumber="232"><Topic ID="505fda07-b4f3-45fb-83d9-8642554e2773" Type="500" IDType="3" User="" UserSID=""><State  
 ID="2" Criticality="0"/><UserParameters Flags="0"  
 Count="1"><Param>200</Param></UserParameters></StateMessage></ReportBody></Report>  
 StateMessage 1/20/2014 2:46:56 PM  
 Successfully forwarded State Messages to the MP StateMessage 1/20/2014 2:46:56 PM 3508 (0x0DB4)



---

## STATE MESSAGE PROCESSING FLOW

We now know how a state message is recorded and the WMI location where these state messages are stored. We also know that unsent state messages on a client are sent to the management point every 15 minutes by default, per the State Message Reporting Cycle. This schedule can be modified in the Custom or Default Client Settings -> State Messaging section.

Although StateMessage.log reports that it "Successfully forwarded State Messages to the MP," the State Message component is not actually sending these messages itself. All messages sent and received from the management point are handled by the CCM Messaging component on the client. CCM Messaging is the actual component that communicates with the management point for sending and receiving data. The management point has various queues defined to handle different kinds of incoming traffic. For state messages, the queue that handles this traffic is the **MP\_RelayEndpoint** queue.

1. [State Message component on client starts sending messages to the management point.](#)
2. [CCM Messaging sends a message containing the State Message XML Body to the management point.](#)
3. [Message is received on the management point, and then MP Relay processes the message and creates a SMX file.](#)
4. [MP File Dispatch Manager sends the SMX file to the Site Server \(only when the management point is not co-located on Site Server\).](#)
5. [StateSys component on Site Server processes the State Message to the database.](#)

**The State Message component starts sending messages to the management point.**

### StateMessage.log:

```
StateMessage body: <?xml version="1.0" encoding="UTF-16"?>
<Report><ReportHeader><Identification><Machine><ClientInstalled>1</ClientInstalled><ClientType>1</ClientType><ClientID>GUID:
A1006D0E-CF56-41D1-A006-
6330EFC39381</ClientID><ClientVersion>5.00.7958.1000</ClientVersion><NetBIOSName>PS1WIN7X64</NetBIOSName><CodePage
>437</CodePage><SystemDefaultLCID>1033</SystemDefaultLCID><Priority>5</Priority></Machine></Identification><ReportDetails
><ReportContent>State Message
Data</ReportContent><ReportType>Full</ReportType><Date>20140120194656.903000+000</Date><Version>1.0</Version><Forma
t>1.0</Format></ReportDetails></ReportHeader><ReportBody><StateMessage MessageTime="20140120171855.573000+000"
SerialNumber="232"><Topic ID="505fda07-b4f3-45fb-83d9-8642554e2773" Type="500" IDType="3" User="" UserSID=""/><State
ID="2" Criticality="0"/><UserParameters Flags="0"
Count="1"><Param>200</Param></UserParameters></StateMessage></ReportBody></Report>
StateMessage 1/20/2014 2:46:56 PM
Successfully forwarded State Messages to the MP StateMessage 1/20/2014 2:46:56 PM 3508 (0x0DB4)
```

**CCM Messaging sends a message containing the State Message XML Body to the management point.**

CCM Messaging sends a message to the *MP\_RelayEndpoint* queue successfully. This message does not have a reply, unlike the one we noticed earlier in the "WSUS Location Request" section where the message with the Location Request received a reply.

### CcmMessaging.log:

```
Sending async message '{95F79010-D0EB-49A6-8A1E-3897883105F2}' to outgoing queue 'mp:mp_relayendpoint' CcmMessaging
1/20/2014 2:46:56 PM 3508 (0x0DB4)
```

```
Sending outgoing message '{95F79010-D0EB-49A6-8A1E-3897883105F2}'. Flags 0x200, sender account empty      CcmMessaging
1/20/2014 2:46:57 PM    3004 (0x0BBC)
POST: Host=PS1SYS.CONTOSO.COM, Path=/ccm_system/request, Port=443, Protocol=https, Flags=512, Options=480
      CcmMessaging 1/20/2014 2:46:57 PM    3004 (0x0BBC)
Message '{95F79010-D0EB-49A6-8A1E-3897883105F2}' doesn't have reply      CcmMessaging 1/20/2014 2:46:57 PM    3004
(0x0BBC)
OutgoingMessage(Queue='mp_mp_relayendpoint', ID={95F79010-D0EB-49A6-8A1E-3897883105F2}): Delivered successfully to host
'PS1SYS.CONTOSO.COM'. CcmMessaging 1/20/2014 2:46:57 PM    3004 (0x0BBC)
```

**The message is received on the management point, and then MP\_Relay processes the message and creates an SMX file.**

As all messages are sent using HTTP/HTTPS and are received by IIS. In this example, this request is made to the CCM\_System virtual directory.

**IIS Log:**

```
192.168.2.12 CCM_POST /ccm_system/request - 443 - 192.168.2.62 ccmhttp - 200 0 0 542 31
```

Once the message is received successfully on the management point, the MP\_Relay component processes this message, converts the message into an SMX file, and moves the SMX file to the appropriate location depending on whether the management point is co-located on the site server or not.

On Remote management point: \SMS\mp\outboxes\StateMsg.box

Management point co-located on Site Server: \inboxes\auth\StateSys.box\incoming

**MP\_Relay.log on MP co-located on Site Server:**

```
Mp Message Handler: start message processing for Relay. ----- MP_RelayEndpoint
Mp Message Handler: FileType=SMX      MP_RelayEndpoint
Message Body : <XML Body Truncated>   MP_RelayEndpoint
Relay: Outbox dir: E:\ConfigMgr\inboxes\auth\statesys.box\incoming MP_RelayEndpoint
Priority in the message = 5MP_RelayEndpoint
State Priority Directory = E:\ConfigMgr\inboxes\auth\statesys.box\incoming MP_RelayEndpoint
Inv-Relay: Task completed successfully MP_RelayEndpoint
```

In our example, because the management point is remote to the Site Server, the MP\_Relay component moves the file to the \SMS\Outboxes\StateMsg.box folder. Also note that the XML body looks identical to what was logged in StateMessage.log on the client.

**MP\_Relay.log on Remote MP:**

```
Mp Message Handler: start message processing for Relay. ----- MP_RelayEndpoint      1/20/2014 2:46:57 PM
Mp Message Handler: FileType=SMX      MP_RelayEndpoint      1/20/2014 2:46:57 PM
Message Body :
<?xml version="1.0" encoding="UTF-16"?>
<Report><ReportHeader><Identification><Machine><ClientInstalled>1</ClientInstalled><ClientType>1</ClientType><ClientID>GUID:
A1006D0E-CF56-41D1-A006-
6330EFC39381</ClientID><ClientVersion>5.00.7958.1000</ClientVersion><NetBIOSName>PS1WIN7X64</NetBIOSName><CodePage
>437</CodePage><SystemDefaultLCID>1033</SystemDefaultLCID><Priority>5</Priority></Machine></Identification><ReportDetails
><ReportContent>State Message
Data</ReportContent><ReportType>Full</ReportType><Date>20140120194656.903000+000</Date><Version>1.0</Version><Forma
t>1.0</Format></ReportDetails></ReportHeader><ReportBody><StateMessage MessageTime="20140120171855.573000+000"
```

```

SerialNumber="232"><Topic ID="505fda07-b4f3-45fb-83d9-8642554e2773" Type="500" IDType="3" User="" UserSID=""/><State
ID="2" Criticality="0"/><UserParameters Flags="0"
Count="1"><Param>200</Param></UserParameters></StateMessage></ReportBody></Report>
MP_RelayEndpoint 1/20/2014 2:46:57 PM
Inv-Relay Task: Processing message body MP_RelayEndpoint 1/20/2014 2:46:57 PM
Relay: Outbox dir: C:\SMS\mp\outboxes\StateMsg.box MP_RelayEndpoint 1/20/2014 2:46:57 PM
Priority in the message = 5MP_RelayEndpoint 1/20/2014 2:46:57 PM
State Priority Directory = C:\SMS\mp\outboxes\StateMsg.box MP_RelayEndpoint 1/20/2014 2:46:57 PM
Inv-Relay: Task completed successfully MP_RelayEndpoint 1/20/2014 2:46:57 PM

```

**MP File Dispatch Manager sends the SMX file to the Site Server (only when the management point is not co-located on Site Server).**

When the management point is remote to the Site Server, after the file arrives in outboxes\StateMsg.box, MP File Dispatch Manager (MPFDM) is responsible for moving these files to the StateMsg.box inbox on the Site Server. When the management point is co-located on the Site Server, these files are moved directly to the appropriate Inbox folder, so MPFDM is not involved.

**MPFDM.log on a Remote MP:**

```

Moved file C:\SMS\MP\OUTBOXES\statemsg.box\TAZGYTSJ.SMX to
\\PS1SITE.CONTOSO.COM\SMS_PS1\inboxes\auth\statesys.box\incoming\TAZGYTSJ.SMX
SMS_MP_FILE_DISPATCH_MANAGER 1/20/2014 4:17:07 PM

```

For MPFDM to move the files to the appropriate inbox, the remote management point must be able to access the registry of the Site Server to determine the Inbox source locations. For this to work, the Remote Registry service must be running, and Registry Access should not be blocked via Group Policy. MPFDM determines the Inbox locations by accessing the following key on the Site Server:

**HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\SMS\Inbox Source**

**StateSys component on Site Server processes the State Message to the database.**

After the file arrives in \inboxes\auth\StateSys.box on the Site Server, the State System Manager (StateSys) component wakes up and processes the SMX file(s).

**StateSys.log with Verbose Logging:**

```

Inbox notification triggered, pause for 10 seconds.... SMS_STATE_SYSTEM
Found new state messages to process, starting processing thread SMS_STATE_SYSTEM
Thread "State Message Processing Thread #0" id:4316 started SMS_STATE_SYSTEM
total chucks loaded (1) SMS_STATE_SYSTEM
CMessageProcessor - Processing file: YCE2H3VD.SMX SMS_STATE_SYSTEM
CMessageProcessor - Processed 1 records with 0 invalid records. SMS_STATE_SYSTEM
CMessageProcessor - Processed 1 message files in this batch, with 0 bad files. SMS_STATE_SYSTEM
total chucks loaded (0) SMS_STATE_SYSTEM
Thread "State Message Processing Thread #0" id:4316 terminated normally SMS_STATE_SYSTEM

```

**StateSys.log without Verbose Logging:**

```

Found new state messages to process, starting processing thread SMS_STATE_SYSTEM 1/20/2014 4:47:19 PM 3068
(0x0BFC)
Thread "State Message Processing Thread #0" id:1988 started SMS_STATE_SYSTEM 1/20/2014 4:47:19 PM 1988 (0x07C4)
total chucks loaded (1) SMS_STATE_SYSTEM 1/20/2014 4:47:19 PM 1988 (0x07C4)
total chucks loaded (0) SMS_STATE_SYSTEM 1/20/2014 4:47:19 PM 1988 (0x07C4)

```

Thread "State Message Processing Thread #0" id:1988 terminated normally SMS\_STATE\_SYSTEM 1/20/2014 4:47:19 PM  
1988 (0x07C4)

Note that the StateSys.log file does not log the file name unless verbose logging is enabled for State System Manager. For the steps to enable verbose logging for State System Manager, see Procedure C.

The SMX file that is moved to the StateSys.box folder contains the Message Body XML. When StateSys processes this file, it calls the **spProcessStateReport** stored procedure and passes this XML body on to the stored procedure as a parameter.

**SQL Profiler:**

```
exec dbo.spProcessStateReport N'<?xml version="1.0" encoding="UTF-16"?>
<Report><ReportHeader><Identification><Machine><ClientInstalled>1</ClientInstalled><ClientType>1</ClientType><ClientID>GUID:
A1006D0E-CF56-41D1-A006-
6330EFC39381</ClientID><ClientVersion>5.00.7958.1000</ClientVersion><NetBIOSName>PS1WIN7X64</NetBIOSName><CodePage
>437</CodePage><SystemDefaultLCID>1033</SystemDefaultLCID><Priority>5</Priority></Machine></Identification><ReportDetails
><ReportContent>State Message
Data</ReportContent><ReportType>Full</ReportType><Date>20140120220131.071000+000</Date><Version>1.0</Version><Forma
t>1.0</Format></ReportDetails></ReportHeader><ReportBody><StateMessage MessageTime="20140120171855.573000+000"
SerialNumber="239"><Topic ID="505fda07-b4f3-45fb-83d9-8642554e2773" Type="500" IDType="3" User="" UserSID=""><State
ID="2" Criticality="0"/><UserParameters Flags="0"
Count="1"><Param>200</Param></UserParameters></StateMessage></ReportBody></Report>'
```

**spProcessStateReport** is a CLR stored procedure, and the CLR definition has the logic to determine the type of State Message being processed. Depending on the type of State Message, it processes the State Message appropriately and inserts the data in the database.

**TIP:**

You can find friendly names of all State Message Topic Types and IDs by querying the SR\_StateNames table. To do this, run the following command:

```
SELECT * FROM SR_StateNames
```

---

## SOFTWARE UPDATE SUMMARIZATION

Before Software Update Compliance data can be presented in the console or reports, the Software Update compliance data must be summarized. This is necessary because the console and reports usually display only summarized data. The State System component on the Site Server performs the Software Update summarization along with summarization for other components, which include applications, DCM deployments, client health, and so forth. You can find information about all the summarization tasks that State System performs by querying the **vSR\_SummaryTasks** view in the Configuration Manager database. State System runs these tasks on a configured schedule and logs detail about each task.

**StateSys.log:**

```
Started task '<TaskName>' SMS_STATE_SYSTEM 2/4/2014 10:49:20 AM 5384 (0x1508)
Task '<TaskName>' completed successfully after running for 15 seconds, with status 8. SMS_STATE_SYSTEM 2/4/2014
10:49:35 AM 5384 (0x1508)
```

For most of these tasks, the status logged by StateSys.log is not an error code, but is instead the count of the number of rows returned by the appropriate SQL stored procedure that performs the summarization.

Summarization tasks specified to Software Updates are:

**SUM Assignment Compliance Evaluator** – Runs every hour by default.

Summarizes state messages for all Software Update Group Assignments (Deployments). This task can be initiated manually *for a specific deployment* by going to Configuration Manager Console -> Monitoring pane -> Deployments -> Right-click the deployment, and then click **Run Summarization**.

**SUM Update Group Status Summarizer** – Runs every hour by default.

Summarizes status of Update Groups. This task can be initiated manually *for a specific Update Group* by navigating to Configuration Manager Console -> Software Library pane -> Software Updates -> Software Update Groups -> Right-click the update group, and then click **Run Summarization**. You can also change the schedule of this task by right-clicking **Software Update Groups** or by selecting **Schedule Summarization** in the ribbon area.

**SUM Update Status Summarizer** - Runs every hour by default.

Summarizes status of updates for all clients. This task can be initiated manually by navigating to Configuration Manager Console -> Software Library pane -> Software Updates node and then clicking **Run Summarization**. You can also change the default schedule by selecting **Schedule Summarization**.

**SUM Migrate Update Status** – Runs every 24 hours by default.

Migrates update status internally within the database. This task cannot be initiated manually from the console.

**SUM Delete Aged Status** – Runs every 24 hours by default.

Deletes aged status from Software Update specific tables in the database. This task cannot be initiated manually from the console.

---

## SOFTWARE UPDATE SWITCHING (SP1 AND R2 ONLY)

In ConfigMgr 2012 SP1 and later versions, a site can have multiple Software Update Points. This provides fault tolerance for situations when a Software Update Point becomes unavailable. For information about Software Update Points Failover and Switching, see the following TechNet resources:

<http://blogs.technet.com/b/configmgrteam/archive/2013/03/27/software-update-points-in-cm2012sp1.aspx>  
[http://technet.microsoft.com/en-us/library/gg712696.aspx#BKMK\\_SUPSwitching](http://technet.microsoft.com/en-us/library/gg712696.aspx#BKMK_SUPSwitching)

## DEPLOYMENT

---

### CREATING A SOFTWARE UPDATE GROUP

When you create a Software Update group in the Configuration Manager console, an instance of the **SMS\_AuthorizationList** class is created. This instance contains information about the Software Update group, and it has relationships with the software updates in the Software Update group.

**SMSProv.log:**

```

CSpClassManager::PreCallAction, dbname=CM_PS1 SMS Provider 1/23/2014 1:19:36 PM 1060 (0x0424)
PutInstanceAsync SMS_AuthorizationList SMS Provider 1/23/2014 1:19:36 PM 1060 (0x0424)
CExtProviderClassObject::DoPutInstanceInstance SMS Provider 1/23/2014 1:19:36 PM 1060 (0x0424)
Updating SDM content definition. SMS Provider 1/23/2014 1:19:36 PM 1060 (0x0424)
Try to sync permission table : Declare @Ids RBAC_Object_Type;insert into @Ids (ObjectKey, ObjectTypeID) values
(N'ScopeId_FC8FCC38-4BB1-4245-92F5-9CE841775019/AuthList_9D013E6D-EF76-43F6-ACC4-80749AB8D90A',34);exec
spRBAC_SyncPermissions @ObjectIds=@Ids,@RoleIds=N'',@AdminIds=N'' SMS Provider 1/23/2014 1:19:41 PM 1060
(0x0424)
Successfully synced permission table SMS Provider 1/23/2014 1:19:41 PM 1060 (0x0424)
Auditing: User CONTOSO\Admin created an instance of class SMS_AuthorizationList. SMS Provider 1/23/2014 1:19:42 PM
1060 (0x0424)

```

As part of the Software Update group creation process, SMSProv inserts data in appropriate CI\_ tables, including the following:

- CI\_ConfigurationItems
- CI\_ConfigurationItemRelations
- CI\_ConfigurationItemRELations\_Flat
- CI\_DocumentStore
- CI\_CIDocuments
- CI\_LocalizedProperties

SMSDBMON monitors when data is inserted into these tables and drops CI Notification (CIN) files in objmgr.box.

**SMSDBMon:**

```

RCV: INSERT on CI_ConfigurationItems for CINotify_iud [16777264 ][60216] SMS_DATABASE_NOTIFICATION_MONITOR
1/23/2014 1:19:47 PM 3908 (0x0F44)
RCV: UPDATE on CI_ConfigurationItems for CINotify_iud [16777264 ][60217] SMS_DATABASE_NOTIFICATION_MONITOR
1/23/2014 1:19:47 PM 3908 (0x0F44)
RCV: INSERT on CI_ConfigurationItemRelations_Flat for CI_ConfigurationItemRelations_Flat_From_iud [16777264 ][60218]
SMS_DATABASE_NOTIFICATION_MONITOR 1/23/2014 1:19:47 PM 3908 (0x0F44)
RCV: INSERT on CI_ConfigurationItemRelations_Flat for CI_ConfigurationItemRelations_Flat_From_iud [16777264 ][60219]
SMS_DATABASE_NOTIFICATION_MONITOR 1/23/2014 1:19:47 PM 3908 (0x0F44)
RCV: INSERT on CI_ConfigurationItemRelations_Flat for CI_ConfigurationItemRelations_Flat_From_iud [16777264 ][60220]
SMS_DATABASE_NOTIFICATION_MONITOR 1/23/2014 1:19:47 PM 3908 (0x0F44)
RCV: INSERT on CI_ConfigurationItemRelations_Flat for CI_ConfigurationItemRelations_Flat_From_iud [16777264 ][60221]
SMS_DATABASE_NOTIFICATION_MONITOR 1/23/2014 1:19:47 PM 3908 (0x0F44)
RCV: INSERT on CI_ConfigurationItemRelations_Flat for CI_ConfigurationItemRelations_Flat_From_iud [16777264 ][60222]
SMS_DATABASE_NOTIFICATION_MONITOR 1/23/2014 1:19:47 PM 3908 (0x0F44)
RCV: INSERT on CI_ConfigurationItemRelations_Flat for CI_ConfigurationItemRelations_Flat_From_iud [16777264 ][60223]
SMS_DATABASE_NOTIFICATION_MONITOR 1/23/2014 1:19:47 PM 3908 (0x0F44)
RCV: UPDATE on CI_ConfigurationItems for CINotify_iud [16777264 ][60224] SMS_DATABASE_NOTIFICATION_MONITOR
1/23/2014 1:19:47 PM 3908 (0x0F44)
RCV: UPDATE on CI_ConfigurationItems for CINotify_iud [16777264 ][60225] SMS_DATABASE_NOTIFICATION_MONITOR
1/23/2014 1:19:47 PM 3908 (0x0F44)
RCV: INSERT on RBAC_ChangeNotification for Rbac_Sync_ChangeNotification [363 ][60226]
SMS_DATABASE_NOTIFICATION_MONITOR 1/23/2014 1:19:47 PM 3908 (0x0F44)
SND: Dropped E:\ConfigMgr\inbox\objmgr.box\16777264.CIN [60225] SMS_DATABASE_NOTIFICATION_MONITOR
1/23/2014 1:19:48 PM 3908 (0x0F44)
SND: Dropped E:\ConfigMgr\inbox\hman.box\363.RBC [60226] SMS_DATABASE_NOTIFICATION_MONITOR 1/23/2014
1:19:48 PM 3908 (0x0F44)

```

Object Replication Manager wakes up when files are dropped in objmgr.box and processes the Software Update group.

**ObjReplMgr.log:**

```

File notification triggered. SMS_OBJECT_REPLICATION_MANAGER 1/23/2014 1:19:47 PM 3380 (0x0D34)
+++Begin processing changed CIN objects SMS_OBJECT_REPLICATION_MANAGER 1/23/2014 1:19:52 PM 3380 (0x0D34)
***** Processing AuthorizationList ScopelId_FC8FCC38-4BB1-4245-92F5-9CE841775019/AuthList_9D013E6D-EF76-43F6-ACC4-
80749AB8D90A ***** SMS_OBJECT_REPLICATION_MANAGER 1/23/2014 1:19:53 PM 3380 (0x0D34)
Deleting notification file E:\ConfigMgr\inboxes\objmgr.box\16777264.CIN SMS_OBJECT_REPLICATION_MANAGER
1/23/2014 1:19:53 PM 3380 (0x0D34)
+++Begin collecting targeting information for Affected CIs SMS_OBJECT_REPLICATION_MANAGER 1/23/2014 1:19:53 PM
3380 (0x0D34)
+++Completed collecting targeting information for Affected CIs SMS_OBJECT_REPLICATION_MANAGER 1/23/2014
1:19:53 PM 3380 (0x0D34)
Affected CIs (1): 16777264 SMS_OBJECT_REPLICATION_MANAGER 1/23/2014 1:19:53 PM 3380 (0x0D34)
CI 16777264 is NOT Targeted SMS_OBJECT_REPLICATION_MANAGER 1/23/2014 1:19:53 PM 3380 (0x0D34)
Successfully processed AuthorizationList ScopelId_FC8FCC38-4BB1-4245-92F5-9CE841775019/AuthList_9D013E6D-EF76-43F6-ACC4-
80749AB8D90A SMS_OBJECT_REPLICATION_MANAGER 1/23/2014 1:19:54 PM 3380 (0x0D34)
Set last row version for Configuration Item to 0x000000000296047 SMS_OBJECT_REPLICATION_MANAGER 1/23/2014
1:19:54 PM 3380 (0x0D34)

```

The changes to the CI\_\* tables are then replicated to the child sites via database replication, allowing the Software Update group to show up on the child site.

Software Update groups are Configuration Items themselves, and the CI Type ID for Software Update groups is 9. You can view the Software Update groups by running the following SQL Query:

```
SELECT * FROM vSMS_ConfigurationItems WHERE CItemType_ID = 9
```

To see the relationships from a Software Update group CI to the Software Update CI's, run the following SQL query:

```
SELECT CIR.* FROM CI_ConfigurationItemRelations CIR
JOIN CI_ConfigurationItems CI ON CIR.FromCI_ID = CI.CI_ID
WHERE CI.CItemType_ID = 9
```

---

#### MANUALLY CREATING A DEPLOYMENT FOR SOFTWARE UPDATE GROUP

When a deployment for a Software Update group is created, an instance of the **SMS\_UpdateGroupAssignment** class is created. This contains information about the deployment.

##### **SMSProv.log:**

```

PutInstanceAsync SMS_UpdateGroupAssignment SMS Provider
CExtProviderClassObject::DoPutInstanceInstance SMS Provider
Auditing: User CONTOSO\Admin created an instance of class SMS_UpdateGroupAssignment. SMS Provider

```

Updates are then downloaded to the specified package source directory by the Software Updates Patch Downloader component.

##### **PatchDownloader.log in %TEMP% directory:**

```

Trying to connect to the root\SMS namespace on the PS1SITE.CONTOSO.COM machine. Software Updates Patch Downloader
1/23/2014 3:31:34 PM 1400 (0x0578)
Connected to \\PS1SITE.CONTOSO.COM\root\SMS Software Updates Patch Downloader 1/23/2014 3:31:34 PM 1400
(0x0578)
Trying to connect to the \\PS1SITE.CONTOSO.COM\root\sms\site_PS1 namespace on the PS1SITE.CONTOSO.COM machine.
Software Updates Patch Downloader 1/23/2014 3:31:34 PM 1400 (0x0578)

```

```

Connected to \\PS1SITE.CONTOSO.COM\root\sms\site_PS1 Software Updates Patch Downloader 1/23/2014 3:31:34 PM
1400 (0x0578)
Download destination = \\PS1SITE\SOURCE\Updates\Win7\d09e9a92-20e7-455a-a51b-aaeca7b7d7e1.1\windows6.1-kb2807986-
x86.cab . Software Updates Patch Downloader 1/23/2014 3:31:34 PM 1400 (0x0578)
Contentsource = http://wsus.ds.download.windowsupdate.com/msdownload/update/software/secu/2013/02/windows6.1-
kb2807986-x86_83d5bb38d8c50d924f3dcd024b20fe33afbd9d14.cab . Software Updates Patch Downloader 1/23/2014
3:31:34 PM 1400 (0x0578)
Downloading content for ContentID = 471, FileName = windows6.1-kb2807986-x86.cab. Software Updates Patch Downloader
1/23/2014 3:31:34 PM 1400 (0x0578)
Download http://wsus.ds.download.windowsupdate.com/msdownload/update/software/secu/2013/02/windows6.1-kb2807986-
x86_83d5bb38d8c50d924f3dcd024b20fe33afbd9d14.cab to C:\Users\Admin\AppData\Local\Temp\2\CABBA79.tmp returns 0
Software Updates Patch Downloader 1/23/2014 3:31:36 PM 5736 (0x1668)
Successfully moved C:\Users\Admin\AppData\Local\Temp\2\CABBA79.tmp to \\PS1SITE\SOURCE\Updates\Win7\d09e9a92-20e7-
455a-a51b-aaeca7b7d7e1.1\windows6.1-kb2807986-x86.cab Software Updates Patch Downloader 1/23/2014 3:31:36 PM
5736 (0x1668)
Renaming \\PS1SITE\SOURCE\Updates\Win7\d09e9a92-20e7-455a-a51b-aaeca7b7d7e1.1 to
\\PS1SITE\SOURCE\Updates\Win7\d09e9a92-20e7-455a-a51b-aaeca7b7d7e1 Software Updates Patch Downloader
1/23/2014 3:31:36 PM 1400 (0x0578)
Successfully moved \\PS1SITE\SOURCE\Updates\Win7\d09e9a92-20e7-455a-a51b-aaeca7b7d7e1.1 to
\\PS1SITE\SOURCE\Updates\Win7\d09e9a92-20e7-455a-a51b-aaeca7b7d7e1 Software Updates Patch Downloader
1/23/2014 3:31:36 PM 1400 (0x0578)

```

After the updates are downloaded, SMS Provider adds each update to the specified package.

#### SMSProv:

```

Requested class =SMS_SoftwareUpdatesPackage SMS Provider 1/23/2014 3:31:36 PM 4060 (0x0FDC)
Requested num keys =1 SMS Provider 1/23/2014 3:31:36 PM 4060 (0x0FDC)
CExtProviderClassObject::DoExecuteMethod AddUpdateContent SMS Provider 1/23/2014 3:31:36 PM 4060 (0x0FDC)
*** SspPackageInst::AddUpdateContent *** SMS Provider 1/23/2014 3:31:36 PM 4060 (0x0FDC)
CObjectLock::UserHasLock: ***** User CONTOSO\Admin has lock for object
SMS_SoftwareUpdatesPackage.PackageID="PS100001" with LockID: DCE6F1B5-1EE8-47CB-85A7-3027E51119A7 *****
SMS Provider 1/23/2014 3:31:36 PM 4060 (0x0FDC)
CObjectLock::ReleaseLock: ***** User CONTOSO\Admin has released lock for object
SMS_SoftwareUpdatesPackage.PackageID="PS100001" with LockID: DCE6F1B5-1EE8-47CB-85A7-3027E51119A7 *****
SMS Provider 1/23/2014 3:31:36 PM 4060 (0x0FDC)
SspPackageInst::AddContent() called for these ContentIDs - {471} SMS Provider 1/23/2014 3:31:36 PM 4060 (0x0FDC)
SspPackageInst::AddContent() called with these CContentSourcePath - {"\\PS1SITE\SOURCE\Updates\Win7"} SMS Provider
1/23/2014 3:31:36 PM 4060 (0x0FDC)
RefreshDPs value is FALSE. DP(s) will not be updated at the end of the operation SMS Provider 1/23/2014 3:31:36 PM
4060 (0x0FDC)
These Contents will be added to Software Updates Package - PS100001 with PackageSource - \\PS1SITE\SOURCE\Updates\Win7
SMS Provider 1/23/2014 3:31:36 PM 4060 (0x0FDC)
Adding Content with ID 471, UniqueID d09e9a92-20e7-455a-a51b-aaeca7b7d7e1 and ContentSource
\\PS1SITE\SOURCE\Updates\Win7 to the Package SMS Provider 1/23/2014 3:31:36 PM 4060 (0x0FDC)
ContentFileName = windows6.1-kb2807986-x86.cab, SourceURL =
http://wsus.ds.download.windowsupdate.com/msdownload/update/software/secu/2013/02/windows6.1-kb2807986-
x86_83d5bb38d8c50d924f3dcd024b20fe33afbd9d14.cab, ImportPath = , ContentFileHash =
SHA1:83D5BB38D8C50D924F3DCD024B20FE33AFBD9D14 SMS Provider 1/23/2014 3:31:36 PM 4060 (0x0FDC)
File Source = \\PS1SITE\SOURCE\Updates\Win7\d09e9a92-20e7-455a-a51b-aaeca7b7d7e1\windows6.1-kb2807986-x86.cab
SMS Provider 1/23/2014 3:31:36 PM 4060 (0x0FDC)
File Destination = \\PS1SITE\SOURCE\Updates\Win7\d09e9a92-20e7-455a-a51b-aaeca7b7d7e1 SMS Provider 1/23/2014
3:31:36 PM 4060 (0x0FDC)
CExtUserContext::LeaveThread : Releasing IWBemContextPtr=57376560 SMS Provider 1/23/2014 3:31:36 PM 4060
(0x0FDC)

```

After all the updates are added to the Package, SMS Provider updates the package:



**SMSProv.log:**

```
CExtUserContext::EnterThread : User=CONTOSO\Admin
Sid=0x0105000000000005150000068830AA65AAB72A155BCE9324F040000 Caching IWbemContextPtr=0000000036B7E50 in
Process 0xc68 (3176) SMS Provider 1/23/2014 3:31:44 PM 1060 (0x0424)
Context: SMSAppName=Configuration Manager Administrator console SMS Provider 1/23/2014 3:31:44 PM 1060 (0x0424)
Context: MachineName=PS1SITE.CONTOSO.COM SMS Provider 1/23/2014 3:31:44 PM 1060 (0x0424)
Context: UserName=CONTOSO\Admin SMS Provider 1/23/2014 3:31:44 PM 1060 (0x0424)
Context: ObjectLockContext=c00c315d-b15d-4b0e-9844-017205cc2443 SMS Provider 1/23/2014 3:31:44 PM 1060
(0x0424)
Context: ApplicationName=Microsoft.ConfigurationManagement.exe SMS Provider 1/23/2014 3:31:44 PM 1060 (0x0424)
Context: ApplicationVersion=5.0.7958.1000 SMS Provider 1/23/2014 3:31:44 PM 1060 (0x0424)
Context: LocaleID=MS\0x409 SMS Provider 1/23/2014 3:31:44 PM 1060 (0x0424)
Context: __ProviderArchitecture=32 SMS Provider 1/23/2014 3:31:44 PM 1060 (0x0424)
Context: __RequiredArchitecture=0 (Bool) SMS Provider 1/23/2014 3:31:44 PM 1060 (0x0424)
Context: __ClientPreferredLanguages=en-US,en SMS Provider 1/23/2014 3:31:44 PM 1060 (0x0424)
Context: __GroupOperationId=755382 SMS Provider 1/23/2014 3:31:44 PM 1060 (0x0424)
Context: __WBEM_CLIENT_AUTHENTICATION_LEVEL=6 SMS Provider 1/23/2014 3:31:44 PM 1060 (0x0424)
CExtUserContext : Set ThreadLocaleID OK to: 1033 SMS Provider 1/23/2014 3:31:44 PM 1060 (0x0424)
CSspClassManager::PreCallAction, dbname=CM_PS1 SMS Provider 1/23/2014 3:31:44 PM 1060 (0x0424)
ExecMethodAsync : SMS_SoftwareUpdatesPackage.PackageID="PS100001"::RefreshPkgSource SMS Provider 1/23/2014
3:31:44 PM 1060 (0x0424)
Requested class =SMS_SoftwareUpdatesPackage SMS Provider 1/23/2014 3:31:44 PM 1060 (0x0424)
Requested num keys =1 SMS Provider 1/23/2014 3:31:44 PM 1060 (0x0424)
CExtProviderClassObject::DoExecuteMethod RefreshPkgSource SMS Provider 1/23/2014 3:31:44 PM 1060 (0x0424)
Auditing: User CONTOSO\Admin called an audited method of an instance of class SMS_SoftwareUpdatesPackage. SMS Provider
1/23/2014 3:31:44 PM 1060 (0x0424)
CExtUserContext::LeaveThread : Releasing IWbemContextPtr=57376336 SMS Provider 1/23/2014 3:31:44 PM 1060
(0x0424)
```

When the Update Group Assignment is created, SMS Provider inserts information about the assignment in the CI\_Assignments table. This then triggers SMSDBMON, which notifies Object Replication Manager to process the Update Group Assignment by dropping a .CIA file in objmgr.box.

**SMSDBMON.log:**

```
RCV: INSERT on CI_CIAssignments for CIAssignmentNotify_iu [16777222 ][60916] SMS_DATABASE_NOTIFICATION_MONITOR
1/23/2014 3:31:37 PM 3908 (0x0F44)
RCV: INSERT on CrpChange_Notify for CrpChange_Notify_ins [14 ][60917] SMS_DATABASE_NOTIFICATION_MONITOR
1/23/2014 3:31:37 PM 3908 (0x0F44)
RCV: UPDATE on CI_CIAssignments for CIAssignmentNotify_iu [16777222 ][60920] SMS_DATABASE_NOTIFICATION_MONITOR
1/23/2014 3:31:37 PM 3908 (0x0F44)
RCV: UPDATE on CI_AssignmentTargetedCIs for CI_AssignmentTargetedCIs_CIAMGR [16777222 ][60921]
SMS_DATABASE_NOTIFICATION_MONITOR 1/23/2014 3:31:37 PM 3908 (0x0F44)
RCV: UPDATE on CI_CIAssignments for CIAssignmentNotify_iu [16777222 ][60923] SMS_DATABASE_NOTIFICATION_MONITOR
1/23/2014 3:31:37 PM 3908 (0x0F44)
RCV: UPDATE on CI_AssignmentTargetedCIs for CI_AssignmentTargetedCIs_CIAMGR [16777222 ][60924]
SMS_DATABASE_NOTIFICATION_MONITOR 1/23/2014 3:31:37 PM 3908 (0x0F44)
RCV: UPDATE on CI_CIAssignments for CIAssignmentNotify_iu [16777222 ][60926] SMS_DATABASE_NOTIFICATION_MONITOR
1/23/2014 3:31:37 PM 3908 (0x0F44)
RCV: UPDATE on CI_AssignmentTargetedCIs for CI_AssignmentTargetedCIs_CIAMGR [16777222 ][60927]
SMS_DATABASE_NOTIFICATION_MONITOR 1/23/2014 3:31:37 PM 3908 (0x0F44)
SND: Dropped E:\ConfigMgr\inbox\objmgr.box\16777222.CIA [60916] SMS_DATABASE_NOTIFICATION_MONITOR
1/23/2014 3:31:37 PM 3908 (0x0F44)
SND: Dropped E:\ConfigMgr\inbox\policy\policytargeteval\14.CRP [60917] SMS_DATABASE_NOTIFICATION_MONITOR
1/23/2014 3:31:37 PM 3908 (0x0F44)
RCV: INSERT on PolicyAssignmentChg_Notify for PolicyAssignmentChg_Notify_iu [16786995 ][60929]
SMS_DATABASE_NOTIFICATION_MONITOR 1/23/2014 3:31:47 PM 3908 (0x0F44)
```

```

SND: Dropped E:\ConfigMgr\inboxes\policypv.box\policytargeteval\16786995.PAC [60929]
      SMS_DATABASE_NOTIFICATION_MONITOR 1/23/2014 3:31:47 PM 3908 (0x0F44)
RCV: INSERT on PkgNotification for PkgNotify_Add [PS100001 ][60930] SMS_DATABASE_NOTIFICATION_MONITOR
      1/23/2014 3:31:52 PM 3908 (0x0F44)
SND: Dropped E:\ConfigMgr\inboxes\distmgr.box\PS100001.PKN [60930] SMS_DATABASE_NOTIFICATION_MONITOR
      1/23/2014 3:31:52 PM 3908 (0x0F44)
RCV: INSERT on PolicyAssignmentChg_Notify for PolicyAssignmentChg_Notify_iu [16786995 ][60931]
      SMS_DATABASE_NOTIFICATION_MONITOR 1/23/2014 3:32:02 PM 3908 (0x0F44)
RCV: UPDATE on PolicyAssignmentChg_Notify for PolicyAssignmentChg_Notify_iu [16786995 ][60932]
      SMS_DATABASE_NOTIFICATION_MONITOR 1/23/2014 3:32:02 PM 3908 (0x0F44)
SND: Dropped E:\ConfigMgr\inboxes\policypv.box\policytargeteval\16786995.PAC [60931]
      SMS_DATABASE_NOTIFICATION_MONITOR 1/23/2014 3:32:02 PM 3908 (0x0F44)

```

After Object Replication Manager detects the CIA file in objmgr.box, it processes the file and creates the policy for the Software Update Assignment.

**ObjMgr.log:**

```

File notification triggered. SMS_OBJECT_REPLICATION_MANAGER 1/23/2014 3:31:37 PM 3380 (0x0D34)
+++Begin processing changed CIA objects SMS_OBJECT_REPLICATION_MANAGER 1/23/2014 3:31:37 PM 3380 (0x0D34)
**** Processing Update Group Assignment {3ACE84D4-7B2A-4D86-81AF-07E2AC255745} ****
      SMS_OBJECT_REPLICATION_MANAGER 1/23/2014 3:31:37 PM 3380 (0x0D34)
Deleting notification file E:\ConfigMgr\inboxes\objmgr.box\16777222.CIA SMS_OBJECT_REPLICATION_MANAGER
      1/23/2014 3:31:37 PM 3380 (0x0D34)
CI Assignment {3ACE84D4-7B2A-4D86-81AF-07E2AC255745} has 3 Targeted CI(s) SMS_OBJECT_REPLICATION_MANAGER
      1/23/2014 3:31:37 PM 3380 (0x0D34)
PolicyID {3ACE84D4-7B2A-4D86-81AF-07E2AC255745} PolicyVersion 1.00 PolicyHash
SHA256:63BAFA808F969849B40B2B727B49BC5093B965782716DDE3490528681CF27ACC
      SMS_OBJECT_REPLICATION_MANAGER 1/23/2014 3:31:37 PM 3380 (0x0D34)
Notifying policy provider about changes in policy content/targeting SMS_OBJECT_REPLICATION_MANAGER 1/23/2014
3:31:37 PM 3380 (0x0D34)
Successfully created policy for CI Assignment {3ACE84D4-7B2A-4D86-81AF-07E2AC255745}
      SMS_OBJECT_REPLICATION_MANAGER 1/23/2014 3:31:37 PM 3380 (0x0D34)
Notifying policy provider about changes in policy content/targeting SMS_OBJECT_REPLICATION_MANAGER 1/23/2014
3:31:38 PM 3380 (0x0D34)
Successfully updated Policy Targeting for CI Assignment {3ACE84D4-7B2A-4D86-81AF-07E2AC255745}
      SMS_OBJECT_REPLICATION_MANAGER 1/23/2014 3:31:38 PM 3380 (0x0D34)
No file trigger for E:\ConfigMgr\inboxes\objmgr.box\16777222.CIV - status 2 SMS_OBJECT_REPLICATION_MANAGER
      1/23/2014 3:31:38 PM 3380 (0x0D34)
Assigned CIs: [ 16777264 ] SMS_OBJECT_REPLICATION_MANAGER 1/23/2014 3:31:38 PM 3380 (0x0D34)
Begin processing Assigned CI: [16777264] SMS_OBJECT_REPLICATION_MANAGER 1/23/2014 3:31:38 PM 3380 (0x0D34)
Creating VersionInfo policy for CI 16777264 SMS_OBJECT_REPLICATION_MANAGER 1/23/2014 3:31:38 PM 3380 (0x0D34)
Creating VersionInfo policy Scopeld_FC8FCC38-4BB1-4245-92F5-9CE841775019/AuthList_9D013E6D-EF76-43F6-ACC4-
80749AB8D90A/VI SMS_OBJECT_REPLICATION_MANAGER 1/23/2014 3:31:38 PM 3380 (0x0D34)
16777264 Referenced CIs: [ 929 930 1041 1042 1132 1133 ] SMS_OBJECT_REPLICATION_MANAGER 1/23/2014 3:31:38 PM
3380 (0x0D34)
VersionInfo policy for CI 16777264 is Machine type SMS_OBJECT_REPLICATION_MANAGER 1/23/2014 3:31:38 PM 3380
(0x0D34)
PolicyID Scopeld_FC8FCC38-4BB1-4245-92F5-9CE841775019/AuthList_9D013E6D-EF76-43F6-ACC4-80749AB8D90A/VI PolicyVersion
1.00 PolicyHash SHA256:6EFE96F3D67773CA965EC67EC60B602FC78242509A096FCF44C2D5FDD5B2FC76
      SMS_OBJECT_REPLICATION_MANAGER 1/23/2014 3:31:38 PM 3380 (0x0D34)
Notifying policy provider about changes in policy content/targeting SMS_OBJECT_REPLICATION_MANAGER 1/23/2014
3:31:38 PM 3380 (0x0D34)
Updated dependent policy references to CIA {3ACE84D4-7B2A-4D86-81AF-07E2AC255745}
      SMS_OBJECT_REPLICATION_MANAGER 1/23/2014 3:31:38 PM 3380 (0x0D34)
STATMSG: ID=5800 SEV=I LEV=M SOURCE="SMS Server" COMP="SMS_OBJECT_REPLICATION_MANAGER"
SYS=PS1SITE.CONTOSO.COM SITE=PS1 PID=5404 TID=3380 GMTDATE=Thu Jan 23 20:31:38.889 2014 ISTR0="Microsoft Software
Updates - 2014-01-23 03:30:52 PM" ISTR1="" ISTR2="" ISTR3="" ISTR4="" ISTR5="" ISTR6="" ISTR7="" ISTR8="" ISTR9=""

```

```

NUMATTRS=1 AID0=414 AVAL0="{3ACE84D4-7B2A-4D86-81AF-07E2AC255745}"          SMS_OBJECT_REPLICATION_MANAGER
1/23/2014 3:31:38 PM    3380 (0x0D34)
Successfully updated CRCs for CI Assignment {3ACE84D4-7B2A-4D86-81AF-07E2AC255745}
SMS_OBJECT_REPLICATION_MANAGER    1/23/2014 3:31:38 PM    3380 (0x0D34)
Successfully processed Update Group Assignment {3ACE84D4-7B2A-4D86-81AF-07E2AC255745}
SMS_OBJECT_REPLICATION_MANAGER    1/23/2014 3:31:38 PM    3380 (0x0D34)
Set last row version for CI Assignment to 0x0000000000296628          SMS_OBJECT_REPLICATION_MANAGER    1/23/2014
3:31:39 PM    3380 (0x0D34)

```

After being notified by the Object Replication Manager, Policy Provider updates the policy for the clients.

#### PolicyPv.log:

```

File notification triggered. SMS_POLICY_PROVIDER    1/23/2014 3:31:37 PM    5568 (0x15C0)
Found 14.CRP SMS_POLICY_PROVIDER    1/23/2014 3:31:37 PM    1800 (0x0708)
Adding to delete list: E:\ConfigMgr\inboxes\policypv.box\policytargeteval\14.CRP          SMS_POLICY_PROVIDER    1/23/2014
3:31:37 PM    1800 (0x0708)
Processing any pending PolicyAssignmentChg_Notify SMS_POLICY_PROVIDER    1/23/2014 3:31:47 PM    5568 (0x15C0)
Updating ResPolicyMap SMS_POLICY_PROVIDER    1/23/2014 3:31:47 PM    5568 (0x15C0)
Policy or Policy Target Change Event triggered. SMS_POLICY_PROVIDER    1/23/2014 3:31:47 PM    5568 (0x15C0)
File notification triggered. SMS_POLICY_PROVIDER    1/23/2014 3:31:47 PM    1800 (0x0708)
Building Collection Change List from Collection Member Notification files          SMS_POLICY_PROVIDER    1/23/2014 3:31:57 PM
5568 (0x15C0)
--Handle PolicyAssignment Resigning          SMS_POLICY_PROVIDER    1/23/2014 3:31:57 PM    5568 (0x15C0)
Completed batch with beginning PADBID = 16786995 ending PADBID = 16786996.          SMS_POLICY_PROVIDER    1/23/2014
3:31:57 PM    5568 (0x15C0)
--Process Policy Changes SMS_POLICY_PROVIDER    1/23/2014 3:31:57 PM    5568 (0x15C0)
Found some Policy changes, returning New LastRowversion=0x000000000029662B          SMS_POLICY_PROVIDER    1/23/2014
3:31:57 PM    5568 (0x15C0)
Processing Updated Policies          SMS_POLICY_PROVIDER    1/23/2014 3:31:57 PM    5568 (0x15C0)
Building Collection Change List from New and Targeting Changed Policies          SMS_POLICY_PROVIDER    1/23/2014 3:31:57 PM
5568 (0x15C0)
--Update Policy Targeting Map          SMS_POLICY_PROVIDER    1/23/2014 3:31:57 PM    5568 (0x15C0)
*** Evaluating Collection 14 for targeting changes ***          SMS_POLICY_PROVIDER    1/23/2014 3:31:57 PM    5568 (0x15C0)
Advanced client policy changes detected for collection 14, *** 5 Added & 0 Deleted ***. SMS_POLICY_PROVIDER    1/23/2014
3:31:57 PM    5568 (0x15C0)
--Process Policy Targeting Map          SMS_POLICY_PROVIDER    1/23/2014 3:31:57 PM    5568 (0x15C0)
*** Process notification table to update resultant targeting table ***          SMS_POLICY_PROVIDER    1/23/2014 3:31:57 PM
5568 (0x15C0)

```

SQL Profiler covering the entire process displays the following:

#### SQL Profiler:

```

insert into CI_CIAssignments (AssignmentAction, Description, AssignmentName, DesiredConfigType, DisableMomAlerts, DPLocality,
AssignmentEnabled, EnforcementDeadline, EvaluationSchedule, ExpirationTime, LimitStateMessageVerbosity,
LogComplianceToWinEvent, NonComplianceCriticality, NotifyUser, OverrideServiceWindows, PersistOnWriteFilterDevices,
RaiseMomAlertsOnFailure, RandomizationEnabled, RebootOutsideOfServiceWindows, SendDetailedNonComplianceStatus,
StartTime, StateMessagePriority, StateMessageVerbosity, SuppressReboot, UseBranchCache, UseGMTTimes, UserUIExperience,
WoLEnabled, TargetCollectionID, LocaleID, Assignment_UniqueID, SourceSite, LastModifiedBy, AssignmentType, CreationTime,
LastModificationTime, IsTombstoned) values (2, N'', N'Microsoft Software Updates - 2014-01-23 03:30:52 PM', 1, 0, 16, 1,
'01/30/2014 15:30:00', null, null, 1, 0, null, 1, 0, 1, 0, null, 0, 0, '01/23/2014 15:31:00', 5, 5, 0, 1, 0, 1, 0, 14, 1033, N'{3ACE84D4-7B2A-
4D86-81AF-07E2AC255745}', N'PS1', N'CONTOSO\Admin', 5, '01/23/2014 20:31:31', '01/23/2014 20:31:31', 0)
;

```

```

insert into CI_AssignmentTargetedGroups (CI_ID, AssignmentID) values (16777264, 16777222)

```

```
insert into CI_ContentPackages (Content_ID, ContentSubFolder, ContentVersion, Content_UniqueID, MinPackageVersion,PkgID)
VALUES ('471', N'd09e9a92-20e7-455a-a51b-aaeca7b7d7e1', '1', N'd09e9a92-20e7-455a-a51b-aaeca7b7d7e1', '0', N'PS100001')
```

```
insert Policy (Version, PolicyHash, PolicyFlags, PolicyPriority, DeviceVersion, PolicyID)
values(N'1.00', N'SHA256:63BAFA808F969849B40B2B727B49BC5093B965782716DDE3490528681CF27ACC', 16592, 25, N'',
N'{3ACE84D4-7B2A-4D86-81AF-07E2AC255745}')
```

```
insert PolicyAssignment(PolicyAssignmentID, PADBID, Version, PolicyID, IsTombstoned, LastUpdateTime)
values(N'{8d9ba949-d038-4c09-a0cc-af3f07c39d71}', 16786995, N'1.00', N'{3ACE84D4-7B2A-4D86-81AF-07E2AC255745}', 0,
GetUTCDate())
```

```
DECLARE @AssignedCIs TABLE(CI_ID INT)
BEGIN
INSERT INTO @AssignedCIs
SELECT DISTINCT ATG.CI_ID FROM CI_AssignmentTargetedGroups ATG
INNER JOIN vCI_CIAssignments CIA ON CIA.AssignmentID = ATG.AssignmentID
WHERE CIA.Assignment_UniqueID = '{3ACE84D4-7B2A-4D86-81AF-07E2AC255745}'
IF @@ROWCOUNT = 0
BEGIN
INSERT INTO @AssignedCIs
SELECT DISTINCT ATCI.CI_ID FROM vCI_AssignmentTargetedCIs_Actual ATCI
INNER JOIN vCI_CIAssignments CIA ON CIA.AssignmentID = ATCI.AssignmentID
WHERE CIA.Assignment_UniqueID = '{3ACE84D4-7B2A-4D86-81AF-07E2AC255745}'END
END
SELECT DISTINCT CI_ID FROM @AssignedCIs
```

```
insert Policy (Version, PolicyHash, PolicyFlags, PolicyPriority, DeviceVersion, PolicyID)
values(N'1.00', N'SHA256:6EFE96F3D67773CA965EC67EC60B602FC78242509A096FCF44C2D5FDD5B2FC76', 208, 25, N'',
N'ScopeId_FC8FCC38-4BB1-4245-92F5-9CE841775019/AuthList_9D013E6D-EF76-43F6-ACC4-80749AB8D90A/VI')
```

```
UPDATE Policy SET DeviceBody = NULL where PolicyID='ScopeId_FC8FCC38-4BB1-4245-92F5-9CE841775019/AuthList_9D013E6D-
EF76-43F6-ACC4-80749AB8D90A/VI'
```

```
insert PolicyAssignment(PolicyAssignmentID, PADBID, Version, PolicyID, IsTombstoned, LastUpdateTime)
values(N'{64ed94a2-ff08-42a7-9e42-b292409c79e8}', 16786996, N'1.00', N'ScopeId_FC8FCC38-4BB1-4245-92F5-
9CE841775019/AuthList_9D013E6D-EF76-43F6-ACC4-80749AB8D90A/VI', 0, GetUTCDate())
```

```
insert CI_AssignmentCRCs (AssignmentID, AssignmentCRC, PolicyCRC, ComplianceCRC) values (16777222, N'7a2e8acd', N'c10ba7c5',
N'5aeb49f4')
```

```
insert into CI_ContentPackages (Content_ID, ContentSubFolder, ContentVersion, Content_UniqueID, MinPackageVersion,PkgID)
VALUES ('534', N'de62f3b3-615b-4800-b6ba-51d7c826dd08', '1', N'de62f3b3-615b-4800-b6ba-51d7c826dd08', '0', N'PS100001')
```

---

## CREATING A DEPLOYMENT USING AN AUTOMATIC DEPLOYMENT RULE

Automatic Deployment Rule execution is triggered manually, per a schedule, or after Software Update synchronization is completed. The Rule Engine component evaluates the rule, and if any software updates match the defined criteria, the Rule Engine downloads the updates, creates a Software Update group, and creates a Software Update Group Assignment. The following example shows the process of Software Update group and Deployment creation:

---

### RuleEngine.log showing beginning of Rule Processing:

```
Found notification file E:\ConfigMgr\inboxes\RuleEngine.box\1.RUL SMS_RULE_ENGINE 2/6/2014 3:08:51 PM 5488
(0x1570)
```

RuleSchedulerThred: Change in Rules Object Signalled.	SMS_RULE_ENGINE	2/6/2014 3:08:51 PM	6696 (0x1A28)
Constructing Rule 1 using Auto Deployment Rule Factory	SMS_RULE_ENGINE	2/6/2014 3:08:51 PM	5488 (0x1570)
Populating Rule Skeleton	SMS_RULE_ENGINE	2/6/2014 3:08:51 PM	5488 (0x1570)
Populating Criterion Skeleton	SMS_RULE_ENGINE	2/6/2014 3:08:51 PM	5488 (0x1570)
Populating Action Skeleton	SMS_RULE_ENGINE	2/6/2014 3:08:51 PM	5488 (0x1570)
Populating Action Skeleton	SMS_RULE_ENGINE	2/6/2014 3:08:51 PM	5488 (0x1570)
CRuleHandler: Need to Process 1 rules	SMS_RULE_ENGINE	2/6/2014 3:08:51 PM	5488 (0x1570)

**RuleEngine.log showing Rule Processing and query to run to find updates matching defined criteria:**

CRuleHandler: Processing Rule with ID:1, Name:ADR_Test.	SMS_RULE_ENGINE	2/6/2014 3:08:51 PM	5488 (0x1570)
Evaluating Update Criteria for AutoDeployment Rule 1	SMS_RULE_ENGINE	2/6/2014 3:08:51 PM	5488 (0x1570)
Evaluating Update Criteria...	SMS_RULE_ENGINE	2/6/2014 3:08:51 PM	5488 (0x1570)
Rule Criteria is: <UpdateXML xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" Name="SMS_SoftwareUpdate" LocaleId="1033"><UpdateXMLDescriptionItems><UpdateXMLDescriptionItem PropertyName="_Product" UIPropertyName=""><MatchRules><string>'Product:a38c835c-2950-4e87-86cc-6911a52c34a3'</string></MatchRules></UpdateXMLDescriptionItem><UpdateXMLDescriptionItem PropertyName="IsSuperseded" UIPropertyName=""><MatchRules><string>false</string></MatchRules></UpdateXMLDescriptionItem><UpdateXMLDescriptionItem PropertyName="_UpdateClassification" UIPropertyName=""><MatchRules><string>'UpdateClassification:e0789628-ce08-4437-be74-2495b842f43b'</string></MatchRules></UpdateXMLDescriptionItem></UpdateXMLDescriptionItems></UpdateXML>			
SMS_RULE_ENGINE	2/6/2014 3:08:51 PM	5488 (0x1570)	
Inserting PropertyName:_Product, PropertyValue:'Product:a38c835c-2950-4e87-86cc-6911a52c34a3'	SMS_RULE_ENGINE	2/6/2014 3:08:51 PM	5488 (0x1570)
Inserting PropertyName:IsSuperseded, PropertyValue:false	SMS_RULE_ENGINE	2/6/2014 3:08:51 PM	5488 (0x1570)
Inserting PropertyName:_UpdateClassification, PropertyValue:'UpdateClassification:e0789628-ce08-4437-be74-2495b842f43b'	SMS_RULE_ENGINE	2/6/2014 3:08:51 PM	5488 (0x1570)
Query to run is: select CI_ID from dbo.fn_ListUpdateCis(1033) ci~where IsExpired=0~ and (IsSuperseded=0)~ and (CI_ID in (select CI_ID from v_Categories_All where CategoryInstance_UniqueID in (N'Product:a38c835c-2950-4e87-86cc-6911a52c34a3'))~ and (CI_ID in (select CI_ID from v_Categories_All where CategoryInstance_UniqueID in (N'UpdateClassification:e0789628-ce08-4437-be74-2495b842f43b')))	SMS_RULE_ENGINE	2/6/2014 3:08:51 PM	5488 (0x1570)
Rule resulted in a total of 1 updates	SMS_RULE_ENGINE	2/6/2014 3:08:51 PM	5488 (0x1570)
Evaluation Resultant XML is: <EvaluationResultXML xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"><DefinitionUpdates/><CI_IDs><CI_ID>4514</CI_ID></CI_IDs></EvaluationResultXML>	SMS_RULE_ENGINE	2/6/2014 3:08:51 PM	5488 (0x1570)

**RuleEngine.log showing Download being initiated for actionable updates:**

Enforcing Content Download Action	SMS_RULE_ENGINE	2/6/2014 3:08:51 PM	5488 (0x1570)
Download Rule Action XML is: <ContentActionXML xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"><PackageID>CS100006</PackageID><ContentLocales><Locale>Locale:9</Locale><Locale>Locale:0</Locale></ContentLocales><ContentSources><Source Name="Internet" Order="1"/><Source Name="WSUS" Order="2"/><Source Name="UNC" Order="3" Location=""></Source Name="UNC" Order="3" Location=""></ContentSources></ContentActionXML>	SMS_RULE_ENGINE	2/6/2014 3:08:51 PM	5488 (0x1570)
Criteria Filter Result XML is: <EvaluationResultXML xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema"><DefinitionUpdates/><CI_IDs><CI_ID>4514</CI_ID></CI_IDs></EvaluationResultXML>	SMS_RULE_ENGINE	2/6/2014 3:08:51 PM	5488 (0x1570)
1 update(s) need to be downloaded in package "CS100006" (\\CS1SITE\SOURCE\Updates\EPDefinitions)	SMS_RULE_ENGINE	2/6/2014 3:08:51 PM	5488 (0x1570)
List of update(s) which match the content rule criteria = {4514}	SMS_RULE_ENGINE	2/6/2014 3:08:51 PM	5488 (0x1570)
Downloading contents (count = 34) for UpdateID 4514	SMS_RULE_ENGINE	2/6/2014 3:08:51 PM	5488 (0x1570)
List of update content(s) which match the content rule criteria = {737,738,739,740,741,742,2182,2183,2184,2185,2186,2187,2188,2189,3047,3048,3187,3188,3189,3190,3191,3192,3545,3546,3547,3548,3549,3550,3551,3552,3553,3554,3555,3556}	SMS_RULE_ENGINE	2/6/2014 3:08:51 PM	5488 (0x1570)
Contents 737 is already present in the package "CS100006". Skipping download.	SMS_RULE_ENGINE	2/6/2014 3:08:51 PM	5488 (0x1570)

Contents 738 is already present in the package "CS100006". Skipping download. PM 5488 (0x1570)	SMS_RULE_ENGINE	2/6/2014 3:08:51
1 of 1 updates are downloaded and will be added to the Deployment. 5488 (0x1570)	SMS_RULE_ENGINE	2/6/2014 3:08:51 PM

**RuleEngine.log showing creation of Update Group and Deployment:**

We need to create a new UpdateGroup/Deployment	SMS_RULE_ENGINE	2/6/2014 3:08:51 PM	5488 (0x1570)
Associated Update Group: Scopeld_FC8FCC38-4BB1-4245-92F5-9CE841775019/AuthList_4d3480d5-de12-4864-b872-187479e2b381 with RBAC Scope SMS00UNA	SMS_RULE_ENGINE	2/6/2014 3:08:55 PM	5488 (0x1570)

The following examples illustrate the Update Group creation process:

**SMSDBMON.log:**

RCV: INSERT on CI_ConfigurationItems for CINotify_iud [16777275 ][66146]	SMS_DATABASE_NOTIFICATION_MONITOR
2/6/2014 3:09:01 PM 3484 (0x0D9C)	
RCV: INSERT on CI_ConfigurationItemRelations_Flat for CI_ConfigurationItemRelations_Flat_From_iud [16777275 ][66148]	SMS_DATABASE_NOTIFICATION_MONITOR
2/6/2014 3:09:01 PM 3484 (0x0D9C)	
RCV: INSERT on CI_ConfigurationItemRelations_Flat for CI_ConfigurationItemRelations_Flat_From_iud [16777275 ][66149]	SMS_DATABASE_NOTIFICATION_MONITOR
2/6/2014 3:09:01 PM 3484 (0x0D9C)	
SND: Dropped E:\ConfigMgr\inboxes\objmgr.box\16777275.CIN [66148]	SMS_DATABASE_NOTIFICATION_MONITOR
2/6/2014 3:09:01 PM 3484 (0x0D9C)	
SND: Dropped E:\ConfigMgr\inboxes\objmgr.box\16777275.CIN [66149]	SMS_DATABASE_NOTIFICATION_MONITOR
2/6/2014 3:09:01 PM 3484 (0x0D9C)	

**ObjReplMgr.log:**

File notification triggered.	SMS_OBJECT_REPLICATION_MANAGER	2/6/2014 3:09:01 PM	6868 (0x1AD4)
***** Processing AuthorizationList Scopeld_FC8FCC38-4BB1-4245-92F5-9CE841775019/AuthList_4d3480d5-de12-4864-b872-187479e2b381 *****	SMS_OBJECT_REPLICATION_MANAGER	2/6/2014 3:09:06 PM	6868 (0x1AD4)
Deleting notification file E:\ConfigMgr\inboxes\objmgr.box\16777275.CIN	SMS_OBJECT_REPLICATION_MANAGER	2/6/2014 3:09:06 PM	6868 (0x1AD4)
Added CI with CI_ID=4514 to the deployment	SMS_OBJECT_REPLICATION_MANAGER	2/6/2014 3:09:06 PM	6868 (0x1AD4)
Created file trigger for E:\ConfigMgr\inboxes\objmgr.box\16777228.CIA	SMS_OBJECT_REPLICATION_MANAGER	2/6/2014 3:09:08 PM	6868 (0x1AD4)
Created file trigger for E:\ConfigMgr\inboxes\objmgr.box\16777228.CIV	SMS_OBJECT_REPLICATION_MANAGER	2/6/2014 3:09:08 PM	6868 (0x1AD4)
Successfully processed AuthorizationList Scopeld_FC8FCC38-4BB1-4245-92F5-9CE841775019/AuthList_4d3480d5-de12-4864-b872-187479e2b381	SMS_OBJECT_REPLICATION_MANAGER	2/6/2014 3:09:08 PM	6868 (0x1AD4)
Set last row version for Configuration Item to 0x000000000487EA9	SMS_OBJECT_REPLICATION_MANAGER	2/6/2014 3:09:08 PM	6868 (0x1AD4)

The following example shows the Deployment creation process:

**SMSDBMON.log:**

RCV: INSERT on CI_CIAssignments for CIAssignmentNotify_iu [16777228 ][66190]	SMS_DATABASE_NOTIFICATION_MONITOR
2/6/2014 3:09:01 PM 3484 (0x0D9C)	
SND: Dropped E:\ConfigMgr\inboxes\objmgr.box\16777228.CIA [66190]	SMS_DATABASE_NOTIFICATION_MONITOR
2/6/2014 3:09:01 PM 3484 (0x0D9C)	

**ObjReplMgr.log:**

+++Begin processing changed CIA objects	SMS_OBJECT_REPLICATION_MANAGER	2/6/2014 3:09:13 PM	6868 (0x1AD4)
***** Processing Update Group Assignment {2ba787b6-4ee9-4b33-b0ff-8663d181c84d} *****	SMS_OBJECT_REPLICATION_MANAGER	2/6/2014 3:09:13 PM	6868 (0x1AD4)

```

Deleting notification file E:\ConfigMgr\inbox\objmgr.box\16777228.CIA SMS_OBJECT_REPLICATION_MANAGER
2/6/2014 3:09:13 PM 6868 (0x1AD4)
CI Assignment {2ba787b6-4ee9-4b33-b0ff-8663d181c84d} has 1 Targeted CI(s) SMS_OBJECT_REPLICATION_MANAGER
2/6/2014 3:09:13 PM 6868 (0x1AD4)
PolicyID {2ba787b6-4ee9-4b33-b0ff-8663d181c84d} PolicyVersion 1.00 PolicyHash
SHA256:0C6D50CBFB36750CCA381B61E014A6C55D821001487C824F9112DAA1C64BAD32
SMS_OBJECT_REPLICATION_MANAGER 2/6/2014 3:09:13 PM 6868 (0x1AD4)
Notifying policy provider about changes in policy content/targeting SMS_OBJECT_REPLICATION_MANAGER 2/6/2014 3:09:13
PM 6868 (0x1AD4)
Successfully created policy for CI Assignment {2ba787b6-4ee9-4b33-b0ff-8663d181c84d}
SMS_OBJECT_REPLICATION_MANAGER 2/6/2014 3:09:13 PM 6868 (0x1AD4)
Notifying policy provider about changes in policy content/targeting SMS_OBJECT_REPLICATION_MANAGER 2/6/2014 3:09:13
PM 6868 (0x1AD4)
Successfully updated Policy Targeting for CI Assignment {2ba787b6-4ee9-4b33-b0ff-8663d181c84d}
SMS_OBJECT_REPLICATION_MANAGER 2/6/2014 3:09:13 PM 6868 (0x1AD4)
Found file trigger for E:\ConfigMgr\inbox\objmgr.box\16777228.CIV SMS_OBJECT_REPLICATION_MANAGER 2/6/2014 3:09:13
PM 6868 (0x1AD4)
Assigned CIs: [ 16777275 ] SMS_OBJECT_REPLICATION_MANAGER 2/6/2014 3:09:13 PM 6868 (0x1AD4)
Begin processing Assigned CI: [16777275] SMS_OBJECT_REPLICATION_MANAGER 2/6/2014 3:09:13 PM 6868 (0x1AD4)
Creating VersionInfo policy for CI 16777275 SMS_OBJECT_REPLICATION_MANAGER 2/6/2014 3:09:13 PM 6868 (0x1AD4)
Creating VersionInfo policy Scopeld_FC8FCC38-4BB1-4245-92F5-9CE841775019/AuthList_4d3480d5-de12-4864-b872-
187479e2b381/VI SMS_OBJECT_REPLICATION_MANAGER 2/6/2014 3:09:13 PM 6868 (0x1AD4)
16777275 Referenced CIs: [ 1395 1396 1397 1398 1399 1400 1401 3013 3014 3015 3016 3017 3018 3019 3020 3021 3959 3960 3961
4112 4113 4114 4115 4116 4117 4118 4502 4503 4504 4505 4506 4507 4508 4509 4510 4511 4512 4513 4514 ]
SMS_OBJECT_REPLICATION_MANAGER 2/6/2014 3:09:13 PM 6868 (0x1AD4)
VersionInfo policy for CI 16777275 is Machine type SMS_OBJECT_REPLICATION_MANAGER 2/6/2014 3:09:17 PM 6868
(0x1AD4)
PolicyID Scopeld_FC8FCC38-4BB1-4245-92F5-9CE841775019/AuthList_4d3480d5-de12-4864-b872-187479e2b381/VI PolicyVersion
1.00 PolicyHash SHA256:01BECBBF2B3EE56BD5B0742A04404C1C895A4C87B6915D55078AB157FEBA1E0F
SMS_OBJECT_REPLICATION_MANAGER 2/6/2014 3:09:17 PM 6868 (0x1AD4)
Notifying policy provider about changes in policy content/targeting SMS_OBJECT_REPLICATION_MANAGER 2/6/2014 3:09:17
PM 6868 (0x1AD4)
Updated dependent policy references to CIA {2ba787b6-4ee9-4b33-b0ff-8663d181c84d}SMS_OBJECT_REPLICATION_MANAGER
2/6/2014 3:09:17 PM 6868 (0x1AD4)
STATMSG: ID=5800 SEV=I LEV=M SOURCE="SMS Server" COMP="SMS_OBJECT_REPLICATION_MANAGER"
SYS=PS1SITE.CONTOSO.COM SITE=PS1 PID=6176 TID=6868 GMTDATE=Thu Feb 06 20:09:17.989 2014 ISTR0="ADR_Test" ISTR1=""
ISTR2="" ISTR3="" ISTR4="" ISTR5="" ISTR6="" ISTR7="" ISTR8="" ISTR9="" NUMATTRS=1 AID0=414 AVAL0="{2ba787b6-4ee9-4b33-
b0ff-8663d181c84d}" SMS_OBJECT_REPLICATION_MANAGER 2/6/2014 3:09:17 PM 6868 (0x1AD4)
Successfully updated CRCs for CI Assignment {2ba787b6-4ee9-4b33-b0ff-8663d181c84d}SMS_OBJECT_REPLICATION_MANAGER
2/6/2014 3:09:18 PM 6868 (0x1AD4)
Successfully processed Update Group Assignment {2ba787b6-4ee9-4b33-b0ff-8663d181c84d}
SMS_OBJECT_REPLICATION_MANAGER 2/6/2014 3:09:18 PM 6868 (0x1AD4)
Set last row version for CI Assignment to 0x000000000487EB6 SMS_OBJECT_REPLICATION_MANAGER 2/6/2014 3:09:18
PM 6868 (0x1AD4)
+++Completed processing changed CIA objects SMS_OBJECT_REPLICATION_MANAGER 2/6/2014 3:09:18 PM 6868
(0x1AD4)

```

The following example shows the Policy creation process:

**SMSDBMON.log:**

```

RCV: INSERT on CrpChange_Notify for CrpChange_Notify_ins [15 ][66199] SMS_DATABASE_NOTIFICATION_MONITOR
2/6/2014 3:09:16 PM 3484 (0x0D9C)
RCV: INSERT on RBAC_ChangeNotification for Rbac_Sync_ChangeNotification [399 ][66200]
SMS_DATABASE_NOTIFICATION_MONITOR 2/6/2014 3:09:16 PM 3484 (0x0D9C)
SND: Dropped E:\ConfigMgr\inbox\policy\policytargeteval\15.CRP [66199] SMS_DATABASE_NOTIFICATION_MONITOR
2/6/2014 3:09:16 PM 3484 (0x0D9C)

```

SND: Dropped E:\ConfigMgr\inboxes\hman.box\399.RBC [66200] SMS\_DATABASE\_NOTIFICATION\_MONITOR 2/6/2014 3:09:16 PM 3484 (0x0D9C)

RCV: INSERT on PolicyAssignmentChg\_Notify for PolicyAssignmentChg\_Notify\_iu [16787957 ][66201] SMS\_DATABASE\_NOTIFICATION\_MONITOR 2/6/2014 3:09:26 PM 3484 (0x0D9C)

SND: Dropped E:\ConfigMgr\inboxes\policypv.box\policytargeteval\16787957.PAC [66201] SMS\_DATABASE\_NOTIFICATION\_MONITOR 2/6/2014 3:09:26 PM 3484 (0x0D9C)

RCV: INSERT on PolicyAssignmentChg\_Notify for PolicyAssignmentChg\_Notify\_iu [16787957 ][66202] SMS\_DATABASE\_NOTIFICATION\_MONITOR 2/6/2014 3:09:41 PM 3484 (0x0D9C)

RCV: UPDATE on PolicyAssignmentChg\_Notify for PolicyAssignmentChg\_Notify\_iu [16787957 ][66203] SMS\_DATABASE\_NOTIFICATION\_MONITOR 2/6/2014 3:09:41 PM 3484 (0x0D9C)

SND: Dropped E:\ConfigMgr\inboxes\policypv.box\policytargeteval\16787957.PAC [66202] SMS\_DATABASE\_NOTIFICATION\_MONITOR 2/6/2014 3:09:41 PM 3484 (0x0D9C)

SND: Dropped E:\ConfigMgr\inboxes\policypv.box\policytargeteval\16787957.PAC [66203] SMS\_DATABASE\_NOTIFICATION\_MONITOR 2/6/2014 3:09:41 PM 3484 (0x0D9C)

### PolicyPv.log

File notification triggered. SMS\_POLICY\_PROVIDER 2/6/2014 3:09:26 PM 2308 (0x0904)

--Process Collection Changes SMS\_POLICY\_PROVIDER 2/6/2014 3:09:31 PM 5860 (0x16E4)

Building Collection Change List from Collection Change Notification files SMS\_POLICY\_PROVIDER 2/6/2014 3:09:31 PM 5860 (0x16E4)

--Process Collection Member Changes SMS\_POLICY\_PROVIDER 2/6/2014 3:09:31 PM 5860 (0x16E4)

Building Collection Change List from Collection Member Notification files SMS\_POLICY\_PROVIDER 2/6/2014 3:09:31 PM 5860 (0x16E4)

--Handle PolicyAssignment Resigning SMS\_POLICY\_PROVIDER 2/6/2014 3:09:31 PM 5860 (0x16E4)

Found the certificate that matches the SHA1 hash. SMS\_POLICY\_PROVIDER 2/6/2014 3:09:31 PM 5860 (0x16E4)

Completed batch with beginning PADBID = 16787957 ending PADBID = 16787958. SMS\_POLICY\_PROVIDER 2/6/2014 3:09:31 PM 5860 (0x16E4)

--Process Policy Changes SMS\_POLICY\_PROVIDER 2/6/2014 3:09:31 PM 5860 (0x16E4)

Found some Policy changes, returning New LastRowversion=0x0000000000487EB7 SMS\_POLICY\_PROVIDER 2/6/2014 3:09:31 PM 5860 (0x16E4)

Processing Updated Policies SMS\_POLICY\_PROVIDER 2/6/2014 3:09:31 PM 5860 (0x16E4)

Building Collection Change List from New and Targeting Changed Policies SMS\_POLICY\_PROVIDER 2/6/2014 3:09:31 PM 5860 (0x16E4)

--Update Policy Targeting Map SMS\_POLICY\_PROVIDER 2/6/2014 3:09:31 PM 5860 (0x16E4)

\*\*\*\* Evaluating Collection 15 for targeting changes \*\*\*\* SMS\_POLICY\_PROVIDER 2/6/2014 3:09:31 PM 5860 (0x16E4)

--Process Policy Targeting Map SMS\_POLICY\_PROVIDER 2/6/2014 3:09:31 PM 5860 (0x16E4)

\*\*\*\* Process notification table to update resultant targeting table \*\*\*\* SMS\_POLICY\_PROVIDER 2/6/2014 3:09:31 PM 5860 (0x16E4)

--Process Targeting and Collection Membership changes SMS\_POLICY\_PROVIDER 2/6/2014 3:09:31 PM 5860 (0x16E4)

Updating Policy Map SMS\_POLICY\_PROVIDER 2/6/2014 3:09:31 PM 5860 (0x16E4)

--UpdateMDMUserTargetingForUser SMS\_POLICY\_PROVIDER 2/6/2014 3:09:31 PM 5860 (0x16E4)

Start Update MDM User Targeting For User SMS\_POLICY\_PROVIDER 2/6/2014 3:09:31 PM 5860 (0x16E4)

--UpdatePolicyMapForPA SMS\_POLICY\_PROVIDER 2/6/2014 3:09:31 PM 5860 (0x16E4)

Found 16787957.PAC SMS\_POLICY\_PROVIDER 2/6/2014 3:09:31 PM 5860 (0x16E4)

Adding to delete list: E:\ConfigMgr\inboxes\policypv.box\policytargeteval\16787957.PAC SMS\_POLICY\_PROVIDER 2/6/2014 3:09:31 PM 5860 (0x16E4)

Updating ResPolicyMap SMS\_POLICY\_PROVIDER 2/6/2014 3:09:31 PM 5860 (0x16E4)

### RuleEngine.log showing Rule Processing completion:

CRuleHandler: Rule 1 Successfully Applied! SMS\_RULE\_ENGINE 2/6/2014 3:08:55 PM 5488 (0x1570)

Updated Success Information for Rule: 1 SMS\_RULE\_ENGINE 2/6/2014 3:08:55 PM 5488 (0x1570)




---

## DEPLOYMENT EVALUATION AND UPDATE INSTALLATION ON CLIENTS

After the deployment and the deployment policy has been created on the server, clients receive the policy on the next policy evaluation cycle. Before reviewing the Deployment Evaluation process, it's important to find the Deployment Unique ID of the deployment by adding the Deployment Unique ID column in the console. For the deployment we're going to focus on in the following log excerpts, the Deployment Unique ID is B040D195-8FA8-48D3-953F-17E878DAB23D.

### SUG4

Icon	Name	Deployment Type	Deployment Unique ID
	Microsoft Software Updates - ...	Group	{B040D195-8FA8-48D3-953F-17E878DAB23D}

Policy Agent receives the policy on manual policy retrieval or on schedule:

#### PolicyAgent.log:

```
Initializing download of policy 'CCM_Policy_Policy5.PolicyID="{B040D195-8FA8-48D3-953F-17E878DAB23D}",PolicySource="SMS:PR1",PolicyVersion="1.00"' from
'http://PR1SITE.CONTOSO.COM/SMS_MP/.sms_pol?{B040D195-8FA8-48D3-953F-17E878DAB23D}.SHA256:0EE489DB3036BE80BB43676340249A254278BEBDDD80B6004C11FF10F12BC9D6'
PolicyAgent_ReplyAssignments 2/9/2014 7:05:01 PM 2572 (0x0AOC)
Download of policy CCM_Policy_Policy5.PolicyID="{B040D195-8FA8-48D3-953F-17E878DAB23D}",PolicySource="SMS:PR1",PolicyVersion="1.00" completed (DTS Job ID: {D53DAB18-ED97-4373-A3BE-3FBA5DB3C6C6}) PolicyAgent_PolicyDownload 2/9/2014 7:05:01 PM 2572 (0x0AOC)
```

#### PolicyEvaluator.log:

```
Initializing download of policy 'CCM_Policy_Policy5.PolicyID="{B040D195-8FA8-48D3-953F-17E878DAB23D}",PolicySource="SMS:PR1",PolicyVersion="1.00"' from
'http://PR1SITE.CONTOSO.COM/SMS_MP/.sms_pol?{B040D195-8FA8-48D3-953F-17E878DAB23D}.SHA256:0EE489DB3036BE80BB43676340249A254278BEBDDD80B6004C11FF10F12BC9D6'
PolicyAgent_ReplyAssignments 2/9/2014 7:05:01 PM 2572 (0x0AOC)
Download of policy CCM_Policy_Policy5.PolicyID="{B040D195-8FA8-48D3-953F-17E878DAB23D}",PolicySource="SMS:PR1",PolicyVersion="1.00" completed (DTS Job ID: {D53DAB18-ED97-4373-A3BE-3FBA5DB3C6C6}) PolicyAgent_PolicyDownload 2/9/2014 7:05:01 PM 2572 (0x0AOC)
```

After the policy is evaluated, the scheduler for the deadline is evaluated. This is done by the scheduler component. In this case, deadline randomization is disabled in Computer Agent client settings. Therefore, the deployment evaluation will be initiated on deadline and without randomization.

#### Scheduler.log:

```
Initialized trigger ("3E692B0000080000") for schedule 'Machine/DEADLINE:{B040D195-8FA8-48D3-953F-17E878DAB23D}':
Conditions=1 with deadline 4320 minutes
Allow randomization override=1
HasMissedOccurrence=FALSE
ScheduleLoadedTime="02/09/2014 19:05:947"
LastFireTime="00/00/00 00:00:00"
CurrentTime="02/09/2014 19:05:947" Scheduler 2/9/2014 7:05:01 PM 3260 (0x0CBC)
```

```
Processing trigger '3E692B0000080000' for scheduler 'Machine/DEADLINE:{B040D195-8FA8-48D3-953F-17E878DAB23D}'.
MaxRandomDelay = 120, MissedOccur = 0, RandomizeEvenIfMissed = 1, PreventRandomizationInducedMisses = 0 Scheduler
2/9/2014 7:05:01 PM 3260 (0x0CBC)
Randomization is disabled in client settings and this schedule is set to honor client setting. Scheduler 2/9/2014 7:05:01
PM 3260 (0x0CBC)
SMSTrigger '3E692B0000080000' for scheduler 'Machine/DEADLINE:{B040D195-8FA8-48D3-953F-17E878DAB23D}' will fire at
02/09/2014 07:15:00 PM without randomization. Scheduler 2/9/2014 7:05:01 PM 3260 (0x0CBC)
```

At the scheduled deadline, Scheduler notifies Updates Deployment Agent to initiate the Deployment Evaluation process.

#### Scheduler.log:

```
Sending message for schedule 'Machine/DEADLINE:{B040D195-8FA8-48D3-953F-17E878DAB23D}' (Target:
'direct:UpdatesDeploymentAgent', Name: '') Scheduler 2/9/2014 7:15:00 PM 3216 (0x0C90)
SMSTrigger '3E692B0000080000' (Schedule ID: 'Machine/DEADLINE:{B040D195-8FA8-48D3-953F-17E878DAB23D}', Message Name:
'', Target: 'direct:UpdatesDeploymentAgent') will never fire again. Scheduler 2/9/2014 7:15:00 PM 3216 (0x0C90)
```

#### UpdatesDeployment.log:

```
Message received: '<?xml version='1.0' ?>
<CIAssignmentMessage MessageType='EnforcementDeadline'>
  <AssignmentID>{B040D195-8FA8-48D3-953F-17E878DAB23D}</AssignmentID>
</CIAssignmentMessage>' UpdatesDeploymentAgent 2/9/2014 7:15:00 PM 3216 (0x0C90)
```

Updates Deployment Agent starts the Deployment Evaluation process by requesting a Software Update scan to make sure that the deployed updates are still applicable.

#### UpdatesDeploymentAgent.log:

```
Assignment {B040D195-8FA8-48D3-953F-17E878DAB23D} has total CI = 3 UpdatesDeploymentAgent 2/9/2014 7:15:00
PM 3216 (0x0C90)
Deadline received for assignment ({B040D195-8FA8-48D3-953F-17E878DAB23D}) UpdatesDeploymentAgent
2/9/2014 7:15:00 PM 3216 (0x0C90)
Detection job ({99ADA372-0738-44E4-9C4D-EBA30F23E9FD}) started for assignment ({B040D195-8FA8-48D3-953F-17E878DAB23D})
UpdatesDeploymentAgent 2/9/2014 7:15:00 PM 3216 (0x0C90)
```

#### UpdatesHandler.log:

```
Successfully initiated scan for job ({99ADA372-0738-44E4-9C4D-EBA30F23E9FD}). UpdatesHandler 2/9/2014 7:15:04 PM
3696 (0x0E70)
Scan completion received for job ({99ADA372-0738-44E4-9C4D-EBA30F23E9FD}). UpdatesHandler 2/9/2014 7:15:04 PM
3696 (0x0E70)
Initial scan completed for the job ({99ADA372-0738-44E4-9C4D-EBA30F23E9FD}). UpdatesHandler 2/9/2014 7:15:04 PM
3696 (0x0E70)
Evaluating status of the updates for the job ({99ADA372-0738-44E4-9C4D-EBA30F23E9FD}). UpdatesHandler 2/9/2014 7:15:04
PM 3696 (0x0E70)
CompleteJob - Job ({99ADA372-0738-44E4-9C4D-EBA30F23E9FD}) removed from job manager list. UpdatesHandler
2/9/2014 7:15:04 PM 3696 (0x0E70)
```

At this point the scan request is handled by Scan Agent component. Scan Agent calls **WUAHandler** to perform a scan and then hands the results back to Updates Handler and Updates Deployment Agent. For more information about the scan process, see [Software Update Scan on Clients](#). After the scan is completed, Updates Deployment Agent is notified.

#### UpdatesDeploymentAgent.log:

```
DetectJob completion received for assignment ({B040D195-8FA8-48D3-953F-17E878DAB23D}) UpdatesDeploymentAgent
2/9/2014 7:15:04 PM 3696 (0x0E70)
Making updates available for assignment ({B040D195-8FA8-48D3-953F-17E878DAB23D}) UpdatesDeploymentAgent
2/9/2014 7:15:04 PM 3696 (0x0E70)
```

```
Update (Site_D3A5F7EA-25D4-4C6B-B47C-C74997522A76/SUM_e06056e3-0199-4c68-8ac3-bdddf356a0a) Name (Security Update for Windows Server 2008 R2 x64 Edition (KB2698365)) ArticleID (2698365) added to the targeted list of deployment ({B040D195-8FA8-48D3-953F-17E878DAB23D}) UpdatesDeploymentAgent 2/9/2014 7:15:04 PM 3696 (0x0E70)
Update (Site_D3A5F7EA-25D4-4C6B-B47C-C74997522A76/SUM_ada7cf51-66b0-4a00-b37b-68d569d6ff8b) Name (Security Update for Windows Server 2008 R2 x64 Edition (KB2712808)) ArticleID (2712808) added to the targeted list of deployment ({B040D195-8FA8-48D3-953F-17E878DAB23D}) UpdatesDeploymentAgent 2/9/2014 7:15:04 PM 3696 (0x0E70)
Update (Site_D3A5F7EA-25D4-4C6B-B47C-C74997522A76/SUM_3cbcf577-5139-49b8-afe8-620af5c52f95) Name (Security Update for Windows Server 2008 R2 x64 Edition (KB2705219)) ArticleID (2705219) added to the targeted list of deployment ({B040D195-8FA8-48D3-953F-17E878DAB23D}) UpdatesDeploymentAgent 2/9/2014 7:15:04 PM 3696 (0x0E70)
```

At this point, Updates Deployment Agent raises State Messages for the deployment to update the current Evaluation and Compliance state.

#### UpdatesDeploymentAgent.log:

```
Raised assignment ({B040D195-8FA8-48D3-953F-17E878DAB23D}) state message successfully. TopicType = Evaluate, StateId = 2, StateName = ASSIGNMENT_EVALUATE_SUCCESS UpdatesDeploymentAgent 2/9/2014 7:15:04 PM 3696 (0x0E70)
Raised assignment ({B040D195-8FA8-48D3-953F-17E878DAB23D}) state message successfully. TopicType = Compliance, Signature = 5e176837, IsCompliant = False UpdatesDeploymentAgent 2/9/2014 7:15:04 PM 3696 (0x0E70)
```

Updates Deployment Agent now starts a job to download the software update files from the Distribution Point.

#### UpdatesDeploymentAgent.log:

```
DownloadCIContents Job ({C531FD04-FADA-4F75-A399-EEA2D3EDB56C}) started for assignment ({B040D195-8FA8-48D3-953F-17E878DAB23D}) UpdatesDeploymentAgent
Progress received for assignment ({B040D195-8FA8-48D3-953F-17E878DAB23D}) UpdatesDeploymentAgent
Update (Site_D3A5F7EA-25D4-4C6B-B47C-C74997522A76/SUM_e06056e3-0199-4c68-8ac3-bdddf356a0a) Progress: Status = ciStateDownloading, PercentComplete = 0, Result = 0x0 UpdatesDeploymentAgent
Update (Site_D3A5F7EA-25D4-4C6B-B47C-C74997522A76/SUM_ada7cf51-66b0-4a00-b37b-68d569d6ff8b) Progress: Status = ciStateDownloading, PercentComplete = 0, Result = 0x0 UpdatesDeploymentAgent
Update (Site_D3A5F7EA-25D4-4C6B-B47C-C74997522A76/SUM_3cbcf577-5139-49b8-afe8-620af5c52f95) Progress: Status = ciStateDownloading, PercentComplete = 0, Result = 0x0 UpdatesDeploymentAgent
```

#### UpdatesHandler.log:

```
Initiating download for the job ({C531FD04-FADA-4F75-A399-EEA2D3EDB56C}).UpdatesHandler
Update Id = 3cbcf577-5139-49b8-afe8-620af5c52f95, State = StateDownloading, Result = 0x0 UpdatesHandler
Update Id = ada7cf51-66b0-4a00-b37b-68d569d6ff8b, State = StateDownloading, Result = 0x0 UpdatesHandler
Update Id = e06056e3-0199-4c68-8ac3-bdddf356a0a, State = StateDownloading, Result = 0x0 UpdatesHandler
Timeout Options: Priority = 2, DPLocality = 1048578, Location = 604800, Download = 864000, PerDPInactivity = 0, TotalInactivityTimeout = 0, bUseBranchCache = True, bPersistOnWriteFilterDevices = True, bOverrideServiceWindow = False
UpdatesHandler
```

Updates Handler initiates the download request from Content Access Service for the three actionable updates listed above. Note that the download job is started for the child update in the bundle, and the Content ID is logged.

#### UpdatesHandler.log:

```
Bundle update (3cbcf577-5139-49b8-afe8-620af5c52f95) is requesting download from child updates for action (INSTALL)
UpdatesHandler
Content Text = <Content ContentId="fbb5724a-aa0f-47f9-908a-47068fd8ad6f" Version="1"><FileContent Name="windows6.1-kb2705219-v2-x64.cab" Hash="8E8E0175D46B5A8D52C4856FA3D282FAA12ACD63" HashAlgorithm="SHA1" Size="199093"/></Content>
Bundle update (ada7cf51-66b0-4a00-b37b-68d569d6ff8b) is requesting download from child updates for action (INSTALL)
UpdatesHandler
```

```
Content Text = <Content ContentId="3e9b1132-9ccd-439d-b32a-5cefd19735d1" Version="1"><FileContent Name="windows6.1-kb2712808-x64.cab" Hash="060B60401B3DE3DCE053A68C65E9EB050874EB80" HashAlgorithm="SHA1" Size="805071"/></Content>
```

Bundle update (e06056e3-0199-4c68-8ac3-bdddf356a0a) is requesting download from child updates for action (INSTALL)  
UpdatesHandler

```
Content Text = <Content ContentId="d2a9ee23-9cab-4843-b040-e2da1cc167e9" Version="1"><FileContent Name="windows6.1-kb2698365-x64.cab" Hash="BF20BB36FC73COD1F53EA1E635B8AA46C71D7B1F" HashAlgorithm="SHA1" Size="2496330"/></Content>
```

Content Access Service starts a download job for each of these updates and creates a Content Transfer Manager (CTM) job. A CTM Job is created for each update separately, and CAS.log entries look similar to the following for each update:

#### CAS.log:

```
Requesting content fbb5724a-aa0f-47f9-908a-47068fd8ad6f.1, size(KB) 0, under context System with priority Medium
ContentAccess 2/9/2014 7:15:05 PM 3216 (0x0C90)
Created and initialized a DownloadContentRequest ContentAccess 2/9/2014 7:15:05 PM 3216 (0x0C90)
Target location for content fbb5724a-aa0f-47f9-908a-47068fd8ad6f.1 is C:\Windows\ccmcache\1 ContentAccess
2/9/2014 7:15:05 PM 3216 (0x0C90)
CDownloadManager::RequestDownload fbb5724a-aa0f-47f9-908a-47068fd8ad6f.1.System ContentAccess 2/9/2014 7:15:05
PM 3216 (0x0C90)
Submitted CTM job {E0452CF4-5B04-4A1A-B8EB-10B11B063249} to download Content fbb5724a-aa0f-47f9-908a-47068fd8ad6f.1
under context System ContentAccess 2/9/2014 7:15:05 PM 3216 (0x0C90)
Successfully created download request {856FA4CA-D02A-4E2C-841E-841ED3C7EC01} for content fbb5724a-aa0f-47f9-908a-
47068fd8ad6f.1 ContentAccess 2/9/2014 7:15:05 PM 3216 (0x0C90)
Created and submitted a new Content Request for fbb5724a-aa0f-47f9-908a-47068fd8ad6f.1.System ContentAccess
2/9/2014 7:15:05 PM 3216 (0x0C90)
```

Content Transfer Manager now starts working on the download job. It first requests the location for the content that must be downloaded. This location request is handled by Location Services, which sends the location request to the management point, obtains the location response, and then hands it back to the Content Transfer Manager.

#### ContentTransferManager.log:

```
Starting CTM job {E0452CF4-5B04-4A1A-B8EB-10B11B063249}. ContentTransferManager 2/9/2014 7:15:05 PM 3216
(0x0C90)
CTM job {E0452CF4-5B04-4A1A-B8EB-10B11B063249} entered phase CCM_DOWNLOADSTATUS_DOWNLOADING_DATA
ContentTransferManager 2/9/2014 7:15:05 PM 3216 (0x0C90)
Queued location request '{C56C01F2-2388-4710-BF3B-A526DB40E35F}' for CTM job '{E0452CF4-5B04-4A1A-B8EB-10B11B063249}'.
ContentTransferManager 2/9/2014 7:15:05 PM 3216 (0x0C90)
CCTMJob::EvaluateState(JobID={E0452CF4-5B04-4A1A-B8EB-10B11B063249}, State=RequestedLocations) ContentTransferManager
2/9/2014 7:15:05 PM 3216 (0x0C90)
```

#### LocationServices.log:

```
Created filter for LS request {C56C01F2-2388-4710-BF3B-A526DB40E35F}. LocationServices 2/9/2014 7:15:05 PM 3216
(0x0C90)
ContentLocationReply : <ContentLocationReply SchemaVersion="1.00"><ContentInfo
PackageFlags="0"><ContentHashValues/></ContentInfo><Sites><Site><MPSite SiteCode="PR1" MasterSiteCode="PR1"
SiteLocality="LOCAL" IISPreferredPort="80" IISSSLPreferredPort="443"/><LocationRecords><LocationRecord><URL
Name="http://PR1SITE.CONTOSO.COM/SMS_DP_SMSPKG$/fbb5724a-aa0f-47f9-908a-47068fd8ad6f"
Signature="http://PR1SITE.CONTOSO.COM/SMS_DP_SMSGIG$/fbb5724a-aa0f-47f9-908a-47068fd8ad6f.1.tar"/><ADSite
Name="Default-First-Site-Name"/><IPSubnets><IPSubnet Address="192.168.10.0"/><IPSubnet Address=""/></IPSubnets><Metric
Value=""/><Version>7958</Version><Capabilities SchemaVersion="1.0"><Property Name="SSLState"
Value="0"/></Capabilities><ServerRemoteName>PR1SITE.CONTOSO.COM</ServerRemoteName><DPTType>SERVER</DPTType><Win
dows
Trust="1"/><Locality>LOCAL</Locality></LocationRecord></LocationRecords></Site></Sites><RelatedContentIDs/></ContentLocati
onReply> LocationServices 2/9/2014 7:15:05 PM 3532 (0x0DCC)
```

```
Distribution Point='http://PR1SITE.CONTOSO.COM/SMS_DP_SMSPKG$/fbb5724a-aa0f-47f9-908a-47068fd8ad6f', Locality='LOCAL',
DPTType='SERVER', Version='7958', Capabilities='<Capabilities SchemaVersion="1.0"><Property Name="SSLState"
Value="0"/></Capabilities>', Signature='http://PR1SITE.CONTOSO.COM/SMS_DP_SMSSIG$/fbb5724a-aa0f-47f9-908a-
47068fd8ad6f.1.tar', ForestTrust='TRUE', LocationServices 2/9/2014 7:15:05 PM 3532 (0x0DCC)
Calling back with locations for location request {C56C01F2-2388-4710-BF3B-A526DB40E35F} LocationServices 2/9/2014 7:15:05
PM 3532 (0x0DCC)
```

Content Transfer Manager receives the Distribution Point location for the requested content and starts a Data Transfer Service job to initiate the download of the update.

#### ContentTransferManager.log:

```
CCTMJob::UpdateLocations({E0452CF4-5B04-4A1A-B8EB-10B11B063249}) ContentTransferManager 2/9/2014 7:15:05 PM
3532 (0x0DCC)
CTM_NotifyLocationUpdate ContentTransferManager 2/9/2014 7:15:05 PM 3532 (0x0DCC)
Persisted location 'http://PR1SITE.CONTOSO.COM/SMS_DP_SMSPKG$/fbb5724a-aa0f-47f9-908a-47068fd8ad6f', Order 0, for CTM
job {E0452CF4-5B04-4A1A-B8EB-10B11B063249} ContentTransferManager 2/9/2014 7:15:05 PM 3532 (0x0DCC)
Persisted locations for CTM job {E0452CF4-5B04-4A1A-B8EB-10B11B063249}:
(LLOCAL) http://PR1SITE.CONTOSO.COM/SMS_DP_SMSPKG$/fbb5724a-aa0f-47f9-908a-47068fd8ad6f
ContentTransferManager 2/9/2014 7:15:05 PM 3532 (0x0DCC)
CTM job {E0452CF4-5B04-4A1A-B8EB-10B11B063249} (corresponding DTS job {594E9A72-43D1-48D1-A639-D18DF7D286A2})
started download from 'http://PR1SITE.CONTOSO.COM/SMS_DP_SMSPKG$/fbb5724a-aa0f-47f9-908a-47068fd8ad6f' for full
content download. ContentTransferManager 2/9/2014 7:15:05 PM 3532 (0x0DCC)
CCTMJob::EvaluateState(JobID={E0452CF4-5B04-4A1A-B8EB-10B11B063249}, State=DownloadingData) ContentTransferManager
2/9/2014 7:15:05 PM 3732 (0x0E94)
CTM job {E0452CF4-5B04-4A1A-B8EB-10B11B063249} entered phase CCM_DOWNLOADSTATUS_DOWNLOADING_DATA
ContentTransferManager 2/9/2014 7:15:05 PM 3532 (0x0DCC)
```

#### CAS.log:

```
Location update from CTM for content fbb5724a-aa0f-47f9-908a-47068fd8ad6f.1 and request {856FA4CA-D02A-4E2C-841E-
841ED3C7EC01} ContentAccess 2/9/2014 7:15:05 PM 3216 (0x0C90)
Download location found 0 - http://PR1SITE.CONTOSO.COM/SMS_DP_SMSPKG$/fbb5724a-aa0f-47f9-908a-47068fd8ad6f
ContentAccess 2/9/2014 7:15:05 PM 3216 (0x0C90)
Download request only, ignoring location update ContentAccess 2/9/2014 7:15:05 PM 3216 (0x0C90)
Download started for content fbb5724a-aa0f-47f9-908a-47068fd8ad6f.1 ContentAccess 2/9/2014 7:15:05 PM 848
(0x0350)
```

At this point, Data Transfer Service creates a BITS job to download the file and then monitors the download progress.

#### DataTransferService.log:

```
DTSJob {594E9A72-43D1-48D1-A639-D18DF7D286A2} created to download from
'http://PR1SITE.CONTOSO.COM:80/SMS_DP_SMSPKG$/fbb5724a-aa0f-47f9-908a-47068fd8ad6f' to 'C:\Windows\ccmcache\1'.
DataTransferService 2/9/2014 7:15:05 PM 3532 (0x0DCC)
DTSJob {594E9A72-43D1-48D1-A639-D18DF7D286A2} in state 'DownloadingManifest'. DataTransferService 2/9/2014 7:15:05
PM 3216 (0x0C90)
CDTSJob::ProcessManifestCallback - processing manifest for job '{594E9A72-43D1-48D1-A639-D18DF7D286A2}'.
DataTransferService 2/9/2014 7:15:05 PM 3532 (0x0DCC)
DTSJob {594E9A72-43D1-48D1-A639-D18DF7D286A2} in state 'RetrievedManifest'. DataTransferService 2/9/2014 7:15:05
PM 3532 (0x0DCC)
Execute called for DTS job '{594E9A72-43D1-48D1-A639-D18DF7D286A2}'. Current state: 'RetrievedManifest'.
DataTransferService 2/9/2014 7:15:05 PM 3532 (0x0DCC)
DTSJob {594E9A72-43D1-48D1-A639-D18DF7D286A2} in state 'PendingDownload'. DataTransferService 2/9/2014 7:15:05
PM 3532 (0x0DCC)
Starting BITS download for DTS job '{594E9A72-43D1-48D1-A639-D18DF7D286A2}'. DataTransferService 2/9/2014 7:15:05
PM 3532 (0x0DCC)
DTSJob {594E9A72-43D1-48D1-A639-D18DF7D286A2} set BITS job to use default credentials. DataTransferService
2/9/2014 7:15:06 PM 3532 (0x0DCC)
```

```

Starting BITS job '{38E74FCB-4397-4CA9-94AE-BDD49F550EC9}' for DTS job '{594E9A72-43D1-48D1-A639-D18DF7D286A2}' under
user 'S-1-5-18'. DataTransferService      2/9/2014 7:15:06 PM      3532 (0x0DCC)
DTS::SetCustomHeadersOnBITSJob - setting custom headers on DTS job '{594E9A72-43D1-48D1-A639-D18DF7D286A2}':
<none> DataTransferService      2/9/2014 7:15:06 PM      3532 (0x0DCC)
DTS::AddTransportSecurityOptionsToBITSJob - Removing security info from DTS job '{594E9A72-43D1-48D1-A639-D18DF7D286A2}'.
DataTransferService      2/9/2014 7:15:06 PM      3532 (0x0DCC)
DTSJob {594E9A72-43D1-48D1-A639-D18DF7D286A2} in state 'DownloadingData'. DataTransferService      2/9/2014 7:15:06
PM      3532 (0x0DCC)
Job: {594E9A72-43D1-48D1-A639-D18DF7D286A2}, Total Files: 1, Transferred Files: 0, Total Bytes: 199093, Transferred Bytes: 5760
DataTransferService      2/9/2014 7:15:06 PM      2656 (0x0A60)
Job: {594E9A72-43D1-48D1-A639-D18DF7D286A2}, Total Files: 1, Transferred Files: 0, Total Bytes: 199093, Transferred Bytes:
199093 DataTransferService      2/9/2014 7:15:12 PM      2656 (0x0A60)
CDTSJob::JobTransferred : DTS Job ID='{594E9A72-43D1-48D1-A639-D18DF7D286A2}' BITS Job ID='{38E74FCB-4397-4CA9-94AE-
BDD49F550EC9}' DataTransferService      2/9/2014 7:15:12 PM      2552 (0x09F8)
Job: {594E9A72-43D1-48D1-A639-D18DF7D286A2}, Total Files: 1, Transferred Files: 1, Total Bytes: 199093, Transferred Bytes:
199093 DataTransferService      2/9/2014 7:15:12 PM      2552 (0x09F8)
DTSJob {594E9A72-43D1-48D1-A639-D18DF7D286A2} in state 'RetrievedData'. DataTransferService      2/9/2014 7:15:12 PM
2552 (0x09F8)
DTSJob {594E9A72-43D1-48D1-A639-D18DF7D286A2} successfully completed download. DataTransferService
2/9/2014 7:15:12 PM      2552 (0x09F8)
BITS job '{38E74FCB-4397-4CA9-94AE-BDD49F550EC9}' is not found. The BITS job may have completed already.
DataTransferService      2/9/2014 7:15:12 PM      2552 (0x09F8)
CBITSDownloadMonitor(DTSJobID={594E9A72-43D1-48D1-A639-D18DF7D286A2}, BITSJobID={38E74FCB-4397-4CA9-94AE-
BDD49F550EC9}) ignoring cancelled object. DataTransferService      2/9/2014 7:15:12 PM      2552 (0x09F8)
DTSJob {594E9A72-43D1-48D1-A639-D18DF7D286A2} in state 'NotifiedComplete'. DataTransferService      2/9/2014 7:15:12
PM      3532 (0x0DCC)
DTS job {594E9A72-43D1-48D1-A639-D18DF7D286A2} has completed:
Status : SUCCESS,
Start time : 02/09/2014 19:15:05,
Completion time : 02/09/2014 19:15:12,
Elapsed time : 7 seconds DataTransferService      2/9/2014 7:15:12 PM      3532 (0x0DCC)

```

After the download is complete, CTM and CAS are notified, and they mark the download jobs as completed. CAS performs a hash verification of the downloaded content to ensure the integrity of the downloaded file. This process occurs for each file, although this example is just focused on a single update getting downloaded.

**ContentTransferManager.log:**

```

CCTMJob::EvaluateState(JobID={E0452CF4-5B04-4A1A-B8EB-10B11B063249}, State=Success) ContentTransferManager
CCTMJob::EvaluateState(JobID={E0452CF4-5B04-4A1A-B8EB-10B11B063249}, State=Complete) ContentTransferManager

```

**CAS.log:**

```

Download completed for content fbb5724a-aa0f-47f9-908a-47068fd8ad6f.1 under context System ContentAccess
2/9/2014 7:15:12 PM      3532 (0x0DCC)
The hash we are verifying is SDMPackage:<Content ContentId="fbb5724a-aa0f-47f9-908a-47068fd8ad6f" Version="1"><FileContent
Name="windows6.1-kb2705219-v2-x64.cab" Hash="8E8E0175D46B5A8D52C4856FA3D282FAA12ACD63" HashAlgorithm="SHA1"
Size="199093"/></Content>
ContentAccess      2/9/2014 7:15:12 PM      3532 (0x0DCC)
CContentAccessService::NotifyDownloadComplete Start Content Hashing ContentAccess      2/9/2014 7:15:12 PM      3532
(0x0DCC)
Hashing file c:\windows\ccmcache\1\windows6.1-kb2705219-v2-x64.cab
ContentAccess      2/9/2014 7:15:12 PM      3532 (0x0DCC)
Hash matches ContentAccess      2/9/2014 7:15:12 PM      3532 (0x0DCC)
Hash verification succeeded for content fbb5724a-aa0f-47f9-908a-47068fd8ad6f.1 downloaded under context System
ContentAccess      2/9/2014 7:15:12 PM      3532 (0x0DCC)

```

When the download is complete, Updates Deployment Agent raises a State Message to update the current enforcement state and then starts the installation of the update.

**UpdatesDeploymentAgent.log:**

Raised assignment ({B040D195-8FA8-48D3-953F-17E878DAB23D}) state message successfully. **TopicType = Enforce**, StateId = 8, StateName = **ASSIGNMENT\_ENFORCE\_ADVANCE\_DOWNLOAD\_SUCCESS** UpdatesDeploymentAgent 2/9/2014 7:15:16 PM 3532 (0x0DCC)

Starting install for assignment ({B040D195-8FA8-48D3-953F-17E878DAB23D}) UpdatesDeploymentAgent 2/9/2014 7:15:16 PM 3532 (0x0DCC)

ApplyCIs - JobId = {CEE4AA3A-DE7B-4D9F-8949-E421BBBBF2993} UpdatesDeploymentAgent 2/9/2014 7:15:16 PM 3532 (0x0DCC)

Update (Site\_D3A5F7EA-25D4-4C6B-B47C-C74997522A76/SUM\_3cbcf577-5139-49b8-afe8-620af5c52f95) Progress: Status = ciStateWaitInstall, PercentComplete = 0, DownloadSize = 0, Result = 0x0 UpdatesDeploymentAgent 2/9/2014 7:15:16 PM 2860 (0x0B2C)

Update (Site\_D3A5F7EA-25D4-4C6B-B47C-C74997522A76/SUM\_ada7cf51-66b0-4a00-b37b-68d569d6ff8b) Progress: Status = ciStateWaitInstall, PercentComplete = 0, DownloadSize = 0, Result = 0x0 UpdatesDeploymentAgent 2/9/2014 7:15:16 PM 2860 (0x0B2C)

Update (Site\_D3A5F7EA-25D4-4C6B-B47C-C74997522A76/SUM\_e06056e3-0199-4c68-8ac3-bdddff356a0a) Progress: Status = ciStateWaitInstall, PercentComplete = 0, DownloadSize = 0, Result = 0x0 UpdatesDeploymentAgent 2/9/2014 7:15:16 PM 2860 (0x0B2C)

**UpdatesHandler.log:**

Job {CEE4AA3A-DE7B-4D9F-8949-E421BBBBF2993} is starting execution UpdatesHandler 2/9/2014 7:15:16 PM 1428 (0x0594)

CDeploymentJob::InstallUpdatesInBatch - Batch or non-batch install is not in progress for the job ({CEE4AA3A-DE7B-4D9F-8949-E421BBBBF2993}). So allowing install.. UpdatesHandler 2/9/2014 7:15:16 PM 3216 (0x0C90)

Update (3cbcf577-5139-49b8-afe8-620af5c52f95) added to the installation batch UpdatesHandler 2/9/2014 7:15:16 PM 3216 (0x0C90)

Update (ada7cf51-66b0-4a00-b37b-68d569d6ff8b) added to the installation batch UpdatesHandler 2/9/2014 7:15:16 PM 3216 (0x0C90)

Update (e06056e3-0199-4c68-8ac3-bdddff356a0a) added to the installation batch UpdatesHandler 2/9/2014 7:15:17 PM 3216 (0x0C90)

Got execute info for (3) updates UpdatesHandler 2/9/2014 7:15:17 PM 3216 (0x0C90)

**Updates installation started as batch** UpdatesHandler 2/9/2014 7:15:26 PM 3216 (0x0C90)

Windows Update Agent Handler copies the downloaded binaries to the Windows Update Agent cache (C:\Windows\SoftwareDistribution\Download) directory and instructs Windows Update Agent to start the installation process.

**WUAHandler.log:**

Adding file to list for CopyToCache(): C:\Windows\ccmcache\1\windows6.1-kb2705219-v2-x64.cab WUAHandler 2/9/2014 7:15:25 PM 3216 (0x0C90)

CopyToCache() for update (fbb5724a-aa0f-47f9-908a-47068fd8ad6f) completed successfully WUAHandler 2/9/2014 7:15:26 PM 3216 (0x0C90)

Adding file to list for CopyToCache(): C:\Windows\ccmcache\2\windows6.1-kb2712808-x64.cab WUAHandler 2/9/2014 7:15:26 PM 3216 (0x0C90)

CopyToCache() for update (3e9b1132-9ccd-439d-b32a-5cefd19735d1) completed successfully WUAHandler 2/9/2014 7:15:26 PM 3216 (0x0C90)

Adding file to list for CopyToCache(): C:\Windows\ccmcache\3\windows6.1-kb2698365-x64.cab WUAHandler 2/9/2014 7:15:26 PM 3216 (0x0C90)

CopyToCache() for update (d2a9ee23-9cab-4843-b040-e2da1cc167e9) completed successfully WUAHandler 2/9/2014 7:15:26 PM 3216 (0x0C90)

Update(s) downloaded to WUA file cache, starting installation. WUAHandler 2/9/2014 7:15:26 PM 3216 (0x0C90)

**Async installation of updates started.** WUAHandler 2/9/2014 7:15:26 PM 3216 (0x0C90)

Update 1 (3cbcf577-5139-49b8-afe8-620af5c52f95) finished installing (0x00000000), Reboot Required? Yes WUAHandler 2/9/2014 7:15:29 PM 2840 (0x0B18)

Update 2 (ada7cf51-66b0-4a00-b37b-68d569d6ff8b) finished installing (0x00000000), Reboot Required? Yes WUAHandler 2/9/2014 7:15:30 PM 996 (0x03E4)

```
Update 3 (e06056e3-0199-4c68-8ac3-bdddff356a0a) finished installing (0x00000000), Reboot Required? Yes WUAHandler
2/9/2014 7:15:39 PM 268 (0x010C)
Async install completed. WUAHandler 2/9/2014 7:15:39 PM 2396 (0x095C)
Installation of updates completed. WUAHandler 2/9/2014 7:15:39 PM 2604 (0x0A2C)
```

**WindowsUpdate.log:**

```
2014-02-09 19:15:26:130 800 ed0 Agent ** START ** Agent: Installing updates [CallerId = CcmExec]
2014-02-09 19:15:26:130 800 ed0 Agent * Updates to install = 3
2014-02-09 19:15:26:254 1048 84c Handler Starting install of CBS update FBB5724A-AA0F-47F9-908A-
47068FD8AD6F
2014-02-09 19:15:29:218 1048 84c Handler Completed install of CBS update with type=3, requiresReboot=1,
installerError=0, hr=0x0
2014-02-09 19:15:29:265 1048 84c Handler Starting install of CBS update 3E9B1132-9CCD-439D-B32A-
5CEFD19735D1
2014-02-09 19:15:30:435 1048 84c Handler Completed install of CBS update with type=3, requiresReboot=1,
installerError=0, hr=0x0
2014-02-09 19:15:30:451 1048 84c Handler Starting install of CBS update D2A9EE23-9CAB-4843-B040-
E2DA1CC167E9
2014-02-09 19:15:39:296 1048 84c Handler Completed install of CBS update with type=3, requiresReboot=1,
installerError=0, hr=0x0
2014-02-09 19:15:39:327 788 9f8 COMAPI - Reboot required = Yes
2014-02-09 19:15:39:327 788 9f8 COMAPI -- END -- COMAPI: Install [ClientId = CcmExec]
```

After the updates are installed, Updates Deployment Agent checks whether any updates require a reboot, and then it notifies the user if client settings are configured to allow notifications.

**UpdatesDeployment.log:**

```
No installations in pipeline, notify reboot. NotifyUI = True UpdatesDeploymentAgent 2/9/2014 7:15:39 PM 3216
(0x0C90)
Notify reboot with deadline = Sunday, Feb 09, 2014. - 19:15:39, Ignore reboot Window = False, NotifyUI = True
UpdatesDeploymentAgent 2/9/2014 7:15:39 PM 3216 (0x0C90)
Raised assignment ({B040D195-8FA8-48D3-953F-17E878DAB23D}) state message successfully. TopicType = Enforce, StateId = 5,
StateName = ASSIGNMENT_ENFORCE_PENDING_REBOOT UpdatesDeploymentAgent 2/9/2014 7:15:39 PM 2604
(0x0A2C)
```

After the computer restarts, a post-reboot detection scan is started for the deployment to verify that updates are installed, and to raise state messages for the update and deployment to indicate that updates are installed and that enforcement was successful.

**UpdatesDeployment.log:**

```
CTargetedUpdatesManager::DetectRebootPendingUpdates - Total Pending reboot updates = 3 UpdatesDeploymentAgent
2/9/2014 7:18:56 PM 2780 (0x0ADC)
Initiated detect for pending reboot updates after system restart - JobId = {53F4851F-7E63-4C7E-952D-78345039FFFC}
UpdatesDeploymentAgent 2/9/2014 7:18:56 PM 2780 (0x0ADC)
CUpdatesJob({53F4851F-7E63-4C7E-952D-78345039FFFC}): Job completion received. UpdatesDeploymentAgent
2/9/2014 7:19:19 PM 2436 (0x0984)
CUpdatesJob({53F4851F-7E63-4C7E-952D-78345039FFFC}): Detect after reboot job completed with result = 0x0
UpdatesDeploymentAgent 2/9/2014 7:19:19 PM 2436 (0x0984)

Raised update (Site_D3A5F7EA-25D4-4C6B-B47C-C74997522A76/SUM_e06056e3-0199-4c68-8ac3-bdddff356a0a) enforcement
state message successfully. StateId = 10, StateName = CI_ENFORCEMENT_SUCCESSFULL UpdatesDeploymentAgent
2/9/2014 7:19:19 PM 2436 (0x0984)
Raised update (Site_D3A5F7EA-25D4-4C6B-B47C-C74997522A76/SUM_ada7cf51-66b0-4a00-b37b-68d569d6ff8b) enforcement
state message successfully. StateId = 10, StateName = CI_ENFORCEMENT_SUCCESSFULL UpdatesDeploymentAgent
2/9/2014 7:19:19 PM 2436 (0x0984)
```



Raised update (Site\_D3A5F7EA-25D4-4C6B-B47C-C74997522A76/SUM\_3cbcf577-5139-49b8-afe8-620af5c52f95) enforcement state message successfully. StateId = 10, StateName = **CI\_ENFORCEMENT\_SUCCESSFULL** UpdatesDeploymentAgent  
2/9/2014 7:19:19 PM 2436 (0x0984)

Raised assignment ({B040D195-8FA8-48D3-953F-17E878DAB23D}) state message successfully. **TopicType = Compliance**, Signature = 5e176837, **IsCompliant = True** UpdatesDeploymentAgent 2/9/2014 7:19:19 PM 2456 (0x0998)

Raised assignment ({B040D195-8FA8-48D3-953F-17E878DAB23D}) state message successfully. **TopicType = Enforce**, StateId = 4, StateName = **ASSIGNMENT\_ENFORCE\_SUCCESS** UpdatesDeploymentAgent 2/9/2014 7:19:19 PM 2456 (0x0998)

---

## STATE MESSAGE REPORTING

Throughout the deployment phase, multiple State Messages are raised to indicate the current state of the updates and of the deployment itself. After these state messages are raised, they are processed the way that was described earlier in the [“State Message Processing Flow”](#) section.

All examples below are based on updates that are deployed to a Windows 7-based client and with settings configured with the following values.

### Computer Restart Client settings:

Display a temporary notification to the user that indicates the interval before the user is logged off or the computer restarts (minutes) – 90 minutes

Display a dialog box that the user cannot close, which displays the countdown interval before the user is logged off or the computer restarts (minutes) – 15 minutes

### Computer Agent Client Settings:

Deployment deadline greater than 24 hours, remind user every (hours) – 48

Deployment deadline less than 24 hours, remind user every (hours) – 4

Deployment deadline less than 1 hour, remind user every (minutes) – 15

Show notifications for new deployments – Yes

Disable deadline randomization – Yes

**NOTE** Suppress system restart option takes precedence over other options.

---

## SCENARIO 1 – SUPPRESS RESTART DISABLED

### **Deployment Configuration:**

Deployment – Required

Available Time – As soon as possible

Deadline – In Future

User notifications – Display in Software Center & show all notifications

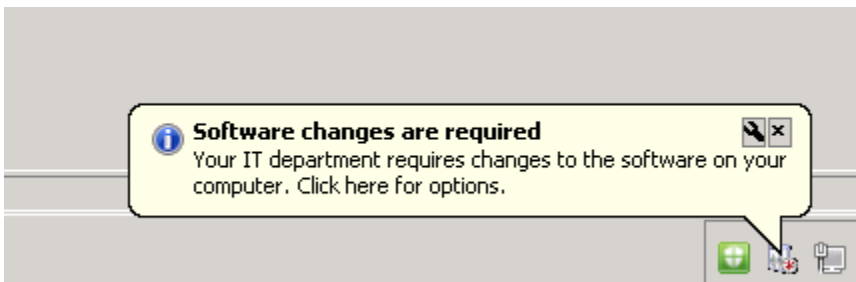
Deadline behavior for Maintenance Windows – Software Update installation and System restart unchecked

Suppress – Servers & Workstations unchecked

Maintenance Window – None

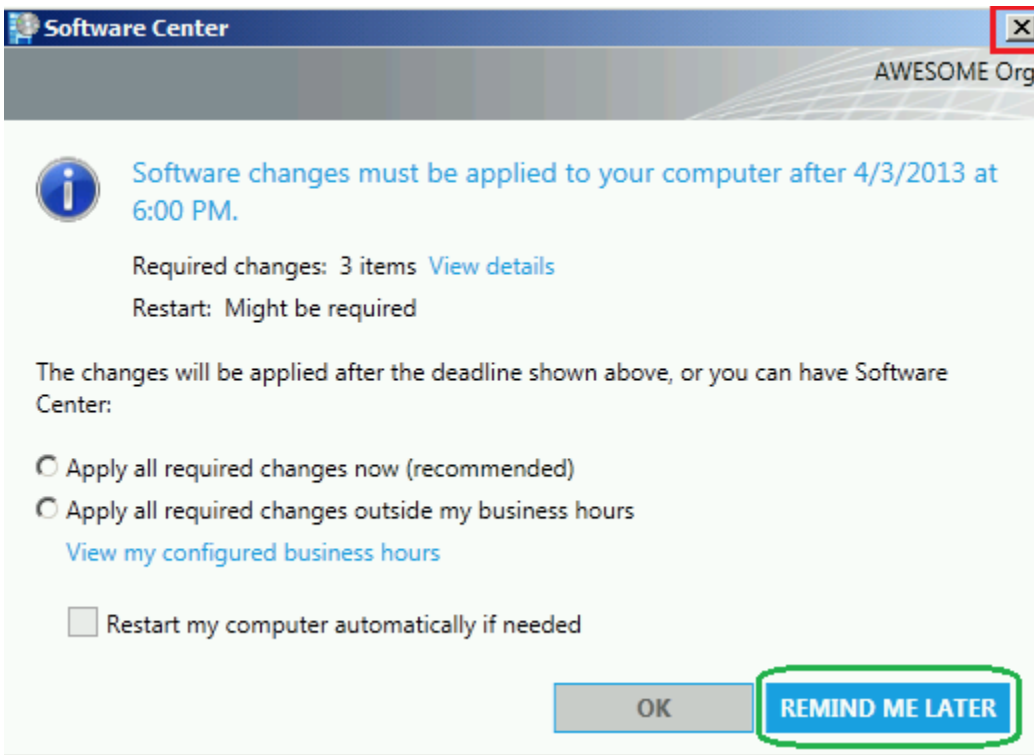
### **End User Experience:**

User receives a balloon pop-up notification after the policy arrives on the client and assignment is activated:

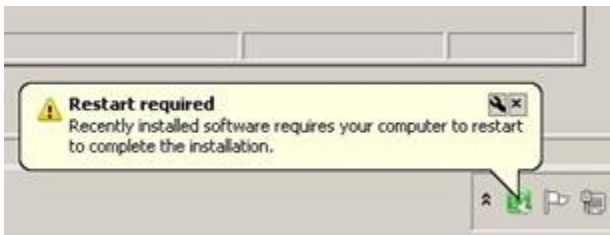


Based on the deadline reminders configured in the Computer Agent client settings, the user receives this balloon notification at configured intervals. Upon clicking the notification, the following dialog box is displayed. Note that the balloon pop-ups appear as long as the user doesn't open the dialog box and then close it by clicking the X button (as this

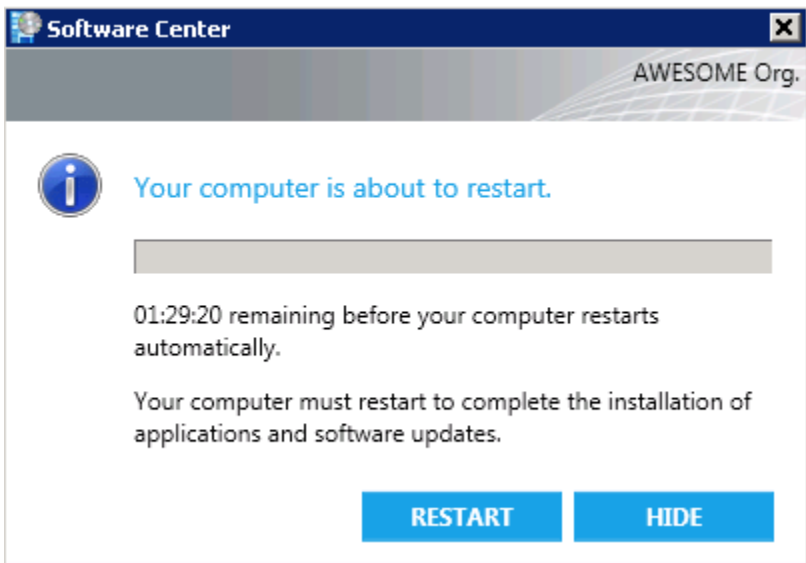
instructs Software Center to not display any further reminders). If the user clicks the **Remind me later** option, he or she continues to receive reminders based on the configured settings.



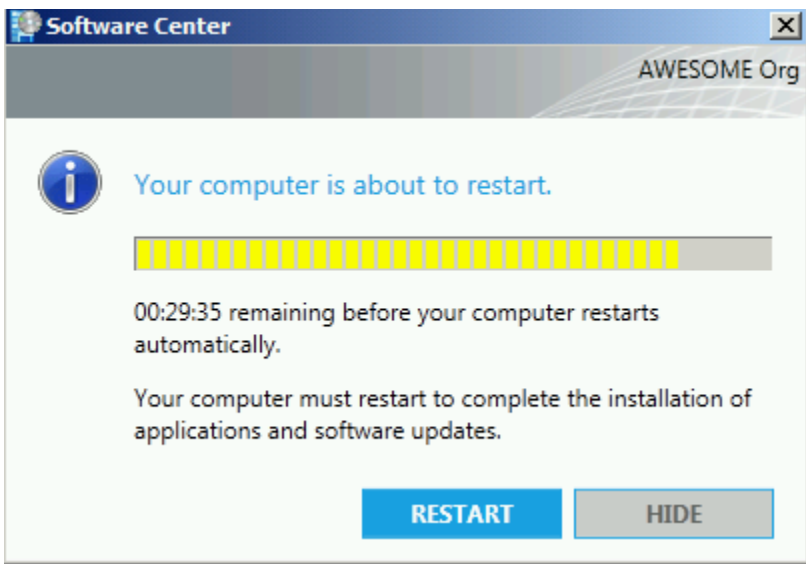
Updates are downloaded and installed at deadline (with a max randomization time of 2 hours), and the user receives a restart notification balloon pop-up stating that a system restart is required.



If the user clicks the notification, he or she sees the restart notification timer as configured in the **Computer Restart** client settings, which the user can hide. If the user clicks **Hide**, the user is not reminded again until the final countdown timer is reached.



After the timer reaches the "Final countdown" stage that's configured in the **Computer Restart** client settings, the user cannot hide the restart notification pop-up.



At the end of the configured interval, the system restarts.

---

## SCENARIO 2 – SUPPRESS RESTART ENABLED

### Deployment Configuration:

Deployment – Required

Available Time – As soon as possible

Deadline – In Future

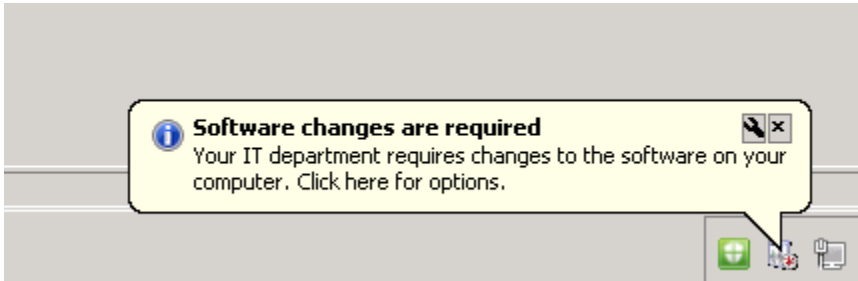
User notifications – Display in Software Center & show all notifications

Deadline behavior for Maintenance Windows – Software Update installation and System restart unchecked

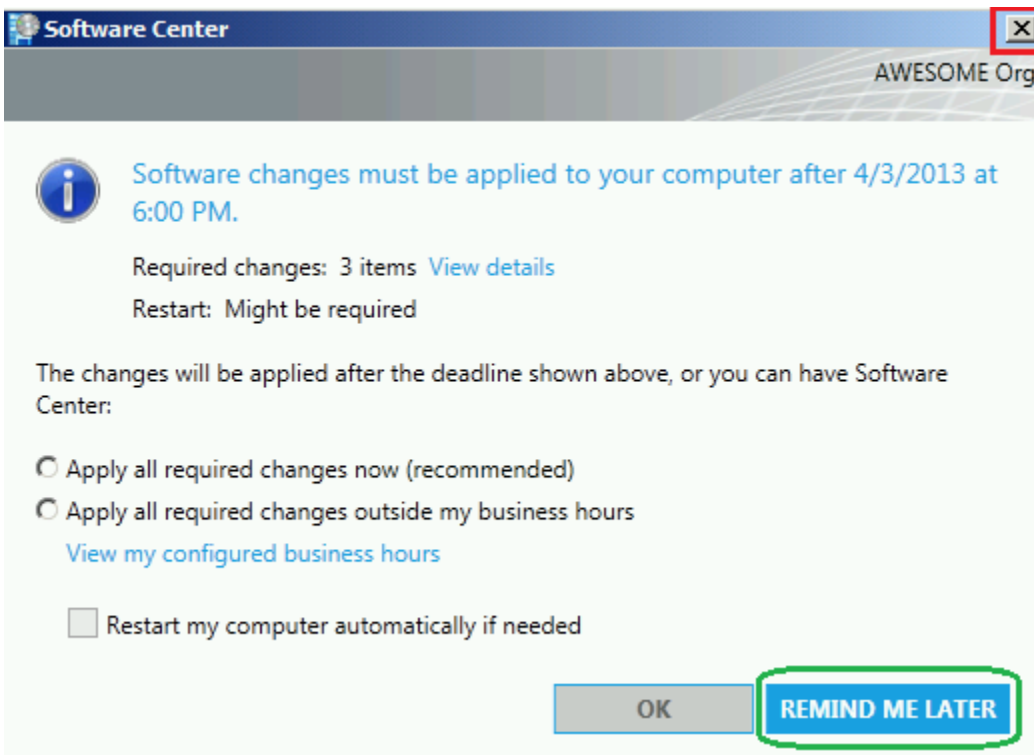
Suppress – Servers & Workstations checked

**End User Experience:**

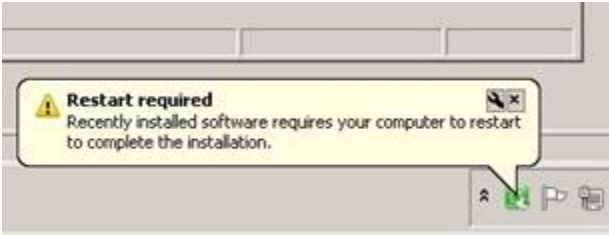
User receives a balloon pop-up notification after the policy arrives on the client and assignment is activated:



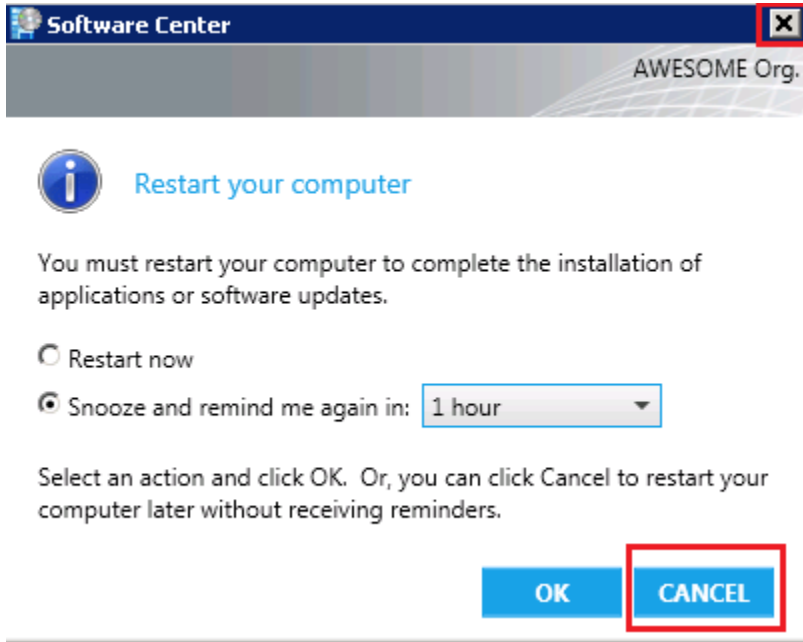
Based on the deadline reminders that are configured in the Computer Agent client settings, the user receives this balloon notification at configured intervals. After the user clicks the notification, the following dialog box is displayed. Note that the balloon pop-ups appear as long as the user doesn't open the dialog box and then close it by clicking the X button (That instructs Software Center not to display any further reminders.) If the user clicks on **Remind me later**, the user continues to receive reminders based on the configured settings.



Updates are downloaded and installed at deadline (with a max randomization time of 2 hours if deadline randomization is enabled), and the user receives a restart notification balloon pop-up stating that a system restart is required.



In this example, because the restart was suppressed, the user receives the following dialog box when he or she clicks the balloon notification pop-up. The user continues to receive this restart reminder based on the time selected in the dialog box unless he or she clicks **Cancel** or closes the dialog box by clicking **X**.



---

### SCENARIO 3 – OVERRIDE MAINTENANCE WINDOW WITHOUT SUPPRESSING REBOOT

#### **Deployment Configuration:**

Deployment – Required

Available Time – As soon as possible

Deadline – Current Time

User notifications – Display in Software Center & show all notifications

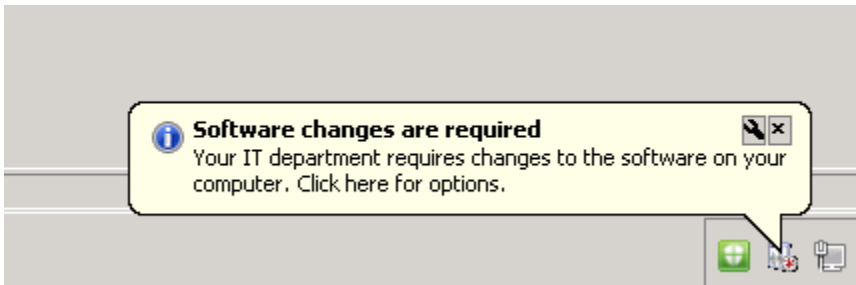
Deadline behavior for Maintenance Windows – Software Update installation checked and System restart checked

Suppress – Servers & Workstations unchecked

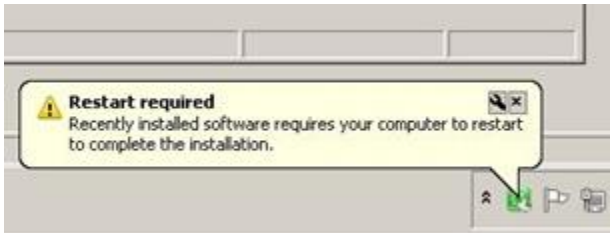
Maintenance Window – In future

#### **End User Experience:**

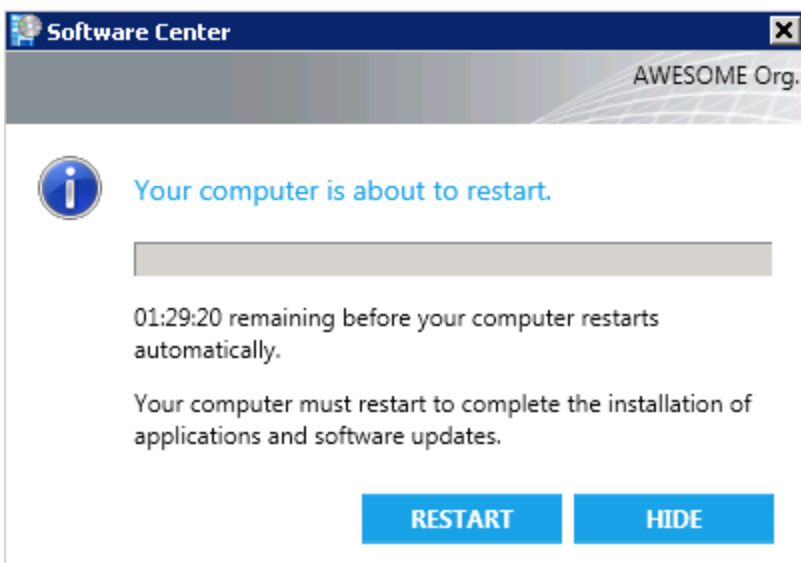
User gets a balloon pop-up notification after the policy arrives on the client and assignment is activated:



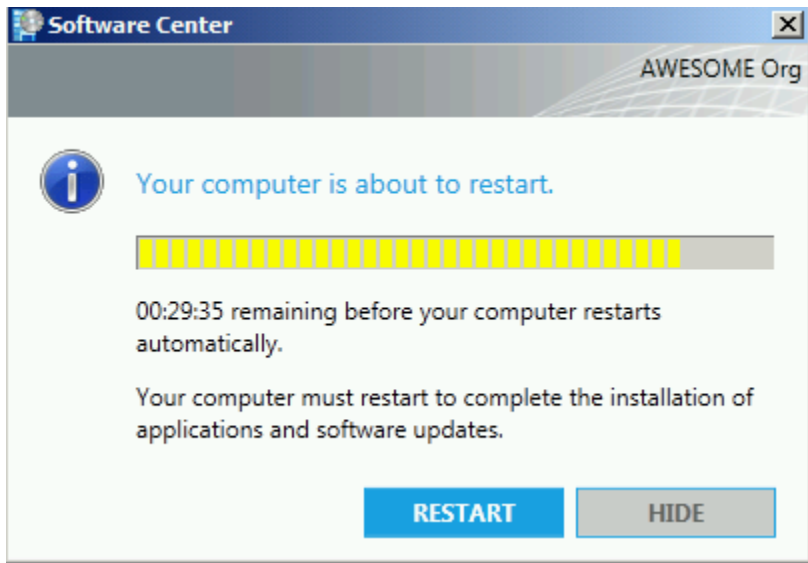
Updates are downloaded and installed at deadline (with a max randomization time of 2 hours if deadline randomization is enabled) and the user gets a restart notification balloon pop-up stating that a system restart is required.



If the user clicks the notification, he or she sees the restart notification timer as configured in the **Computer Restart** client settings, which can then be hidden. If the user clicks **Hide**, the user is not reminded again until the final countdown stage is reached.



After the timer reaches the "Final countdown" stage that's configured in **Computer Restart** client settings, the user cannot hide the restart notification pop-up.



At the end of the configured interval, the system restarts.



## BEST PRACTICES

Best Practices for WSUS Server SSL Configuration:

<http://blogs.technet.com/b/sus/archive/2011/08/15/best-practices-for-securing-wsus-with-ssl.aspx>

Best Practices for Software Updates Management in Configuration Manager:

<http://technet.microsoft.com/en-us/library/hh692394.aspx>

Best Practices for Endpoint Protection:

<http://technet.microsoft.com/en-us/library/hh508771.aspx>

## TROUBLESHOOTING

### SYNCHRONIZATION

Before troubleshooting synchronization issues, verify that the following prerequisites are met:

- If you're running WSUS 3.0 SP2, KB [2734608](#) must be installed on the WSUS server. To check whether [2734608](#) is installed, see the "How to check WSUS Server Version" section later in this white paper.
- When the Software Update Point is installed on a remote site system server, the WSUS Administration console must be installed on the site server. If you're running WSUS 3.0 SP2, KB [2734608](#) must be installed on top of the WSUS Administration console.
- After you install KB 2734608 (remotely or locally), a system restart may be required.
- Verify that the WSUS installation that's running on the Software Update Point is not incorrectly configured to be a replica. For more information, see the "Procedure: Check the Update Source Settings in WSUS" section.
- Verify that the Update Services service is running on the WSUS computer.
- Verify that the Default website or WSUS Administration website is running on the WSUS computer.

---

### RELEVANT DATA

**WsyncMgr.log and WCM.log** - Located on the Site Server in `<ConfigMgrInstallDir>\Logs`

**WSUSCtrl.log** - Located on the Software Update Point Server in `<DriveWithMostFreeSpace>:\SMS\Log`s

**SoftwareDistribution.log** - Located on the Software Update Point Server in `\Program Files\Update Services\LogFiles`

**IIS Logs from the Software Update Point** - Usually located under `%SystemDrive%\inetpub\Log`s

**Application and System Event Logs** from the Software Update Point

---

### SYNCHRONIZATION FAILS WITH "WSUS SERVER NOT CONFIGURED"

WSUS Configuration Manager (WCM) configures the WSUS computer once every hour to make sure that the settings that are configured in WSUS match the settings that are specified in the Configuration Manager console. If WCM fails to

configure the WSUS computer, synchronization attempts will trigger the following error. In most cases there will not be any extra information in the WsyncMgr.log file, and you have to review the WCM.log file for additional errors.

**WsyncMgr.log on Site Server shows:**

Sync failed: WSUS server not configured. Please refer to WCM.log for configuration error details. Source: CWSyncMgr::DoSync  
Sync failed. Will retry in 60 minutes

## Synchronization fails because of authentication and proxy issues

Error messages may include the following:

*HTTP Status 401 Unauthorized*

*HTTP Status 403 Forbidden*

*HTTP Status 407 Proxy Authentication Required*

*HTTP Status 502 Proxy Error*

*No connection could be made because the target machine actively refused it*

*Authentication failed because the remote party has closed the transport stream*

Steps to try:

- Verify that the Update Services service is running on the WSUS computer.
- Verify that the Default Website or WSUS Administration website is running on the WSUS computer.
- Verify that the fully qualified domain name (FQDN) for the software Update Point site system server is correct and accessible from the Site Server.
- If the Software Update Point is remote from the Site Server, verify that you can connect to the WSUS computer from the Site Server. For more information, see the "[How to Test Connectivity from Site Server to WSUS](#)" section.
- Check the port settings configured for the Software Update Point and verify that they are the same as the port settings that are configured for the website used by WSUS on the Software Update Point. For more information, see the "[Procedure: How to determine the Port Settings used by WSUS](#)" section.
- Verify that the proxy configuration and account for the Software Update Point is correct. For more information, see the "[Procedure: How to configure Proxy Settings for the Software Update Point](#)" section.
- Verify that the Software Update Point connection account is configured (if required) and that it has the permissions to connect to the WSUS computer. For more information, see the "[Procedure: How to configure WSUS Server Connection account for the Software Update Point](#)" section.
- Verify that the permissions on the ApiRemoting30 Virtual Directory are set correctly. For more information, see the "[Procedure: Check Permissions on ApiRemoting30 Virtual Directory](#)" section.
- If the Software Update Point is configured for SSL (HTTPS), verify that WSUS is correctly configured for SSL. For more information, see the "[Procedure: Configure Software Update Point for Secure Sockets Layer \(SSL\)](#)" section.
- Review WSUSCtrl.log for errors. For more information, see the "WSUS Control Manager (WSUSCtrl) reports an error" section.

## Synchronization fails because of Web Service issues

Error messages may include the following:

*HTTP Status 500 Internal Server Error*

*HTTP Status 503 Service Unavailable*

### Steps to try:

- Verify that Update Services is running on the WSUS computer.
- Verify that the Default website or the WSUS Administration website is running on the WSUS computer.
- Check the port settings configured for the Software Update Point, and verify that they are the same as the port settings configured for the website used by WSUS on the Software Update Point. For more information, see the [“Procedure: How to determine the Port Settings used by WSUS”](#) section.
- Review WSUSCtrl.log for errors. For more information, see the [“WSUS Control Manager \(WSUSCtrl\) reports an error”](#) section.

### **Synchronization fails because of SSL issues: The remote certificate is invalid according to the validation procedure**

- Verify that the certificate configured for the WSUS website is configured with the correct FQDN. If the certificate doesn't have the proper FQDN, see KB [931351](#) for steps about adding a Subject Alternate Name to a certificate.
- Verify that the certificate has not expired.

For more information, see the [“Procedure: Configure Software Update Point for Secure Sockets Layer \(SSL\)”](#) section.

---

### SYNCHRONIZATION FAILS BECAUSE OF ISSUES WITH THE EULA

- Review SoftwareDistribution.log on the WSUS computer to find out why the EULA is not being downloaded. You can look for “.txt” in the log to find the relevant entries.
- Verify that the firewall is configured to allow communication with Microsoft Update. For more information, see the [“Configure the Firewall”](#) TechNet link.
- Check the proxy configuration. For more information, see the [“Procedure: How to configure Proxy Settings for the Software Update Point”](#) section.
- Run the `%ProgramFiles%\Update Services\Tools\wsusutil.exe reset` command to instruct WSUS to re-download the missing content, including EULAs.

---

### SYNCHRONIZATION FAILS BECAUSE OF ERRORS COMMUNICATING WITH MICROSOFT UPDATE

#### Error messages may include:

*A connection attempt failed because the connected party did not properly respond after a period of time, or established connection failed because connected host has failed to respond.*

*0x80072EFE - The connection with the server was terminated abnormally*

#### Steps to try:

- Verify that the WSUS computer can connect to the Internet.
- Verify that the firewall is configured to allow communication with Microsoft Update. For more information, see the [“Configure the Firewall”](#) TechNet link.
- Check the proxy configuration. For more information, see the [“Procedure: How to configure Proxy Settings for the Software Update Point”](#) section.

---

### WSUS CONTROL MANAGER (WSUSCTRL) REPORTS AN ERROR

Unlike WCM and WSyncMgr, WSUS Control Manager resides on the Software Update Point itself. Therefore, if SUP is remote, WSUSCtrl.log will be present on the SUP instead of on the Site Server. WSUS Control Manager periodically checks WSUS to make sure that WSUS components are healthy. If unhealthy, WCM and WSyncMgr cannot communicate with WSUS. In most cases, errors in WCM.log resemble those in WsyncMgr.log, however an exception to this could be when the SUP is remote to the Site Server. If WSUS components are healthy, WSUSCtrl.log on the remote SUP does not report any errors. However, if the Site Server cannot connect to the WSUS computer remotely, you will see errors in WCM.log and/or WSyncMgr.log even though WSUS itself is healthy.

To check whether WSUS is functioning as expected, run the following command on the WSUS computer, and then review the Application log in Event Viewer for errors:

**%ProgramFiles%\Update Services\Tools\wsusutil.exe check health**

To check connectivity from the Site Server to the WSUS server, see the "[How to Test Connectivity from Site Server to WSUS](#)" section.

## COMPLIANCE

### RELEVANT DATA

**WindowsUpdate.log** – Located in %windir% directory

**CCM Logs** – Usually located in \Windows\CCM\Logs directory

**Application and System Event Logs**

### SCAN FAILURES

When troubleshooting scan failures, the logs you should look at are WUAHandler.log and WindowsUpdate.log. As WUAHandler simply reports what Windows Update Agent reported, the error in WUAHandler would be the same error that was reported by the Windows Update Agent itself. Therefore, more information about the error could be found in WindowsUpdate.log. To understand how to read WindowsUpdate.log, see the "[How to read the WindowsUpdate.log file](#)" KB article.

There are a number of reasons why Software Update scan could fail. Some common reasons involve communication or firewall issues between the client and the Software Update Point computer. You can find the complete list of Windows Update error codes here:

938205 - Windows Update error code list (<http://support.microsoft.com/kb/938205>)

**Scan failures due to missing or corrupt components: 0x80245003, 0x80070514, 0x8DDD0018, 0x80246008, 0x80200013, 0x80004015, 0x800A0046, 0x800A01AD, 0x80070424, 0x800B0100, 0x80248011.**

- A number of issues with Software Update scan can be caused by missing or corrupted files or registry keys, component registrations, and so forth. You can run the Windows Update Troubleshooter to detect and fix these issues automatically. For more information, see the "[How to use Windows Update Troubleshooter and update the Windows Update Agent](#)" section.
- Reset the Windows Update Agent Data Store. For more information, see the "[How to reset the Windows Update Agent Data Store](#)" section.

### Scan fails with Proxy related errors: 0x80244021, 0x8024401B, 0x80240030, 0x8024402C

- Verify the proxy settings on the client, and make sure they are configured correctly. For more information, see the [“How to check Proxy Settings on a Client”](#) section.

### Scan fails with HTTP timeout errors: 0x80072ee2, 0x8024401C, 0x80244023

- Verify connectivity with WSUS computer. See the [“How to verify connectivity on a client against the WSUS Server”](#) section.
- Review IIS logs on the WSUS computer to confirm that the HTTP errors are being returned from WSUS. If the WSUS computer is not returning the error then the issue is likely with an intermediate firewall or proxy.
- Verify Proxy Settings. See the [“How to check Proxy settings on a client”](#) section.
- Verify that the WSUS ports are accessible. See the [“How to check if WSUS Server Ports are accessible from the client”](#) section.

### Scan fails with authentication errors: 0x80244017 (HTTP Status 401), 0x80244018 (HTTP Status 403)

- Verify connectivity with the WSUS computer. See the [“How to verify connectivity on a client against the WSUS Server”](#) section.
- Review IIS logs on the WSUS computer to confirm that the HTTP errors are being returned from WSUS. If the WSUS computer is not returning the error, the issue is likely with an intermediate firewall or proxy.
- Verify the proxy settings. See the [“How to check Proxy settings on a client”](#) section.
- Verify that the WSUS ports are accessible. See the [“How to check if WSUS Server Ports are accessible from the client”](#) section.

### Scan fails with Error 0x80072f0c

0x80072f0c means “A certificate is required to complete client authentication.” This error should occur only if the WSUS computer is configured to use SSL. As part of the SSL configuration, WSUS virtual directories must be configured to use SSL and set to “Ignore” client certificates. If the WSUS website or any of those virtual directories are incorrectly configured to “Accept” or “Require” client certificates, you will receive this error. For more information about configuring WSUS for SSL see the [“Configure Software Update Point for SSL”](#) section.

---

### GROUP POLICY OVERRIDES WSUS SERVER

The Software Updates feature automatically configures a local Group Policy setting for the Configuration Manager client so that it is configured with the Software Update Point source location and port number. Both the server name and port number are required for the client to find the Software Update Point.

If an Active Directory Group Policy setting is applied to computers for Software Update Point client installation, this overrides the local Group Policy setting. Unless the value of the setting that’s defined in Group Policy is exactly the same as the one that’s being set by Configuration Manager (server name and port), the Configuration Manager Software Updates scan will fail on the client. In this case, WUAHandler.log shows the following:

```
Group policy settings were overwritten by a higher authority (Domain Controller) to: Server http://server and Policy ENABLED
```

## **Solution**

The Software Update Point for client installation and software updates must be the same server, and must be specified in the Active Directory Group Policy setting with the correct name format and port information. For example, this would be **http://server1.contoso.com:80** if the Software Update Point was using the default website.

---

### COMPLIANCE RESULTS UNKNOWN

- Review PolicyAgent.log on the client to verify that the client is receiving policies.
- Verify that Software Update synchronization is successful on the Software Update Point. If synchronization fails see the [“Troubleshooting Synchronization”](#) section.
- Review WUAHandler.log and WindowsUpdate.log to make sure that Software Update scans are successful. If the scan fails see the [“Troubleshooting Scan Failures”](#) section.
- If WUAHandler.log does not exist and is not created after initiating a scan cycle, the issue most likely occurs because either Software Update Scan Policy or WSUS Server Location is not available. Review the [“Software Update Scan Policy”](#) and [“Clients are unable to find the WSUS Source Location”](#) sections.
- If the scan is successful, the client should send State Messages to the management point to indicate the update status. To understand how State Messages Processing works, see the [“State Message Processing flow”](#) section.

---

### CLIENTS ARE UNABLE TO FIND THE WSUS SOURCE LOCATION

- To understand the flow for obtaining the WSUS location, see the [“WSUS Server Location”](#) section, and review the client and management point logs.
- Enable verbose and debug logging on the client and management point by following the steps in the [“How to enable verbose & debug logging on the Configuration Manager Client and Management Point”](#) section.
- Verify that there are no communication errors in CcmMessaging.log on the client.
- If the management point returns an empty WSUS location response, this could be caused by a mismatch in the Content Version of WSUS, which, in turn, could be a result of failed synchronization. You can find the Content Version of the Software Update Point by navigating to Configuration Manager Console -> Monitoring pane -> Software Update Point Synchronization Status.
- Review the data in *CI\_UpdateSources*, *WSUSServerLocations* and *Update\_SyncStatus* tables, and verify that the Update Source Unique ID and Content Version matches across these tables.

## DEPLOYMENT

---

### RELEVANT DATA

**WindowsUpdate.log** – Located in %windir% directory

**CCM Logs** – Usually located in \Windows\CCM\Logs directory

**Application and System Event Logs**

---

### UPDATES FAIL TO GET DOWNLOADED

- Review CAS.log, ContentTransferManager.log and DataTransferService.log for errors. To understand how updates are downloaded, see the “[Deployment Evaluation and Update Installation on Clients](#)” section.
- Verify that the client is in the appropriate boundary associated with the boundary group for the Distribution Point.
- Check the Software Update Package status, and verify that the software updates are downloaded and installed on the Distribution Points.
- If the content is not installed on the Distribution Point that’s associated with the client’s boundary group, check whether Fallback for Content location needs to be enabled. For more information, see <http://blogs.technet.com/b/cmpfekevin/archive/2013/03/05/what-is-fallback-and-what-does-it-mean.aspx>
- If the client receives the download location but fails to download content, you can try to download the content manually by accessing the URL for the content. You can find the URL by reviewing DataTransferServices.log.

---

## UPDATE INSTALLATION FAILS

- Check to see if the scan failed during the deployment evaluation. For troubleshooting scan errors, see “[Scan Failures](#)” section.
- Review WUAHandler.log and WindowsUpdate.log to find the errors received during update installation.
- Try to install the update manually or from Microsoft Update (if possible) to see if the update installation is successful.
- Most .NET update failures are caused due to corrupt .NET installations. In these cases, attempt to install the update manually. If the install fails, you can refer to the steps in the following Knowledge Base article to repair the .NET installation:  
[976982](http://support.microsoft.com/kb/976982) - .NET Framework update installation error: "0x80070643" or "0x643"  
(<http://support.microsoft.com/kb/976982>)

---

## UNEXPECTED REBOOTS OR UPDATES ARE INSTALLED OUTSIDE OF A MAINTENANCE WINDOW

- If possible, enable verbose & debug logging if the issue can be reproduced. See the “[How to enable verbose and debug logging for the Configuration Manager client](#)” section.
- Review ServiceWindowManager.log and identify the service windows available. For more information see the “[How to review ServiceWindowManager.log](#)” section.
- Review UpdatesDeployment.log, and locate the following line to check whether the deployment was set to ignore the maintenance window:

*Notify reboot with deadline = Sunday, Feb 09, 2014. - 21:30:17, **Ignore reboot Window = True**, NotifyUI = True*

- Review MaintenanceCoordinator.log, and locate the following line to check whether deployment was set to ignore the maintenance window. A value of 1 for *swoverride* means that the ignore maintenance window setting is enabled.

*RequestPersistence(id=Update download job, persist=1, **swoverride=1**, swType=4, pendingWFDisable=0, deadline=1)*

- Review SCNotify.log, and look for the following lines to check whether the user clicked the restart notification to initiate a restart:

*ConfirmRestartDialog: User chose to restart/logoff. (Microsoft.SoftwareCenter.Client.Pages.ConfirmRestartDialog at ButtonRestart\_Click)*

*ConfirmRestartDialog: user is allowed to restart (Microsoft.SoftwareCenter.Client.Pages.ConfirmRestartDialog at ButtonRestart\_Click)*

*The user is allowed to restart the computer. Initiating restart. (Microsoft.SoftwareCenter.Client.Data.WmiDataConnector at RestartComputer)*

- Check the deployment properties in the Configuration Manager console to check whether the deployment is set to override maintenance windows. If the deployment is not set to override maintenance windows, but the client logs suggest that override maintenance window was set, review the audit status messages to check whether the deployment was modified by someone. For more information, see the [“How to review the Audit Status messages to find if a Deployment was modified”](#) section.

## PROCEDURES

### A. LOGGING

---

#### HOW TO ENABLE VERBOSE & DEBUG LOGGING ON THE CONFIGURATION MANAGER CLIENT & MANAGEMENT POINT

##### To enable Verbose and Debug Logging

1. **Verbose logging** is enabled by creating **HKLM\Software\Microsoft\CCM\Logging\@GLOBAL\LogLevel** as a **REG\_DWORD** with a value of **0x0**.
2. **Debug logging** for the client is enabled by creating **HKLM\Software\Microsoft\CCM\Logging\DebugLogging\Enabled** as a **REG\_SZ** with a value of **True**
3. Once set, restart the SMS Agent Host service to enable the changes.

##### To increase Log File Size and Max History

1. CCM log size can be increased to 5 MB by setting **HKLM\Software\Microsoft\CCM\Logging\@GLOBAL\LogMaxSize** as **REG\_DWORD** to **5242880** (decimal)
2. The number of log files to be retained can be increased to 4 by setting **HKLM\Software\Microsoft\CCM\Logging\@GLOBAL\LogMaxHistory** as **REG\_DWORD** with a value of **4**
3. Once set, restart the SMS Agent Host service to enable the changes.

**NOTE** On the management point, you may need to restart IIS Services for verbose logging to take effect for some logs.

---

#### HOW TO ENABLE VERBOSE LOGGING FOR STATE SYSTEM COMPONENT ON THE SITE SERVER

##### To enable Verbose Logging for State System (StateSys)

Set the value of the Verbose Logging REG\_DWORD value to **1** at the following location:

**HKKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\SMS\Components\SMS\_STATE\_SYSTEM**

**NOTE** This does not require restarting SMS\_Executive service or the SMS\_STATE\_SYSTEM thread.

---

#### HOW TO ENABLE VERBOSE LOGGING FOR WSUS SYNCHRONIZATION MANAGER (WSYNMGR)



### To enable verbose logging for WsyncMgr.log:

Create or modify the following registry key on the Site Server and set the value to **4**:

**HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\SMS\Tracing\SMS\_WSUS\_SYNC\_MANAGER\LogLevel (REG\_DWORD)**

---

### HOW TO ENABLE SQL TRACING FOR CONFIGURATION MANAGER LOGS

#### To enable SQL Tracing for Configuration Manager logs

Set the value of **SqIEnabled** REG\_DWORD value to **1** at the following location:

**HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\SMS\Tracing**

**NOTE** This does not require restarting SMS\_Executive Service, and it enables SQL Tracing for all Configuration Manager server logs. You cannot enable SQL Tracing for a specific log. SQL Tracing can significantly increase log activity and should be turned off as soon as possible.

---

### HOW TO ENABLE VERBOSE LOGGING FOR WINDOWS UPDATE AGENT

To turn on verbose logging, add the following registry key with two values:

**HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\Trace**

Value name: **Flags**

Value type: REG\_DWORD

Value data: **00000007**

Value name: Level

Value type: REG\_DWORD

Value data: **00000004**

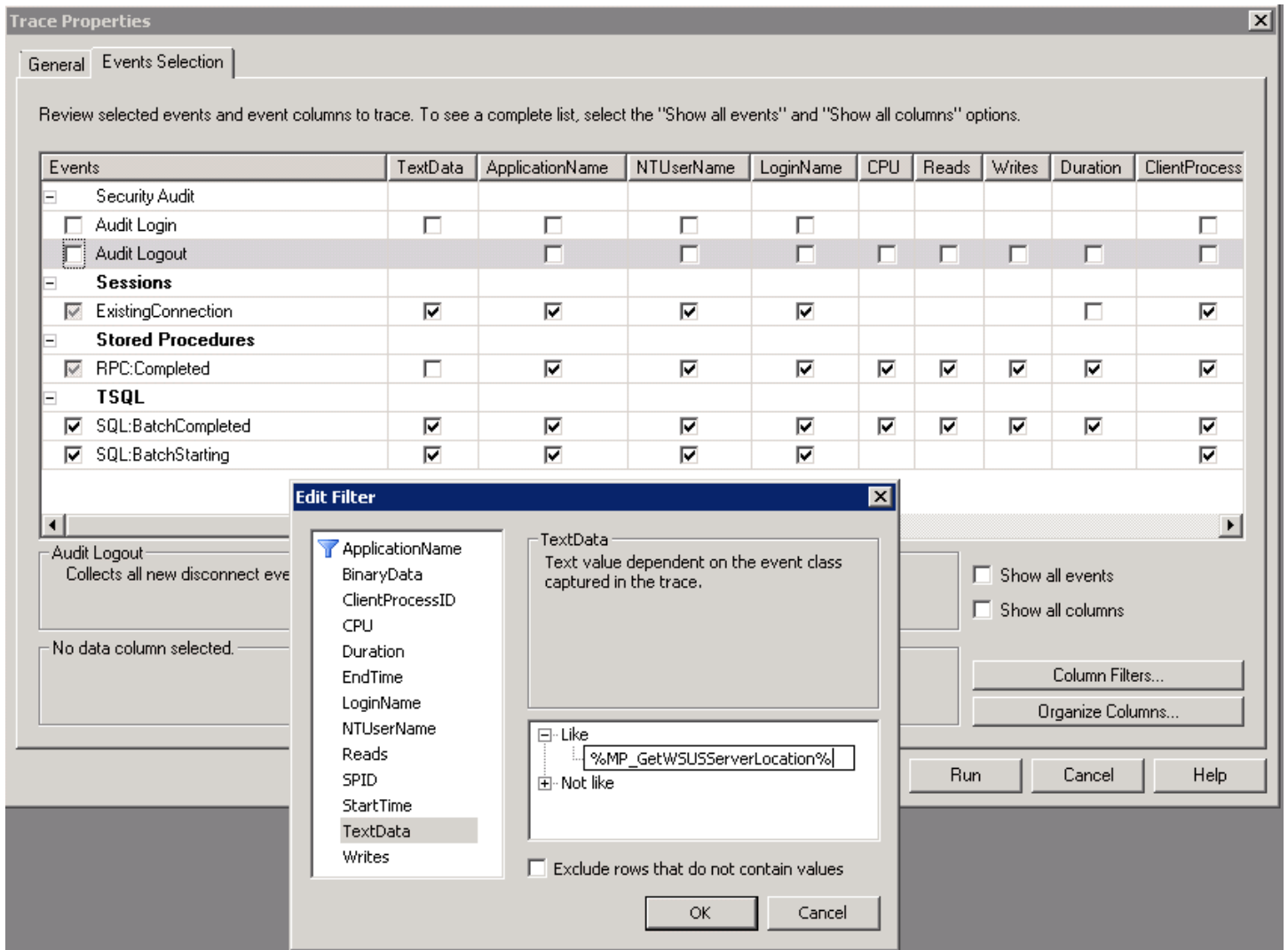
This registry key turns on an extended tracing to the %systemroot%\Windowsupdate.log file. Additionally, this registry key turns on an extended tracing to any attached debuggers.

**NOTE** Extended verbose logging can be enabled by setting the value of **Flags** to 17 instead of 7. However, this will greatly increase the size of WindowsUpdate.log.

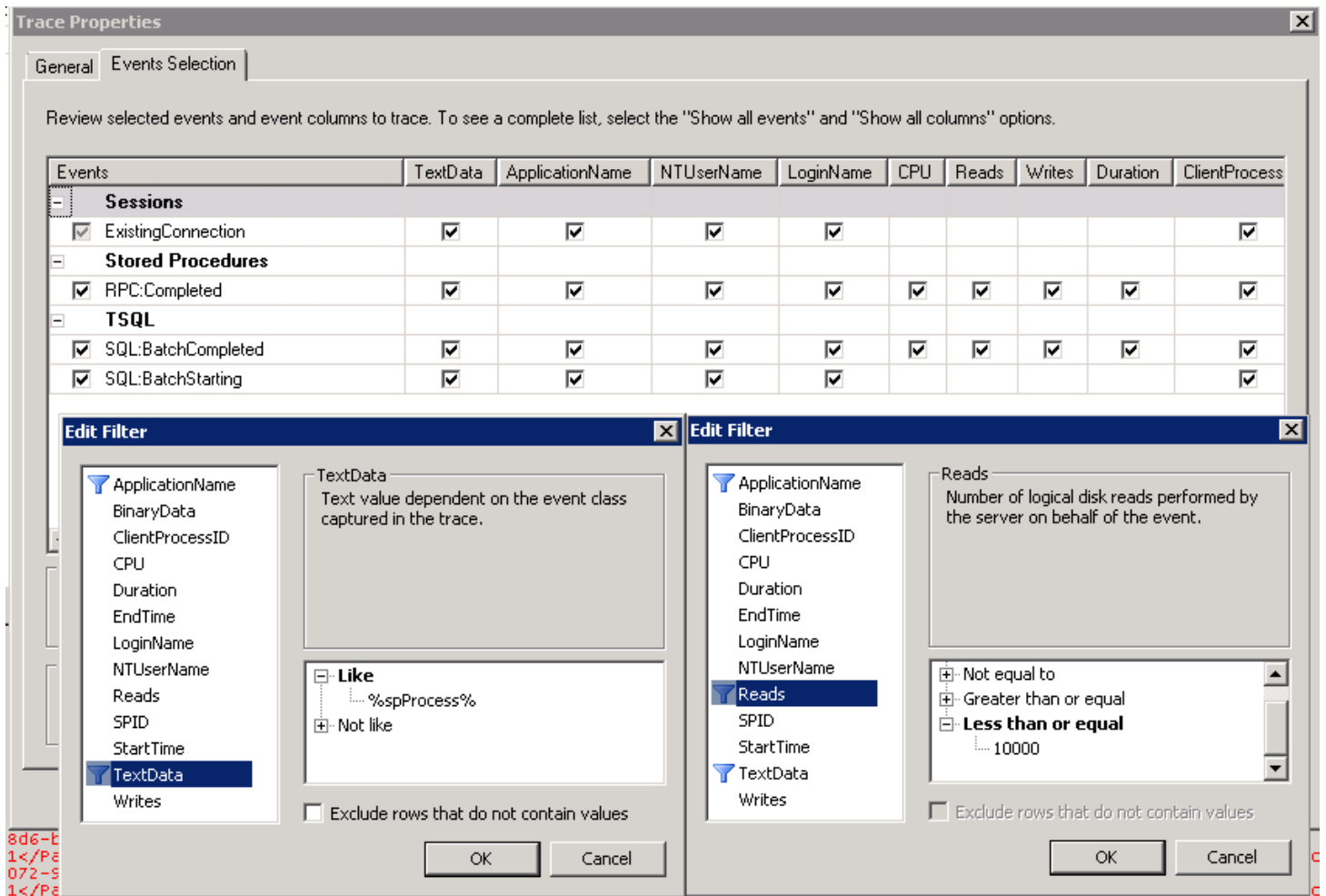
---

### HOW TO CONFIGURE SQL PROFILER TO TROUBLESHOOT WSUS LOCATION REQUEST ISSUES.

In some cases you may need to run a SQL Profiler to find the call to the **MP\_GetWSUSServerLocation** stored procedure and see what parameters are being passed. In order to do this you can configure the SQL Profiler as shown below:



HOW TO CONFIGURE SQL PROFILER TO SEE STATE MESSAGE PROCESSING.



## B. SYNCHRONIZATION

### HOW TO CONFIGURE PROXY SETTINGS FOR THE SOFTWARE UPDATE POINT

When there is a proxy server between the WSUS computer and the upstream update source, the proxy settings must be configured for the Site System as well as the Software Update Point role. The proxy server settings are site system specific, which means that all site system roles use the proxy server settings that you specify. For more information, see [Technical Reference for Accounts used in Configuration Manager](#).

To check the currently configured proxy settings for the computer, see the [“How to Check Proxy Configuration on a Computer”](#) section.

#### To configure the proxy settings for the Site System

1. In the Configuration Manager console, navigate to **Administration pane -> Site Configuration -> Servers and Site System Roles** and click on <SiteSystemName> on the right pane.
2. In the bottom pane, right-click **Site System** and then click **Properties**.
3. Go to the **Proxy** tab and specify the proxy server name, port and credentials (if required).

#### To configure the proxy settings for the Software Update Point

1. In the Configuration Manager console, navigate to **Administration pane -> Site Configuration -> Servers and Site System Roles** and click on <SiteSystemName> on the right pane.
2. In the bottom pane, right-click **Software Update Point** and then click **Properties**.
3. Go to the **Proxy and Account Settings** tab, and select **Use a proxy server when synchronizing software updates**.
4. (Optional) To configure ADRs to use a proxy, go to the **Proxy And Account Settings** tab, and select **Use a proxy server when downloading content by using automatic deployment rules**.

#### To verify Proxy Settings in the WSUS Console

1. Open the WSUS console.
2. Click **Options** in the tree pane, and then click **Update Source and Proxy Server** in the display pane.
3. Click the **Proxy Server** tab. The proxy settings displayed should match the settings configured for the Software Update Point in Configuration Manager. If the settings do not match, check WCM.log on the Site Server.

For more information, see the “Proxy Server Settings” section on the following TechNet website:

[http://technet.microsoft.com/en-us/library/gg712312.aspx#BKMK\\_InstallSUP](http://technet.microsoft.com/en-us/library/gg712312.aspx#BKMK_InstallSUP)

---

#### HOW TO CHECK PROXY CONFIGURATION ON A COMPUTER

Review the proxy configuration for the logged-in user by running the following command:

```
netsh winhttp show proxy
```

To review the proxy configuration for the SYSTEM account, open a command prompt by running the following command:

```
psexec -s -i cmd
```

In the Command Prompt window, run **whoami** to confirm that the command window is running under the System account. Run the **netsh** command again and review the proxy configuration for the System account. You can also start Internet Explorer from this command window and review the proxy configured in Internet Explorer. In some cases you may have to clear the **Automatically Detect Settings** check box, and set the correct proxy.

To force WinHTTP to use Proxy Configuration from Internet Explorer, run the following command:

```
netsh winhttp import proxy source =ie
```

For more help with Netsh WinHTTP commands, see the following:

[http://technet.microsoft.com/en-us/library/cc731131\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/cc731131(v=ws.10).aspx)

---

#### HOW TO CONFIGURE WSUS SERVER CONNECTION ACCOUNT FOR THE SOFTWARE UPDATE POINT

If the Software Update Point is remote to the Site Server, and if the Site Server computer account does not have permissions to connect to the WSUS computer, you must specify a WSUS connection account that Configuration Manager can use to connect to the WSUS computer. This account is used by WCM and WSyncMgr, and it must be a local administrator on the computer where WSUS is installed. Additionally, the account must be part of the local WSUS Administrators group. For more information, see [Technical Reference for Accounts Used in Configuration Manager](#).

#### To configure the WSUS Server connection account for the Software Update Point

1. In the Configuration Manager console, navigate to **Administration pane -> Site Configuration -> Servers and Site System Roles** and click on <SiteSystemName> on the right pane.
2. In the bottom pane, right-click **Software Update Point** and then click **Properties**.
3. On the **Proxy And Account Settings** tab, specify the connection account under **WSUS Server Connection Account**.

---

## HOW TO DETERMINE THE PORT SETTINGS USED BY WSUS

Port settings are configured when the Software Update Point site system role is created. These port settings must be the same as the port settings used by the WSUS website, or else WSUS Synchronization Manager will fail to connect to WSUS running on the Software Update Point to request synchronization. The following procedures provide information about how to verify the port settings used by WSUS and the Software Update Point.

### To determine the WSUS port settings in IIS 6.0

1. On the WSUS server, open Internet Information Services (IIS) Manager.
2. Expand **Web Sites**, right-click the website for the WSUS server, and then click **Properties**.
3. Click the **Web Site** tab. The HTTP port setting is displayed in **TCP port**, and the HTTPS port setting is displayed in **SSL port**.

### To determine the WSUS port settings used in IIS 7.0 and above

1. On the WSUS server, open Internet Information Services (IIS) Manager.
2. Expand **Sites**, right-click the website for the WSUS server and then click **Edit Bindings**. In the **Site Bindings** dialog box, the HTTP and HTTPS port values are displayed in the **Port** column.

### To configure ports for the Software Update Point

1. In the Configuration Manager console, navigate to **Administration pane -> Site Configuration -> Servers and Site System Roles**, and click on <SiteSystemName> on the right pane.
2. In the bottom pane, right-click **Software Update Point** and then click **Properties**.
3. Go to the **General** tab and specify/verify the WSUS configuration port numbers.

---

## VERIFY ANONYMOUS ACCESS IS ENABLED ON THE DSSAUTHWEBSERVICE VIRTUAL DIRECTORY

When WSUS Synchronization Manager on child sites receives a synchronization request from the parent site, anonymous access must be enabled on the DssAuthWebService virtual directory for the WSUS website in Internet Information Services (IIS). Use the following procedure to configure anonymous access and verify that it is enabled on the virtual directory.

### To verify anonymous access on the DssAuthWebService virtual directory

1. On the WSUS computer, open **Internet Information Services (IIS) Manager**.
2. Expand **Sites**, then expand the website for the WSUS server, then click on the **DssAuthWebService** virtual directory.
3. In the **Features view**, double-click **Authentication** and verify that **Anonymous Authentication** is **Enabled**.

---

## CHECK PERMISSIONS ON THE APIREMOTING30 VIRTUAL DIRECTORY

When WSUS Synchronization Manager initiates synchronization, the computer and Administrator accounts must have access to the ApiRemoting30 virtual directory under the WSUS website in Internet Information Services (IIS). Use the following procedure to check the permissions for this virtual directory.

## To check permissions on the ApiRemoting30 virtual directory

1. On the WSUS computer, open **Internet Information Services (IIS) Manager**.
2. Expand **Sites**, expand the website for the WSUS server, right-click the **ApiRemoting30** virtual directory, and then select **Edit Permissions**.

---

## CHECK THE UPDATE SOURCE SETTINGS IN WSUS

When you troubleshoot software updates synchronization issues in Configuration Manager, you might have to check the update source settings in the WSUS console on the Software Update Point site system server. These settings are set automatically by WCM. If these settings do not match, review WCM.log.

### To check the update source settings in WSUS

1. Open the WSUS console on the Software Update Point.
2. Click **Options** in the console tree pane.
3. Click **Update Source and Proxy Server** in the display pane.
4. Verify that the settings below are configured appropriately.

**Synchronize from Microsoft Update:** This setting should generally be selected when you are in the WSUS console on the Software Update Point for the top-level site. Note that starting with Configuration Manager 2012 SP1 you can specify an existing WSUS server as the upstream synchronization source location for the top-level site. If you have specified an existing WSUS computer as the upstream source location then this option should not be selected.

**Synchronize from another Windows Server Update Services server:** This setting should generally be selected when you are in the WSUS console for:

- Software Update Points for top-level site if an upstream source location is specified instead of Microsoft Update.
- Software Update Points for a Primary site.
- Additional Software Update Points installed in the Primary Site.
- Internet-based Software Update Points.
- Software Update Points for a Secondary Site.

**Server name:** The fully qualified domain name (FQDN) name of the upstream update source should be displayed.

- For the first Software Update Point in the Primary site, this should be the Software Update Point for the parent site.
- For additional Software Update Points in the site, this should be the first Software Update Point on the same site.
- For an Internet-based Software Update Point this is the first Software Update Point on the same site.

**Port number:** This should display the port number for the upstream WSUS computer. To determine the port number being used on the upstream WSUS computer see the “Procedure: How to determine the port settings used by WSUS” section.

**Use SSL when synchronizing update information:** When the Software Update Point is in HTTPS mode, this setting must be selected. When using SSL for software updates, several requirements apply. For more information, see [Procedure: Configure Software Updates for Secure Sockets Layer \(SSL\)](#).

**This server is a replica of the upstream server:** This setting should never be selected on the Software Update Point for the Top-Level site or the first Software Update Point for the Primary Site. This setting should be selected on:

- Internet based Software Update Points.
- Additional Software Update Points for the Primary Site.
- Software Update Points for the Secondary Site.

---

## HOW TO TEST CONNECTIVITY FROM SITE SERVER TO WSUS

If the WSUS computer is remote to the Site Server, the WSUS administration console must be installed on the Site Server. This is because the WSUS Administration Console installs the required APIs that are used by Configuration Manager to connect to the WSUS computer. To test whether Configuration Manager can connect to the WSUS computer, use the locally installed WSUS administration console.

### To connect to the remote WSUS computer using the WSUS administration console

1. Start the **WSUS administration console**.
2. Right-click **Update Services** in the tree view, and select **Connect to Server**.
3. Specify the **Server Name** and **Port Number** of the remote WSUS computer, and click **Connect**.

It is important that you specify the FQDN of the Server and the correct Port Number for the connection. If you don't know the port number see the "How to determine the Port Settings used by WSUS" section.

---

## HOW TO CHECK WSUS SERVER VERSION

To check the WSUS server version, start the **WSUS console** and then click on the **Server Name**. You will find the server version under **Overview -> Connection -> Server Version**.

**Table 1: List of current WSUS Server Versions**

WSUS 3.0 SP1	3.1.6001.65
WSUS 3.0 SP2	3.2.7600.226
WSUS 3.0 SP2 + KB2530678	3.2.7600.236
WSUS 3.0 SP2 + KB2720211	3.2.7600.251
WSUS 3.0 SP2 + KB2734608	3.2.7600.256
WSUS 3.0 SP2 + KB2828185	3.2.7600.262
WSUS on Server 2012	6.2.9200.16384
WSUS on Server 2012 + KB2838998	6.2.9200.16384 (does not increment)
WSUS on Server 2012 + KB2819484	6.2.9200.16553
WSUS on Server 2012 R2	6.3.9600.16384

**NOTE** If you review the version in WSUS Console -> Help-> About Update Services, the version may not reflect the installed updates. See the steps above to determine the version.

---

## CONFIGURE SOFTWARE UPDATE POINT FOR SECURE SOCKETS LAYER (SSL)

When the site is configured in "HTTPS only" mode, the Software Update Point is automatically configured to use SSL. When the site is in "HTTPS or HTTP" mode, you can choose to configure the Software Update Point to use SSL. When the Software Update Point is configured to use SSL the WSUS computer must be explicitly configured to use SSL as well. Before you configure SSL please review the [Certificate Requirements](#) and make sure that a Server Authentication certificate is installed on the Software Update Point server.

### To verify that the Software Update Point is configured for SSL

1. In the Configuration Manager console, navigate to **Administration pane -> Site Configuration -> Servers and Site System Roles**, and click **<SiteSystemName>** on the right pane.
2. In the bottom pane, right-click **Software Update Point**, and then click **Properties**.
3. On the **General** tab, click **Require SSL communication to the WSUS Server**.

#### To verify that WSUS Server is configured for SSL

1. Open the **WSUS console** on the Software Update Point for the site.
2. Click **Options** in the console tree pane.
3. Click **Update Source and Proxy Server** in the display pane.
4. Verify that **Use SSL when synchronizing update information** is selected.

#### To add the Server Authentication certificate to the WSUS Administration website

1. On the WSUS computer, open Internet Information Services (IIS) Manager.
2. Expand **Sites**, right-click **Default Web Site** or **WSUS Administration** website if WSUS is configured to use a custom website, and then select **Edit Bindings**.
3. Click the **HTTPS** entry and then click **Edit**.
4. In the **Edit Site Binding** dialog box, select the **Server Authentication** certificate and then click **OK**.
5. Click **OK** in the **Edit Site Binding** dialog box and then click **Close**.
6. Close Internet Information Services (IIS) Manager.

**IMPORTANT** Make sure that the FQDN specified in the Site System properties matches the FQDN specified in the certificate. If the Software Update Point accepts connections from the Intranet only, the Subject Name or Subject Alternative Name must contain the Intranet FQDN. When the Software Update Point accepts client connections from the Internet only, the certificate must still contain both the Internet FQDN and the Intranet FQDN because WCM and WSynMgr still use the Intranet FQDN to connect to the Software Update Point. If the Software Update Point accepts connections from both the Internet and the Intranet, both the Internet FQDN and the Intranet FQDN must be specified by using the ampersand (&) symbol delimiter between the two names.

#### To configure SSL on the WSUS computer

The following link applies to System Center Configuration Manager 2007 but the same steps can also be used to configure SSL on WSUS in ConfigMgr 2012: <http://technet.microsoft.com/en-us/library/bb633246.aspx>

**IMPORTANT** You cannot configure the whole WSUS website to require SSL, because all traffic to the WSUS site would have to be encrypted. WSUS encrypts update metadata only. If a computer tries to retrieve update files on the HTTPS port, the transfer will fail.

## C. COMPLIANCE

---

### HOW TO CHECK PROXY SETTINGS ON A CLIENT

The Windows Update Agent uses WinHTTP to scan for available updates. When there is a proxy server between the client and the WSUS computer, the proxy settings must be configured properly on the clients to allow them to communicate with WSUS using FQDN.

In the case of proxy issues, WindowsUpdate.log may report errors that resemble the following:

*0x80244021 or HTTP Error 502 - Bad gateway*

*0x8024401B or HTTP Error 407 - Proxy Authentication Required.*



0x80240030 - The format of the proxy list was invalid

0x8024402C - The proxy server or target server name cannot be resolved.

In most cases, you can bypass the proxy for local addresses, as the WSUS computer is located within the intranet anyway. However, if the client is on the Internet, you must make sure that the proxy server is configured to allow that communication.

**To view WinHTTP Proxy Settings, you can run the following commands:**

On Windows XP: **proxycfg.exe**

On Windows Vista or above: **netsh winhttp show proxy**

Because proxy settings configured in Internet Explorer are part of the WinINET proxy settings, WinHTTP proxy settings are not necessarily the same as the proxy settings configured in Internet Explorer. However, if the proxy settings are set correctly in IE you can import the proxy configuration from IE.

**To import proxy configuration from Internet Explorer, you can run the following commands:**

On Windows XP: **proxycfg.exe -u**

On Windows Vista and above you can run: **netsh winhttp import proxy source =ie**

For more information see the following:

[900935](#) - How the Windows Update client determines which proxy server to use to connect to the Windows Update Web site (<http://support.microsoft.com/kb/900935>)

---

## HOW TO CHECK IF WSUS SERVER PORTS ARE ACCESSIBLE FROM THE CLIENT

WSUS can be configured to use any of the following ports: 80, 443 or 8530, 8531.

For clients to communicate with the WSUS computer, the appropriate ports must be allowed on the firewall on the WSUS computer. To determine the ports used by the Software Update Point, see the "How to determine the port settings used by WSUS" section.

To check port connectivity from the client, run the following command:

**telnet SUPSERVER.CONTOSO.COM <PortNumber>**

For example: **telnet SUPSERVER.CONTOSO.COM 8530**

If the port is not accessible, telnet will return an error that resembles the following, suggesting that firewall rules must be configured to allow communication for the WSUS Server ports:

*Could not open connection to the host, on port <PortNumber>*

---

## HOW TO VERIFY CONNECTIVITY ON A CLIENT AGAINST THE WSUS (SOFTWARE UPDATE POINT) SERVER

During a scan, the Windows Update Agent needs to communicate with the ClientWebService and SimpleAuthWebService virtual directories on the WSUS Server in order to perform a scan. If the client cannot

communicate with the WSUS Server, the scan fails. This can happen for a number of reasons, including Port configuration, Proxy configuration, Firewalls, and Network connectivity.

To find the URL of the WSUS computer, check the following registry key:

**HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate**

Access the following URL to verify connectivity between the client and the WSUS computer:

***<http://SUPSERVER.CONTOSO.COM:8530/Selfupdate/wuident.cab>***

To check whether the client can access the ClientWebService virtual directory, try to access the following URL:

***<http://SUPSERVER.CONTOSO.COM:8530/ClientWebService/wusserversversion.xml>***

To check whether the client can access the SimpleAuthWebService, try to access the following URL:

***<http://SUPSERVER.CONTOSO.COM:8530/SimpleAuthWebService/SimpleAuth.asmx>***

If any of these fail, some of the possible reasons include:

- Name resolution issues on the client. Verify that you can resolve the FQDN of the WSUS computer.
- Proxy configuration issues. See the “[How to check proxy settings on a client](#)” section.
- Port access issues. See the “[How to check if WSUS Server Ports are accessible from the client](#)” section.
- Other network-related connectivity issues.

---

## HOW TO RESET THE WINDOWS UPDATE AGENT DATA STORE

**To reset the Windows Update Agent data store, follow these steps:**

- Stop the Windows Update service by running the following command: **net stop wuauerv**
- Rename the C:\Windows\SoftwareDistribution folder as C:\Windows\SoftwareDistribution.old.
- Start the Windows Update service by running the following command: **net start wuauerv**
- Initiate a Software Update scan cycle.

---

## HOW TO USE WINDOWS UPDATE TROUBLESHOOTER AND UPDATE THE WINDOWS UPDATE AGENT TO THE LATEST VERSION

The Windows Update Troubleshooter can help resolve some common Windows Update issues that are caused by corrupted or missing components. You can find the Windows Update Troubleshooter along with the list of error codes it detects in the following document:

[2714434](#) - Description of the Windows Update Troubleshooter (<http://support.microsoft.com/kb/2714434>)

For information on how to update the Windows Update Agent, please see the following:

## D. DEPLOYMENT

### HOW TO REVIEW SERVICEWINDOWMANAGER.LOG

ServiceWindowManager.log contains information about maintenance windows and their start/end times. This can be very useful when you're troubleshooting issues related to software update installation on clients.

To find a list of the available maintenance windows (service windows) on a client, open ServiceWindowManager.log, and search for the "Refreshing Service Windows" string. Immediately following this line, you will see a list of the applicable service windows on the machine, such as the following:

```
Refreshing Service Windows..... ServiceWindowManager
  Populating instance of ServiceWindow with ID=7cb56688-692f-4fae-b398-0e3ff4413adb,
ScheduleString=02C159C0381A200002C159C0381B200002C159C0381C200002C159C0381D200002C159C0381E2000, Type=6
  ServiceWindowManager
  This is a one shot Service Window that has already finished. ServiceWindowManager
  Duration for the Service Window is Total days: 0, hours: 00, mins: 00, secs: 00 ServiceWindowManager
  Populating instance of ServiceWindow with ID=90a5f436-364c-48c7-8dc7-c5014abcbea8, ScheduleString=00084AC028592000,
Type=6 ServiceWindowManager
  StartTime is 02/09/14 00:00:00 ServiceWindowManager
  Duration for the Service Window is Total days: 1, hours: 05, mins: 00, secs: 00 ServiceWindowManager
  Populating instance of ServiceWindow with ID=45dca355-3249-4845-b8aa-72d0e604548e, ScheduleString=02C24AC0381C2000,
Type=6 ServiceWindowManager
  StartTime is 02/12/14 22:00:00 ServiceWindowManager
  Duration for the Service Window is Total days: 0, hours: 07, mins: 00, secs: 00 ServiceWindowManager
  Populating instance of ServiceWindow with ID=87e4759c-2884-45e6-9261-c33ba53f596c, ScheduleString=02C24AC0381D2000,
Type=6 ServiceWindowManager
  StartTime is 02/13/14 22:00:00 ServiceWindowManager
  Duration for the Service Window is Total days: 0, hours: 07, mins: 00, secs: 00 ServiceWindowManager
  Populating instance of ServiceWindow with ID={1E957DDD-0A26-434C-952A-586F3E31E319},
ScheduleString=00302B0018192000, Type=1 ServiceWindowManager
  StartTime is 02/16/14 01:00:00 ServiceWindowManager
  Duration for the Service Window is Total days: 0, hours: 03, mins: 00, secs: 00 ServiceWindowManager
  Populating instance of ServiceWindow with ID=36da6950-3d1e-4027-be0e-7b16a4daee7e, ScheduleString=02C24AC0101E2000,
Type=6 ServiceWindowManager
  StartTime is 02/14/14 22:00:00 ServiceWindowManager
  Duration for the Service Window is Total days: 0, hours: 02, mins: 00, secs: 00 ServiceWindowManager
  Populating instance of ServiceWindow with ID=028bfbc0-7120-4081-a268-0e664a92ac4a, ScheduleString=00074AC0005F2000,
Type=6 ServiceWindowManager
  StartTime is 02/15/14 00:00:00 ServiceWindowManager
  Duration for the Service Window is Total days: 1, hours: 00, mins: 00, secs: 00 ServiceWindowManager
  Populating instance of ServiceWindow with ID=49fd80be-ac4b-4877-974d-ecd09958926d, ScheduleString=02C24AC0381B2000,
Type=6 ServiceWindowManager
  StartTime is 02/11/14 22:00:00 ServiceWindowManager
  Duration for the Service Window is Total days: 0, hours: 07, mins: 00, secs: 00 ServiceWindowManager
  Populating instance of ServiceWindow with ID=ad27b0ca-8c74-43c7-8200-1f601880bd75, ScheduleString=02C24AC0381A2000,
Type=6 ServiceWindowManager
  StartTime is 02/10/14 22:00:00 ServiceWindowManager
  Duration for the Service Window is Total days: 0, hours: 07, mins: 00, secs: 00 ServiceWindowManager
```

Generally, Service windows with IDs containing all lowercase alpha-numeric characters are non-business hour (NBH) maintenance windows. These are based on business hours configured in Software Center. However, Service Windows with IDs containing all uppercase alpha-numeric characters are maintenance windows defined for the collection in the Configuration Manager console. In the preceding log excerpt, all Service windows are non-business hour windows except the one with ID 1E957DDD-0A26-434C-952A-586F3E31E319 (which is a maintenance window defined for the collection that holds the client).

---

## HOW TO REVIEW THE AUDIT STATUS MESSAGES TO FIND IF A DEPLOYMENT WAS MODIFIED

To review audit status messages, go to Configuration Manager Console -> Monitoring pane -> System Status -> Status Message Queries. Right-click **All Status Messages**, click **Show Messages**, select the timeframe, and then click **OK**. In the Configuration Manager Status Message Viewer window, go to View -> Filter and filter for Message ID = 30197.

If the Deployment was modified, you will see a Status Message that resembles the following:

SeverityType	Site code	Date / Time	System Component	Message ID	Description
Information	Audit PR1	2/9/2014 11:57:49 PM	PR1SITE.CONTOSO.COM Microsoft.ConfigurationManagement.exe	30197	User " <b>DOMAIN\User</b> " modified updates assignment 4 ({ <b>BAFB1BDB-7A6C-4DCF-9866-6C22DF92346A</b> }).

## ADDITIONAL RESOURCES

### HOW MANY CLIENTS CAN THE SOFTWARE UPDATE POINT SUPPORT?

[http://technet.microsoft.com/en-us/library/gg712696.aspx#BKMK\\_SUMCapacity](http://technet.microsoft.com/en-us/library/gg712696.aspx#BKMK_SUMCapacity)

### WHAT'S THE MAXIMUM NUMBER OF UPDATES YOU CAN HAVE IN A DEPLOYMENT?

[http://technet.microsoft.com/en-us/library/gg712696.aspx#BKMK\\_SUMCapacity](http://technet.microsoft.com/en-us/library/gg712696.aspx#BKMK_SUMCapacity)

### CAN I MANAGE SOFTWARE UPDATES FOR CLIENTS IN AN UNTRUSTED FOREST?

[http://technet.microsoft.com/en-us/library/gg712701.aspx#Plan\\_Com\\_X\\_Forest](http://technet.microsoft.com/en-us/library/gg712701.aspx#Plan_Com_X_Forest)  
[http://technet.microsoft.com/en-us/library/gg712696.aspx#BKMK\\_SUP\\_CrossForest](http://technet.microsoft.com/en-us/library/gg712696.aspx#BKMK_SUP_CrossForest)