Microsoft

Managing Enterprise Devices and Apps

Exam Ref 70-696

Orin Thomas

PUBLISHED BY
Microsoft Press
A Division of Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052-6399

Library of Congress Control Number: 2014951937
ISBN: 978-0-7356-9559-7

Printed and bound in the United States of America.

First Printing

Microsoft Press books are available through booksellers and distributors worldwide. If you need support related to this book, email Microsoft Press Book Support at mspinput@microsoft.com. Please tell us what you think of this book at http://www.microsoft.com/learning/booksurvey.

Acquisitions Editor: Alison Hirsch
Developmental Editor: Alison Hirsch
Editorial Production: nSight, Inc.
Technical Reviewer: Randall Galloway; Technical Review services provided by Content Master, a member of CM Group, Ltd.
Copyeditor: Kerin Forsyth
Indexer: Lucie Haskins
Cover: Twist Creative • Seattle

Contents at a glance

This page intentionally left blank

Contents

What do you think of this book? We want to hear from you!

Microsoft is interested in hearing your feedback so we can continually improve our books and learning resources for you. To participate in a brief online survey, please visit:

www.microsoft.com/learning/booksurvey/

Introduction

The Microsoft 70-696 Managing Enterprise Devices and Apps certification exam deals with advanced topics including virtual application management, RemoteApp, third-party software updates, configuration and compliance management. Some of the exam comprises topics that even experienced Configuration Manager administrators encounter on an infrequent basis.

Candidates for this exam are Information Technology (IT) Professionals who want to validate their advanced System Center 2012 R2 and Microsoft Intune device and application management skills and knowledge. To pass this exam, candidates require strong understanding of how to configure and manage virtual, mobile, and desktop applications. They also need to know how to manage software updates, compliance settings, inventory, and endpoint protection configuration using System Center 2012 R2 Configuration Manager and Microsoft Intune. To pass, candidates require a thorough theoretical understanding as well as meaningful practical experience implementing the technologies involved.

This book covers every exam objective, but it does not cover every exam question. Only the Microsoft exam team has access to the exam questions themselves, and Microsoft regularly adds new questions to the exam, making it impossible to cover specific questions. You should consider this book a supplement to your relevant real-world experience and other study materials. If you encounter a topic in this book with which you do not feel completely comfortable, use the links in the text to find more information and take the time to research and study the topic. Great information is available on TechNet, Channel 9, product team blogs, and online forums.

Microsoft certifications

Microsoft certifications distinguish you by proving your command of a broad set of skills and experience with current Microsoft products and technologies. The exams and corresponding certifications are developed to validate your mastery of critical competencies as you design and develop—or implement and support—solutions with Microsoft products and technologies both on-premises and in the cloud. Certification brings a variety of benefits to the individual and to employers and organizations.

MORE INFO **ALL MICROSOFT CERTIFICATIONS**

For information about Microsoft certifications, including a full list of available certifications, go to *http://www.microsoft.com/learning/en/us/certification/cert-default.aspx*.

Free ebooks from Microsoft Press

From technical overviews to in-depth information on special topics, the free ebooks from Microsoft Press cover a wide range of topics. These ebooks are available in PDF, EPUB, and Mobi for Kindle formats, ready for you to download at:

http://aka.ms/mspressfree

Check back often to see what is new!

Errata, updates, & book support

We've made every effort to ensure the accuracy of this book. If you discover an error, please submit it to us via *mspinput@microsoft.com*. You can also reach the Microsoft Press Book Support team for other assistance via the same email address. Please note that product support for Microsoft software and hardware is not offered through the previous addresses. For help with Microsoft software or hardware, go to *http://support.microsoft.com*.

We want to hear from you

At Microsoft Press, your satisfaction is our top priority, and your feedback our most valuable asset. Please tell us what you think of this book at:

http://aka.ms/tellpress

The survey is short, and we read every one of your comments and ideas. Thanks in advance for your input!

Stay in touch

Let's keep the conversation going! We're on Twitter: *http://twitter.com/MicrosoftPress*.

CHAPTER 3

Plan and implement software updates

The timely and regular deployment of software updates is a task that almost all IT professionals have to manage. Microsoft provides the Windows Server Update Services (WSUS) role as a freely available add-on to enable organizations to manage the deployment of updates to computers in their environment. Although WSUS is functional, it has its limitations. That's when products such as System Center Updates Publisher and System Center 2012 R2 Configuration Manager are useful. In this chapter, you learn about deploying third-party updates by using System Center Updates Publisher, deploying updates by using Configuration Manager, and deploying and managing updates by using Microsoft Intune.

Objectives in this chapter:

- Objective 3.1: Plan and deploy third-party updates.
- Objective 3.2: Deploy software updates by using Configuration Manager and Windows Server Update Services (WSUS).
- Objective 3.3: Deploy software updates by using Microsoft Intune.

Objective 3.1: Plan and deploy third-party updates

In this section, you learn about System Center Updates Publisher and how you can use this application to publish updates from third-party vendors to a WSUS server and Configuration Manager.

This section covers the following topics:

- System Center Updates Publisher
- System Center Updates Publisher options
- Managing updates

System Center Updates Publisher

System Center Updates Publisher (SCUP) 2011 is an application you can use with Configuration Manager to manage software updates that third-party vendors and your own organization produce. By using SCUP, you can import software updates from catalogs third-party vendors publish so that these updates can be deployed through Configuration Manager. You can also use SCUP to import software updates your own organization creates. For example, if your organization has created software that is deployed to a large number of client computers, and that software requires software updates to be deployed, you can use SCUP to import those updates so that you can use Configuration Manager to deploy them.

> ***MORE INFO*** **SYSTEM CENTER UPDATES PUBLISHER**
>
> **You can learn more about System Center Updates Publisher at *http://technet.microsoft.com/en-US/library/hh134747.aspx*.**

Operating system and software requirements

You can deploy SCUP 2011 on the following operating systems:

- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2
- Windows Server 2008
- Windows 8.1
- Windows 8
- Windows 7
- Windows Vista

The dependencies for SCUP are governed by the operating system platform you use to host it. If you use Windows 8, Windows 8.1, Windows Server 2012, or Windows Server 2012 R2 clients in your environment, you must deploy SCUP on a computer running either Windows Server 2012 or Windows Server 2012 R2.

- When installing System Center Updates Publisher on Windows Server 2012 and Windows Server 2012 R2, ensure that you have installed the remote server administration tools and the WSUS role.
- When installing System Center Updates Publisher on Windows Server 2008 and Windows Server 2008 R2, you should install WSUS 3.0 SP2 and install .NET Framework 4 as well as hotfix KB2530678.

Certificate requirements

SCUP requires a signing certificate to sign updates digitally that it publishes. This digital signature enables clients to verify the integrity of the updates. You can obtain a certificate from a trusted certificate authority (CA) or have SCUP create a self-signed certificate. Certificates must be trusted by clients of the update server and by the update server itself. This requirement is not a problem if you have obtained the certificate from a CA that client computers trust but requires special configuration of clients if you use the self-signed certificate.

When you obtain a signing certificate for Updates Publisher 2011 from a CA, ensure that it has the following properties:

- Enable The Allow Private Key To Be Exported Option
- Set Key Usage To Digital Signature
- Set Minimum Key Size To A Value Equal To Or Greater Than 2048 Bit

If you use a self-signed certificate, export the self-signed certificate from the server that hosts SCUP by using the certificates snap-in of the Microsoft Management console. You then import the certificate into the Trusted Root Certification Authorities certificate store. You can do this manually on each client, or you can use Active Directory to publish the self-signed certificate to the Trusted Root Certification Authorities certificate store on computers that are members of the domain.

EXAM TIP

Remember the process for using self-signed certificates with SCUP.

MORE INFO **SCUP CERTIFICATES**

You can learn more about SCUP certificates at *http://technet.microsoft.com/en-us/library/hh134732.aspx*.

SCUP options

Depending on the details of your SCUP deployment, you can choose to publish updates to a WSUS server or to a WSUS server integrated with Configuration Manager. Update Server options, shown in Figure 3-1, enable you to configure whether Updates Publisher 2011 publishes software updates to a WSUS update server and whether the update server is local or remote and to specify the certificate that Updates Publisher 2011 uses to publish software updates. All software updates must be digitally signed when they are published. Use this option when clients update using only WSUS.

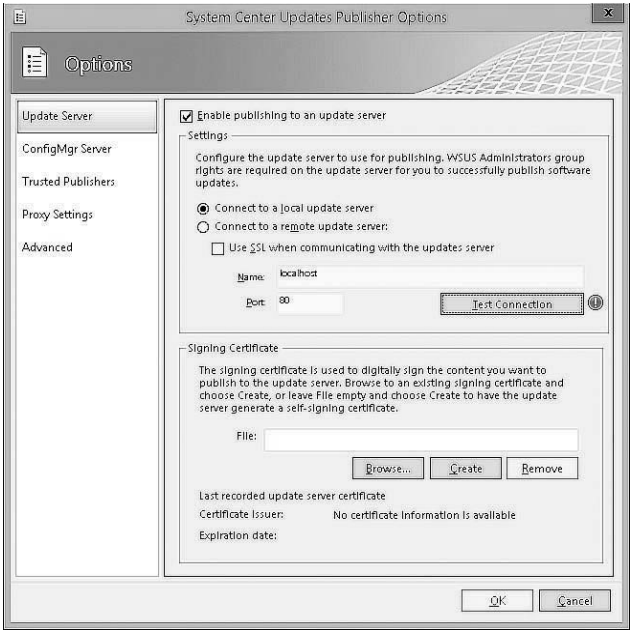

FIGURE 3-1 System Center Updates Publisher Options

ConfigMgr Server options, shown in Figure 3-2, enable you to configure how Updates Publisher 2011 interacts with System Center 2012 R2 Configuration Manager to publish software updates. You should always publish to the top-level WSUS server in your Configuration Manager environment because this ensures that all child sites have access to SCUP published updates. Use this option if Configuration Manager manages software updates in your organization's environment.

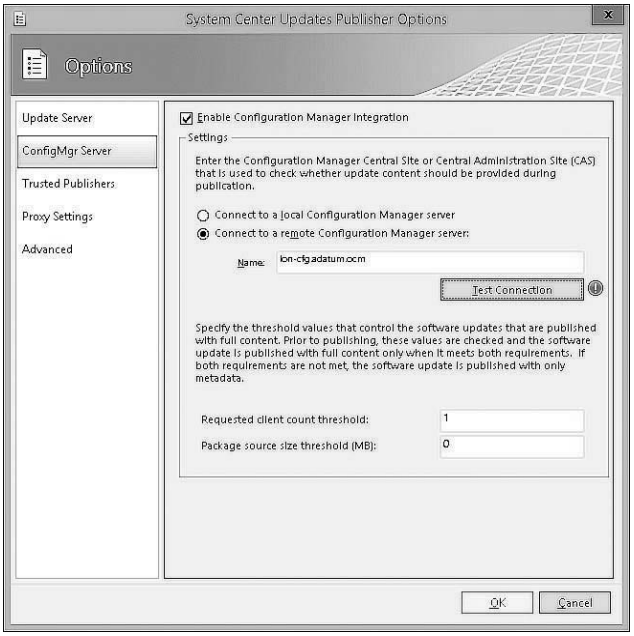

FIGURE 3-2 Configuration Manager integration

MORE INFO **INTEGRATING SCUP WITH CONFIGURATION MANAGER**

You can learn more about integrating SCUP with Configuration Manager at *http://technet.microsoft.com/en-us/library/hh134775.aspx*.

Trusted Publishers options, shown in Figure 3-3, enable you to configure which publishers SCUP trusts. This includes adding and removing trusted publishers. You can also view the certificate of trusted publishers. You automatically add a publisher to the list of trusted publishers when you import a catalog into SCUP and when you publish a software update.

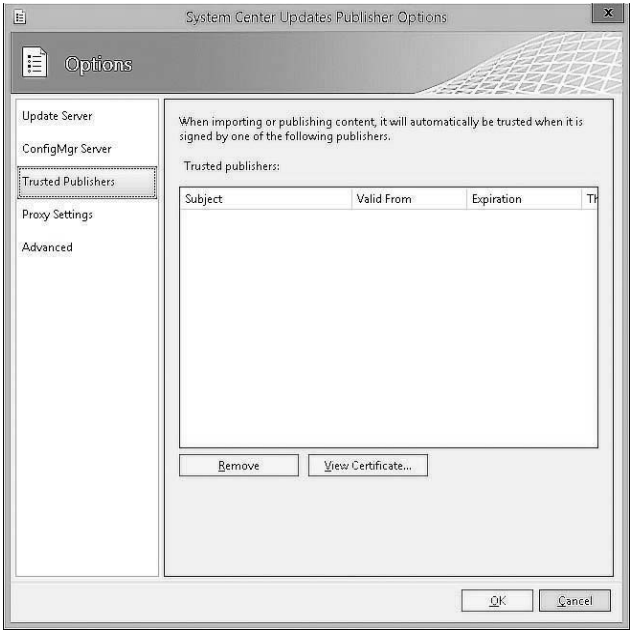

FIGURE 3-3 Trusted Publishers

Proxy Settings options, shown in Figure 3-4, enable you to configure proxy settings when you use SCUP to import software update catalogs from the Internet or when you publish software update catalogs to the Internet.

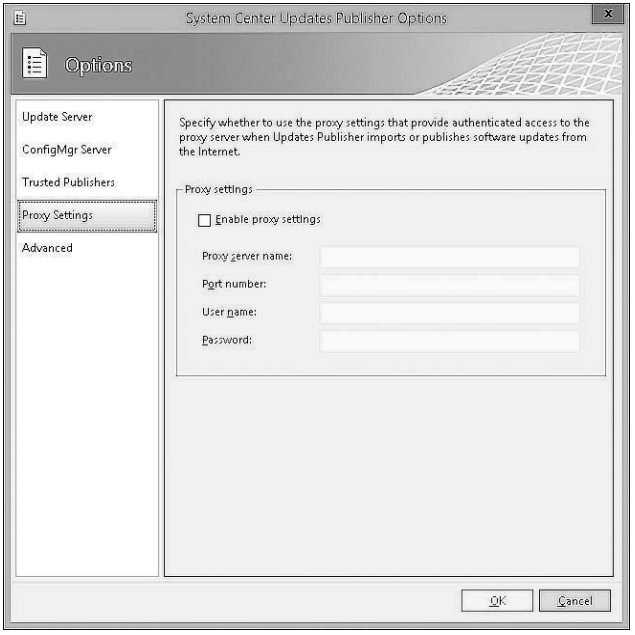

FIGURE 3-4 Proxy Settings

Advanced options, shown in Figure 3-5, enable you to configure the following:

- Add Timestamp When Signing Updates
- Check For New Catalog Alerts On Startup
- Enable Certificate Revocation Checking For Digitally Signed Catalog Files
- Local Source Publishing

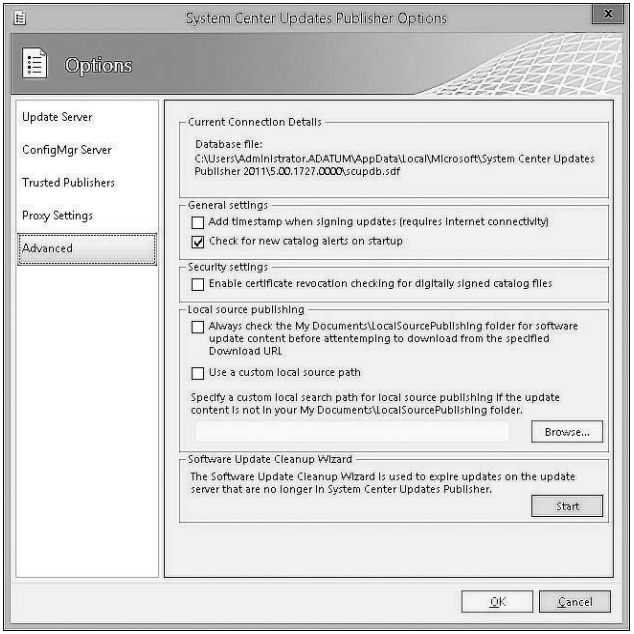

FIGURE 3-5 Advanced options

MORE INFO **SCUP OPTIONS**

You can learn more about SCUP options at *http://technet.microsoft.com/en-us/library/hh134775.aspx*.

Managing updates

After you have integrated SCUP into your organization's updates infrastructure, you need to start importing and publishing updates. You can add an update directly from a standalone update file, or you can subscribe to a vendor's catalog file. You use the four workspaces of the SCUP console to accomplish these tasks.

Updates workspace

Use the Updates workspace to create software updates and software update bundles, publish a software update, duplicate an update, delete a software update or bundle, export an update or bundle, and assign a software update or bundle to a publication. Figure 3-6 shows the Updates workspace. A bundle is a collection of updates.

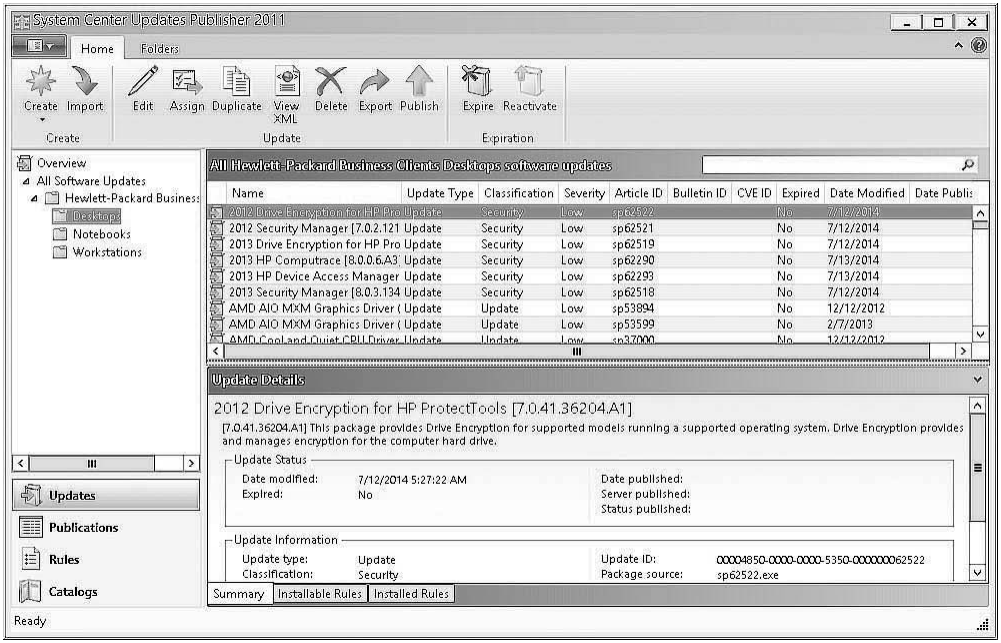

FIGURE 3-6 Updates workspace

To create a software update, perform the following steps:

1. In the Updates workspace of the System Center Updates Publisher 2011 console, click Create on the ribbon and then click Software Update.
2. In the Package Information section, provide the following information:
   - **Package Source** Provide the location to an MSI file that contains the software update package.
   - **Use A Local Source To Publish Software Update Content** Use this option to specify a local UNC or URL that hosts content.
   - **Binary Language** Use this option to specify the language of the update.
   - **Success Return Codes** This option displays any codes returned during installation that indicate that the update has installed correctly.

- **Success Pending Reboot Codes** This option displays any codes returned during installation that indicate that the update will complete installation correctly pending a reboot.
- **Command Line** Use the command line to install the update.

3. In the Required Information section, provide the following information:
   - **Language** Specify the language of the title and description.
   - **Title** Specify the name of the software update.
   - **Description** Describe the software update.
   - **Classification** Choose from among Critical Update, Feature Pack, Update, Security Update, Service Pack, Tool, Driver, and Update Rollup.
   - **Vendor** Select the vendor for the software update.
   - **Product** Specify which product is updated by the update.
   - **More Info** Specify a URL that provides more information about the update.
4. In the Optional Information section, provide the following information if necessary:
   - **Bulletin ID** If a bulletin exists to describe the update, provide the identifier here.
   - **Article ID** If an article exists to describe the update, provide the article ID here.
   - **CVE ID** Provide the CVE (Common Vulnerabilities and Exposures) ID number.
   - **Support URL** Provide a URL for more information about the update.
   - **Severity** Choose the severity of the update for security updates. Choose from among None, Critical, Important, Moderate, and Low.
   - **Impact** Specify the update impact. Choose from among Normal, Minor, and Requires Exclusive Handling. If an update requires exclusive handling, it must be installed separately from other updates.
   - **Restart Behavior** This option provides information about what happens after the update installs. Choose from among Never Reboots, Always Requires Reboot, and Can Request Reboot.
5. In the Prerequisite dialog box, provide information about any software updates that must be present on the target computer for this update to install.
6. In the Superseded Updates dialog box, provide information about any existing updates that this update supersedes.

   When you publish this update, Configuration Manager marks all software updates that you specify on this page as expired.
7. In the Installable Rules dialog box, provide information that enables the software update client to determine whether the update should be installed.

MORE INFO **UPDATES WORKSPACE**

You can learn more about the Updates workspace at *http://technet.microsoft.com/en-US/library/hh134756.aspx*.

Catalogs workspace

The Catalogs workspace enables you to add catalogs to SCUP. Catalogs are collections of updates, usually from third-party vendors. Use the Catalogs workspace to subscribe to software updates catalogs (including partner catalogs), to edit catalog subscriptions, and to import software updates from catalogs into the Updates Publisher 2011 repository. After the software updates are imported into the repository, you can publish or export them to an external catalog. Figure 3-7 shows the Catalogs workspace.

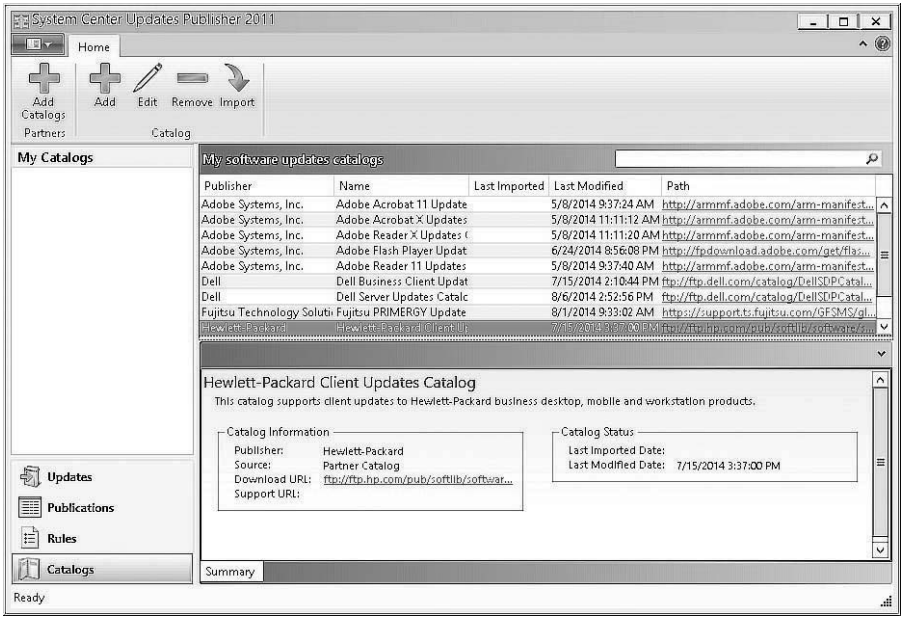

FIGURE 3-7 Catalogs workspace

EXAM TIP

Remember that you use the Catalogs workspace to subscribe to the updates catalogs that third-party vendors publish.

MORE INFO **CATALOGS WORKSPACE**

You can learn more about the Catalogs workspace at *http://technet.microsoft.com/en-US/library/hh134765.aspx*.

Publications workspace

When you publish a software update to WSUS or Configuration Manager by using SCUP, you can choose to publish all content associated with the software update or just publish metadata associated with the update. You define publications in the Updates workspace. You use the Publications workspace to publish a publication to an update server, export a publication, and remove software updates from a publication.

> ***MORE INFO*** **PUBLICATIONS WORKSPACE**
>
> **You can learn more about the Publications workspace at *http://technet.microsoft.com/en-US/library/hh134767.aspx*.**

Rules workspace

Applicability rules enable you to determine whether the computer that is the target of the update has the prerequisites for the installation update. For example, Figure 3-8 shows an applicability rule related to the Notepad.exe file.

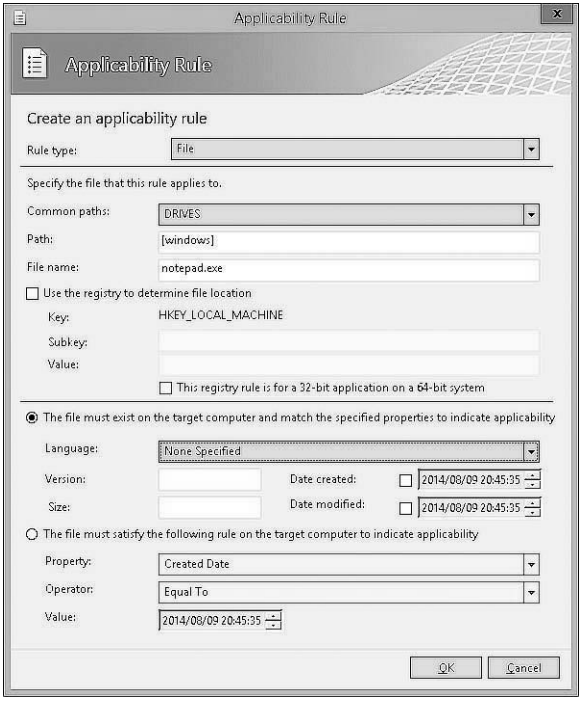

FIGURE 3-8 Applicability rule

You can use the Rules workspace to create, edit, and delete rules and rule sets. You can create two types of applicability rules:

- **Installable rules** This rule type determines whether a target computer requires a software update.
- **Installed rules** This rule type determines whether an update is already present on a computer.

MORE INFO **RULES WORKSPACE**

You can learn more about the Rules workspace at *http://technet.microsoft.com/en-US/library/hh134743.aspx*.

Thought experiment

Third-party software updates at Tailspin Toys

You are the server administrator at Tailspin Toys. Tailspin Toys uses WSUS to deploy Microsoft software updates to client computers on its internal network. All of the computers deployed at Tailspin Toys have software installed that was created by a specific third-party vendor. This third-party vendor publishes an update catalog that is compatible with System Center Updates Publisher. You have deployed SCUP on a computer running Windows Server 2012 R2. You have obtained a signing certificate from an internal CA. With this information in mind, answer the following questions:

1. **What steps can you take to minimize the complexity of obtaining and importing updates from the third-party vendor into SCUP?**
2. **Which computers in the organization need to trust the CA that issued the signing certificate installed on the SCUP server?**

Objective summary

- System Center Updates Publisher enables you to deploy third-party software updates to WSUS or Configuration Manager servers so that these updates can be deployed to clients of these servers.
- You can subscribe to update catalogs that third-party vendors publish. From these catalogs, you can import updates.
- You can publish updates or update bundles to WSUS or Configuration Manager servers.
- Rules enable you to perform checks on clients to determine update applicability.

Objective review

Answer the following questions to test your knowledge of the information in this objective. You can find the answers to these questions and explanations of why each answer choice is correct or incorrect in the "Answers" section at the end of the chapter.

1. Which type of applicability rule should you configure to determine whether an update is already present on a computer?
   - **A.** Installable rule
   - **B.** Installed rule
   - **C.** Automatic approval rule
   - **D.** Automatic deployment rule
2. Which SCUP workspace do you use to remove a software update from publication?
   - **A.** Updates workspace
   - **B.** Catalogs workspace
   - **C.** Publications workspace
   - **D.** Rules workspace
3. You are adding an update from a third-party vendor in preparation for publishing that update to your organization's Configuration Manager deployment. The update requires a computer restart to complete installation. Which of the following sections in the Optional Information window enables you to provide this information?
   - **A.** Restart Behavior
   - **B.** Impact
   - **C.** Severity
   - **D.** CVE ID

Objective 3.2: Deploy software updates by using Configuration Manager and WSUS.

Integrating Configuration Manager with WSUS provides many benefits to an administrator responsible for ensuring that computers in his or her organization remain up to date. Using Configuration Manager gives you much more control over update deployment, enabling you to specify when updates will be installed and giving you detailed information about whether Configuration Manager clients comply with previously deployed updates.

This section covers the following topics:

- Configuration Manager software update point
- Software update client settings
- Managing updates
- Monitoring and troubleshooting software updates
- Automatic deployment rules

Software updates in Configuration Manager

Configuration Manager integrates with the WSUS engine to synchronize with the Microsoft Update servers to retrieve metadata for software updates, assess which software updates are required for Configuration Manager clients, and then deploy those updates to clients. You get the following benefits by using Configuration Manager to manage software updates instead of using WSUS by itself:

- **Scan and deploy functionality** You can scan a collection of client computers for required updates, analyze results, and then deploy updates to those client computers.
- **Compliance integration** You can integrate the software updates feature with other Configuration Manager functionality, such as compliance baselines and task sequences, for operating system deployment.
- **Collection-based maintenance windows** Use this feature to ensure that Configuration Manager only applies updates during approved maintenance periods.
- **Enhanced monitoring and reporting** Compared to WSUS, Configuration Manager provides extensive monitoring capabilities, such as detailed state messages, status updates, and alerts for key software-update issues. Configuration Manager also provides an extensive number of reports to show your entire organization's deployment status and compliance statistics with respect to updates.
- **Wake on LAN and power management support** Configuration Manager includes support for technology that wakes up a computer on a local area network (Wake On LAN technology). This feature enables you to deploy software updates after business hours without requiring users to leave their computers on, which consumes power unnecessarily.
- **Support for Network Access Protection (NAP)** With the integration of NAP and the System Health Validator point site system role, you can define what software updates are required for computers to connect to and communicate with the network resources. This differs from WSUS integration with NAP, by which, rather than requiring specific updates to be deployed, you test to see whether an update check was performed recently and detected updates of a specific type have been installed.

Configuration Manager software update point

The software update point is a Configuration Manager site system role that supports software update management. It integrates WSUS with the Configuration Manager infrastructure. In multisite Configuration Manager deployments, each site usually contains a software update point. You typically configure the software update point at the hierarchy's top-level site to synchronize updates from Microsoft Update. Then, you configure the software update points in each child site to synchronize updates from the upstream update server in the parent site.

The deployment of software update points in secondary sites is optional. It is generally a good idea to deploy a software update point in a secondary site when there is limited network bandwidth between client computers and site systems in the primary site. When you configure a software update point in a secondary site, the WSUS installation is configured as a replica of the WSUS instance located in the primary site. Clients located within the secondary site boundaries are configured to communicate with the local software update point in the secondary site. In this configuration, you continue to manage all deployments from the primary site.

System Center 2012 R2 Configuration Manager supports multiple software update points in each site. When you deploy multiple software update points in a site, those software update points are automatically load balanced in the following way: Configuration Manager initially assigns a client to a software update point. The client retains that assignment unless it experiences a software-update failure such as the WSUS server being unavailable or unresponsive. The client retries to connect to the software update point a minimum of four times at 30-minute intervals. After the fourth attempt, the client waits an additional two minutes and then chooses another software update point randomly from the site, with a priority of a software update point that resides in the same forest.

If you deploy the software update point on a computer that hosts additional site system roles, you can support up to 25,000 clients. If the software update point site system role is deployed by itself, it can support up to 100,000 clients.

Deployment

When you install a software update point, you must configure it to communicate with the WSUS through the appropriate ports. By default, when you install WSUS on a computer running Windows Server 2012 or Windows Server 2012 R2, it creates a dedicated website for WSUS and configures ports 8530 for HTTP and 8531 for HTTPS.

A Configuration Manager software update point has the following prerequisites:

- **WSUS 3.0 SP2 or newer** The Software Updates feature requires WSUS 3.0 Service Pack 2 (SP2) or newer for software-updates catalog synchronization and client scanning for compliance assessments with respect to software updates. For Windows Server 2008 R2, you must download and install WSUS and related prerequisites on a system before configuring that system as a Configuration Manager site system for a software update point. From Windows Server 2012 onward, WSUS is a built-in role.

- **WSUS 3.0 SP2 or newer administration console** If WSUS is not installed on the site server, you must install the WSUS administration console on the Configuration Manager site server. This enables the site server and the WSUS server to communicate with each other.
- **Configuration Manager roles** The software update point also requires the management point and distribution point roles to be deployed.
- **Configuration Manager reporting services point** Although not a primary prerequisite, before you can use software updates reports you need to configure a reporting services point site system. However, because other Configuration Manager features require the reporting services point, you most likely have deployed it within your infrastructure already.

As you deploy and configure the software update point, ensure that the site system role is working as expected. Component Status provides status messages related to the components used during the software update configuration. In the Monitoring workspace, expand System Status and then click Component Status. The following components are related to the software update point:

- **SMS_WSUS_CONTROL_MANAGER** Displays status information related to the installation of the component on the software update point. This component also provides information about the availability of the component on the server. The related WSUSCtrl.log stores detailed information.
- **SMS_WSUS_CONFIGURATION_MANAGER** Displays status information related to the success or failure of configuration settings for the software update point. The related WCM.log stores detailed information.

Synchronizing the update point

The software update process begins when the top-level site (central administration site or standalone primary site) downloads the metadata of the software update catalog that identifies each update and the products to which it applies. Depending on synchronization settings that you configure within the Configuration Manager console, the software-updates synchronization process retrieves the metadata from an upstream software update point or from Microsoft Update. You can schedule metadata synchronization as part of the software update point properties, or you can initiate the update manually.

To synchronize the metadata of the software update catalog, follow these steps:

1. Select the software update classes and products for synchronization and then synchronize them either based on a schedule that you configure or by initiating the synchronization manually. The WSUS Synchronization Manager on the site server calls an application programming interface (API) to request the WSUS server to initiate synchronization with Microsoft Update or with an existing WSUS server that is not in the Configuration Manager hierarchy.

2. The WSUS server requests the metadata of the software update catalog from Microsoft Update, which returns it to the WSUS server. If the synchronization occurs on a configured schedule, the software update point performs a full synchronization and applies all metadata changes, such as additions, modification, or removals. If you initiate the synchronization manually, the software update point inserts only new catalog metadata into the site database. This results in faster synchronization. The WSUS server stores the metadata in the WSUS database, and the WSUS Synchronization Manager continues to poll the WSUS server until synchronization is complete.
3. When WSUS Synchronization Manager polling detects that WSUS synchronization is complete, it requests the software update metadata from the WSUS server and inserts it into the Configuration Manager site database. When synchronization is complete, the SMS_WSUS_SYNC_MANAGER component creates status message 6702. You also can verify a successful synchronization by reviewing the site server's Wsyncmgr.log for a reference to status message 6702. If synchronization fails, the WSUS Synchronization Manager schedules another attempt within 60 minutes. Status message 6703 also provides information about the failure. When the metadata synchronization process is complete, you can view the software updates from within the Configuration Manager console.

When the software update point that is located in the central administration site completes metadata synchronization, the metadata replicates to all child primary site databases by using database replication. After data replication is complete for the site databases, the child site's WSUS Synchronization Manager requests the WSUS database instance running on the child site's software update point to initiate synchronization with the upstream WSUS server in the central site. Child sites always perform a full synchronization. The WSUS Synchronization Manager in each primary site then sends a replication request to any of its respective child secondary sites that contain a software update point.

If you have a software update point that you do not configure to synchronize with an upstream server (for example, a software update point that is located in a perimeter network), you can export and import updates manually by using the WSUSutil tool. Using WSUSutil to export or import metadata requires local administrative privileges on the WSUS server. You must run the tool locally on the server. Use the following process to export and import the metadata:

1. On the export server, copy all the files and folders from WSUSInstallationDrive\WSUS \WSUSContent\ to the import server. This ensures that locally stored updates and applicable license terms are available to the import server.
2. On the export server, open a command prompt, type the following command, and then press Enter:

```
wsusutil.exe export <packagename> <logfilename>
```

3. Move the exported package to the import server, open a command prompt, type the following command, and then press Enter:

```
wsusutil.exe import <packagename> <logfilename>
```

Software Update Manager security role

To configure the site system role for the software update point, you need to be a member of the Full Administrator security role. The Software Update Manager role should be associated with administrative users who need to perform software update–related tasks. This role includes the following permissions:

- Allows you to delegate the management of software updates.
- Allows you to define and deploy software updates to clients.
- Provides permissions to create and modify software update packages, Software Update Groups, deployment templates, and provides the ability to enable software updates for NAP.

Software update client settings

In the Administration workspace, you use the Client Settings node to specify settings related to various client agent components, including the Software Updates agent. You can use the Default Client Settings object to apply configuration settings for software updates to the hierarchy's clients. You can create and configure a Custom Client Device Settings object if you have unique software updates settings that you want to apply to members of a specific collection.

The Computer Agent section of the Default Settings dialog box provides the Disable Deadline Randomization setting for controlling the deployment of software updates. This Yes or No setting determines whether updates deploy at the designated time or use a random start time of up to two hours after the scheduled beginning of the deployment.

The Software Updates section, shown in Figure 3-9, contains the following settings that configure how client computers deploy software updates:

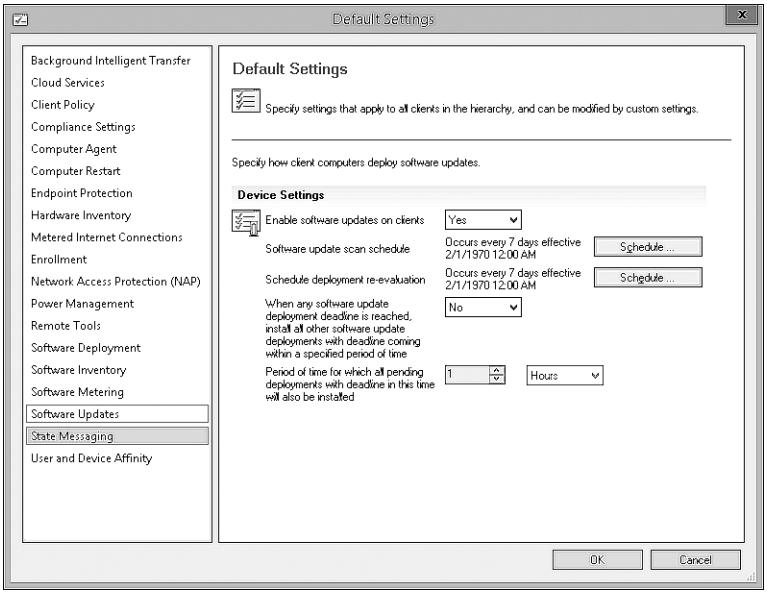

FIGURE 3-9 Software Updates

- **Enable Software Updates On Clients** Specifies whether the Software Updates agent is enabled or disabled on client computers. Setting the option to Yes enables software updates, which is the default setting. Setting the option to No disables software updates on clients.
- **Software Update Scan Schedule** Specifies how often the client computer initiates a scan for software updates compliance. By default, the software update scan occurs every seven days.
- **Schedule Deployment Re-evaluation** Configures how often the Software Updates agent reevaluates software updates for installation status. This setting is useful if a user has uninstalled a deployed update. This setting initiates reevaluation, and if an update is missing, it reinstalls that update automatically according to the reevaluation schedule that you configure. By default, deployment reevaluation is every seven days.
- **When Any Software Update Deployment Deadline Is Reached, Install All Other Software Update Deployments With Deadline Coming Within A Specified Period Of Time** Specifies whether to enforce all required software update deployments that have installation deadlines within a specific period if a single update reaches its installation deadline. Setting the option to Yes enables the setting. Setting it to No disables the setting, which is the default configuration.

- **Period Of Time For Which All Pending Deployments With Deadline In This Time Will Also Be Installed** Specifies the period for the previous setting. When you set the previous setting to Yes, you can specify a period. Required updates within the specified period deploy when another update reaches its deadline. The default setting is one hour.

Maintenance windows, shown in Figure 3-10, enable you to prevent systems from rebooting during critical times. For example, deploying updates in the middle of the workday would most likely be disruptive to your users, so you can configure a maintenance window so that update deployment would occur only after 4:00 P.M. or 5:00 P.M.

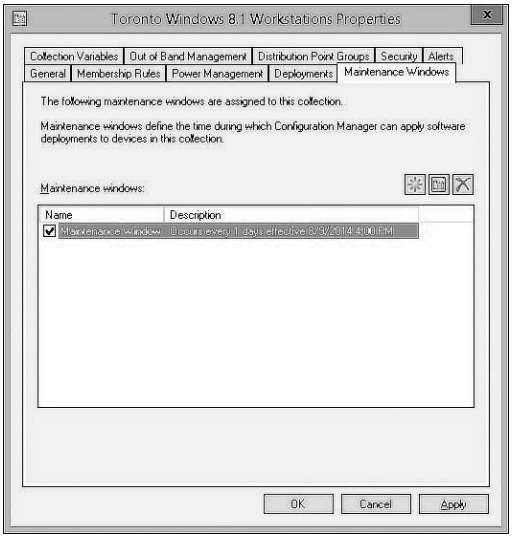

FIGURE 3-10 Maintenance Windows tab

Use maintenance windows to control when:

- Required software deployments can run.
- Software updates will deploy.
- Compliance settings deployments and evaluations can run.
- Operating system deployments can occur.
- Task sequence deployments can run.

By specifying available windows for these tasks to run, you can prevent unnecessary interruptions for users. Maintenance windows only apply to when deployments are allowed to run. You can schedule the deployments to download and run locally so that downloads can occur before the maintenance window.

You configure maintenance windows in the properties of a device collection on the Maintenance Windows tab. You can configure multiple windows on a collection, and a device can be in multiple collections that have scheduled maintenance windows. Each maintenance

window is defined by the start time, end time, and recurrence pattern. In addition, you can configure the maintenance windows to All Deployments, only Software Updates, or only Task sequences.

Any reboots caused by a deployment can occur only during a maintenance window. Therefore, you should configure your software updates maintenance windows to be long enough to deploy all the appropriate updates to prevent reboots during working hours. Each maintenance window must be configured for less than 24 hours.

When a device is affected by multiple maintenance windows, the maintenance windows are cumulative. For example, if a device is in a collection with a maintenance window from 12:00 A.M. to 3:00 A.M. and in a different collection with a maintenance window from 2:00 A.M. to 5:00 A.M., its effective maintenance window would be from 12:00 A.M. to 5:00 A.M.

Maintenance windows only affect deployments that start automatically. If a user starts a deployment from the application catalog or from the software center, the application will install, and any required reboots will occur.

Scanning for update compliance

When the initial scan begins on a client, the Software Updates agent submits a request to the management point to find the WSUS server that the scan will use. After the management point provides the WSUS server location, the agent enables the Specify Intranet Microsoft Update Service Location local Group Policy setting located at Computer Configuration \Administrative Templates\Windows Components\Windows Update and then configures the policy setting with the URL of the server that is running the software update point.

If you configure Windows Update settings in an Active Directory–based Group Policy Object (GPO), the Active Directory settings override the local Group Policy settings that the Software Updates agent configures. Be sure to remove conflicting Group Policy settings from Active Directory when integrating software updates by using Configuration Manager.

The Software Updates agent then passes a scan request to the Windows Update agent. The Windows Update agent connects to the WSUS server, retrieves the software updates metadata, and then performs a local scan on the client. The Windows Update agent sends the compliance results to the management point by using state messages. The management point forwards the results to the site server, which then inserts them in the site database.

The process to scan clients for update compliance is as follows:

1. Per the schedule that you configure, or when you initiate the scan manually, the client receives machine policy from the Management point. The machine policy configures local Group Policy settings with the name of the software update point that the Windows Update agent should use. The machine policy also provides the schedules for scanning and reevaluation.
2. The compliance scan initiates on the client. The Windows Update agent on the client connects to the WSUS server, retrieves the software update metadata, and initiates the

compliance scan. The client returns a list that reflects the compliance state for every update evaluated.

3. If configured, WSUS stores the scan results in the WSUS database. This setting is not enabled by default.
4. The client stores the compliance scan results in Windows Management Instrumentation (WMI) and then sends the results as a batch to the management point as state messages. The client then sends the state messages to the management point in bulk every 15 minutes by default.
5. The management point sends the results to the site server, which then enters them in the site database.
6. You can view the compliance scan results by using the Configuration Manager console or by using reports in categories such as the Software Updates – D Scan category and Software Updates – A Compliance category.

Compliance states

When a client computer performs a deployment evaluation for software updates, Configuration Manager creates a state message that contains the software update's compliance state for each update that it is evaluating. Configuration Manager then sends state messages to the site server through the management point, which then inserts them in the site database. A database summarization process occurs, which summarizes the results into specific compliance states. For each update, the Configuration Manager console displays the number of client computers in each compliance state.

Compliance states are as follows:

- **Required** The software update is applicable to and required on the client computer. The site server also might report this state for three scenarios:
  - If the software update is deployed but not installed
  - If the state messages have not been received on the site server
  - If the update requires a computer restart before it completes
- **Installed** The software update has installed on the computer.
- **Not Required** The software update is not applicable to the client computer.
- **Unknown** The site server has not received any information about the specific update from the client computer. The site server might report this state for three scenarios:
  - The client computer's compliance scan has not been reported.
  - The scan was not successful.
  - The scan was successful, but the state message has not been processed at the site server due to a backlog state or a corrupt state message file.

Managing updates

Managing software updates includes determining what software updates to deploy, deploying the updates to client devices, and then monitoring the results of the software updates deployment. To improve efficiency and consistency of software updates management, you can use software update groups.

Software update groups

A software update group is a logical collection of software updates that can be deployed as a single unit.

Using a software update group has many advantages, including the following:

- **Ensuring ease of management when you deploy multiple updates** You can use a software update group to organize multiple software updates into a single object that a deployment can reference for targeted collections. You can run the Download Software Updates Wizard based on a software update group and then create a deployment package. This package references specific software-update installation files and then distributes the files to distribution points. You also can use the Deploy Software Updates Wizard for a software update group to deploy the updates within that software update group to a targeted collection.
- **Providing easy tracking capabilities for the compliance status for multiple updates** A software update group includes only the software updates that you add. You can use the software update group to monitor the compliance status for target systems. In addition, when you use software update groups to create deployment packages, you can use reports such as the Compliance 1 – Overall Compliance and the Compliance 3 – Update Group (per update) to obtain status for each software update within the group.
- **Enabling the delegation of software update administration** Using a software update group enables you to delegate the administration of software updates. For each software update group, you can set one or more security scopes, which you then can reference when you add an administrative user to whom you assign the Software Update Manager security role.

To create a software update group, select one or more updates and then, on the ribbon, click Create Software Update Group. In the Create Software Update Group dialog box, you can set options for a group name and description.

You can add software updates to an existing software update group by selecting the update and then clicking the Edit Membership button on the Home tab on the ribbon. This displays a list of available software update groups that you can then select as required.

Downloading updates

Deploying software updates involves creating a deployment package, downloading the software update files, and then distributing them to distribution points. Verify that the content is available on distribution points before you deploy the software updates to clients.

You can use the Download Software Updates Wizard to create the deployment package, define the distribution points, and specify the download location of the update files. Start the wizard by selecting one or multiple software updates or a software update group and then clicking the Download button on the ribbon.

When you run the Download Software Updates Wizard, you configure the following:

- **Deployment Package** Enables you to select an existing deployment package or create a new one. The deployment package specifies its source, which is the location to which the source files download and from which the client distributes them to distribution points. You must create and share the package source folder that the deployment package uses. Each deployment package uses a specific shared folder.
- **Distribution Points** Enables you to specify the distribution points or distribution point groups that host the deployment package files. This page displays only if you are creating a new deployment package.
- **Distribution Settings** Enables you to specify several distribution options. This page displays only when you are creating a new deployment package. The options that you can specify include the following:
  - **Distribution Priority** You can specify the priority in which the client sends packages to distribution points. The client sends packages with a high priority before sending packages that you configure with a medium or low priority.
  - **Distribute The Content For This Package To Preferred Distribution Points** If you select this option, a client request causes the local distribution point to download the package if it has not downloaded already.
  - **Prestaged Distribution Point Settings** This section provides options for controlling the behavior of distribution points that you configure to support prestaged content.
- **Download Location** Specifies the location from which the software update point downloads the software update files. If you have an Internet connection, you can select Download Software Updates From The Internet. If you do not have an Internet connection, you can download the software updates manually and then store the files on an accessible network location. You can select Download Software Updates From A Location On My Network and then provide the network location of the stored files.
- **Language Selection** Specifies the languages that should be downloaded for each software update file.

Update deployment

When you deploy software updates to client computers, the software-update deployment information is added to the Configuration Manager machine policy. The client computer becomes aware of the deployment on the next machine policy retrieval and evaluation cycle. The cycle's default setting is every 60 minutes.

To deploy software updates to client computers, you first must create a deployment package. You do so by running the Deploy Software Updates Wizard, which you can invoke by selecting specific updates or by selecting a software update group and then clicking Deploy On The Ribbon.

To deploy software updates:

1. In the System Center 2012 R2 Configuration Manager console, use the Deploy Software Updates Wizard to create a new deployment package. In the wizard, you can define numerous settings, such as:
   - Software updates or software update group that the deployment includes.
   - Collection or collections that the deployment targets.
   - Deployment settings that you should use, such as whether the updates are required or available and whether to turn on the Wake On LAN functionality.
   - Deployment scheduling, which specifies when the software will be available, and the deadline for the installation.
   - User experience, such as notifications and restart behavior.
   - Alert settings.
   - Download and installation settings for slow networks.
   - Locations of the package source and distribution points.
   - Whether you want to download software updates from the Internet or from a network location.
   - Language selection for the updates.
2. The site server requests the software updates' binaries from the download location that you define in the deployment. These binaries can come from Microsoft Update or from a local source.
3. The site server copies the software update binaries to the content library on the distribution point. The site server adds the new software update deployment to the machine policy.
4. At the client policy polling interval, the client retrieves the machine policy from the management point and receives the new deployment information.
5. If the software update catalog has changed, the client scans for each software update to verify that it is still required. If you configure the software-update deployment type as Required, the client requests the binaries from the distribution point for each

required update and then stores them in the local cache. If you configure the deployment type as Available, the updates download when the user invokes the installation.

6. The client sends a state message to the management point that reports that the software update was downloaded. The management point forwards the state message to the site server, which then enters the message into the database.
7. When the installation deadline for the software update arrives or you initiate the update installation manually, the client scans for each software update to verify that it still is required. The client then installs the software update, performs another scan on the client to verify that the update is no longer required, and then sends a state message to the management point that indicates the update has been installed. If a restart is necessary, the state message indicates that the client computer is pending a restart. After the restart, a scan begins to verify that the software update is complete and no longer required and creates a state message to indicate that the update has installed. For each software update that fails to install, an error-status message is sent to the management point, which forwards the messages to the site server. The site server then inserts status messages into the database.

Client computers initiate a deployment reevaluation cycle every seven days by default. During this evaluation cycle, the client computer scans for previously deployed and installed software updates. If any are missing, the software updates are reinstalled on the client.

Monitoring and troubleshooting software updates

You can use several methods to monitor and troubleshoot the client compliance and deployment of software updates, including the All Software Updates results pane, alerts, status messages, reports, WSUS logs, server-side logs, and client logs.

Monitoring software update processes

You need to monitor three basic activities when using Configuration Manager to manage software updates. These are synchronization, distribution, and client deployment.

To verify that the software update point has the most recent list of available updates, it needs to be able to perform synchronization successfully. You can use the following methods to monitor software update point synchronization:

- **Software Update Point Synchronization Status** Located in the Monitoring workspace, the Software Update Point Synchronization Status node provides detailed information related to the synchronization status for all software update points in the hierarchy. Details include the synchronization source, last synchronization date and time, synchronization status, and error codes for failures.
- **Alerts** When you configure the synchronization schedule for the software update point, you can configure an alert to generate if synchronization fails on any site in the hierarchy. You also can modify this setting from the Sync Schedule tab of the Software

Update Component Properties dialog box. You can view alerts from the Alerts node in the Monitoring workspace.

- **SMS_WSUS_SYNC_MANAGER** This method displays status information related to both WSUS synchronization and site database synchronization with WSUS. The wsyncmgr.log stores detailed information and is located in either the INSTALL_PATH \Logs folder or the SMS_CCM\Logs folder, if the system is a management point.

You can use one of the following methods to ensure that update content distributes successfully to distribution points:

- **Content Status** In the Monitoring workspace, under the Distribution Status node, you can click Content Status. When you click this node, the results pane displays a list of all content that has been distributed. You can right-click a specific content type, such as a software update package, and then click View Status to display status and progress information related to content distribution to distribution points.
- **Package Transfer Manager** The Package Transfer Manager component (SMS_PACKAGE_TRANSFER_MANAGER) provides status information related to content transfers to distribution points. You can find the related PkgXferMgr.log on the site server in the <*Configuration Manager Installation Path*>\Logs folder. This log file provides verbose installation and configuration information related to content distribution to remote distribution points.

After update content has been transmitted to distribution points, you can use the following elements to monitor the deployment of that content to Configuration Manager clients:

- **Deployment Status** When you click the Deployments node, the results pane shows a list of all current deployments, including deployments related to the software update feature. You can right-click a specific deployment and then click View Status to display status information related to a specific software update deployment.
- **Alerts** When you create a deployment, you can enable alerts based on specified criteria. For example, you might want an alert to be generated if client compliance for the deployment is below a specific percentage. You view generated alerts from the Alerts node in the Monitoring workspace.

Software Updates reports

The Reporting node in the Monitoring workspace contains reports that are organized within specific categories as shown in Figure 3-11. You can use reports to provide information to anyone who has permission to access the reporting feature.

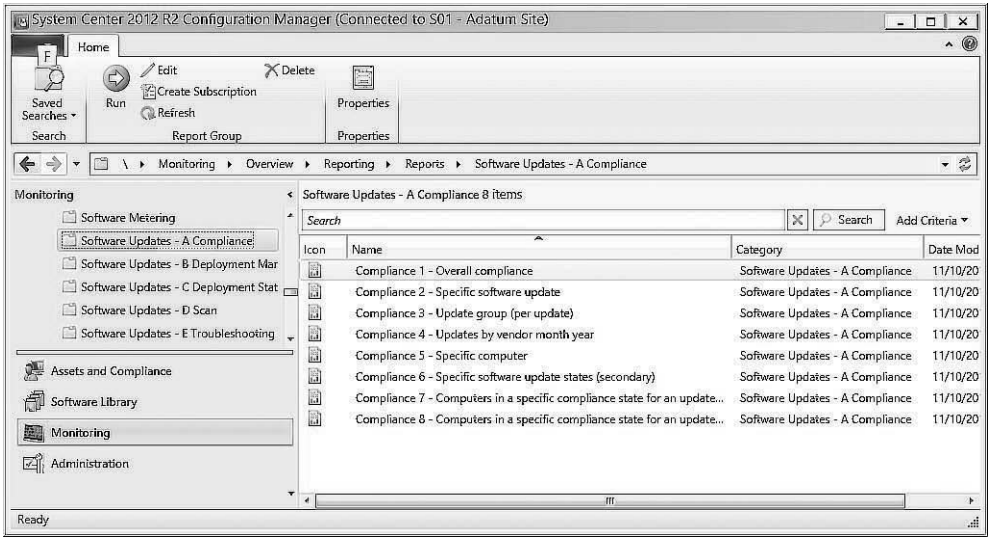

FIGURE 3-11 Software Updates reports

These reports are grouped as follows:

- **Software Updates – A Compliance** Contains reports related to compliance based on specific software updates, software update groups, or computers. Reports include:
  - Compliance 1 - Overall Compliance.
  - Compliance 2 - Specific Software Update.
  - Compliance 3 - Update Group (Per Update).
  - Compliance 4 - Updates By Vendor Month Year.
  - Compliance 5 - Specific Computer.
  - Compliance 6 - Specific Software Update Status (Secondary).
  - Compliance 7 - Computers In A Specific Compliance State For An Update Group (Secondary).
  - Compliance 8 - Computers In A Specific Compliance State For An Update (Secondary).
- **Software Updates – B Deployment Management** Contains reports that provide information related to deployments and the updates contained within specific deployments. Reports include:
  - Management 1 - Deployments Of An Update Group.
  - Management 2 - Updates Required But Not Deployed.

- Management 3 - Updates In A Deployment.
- Management 4 - Deployments That Target A Collection.
- Management 5 - Deployments That Target A Computer.
- Management 6 - Deployments That Contain A Specific Update.
- Management 7 - Updates In A Deployment Missing Content.
- Management 8 - Computers Missing Content (Secondary).

- **Software Updates – C Deployment States** Contains reports that illustrate the enforcement and evaluation states of a computer or specific deployment. Reports include:
  - States 1 - Enforcement States For A Deployment.
  - States 2 - Evaluation States For A Deployment.
  - States 3 - States For A Deployment And Computer.
  - States 4 - Computers In A Specific State For Deployment (Secondary).
  - States 5 - States For An Update In A Deployment (Secondary).
  - States 6 - Computers In A Specific Enforcement State For An Update (Secondary).
- **Software Updates – D Scan** Contains reports that display the last scan states by collection and by site. Reports include:
  - Scan 1 - Last Scan States By Collection.
  - Scan 2 - Last Scan States By Site.
  - Scan 3 - Clients Of A Collection Reporting A Specific State (Secondary).
  - Scan 4 - Clients Of A Site Reporting A Specific State (Secondary).
- **Software Updates – E Troubleshooting** Contains reports that display information related to scan and deployment errors. Reports include:
  - Troubleshooting 1 - Scan Errors.
  - Troubleshooting 2 - Deployment Errors.
  - Troubleshooting 3 - Computers Failing With A Specific Scan Error (Secondary).
  - Troubleshooting 4 - Computers Failing With A Specific Deployment Error (Secondary).

Update-related log files

Configuration Manager log files provide detailed information about software-updates components. You can use log files to help verify functionality or troubleshoot issues.

SITE SERVER LOG FILES

You can find the Site Server log files in the following folders on the site server, in the *<InstallationPath>*\Logs folder. These log files include:

- **PatchDownloader.log** Located on the Configuration Manager console computer that you use to run the wizard to download the update, this log file provides information about downloading software updates, from the update source that you specify in the software updates metadata to the designated download destination.
- **WCM.log** Located on the site server, this log file provides information about the software update-point configuration and about connecting to the WSUS server for subscribed update categories, classifications, and languages.
- **wsyncmgr.log** Located on the site server, this log file provides information about the software-updates synchronization process.

SOFTWARE UPDATE POINT LOG FILES

Software update point log files are located on the software update point (WSUS server) in both the %ProgramFiles%\Update Services\Logfiles folder and the C:\Program Files\Microsoft Configuration Manager\Logs folder. These log files include:

- **WSUSCtrl.log** This log file provides information about the configuration, database connectivity, and health of the site's WSUS server.
- **SoftwareDistribution.log** This log file provides information about the software updates that synchronize from the configured update source to the WSUS server database.

CLIENT COMPUTER SOFTWARE UPDATE LOG FILES

In some cases, you'll need to investigate a client computer to determine why software updates are not being applied. Log files are located on the client computer, in both the %windir%\CCM\Logs and the %ProgramFiles%\SMS_CCM\Logs folders (for management points). These logs include:

- **ScanAgent.log** This log file provides information about the scan requests for software updates, what tool is requested for the scan, and the WSUS location.
- **WUAHandler.log** This log file provides information about when the Windows Update agent searches for software updates.
- **WindowsUpdate.log** Found on the client in the %windir% folder, this log file provides information about when the Windows Update agent connects to the WSUS server and retrieves the software updates for compliance assessment and whether there are updates to the agent components.
- **UpdatesHandler.log** This log file provides information about software update compliance scanning and the download and installation of software updates on the client.
- **UpdatesStore.log** This log file provides information about the compliance status for the software updates that the compliance scan cycle assesses.

- **UpdatesDeployment.log** This log file provides information about the deployment on the client, including software update activation, evaluation, and enforcement. Verbose logging shows additional information about the interaction with the client user interface.

Automatic deployment rules

Automatic deployment rules help you automate the deployment of specific update types, depending on the criteria that you configure. You can use an automatic deployment rule to automate:

- Selection of software updates per criteria that you specify.
- Creation of a software update group that contains the selected updates.
- Download and distribution of software-update content to distribution points.
- Deployment of updates to client computers.

Automatic deployment rules are beneficial for managing routine updates, such as monthly deployments of software updates and definition updates for antimalware solutions such as System Center 2012 R2 Endpoint Protection (Endpoint Protection).

An automatic deployment rule relies on property filters and search criteria that you configure to specify the updates that become part of an associated software update group. For example, you might want to automate creation of a software update group that contains any definition updates released within the past week. To meet this requirement, you configure a rule based on the Date Revised and Update Classification property filters. The Date Revised filter would contain a criterion that selects updates released within the past week, and you would configure the Update Classification filter to select Definition Updates.

After the rule runs, you have the option to:

- Enable download and deployment of the updates within a software update group.
- Use the rule to automate membership creation or updating for a software update group and create the deployment object. This enables you to verify the list of the group's software updates and then enable the update group's deployment manually as needed.

You use the Create Automatic Deployment Rule Wizard to specify settings that relate to the automatic deployment rule. To start the wizard, use the following procedure:

1. From the Software Library workspace, expand the Software Updates node.
2. Select Automatic Deployment Rules.
3. On the ribbon, click Create Automatic Deployment Rule.

On the pages of the Create Automatic Deployment Rule Wizard, described in Table 3-1, provide the following settings:

TABLE 3-1 Automatic Deployment Rule Wizard pages and settings

Page	Description
General	Enables you to configure general information for the automatic deployment rule, including the following: ■ **Name** Use to provide the name associated with the automatic deployment rule. ■ **Description** Use to provide additional information about the rule. ■ **Template** Select a previously saved deployment template or use the built-in Definition Updates or Patch Tuesday templates. Create a deployment template to save the current configuration settings for the deployment during the wizard's last step. ■ **Collection** Specify the collection that the software update deployment is targeting. ■ **Software Update Group** Add software updates to an existing software update group or ensure creation of a new software update group each time the rule runs. ■ **Enable The Deployment After This Rule Runs** Specify whether the updates deploy to clients immediately after rule evaluation. If you do not select this option, you need to enable the deployment of the software update group manually.
Deployment Settings	Enables you to configure specific deployment settings, such as: ■ **Use Wake On LAN To Wake Up Clients For Required Deployments** Select this check box to enable Wake On LAN functionality. ■ **Detail Level** Specify the amount of information the client returns. Options include All Messages, Only Success And Error Messages, and Only Error Messages. ■ **License Agreement** Choose automatic deployment of software updates that do not include a license agreement or choose deployment of software updates regardless of whether they have a license agreement.
Software Updates	Enables you to select the property filters and specify the respective search criteria you use to add software updates to the associated software update group.
Evaluation Schedule	Enables you to specify a schedule for running a rule. By default, the evaluation schedule is set to run after any software update-point synchronization. If you choose to run the rule on a specific schedule, you should ensure that the evaluation schedule does not exceed the frequency of the synchronization schedule for the software update point.

Page	Description
Deployment Schedule	Enables you to configure deployment schedule settings, including: ■ Whether the schedule is evaluated by using the client's local time or Coordinated Universal Time. The latter ensures that deployment occurs at the same time for all clients, regardless of their time zone location. ■ Software available time. The Software Available Time section enables you to schedule when the deployment will become available to clients. ■ An installation deadline. When a scheduled deadline is reached, the software updates in the associated software update group install on the client computers, and the computers restart if necessary and allowed.
User Experience	Enables you to specify various options for the user experience. Three sections outline the user experience: ■ **User Visual Experience** Use one of three options for user notifications selection: Display In Software Center And Show All Notifications; Display In Software Center, And Only Show Notification For Computer Restarts; and Hide In Software Center And All Notifications. ■ **Deadline Behavior** Specify activities that can take place outside a configured maintenance window. The options include Software Installation and System Restart. ■ **Device Restart Behavior** Specify whether to suppress a restart for servers, workstations, or both.
Alerts	Enables you to specify criteria for generating a Configuration Manager alert. You also can specify alert behavior in relation to Operations Manager. For example, to minimize false alerts, you might choose to disable Operations Manager alerts whenever software updates install on a computer.
Download Settings	On the Download Settings page, you can: ■ Specify how software updates run when connected to a slow or unreliable network boundary. By design, when a client connects to a fast network boundary, the client downloads content from the distribution point and then installs the software updates locally. By default, when a client connects to a slow network boundary, the client does not install software updates. ■ Configure the deployment so that clients can download updates from an unprotected distribution point if they are not available on a protected distribution point. ■ Enable peer-to-peer content distribution, which uses BranchCache functionality. ■ Configure clients to download the content directly from Microsoft Updates if it is not available on a distribution point. ■ Configure clients on a metered connection to download the content after the installation deadline.
Deployment Package	Enables you to select an existing deployment package or create a new deployment package so that updates deploy from an automatic deployment rule. The deployment package specifies the package source for the deployment. You must create and share the package source folder that the deployment package uses. Each deployment package uses its own shared folder.

Page	Description
Distribution Points	Enables you to specify the distribution points or distribution-point groups that host the package files for deployment. This page is visible only if you are creating a new deployment package.
Download Location	Enables you to specify the location from which you download the software update files. If you have an Internet connection from the software update point, you can select Download Software Updates From The Internet. If you do not have an Internet connection from the software update point, you can download the software updates manually from a different computer and then store the files on an accessible network location.
Language Selection	Specifies the languages that you should download for each software update file.
Summary	The summary page enables you to verify the Automatic Deployment Rule Wizard settings. You also can click the Save As Template button to save the settings that you want to use for subsequent deployments. When you click the Save As Template button, you can select the specific settings that you want to include in the saved template.

MORE INFO **AUTOMATIC DEPLOYMENT RULES**

You can learn more about automatic deployment rules at *http://technet.microsoft.com/en-us/library/gg682168.aspx#BKMK_DeploymentWorkflows*.

Thought experiment

Deploying a Configuration Manager software update point at Fabrikam

You are the server administrator at Fabrikam. You are planning the deployment of Configuration Manager, which you will initially use to manage software updates. You have deployed WSUS 4.0 on a computer running Windows Server 2012 R2. This computer will host only the WSUS role and no Configuration Manager site system roles. With this information in mind, answer the following questions:

1. **What software element must you deploy on the site server if it is to host the software update point role?**
2. **Which other Configuration Manager roles must be present in the Configuration Manager site to support the software update point?**

Objective summary

- The Configuration Manager software update point integrates with WSUS to allow software updates to be deployed to Configuration Manager clients.
- The Configuration Manager software update point integrates with WSUS 3.0 SP2 or newer.
- The software-updates synchronization process retrieves the metadata from an upstream software update point or from Microsoft Update.

- You configure Client Settings to specify the software update configuration settings for Configuration Manager clients.
- Scanning for compliance enables you to determine whether Configuration Manager clients are missing updates.
- A software update group is a collection of software updates.
- Deploying software updates involves creating a deployment package, downloading the software update files, and then distributing them to distribution points.
- You can use several methods to monitor and troubleshoot the client compliance and deployment of software updates, including the All Software Updates results pane, alerts, status messages, reports, WSUS logs, server-side logs, and client logs.

Objective review

Answer the following questions to test your knowledge of the information in this objective. You can find the answers to these questions and explanations of why each answer choice is correct or incorrect in the "Answers" section at the end of the chapter.

1. You are configuring the connection between the Configuration Manager software update point and a separate WSUS server hosted on a computer running the Windows Server 2012 R2 operating system. This WSUS server is configured using default ports and is configured to accept only secure (HTTPS) traffic. Which port will the Configuration Manager software update point need to use for a connection?
   - **A.** 8530
   - **B.** 8531
   - **C.** 80
   - **D.** 443
2. Which of the following log files would you examine to review information about synchronization between the software update point and a WSUS server?
   - **A.** Wsyncmgr.log
   - **B.** WSUSCtrl.log
   - **C.** SoftwareDistribution.log
   - **D.** ScanAgent.log
3. Which of the following compliance states indicates that an update should be deployed to a client computer?
   - **A.** Unknown
   - **B.** Installed
   - **C.** Not Required
   - **D.** Required

Objective 3.3: Deploy software updates by using Microsoft Intune

Microsoft Intune provides you with an alternative method of managing software updates for computers that are outside the perimeter network or in remote branch offices where deploying a WSUS server or Configuration Manager is impractical. In this section, you learn how you can manage software updates with Intune.

This section covers the following topics:

- Microsoft Intune update policies
- Update categories and classifications
- Approving updates
- Automatic approval rules
- Third-party updates

Microsoft Intune update policies

Intune can provide software updates to clients on which the Intune agent is installed. When you install the Intune agent on a computer, the computer retrieves updates from Intune. You should ensure that any Group Policy settings configuring an update server are removed prior to deploying the Intune agent because the settings might interfere with the computer retrieving updates.

How Intune clients retrieve updates is determined by Intune policies, which include settings related to endpoint protection, network bandwidth, user device linking, and updates. The updates settings enable you to configure settings around the installation of software updates and applications.

To create an update policy, perform the following steps:

1. In the Intune Administrator console, click Policy, click Overview, and then click Add Policy under Tasks.
2. In the Create A New Policy dialog box, click Windows Intune Agent Settings, select Create And Deploy A Custom Policy, as shown in Figure 3-12, and then click the Create Policy button.

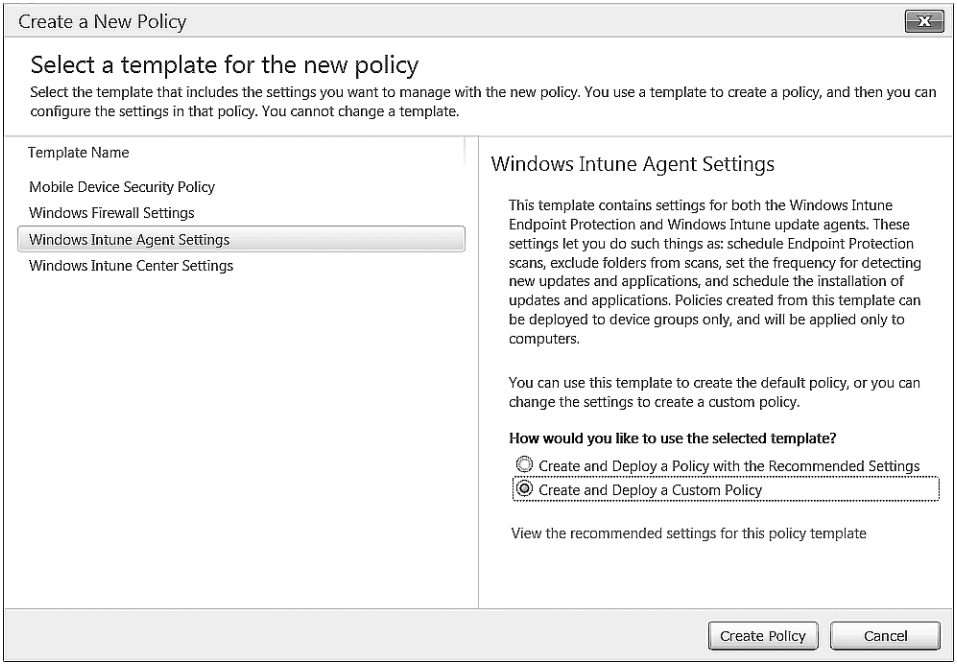

FIGURE 3-12 Creating a policy

3. In the Updates section, shown in Figure 3-13, configure the following settings:
   - **Name** Type a name for the policy on the General page.
   - **Update And Application Detection Frequency (Hours)** Indicate how often you want the client to check for updates.
   - **Automated Or Prompted Installation Of Updates And Applications** Configure whether updates and applications are installed automatically according to a schedule, or the user is prompted for the installation of updates and applications.
   - **Allow Immediate Installation Of Updates That Do Not Interrupt Windows** Specify whether updates that do not require a restart will be installed immediately.
   - **Delay To Restart Windows After Installation Of Scheduled Updates And Applications (Minutes)** Specify how long the computer will wait.
   - **Allow Logged On User To Control Windows Restart After Installation Of Scheduled Updates And Applications** This option allows a signed-on user to control whether a computer restarts after the installation of applications and updates.
   - **Prompt User To Restart Windows During Windows Intune Client Agent Mandatory Updates** Determines whether the user is prompted after the installation of a mandatory update that requires a restart.

- **Windows Intune Client Agent Mandatory Updates Installation Schedule** Specify when mandatory updates will be installed.
- **Delay Between Prompts To Restart Windows After Installation Of Scheduled Updates And Applications (Minutes)** Specify the period between restart prompts.

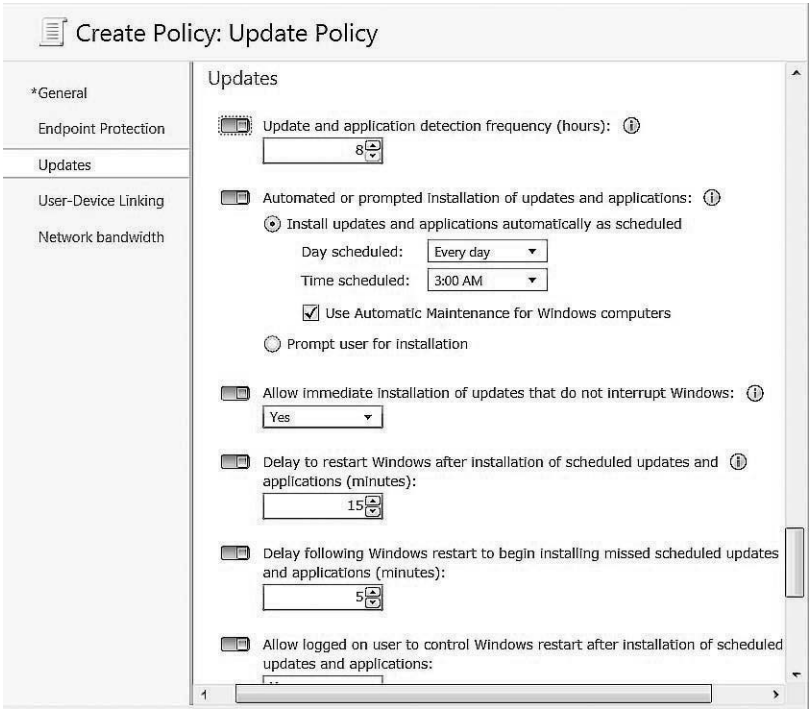

FIGURE 3-13 Updating a policy

4. Click Save Policy to save the policy.
5. In the Do You Want To Deploy This Policy Now pop-up box, click Yes.
6. In the Manage Deployment dialog box, shown in Figure 3-14, select the computers to which you want to deploy the policy and then click OK.

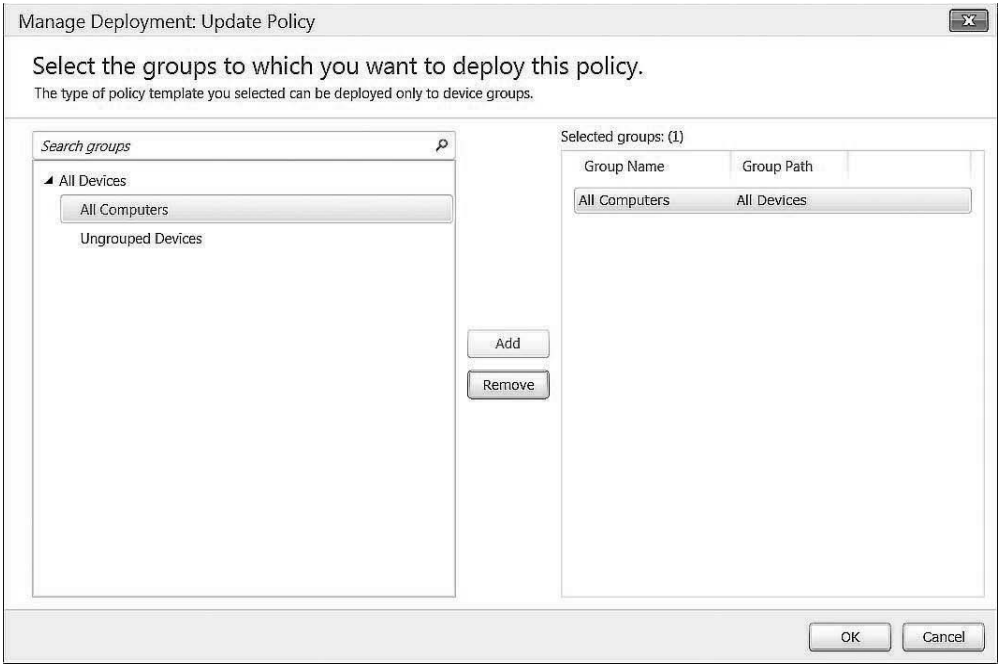

FIGURE 3-14 Selecting groups

Updating categories and classifications

Update categories and classifications to configure the products and update classifications for which Intune will manage updates. Although you can configure Intune to manage updates for almost every currently supported Microsoft product, you should only configure Intune so that it manages updates for products that are actually installed on computers that have the Intune agent. Figure 3-15 shows that Intune can manage the following update classifications:

- Critical Updates
- Security Updates
- Definition Updates
- Service Packs
- Update Rollups

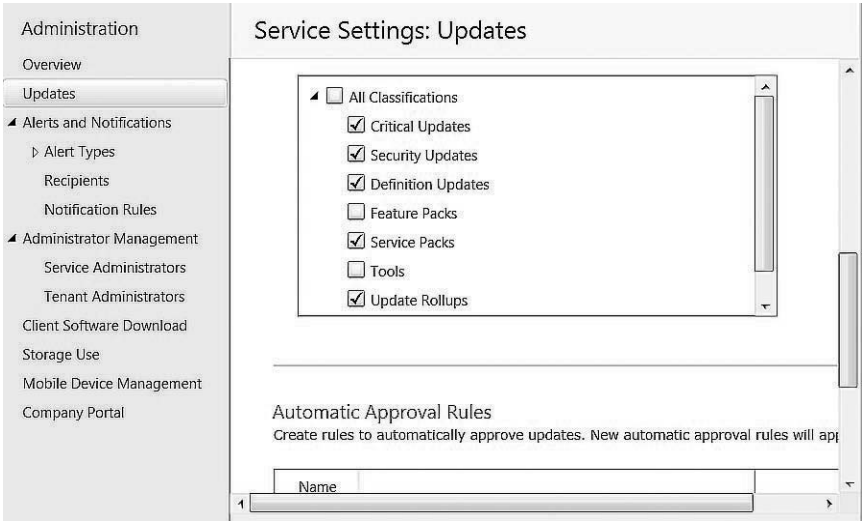

FIGURE 3-15 Service Settings: Updates

Approving updates

To deploy updates to Intune clients, approve them in the Intune Administration console. To approve an update, perform the following steps:

1. In the Intune Administration console, click Updates.
2. In the All Updates node, shown in Figure 3-16, select the update that you want to approve and click Approve.

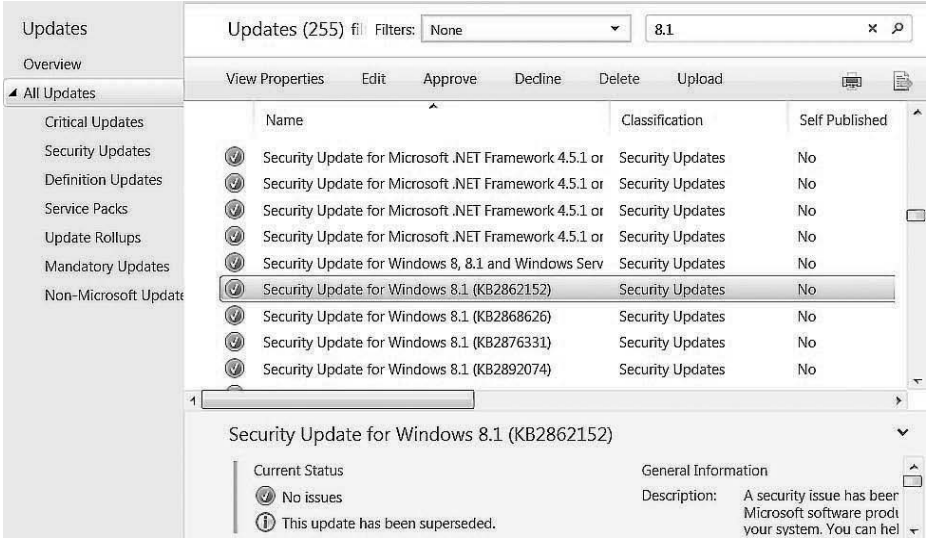

FIGURE 3-16 All Updates

3. On the Select Groups page, shown in Figure 3-17, select the groups to which you want to deploy the update and click Add. Then click Next.

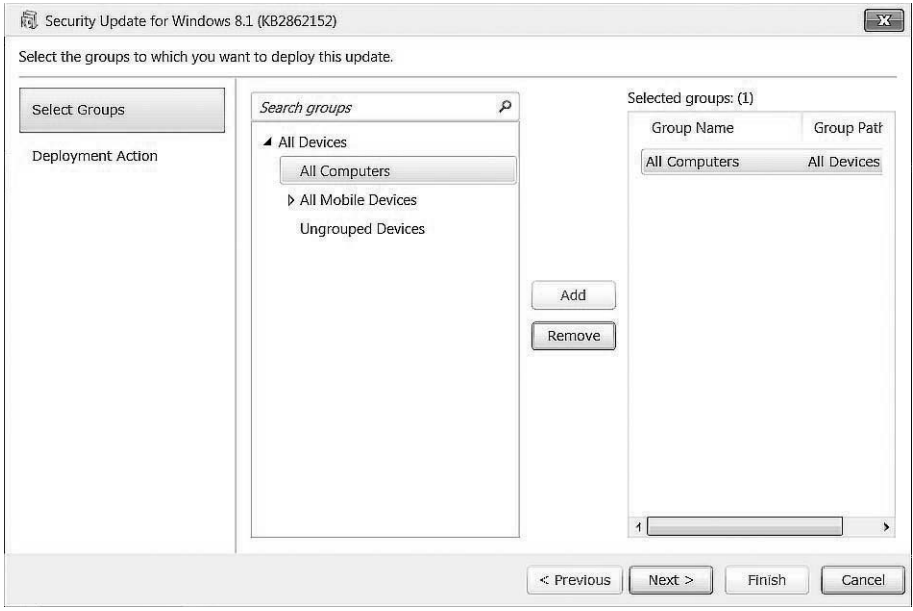

FIGURE 3-17 Select Groups

4. On the Deployment Action page, shown in Figure 3-18, select the approval status for the update. You can choose from among Required Install, Do Not Install, Available Install, and Uninstall. Then click Finish.

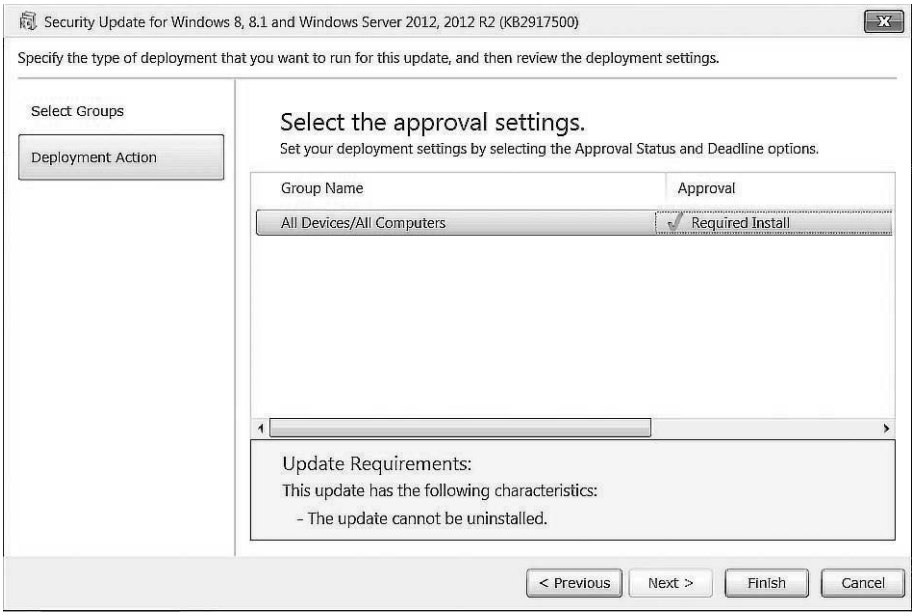

FIGURE 3-18 Deployment Action

Automatic approval rules

Automatic approval rules enable you to configure Intune to approve updates automatically, based on product category and update classification. When you configure an automatic approval rule, the update will be deployed automatically rather than requiring an administrator to perform manual approval. For example, you might configure an automatic approval rule for Windows 8.1 operating system updates that are classified as critical or security. Any Windows 8.1 operating system update that Microsoft publishes that has the critical or security classification will automatically be published to Intune clients.

EXAM TIP

Remember that approval rules will work only if Intune manages the products and classifications that are the subject of the rule. There's no point creating an approval rule for Windows 8.1 updates if Intune isn't configured to manage updates for Windows 8.1.

To create an automatic approval rule, perform the following steps:

1. In the Administration workspace of the Intune Administration console, click Updates and then scroll to Automatic Approval Rules. Click the New button.
2. On the General page of the Create Automatic Approval Rule Wizard, create a name and provide a description for the rule. Then click Next.

3. On the Product Categories page, select the products to which the automatic approval rule applies. Then click Next.

   Figure 3-19 shows Windows 8.1 selected.

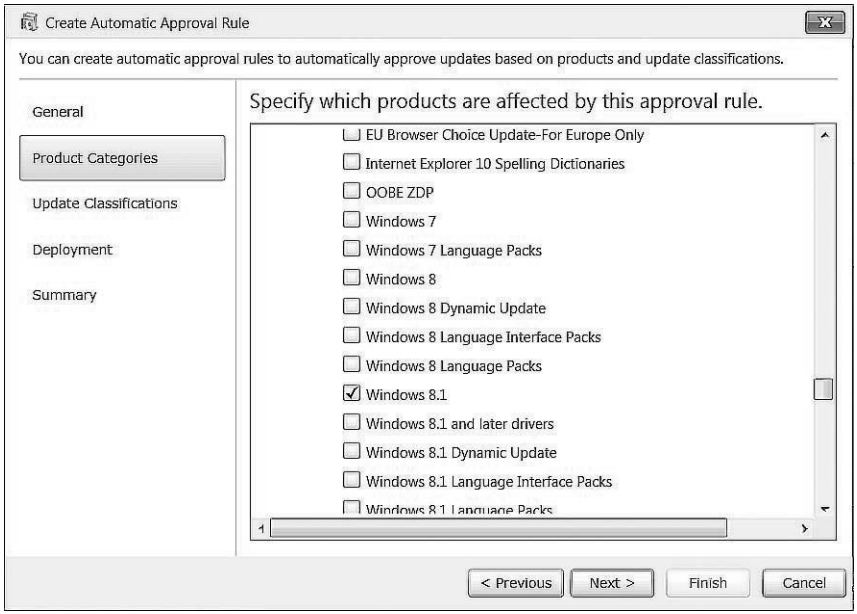

FIGURE 3-19 Product Categories

4. On the Update Classifications page, select the update classifications for which the rule will perform an automatic approval. Then click Next. Figure 3-20 shows Critical Updates and Security Updates selected.

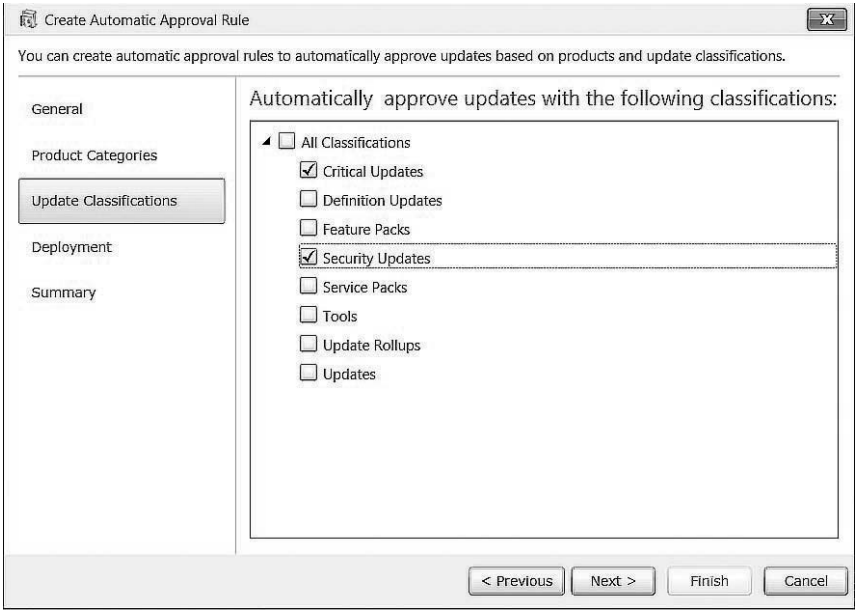

FIGURE 3-20 Update Classifications

5. On the Deployment page, select the Intune groups for which the automatic approval rule will approve the update. You can also configure an installation deadline for updates approved by this rule. Then click Add. Figure 3-21 shows the All Computers group selected and an installation deadline of 14 Days After Approval. Click Next to proceed.

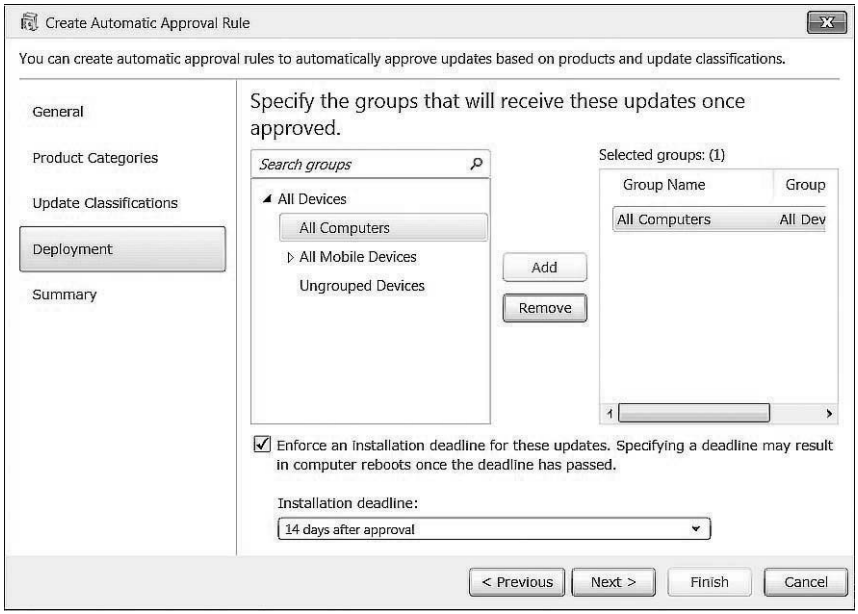

FIGURE 3-21 Deployment

6. On the Summary page, click Finish to complete the installation of the updates.

Third-party updates

You can use Intune to deploy updates from vendors other than Microsoft. You do this by manually uploading the update files, which can be in .msi, .msp, or .exe format. To upload and configure a third-party update to Intune, perform the following steps:

1. In the Updates workspace of the Intune Administration console, click Upload under Tasks.
2. On the Update Files page, select the file you want to upload and click Next.
3. Select a classification.

   You can choose from among Updates, Critical Updates, Security Updates, Update Rollups, or Service Packs. Then click Next.
4. On the Requirement page, select the operating system and architecture (x86 or x64) requirements for the update and then click Next.
5. On the Detection Rules page, specify how Intune can check whether the update has already been deployed on the Intune client.

   This check can be performed by looking for an existing file, an MSI product code, or a specific registry key. Click Next.
6. On the Prerequisites page, identify any prerequisite software required for update installation and then click Next.

You can specify None if no prerequisites are required or specify an existing file, an MSI product code, or a specific registry key.

7. On the Command Line Arguments page, specify any command-line arguments required to deploy the update and then click Next.
8. On the Return Codes page, specify how Intune should interpret return codes the update installation generates. Click Next. Finally, click Upload to complete.

After the update is uploaded to Intune, you can approve it using the same method you use to approve other software updates.

EXAM TIP

Remember that you can use SCUP or Intune to publish third-party updates to computers.

Thought experiment

Intune for update deployment for Contoso remote clients

You are responsible for managing software updates for remote clients at Contoso. All remote clients use the Windows 8.1 operating system and run the same suite of third-party applications. You want to ensure that any security and critical updates are deployed as soon as possible. You will review other updates before deciding to deploy them. With this information in mind, answer the following questions:

1. **How can you ensure that Windows 8.1 security and critical updates are installed as soon as possible?**
2. **What steps must you take to deploy updates for the suite of third-party applications?**

Objective summary

- Intune can provide updates to clients on which the Intune agent is installed.
- You select which updates Intune provides to clients, based on product and update classification.
- When you manually approve updates, you select the group for which the update is approved and specify a deployment action.
- Automatic approval rules enable you to deploy updates automatically, based on product and update classification.
- You can upload third-party updates to Intune and distribute them to Intune clients.

Objective review

Answer the following questions to test your knowledge of the information in this objective. You can find the answers to these questions and explanations of why each answer choice is correct or incorrect in the "Answers" section at the end of the chapter.

1. You have noticed that, although updates for Windows 7 are present within the list of available updates in the Intune console, updates for Windows 8 and Windows 8.1 are not present. Which of the following should you configure to resolve this problem?
   - **A.** Automatic approval rules
   - **B.** Third-party updates
   - **C.** Update policies
   - **D.** Update categories and classifications
2. You want to ensure that a user who is signed on to a computer can control whether Windows restarts after the installation of scheduled updates deployed from Intune. Which of the following would you configure to accomplish this goal?
   - **A.** Update categories and classifications
   - **B.** Update policies
   - **C.** Third-party updates
   - **D.** Automatic approval rules
3. You want computers running Windows 8.1 in your organization's Melbourne branch office to install critical operating system updates automatically. Computers running Windows 8.1 in your organization's Canberra office should install critical operating system updates only if an administrator manually approves those updates. Which of the following should you configure to accomplish this goal? (Choose two. Each correct answer provides part of a complete solution.)
   - **A.** Configure multiple computer groups.
   - **B.** Configure update policies.
   - **C.** Configure update categories and classifications.
   - **D.** Configure automatic approval rules.

Answers

Objective 3.1

Thought experiment

1. Use the Catalogs workspace of the System Center Updates Publisher console to subscribe to the update catalog the third-party vendor published.
2. The WSUS server and WSUS clients must trust the CA that issued the signing certificate installed on the SCUP server.

Objective review

1. **Correct answer:** B
   - A. **Incorrect:** The Installable rule type determines whether a target computer requires a software update.
   - B. **Correct:** The Installed rule type determines whether an update is already present on a computer.
   - C. **Incorrect:** Automatic approval rules are used with Intune to deploy updates automatically, based on classification and product.
   - D. **Incorrect:** Automatic deployment rules are used with Configuration Manager to deploy updates automatically, based on classification and product.
2. **Correct answer:** C
   - A. **Incorrect:** You use the Updates workspace to manage updates and update bundles, but you use the Publications workspace to remove a software update from publication.
   - B. **Incorrect:** You use the Catalogs workspace to subscribe to updates catalogs that third-party vendors publish.
   - C. **Correct:** You use the Publications workspace to remove a software update from publication.
   - D. **Incorrect:** You use the Rules workspace to edit rules that determine whether an update should be installed.
3. **Correct answer:** A
   - A. **Correct:** You specify whether an update requires a restart in the Restart Behavior section.
   - B. **Incorrect:** You use the Impact section to specify how an update should be handled—for example, whether it must be installed independently of other updates.

C. **Incorrect:** You use Severity to specify the security implications of an update.

D. **Incorrect:** You use the CVE ID field to specify the common vulnerabilities and exposures identifier.

Objective 3.2

Thought experiment

1. You must ensure that the WSUS console is deployed on the site server, given that WSUS is hosted on a separate server. This allows communication between the software update point and the WSUS server.
2. You must ensure that the management point and distribution point roles are also deployed.

Objective review

1. **Correct answer:** B

   A. **Incorrect:** Port 8530 is used for HTTP communication in the default configuration of WSUS on Windows Server 2012 R2. You need to use port 8531 when configuring communication by using HTTPS.

   B. **Correct:** You need to use port 8531 when configuring communication by using HTTPS.

   C. **Incorrect:** Port 80 is usually reserved for HTTP traffic. With WSUS on Windows Server 2012 R2, the default HTTP port is 8530.

   D. **Incorrect:** Although port 443 is usually reserved for HTTPS traffic and was used for secure communication with earlier versions of WSUS, more recent versions of WSUS use port 8531 for HTTPS communication.

2. **Correct answer:** A

   A. **Correct:** Located on the site server, the Wsyncmgr.log log file provides information about the software-updates synchronization process.

   B. **Incorrect:** The WSUSCtrl.log log file provides information about the configuration, database connectivity, and health of the site's WSUS server.

   C. **Incorrect:** The SoftwareDistribution.log log file provides information about the software updates that synchronize from the configured update source to the WSUS server database.

   D. **Incorrect:** Located on the client computer, the ScanAgent.log log file provides information about the scan requests for software updates, which tool is requested for the scan, and the WSUS location.

3. **Correct answer:** D
   A. **Incorrect:** The Unknown compliance state indicates that the site server has not received information from the client computer. Although the update might be required, this is not the best answer.
   B. **Incorrect:** The Installed compliance state indicates that the update has been installed.
   C. **Incorrect:** The Not Required compliance state indicates that the update does not need to be deployed.
   D. **Correct:** The Required compliance state indicates that the update should be deployed to the client computer.

Objective 3.3

Thought experiment

1. Create an automatic approval rule that approves all critical and security updates for computers running Windows 8.1.
2. Import third-party updates into Intune and then approve them for distribution.

Objective review

1. **Correct answer:** D
   A. **Incorrect:** Automatic approval rules automatically approve updates based on product and classification. If the Windows 8 and Windows 8.1 updates are not present in the Intune console, you need to change the update categories and classifications settings.
   B. **Incorrect:** You can upload third-party updates to Intune, but you should configure update categories and classifications to ensure that specific Microsoft operating systems and products are covered.
   C. **Incorrect:** Update policies specify when and how updates will be deployed. You do not use them to configure which updates will be deployed.
   D. **Correct:** You need to configure update categories and classifications to ensure that updates for Windows 8.1 will be available to your Intune deployment.
2. **Correct answer:** B
   A. **Incorrect:** You configure update categories and classifications to ensure that updates for specific products and for specific classifications will be available to your Intune deployment.
   B. **Correct:** Update policies specify when and how updates will be deployed, including whether a signed-on user can override a restart required to complete update installation.

C. **Incorrect:** You can upload third-party updates to Intune, but this doesn't involve controlling restart behavior.

D. **Incorrect:** Automatic approval rules automatically approve updates based on product and classification. They do not control restart behavior.

3. **Correct answers:** A and D

A. **Correct:** You need to configure a group for the Melbourne computers and then configure an automatic approval rule.

B. **Incorrect:** Update policies do not determine which updates are installed, just when and how the updates are installed.

C. **Incorrect:** You only need to configure update categories and classifications if Intune isn't obtaining updates of the required category and classification.

D. **Correct:** You need to configure a group for the Melbourne computers and then configure an automatic approval rule.

This page intentionally left blank

This page intentionally left blank

Index

Numbers and Symbols

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

X