



Microsoft®

System Center Configuration Manager

**Software Center Update Publisher (SCUP) /
Software Update Point (SUP)**

APSCNLAN Support

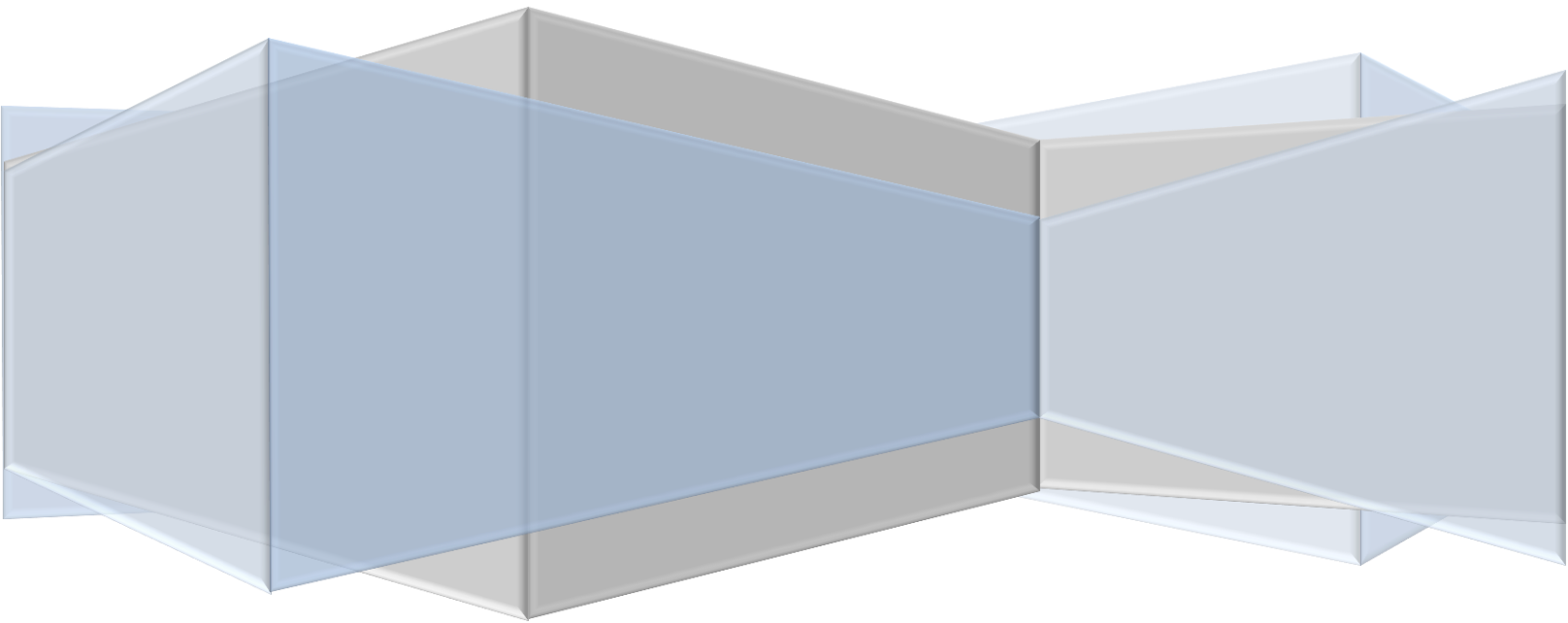


Table of Contents

Setup WSUS and SCUP	1
Setup WSUS for System Center Software Update Point (SUP).....	1
Installing WSUS	1
Setup SCUP 2011.....	3
Installation	3
Configuring SCUP 2011	4
Export SCUP Certificate	6
Setting up GPO to deploy Certificate	7
Creating GPO for the domain	7
Creating Package/Program for distribution of Certificate to client systems.....	9
Adding and deploying partner catalog.....	10
Publish 3 rd Party Updates	12
Software Update Point Site System Role	14
Install and Configure a Software Update Point	14
Create Folders and Collections for SUP.....	16
Initiating the SUP Synchronization.....	18
Automatic Deployment Rules.....	19
ADR: Endpoint Protection.....	19
ADR: Windows 7 Patch Tuesday	23
ADR: Adobe Updates.....	29
Monitoring and Troubleshooting.....	32
Monitor the WsyncMgr.log file to determine Sync Activity	32
Monitor the RuleEngine.log file to determine ADR activity	33
Monitor our Deployment Package getting distributed to our Distribution Points.....	36
Monitor the Windows update process on our clients	38

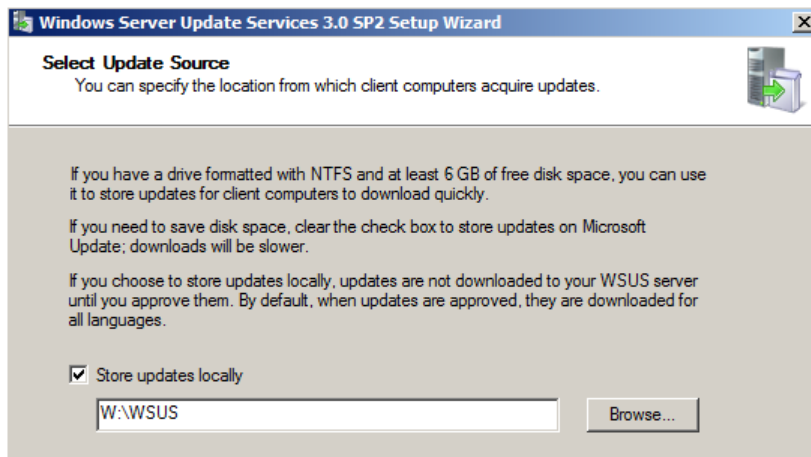
Setup WSUS and SCUP

Setup WSUS for System Center Software Update Point (SUP)

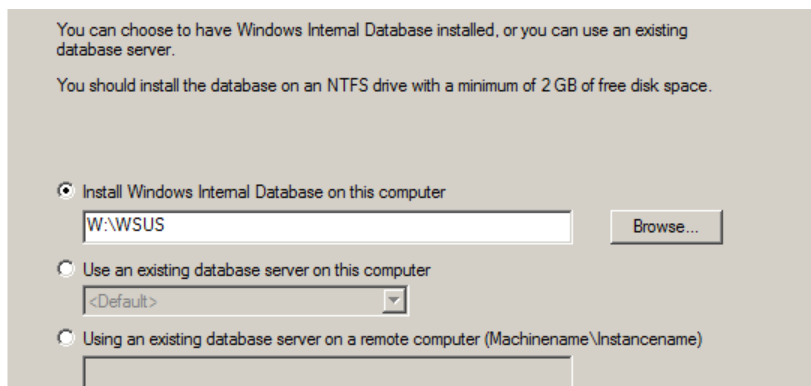
The WSUS Setup Wizard is launched from Server Manager or from the WSUSSetup.exe file.

Installing WSUS

1. On the Welcome page of the Windows Server Update Services 3.0 Setup Wizard, click **Next**.
2. On the Installation Mode Selection page, select **Full server installation including Administration Console** if you want to install the WSUS server on this computer.
3. On the License Agreement page, read the terms of the license agreement, click **I accept the terms of the License agreement**, and then click **Next**.
4. You can specify where clients get updates on the Select Update Source page of the installation wizard. By default, the **Store updates locally** check box is selected and updates will be stored on the WSUS server in the location that you specify. If you clear the **Store updates locally** check box, client computers obtain approved updates by connecting to Microsoft Update. Make your selection, and then click **Next**.

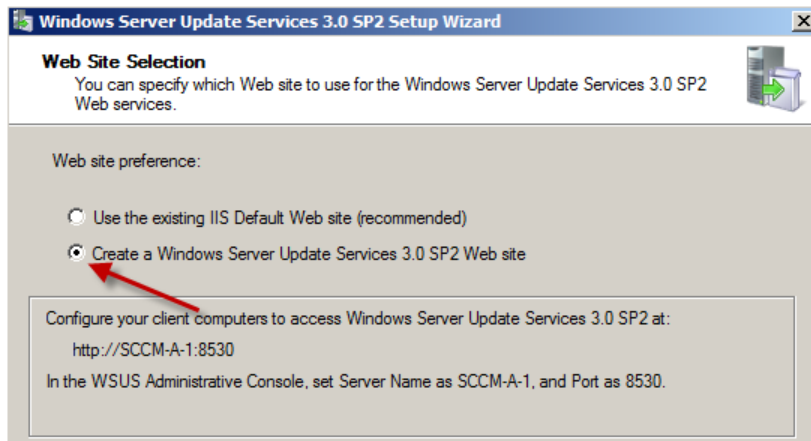


5. On the Database Options page, select the software that will be used to manage the WSUS database. By default, the installation wizard offers to install **Windows® Internal Database**. Click **Next**.

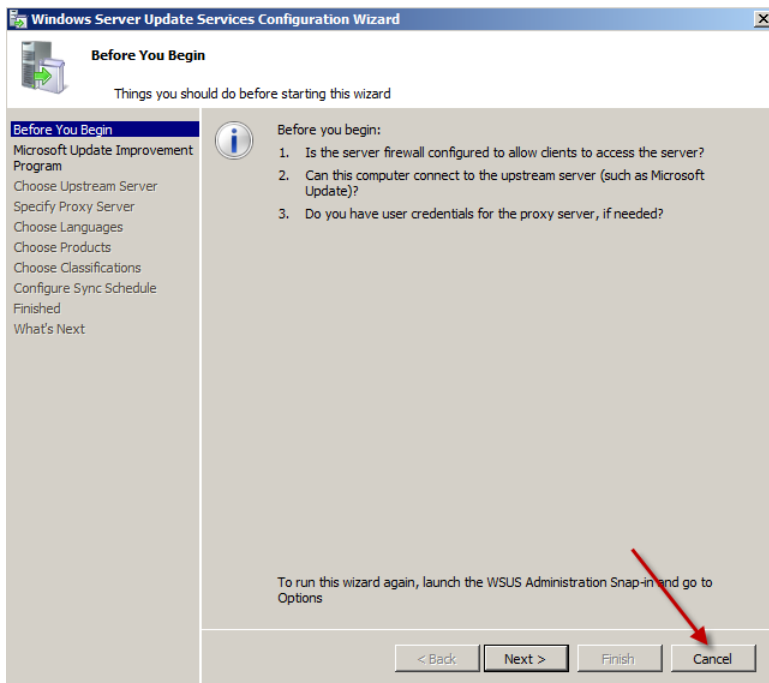


6. On the Web Site Selection page, specify the Web site that WSUS will use. System Center Configuration Manager Will be using port 80, so you can create an alternate site on port 8530 or 8531 by selecting **Create a Windows**

Server Update Services 3.0 SP2 Web site. Click Next.



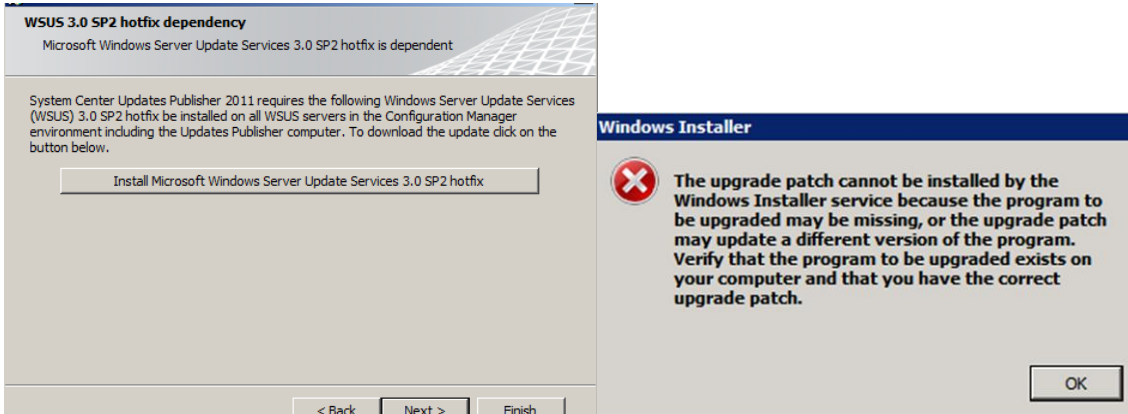
7. On the **Ready to Install Windows Server Update Services** page, review the selections, and then click **Next**.
8. The final page of the installation wizard will let you know if the WSUS installation completed successfully. After you click **Finish** the configuration wizard will start. Close the Configuration Wizard. We will configure WSUS inside the SCCM Console.



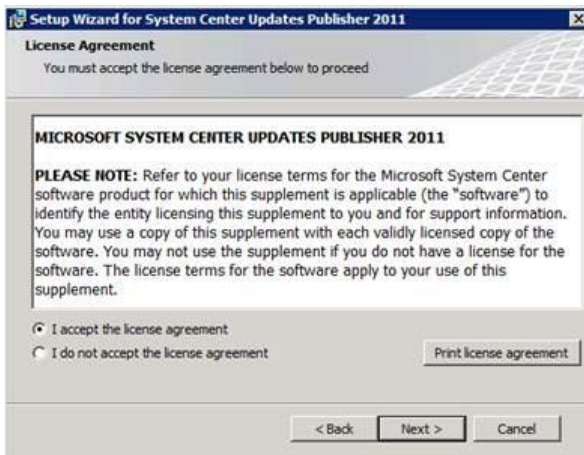
Setup SCUP 2011

Installation

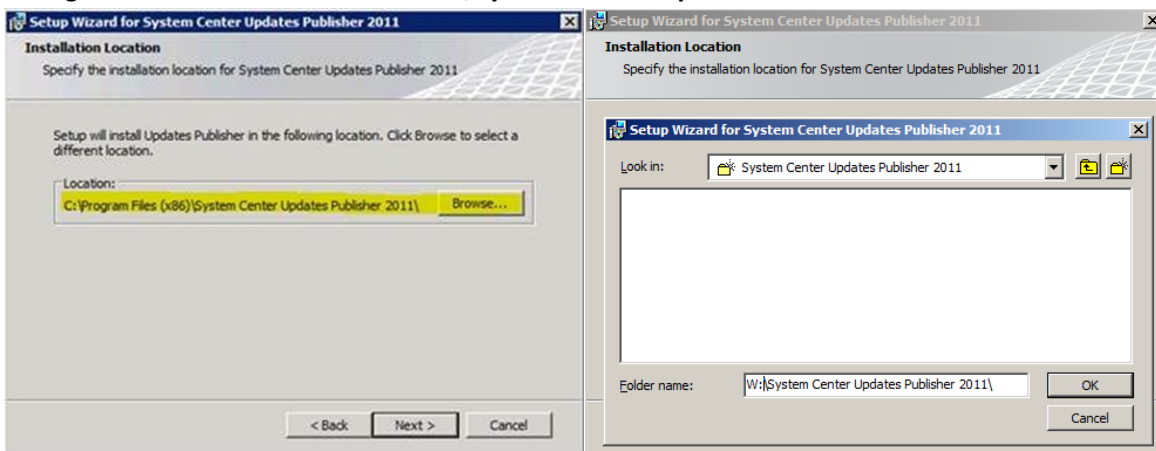
1. Download SCUP 2011 from this link - <http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=11940>
2. Locate SystemCenterUpdatesPublisher.msi and double click on it to start the installation of SCUP 2011. Click "Install Microsoft Windows Server Update Services 3.0 Sp2 hotfix" if it is not installed already and click **Next** to continue



3. **Accept** the License Agreement and click Next.



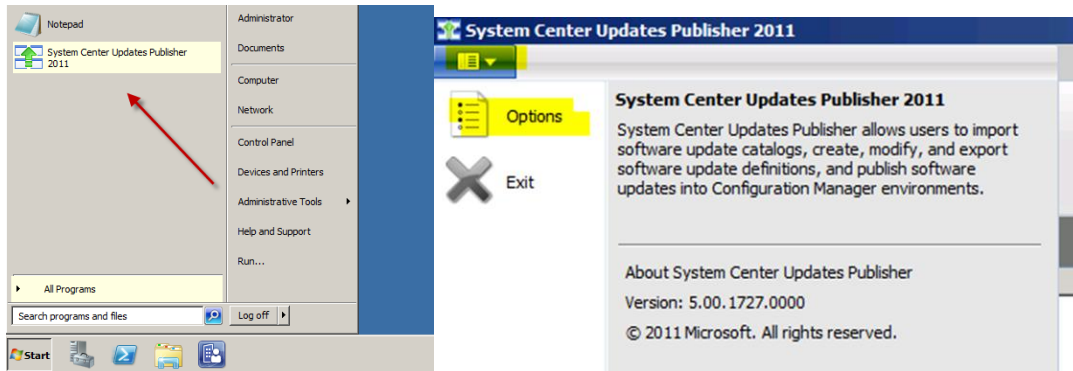
4. Change the Installation Location to **w:\ System Center Update Publisher 2011**.



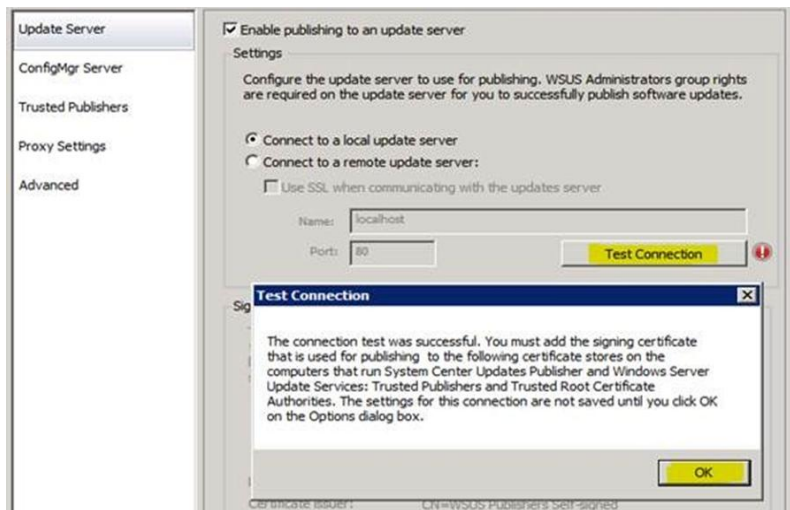
5. Click Next until you reach Finish option.

Configuring SCUP 2011

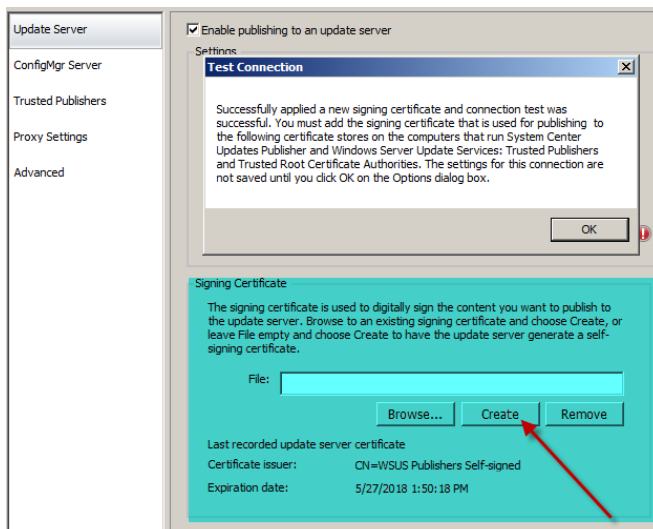
1. Connect to SCUP 2011 console and choose "Options"



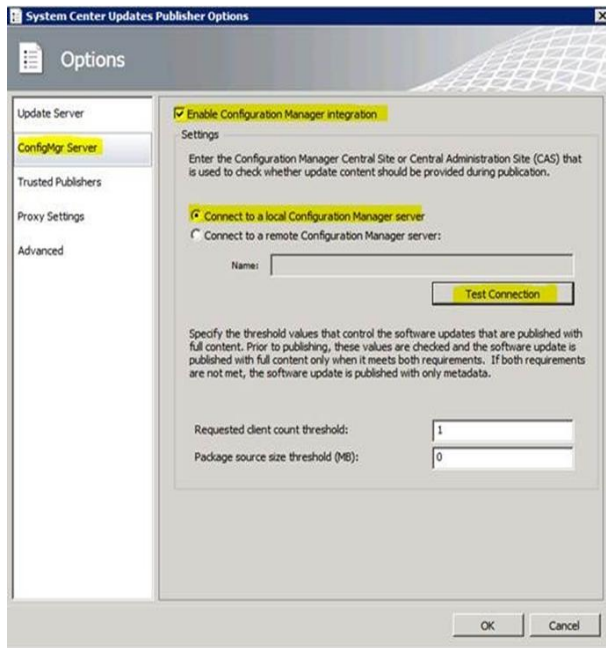
2. Check "Enable publishing to an update server" option under "Update Server" tab
3. If Update server is local then choose "Connect to a local update server". Click on "Test Connection" and make sure it is able to connect successfully.



4. If you are **not** running your own CA Server, you will need to create a Self-Signed Certificate. Click Create and then OK.



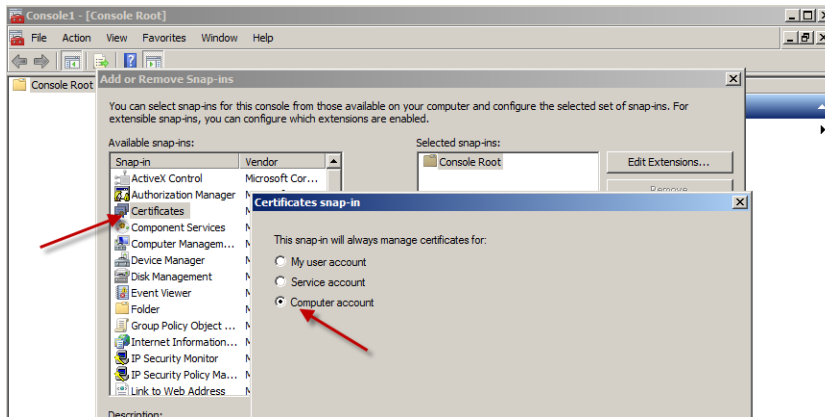
5. Under "ConfigMgr Server" tab, check "Enable Configuration Manager integration" option and choose local or remote ConfigMgr server accordingly. Again, click on "Test Connection" to make sure it is able to connect successfully.



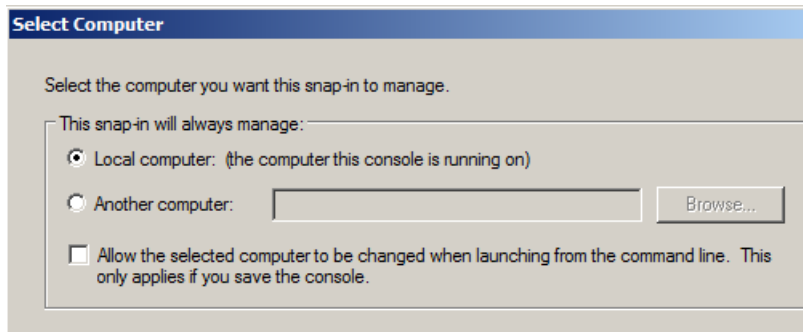
6. Set Proxy Settings and other options under Advanced tab according to your environment.

Export SCUP Certificate

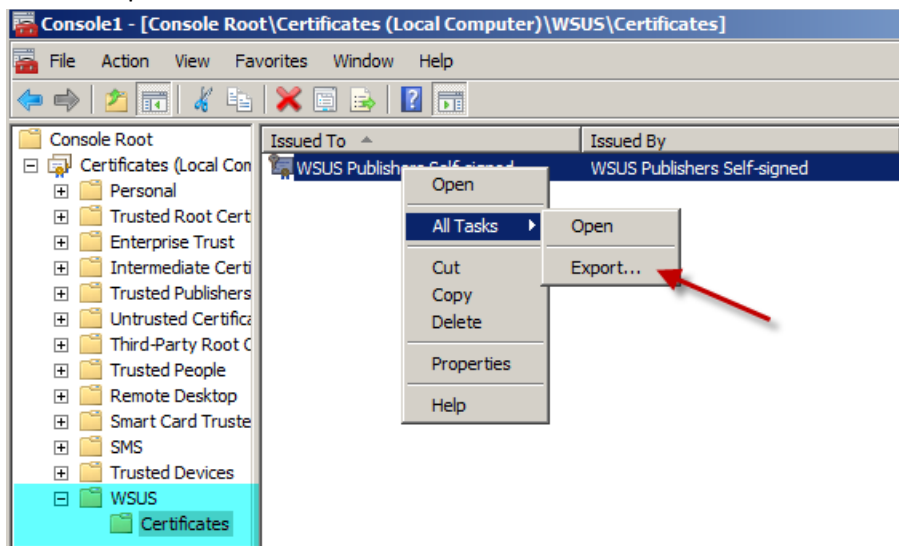
1. Run MMC and add the Certificate Snap-In



2. Choose Local Computer: (the computer the console is running on)



3. Browse down to the WSUS\Certificate and Right Click the WSUS Published Certificate and under All Tasks, Choose Export.

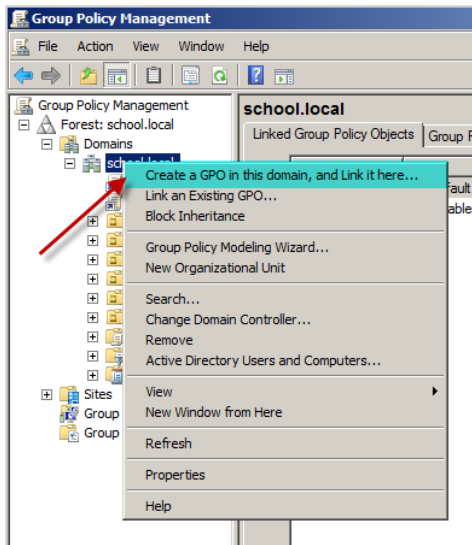


4. Take the defaults for the Certificate Export Wizard. Name the certificate SCUPCert.cer.
5. Browse to the Trusted Root Certificate Authorities \ Certificates and right click and import the SCUPCert.Cer you just created.
6. Browse to the Trusted Publishers\Certificate and right click and import the SCUPCert.Cer you just created.

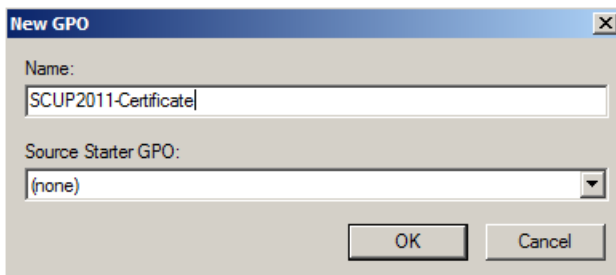
Setting up GPO to deploy Certificate

Creating GPO for the domain

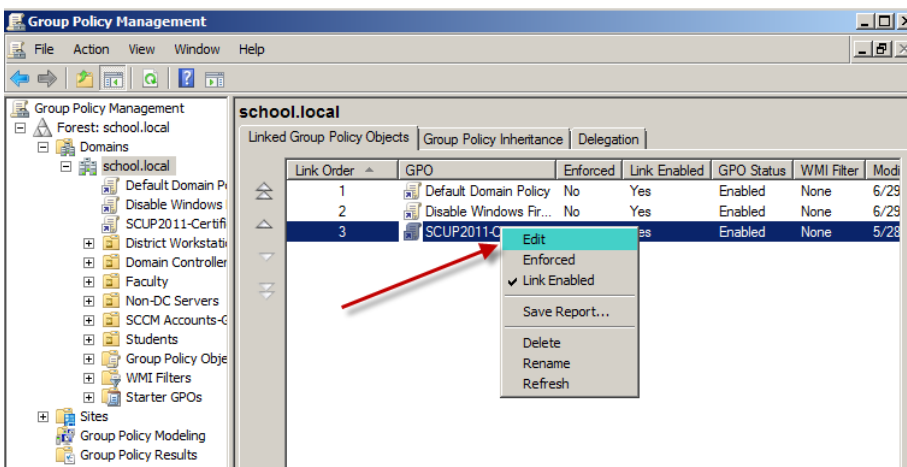
1. Connect to Group Policy Management through MMC



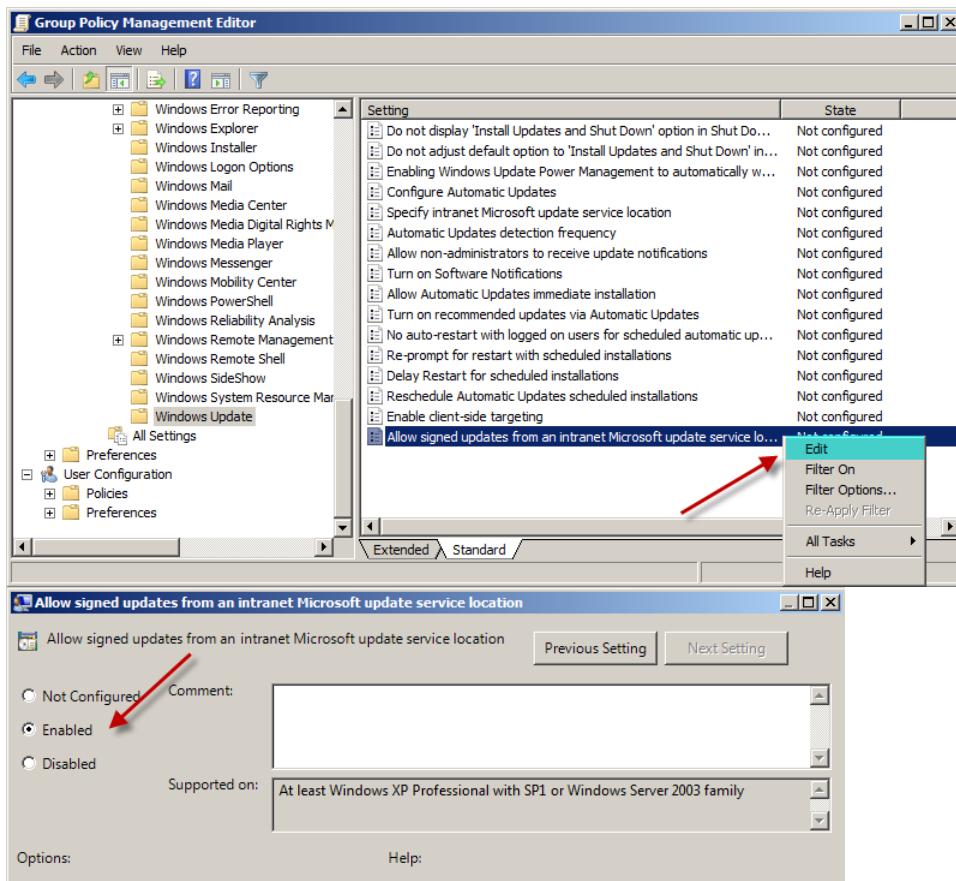
2. Browse through the Domain and right click and choose "Create a GPO in this domain, and Link it here..." option



3. Fill out the Name and Source Starter GPO information



4. Right click on that GPO you just created and click "Edit"



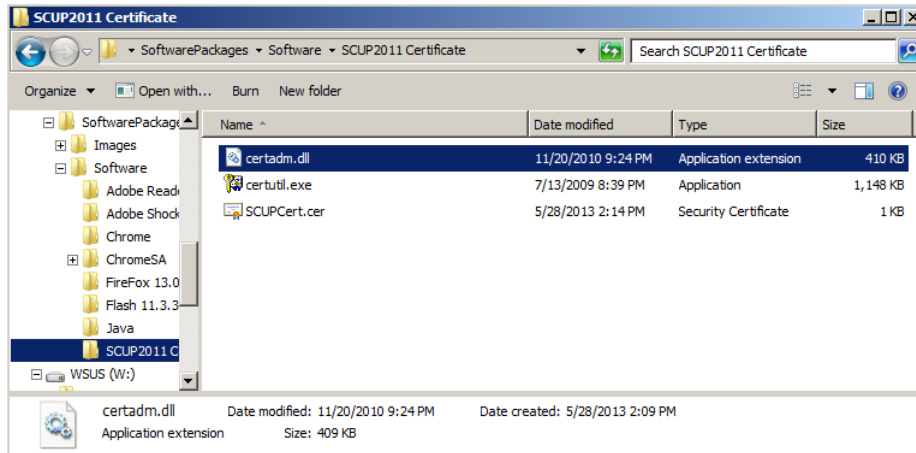
5. Go to Computer Configuration \ Policies\Administrative Templates \Windows Components \Windows Update \ "Allow signed updates from an intranet Microsoft update service location" and Enabled it.
6. Once you create above GPO then refresh group policy on any client which is part of the domain and check the following registry key to make sure this GPO has been applied properly:

HKLM\ Software \Policies \Microsoft\Windows \Windows Update \AcceptTrustedPublisherCerts and the value for this REG_DWORD is set to 1

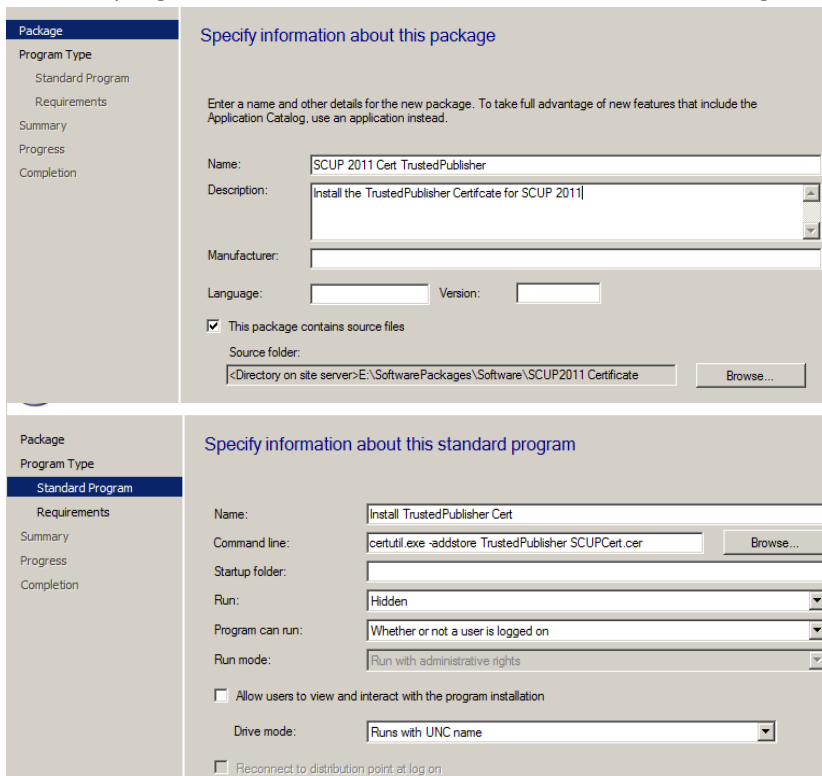
Creating Package/Program for distribution of Certificate to client systems

Important: You need to deploy certificate to all of the systems that are ConfigMgr clients in your environment.

1. Create Package with the following files as a source:

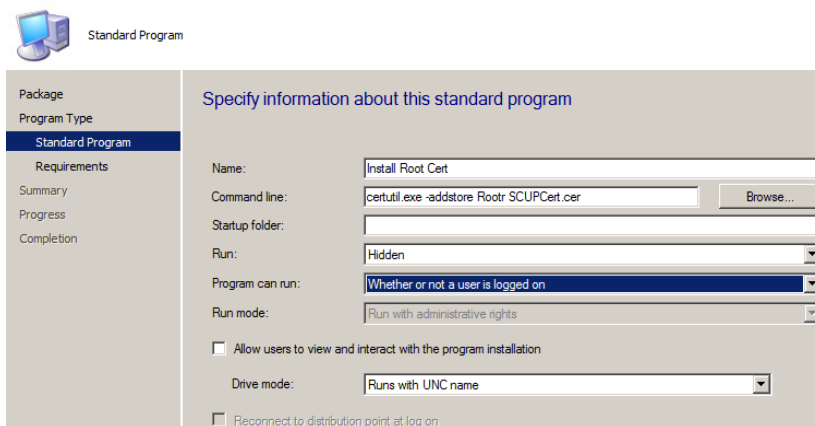
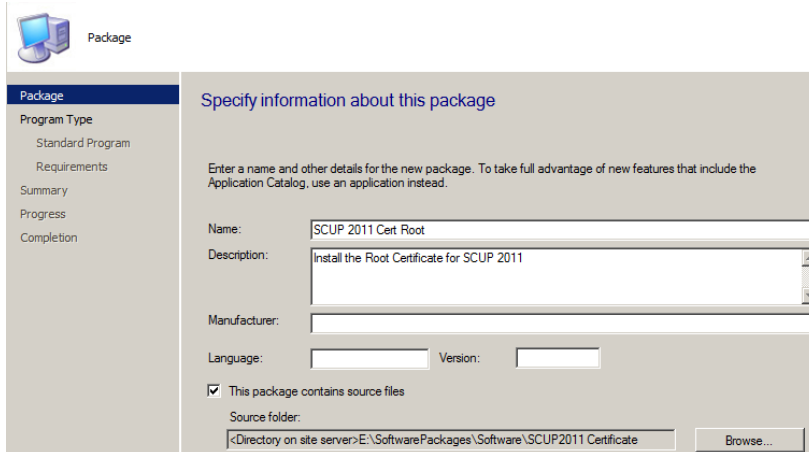


- a. **Certutil.exe** (This file is part of Windows 2003 server and located under %windir%\system32, by default.) If you still have 32bit workstations on your network, you will have to get this file from a 32bit Windows 7 workstation.
 - b. **Certadm.dll** (This file is part of Windows 2003 server and located under %windir%\system32, by default.)
 - c. **SCUPCert.cer** (This file is the one you exported from WSUS server)
2. Create a program (to store certificate to TrustedPublisher) using the following options and command line:



- a. Command Line: certutil.exe -addstore TrustedPublisher SCUPCert.cer

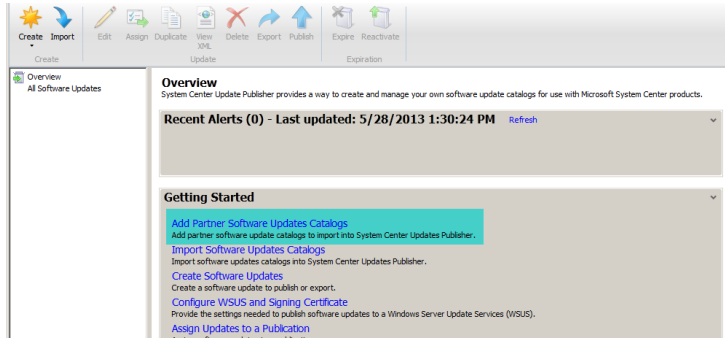
- b. Run: Hidden
- 3. Create a second program (to store certificate to the Root) using the following command line and options (i.e. dependency chain with first program):



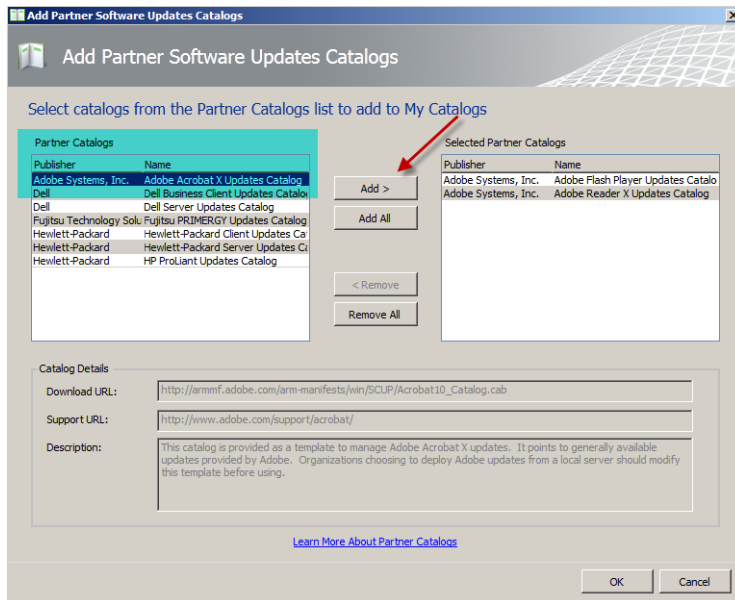
- a. Command Line: certutil.exe -addstore Root SCUPCert.cer
- b. Run: Hidden
- 4. Distribute the 2 Programs
- 5. Deploy "SCUP 2011 Cert Root program" as this root program is running another program first (TrustedPublisher Cert).
- 6. Once you are done with deployment of the certificate then you will be able to deploy SCUP updates to your ConfigMgr environment.

Adding and deploying partner catalog

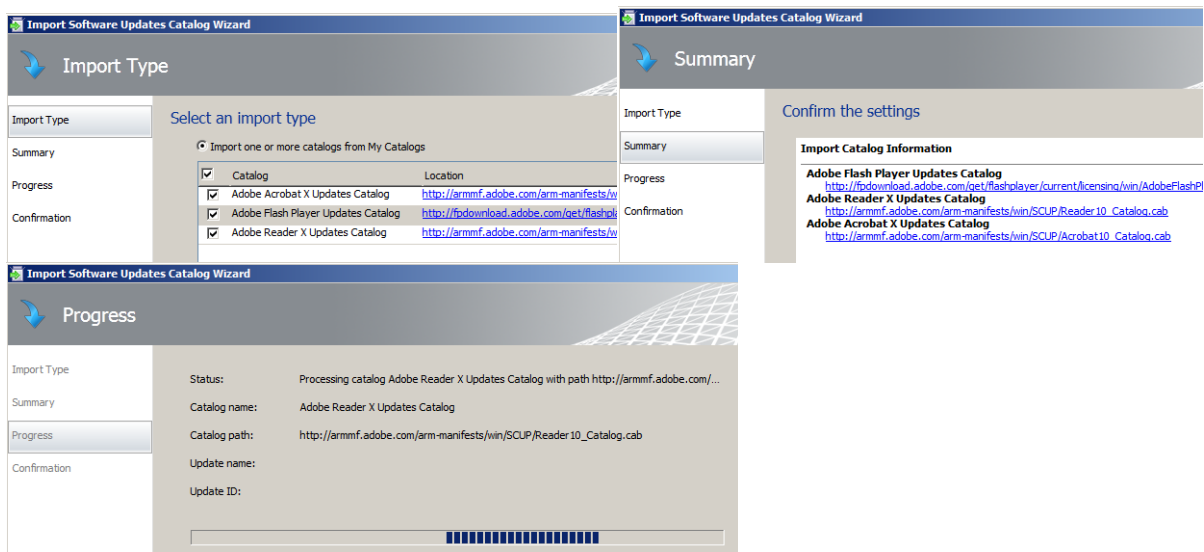
1. Connect to SCUP 2011 console and In the Overview Screen, click on "Add Partner Software Updates Catalogs"



2. Highlight the catalog and click on Add



3. Go to Catalogs tab and you will see the list of catalogs. Highlight the one you want to import and right click and choose "Import"

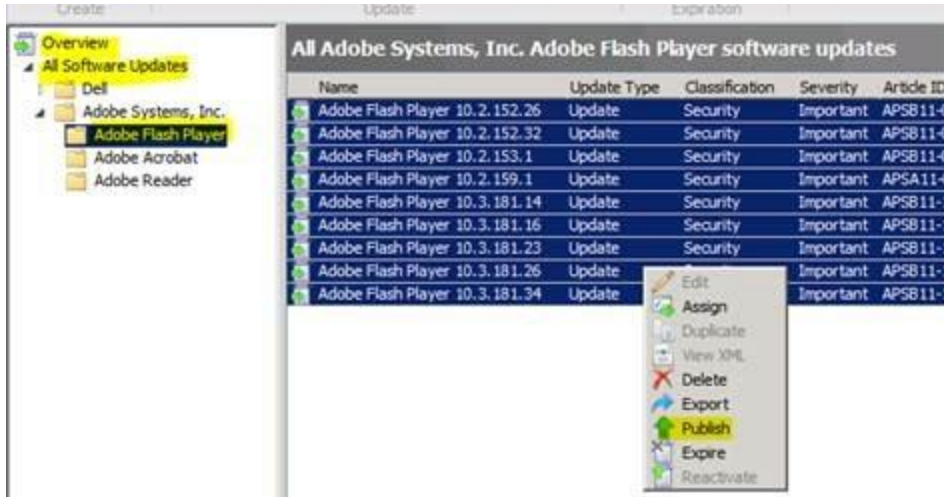


4. Follow the wizard by clicking Next Accept the Certificate if Prompted.

Publish 3rd Party Updates

Once 3rd party catalog is successfully imported into SCUP then you need to publish those updates so that they can be synced with Configuration Manager.

1. Click on Updates tab and choose the updates you want to publish



2. Choose **Full Content** and Click **Next** and follow the wizard to complete the publish process. Accept the Certificates if Prompted.



3. Once Updates are published then you can sync them with Configuration Manager using Configuration Manager Console. Once they are in Configuration Manager Console then those updates are available for deployment just like any other Microsoft updates

4. To run the sync, connect to the Configuration Manager 2012 console and browse through Software Updates node and right click on "All Software Updates" and choose " Synchronize Software Updates" option
5. Review WsyncMgr.log and notice the following:
6. Once they are successfully synchronized with Configuration Manager then you will be able to see it in the console and able to deploy them just like any other updates.

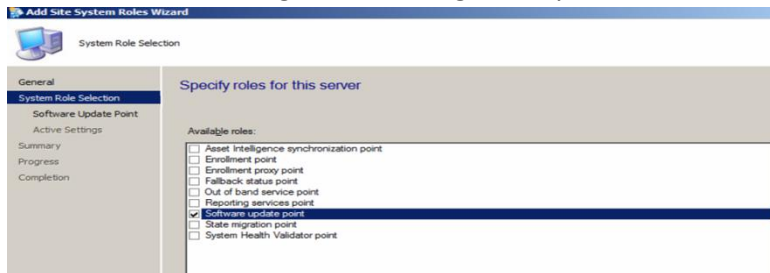
Software Update Point Site System Role

Install and Configure a Software Update Point

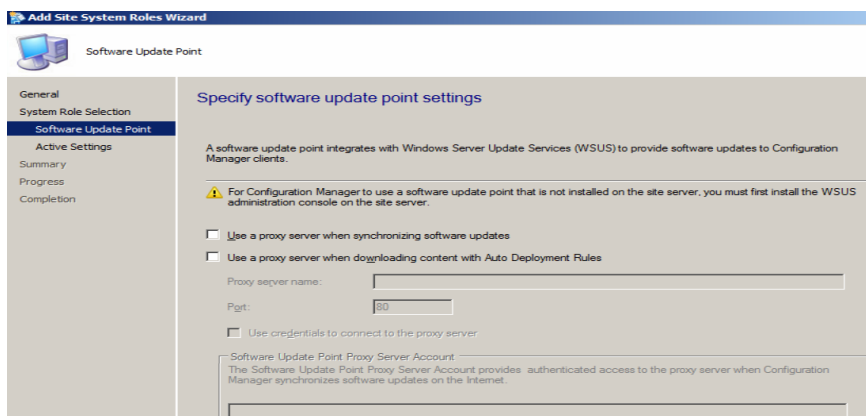
The software update point site system role must be created on a server that has WSUS installed. The software update point interacts with the WSUS services to configure the software update settings and to request synchronization of software updates metadata.

You can add the software update point site system role to an existing site system server or you can create a new one.

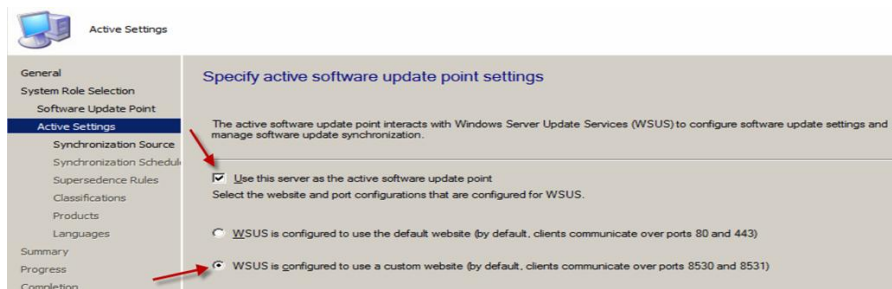
1. On the **System Role Selection** page of the **Create Site System Server Wizard** or **Add Site System Roles Wizard** , depending on whether you add the site system role to a new or existing site server, select **Software update point**, and then configure the software update point settings in the wizard. The settings are different depending on the version of Configuration Manager that you use



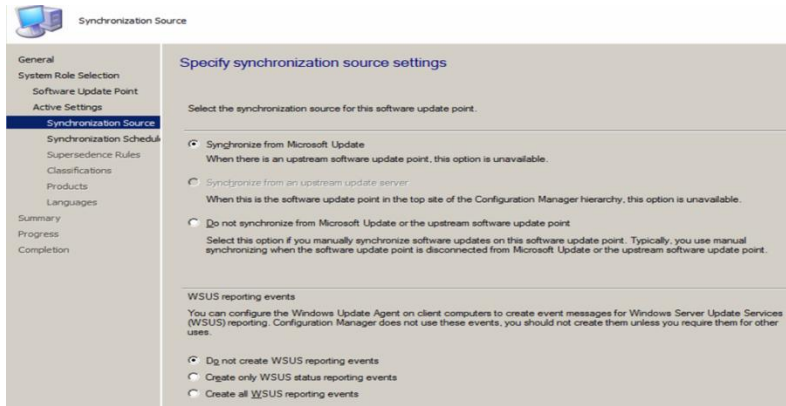
2. Proxy Server Settings - You can configure the proxy server settings on different pages of the **Create Site System Server Wizard** or **Add Site System Roles Wizard** depending on the version of Configuration Manager that you use.



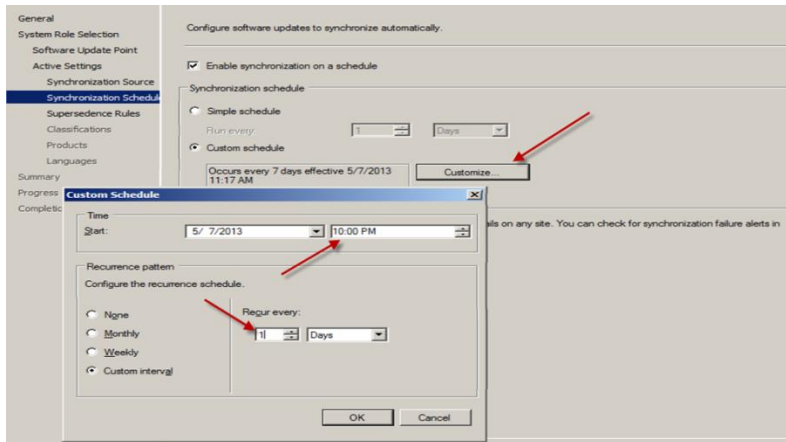
3. On the **Active Settings** page of the wizard, Select **Use this server as the active software update point**. Select **WSUS is configured to use the custom website by default, clients communicate over ports 8530 and 8531**. Click Next



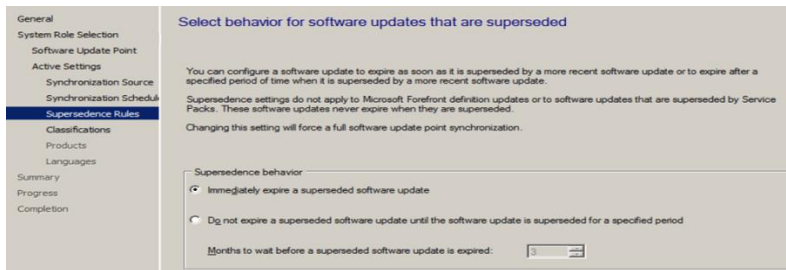
- On the **Synchronization Source** page for the wizard, Select Synchronize from Microsoft Updates and Select Do not create WSUS reporting events. Click Next.



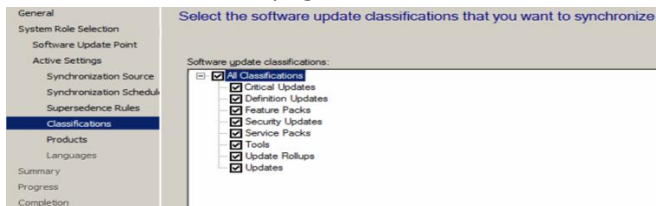
- On the **Synchronization Schedule** page of the wizard, Click on **Customize** and set the **Custom Schedule** to **Every 1 day at 10:00 pm**, Click **OK** and **Next**.



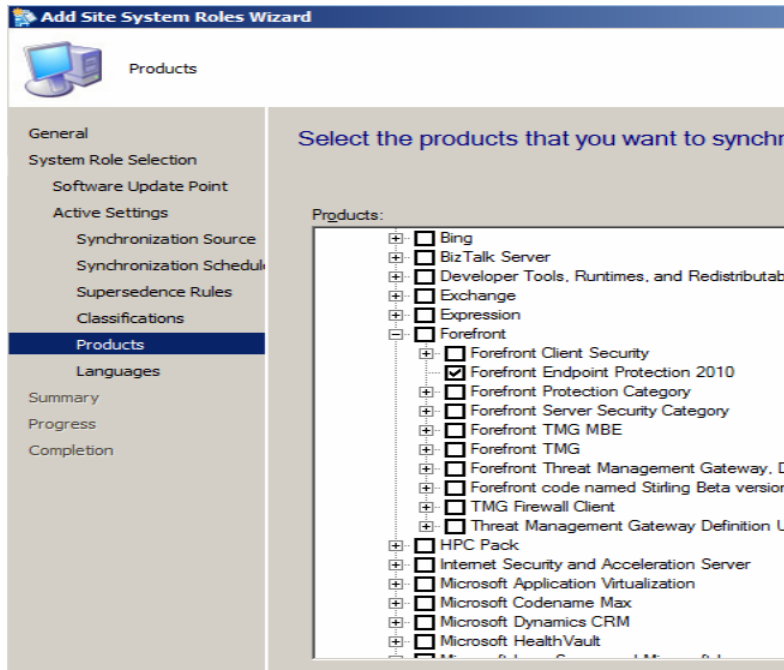
- On the **Supersede Rules** page of the wizard, Select **Immediately expire a suspended software update**. Click **Next**.



- On the **Classifications** page of the wizard, Select **ALL** of the Classifications. Click **Next**.



- On the **Products** page of the wizard, Select all of the products you wish to update. Make sure you include Forefront Endpoint Protection 2010.



- On the **Languages** page of the wizard, Select **English**. Click **Next** to finish out the Wizard.

Create Folders and Collections for SUP

To make the management of Software Updates easier we will first create some **Folders** and populate them with **Collections**. You can do this manually in the **Assets and Compliance** workspace or you can do it in an automated way using PowerShell. The below script will create a nice **Folder and Collection** structure sorting the Client Operating Systems and 3 Windows Server Operating Systems, in addition, the server Operating Systems are further divided into **Automatic** patching, **Manual** patching and **Maintenance Windows** collections. Here's the script we found on Windows-noob.com.

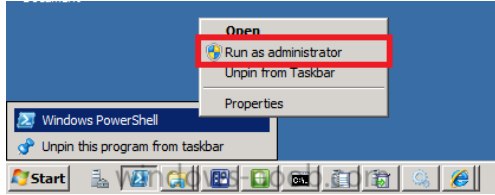
- Download [powershell scripts.zip](#) –

http://www.windows-noob.com/forums/index.php?app=core&module=attach§ion=attach&attach_id=8609

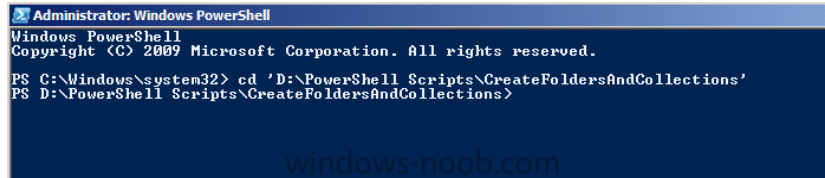
Note: You may have to do the following for the downloaded powershell scripts.

- Save the script file on your computer, locate the saved script file.
- Extract the contents and then locate the powershell PS1 scripts, right-click each script file, and then click Properties.
- Click **Unblock**.

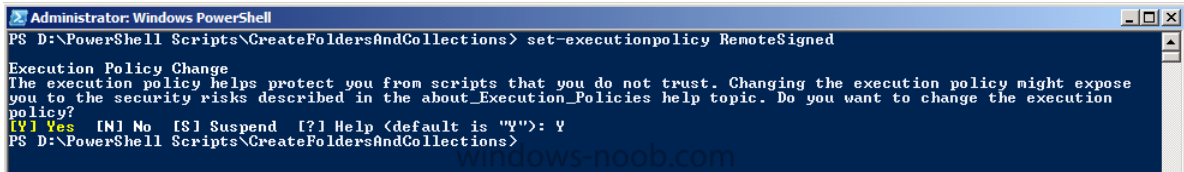
- Run the script in a **Windows PowerShell** session as administrator by right-clicking on the Windows PowerShell icon and choosing **Run As Administrator** as in the screenshot below.



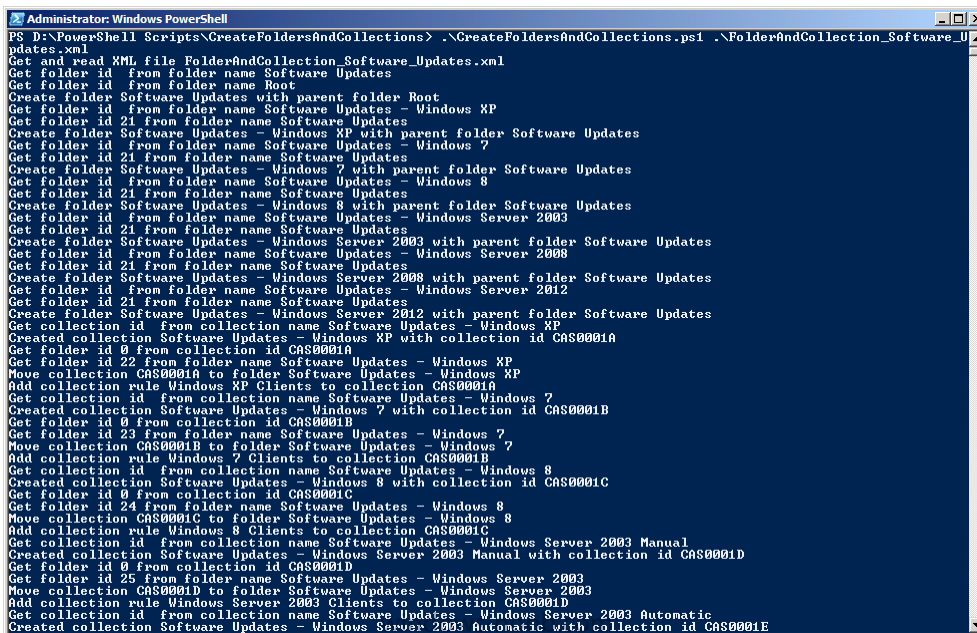
- Change to the **Directory** where you've unzipped the script using **CD** (to change directory).



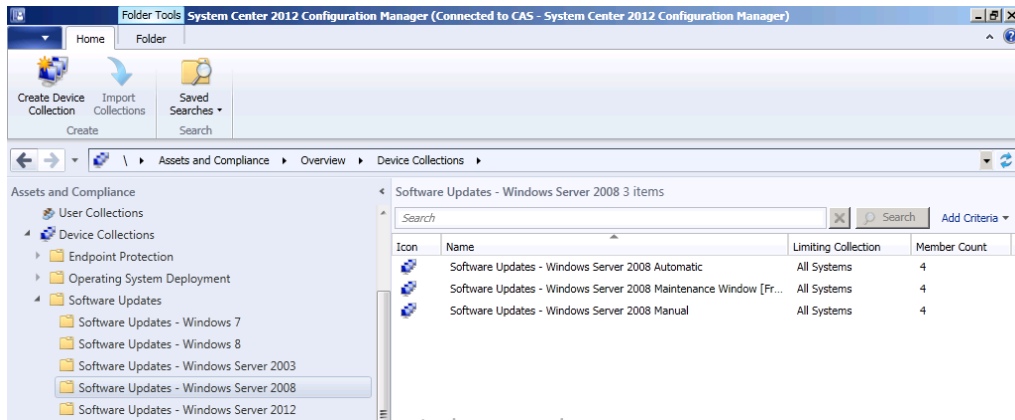
- Once done we need to **Set the Execution Policy** to allow this script (RemoteSigned) to run.
 - Set-ExecutionPolicy RemoteSigned** and answer **Yes** to the prompt.



- Run the script as follows:-
`.\CreateFoldersAndCollections.ps1 .\FolderAndCollections_Software_Updates.xml`
- The screen will update once you press enter...



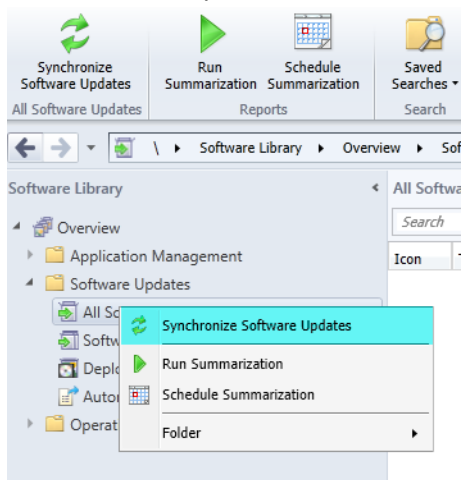
- d. Once the script is complete you can open the console in **Assets and Compliance** and refresh, you'll see the following Folders and Collections are already created.



5. Note: All of the collections have Membership queries to automatically populate the collections based on Operating System version. You may want to edit the queries further in order to exclude (or include) computers otherwise you will have overlap between those three Windows Server Collections where servers show up in all three of the respective collections.

Initiating the SUP Synchronization

Before starting our activity we want to make sure that the updates that we are looking at are **current and relevant** therefore we'll synchronize our **Software Update Point** with **Microsoft Windows Update**.



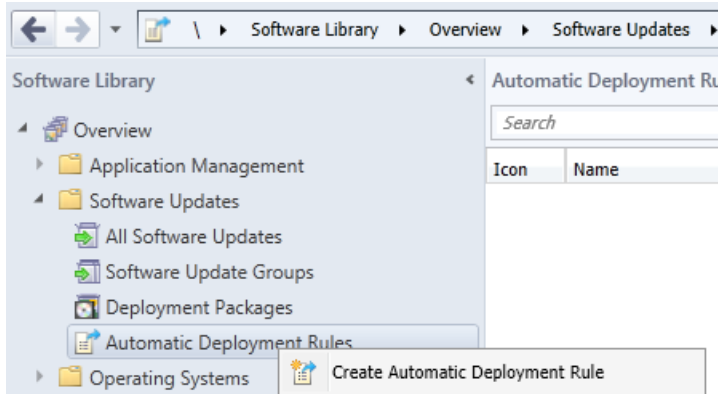
Tip: There are two types of sync, Full or Delta. A **Full sync** is performed on **schedule** (as defined in the Software Update Point scheduled synchronization), whereas a **Delta sync** occurs when you initiate a sync in the console. If a sync fails for whatever reason then it will be **retried every 60 minutes**.

Automatic Deployment Rules

Before starting this step create a folder on **W:\sources** on the SCCM-A-1 server to store our Updates. Our sources folder is shared as **source\$**. Give **Domain Admins**, **SCCM Admins**, **SCCM Servers**, and **SCCM-A-1\Administrator** Full Control to the Share as well as Security Level Rights. Also, add Everyone to the Share with Full Access. **DO NOT** add Everyone to the Security Level Rights

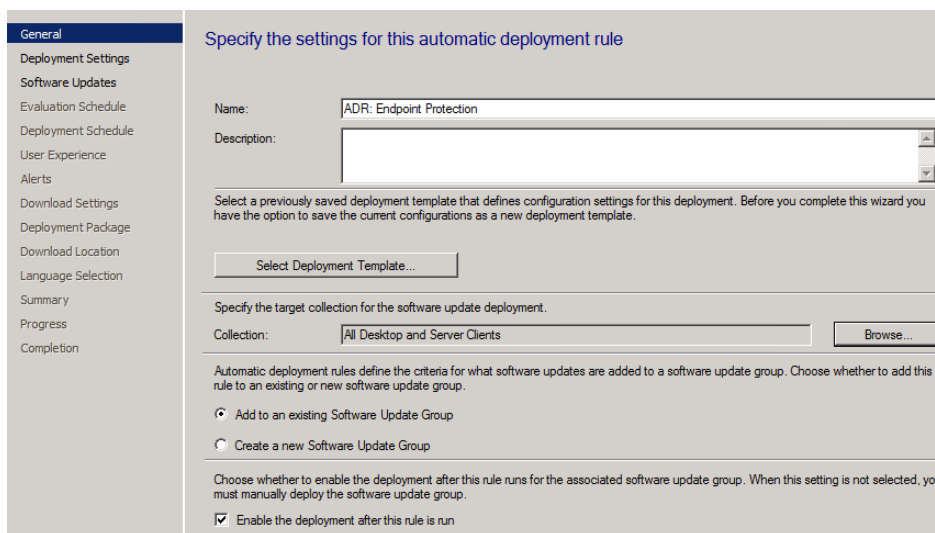
ADR: Endpoint Protection

1. In the Configuration Manager console, click **Software Library**, expand **Software Updates** and click **right click on Automatic Deployment Rules** and choose **Create Automatic Deployment Rule**,



2. Fill in the details as below, for name use **ADR: Endpoint Protection**, the naming is important, think weeks, months, years ahead when you are searching for that **Automatic Deployment Rule** you or someone else created, prepending **ADR: Endpoint Protection** will easily separate these ADR's from other ADR's created by you or other admins for patch Tuesday software updates for example.

For target collection **choose the collection you want to target with these definition updates**, in our example we will select the **All Workstations and Servers Clients** collection. Click **Next**.



Specify the settings for this automatic deployment rule

Name:

Description:

Select a previously saved deployment template that defines configuration settings for this deployment. Before you complete this wizard you have the option to save the current configurations as a new deployment template.

Specify the target collection for the software update deployment.

Collection:

Automatic deployment rules define the criteria for what software updates are added to a software update group. Choose whether to add this rule to an existing or new software update group.

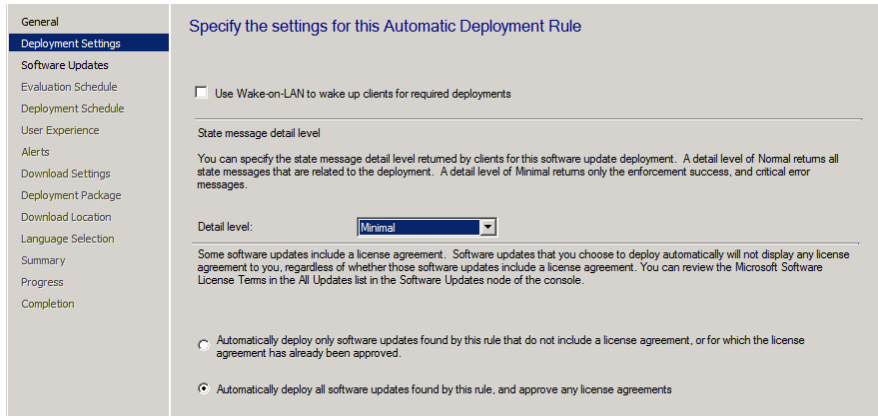
Add to an existing Software Update Group

Create a new Software Update Group

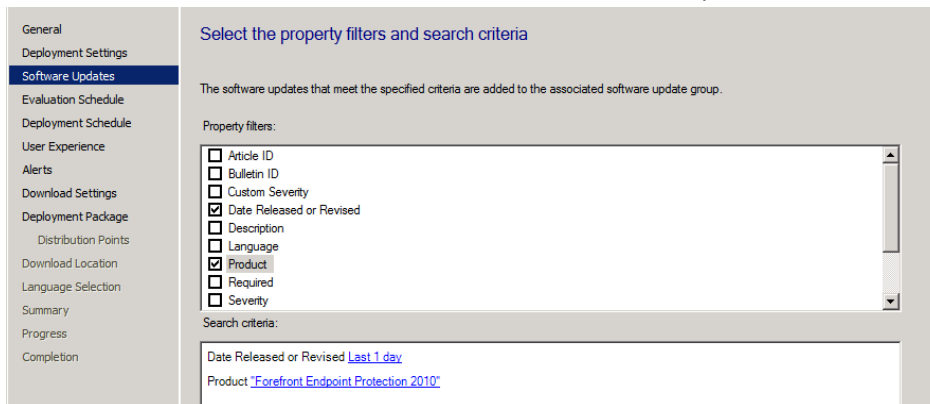
Choose whether to enable the deployment after this rule runs for the associated software update group. When this setting is not selected, you must manually deploy the software update group.

Enable the deployment after this rule is run

- On the **Deployment Settings** page of the wizard select **Minimal** from the **Detail level** drop-down list and then click **Next**, this reduces the content of **State Messages** returned and thus reduces Configuration Manager **Server load**. Click **Next**.

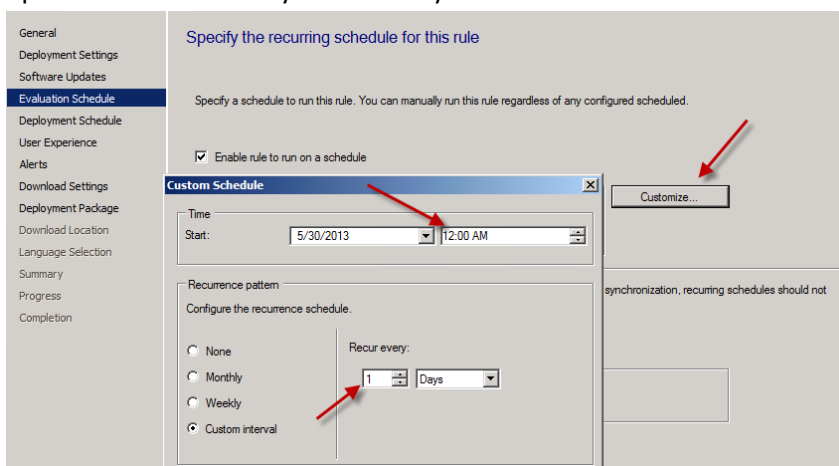


- On the **Software Updates** page select **Date Released or Revised**, choose **Last 1 day**, and select **Products**, then select **Forefront Protection 2010** from the list of available products. Click **Next**.



- On the **Evaluation Schedule** page, click on **Customize** and set it to run **every 1 days**,

Tip: notice that the **Synchronization Schedule** is listed below, make sure that the **SUP synchronizes at least 2 hours** before you evaluate for Forefront Endpoint Protection definition updates, there is no point checking for updates if we haven't synchronized yet. Click **OK** and **Next**.



- On the **Deployment Schedule** page, set Time based on: **UTC** if you want all clients in the hierarchy to install the latest definitions at the same time, this setting is a recommended best practice. For **software available** select **2 hours** to allow sufficient time for the Deployment to reach all **Distribution Points** and select **As soon as possible** for the **installation Deadline**. Click **Next**.

Note: Software update deadlines are **randomized over a 2-hour period** to prevent all clients from requesting an update at the same time.

General
Deployment Settings
Software Updates
Evaluation Schedule
Deployment Schedule
User Experience
Alerts
Download Settings
Deployment Package
Distribution Points
Download Location
Language Selection
Summary
Progress
Completion

Configure schedule details for this deployment

Schedule evaluation
Specify if the schedule for this deployment is evaluated based upon Universal Coordinated Time (UTC) or the local time of the client.

Time based on: **UTC**

Software available time
Specify when software updates are available. After this rule is run, software updates are distributed to the content server. Then the software updates are available to install as soon as possible or scheduled to install at a configured period of time after the rule is run.
Note: You must enable this deployment before software updates are available to install.

As soon as possible
 Specific time: **2** Hours
Available time:

Installation deadline
Specify an deadline for required software updates. The deadline is determined by adding the deadline time to the installation time. When the deadline is reached, required software updates are installed on the device and the device is restarted if necessary.

As soon as possible
 Specific time: **7** Days
Deadline Time (from deployment available time):

- On the **User Visual Experience** page, select **Hide in Software Center and all notifications** from the drop down menu and **suppress restarts on Servers**. Click **Next**.

General
Deployment Settings
Software Updates
Evaluation Schedule
Deployment Schedule
User Experience
Alerts
Download Settings
Deployment Package
Distribution Points
Download Location
Language Selection
Summary
Progress
Completion

Specify the user experience for this deployment

User visual experience
User notifications: **Hide in Software Center and all notifications**

Deadline behavior
When the installation deadline is reached, allow the following activities to be performed outside of any defined maintenance windows:

Software Installation
 System restart (if necessary)

Device restart behavior
Some software updates require a system restart to complete the installation process. You can suppress this restart on servers and workstations.
Suppress the system restart on the following devices:

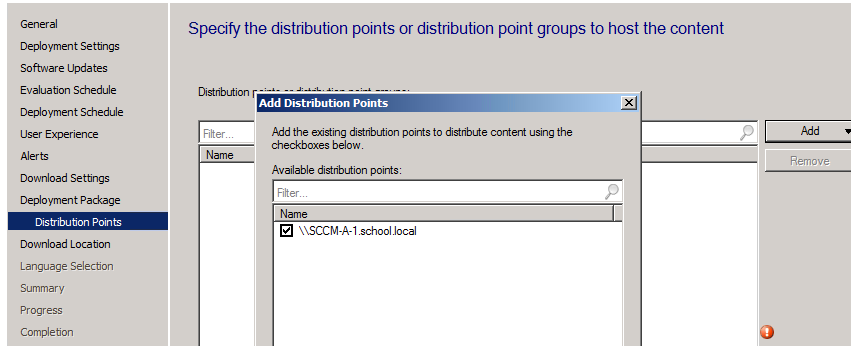
Servers
 Workstations

- On the **Alerts** page, enable the option to generate an alert, set the compliance percentage to be equal to the SLA you expect for that site, in this example we'll select 85%. Click **Next**.

- On the **Download Settings** page, we want to be sure that our clients get these malware definitions regardless of whether they are on slow site boundaries or not, so we will set both options accordingly. Click **Next**.

- For **Deployment Package** page, we need to create a **New Deployment Package**, give it a suitable name like **Endpoint Protection Definition Updates** and point it to a previously created shared folder ([\\scm-a-1\source\\$\EndpointUpdates](#)). Click **Next**.

11. On the **Distribution Points** page, click on the drop down **Add** button and select **distribution point**, select our distribution point on our primary server (SCCM-A-1) and click **OK** and **Next**.

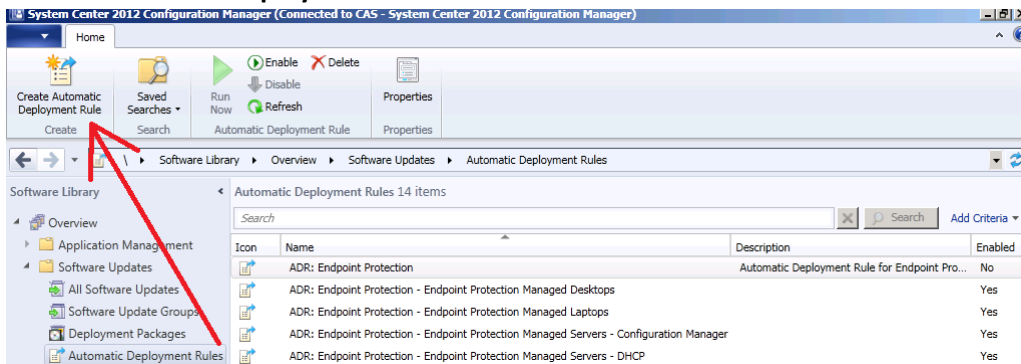


12. Click your way through the rest of the Wizard until you reach the **summary** screen but before finishing the wizard.

ADR: Windows 7 Patch Tuesday

Now we will create a new ADR to automatically deploy **Windows 7 Updates** once a month on a **recurring schedule** (after **patch Tuesday**, Microsoft releases new updates every month on the **second Tuesday of the month**). Once you understand how this works you can customize it to suit your needs to keep your systems patched in an automated way on a **recurring schedule**.

1. In the **Software Updates** section of the console, select **Automatic Deployment Rules** and in the ribbon click **Create Automatic Deployment Rule**.



2. On the General page of the wizard, enter Name **ADR: Software Updates - Windows 7 monthly Updates**. Click on **browse** and you'll notice our nice folder and collection structure makes it easy to select the right collection, select the **Software Updates - Windows 7** collection. As this ADR is for **Patch Tuesday** and occurs on a **recurring schedule every month**, we will choose to **create a new software update group** every time it runs; this means that we can have a single software update group to **measure compliance** against when the rule runs.

General

Specify the settings for this automatic deployment rule

Name:

Description:

Select a previously saved deployment template that defines configuration settings for this deployment. Before you complete this wizard you have the option to save the current configurations as a new deployment template.

Specify the target collection for the software update deployment.

Collection:

Automatic deployment rules define the criteria for what software updates are added to a software update group. Choose whether to add this rule to an existing or new software update group.

Add to an existing Software Update Group

Create a new Software Update Group

Choose whether to enable the deployment after this rule runs for the associated software update group. When this setting is not selected, you must manually deploy the software update group.

Enable the deployment after this rule is run

Device Collections

Name	Member Count
Software Updates - Windows 7	1

- On the **Deployment Settings** page, set the verbosity level of state messages to **Normal** (default is minimal) as we want to be able to determine what went wrong if some computers are **not compliant** after the rule is run and having all those state messages will help.

Deployment Settings

Specify the settings for this Automatic Deployment Rule

Use Wake-on-LAN to wake up clients for required deployments

State message detail level

You can specify the state message detail level returned by clients for this software update deployment. A detail level of Normal returns all state messages that are related to the deployment. A detail level of Minimal returns only the enforcement success, and critical error messages.

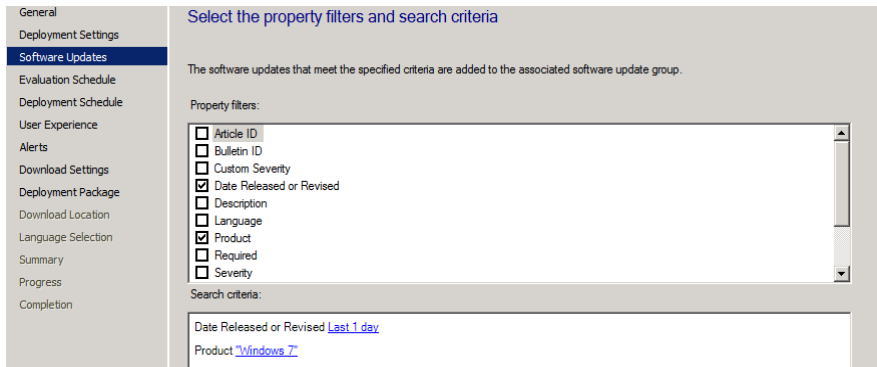
Detail level:

Some software updates include a license agreement. Software updates that you choose to deploy automatically will not display any license agreement to you, regardless of whether those software updates include a license agreement. You can review the Microsoft Software License Terms in the All Updates list in the Software Updates node of the console.

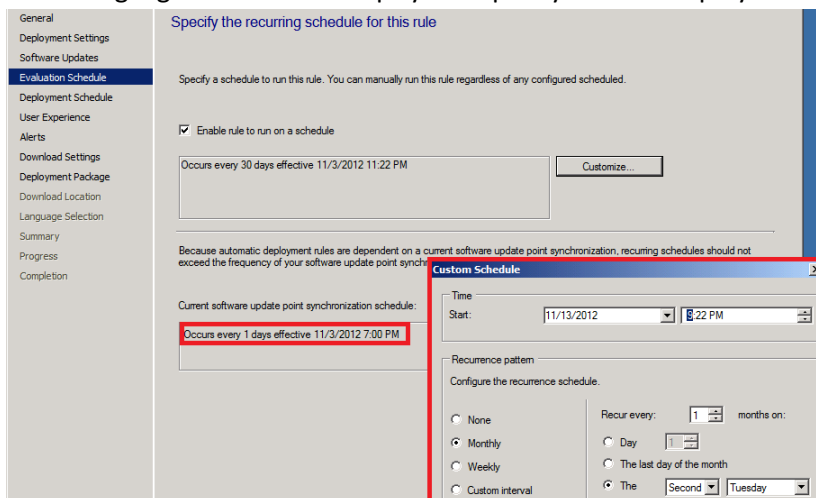
Automatically deploy only software updates found by this rule that do not include a license agreement, or for which the license agreement has already been approved.

Automatically deploy all software updates found by this rule, and approve any license agreements

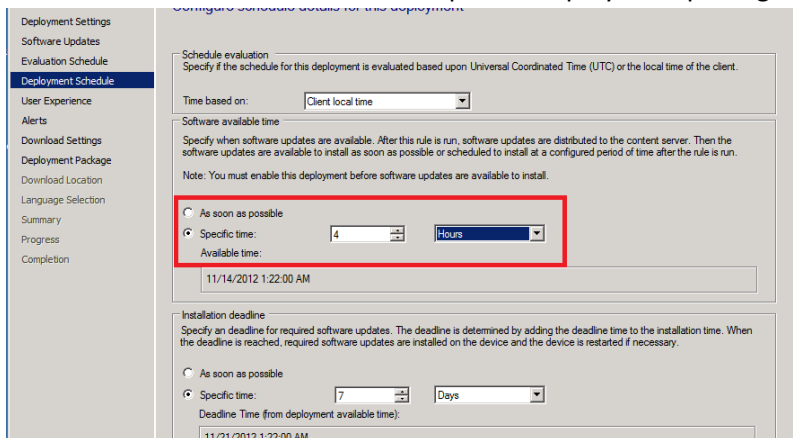
4. On the Software Updates screen select the following options:
 - a. Date release or revised **Last 1 day**
 - b. Product **Windows 7** (This means that when the rule runs it will find all **Windows 7 updates released in the last 1 day**)



5. On the **Evaluation Schedule** screen click on **Customize** and set the schedule accordingly, set it to start running on the **second Tuesday** of the current month, and to **recur monthly** on the second Tuesday of every month at **least two hours after the SUP has synced** (which should give it time to sync). You can see that the SUP sync time is highlighted and that helps you to plan your ADR deployment.



6. On the **Deployment Schedule** screen set the **Software Available Time** to be at least **4 hours** after the rule has run in order for the actual software updates deployment packages to reach the destination distribution points.



- On the **User Experience** screen, for **User Notification** select **Display in Software Center and show all notifications**. If you were targeting **Server Operating systems** with **automatic deployment rules** then you'd probably want to **suppress the system restart**.

Specify the user experience for this deployment

User visual experience

User notifications: **Display in Software Center and show all notifications**

Deadline behavior

When the installation deadline is reached, allow the following activities to be performed outside of any defined maintenance windows:

Software Installation

System restart (if necessary)

Device restart behavior

Some software updates require a system restart to complete the installation process. You can suppress this restart on servers and workstations.

Suppress the system restart on the following devices:

Servers

Workstations

- If you want to be alerted when the compliance threshold is **below the desired compliance level** then select the next option on the **Alerts** screen.

Specify software update alert options for this deployment

Configuration Manager alerts

Specify the criteria for generating a Configuration Manager alert.

Generate an alert when the following conditions are met

Client compliance is below the following percent:

Offset from the deadline:

Alerts are generated after the installation deadline is reached.

Deadline time:

Operations Manager alerts

System Center Operations Manager might generate alerts when a device installs a software update. To avoid receiving alerts for planned maintenance, you can disable these alerts during the duration of the software update installation process.

Disable Operations Manager alerts while software updates run

Generate Operations Manager alert when a software update installation fails

- On the **Download Settings** page, leave it as default. Click Next.

Specify the software updates download behavior for clients on slow site boundaries.

Select the deployment option to use when a client is within a slow or unreliable network boundary, or when the client uses a fallback source location for content.

Deployment options:

Do not install software updates

Download software updates from distribution point and install

When software updates are not available on any preferred distribution points, clients can download and install software updates from a fallback source location for content.

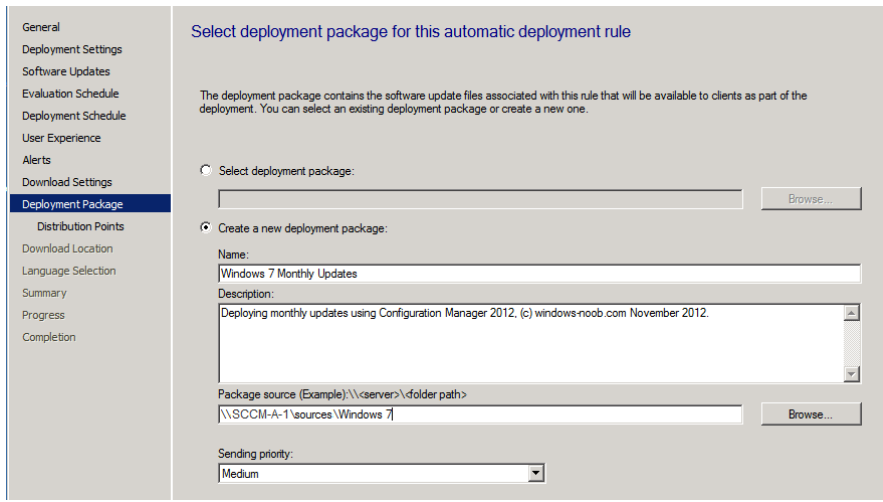
Deployment options:

Do not install software updates

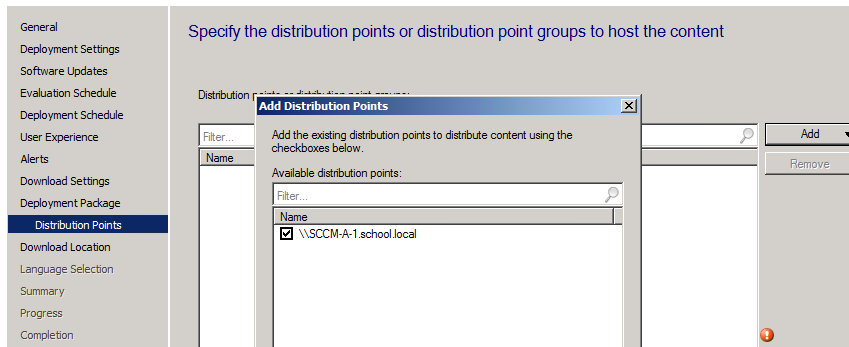
Download and install software updates from the fallback content source location

Allow clients to share content with other clients on the same subnet

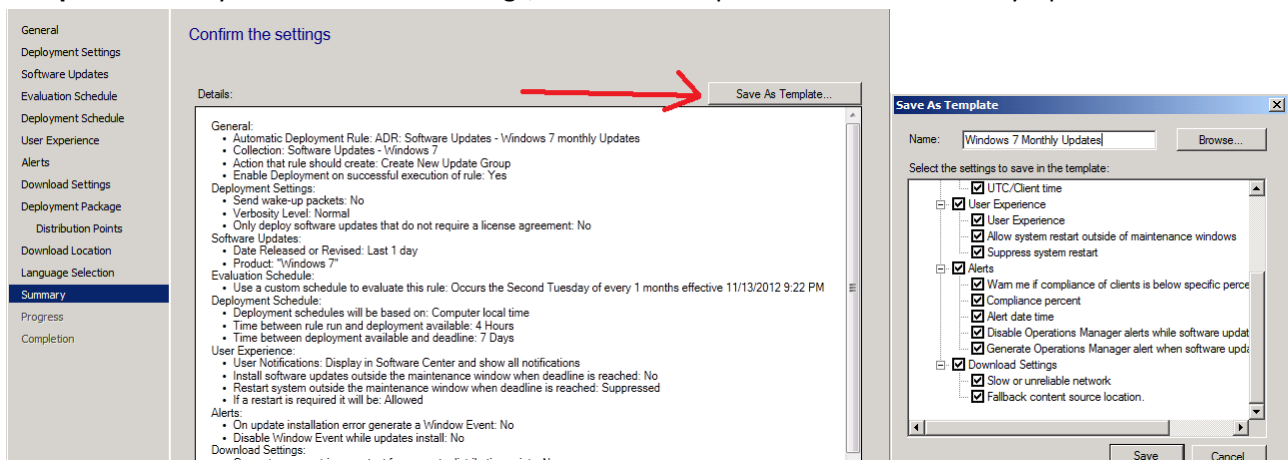
10. On the Deployment Package screen, select to **create a new deployment package** (as none will exist that we want to use). Once it has run, you can **retire that rule** by **disabling** it (right click on the ADR, choose Disable) and then you should recreate an identical rule except in the replacement rule, for Deployment Package choose the **previously created package** (Windows 7 Monthly Updates) so that it re-uses the package every month.



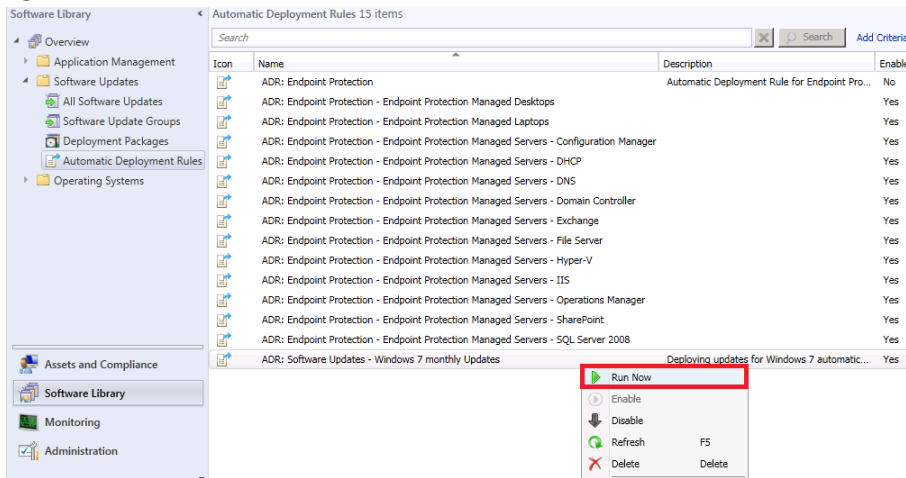
11. On the **Distribution Points** page, click on the drop down **Add** button and select **distribution point**, select our distribution point on our primary server (SCCM-A-1) and click ok.



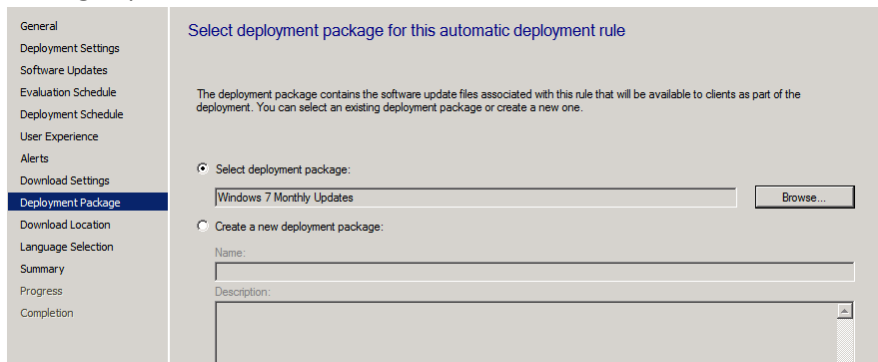
12. Continue through the rest of the wizard through to the **Summary** screen, on that screen click on **Save as Template** so that you can reuse the settings, Name the template Windows 7 Monthly Updates



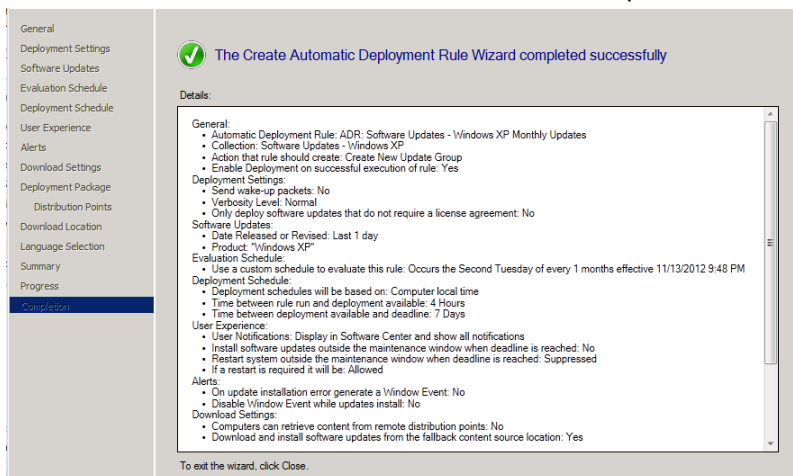
13. Right Click on the newly created ADR and choose **Run Now**, we do this to create the **Deployment Package**. After running the rule, verify that the Deployment Package is indeed created and when done, right click on the ADR again, and choose **Disable**.



14. Once done recreate the rule (the ADR: Software Updates – Windows 7 Monthly Updates) but this time use the Windows 7 Monthly Updates Template and point it to that package during the wizard in the **Select Deployment Package** option like in the screenshot below.



15. Repeat the above for your **Windows XP** clients just as we've done for **Windows 7**, except obviously change the **Product name** from Windows 7 to Windows XP and point the collection to the **Windows XP** equivalent...

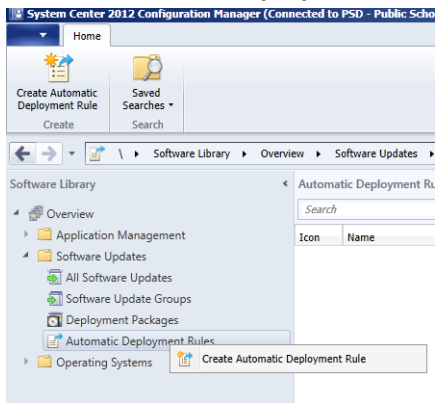


16. At this point your ADR's are created and you are ready to sit back and watch as your Windows XP and Windows 7 clients get automatically patched on Patch Tuesday. Awesome.

Icon	Name	Description	Enabled
[Icon]	ADR: Software Updates - Windows 7 Monthly Updates	Deploying updates for Windows 7 automatic...	Yes
[Icon]	ADR: Software Updates - Windows XP Monthly Updates	(c) windows-noob.com November 2012	Yes
[Icon]	ADR: Endpoint Protection	Automatic Deployment Rule for Endpoint Pro...	No
[Icon]	ADR: Endpoint Protection - Endpoint Protection Managed Desktops		Yes
[Icon]	ADR: Endpoint Protection - Endpoint Protection Managed Laptops		Yes
[Icon]	ADR: Endpoint Protection - Endpoint Protection Managed Servers - Configuration Manager		Yes
[Icon]	ADR: Endpoint Protection - Endpoint Protection Managed Servers - DHCP		Yes
[Icon]	ADR: Endpoint Protection - Endpoint Protection Managed Servers - DNS		Yes
[Icon]	ADR: Endpoint Protection - Endpoint Protection Managed Servers - Domain Controller		Yes
[Icon]	ADR: Endpoint Protection - Endpoint Protection Managed Servers - Exchange		Yes
[Icon]	ADR: Endpoint Protection - Endpoint Protection Managed Servers - File Server		Yes
[Icon]	ADR: Endpoint Protection - Endpoint Protection Managed Servers - Hyper-V		Yes
[Icon]	ADR: Endpoint Protection - Endpoint Protection Managed Servers - IIS		Yes
[Icon]	ADR: Endpoint Protection - Endpoint Protection Managed Servers - Operations Manager		Yes
[Icon]	ADR: Endpoint Protection - Endpoint Protection Managed Servers - SharePoint		Yes
[Icon]	ADR: Endpoint Protection - Endpoint Protection Managed Servers - SQL Server 2008		Yes
[Icon]	ADR: Software Updates - Windows 7 monthly Updates	Deploying updates for Windows 7 automatic...	No
[Icon]	ADR: Software Updates - Windows XP Monthly Updates		No

ADR: Adobe Updates

1. In the **Software Updates** section of the console, select **Automatic Deployment Rules** and in the ribbon click **Create Automatic Deployment Rule**.



2. On the General page of the wizard, enter Name **ADR: Adobe Software Update**. Click on **browse** and you'll notice our nice folder and collection structure makes it easy to select the right collection, select the **All Desktop and Server Clients** collection. Choose to **Add to an existing Software Update Group**. Click Next.

Specify the settings for this automatic deployment rule

Name:

Description:

Select a previously saved deployment template that defines configuration settings for this deployment. Before you complete this wizard you have the option to save the current configurations as a new deployment template.

Specify the target collection for the software update deployment.

Collection:

Automatic deployment rules define the criteria for what software updates are added to a software update group. Choose whether to add this rule to an existing or new software update group.

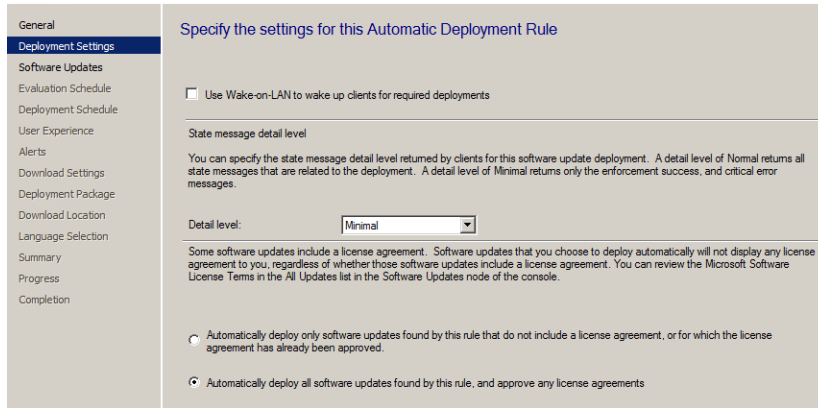
Add to an existing Software Update Group

Create a new Software Update Group

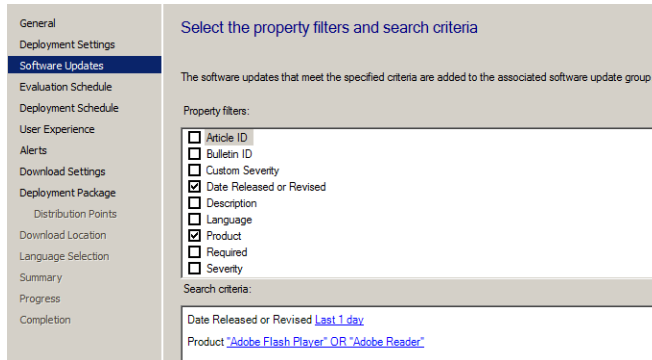
Choose whether to enable the deployment after this rule runs for the associated software update group. When this setting is not selected, you must manually deploy the software update group.

Enable the deployment after this rule is run

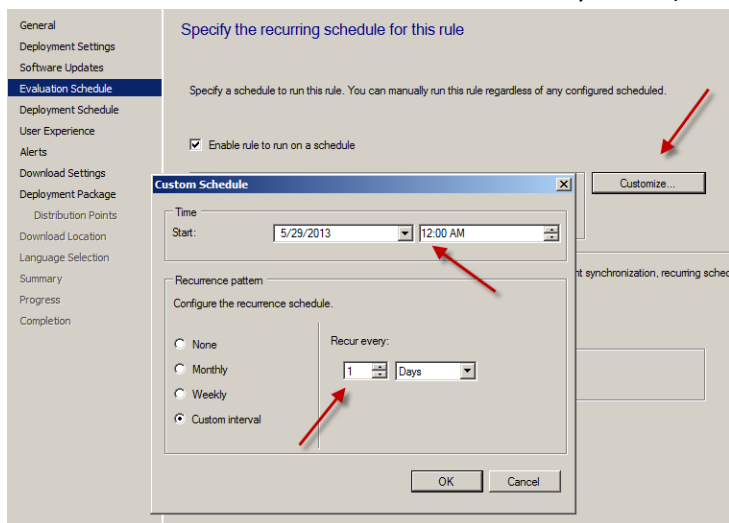
- On the **Deployment Settings** page, set the verbosity level of state messages to **Normal** (default is minimal) as we want to be able to determine what went wrong if some computers are **not compliant** after the rule is run and having all those state messages will help.



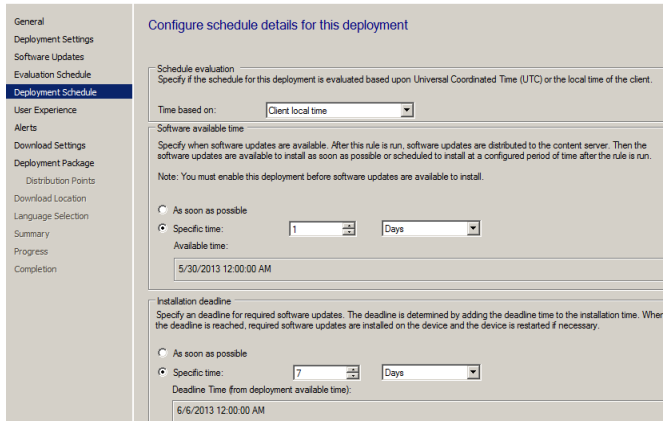
- On the Software Updates screen select the following options:
 - Date release or revised **Last 1 day**
 - Product **Adobe Flash Player** and **Adobe Reader**



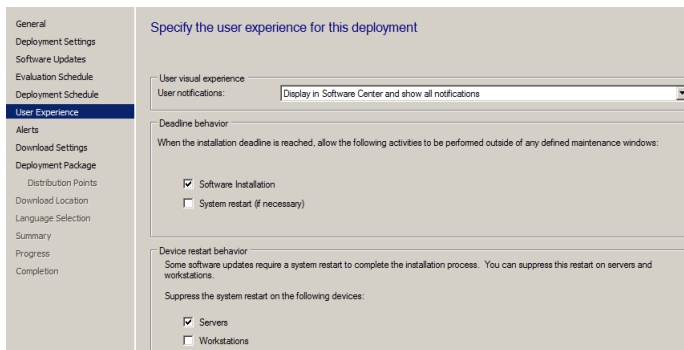
- On the **Evaluation Schedule** screen click on **Customize** and set the schedule accordingly, set it to start running at **12:00 AM** at least two hours after the SUP has synced (which should give it time to sync).



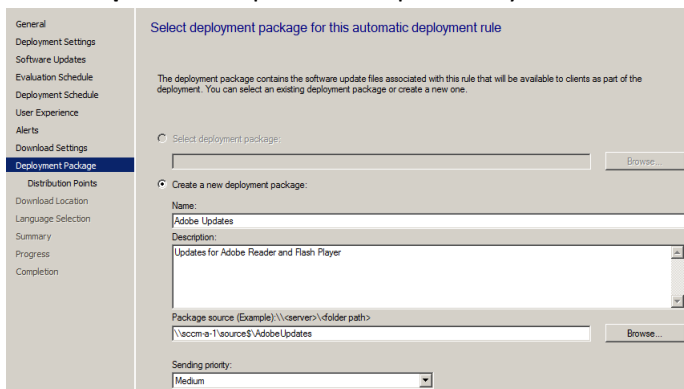
- On the **Deployment Schedule** screen set the **Software Available Time** to be at least **1 Day** after the rule has run in order for the actual software updates deployment packages to reach the destination distribution points.



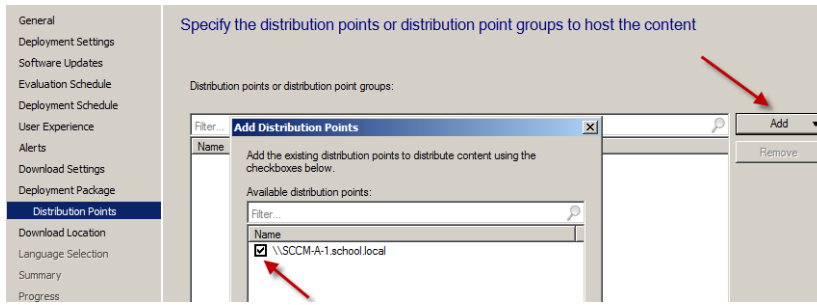
- On the **User Experience** screen, for **User Notification** select **Display in Software Center and show all notifications**. If you were targeting **Server Operating systems** with **automatic deployment rules** then you'd probably want to **suppress the system restart**.



- If you want to be alerted when the compliance threshold is **below the desired compliance level** then select the next option on the **Alerts** screen.
- On the **Download Settings** page, leave it as default. Click Next.
- On the **Deployment Package** screen, select to **create a new deployment package**, give it a suitable name like **Adobe Updates** and point it to a previously created shared folder (`\\sccm-a-1\source$\AdobeUpdates`)



- On the **Distribution Points** page, click on the drop down **Add** button and select **distribution point**, select our distribution point on our primary server (SCCM-A-1) and click ok.



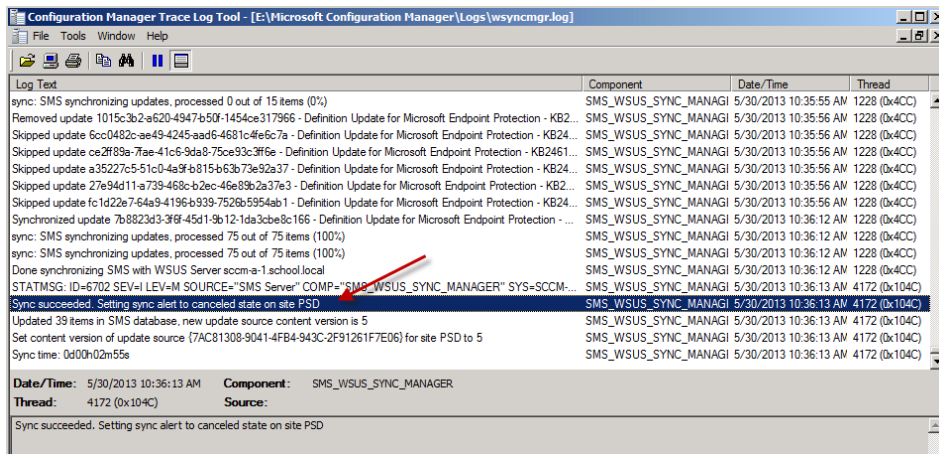
12. Click through the rest of the Wizard. Right Click the new ADR and chose Run now.

Monitoring and Troubleshooting

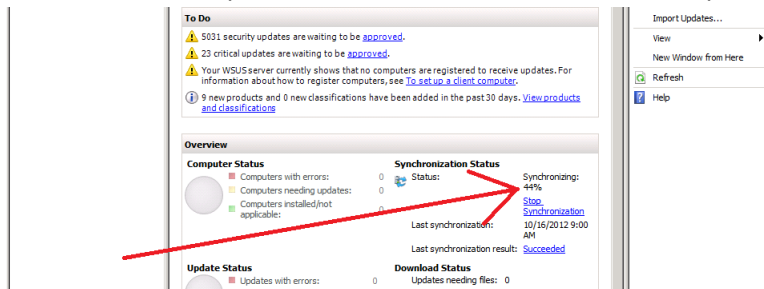
Montior the WsyncMgr.log file to determine Sync Activity

To monitor the sync progress open the **WsyncMgr.log**. Before continuing, confirm that the **sync has succeeded** on your PSD server by looking for the following line in **WsyncMgr.log**

Sync Succeeded. Setting sync alert to cancelled state on site PSD.



Tip: To watch the sync in real-time you can start the **Windows Server Update Services Console**, this will show you any error messages pertaining to the synchronization process (such as services that are not started when they should be) and will give you a percentage reading as the sync takes place. **DO NOT** make any changes to the WSUS system using the Windows Server Update Services Console. This will mess up Software Update Point configuration.

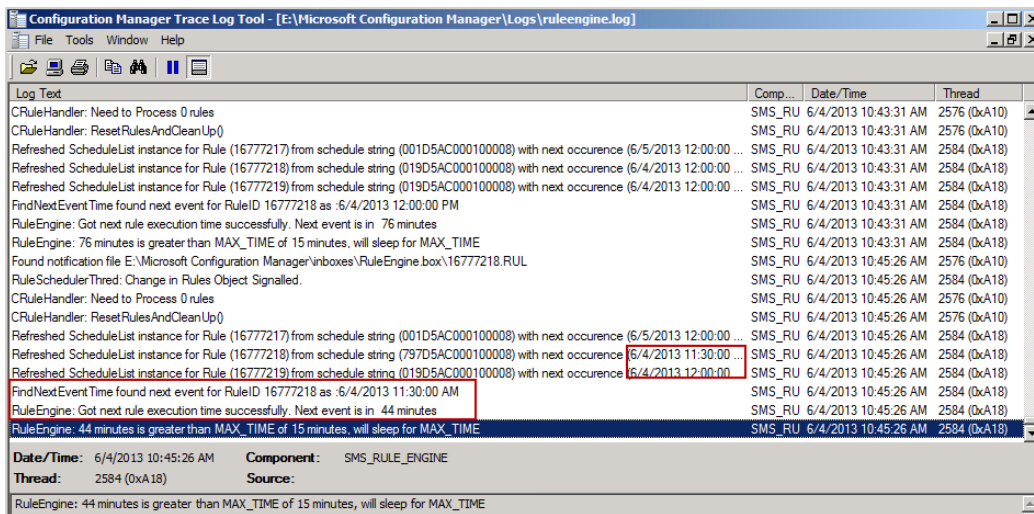


Monitor the RuleEngine.log file to determine ADR activity

To get a better understanding of what happens when our ADR runs we will monitor the log it uses for processing ADRs. On Patch Tuesday when our ADR runs it logs the fact to the **RuleEngine.log** file.

Tip: The **RuleEngine.Log** file is located in **E:\Microsoft Configuration Manager\Logs**

Open this log file in **CMTrace** and you'll see the following when the ADR runs on a schedule. Notice that I've configured my rule to run in a few minutes from now purely for the purpose of capturing the event in the log.



The screenshot shows the Configuration Manager Trace Log Tool interface. The main window displays a list of log entries with columns for Log Text, Component, Date/Time, and Thread. The log text includes various events such as 'CRuleHandler: Need to Process 0 rules', 'Refreshed ScheduleList instance for Rule (16777218) from schedule string (019D5AC000100008) with next occurrence (6/4/2013 12:00:00 ...', and 'RuleEngine: Got next rule execution time successfully. Next event is in 44 minutes'. A red box highlights the entry: 'Refreshed ScheduleList instance for Rule (16777219) from schedule string (019D5AC000100008) with next occurrence 6/4/2013 11:30:00 AM'. Below the log list, the Date/Time is 6/4/2013 10:45:26 AM, Component is SMS_RULE_ENGINE, and Thread is 2584 (0xA18).

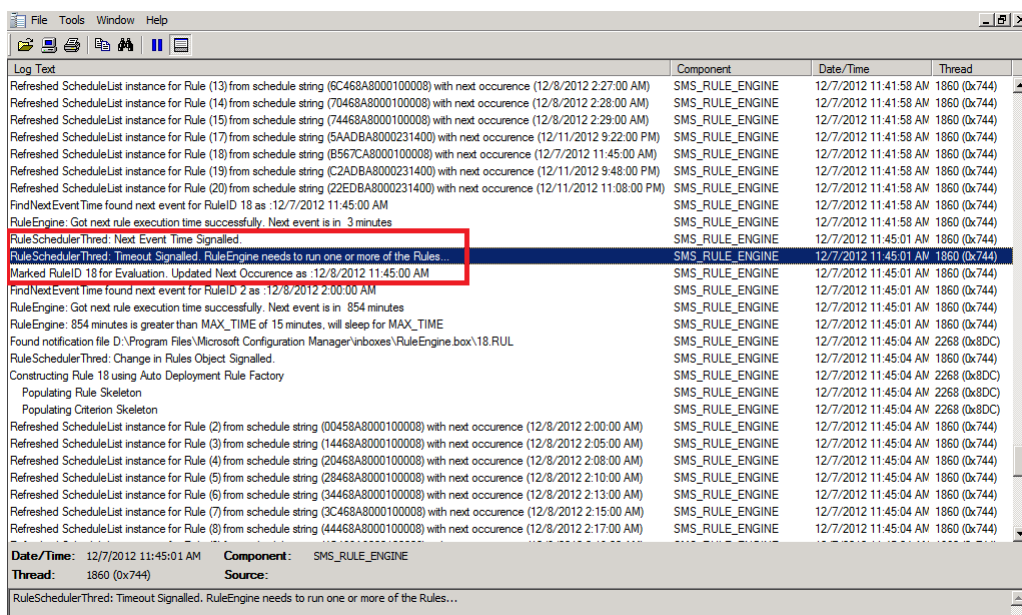
Log Text	Comp...	Date/Time	Thread
CRuleHandler: Need to Process 0 rules	SMS_RU	6/4/2013 10:43:31 AM	2576 (0xA10)
CRuleHandler: ResetRulesAndCleanUp()	SMS_RU	6/4/2013 10:43:31 AM	2576 (0xA10)
Refreshed ScheduleList instance for Rule (16777217) from schedule string (001D5AC000100008) with next occurrence (6/5/2013 12:00:00 ...	SMS_RU	6/4/2013 10:43:31 AM	2584 (0xA18)
Refreshed ScheduleList instance for Rule (16777218) from schedule string (019D5AC000100008) with next occurrence (6/4/2013 12:00:00 ...	SMS_RU	6/4/2013 10:43:31 AM	2584 (0xA18)
Refreshed ScheduleList instance for Rule (16777219) from schedule string (019D5AC000100008) with next occurrence (6/4/2013 12:00:00 ...	SMS_RU	6/4/2013 10:43:31 AM	2584 (0xA18)
FindNextEventTime found next event for RuleID 16777218 as :6/4/2013 12:00:00 PM	SMS_RU	6/4/2013 10:43:31 AM	2584 (0xA18)
RuleEngine: Got next rule execution time successfully. Next event is in 76 minutes	SMS_RU	6/4/2013 10:43:31 AM	2584 (0xA18)
RuleEngine: 76 minutes is greater than MAX_TIME of 15 minutes. will sleep for MAX_TIME	SMS_RU	6/4/2013 10:43:31 AM	2584 (0xA18)
Found notification file E:\Microsoft Configuration Manager\inbox\RuleEngine\box\16777218.RUL	SMS_RU	6/4/2013 10:45:26 AM	2576 (0xA10)
RuleSchedulerThread: Change in Rules Object Signalled.	SMS_RU	6/4/2013 10:45:26 AM	2584 (0xA18)
CRuleHandler: Need to Process 0 rules	SMS_RU	6/4/2013 10:45:26 AM	2576 (0xA10)
CRuleHandler: ResetRulesAndCleanUp()	SMS_RU	6/4/2013 10:45:26 AM	2576 (0xA10)
Refreshed ScheduleList instance for Rule (16777217) from schedule string (001D5AC000100008) with next occurrence (6/5/2013 12:00:00 ...	SMS_RU	6/4/2013 10:45:26 AM	2584 (0xA18)
Refreshed ScheduleList instance for Rule (16777218) from schedule string (797D5AC000100008) with next occurrence 6/4/2013 11:30:00 AM	SMS_RU	6/4/2013 10:45:26 AM	2584 (0xA18)
Refreshed ScheduleList instance for Rule (16777219) from schedule string (019D5AC000100008) with next occurrence 6/4/2013 12:00:00 AM	SMS_RU	6/4/2013 10:45:26 AM	2584 (0xA18)
FindNextEventTime found next event for RuleID 16777218 as :6/4/2013 11:30:00 AM	SMS_RU	6/4/2013 10:45:26 AM	2584 (0xA18)
RuleEngine: Got next rule execution time successfully. Next event is in 44 minutes	SMS_RU	6/4/2013 10:45:26 AM	2584 (0xA18)
RuleEngine: 44 minutes is greater than MAX_TIME of 15 minutes. will sleep for MAX_TIME	SMS_RU	6/4/2013 10:45:26 AM	2584 (0xA18)

Date/Time: 6/4/2013 10:45:26 AM Component: SMS_RULE_ENGINE
Thread: 2584 (0xA18) Source:

RuleEngine: 44 minutes is greater than MAX_TIME of 15 minutes. will sleep for MAX_TIME

When the **actual scheduled time** occurs the **ADR will be triggered** and you'll see lines similar to the following in the log

Note: the **Updated next occurrence** will be **one month from the date listed** (and not one day as in the screenshot below), this screenshot shows one day as I adjusted it to run for this guide as described in the notes above.



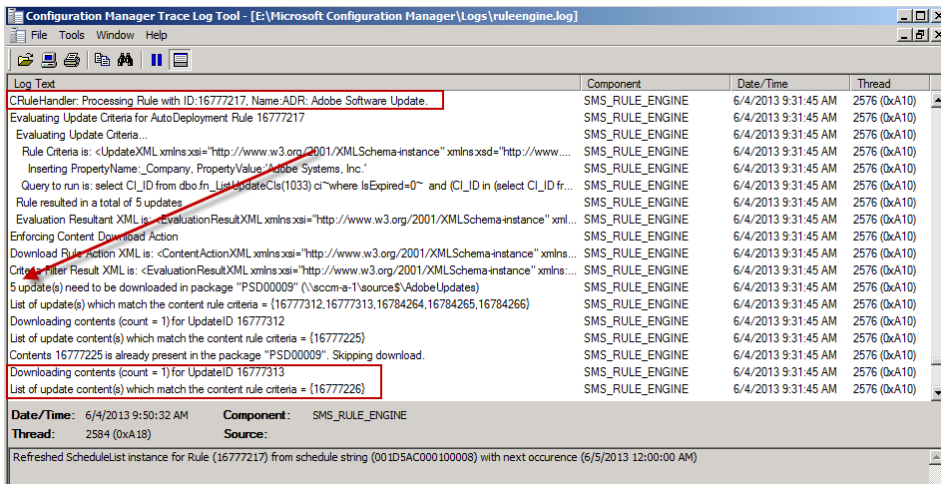
The screenshot shows the Configuration Manager Trace Log Tool interface. The main window displays a list of log entries with columns for Log Text, Component, Date/Time, and Thread. The log text includes various events such as 'Refreshed ScheduleList instance for Rule (13) from schedule string (6C468A8000100008) with next occurrence (12/8/2012 2:27:00 AM)', 'RuleEngine: Got next rule execution time successfully. Next event is in 3 minutes', and 'RuleSchedulerThread: Timeout Signalled. RuleEngine needs to run one or more of the Rules...'. A red box highlights the entry: 'Marked RuleID 18 for Evaluation. Updated Next Occurrence as :12/8/2012 11:45:00 AM'. Below the log list, the Date/Time is 12/7/2012 11:45:01 AM, Component is SMS_RULE_ENGINE, and Thread is 1860 (0x744).

Log Text	Component	Date/Time	Thread
Refreshed ScheduleList instance for Rule (13) from schedule string (6C468A8000100008) with next occurrence (12/8/2012 2:27:00 AM)	SMS_RULE_ENGINE	12/7/2012 11:41:58 AM	1860 (0x744)
Refreshed ScheduleList instance for Rule (14) from schedule string (70468A8000100008) with next occurrence (12/8/2012 2:28:00 AM)	SMS_RULE_ENGINE	12/7/2012 11:41:58 AM	1860 (0x744)
Refreshed ScheduleList instance for Rule (15) from schedule string (74468A8000100008) with next occurrence (12/8/2012 2:29:00 AM)	SMS_RULE_ENGINE	12/7/2012 11:41:58 AM	1860 (0x744)
Refreshed ScheduleList instance for Rule (17) from schedule string (5A4DBA8000231400) with next occurrence (12/11/2012 9:22:00 PM)	SMS_RULE_ENGINE	12/7/2012 11:41:58 AM	1860 (0x744)
Refreshed ScheduleList instance for Rule (18) from schedule string (8567CA8000100008) with next occurrence (12/7/2012 11:45:00 AM)	SMS_RULE_ENGINE	12/7/2012 11:41:58 AM	1860 (0x744)
Refreshed ScheduleList instance for Rule (19) from schedule string (C2ADBA8000231400) with next occurrence (12/11/2012 9:48:00 PM)	SMS_RULE_ENGINE	12/7/2012 11:41:58 AM	1860 (0x744)
Refreshed ScheduleList instance for Rule (20) from schedule string (22EDBA8000231400) with next occurrence (12/11/2012 11:08:00 PM)	SMS_RULE_ENGINE	12/7/2012 11:41:58 AM	1860 (0x744)
FindNextEventTime found next event for RuleID 18 as :12/7/2012 11:45:00 AM	SMS_RULE_ENGINE	12/7/2012 11:41:58 AM	1860 (0x744)
RuleEngine: Got next rule execution time successfully. Next event is in 3 minutes	SMS_RULE_ENGINE	12/7/2012 11:41:58 AM	1860 (0x744)
RuleSchedulerThread: Next Event Time Signalled.	SMS_RULE_ENGINE	12/7/2012 11:45:01 AM	1860 (0x744)
RuleSchedulerThread: Timeout Signalled. RuleEngine needs to run one or more of the Rules...	SMS_RULE_ENGINE	12/7/2012 11:45:01 AM	1860 (0x744)
Marked RuleID 18 for Evaluation. Updated Next Occurrence as :12/8/2012 11:45:00 AM	SMS_RULE_ENGINE	12/7/2012 11:45:01 AM	1860 (0x744)
FindNextEventTime found next event for RuleID 2 as :12/8/2012 2:00:00 AM	SMS_RULE_ENGINE	12/7/2012 11:45:01 AM	1860 (0x744)
RuleEngine: Got next rule execution time successfully. Next event is in 854 minutes	SMS_RULE_ENGINE	12/7/2012 11:45:01 AM	1860 (0x744)
RuleEngine: 854 minutes is greater than MAX_TIME of 15 minutes. will sleep for MAX_TIME	SMS_RULE_ENGINE	12/7/2012 11:45:01 AM	1860 (0x744)
Found notification file D:\Program Files\Microsoft Configuration Manager\inbox\RuleEngine\box\18.RUL	SMS_RULE_ENGINE	12/7/2012 11:45:04 AM	2268 (0x8DC)
RuleSchedulerThread: Change in Rules Object Signalled.	SMS_RULE_ENGINE	12/7/2012 11:45:04 AM	1860 (0x744)
Constructing Rule 18 using Auto Deployment Rule Factory	SMS_RULE_ENGINE	12/7/2012 11:45:04 AM	2268 (0x8DC)
Populating Rule Skeleton	SMS_RULE_ENGINE	12/7/2012 11:45:04 AM	2268 (0x8DC)
Populating Criteron Skeleton	SMS_RULE_ENGINE	12/7/2012 11:45:04 AM	2268 (0x8DC)
Refreshed ScheduleList instance for Rule (2) from schedule string (00458A8000100008) with next occurrence (12/8/2012 2:00:00 AM)	SMS_RULE_ENGINE	12/7/2012 11:45:04 AM	1860 (0x744)
Refreshed ScheduleList instance for Rule (3) from schedule string (14468A8000100008) with next occurrence (12/8/2012 2:05:00 AM)	SMS_RULE_ENGINE	12/7/2012 11:45:04 AM	1860 (0x744)
Refreshed ScheduleList instance for Rule (4) from schedule string (20468A8000100008) with next occurrence (12/8/2012 2:08:00 AM)	SMS_RULE_ENGINE	12/7/2012 11:45:04 AM	1860 (0x744)
Refreshed ScheduleList instance for Rule (5) from schedule string (28468A8000100008) with next occurrence (12/8/2012 2:10:00 AM)	SMS_RULE_ENGINE	12/7/2012 11:45:04 AM	1860 (0x744)
Refreshed ScheduleList instance for Rule (6) from schedule string (34468A8000100008) with next occurrence (12/8/2012 2:13:00 AM)	SMS_RULE_ENGINE	12/7/2012 11:45:04 AM	1860 (0x744)
Refreshed ScheduleList instance for Rule (7) from schedule string (3C468A8000100008) with next occurrence (12/8/2012 2:15:00 AM)	SMS_RULE_ENGINE	12/7/2012 11:45:04 AM	1860 (0x744)
Refreshed ScheduleList instance for Rule (8) from schedule string (44468A8000100008) with next occurrence (12/8/2012 2:17:00 AM)	SMS_RULE_ENGINE	12/7/2012 11:45:04 AM	1860 (0x744)

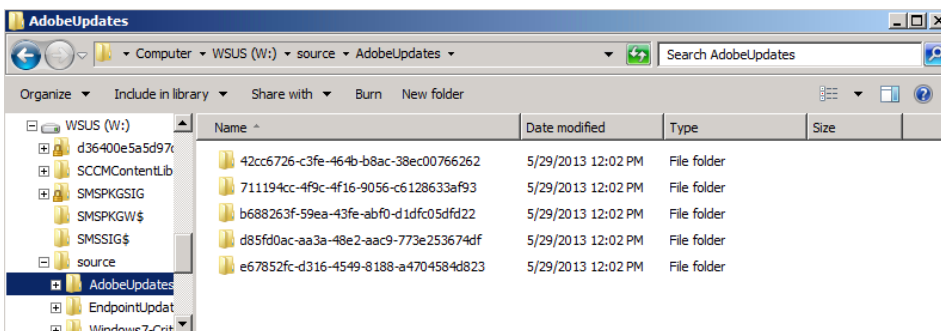
Date/Time: 12/7/2012 11:45:01 AM Component: SMS_RULE_ENGINE
Thread: 1860 (0x744) Source:

RuleSchedulerThread: Timeout Signalled. RuleEngine needs to run one or more of the Rules...

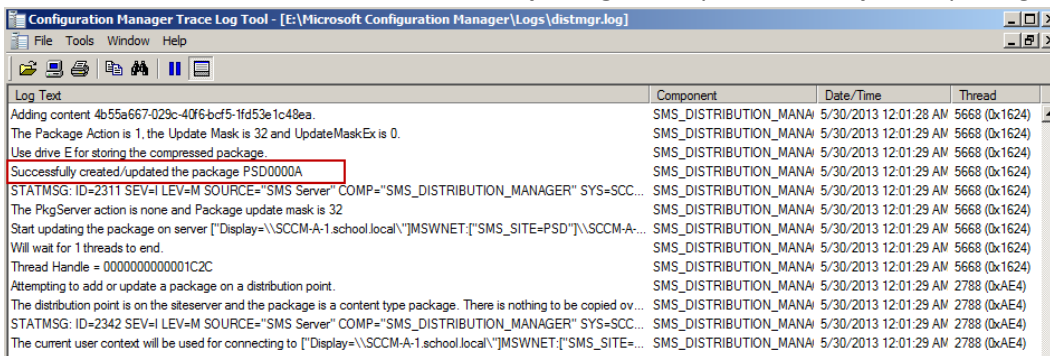
If you scroll further down in the log you'll see our **Adobe Software Updates** ADR is referenced directly and it also informs us if updates need to be downloaded into our previously created package, in this particular case 5 updates need to be downloaded into our package on the SCCM-A-1 server. Underneath that you'll see the ADR is attempting to download content (with content ID) and whether it was successful or not.



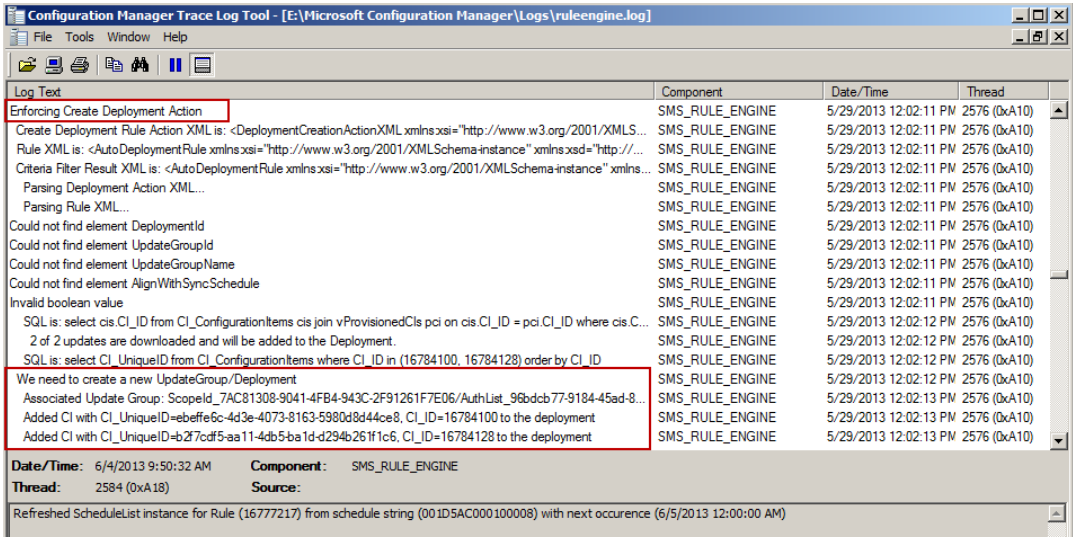
You can also open **Windows Explorer** at this point and browse to the location of your Adobe Updates **package source location**, you'll see that folder filling up with folders which in turn contain files, these are the updates being downloaded.



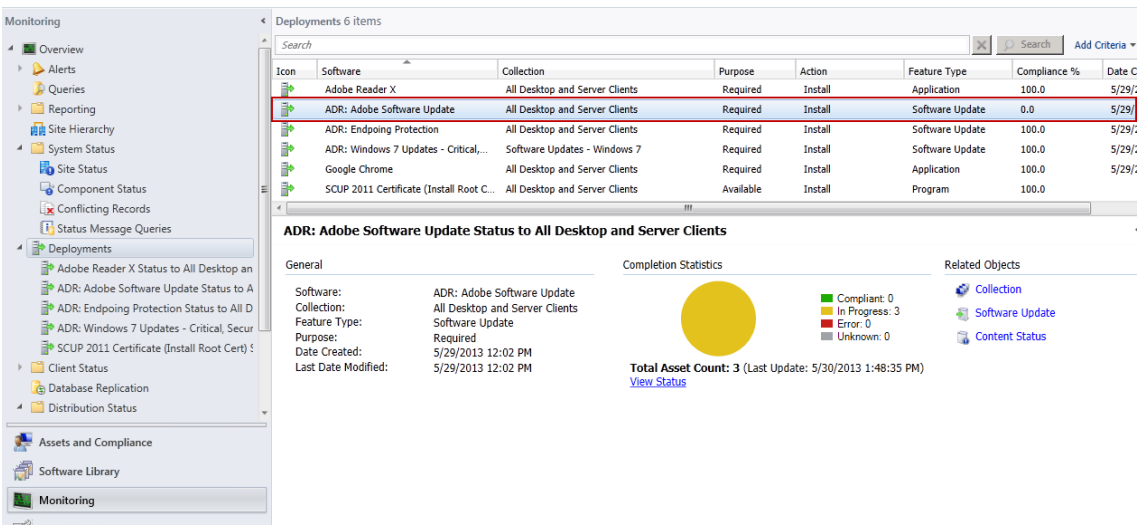
After the ADR has downloaded all the updates it'll update the Deployment Package, look for the line **Updating package "PSD0000A" now where "PSD0000A" is the package ID of your AdobeUpdates package**



After that it will **Enforce the Create Deployment Action** (by creating a new deployment containing the updates it has just downloaded). This can be seen in the **RuleEngine.log** below where it says:



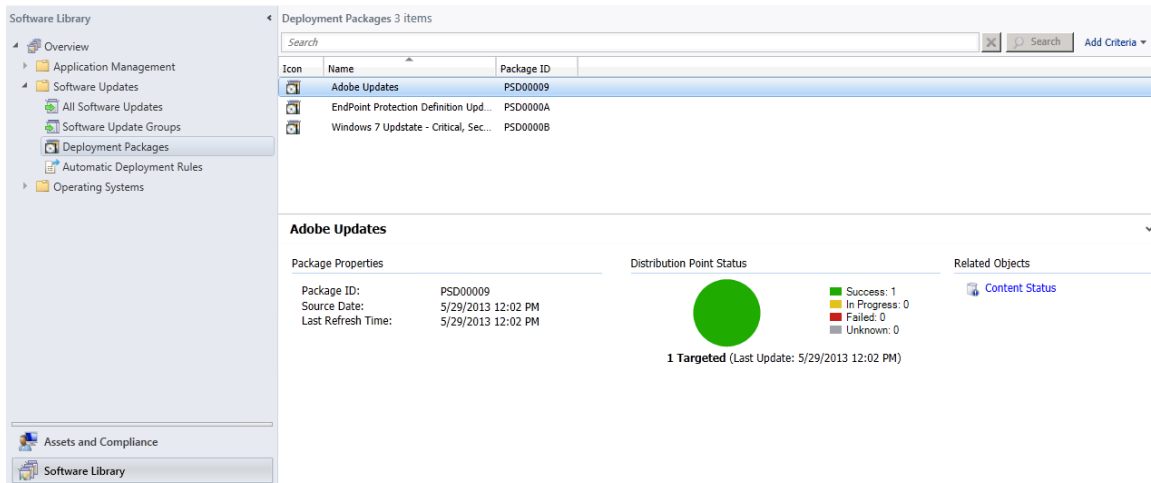
This brand new **deployment** can now be found in the **Monitoring** Workspace by clicking on **Deployments**.



Finally after creating the new deployment the ADR **creates an alert** and updates the **success information** of the rule.

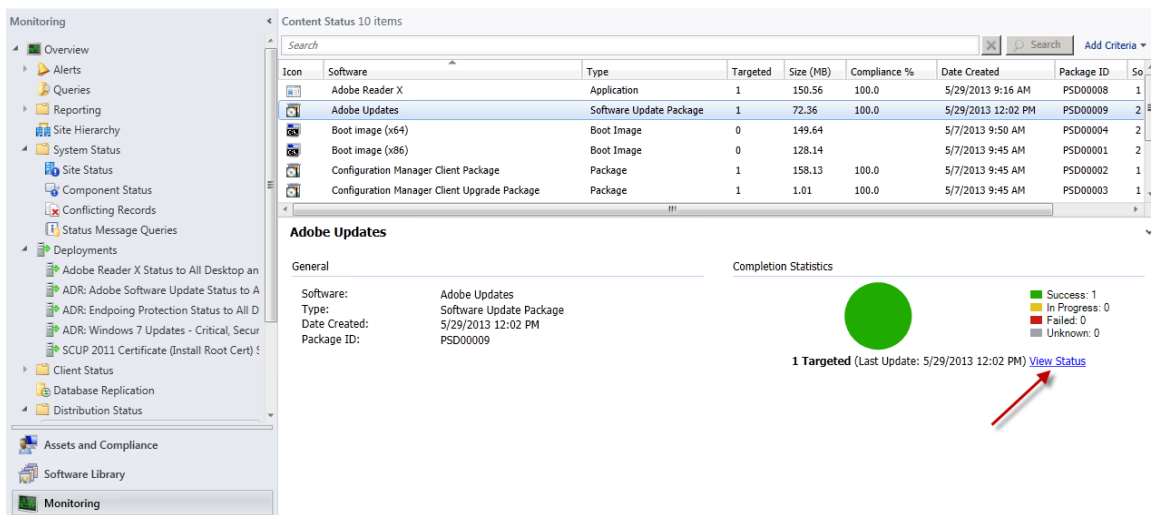
Monitor our Deployment Package getting distributed to our Distribution Points

Now that the ADR has run and our **Deployment Package** has been updated we can check the **status** of the package. In the **Software Library** workspace, select **Software Updates** and expand **Deployment Packages**, select our **Adobe Updates** deployment Package.

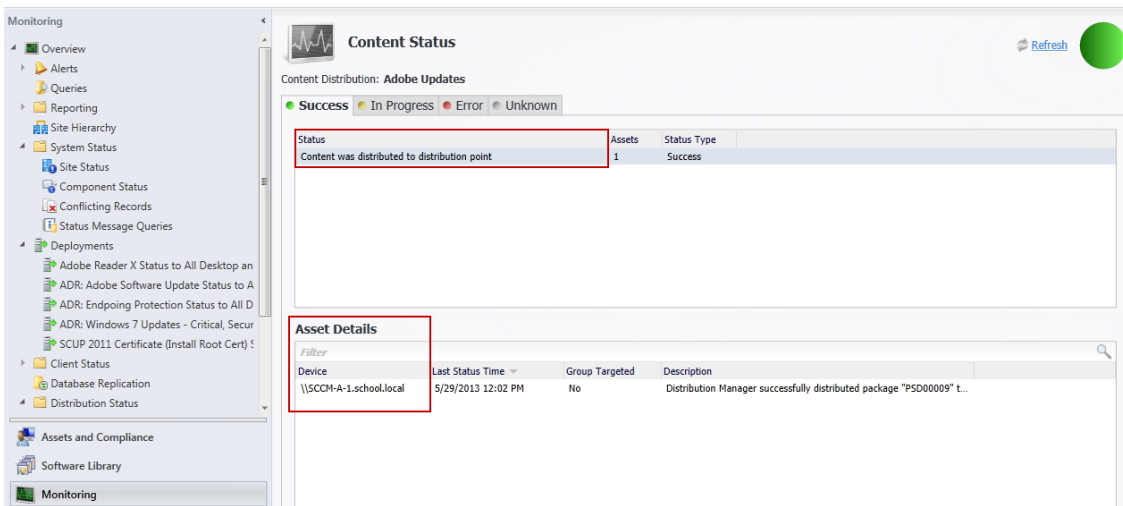


Straight away you can see that the status is good as it is green (successful). However let's dig deeper and click on **Content Status** in the right corner, then select our package in question, **Adobe Updates**.

Once again we can see it is successful, however if you have **multiple distribution points** you may want to know more information. Click on **View Status**.

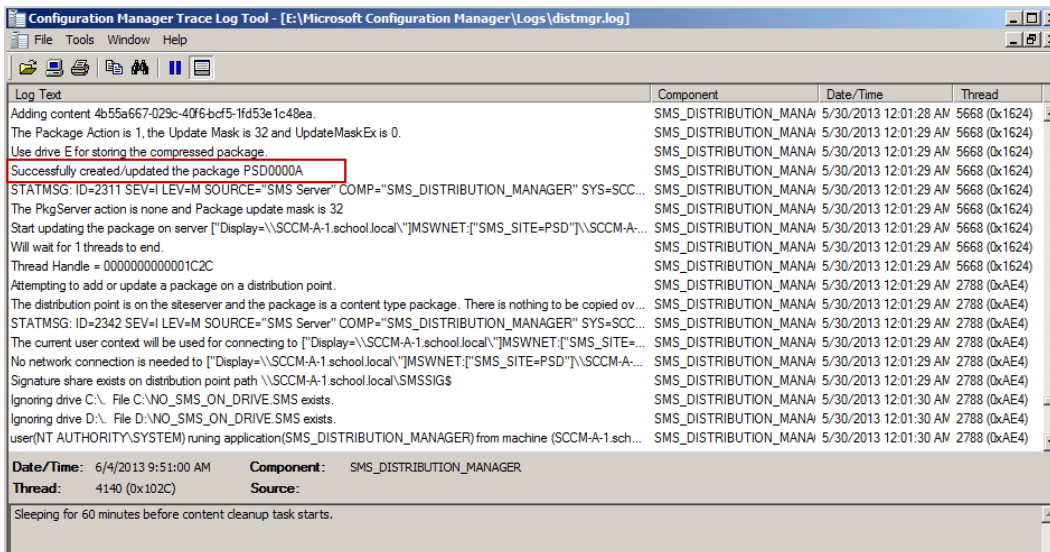


This shows us **4 tabs** where we can review the success or failure of our deployment package getting to our distribution points.

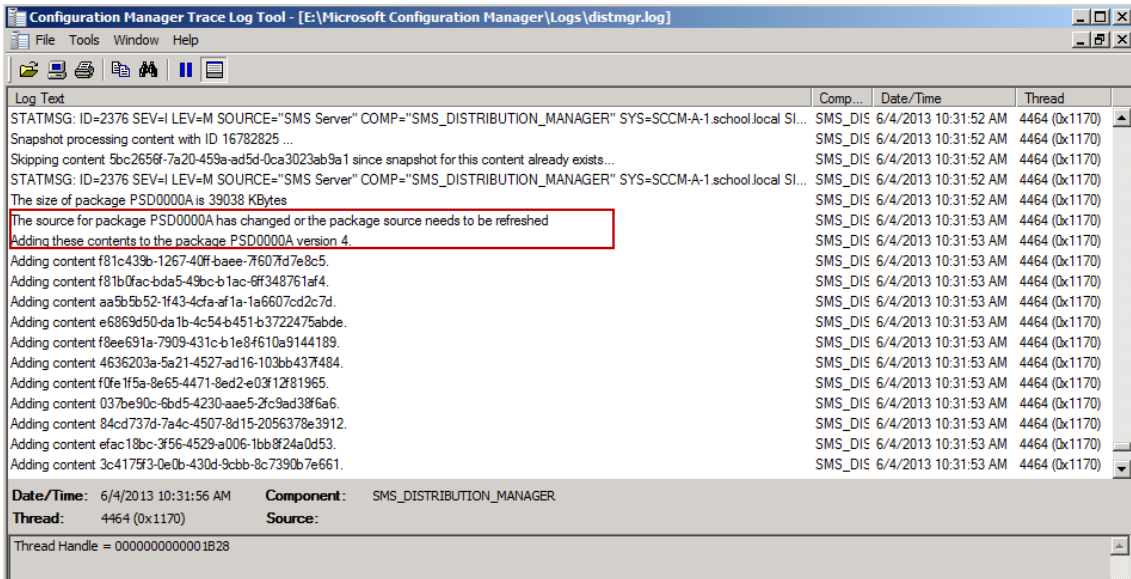


In addition to using the Configuration Manager console to get the status of our Deployment Package (which contains our windows updates), you can review the **distrmgr.log** file on CAS to review when the Deployment Package gets the updates added to it and then when it is distributed to the distribution point(s).

Open the **distrmgr.log** file and look for the line **Found package properties updated information for package 'PSD0000A'** which is our Deployment Package, change the Package ID to suit your own Deployment Package id.

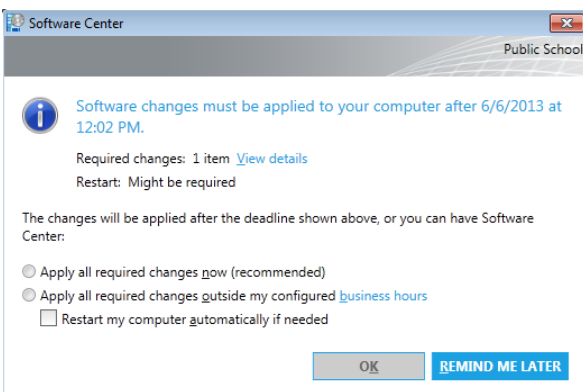
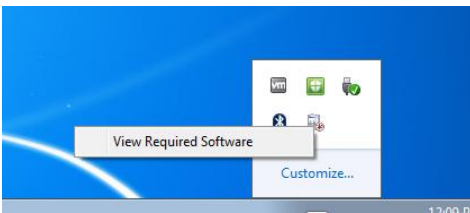


Further down the log you can see that the source for the package has changed or the package source needs to be refreshed. At this point it updates the source version (to 4) and then adds the changed content (new updates)

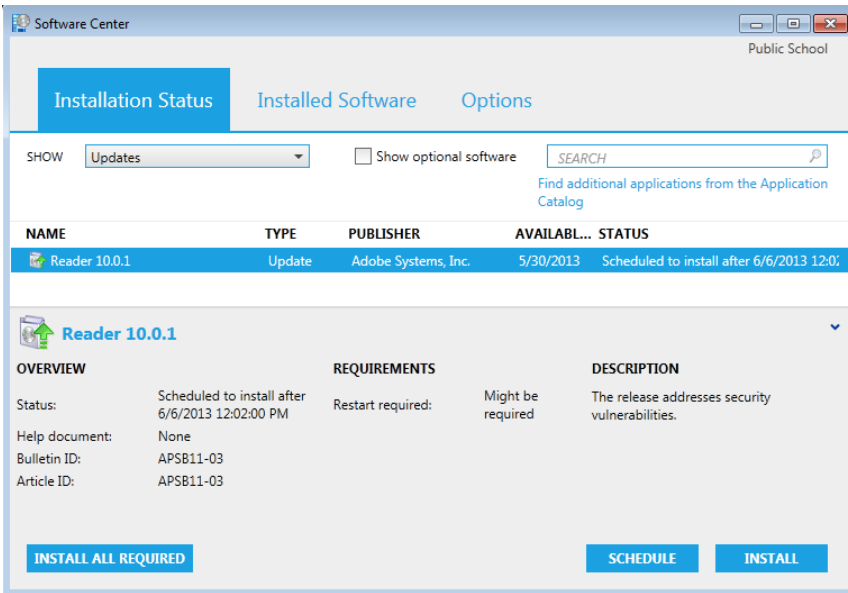


Monitor the Windows update process on our clients

Once the computer has received policy you'll see the following notification telling you that software changes are required, Clicking on that will give you more details of the deployment



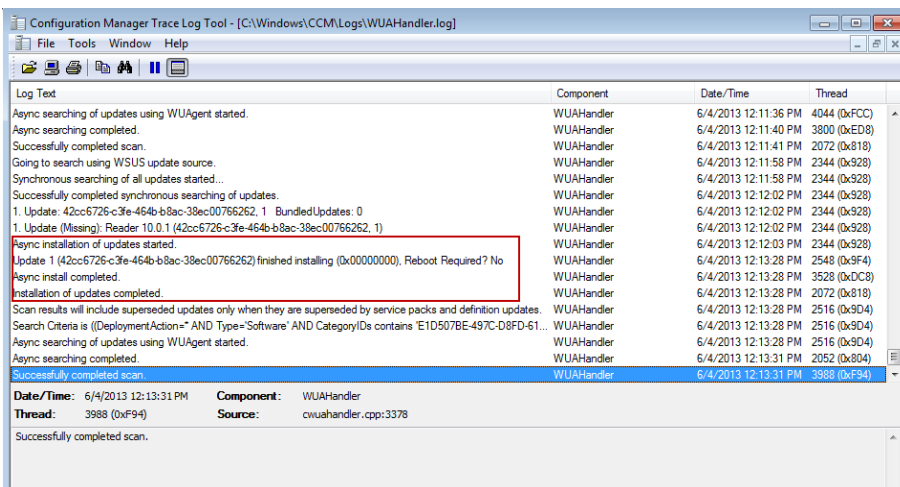
If you click on **View Details** you'll get even more details of what this deployment actually is.. and it is of course our Adobe Updates,



Click on **Install all required** to see what happens when the deadline is met.

The updates are downloaded and installed... if there's a **restart required** you'll be informed of that, you can click on **restart** to speed up the process.

If you want to see the process above via log files you can review the **C:\Windows\CCM\Logs\WUAHandler.log** on the client to see when it scans against our SUP server to see what's available, and it can see that updates are missing, and the updates are installed, you can also see the restart information per update listed, this is the same info that was reflected in the Software Center



In addition to the above log you can review the **C:\Windows\windowsupdate.log** .

It starts the **search for updates** then adds some updates to the search result. Then **downloads** applicable updates to the cache, and then it **installs the updates..** before telling us that it **succeeded installing those updates...**

