Managing Software Updates with System Center 2012 R2 Configuration Manager

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication and is subject to change at any time without notice to you. This document and its contents are provided AS IS without warranty of any kind, and should not be interpreted as an offer or commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

The descriptions of other companies' products in this proposal, if any, are provided only as a convenience to you. Any such references should not be considered an endorsement or support by Microsoft. Microsoft cannot guarantee their accuracy, and the products may change over time. Also, the descriptions are intended as brief highlights to aid understanding, rather than as thorough coverage. For authoritative descriptions of these products, please consult their respective manufacturers.

This deliverable is provided, AS IS without warranty of any kind and MICROSOFT MAKES NO WARRANTIES, EXPRES OR IMPLIED, OR OTHERWISE.

All trademarks are the property of their respective companies.

Printed in the United States of America

Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of the actual companies and products mentioned herein may be the trademarks of their respective owners.

Objectives	After completing this lab, you will be able to: ▪ Configure integration with Configuration Manager 2012 and WSUS 3.0 ▪ Analyze software update compliance ▪ Distribute updates using Configuration Manager 2012 ▪ Create an automatic deployment rule to deploy updates automatically ▪ Use Configuration Manager to report software update compliance status
Prerequisites	This lab requires an installed and functioning Configuration Manager 2012 site with WSUS 3.0 SP2 installed, and software updates inserted into WSUS (Primary1 is the site server virtual machine image). This lab also requires at least one Configuration Manager 2012 client (Client1 is the client computer in addition to the site server virtual machine being installed as a client).
Estimated Time to Complete This Lab	75 Minutes
Computers used in this Lab	🟥 Primary1 🟩 Client1 The password for the **administrator** account on all computers in this lab is: **password**.

1 Configuring Configuration Manager 2012 Integration with WSUS

In this exercise, you will configure Configuration Manager 2012 to integrate with WSUS 3.0 in order to scan for and deploy software updates to the Configuration Manager clients. You will begin by configuring the WSUS 3.0 SP2 computer as a Configuration Manager software update point.

Tasks	Detailed steps
Complete the following task on: **Primary1**	
1. Verify the installation of WSUS 3.0	1. Click **Start | Administrative Tools | Services**. **NOTE**: The Services window appears displaying the services installed locally. 2. What services are installed that indicate that Windows Server Update Services is installed locally? • **Update Services and WsusCertServer** **NOTE**: The WsusCertServer service does not need to be started for Configuration Manager integration with WSUS. 3. Close Services.
2. Start the Configuration Manager 2012 R2 Console	1. On the **Start** menu, click **Configuration Manager Console**. **NOTE**: The System Center 2012 R2 Configuration Manager console window appears displaying the Overview page of the Assets and Compliance workspace. You could also start the Configuration Manager Console by navigating to **Start** | **All Programs** | **Microsoft System Center 2012 R2** | **Configuration Manager Console**.
3. Configure a software update point	1. Click the **Administration** workspace. **Note**: The Administration workspace appears displaying the Overview page in the results pane. 2. In the navigation pane, expand **Site Configuration**, and then click **Sites**. **Note**: The list of sites appears in the results pane. Notice that there is only one site available "MCM". 3. In the navigation pane, click **Servers and Site System Roles**. **Note**: The list of site systems and installed roles appears in the results pane and preview pane respectively. Notice that the site only has one site system, "Primary1", and that this site system does not have the "Software update point" site system role installed currently. In a production environment, it is recommended to set up a remote server as the software update point (which has the WSUS feature installed and running) in the environment and not install the software update point site system role on the site server. However in our lab environment, we'll use a single server to host all roles to reduce the number of images that need to be started at one time. 4. On the **Home** tab of the Ribbon, click **Add Site System Roles**. **Note**: The **Add Site System Roles Wizard General** dialog box appears. Notice that the site is publishing the intranet FQDN of the site server. This information was collected during Configuration Manger Setup as part of the

prerequisite check for the management point role, which is installed on the site server.

5. Click **Next**.

Note: The **Add Site System Roles Wizard System Role Selection** dialog box appears displaying the list of site system roles that can be assigned to this computer.

6. Click **Next**.

Note: The **Add Site System Roles Wizard Proxy** dialog box appears allowing you to configure appropriate proxy settings to use for access to the Internet to download update content for synchronization as well as for downloading content by automatic deployment rules. Since you are in a virtual environment, no proxy servers are required as you will not connect to the Internet. However, in a production environment, you may be required to supply valid proxy configuration to allow the WSUS computer to access the Microsoft Update site on the Internet.

7. Under **Available roles**, select **Software update point**, and then click **Next**.

NOTE: The **Add Site System Roles Wizard Software Update Point** dialog box appears allowing you to configure the protocol and ports for WSUS server access, as well as the type of clients that the software update point will support.

8. Click **Next** to accept the default settings for HTTP communication and intranet-only clients.

NOTE: The **Add Site System Roles Wizard Proxy and Account Settings** dialog box appears allowing you to configure the proxy server configuration for the software update point.

9. Click **Next** to not configure proxy settings.

NOTE: The **Add Site System Roles Wizard Synchronization Source** dialog box appears displaying settings for synchronization with the software update point. Notice that the default configuration is to synchronize with Microsoft Update for catalog metadata. However, since you are in a virtual environment without Internet access, and will perform manual synchronization, you will change the configuration. The second option allows you to configure the software update point to use an upstream WSUS server that may have access to the Internet in the event that the software update point is not capable of accessing the Internet.

10. Click **Do not synchronize from Microsoft Update or upstream data source**, and then click **Next** to not have clients send scan results to WSUS (instead send results only to Configuration Manager).

NOTE: The **Add Site System Roles Wizard Synchronization Schedule** dialog box appears allowing you to configure the schedule to synchronize updates from WSUS with Configuration Manager. Notice that by default, the software update point does not synchronize with the WSUS server automatically. Not having a synchronization schedule is fine in this lab environment, however in a production environment you would want to configure automatic synchronizations. As to how often you want to synchronize, it is not a problem to sync frequently, as it is a delta synchronization process. Notice also that you can configure the site to generate an alert if the synchronization process fails.

11. Click to select **Alert when synchronization fails on any site in the**

hierarchy, and then click **Next** to not schedule synchronization.

NOTE: The **Add Site System Roles Wizard Supersedence Rules** dialog box appears allowing you to configure whether or not you want Configuration Manager to automatically manage superseded updates (which is to immediately expire superseded updates - just as Configuration Manager 2007 does), or if you want to not immediately expire superseded updates for a specific period of time (defaults to three months). Once an update is 'expired' it can no longer be deployed. Superseded updates are expired automatically when superseded.

12. Click **Next** to accept the default configuration to allow the deployment of superseded updates for three months.

NOTE: The **Add Site System Roles Wizard Classifications** dialog box appears displaying the various product categories of updates that are available in Configuration Manager for reporting and deployment. Notice that by default, security updates, service packs, and update rollups are to be managed by Configuration Manager. The WSUS server has critical updates and service packs inserted into its database, so you will set those now.

13. Configure to synchronize only **Critical Updates** and **Service Packs**, and then click **Next**.

NOTE: The **Add Site System Roles Wizard Products** dialog box appears allowing you to configure the various Microsoft software products that can be updated by Configuration Manager. You will configure the appropriate products later in this lab for synchronization, however to start synchronization, you will clear all products. There are specific products selected by default (you would have to expand the "All Products" node and then various other nodes to view them). As this lab environment uses synthetic updates, which are not official Microsoft updates, you *must* clear all existing products.

14. Under **Products**, click to select **All Products**.

Note: This will then select all product, which is not what you want for this specific lab environment. However this process will select all products, which makes it easy to clear all products in the next step. This is only required for this specific lab environment. In your production environment, you would expand "All Products" and then configure the specific products that you do want to synchronize. You will now remove that selection, so that no products are being managed. This again is only for this specific lab configuration.

15. Under **Products**, click to clear **All Products** to not include any Microsoft products, and then click **Next**.

NOTE: The **Add Site System Roles Wizard Languages** dialog box appears displaying the languages that content will be managed for through Configuration Manager. Notice that a total of six languages, including English, are enabled by default. In production, if your environment has to support other locations, you may need to enable other languages for scanning and deployment.

16. Click to clear all languages other than English, and then click **Next**.

Note: The **Add Site System Roles Wizard Summary** dialog box appears indicating that you have successfully completed the wizard and are ready to install this site system role.

17. Click **Next**.

Note: The **Add Site System Roles Wizard Completion** dialog box appears indicating that the wizard completed successfully.

	18. Click **Close**. **Note**: The System Center 2012 R2 Configuration Manager console window appears displaying the site systems and installed roles for the site. Notice that you did not create a new site system for this role and still only have the site server as a site system in the site. It will take a few moments for the "Software update point" site system role to be installed, however it will be displayed in the list of site system roles immediately.

In the following procedure, you will view logs to validate success of the software update point as well as view status messages related to the deployment of the software update point site system role.

Tasks	Detailed steps
Complete the following task on: **Primary1**	
1. Verify the software update point role	1. Open **C:\Program Files\Microsoft Configuration Manager\Logs\SUPSetup.log**. **NOTE:** Notepad appears displaying the contents of the Configuration Manager software update point installation log. Notice that the log indicates that the required WSUS version was detected, and that the installation was successful. 2. Close the SUPSetup.log, and then open **C:\Program Files\Microsoft Configuration Manager\Logs\WSUSCtrl.log**. **NOTE**: Notepad appears displaying the contents of the Configuration Manager WSUS Control Manager's log. Notice that the log indicates there was a successful connection to the WSUS server, and that the local database connection was successful. You have now successfully installed a Configuration Manager software update point on the WSUS 3.0 server. 3. Close the WSUSCtrl.log. **Note**: The System Center 2012 R2 Configuration Manager console window appears displaying the Administration page. 4. Click the **Monitoring** workspace. **Note**: The Monitoring workspace Overview page appears. 5. In the navigation pane, expand **System Status**, and then click **Site Status**. **NOTE** The list of Configuration Manager site system roles and their current status appears in the results pane. Notice that the "Software update point" role is listed, and displays a status of "OK". 6. In the navigation pane, click **Component Status**. **NOTE**: The list of Configuration Manager components and their current status appears in the results pane. 7. In the results pane, click **SMS_WSUS_CONTROL_MANAGER**, and then on the Ribbon, click **Show Messages**. **NOTE**: A new menu appears. 8. Click **All**.

	NOTE: The **Status Messages: Set Viewing Period** dialog box appears prompting for the age of status messages to display. 9. Click **OK** to view messages for the previous 24 hours. **NOTE**: The Configuration Manager Status Message Viewer for <MCM> window appears displaying the status messages for the SMS_WSUS_CONTROL_MANAGER component for the most recent 24 hours. Notice messages with IDs of 1013, 1014, and 1015. These messages indicate that the component should be installed, is being installed, and has been installed. The most recent message, with an ID of 500, indicates that the component was started. These messages are an indication that the software update point has been installed successfully. 10. Close the Configuration Manager Status Message Viewer for <MCM> window. **NOTE**: The list of Configuration Manager components and their current status appears in the results pane.

In the following procedure, you will force synchronization of the Configuration Manager site database with updates from the software update point, which is installed on the Windows Server Update Services (WSUS) computer. After the initial attempt to synchronize, you will then configure the appropriate classifications and products, and force another synchronization event, which will result in updates in the site database for scanning and deployments.

Tasks	**Detailed steps**
Complete the following task on: **Primary1**	
1. Force catalog synchronization	1. Click the **Software Library** workspace. **NOTE**: The Software Library workspace Overview page appears. 2. In the navigation pane, click **Software Updates**. **NOTE**: The Software Updates "Navigation Index" page appears in the results pane. Notice that the "Navigation Index" page displays links to objects that can be managed for software updates. Also notice that no alerts have been generated. 3. In the navigation pane, expand **Software Updates**, and then click **All Software Updates**. **NOTE**: The updates synchronized with Configuration Manager are displayed in the results pane. Notice that by default, no updates are listed. This is due to the fact that synchronization has not yet occurred. 4. On the Ribbon, click **Synchronize Software Updates.** **NOTE**: A **Configuration Manager** message box appears prompting to run the synchronization process on the site. 5. Click **Yes**. **NOTE**: The synchronization process is initiated. This process may take a few minutes to complete. There is no visual indication that the process has completed, so you'll need to view status messages or Configuration Manager log files to verify that the process has completed successfully. This process will determine which update classifications and products are available in the WSUS database. This is required in the lab environment as WSUS is not synchronizing

	with Microsoft Updates to use real Microsoft updates, rather the synthetic updates.
2. Configure products to synchronize	1. Click the **Administration** workspace. **NOTE**: The Administration workspace appears displaying the servers and site system roles installed on the site server computer. 2. In the navigation pane, click **Sites**. **NOTE**: The list of sites appears in the results pane. Notice that there is only one site available. 3. On the Ribbon, click **Settings**, click **Configure Site Components**, and then click **Software Update Point**. **NOTE**: The **Software Update Point Component Properties** dialog box appears displaying the sync settings. 4. Click the **Classifications** tab. **NOTE**: The **Software Update Point Component Properties** dialog box appears displaying the configured classifications. Notice that "Critical Updates" and "Service Packs" are configured to be synchronized. These are appropriate for the lab environment. 5. Click the **Products** tab. **NOTE**: The **Software Update Point Component Properties** dialog box appears allowing you to configure the products to be synchronized. Notice that no products are configured to be synchronized. For the lab environment, you will configure the "LAB" product. 6. Under Products, click to select both **LAB** options, and then click **OK.** **NOTE**: This will configure the software update point to use only updates from the vendor "LAB", which is what the synthetic updates are configured to use. In your production environment, you would still be using "Microsoft" updates, and would select the specific products you want updates to be synchronized for. The list of sites appears in the results pane.
3. Force a synchronization event	1. Click the **Software Library** workspace. **NOTE**: The Software Library workspace appears displaying the updates synchronized in the site. Notice that no updates are displayed. 2. On the Ribbon, click **Synchronize Software Updates**. **NOTE**: A **Configuration Manager** message box appears indicating that a hierarchy wide synchronization event will occur. 3. Click **Yes**. **NOTE**: A synchronization event is started. This will take a few minutes to complete. 4. Click the **Monitoring** workspace. **NOTE** The Monitoring workspace appears displaying the list of Configuration Manager components in the results pane. 5. In the results pane, click **SMS_WSUS_Sync_Manager**, and then on the Ribbon, click **Show Messages**. **NOTE**: A new menu appears with options for the type of messages to display. 6. Click **All**. **NOTE**: The **Status Messages: Set Viewing Period** dialog box appears allowing you to configure the age of the status messages to display. Notice that

the default time period is to display messages from the past 24 hours.

7. Click **OK** to show messages from the past day.

NOTE: The Configuration Manager Status Message Viewer for <MCM><Configuration Manager 2012 R2 Primary Site> window appears displaying the status messages for the WSUS Sync Manager. Notice the most recent messages with IDs of "6701", "6705" and "6702". These messages indicate the sync process has started, is in progress, and completed, respectively.

Remain at this point until the "6702" status message appears. You will need to refresh the list of status messages to display new status messages.

8. On the **File** menu, click **Exit.**

NOTE: The System Center 2012 R2 Configuration Manager console window appears.

9. In the navigation pane, click **Software Update Point Synchronization Status**.

NOTE: The status of the software update point synchronization appears in the results pane, with additional information displayed in the preview pane. Notice that the status is "Completed", no synchronization source listed (the SUP was configured to not sync from a source), the dates and times of the last synchronization attempt and last successful synchronization, as well as the catalog version ("1").

This is a very valuable way to quickly identify the status of your catalog synchronization process for Configuration Manager.

10. Open **C:\Program Files\Microsoft Configuration Manager\Logs\Wsyncmgr.log.**

NOTE: Notepad appears displaying the contents of the WSUS Sync Manager's log file.

11. Search for **synchronizing**.

NOTE: Notepad displays the first occurrence of the text "synchronizing". Notice that the line indicates that the synchronization process is happening with Configuration Manager and the WSUS server Primary1. On later lines of the log, notice the following processes occurring:

- Requested localization languages – one for each language configured in WSUS
- Requested update classification – one for each type of update to be managed
- Synchronizing updates – this begins the process of synchronization of individual updates (numerous pages of updates being synchronized in the lab)
- Done synchronizing SMS with WSUS Server Primary1 – signals the end of the synchronization process
- Updated x items in SMS database – the number depends on the specific lab configuration, catalog, etc. There should be 46 updates in the Configuration Manager database
- The time it took to synchronize the catalog from WSUS to Configuration Manager – in our lab environment, this should only take about one minute

12. Close Notepad, and then return to the System Center 2012 R2 Configuration Manager console window.

NOTE: The System Center 2012 R2 Configuration Manager console appears.

15. Click the **Software Library** workspace.

NOTE: The Software Library workspace appears displaying the available software updates from the **All Software Updates** node. Notice that there are 46 software updates displayed in the results pane and display the following attributes:

- An icon to represent the status of the update
- The update title and bulletin ID
- How many clients have reported the update as being required (none at this point for us as no clients have scanned against the catalog yet)
- Whether or not the update has been downloaded
- Whether or not the update has been deployed

Also notice that in the preview pane, the Summary tab displays details for the update highlighted in the results pane, as well as the statistics related to the compliance for that update. At the current time, there is no status, as no client compliance scans have been completed, and no updates have been deployed. The Deployment tab displays any deployments that include this update (there are none at this time).

2 GENERATING UPDATE STATUS ON THE CONFIGURATION MANAGER 2012 CLIENT

In this exercise, you will force the clients to run a software update scan cycle. This will cause the clients to scan for updates through WSUS, and then store the information in WMI. Configuration Manager will then automatically send the data to the Configuration Manager site through state messages.

Tasks	Detailed steps
Complete the following task on: **Client1** and **Primary1**	
1. Force the software updates scan cycle on the client	1. In **Control Panel**, click **System and Security**, and then start **Configuration Manager**. **NOTE**: The **Configuration Manager Properties** dialog box appears. 2. Click the **Actions** tab**.** **NOTE**: The **Configuration Manager Properties** dialog box displays the available actions for the client. Even if the Software Updates Scan Cycle action may already appear in the list, the catalog version likely has not been updated for the client, so you will start by retrieving policies. 3. Click **Machine Policy Retrieval & Evaluation Cycle**, and then click **Run Now**. **NOTE**: The Configuration Manager client will request new policies, which will include the policy related to the active software update point and catalog version. A **Machine Policy Retrieval & Evaluation Cycle** message box appears indicating the action was initiated, and may take several minutes to complete. 4. Click **OK**. **NOTE**: The **Configuration Manager Properties** dialog box appears. Wait a moment before moving onto the next step to force a catalog scan. If the **Software Updates Scan Cycle** action was not listed, then you will need to close the **Configuration Manager Properties** dialog box, start it again, and then return to the **Actions** tab before moving onto step 5. 5. Click **Software Updates Scan Cycle**, and then click **Run Now**. **NOTE**: If the "Software Updates Scan Cycle" task does not appear, you can force a policy retrieval cycle "Machine Policy Retrieval & Evaluation Cycle", wait a moment, and then check again. The client will force a scan for software updates. A **Software Updates Scan Cycle** message box appears indicating the action was initiated, and may take several minutes to complete. In a production environment, you would not need to force these two actions, as they would happen automatically. You are forcing them in the lab to have them run more quickly than they would in production. Configuration Manager 2012 automatically implements a random scan cycle on each client of up to two hours to spread network load. 6. Click **OK.** **NOTE**: The **Configuration Manager Properties** dialog box appears.

7. Click **OK**, and then open **C:\Windows\WindowsUpdate.log**.

NOTE: Notepad appears displaying the contents of the WindowsUpdate.log. When Configuration Manager initiates a scan for software update compliance, it calls the Windows Update service to actually complete the scan process.

If you scroll to the bottom of the log, you will see references to "Added update" with an update GUID listed. There should be 46 updates added, as indicated by the log line "Found 46 updates and 19 categories in search".

8. Close the **WindowsUpdate.log**.

NOTE: It will take a few minutes for the client to be scanned, and the results to be returned to the Configuration Manager site through state messages. The default state message forwarding interval is set to 15 minutes, though for this lab environment, the interval was set to two minutes. **You should NOT** set this value to anything less than 15 minutes in a production environment, as it can cause a backlog of state messages on the site server.

3 Generating Software Update Compliance Reports

In this exercise, you will view the scan results of clients through software update compliance reports in the Configuration Manager console. This is an easy way to verify the client scan results.

Tasks	Detailed steps
Complete the following task on: **Primary1**	
1. Generate an update status report for software updates	1. Click the **Monitoring** workspace.
	Note: The Monitoring workspace appears displaying the software update point synchronization status.
	2. In the navigation pane, expand **Reporting**, and then click **Reports**.
	NOTE: The list of available reports appears in the results pane. Notice that there are 462 reports available.
	3. In the navigation pane, expand **Reports**, and then click **Software Updates - A Compliance**.
	NOTE: The list of reports in this specific category appears in the results pane. Notice that there are now only eight reports displayed. You could have also used the "Search" feature to search for specific reports.
	4. In the results pane, click **Compliance 2 - Specific software update**, and then on Ribbon, click **Run**.
	NOTE: The **Compliance 2 - Specific software update** report window appears. Notice this is a prompted report, and requires the collection ID and update to search for. The "Update filter" is a filter box for searching for a specific update, or a wildcard of updates.
	5. After **Collection**, click **Values**.
	NOTE: The **Parameter Value** dialog box appears displaying the list of available collections.
	6. Under **Collection**, click **Configuration Manager Clients**, and then click **OK**.
	NOTE: The **Compliance 2 - Specific software update** report window appears allowing you to enter the required values.
	7. In the **Update filter** box, type **English Update1**
	NOTE: There is no space between "Update" and "1".
	8. Click **View Report**.
	NOTE: The **Compliance 2 - Specific software update** report window displays the status of the specific update. Notice that the information in the report includes the title, article ID, bulletin ID, vendor, and the compliance information for the update. The number of systems reporting that the update is required, and those unknown, will depend on how many clients scan results have been processed for. You should two clients that are reporting the update as "Required". It would be recommended to run reports on a collection of clients that you can manage from this site to provide better reporting data and status.
	9. Under **Title**, click **English Update1**.
	NOTE: The **Compliance 6 - Specific software update states**

(secondary) report window displays the status of the specific update. Notice that the information in the report includes the compliance information for the update, including states for required, installed, unknown, and update not required. Notice also that the number of computers, as well as the percentage of computers in each state, are displayed.

10. Under **State**, click **Update is required**.

NOTE: The **Compliance 8 - Computers in a specific compliance state for an update (secondary)** report window displays the status of the specific update for clients that require this update. Notice that the information in the report includes the update information, as well as those clients that have reported that this update is required.

11. Close the **Compliance 8 - Computers in a specific compliance state for an update (secondary) report** window.

NOTE: The list of reports in the specific category appears in the results pane.

12. In the results pane, click **Compliance 5 - Specific computer**, and then on the Ribbon, click **Run.**

NOTE: The **Compliance 5 - Specific computer** report window appears. Notice this is a prompted report, and requires the computer name, with vendor and update class as optional attributes.

13. After **Device Name**, click **Values**.

NOTE: The **Parameter Value** dialog box appears allowing you to select the computer to run the report for.

14. Under **Device Name**, click **Client1.ConfigMgrDom**, and then click **OK**.

NOTE: The **Compliance 5 - Specific computer** report window appears displaying the computer name the report will be run for. The "Vendor" and "Update Class" parameters are optional for this report and default to "<All Values>".

15. Click **View Report**.

NOTE: The **Compliance 5 - Specific computer** report window displays the list of updates and their compliance for the specific Configuration Manager client computer. Notice that the information in the report includes the title, update class, bulletin ID, article ID, vendor, whether the computer is compliant with the update, any deadline for the update installation, the update ID, and an information URL. Notice also that each update is listed as being required.

16. Close the **Compliance 5 - Specific computer** report window.

NOTE: The list of reports in the specific category appears in the results pane.

17. In the navigation pane, click **Software Updates - B Deployment Management**.

NOTE: The list of reports in the specific category appears in the results pane. Notice that there eight reports in this category.

18. In the results pane, click **Management 2 - Updates required but not deployed**, and then on the Ribbon, click **Run.**

NOTE: The **Management 2 - Updates required but not deployed** report window appears. Notice this is a prompted report, and requires the collection to report on and the vendor and update class.

19. After **Collection**, click **Values.**

NOTE: The **Parameter Value** dialog box appears displaying the list of available collections.

20. Under **Collection**, click **Configuration Manager Clients**, and then click **OK**.

NOTE: The **Management 2 - Updates required but not deployed** report window appears allowing configuration of the prompted values.

21. After **Vendor**, click **Values.**

NOTE: The **Parameter Value** dialog box appears displaying the available vendors. In our case, the options are Lab, Local Publisher and Microsoft. The synthetic updates used in this lab use a publisher of "Lab".

22. Under **Vendor**, click **LAB**, and then click **OK.**

NOTE: The **Management 2 - Updates required but not deployed** report window appears allowing configuration of the prompted values.

23. After **Update Class**, click **Values**.

NOTE: The **Parameter Value** dialog box appears displaying the available update classes. Notice that the classes are those available in WSUS.

24. Under **Update Class**, click **Critical Updates**, and then click **OK.**

NOTE: The **Management 2 - Updates required but not deployed** report window appears displaying the configured prompted values.

25. Click **View Report**.

NOTE: The **Management 2 - Updates required but not deployed** report window appears. Notice the report displays information for the appropriate update, including the title, bulletin ID, article ID, the number of client's requiring the update, and information URLs for the collection members.

26. Close the **Management 2 - Updates required but not deployed** report window.

NOTE: The list of reports in the specific category appears in the results pane.

Now that you've viewed the compliance of software updates, for a specific update, a specific computer, and all required updates, through reports, you will have the information necessary to determine which updates to deploy. You will deploy software updates in the next exercise. Note that you can also view compliance information for individual software updates in the "All Software Updates" node, which you will do in the next exercise. Reports are generally easier to view status for update compliance.

4 DEPLOYING SOFTWARE UPDATES USING CONFIGURATION MANAGER SOFTWARE UPDATE MANAGEMENT

In this exercise, you will distribute specific software updates using Configuration Manager and the software updates management feature. The lab procedures will use synthetic updates as no active connection to the Internet is available to use real Microsoft updates.

Tasks	Detailed steps
Complete the following task on: **Primary1**	
1. Summarize software update status in the Configuration Manager console	1. Click the **Software Library** workspace. **NOTE**: The Software Library workspace appears displaying the synchronized software updates in the results pane. Notice that there are 46 updates available. Notice that the "Required" column may still display a value of "0" for all updates, even though you saw updates as required when running reports. This is due to the fact that the console summarization runs on a schedule, whereas reports are on-demand. 2. On the Ribbon, click **Run Summarization**. **NOTE**: A **Configuration Manager** message box appears indicating that this will summarize compliance throughout the hierarchy (you have a standalone primary site in this lab environment). This would happen automatically within the next hour by default. 3. Click **OK**. **NOTE**: The System Center 2012 R2 Configuration Manager console displays the list of software updates in the results pane. 4. Refresh the **All Software Updates** node of the console. **NOTE**: The System Center 2012 R2 Configuration Manager console displays the status of software updates in the results pane. Notice that each update now displays "2" in the "Required" column. Notice also that the preview pane displays update information, as well as statistics for the selected update. If you only forced the "Software Updates Scan Cycle" on one client, then you will only have results for one client.
2. Create a software update group of updates	1. In the **Search** box, type **English update** and then click **Search**. **NOTE**: The filtered view of results for English updates appears in the results pane. Notice that there are now only 13 updates displayed in the results pane, filtered from the original list of 46 updates. 2. Under **Title**, multi-select **English Update1**, **English Update2**, and **English Update3**. 3. On the **Home** tab of the Ribbon, click **Create Software Update Group**. **NOTE**: The **Create Software Update Group** dialog box appears allowing you to provide a name for the software update group, as well as a description for the group. 4. In the **Name** box, type **Lab Critical Updates** and then click **Create**. **NOTE**: The filtered view of results for English updates appears in the results pane. Notice that there are now only 13 updates displayed in the results

	pane, filtered from the original list of 46 updates. 5. In the navigation pane, click **Software Update Groups**. **NOTE**: The software update groups in the site appear in the results pane, with compliance data for the software update group displayed in the preview pane. This data is not up to date, as summarization has not occurred yet. 6. In the results pane, click **Lab Critical Updates**, and then on the Ribbon, click **Show Members**. **NOTE**: The members of the "Lab Critical Updates" software update group are displayed in the results pane with compliance data displayed in the preview pane. Notice that a sticky node for the members is created under the "All Software Updates" node. You will deploy this software update group in the next task. You could also immediately deploy the updates without first creating the software update group, and create the software update group as part of the deployment process.
3. Deploy the software update group	1. In the navigation pane, click **Software Update Groups**. **NOTE**: The one software update group appears in the results pane. 2. On the Ribbon, click **Deploy**. **NOTE**: The **Deploy Software Updates Wizard General** dialog box appears. Notice that if you have saved any software deployment templates, you could select one to use for this deployment from this page. You save software update templates on the "Summary" page of this wizard, or you can migrate templates from an existing Configuration Manager 2007 site. Also notice that the "Software Update/Software Update Group" value is automatically supplied as you launched the wizard from the software update group. 3. In the **Deployment Name** box, type **Lab Critical Updates** 4. In the **Description** box, type **Critical updates for the lab** 5. After **Collection**, click **Browse**. **NOTE**: The **Select Collection** dialog box appears displaying the collections of systems in the site. Notice that the **Select Collections** dialog box displays the number of members of each collection. Notice also that you cannot deploy software updates to user collections, only device collections. 6. Under **Name**, click **Configuration Manager Clients**, and then click **OK**. **NOTE**: The **Deploy Software Updates Wizard General** dialog box appears displaying the deployment and software update group names, as well as the designated collection to be targeted with the deployment. 7. Click **Next**. **NOTE**: The **Deploy Software Updates Wizard Deployment Settings** dialog box appears allowing you to configure if the deployment is required (mandatory) or available (optional), whether or not to wake up clients using Wake-on-LAN, as well as the detail level. The detail level controls the number of state messages for the update deployment. 8. In the **Type of deployment** box, verify that **Required** is displayed. 9. In the **Detail level** box, verify that **Only success and error messages** is displayed, and then click **Next**. **NOTE**: The **Deploy Software Updates Wizard Scheduling** dialog box

appears allowing you to configure when the deployment is available to be installed on the client, the deadline as to when the updates must be installed, and whether the time is based on UTC or the client local time.

10. Under **Installation deadline**, verify that the deadline is set to the default of seven days in the future.

NOTE: in a production environment, you certainly can deploy updates immediately (deadline of "As soon as possible"). However, in the lab, you will leave the deadline in the future to experience the new user interface for software update deployments.

11. Click **Next** to accept the defaults for "Client local time" and the updates are available immediately, with deadline one week in the future.

NOTE: The **Deploy Software Updates Wizard User Experience** dialog box appears allowing you to configure the end user experience with regards to notifications, and the reboot behavior when updates require a system restart, including whether or not installation and reboots should occur outside any configured maintenance windows. Notice that the default is display the notification in Software Center, display all notifications and balloons, to adhere to any applicable maintenance windows, and to not to suppress restarts.

12. Click **Next** to display notifications in Software Center, to deploy within configured maintenance windows (there are none in the lab environment), to not suppress any reboots, and commit changes to Windows Embedded clients.

NOTE: The **Deploy Software Updates Wizard Alerts** dialog box appears allowing you to configure whether or not any alert is generated if the percentage of compliant systems is below a specific percent, as well as whether or not to generate an event in Operations Manager for any failure in the update deployment.

13. Click **Next** to not generate an alert on compliance percentage, nor to generate a Microsoft Operations Manager event when installing updates or in the case of a failure.

NOTE: The **Deploy Software Updates Wizard Download Settings** dialog box appears allowing you to configure whether or not clients can install updates when in slow network boundaries, or when the client's protected distribution point does not contain the update content.

14. Click **Next** to not support slow network boundaries, to allow fallback to unprotected distribution points, to support Branch Cache deployment of updates when available in the environment, to not support fallback to Microsoft Updates if content is not available on Configuration Manager distribution points, and to not allow download at the deadline over metered Internet connections.

NOTE: The **Deploy Software Updates Wizard Deployment Package** dialog box appears prompting to name the new deployment package to add the updates to. The default is to use an existing deployment package if one exists. As this is your first deployment, you do not have one yet, so will need to create a deployment package.

15. In the **Name** box, type **Critical Updates**
16. In the **Description** box, type **Critical updates for all clients**
17. In the **Package source** box, type **\\Primary1\C$\Critical** If this

folder does not exist then create it and then select it

18. Click **Next**.

NOTE: The **Deploy Software Updates Wizard Distribution Points** dialog box appears allowing you to designate the distribution points to distribute the package to. Notice that no distribution points are added to the deployment package by default.

19. Click **Add**.

NOTE: A new menu appears with options for distribution of software update content. Notice that you can distribute to distribution points or distribution point groups. In this lab environment, no distribution point groups have been created, so you will distribute to a distribution point.

20. Click **Distribution Point**.

NOTE: The **Add Distribution Points** dialog box appears displaying the list of available distribution points. Notice that you have one distribution point available in the site.

21. Under **Available distribution points**, click to select **Primary1.ConfigMgrDom.local**, and then click **OK**.

NOTE: The **Deploy Software Updates Wizard Distribution Points** dialog box appears displaying the distribution points to distribute the package to. Notice that the local site server (as a distribution point) is listed.

22. Click **Next**.

NOTE: The **Deploy Software Updates Wizard Download Location** dialog box appears allowing you to configure whether or not to download updates automatically from the Internet or to retrieve them from a network location. In the lab environment, the updates have already been downloaded and staged on the site server's hard drive as no connection to the Internet is available.

23. Click **Download software updates from a location on my network**, and then click **Browse**.

NOTE: The **Select Folder** dialog box appears allowing you to select the source of the updates.

24. Click **C:\Lab Files\WSUS Synthetic**, and then click **Select Folder**.

NOTE: The **Deploy Software Updates Wizard Download Location** dialog box appears displaying the configured source folder.

25. Click **Next**.

NOTE: The **Deploy Software Updates Wizard Language Selection** dialog box appears allowing you to configure which languages updates should be downloaded for. Notice that the default is the same as you configured during the configuration of the software update point.

26. Click **Next** to accept the configured language(s).

NOTE: The **Deploy Software Updates Wizard Summary** dialog box appears indicating you have successfully completed the wizard. Notice that the details include the updates to be deployed, the target collection, and the deployment schedule.

Notice also that if you want to create a deployment template, the **Save As Template** button is available. It would create a software update template of the settings configured during the current **Deploy Software Updates Wizard** session.

	27. Click **Next**. **NOTE**: The **Deploy Software Updates Wizard Progress** dialog box appears displaying the progress of the deployment, which includes the downloading of each update to be deployed, and creating the deployment template and deployment package. When complete, the **Deploy Software Updates Wizard Completion** dialog box appears displaying the status on each phase of the deployment. 28. Verify that each phase of the process was successful, and then click **Close**. **NOTE**: The System Center 2012 R2 Configuration Manager console appears displaying the list of software updates in the results pane.

In the following procedure, you will view the objects created as a result of running the Deploy Software Updates Wizard from the Configuration Manager console.

Tasks	**Detailed steps**
Complete the following task on: 🖥 **Primary1**	
1. View the software update distribution objects	1. In the navigation pane, click **Software Update Groups**. **NOTE**: The software update groups appear in the results pane. There are no software update groups by default, however when running the Deploy Software Updates Wizard, one will be created if not present prior to starting the wizard. In this lab environment, you did create the software update group prior to running the Deploy Software Updates Wizard, however it is not required to do so. 2. In the results pane, click **Lab Critical Updates**. **NOTE**: The preview pane displays summary information for the "Lab Critical Updates" software update group. Notice that it displays the date and time the software update group was created, as well as a chart with client compliance data. Notice that the number of systems that are currently reported as "Non-compliant" (which may not have been updated yet). 3. In the preview pane, click the **Deployment** tab. **NOTE**: The preview pane displays deployment information for the "Lab Critical Updates" software update group. Notice that it displays the deployment name, target collection, whether or not the deployment is enabled (it is enabled by default) and the date and time the deployment was made available for clients. 4. In the navigation pane, click **Deployment Packages**. **NOTE**: The deployment packages appear in the results pane. Notice that there is one deployment package, which was created when running the Deploy Software Updates Wizard. Also notice that the preview pane displays the package properties for the deployment package, as well as the package status on the targeted distribution points. 5. On the Ribbon, click **Show Members**. **NOTE**: The software updates that are included in this deployment package appear in the results pane, with the details of the selected software update displayed in the preview pane. Notice that the deployment package includes

	the three updates you added to the software update group prior to starting the Deploy Software Updates Wizard. Notice also that a "Critical Updates" sticky node is added to the navigation pane under "All Software Updates".

In the following procedure, you will force the Configuration Manager client to retrieve policies, which will provide the software update deployment to the client. You can use both the client and server computer for this procedure.

Tasks	**Detailed steps**
Complete the following task on: 🟩 **Client1** and 🟥 **Primary1**	
1. Install the update on the Configuration Manager client	1. In **Control Panel**, click **System and Security**, and then start **Configuration Manager**. **NOTE**: The **Configuration Manager Properties** dialog box appears. 2. Click the **Actions** tab. **NOTE**: The **Configuration Manager Properties** dialog box displays the available actions for the Configuration Manager client. 3. Click **Machine Policy Retrieval & Evaluation Cycle**, and then click **Run Now**. **NOTE**: The Configuration Manager client will request new policies, which will include the policy related to the software update deployment. A **Machine Policy Retrieval & Evaluation Cycle** message box appears indicating the action was initiated, and may take several minutes to complete. 4. Click **OK**. **NOTE**: This forces the Configuration Manager client to check for new policies. When it has finished the check, the software updates will be available for installation. This is an attended deployment, so you will see the new Configuration Manager user interface. It will take a few minutes for the policy to be downloaded and evaluated before the software updates will be available. Configuration Manager 2012 automatically implements a two hour randomization process for updates that are available currently, however not mandatory until sometime in the future. With that, you may not see the notifications for up to two hours. This randomization is to spread network load for compliance reporting and update installations. To force the updates to be displayed immediately for optional deployment, you must initiate a "Software Updates Deployment Evaluation Cycle". 5. Click **Software Updates Deployment Evaluation Cycle**, and then click **Run Now**. **NOTE**: The Configuration Manager client will evaluate software updates available to the client. When complete, a **Software Updates Deployment Evaluation Cycle** message box appears indicating the action was initiated, and may take several minutes to complete. 6. Click **OK**. A **Software changes are required** balloon appears, as well as a **Software changes are required by your IT department** icon in the System Tray

indicating that new software updates are available.

7. In the System Tray, click the **Software changes are required by your IT department** icon.

NOTE: A new menu appears with "View Required Software" as an option.

8. Click **View Required Software**.

NOTE: The **Software Center** dialog box appears displaying the status of software required on the computer. Notice that there are three "Required changes" pending on the client. Also notice that the actions available are to "Apply all required changes now (recommended)" or "Apply all required changes outside the configured business hours".

9. After **Required changes: 3 items**, click **View details**.

NOTE: The Software Center window appears displaying the "Installation Status" tab. Notice that the three software updates are listed as available updates. Also notice that the "Status" column indicates that the updates will install one week from today. The bottom portion of the **Software Center** displays information on the highlighted update.

10. Under **Name**, click **English Update1**, and then click **INSTALL SELECTED** to perform an installation of the update.

NOTE: The software update is installed on the client. This is a very quick installation. When complete, the Software Center window displays the current status. Notice that the status of English Update1 is now listed as "Installed".

Only install one update at this time.

11. Close **Software Center**.

NOTE: The **Software Center** dialog box appears displaying the status of software required on the computer.

12. Click **Apply all required changes now (recommended)**, and then click **OK**.

NOTE: The **Software Center** dialog box closes and balloons are displayed indicating that software is being downloaded and installed.

You have now deployed the required software updates prior to the installation deadline. You will now validate the status of the updates in the System Center 2012 R2 Configuration Manager console, as well as in reports.

5 VALIDATING CURRENT SOFTWARE UPDATE COMPLIANCE

In this exercise, you will validate that the updates have been deployed successfully. You will begin by generating reports for analysis and reporting of Microsoft update status, and then will validate using the Software Updates node of the Software Library.

Tasks	Detailed steps
Complete the following task on: **Primary1**	
1. Generate an update status report for Microsoft updates	1. In the System Center 2012 R2 Configuration Manager console window, click the **Monitoring** workspace. **Note**: The Monitoring workspace appears displaying the eight reports available in the "Software Updates - B Deployment Management" folder. 2. In the navigation pane, click **Software Updates - A Compliance**. **NOTE**: The list of reports in the "Software Updates - A Compliance" folder appears in the results pane. Notice that there are eight reports displayed. 3. In the results pane, click **Compliance 2 - Specific software update**, and then on the Ribbon, click **Run**. **NOTE**: The **Compliance 2 - Specific software update** report window appears. Notice this is a prompted report, and requires the collection ID and update to report compliance for. 4. After **Collection**, click **Values**. **NOTE**: The **Parameter Value** dialog box appears displaying the list of available collections. 5. Under **Collection**, click **Configuration Manager Clients**, and then click **OK**. **NOTE**: The **Compliance 2 - Specific software update** report window appears displaying the configured values. 6. In the **Update filter** box, type **English Update1** and then click **View Report**. **NOTE**: The **Compliance 2 - Specific software update** report window displays the status of the specific update. Notice that the information in the report includes the title, article ID, bulletin ID, vendor, and the compliance information for the update. Also notice that the software updated now indicates that it is "Installed" on at least one client (depends on how many clients you have available and how many the update was installed on). 7. Close the **Compliance 2 - Specific software** update report window. **NOTE**: The list of reports in the "Software Updates - A Compliance" folder appears in the results pane. 8. In the results pane, click **Compliance 5 - Specific computer**, and then on the Ribbon, click **Run.** **NOTE**: The **Compliance 5 - Specific computer** report window appears. Notice this is a prompted report, and requires the computer name, with vendor and update class as optional attributes. 9. After **Device Name**, click **Values**. **NOTE**: The **Parameter Value** dialog box appears displaying the available

clients in the collection.

10. Under **Device Name**, click **Client1.ConfigMgrDom**, and then click **OK**.

NOTE: The **Compliance 5 - Specific computer** report window appears. Notice this is a prompted report, and requires the computer name, with vendor and update class as optional attributes.

11. Click **View Report**.

NOTE: The **Compliance 5 - Specific computer** report window displays the list of updates and their compliance for the Configuration Manager client computer. Notice that the information in the report includes the title, update class, bulletin ID, article ID, vendor, and whether the computer is compliant with the update, any deadline for the update installation, the update ID, and an information URL. Notice also that the three software updates deployed are no longer listed as being required, but rather as approved and installed (an asterisk in the appropriate columns).

12. Close the **Compliance 5 - Specific computer** report window.

NOTE: The list of reports in the "Software Updates - A Compliance" folder appears in the results pane.

13. In the results pane, click **Compliance 3 – Update group (per update)**, and then on the Ribbon, click **Run**.

NOTE: The **Compliance 3 – Update group (per update)** report window appears. Notice this is a prompted report, and requires the software update group and collection to report on. You could not run this report earlier, as you did not have any software update groups available to report on (software update group is a required parameter for this report).

14. After **Update Group**, click **Values**.

NOTE: The **Parameter Value** dialog box appears displaying the available software update groups. In our case, the only software update group is "Lab Critical Updates".

15. Under **Update Group**, click **Lab Critical Updates**, and then click **OK**.

NOTE: The **Compliance 3 – Update group (per update)** report window appears. Notice this is a prompted report, and now requires the collection to report on.

16. After **Collection**, click **Values.**

NOTE: The **Parameter Value** dialog box appears displaying the list of available collections.

17. Under **Collection**, click **Configuration Manager Clients**, and then click **OK.**

NOTE: The **Compliance 3 – Update group (per update)** report window appears. Notice that both required parameters have now been configured.

18. Click **View Report**.

NOTE: The **Compliance 3 – Update group (per update)** report window appears. Notice the report displays information for the compliance of the software updates in the software update group, with separate rows for each update and its compliance statistics.

19. Close the **Compliance 3 – Update group (per update)** report window.

NOTE: The list of reports in the "Software Updates - A Compliance" folder appears in the results pane.

20. In the results pane, click **Compliance 1 – Overall compliance**, and then on the Ribbon, click **Run**.

NOTE: The **Compliance 1 – Overall compliance** report window appears. Notice this is a prompted report, and requires the software update group and collection to report on. You could not run this report earlier, as you did not have any software update groups available to report on (software update group is a required parameter for this report).

21. After **Update Group**, click **Values.**

NOTE: The **Parameter Value** dialog box appears displaying the available software update groups. In our case, the only software update group is "Lab Critical Updates".

22. Under **Update Group**, click **Lab Critical Updates**, and then click **OK**.

NOTE: The **Compliance 1 – Overall compliance** report window appears. Notice this is a prompted report, and now requires the collection to report on.

23. After **Collection**, click **Values.**

NOTE: The **Parameter Value** dialog box appears displaying the list of available collections.

24. Under **Collection**, click **Configuration Manager Clients**, and then click **OK**.

NOTE: The **Compliance 1 – Overall compliance** report window appears displaying the configured prompted values.

25. Click **View Report**.

NOTE: The **Compliance 1 – Overall compliance** report window appears. Notice the report displays information for the compliance of the software updates in the software update group, with separate rows for the different compliant states that are applicable for this update, such as "Compliant" and "Compliance state unknown".

If your compliance state is still "Compliance state unknown" that is because software update groups summarize compliance independently of software updates (the "Compliance 3 – Update group (per update)" report you ran earlier). If so, skip the remainder of this procedure, and return to the report after summarizing the software update group compliance later in this lab.

26. Under **State Name**, click **Compliant**.

NOTE: The **Compliance 7 – Computers in a specific compliance state for an update group (secondary)** report window appears. Notice the report displays information for information for the clients that are compliant with this software update group. Notice that the report displays the computer name, last logged on user, assigned site code, and Configuration Manager client version.

27. Close the **Compliance 7 – Computers in a specific compliance state for an update group (secondary)** report window.

NOTE: The list of reports in the "Software Updates - A Compliance" folder appears in the results pane.

You have now used Configuration Manager reports to validate that the

	software updates have successfully been installed on the client(s).

In the following procedure, you will view the updated status data for the updates directly from the Configuration Manager console.

Tasks	Detailed steps
Complete the following task on: **Primary1**	
1. View the update status data for individual updates	1. Click the **Software Library** workspace. **NOTE**: The Software Library workspace appears displaying the updates that are included in the software update group that was deployed. Notice that the compliance information displayed in the preview pane is not up to date. 2. In the navigation pane, click **All Software Updates**. **NOTE**: The list of updates appears in the results pane displaying the most recently summarized compliance data (which is summarized every hourly by default). 3. On the Ribbon, click **Run Summarization**. **NOTE**: By default, Configuration Manager only summarizes the software updates information every hour. By forcing the summarization process, you will get up to date information more quickly. A **Configuration Manager** message box appears indicating that the summarization will occur throughout the hierarchy. Wait a moment here to allow the summarization process to complete before refreshing. If you refresh and the data is not update, wait another moment and then proceed. 4. Click **OK**, wait a moment, and then refresh the **All Software Updates** node. **NOTE**: You can either refresh with the "F5" key, or the Refresh button (above the results pane with the two blue arrows). 5. In the results pane, click **English Update1**. **NOTE:** The Summary details and statistics for English Update1 appear in the preview pane. Notice that updated statistics are now available for English Update1. Also notice that the update now shows a status of "Compliant" for at least one client.
2. View update compliance for the software update group	1. In the navigation pane, click **Software Update Groups**. **NOTE**: The software update groups in the site are displayed in the results pane. Notice that you only have one software update group. Notice also that the preview pane displays the current compliance data for the software update group. If the software update group compliance is not 100% compliant for at least one client, force summarization and then refresh. 2. In the results pane, click **Lab Critical Updates**, and then on the Ribbon, click **Show Members**. **NOTE**: The software updates in the software update group are displayed in the results pane. Notice that each of the three updates is now listed as compliant. At this point, with the software update group compliance summarized, you could return to the reporting portion of the previous procedure to run "Compliance 1 - Overall compliance". The software update

	group should now report compliance.
3. View status of the software update deployment	1. Click the **Monitoring** workspace. **NOTE**: The Monitoring workspace appears displaying the reports available in the "Software Updates - A Compliance" category. 2. In the navigation pane, click **Deployments**. **NOTE**: The deployments for the site appear in the results pane. Notice that the "Lab Critical Updates" deployment appears. Notice that the "Feature Type" listed is "Software Update". 3. In the results pane, click **Lab Critical Updates**, and then on the Ribbon, click **Run Summarization**. **NOTE**: A **Configuration Manager** message box appears indicating that the summarization process will occur on all sites in the hierarchy. 4. Click **OK**. **NOTE**: The deployments for the site appear in the results pane. Notice that the "Lab Critical Updates" deployment appears with a "Compliance %" of "0.0". You will need to refresh the display to view the updated deployment status. Notice that the deployment status displays at "In Progress" for both clients. This will remain at this state until the clients next perform their "Software Updates Deployment Evaluation Cycle", which occurs on a weekly basis by default. If you want to view the updated state, initiate that action on the appropriate clients, wait for state messages to be processed, then force deployment summarization in the console. 5. On the Ribbon, click **View Status**. **NOTE**: The Deployment Status page appears in the results page. Notice that the "Compliant" tab displays 2 total assets, with the computer names in the preview pane. You have now configured your lab environment to manage software updates with Configuration Manager 2012. You have created a software update point, synchronized update metadata, scanned clients, deployed updates, and run compliance reports. You also viewed compliance of software updates on individual updates, the software update group, as well as the deployment. In the next exercise, you will experience a new feature for software update management, that being automatic deployment rules.

6 IMPLEMENTING AUTOMATIC DEPLOYMENT RULES TO DEPLOY SOFTWARE UPDATES

In this exercise, you will create an automatic deployment rule to deploy software updates automatically when the custom severity level is set to "Critical". Automatic deployment rules are new features in Configuration Manager 2012 to allow for automatic deployment of software updates when specific criteria is met.

Tasks	Detailed steps
Complete the following task on: **Primary1**	
1. Modify the custom severity of an update	1. Click the **Software Library** workspace. **NOTE**: The Software Library workspace appears displaying the updates in the "Lab Critical Updates" software update group. 2. In the navigation pane, expand **Software Updates**, and then click **All Software Updates**. **NOTE**: The list of all software updates appears in the results pane. Notice that there are 46 updates synchronized in this site. 3. In the results pane, under **Title**, click **Universal Update 1**. **NOTE**: The update summary is displayed in the preview pane. Notice that it is required by all clients that have sent in status. 4. On the **Home** tab of the Ribbon, click **Properties**. **NOTE**: The **Universal Update 1 Properties** dialog box appears displaying update details. 5. Click the **Custom Severity** tab. **NOTE**: The **Universal Update 1 Properties** dialog box appears allowing you to set the custom severity. Notice that the default custom severity is "None". 6. In the **Custom severity** box, click **Critical**, and then click **OK**. **NOTE**: The update summary is displayed in the preview pane. 7. In the preview pane, click the **Deployment** tab. **NOTE**: The deployments for the selected update are displayed in the preview pane. Notice that there are no deployments for this update. This update will be added to an existing software update group (if one exists for the automatic deployment rule) and deployment after the automatic deployment rule has been evaluated, which will occur when you force an evaluation of the automatic deployment rule that you will create next.
2. Create an automatic deployment rule	1. In the navigation pane, click **Automatic Deployment Rules**. **NOTE**: The automatic deployment rules in the site appear in the results pane. Notice that there are no automatic deployment rules created by default. 2. On the Ribbon, click **Create Automatic Deployment Rule**. **NOTE**: The **Create Automatic Deployment Rule Wizard General** dialog box appears allowing you to configure the deployment rule.

4. In the **Name** box, type **Patch Tuesday Critical Updates**
5. In the **Description** box, type **Rule to automatically deploy any updates with a custom severity level set to Critical**
6. After **Collection**, click **Browse**.

NOTE: The **Select Collection** dialog box appears allowing you to select the collection of systems to be targeted by this automatic deployment rule. Notice that the number of members in each collection is displayed.

7. Under **Name**, click **Configuration Manager Clients**, and then click **OK**.

NOTE: The **Create Automatic Deployment Rule Wizard General** dialog box appears displaying the current configuration of the deployment rule. Notice that you can select a deployment template if you have previously saved or migrated one. Software deployment templates will automatically configure most of the settings that you will manually set in this lab. The service pack 1 and R2 releases of Configuration Manager 2012 provides two templates for use, one specifically for "Patch Tuesday" deployments.

8. After **Template**, click **Manage Templates**.

NOTE: The **Select a Template** dialog box appears displaying the available templates for automatic deployment rules.

9. Under **Name**, click **Patch Tuesday**, and then click **OK**.

NOTE: The **Create Automatic Deployment Rule Wizard General** dialog box appears displaying the current configuration of the deployment rule. Notice that by default, any updates that match the automatic deployment rule will be added to a new software update group, and the deployment created will be enabled. If you want to validate the deployment before it is an active deployment, you could configure the ADR to create a disabled deployment which you could then enable as appropriate.

10. Click **Next**.

NOTE: The **Create Automatic Deployment Rule Wizard Deployment Settings** dialog box appears allowing you to configure whether or not Wake-on LAN packets are sent by this rule, the detail level for the deployment, and whether or not to deploy updates that require a EULA.

11. Click **Next** to accept the defaults of not sending Wake-on LAN packets, send success and error messages, and deploy all updates (and if an update requires accepting a EULA, accepting it automatically).

NOTE: The **Create Automatic Deployment Rule Wizard Software Updates** dialog box appears allowing you to specific the specific updates that the deployment rule will deploy. Notice that the default configuration from the deployment template is to deploy any "security updates" released in the previous "one day".

Notice that a "Preview" button is available in Configuration Manager 2012 R2. This allows you to validate the updates that will be selected when the automatic deployment rule runs.

12. Click **Preview**.

NOTE: The **Preview Updates** dialog box appears displaying updates that meet the default filter criteria. Notice that no updates meet the criteria of being released in the last day, and are security updates.

13. Click **Close**.

NOTE: The **Create Automatic Deployment Rule Wizard Software Updates** dialog box appears allowing you to specific the specific updates that the deployment rule will deploy. Notice that the default configuration from the deployment template is to deploy any “security updates” released in the previous “one day”. For the purposes of this lab, you will configure the rule to only deploy updates when the custom severity level has been set to "Critical".

14. Under **Property filters**, click to select **Custom Severity**, and then clear the selections for **Date Released or Revised** and **Update Classification**.

NOTE: The **Create Automatic Deployment Rule Wizard Software Updates** dialog box displays "Custom Severity <items to find>" under **Search criteria**.

15. After **Custom Severity**, click **<items to find>**.

NOTE: The **Search Criteria** dialog box appears displaying the appropriate values that can be selected for Custom Severity.

16. Click to select **Critical**, and then click **OK**.

NOTE: The **Create Automatic Deployment Rule Wizard Software Updates** dialog box displays "Custom Severity "Critical"" under **Search criteria**.

17. Click **Preview**.

NOTE: The **Preview Updates** dialog box appears displaying updates that meet the default filter criteria. Notice that there is now one update that meets the filter criteria.

18. Click **Close**.

NOTE: The **Create Automatic Deployment Rule Wizard Software Updates** dialog box displays "Custom Severity "Critical"" under **Search criteria**.

19. Click **Next**.

NOTE: The **Create Automatic Deployment Rule Wizard Evaluation Schedule** dialog box appears allowing you to configure when the rule will be evaluated. Notice that that the rule is set to evaluate monthly.

20. Click **Next** to accept the default values.

NOTE: The **Create Automatic Deployment Rule Wizard Deployment Schedule** dialog box appears allowing you to configure the schedule for update deployment. This includes the availability and deadline, as well as whether the time is UTC or client local time. If you wanted the updates to be required immediately, you would set the "Installation deadline" to "As soon as possible".

21. Click **Next** to accept the defaults of "Client local time", the updates are available in four hours (this is to allow download and distribution of the updates to appropriate distribution point), and there is a one week period before the deployment becomes required.

NOTE: If you want to validate the actual deployment of updates as a result of the automatic deployment rule, you would want to set the deadline to **As soon as possible**.

The **Create Automatic Deployment Rule Wizard User Experience** dialog box appears allowing you to set the notification settings, reboot suppression value, whether or not the updates will only install during any configured maintenance windows, and whether or not to commit any updates to Windows Embedded devices. Notice that the default for this automatic deployment rules is that the deployments are displayed in Software Center and there are notifications to the user.

22. Click **Next** to accept the default of displaying all notifications, using any applicable maintenance windows, not suppressing any required reboots after update deployment, and committing any changes to Windows Embedded devices.

NOTE: The **Create Automatic Deployment Rule Wizard Alerts** dialog box appears allowing you to configure alerts for compliance less than your threshold, and for integration with Microsoft Operations Manager.

23. Click **Next** to accept the defaults of creating an alert if compliance is not at least 90% one week after the deployment deadline, and to not create any alerts in Operations Manager.

NOTE: The **Create Automatic Deployment Rule Wizard Download Settings** dialog box appears allowing you to configure whether or not clients on slow network boundaries are to install updates, and whether or not to allow fall back to unprotected distribution points if necessary.

24. Click **Next** to install updates on slow boundaries, to allow the use of unprotected distribution points, to allow use of Branch Cache (if configured) to provide updates at remote locations, o download updates from Microsoft Updates if they are not available from a Configuration Manager distribution point, and not to download updates at the deadline over a metered Internet connection.

NOTE: The **Create Automatic Deployment Rule Wizard Deployment Package** dialog box appears allowing you to configure whether or not any updates to be deployed by this automatic deployment rule uses an existing deployment package or automatically creates a new deployment package.

25. Verify that **Select deployment package** is selected, and then click **Browse**.

NOTE: The **Select a Deployment Package** dialog box appears displaying the available deployment packages.

26. Under **Deployment packages**, click **Critical Updates**, and then click **OK**.

NOTE: The **Create Automatic Deployment Rule Wizard Deployment Package** dialog box appears displaying the designated deployment package for new updates.

27. Click **Next**.

NOTE: The **Create Automatic Deployment Rule Wizard Download Location** dialog box appears allowing you to configure the location to get the updates from. Notice that your options are to download from the Internet (Microsoft Update), download from content already downloaded by WSUS, or use content already downloaded. In the lab environment, there is no Internet connection, so the updates have already been downloaded to the site server's drive.

28. Click **Download software updates from a location on my network**, and then click **Browse**.

NOTE: The **Select Folder** dialog box appears.

29. Click **C:\Lab Files\WSUS Synthetic**, and then click **Select Folder**.

	NOTE: The **Create Automatic Deployment Rule Wizard Download Location** dialog box appears displaying the designated location to get the updates from. 30. Click **Next**. **NOTE**: The **Create Automatic Deployment Rule Wizard Language Selection** dialog box appears allowing you to configure the appropriate languages of the updates you want to download. Notice that this matches the language configuration of the software update point during its role configuration. 31. Click **Next**. **NOTE**: The **Create Automatic Deployment Rule Wizard Summary** dialog box appears displaying the configured values for this automatic deployment rule. Notice that the details include the target collection, deployment settings, schedule, etc. Notice also that you can save the current configuration as a deployment template from the Summary wizard page. 32. Click **Next**. **NOTE**: The **Create Automatic Deployment Rule Wizard Completion** dialog box appears indicating that the automatic deployment rule was successfully created. 33. Click **Close**. **NOTE**: The new automatic deployment rule appears in the results pane. In the next task, you will force an evaluation of the new automatic deployment rule. This will trigger the automatic deployment rule to evaluate, and create the new update group.
3. Force evaluation of the automatic deployment rule	1. In the navigation pane, expand **Software Updates**, and then click **Software Update Groups**. **NOTE**: The update groups that are available are displayed in the results pane. Notice that there is only one update group, the one you created in a previous exercise. 2. In the navigation page, click **Automatic Deployment Rules**. **NOTE**: The automatic deployment rules that are available are displayed in the results pane. Notice that there is only one automatic deployment rule, the one you created previously in this exercise. 3. In the results pane, click **Patch Tuesday Critical Updates**, and then on the Ribbon, click **Run Now**. **NOTE**: A **Configuration Manager** message box appears indicating that the automatic deployment rule will be evaluated, and appropriate software updates will be added to the designated software update group. 4. Click **OK**. **NOTE**: The automatic deployment rule evaluation process occurs. There is no visual confirmation that the process has completed. It will take a moment for the automatic deployment rule to run and create the software update group and deployment. 5. In the navigation pane, expand **Software Updates**, and then click **Software Update Groups**. **NOTE**: The software update groups that are available are displayed in the

results pane. Notice that there are now two software update groups, the one you created in a previous exercise, and one with a title of "Patch Tuesday Critical Updates" which you set in the automatic deployment rule. If the new software update group does not appear yet, wait another moment and then refresh the list of software update groups.

6. In the results pane, click **Patch Tuesday Critical Updates**, and then in the preview pane, click the **Deployment** tab.

NOTE: The deployments for the Patch Tuesday Critical Updates software update group appear in the preview pane. Notice that there is a deployment created as a result of the automatic deployment rule evaluation. Notice also that the deployment is enabled.

7. In the navigation pane, click **Deployment Packages**.

NOTE: The deployment packages in the site appear in the results pane. Notice that there is only one deployment package available, "Critical Updates". This deployment package was created earlier in this lab, and was selected as the deployment package to contain the updates matching the automatic deployment rule.

8. In the results pane, click **Critical Updates**, and then on the Ribbon, click **Show Members**.

NOTE: The updates included in the deployment package are displayed in the results pane, along with a sticky node, "Critical Updates" added under "All Software Updates". Notice that "Universal Update 1" has been added to the deployment package. This occurred when the automatic deployment rule was processed.

9. In the results pane, click **Universal Update 1**.

NOTE: The summary information for "Universal Update 1" appears in the preview pane.

10. In the preview pane, click the **Deployment** tab.

NOTE: The deployments for the update appear in the preview pane. Notice that the automatic deployment rule created a new deployment for this update (the name starts with "Patch Tuesday Critical Updates") and that it is enabled by default. Remember that the deployment schedule was set to the default, which would not automatically deploy these updates for a week.

You could then force the client to retrieve machine policies, and then install the update. However, you've already completed those processes earlier, so there is not a requirement to do so unless you have the time to complete the installation of the update.

You have now experienced the management and deployment of software updates using Configuration Manager 2012, including the new automatic deployment rule feature.