Microsoft

Managing Enterprise Devices and Apps

Exam Ref 70-696

Orin Thomas

Microsoft

Managing
Enterprise
Devices and Apps

Exam Ref 70-696

Orin Thomas

Exam Ref 70-696 Managing Enterprise Devices and Apps

Orin Thomas

Microsoft

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.

Microsoft and the trademarks listed at http://www.microsoft.com/about/legal/en/us/IntellectualProperty/Trademarks/EN-US.aspx are trademarks of the Microsoft group of companies. All other marks are property of their respective owners.

The example companies, organizations, products, domain names, email addresses, logos, people, places, and events depicted herein are fictitious. No association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred.

This book expresses the author's views and opinions. The information contained in this book is provided without any express, statutory, or implied warranties. Neither the authors, Microsoft Corporation, nor its resellers, or distributors will be held liable for any damages caused or alleged to be caused either directly or indirectly by this book.

Contents at a glance

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 <ins>http://www.microsoft.com/learning/en/us/certification/cert-default.aspx</ins>.**

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 1. Deploy and manage virtual applications

Virtualized applications provide administrators with more options than traditional applications. Rather than always requiring deployment through local installation, you can stream virtualized applications to clients. Virtualized applications don't make modifications to a client's registry or file system, so they can be removed as cleanly as they are installed. In this chapter, you learn about how to virtualize traditional applications, how to manage a virtualized application environment, and how to use RemoteApp to provide users with local access to applications running on remote servers.

Objectives in this chapter:

- Objective 1.1: Prepare virtual applications.
- Objective 1.2: Manage application virtualization environments.
- Objective 1.3: Deploy and manage RemoteApp.

Objective 1.1: Prepare virtual applications

Microsoft Application Virtualization (App-V) is a technology that enables you to virtualize applications so that they run in an environment that shields them from directly interacting with the operating system. Then you can run applications concurrently that are incompatible with each other. You use a special tool known as a sequencer to virtualize applications.

This section covers the following topics:

- Application virtualization concepts
- Sequencing an application
- Preparing the Sequencer environment
- App-V Connection Groups

Application virtualization concepts

Users can use application virtualization to run applications locally even though those applications are not installed directly on the client computers. This works because App-V client software is installed directly on the client computers and simulates a specially prepared operating system environment. Virtualized applications run within that specially prepared simulated environment.

Virtualized applications do not interact directly with the client operating system but instead interact with the App-V client. The App-V client functions as a proxy through which the application uses operating system resources.

App-V provides the following benefits over traditionally deployed, locally installed applications. With App-V, you can:

- **Run multiple versions of applications without conflict** You can use App-V to run different versions of applications concurrently on the same client computer. For example, it is possible to run Microsoft Word 2007, Word 2010, and Word 2013 concurrently if they are all set up as App-V applications; otherwise, you cannot run these applications side by side on the same

client computer. It also is possible to use App-V in conjunction with Remote Desktop Services (RDS). This enables users to run applications side by side on Remote Desktop Session Host servers.

- **Minimize application conflict** Sometimes two or more applications cause conflicts with each other because of dynamic-link library (DLL) or application programming interface (API) conflicts. However, when you install these applications as App-V applications, there is no conflict because each App-V application runs in its own isolated environment.

- **Simplify application removal** App-V applications are not installed locally, so they can be removed completely. Clean removal is not always possible with applications that are installed directly on Windows-based clients, even if an application has been designed to remove all files and settings when it is uninstalled. Virtualized applications are easily removed after the user signs out from the computer and can be purged automatically from the App-V client cache.

- **Simplify application upgrades** Instead of upgrading a locally installed application on all computers in your organization with a hotfix, service pack, or new versions, the modular nature of virtualized applications enables you to replace one version of an application with an updated version with less effort.

- **Minimize license compliance risks** App-V has license group functionality, so you can ensure that only a specific number of users can run an application at any point in time.

- **Scale infrastructure** Depending on the infrastructure model you use, you can add publishing servers to an App-V deployment as necessary to ensure that service levels are maintained as demand grows.

- **Take advantage of client hardware resources** Even though App-V applications are not installed locally, they can use the local computer's processor and RAM resources. In environments where client computers have inadequate hardware resources, this can lead to a better experience for the user than running applications on a Remote Desktop Session Host server would.

- **Enable users to use roaming applications** If applications are streamed rather than locally installed, users can sign in to any computer that has an App-V client installed and quickly access their application. You can also configure App-V to work with Microsoft User Experience Virtualization to allow users to have application settings for App-V applications roam across client computers.

- **Give users quick access to their applications** Because the application is streamed, access is faster than if the application is fully deployed from the server after the user is signed in. Depending on how you configure App-V, only some parts of the application prepared with App-V might be downloaded to the client computer. This means the user can start using an application without waiting for the entire application to be streamed from the server. App-V application components can be stored in a nonvola-tile cache, so an App-V application can run when a computer is offline and cannot access the server from which it originally streamed the application.

- **Increase security for sensitive applications** You can also configure the App-V client through Group Policy to ensure that applications can be run only when the computer is online. You can use Group Policy to provide sensitive applications to users in environments where employees

are using their personal devices while ensuring that these sensitive applications are not available when the user leaves the organization premises.

More Info: **App-V 5.0 Overview**

You can learn more about App-V 5.0 at *http://technet.microsoft.com/en-us/windows/jj835807.aspx*.

Sequencing an application

Sequencing enables you to create a special version of a normal application that can run in the virtual environment the App-V client provides. In the sequencing process, the Application Virtualization Sequencer records all the modifications the application makes to files and settings during installation.

For example, when you install an application, sequencing writes program files to a particular directory, writes entries to the registry, and creates or modifies initialization (.ini) files and environment variables. The sequencing process records all the information necessary to run the program within the environment the App-V client provides.

The sequencing process involves the following general steps:

1. The Sequencer triggers the application's standard installation process. It then records the following:

   - Files that have been installed
   - Registry settings that have been modified
   - Environment variables that have been configured
   - Dynamic-link libraries (DLLs) that have been registered
   - Any other changes that have occurred to the system

2. The Sequencer creates a virtual environment and loads the application into this environment, including any data and modifications that occurred during the standard installation process.

3. The application starts so that any post-installation configuration tasks can be performed. If this step is not performed during sequencing, users will have to perform these post-installation tasks manually after deployment, storing any configuration settings locally on the client. During this process, the Sequencer determines which program components are required to start the application.

In more detail, to sequence an application you use the Application Virtualization Sequencing Wizard to install the application by performing the following general steps:

1. Open the Sequencer on the client.
2. Create a new virtual application package.
3. Verify that the operating system environment has no issues that might interrupt the sequencing process.
4. Choose the application type.
5. Choose the application installer location.
6. Provide a virtual application package name and a primary virtual application directory. The

Sequencer will trigger the installation.

7. Answer questions that the installation routine presents.

   These can include questions about license agreements, installation location, and other application installation options.

8. Run any additional files the installation might require.

9. Complete the installation.

10. Perform any post-installation configuration tasks.

11. Review the installation report.

12. Configure the streaming options.

13. Select the target operating system.

14. Create the package.

The Sequencer supports applications that need the computer to restart during the installation process. In these cases, the Sequencer will begin again after the client computer restarts and continues to sequence the application.

The App-V 5.0 Sequencer produces applications that you can use only with the App-V 5.0 client. The App-V 5.0 client cannot run applications sequenced for earlier versions of App-V. You must convert those applications to the App-V 5.0 format before they can run on computers running the App-V 5.0 client. You can run App-V 5.0–sequenced applications only on computers running Windows 8.1, Windows 8, Windows 7, Windows Server 2012, Windows Server 2012 R2, and Windows Server 2008 R2 with the Remote Desktop feature.

Custom installation

When you perform a custom application installation, you do not provide the Sequencer with the path to the application installer. Instead, you perform the application installation outside the Sequencer and have it record the changes that occur to files and settings. Custom installation is similar to a standard installation except that for a custom installation, you must manually trigger the installation rather than use the Sequencer to do this.

Sequencer options

Generally, the default Sequencer settings are appropriate for most application sequencing procedures. In some instances, though, you will want to change some or all of the settings. You can see the settings by clicking Options on the Tools menu of the Sequencer, which opens the Options dialog box. The advanced settings include the following:

- **Scratch Directory** Temporary files are saved in this location.
- **Allow Microsoft Update To Run During Monitoring** Microsoft Update runs during the monitoring process. This setting is disabled by default.
- **Append Package Version To Filename** The version number is added to the file name. When an application is resequenced, the version is increased by 1.
- **Always Trust The Source Of Package Accelerators** The Sequencer does not generate a prompt when a package accelerator is not signed by a trusted source.

- **Parse Items** The Sequencer monitors these areas of the file system and settings when sequencing an application.
- **Exclusion Items** The Sequencer does not monitor these areas of the file system and settings when sequencing an application.

The App-V Sequencer also supports the following:

- **Package accelerators** Package accelerators automate the sequencing process. They are useful when you need to sequence a particular application frequently.
- **Add-ons or plug-ins** You can use the Sequencer to create an add-on or plug-in to extend the functionality of an application. For example, you could create an add-on for a sequenced web browser or a graphic design program. When you install an add-on or plug-in, you install the application first and then add the component.
- **Middleware applications** Use the middleware application type to sequence middle-ware or framework software that another sequenced application package requires. For example, a particular environment might be required to run a sequenced application. You can sequence this as middleware.

More Info: **Sequencing an Application**

You can learn more about sequencing an application at *http://technet.microsoft.com/en-us/library/jj713438.aspx*.

Preparing the Sequencer environment

The App-V Sequencer requires the following software:

- Windows 7 (x86 and x64), Windows 8 (x86 or x64), or Windows 8.1 (x86 or x64)
- Microsoft .NET Framework 3.51 and .NET Framework 4.5 (Full)
- Windows PowerShell 3.0 (included with Windows 8.1 and Windows 8)
- Microsoft KB2533623 (an update for Windows 7)
- Microsoft Visual C++ 2008 Redistributable (x86 and x64; executable file install only)

Installing the Sequencer involves running an executable file (.exe) or installing from a Windows installer package file (.msi). If you install from the .msi file, you do not need to install the Visual C++ 2008 Redistributable manually.

You should install the Sequencer on a client computer that runs the same operating system as the clients that will run the sequenced applications. When you are selecting the client on which to install the Sequencer, keep the following guidelines in mind:

- If your end users are using an x64 version of Windows 7, you should sequence applications on a computer running the x64 version of Windows 7 with the App-V Sequencer installed.
- If you have a mix of x86 and x64 clients, you can either sequence the x86 version of an application and deploy it to both architectures or sequence the x86 and x64 versions separately.
- A computer running the Windows 8.1 or Windows 8 operating system will be able to run an application sequenced on a computer running the Windows 7 operating system.
- Although an application sequenced on a computer running the Windows 8.1 or Windows 8

operating system will likely run when deployed through App-V to a computer running the Windows 7 operating system, Microsoft does not recommend this strategy. Instead, you should sequence applications that you intend to run on computers running the Windows 7 operating system on a computer running the Windows 7 operating system.

The client that runs the Sequencer should have no applications installed beyond the base operating system and should be as close to the out-of-the-box experience (OOBE) as possible. As a best practice, do not use an existing computer that has had applications installed and then removed, because some applications might not uninstall fully and thus might affect the sequencing process. This is an important part of ensuring that sequencing works correctly. Sequencing involves capturing only those modifications made during application installation; additional applications and certain services can interrupt the sequencing process, causing it to fail.

In addition to these considerations, avoid using operating system images that include clients from antimalware applications and products such as System Center 2012 Configuration Manager or System Center 2012 Data Protection Manager.

Before performing a sequencing operation on a newly installed computer running the Windows 8.1 operating system, you should disable the following services:

- Windows Defender service
- Windows Search service

Because you need to have the client in as close to an OOBE state as possible each time you sequence an application, it is much more efficient to install the Sequencer on a client that is running as a virtual machine. Then you can use a virtual machine snapshot to return the client to an unmodified configuration after you sequence each application. Ensure that you transfer the sequenced application to a network location before reverting the computer that performs the sequencing role.

More Info: **Deploying the Sequencer**

You can learn more about deploying the App-V Sequencer at *http://technet.microsoft.com/en-us/library/jj713464.aspx*.

App-V Connection Groups

Use App-V Connection Groups to group one or more App-V 5.0 packages. All the applications in an App-V Connection Group can interact with one another as if you had installed them on the same device while still isolating them from the rest of the system. System Center 2012 R2 Configuration Manager (or System Center 2012 Configuration Manager SP1) uses App-V virtual environments to take advantage of the functionality of App-V Connection Groups. An administrator defines the requirements for a virtual environment. When a client system meets those requirements, an App-V Connection Group is created on the client.

To create a virtual environment, perform the following general steps:

1. In the Software Library workspace of the Configuration Manager console, expand the Application Management node and click App-V Virtual Environments.
2. On the ribbon of the Configuration Manager console, click Create Virtual Environment.
3. In the Create Virtual Environment dialog box, provide a name for the virtual environment.

shows this name set to the Adatum App-V virtual environment. Click Add to add an App-V deployment type.
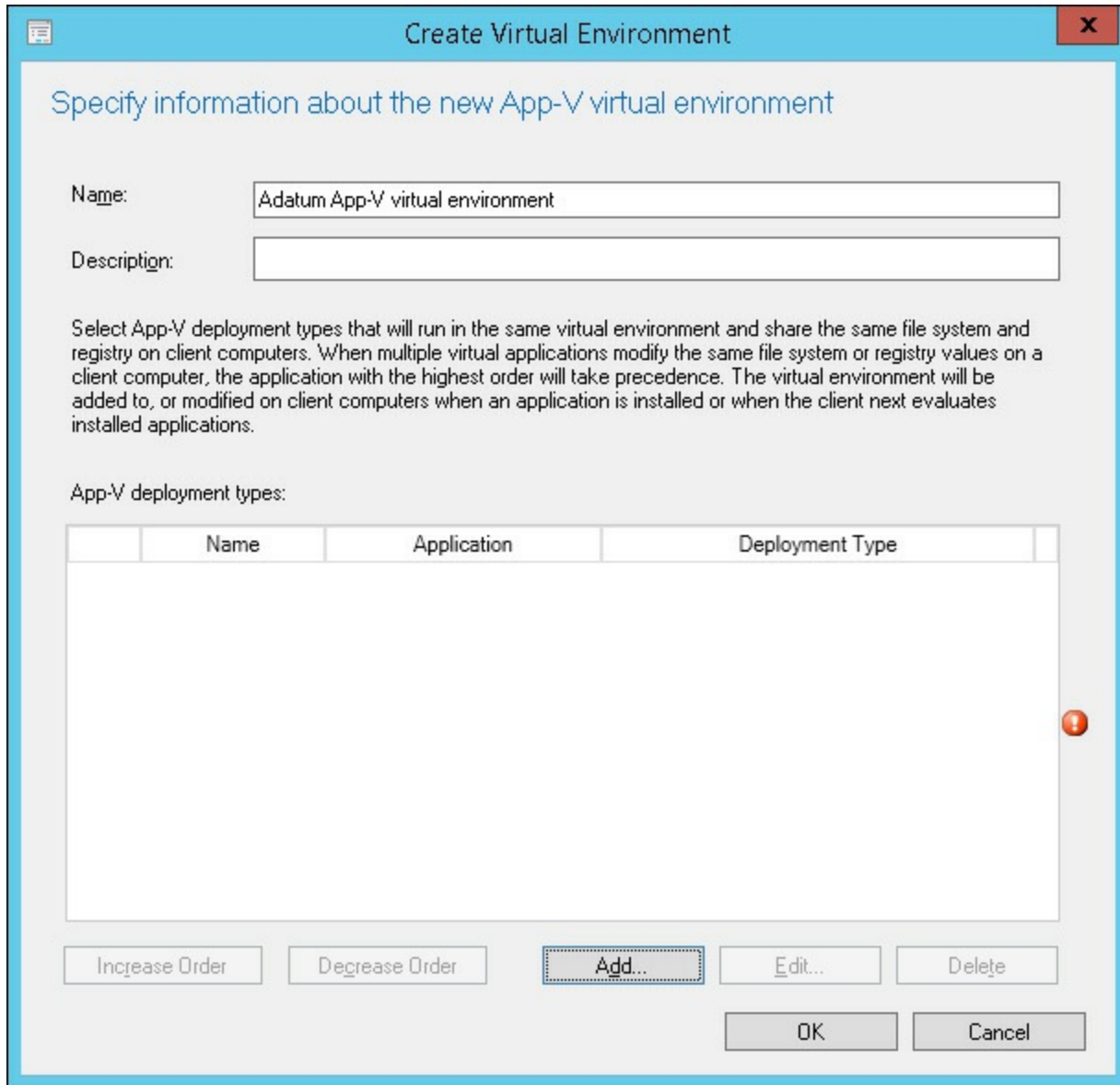
FIGURE 1-1 The Create Virtual Environment dialog box

4. In the Add Applications dialog box, provide a name for the group and click Add to add applications.

5. In the Specify Application dialog box, shown in , select the application you want to add to the group. Click OK.
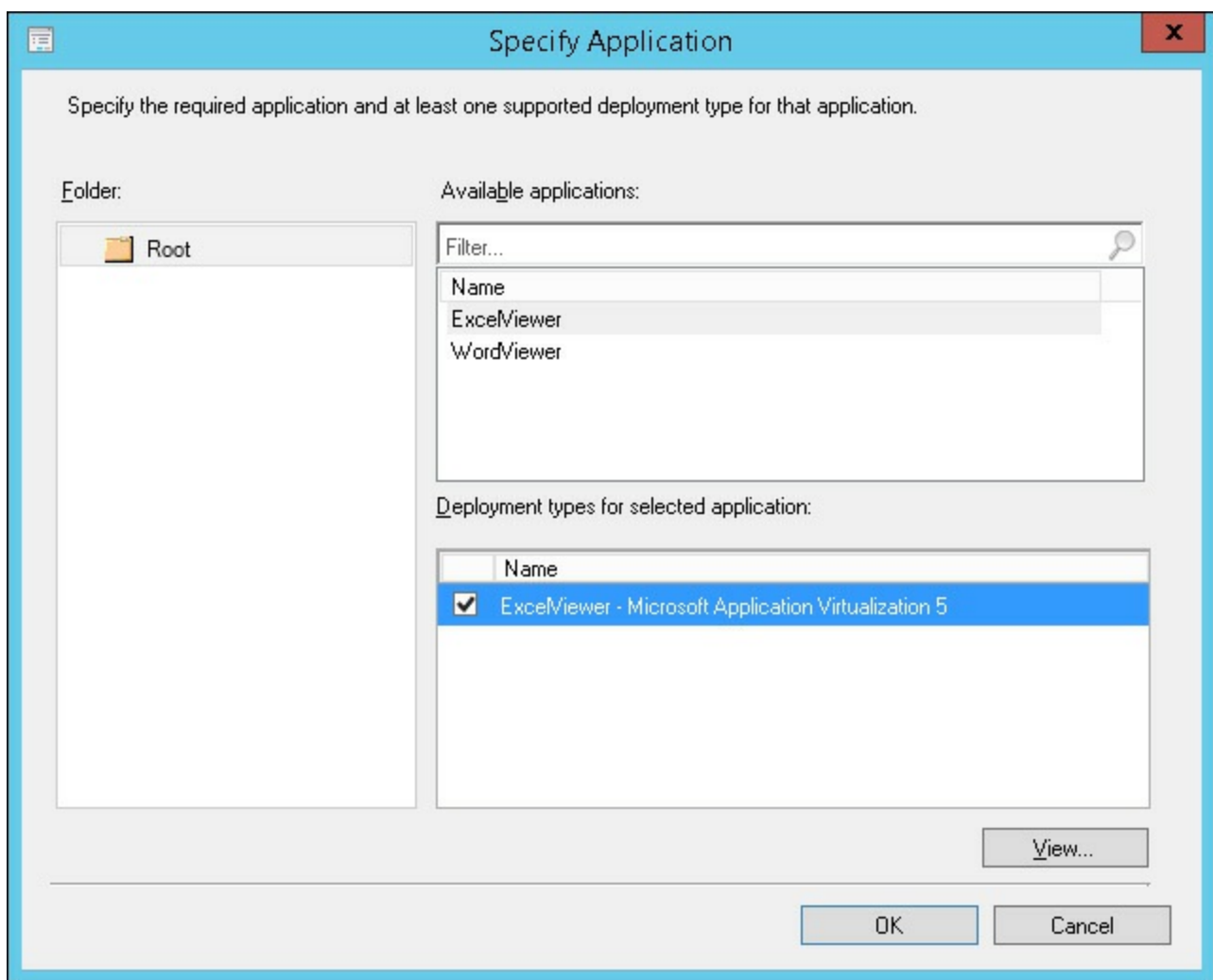
FIGURE 1-2 The Specify Application dialog box

6. In the Add Applications dialog box, add all the applications you want to use with the Connection Group. Figure 1-3 shows ExcelViewer and WordViewer added to the same virtual environment. Click OK.
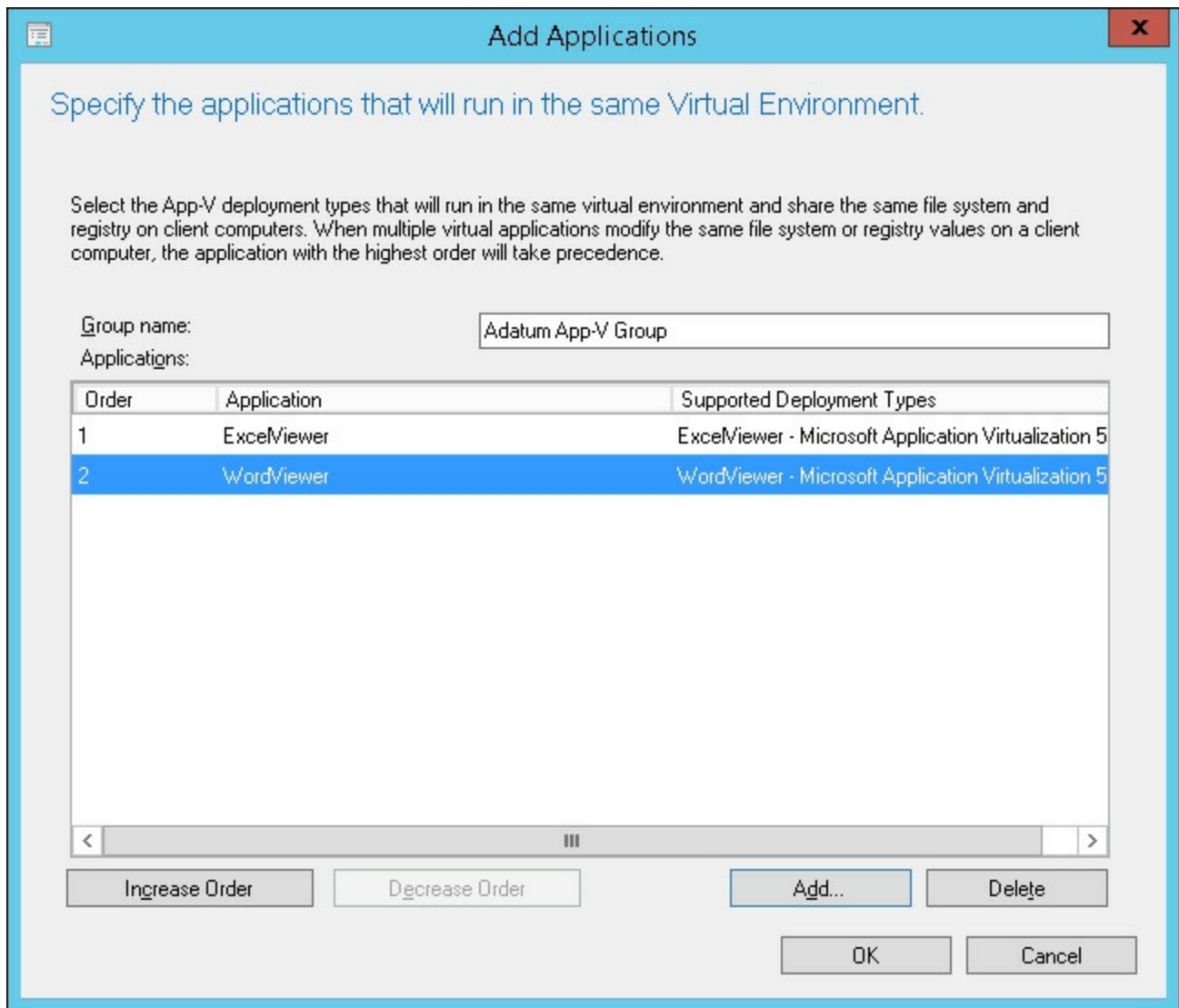
FIGURE 1-3 The Add Applications dialog box

7. In the Create Virtual Environment dialog box, review the applications that have been added to the virtual environment, as shown in Figure 1-4, and then click OK.
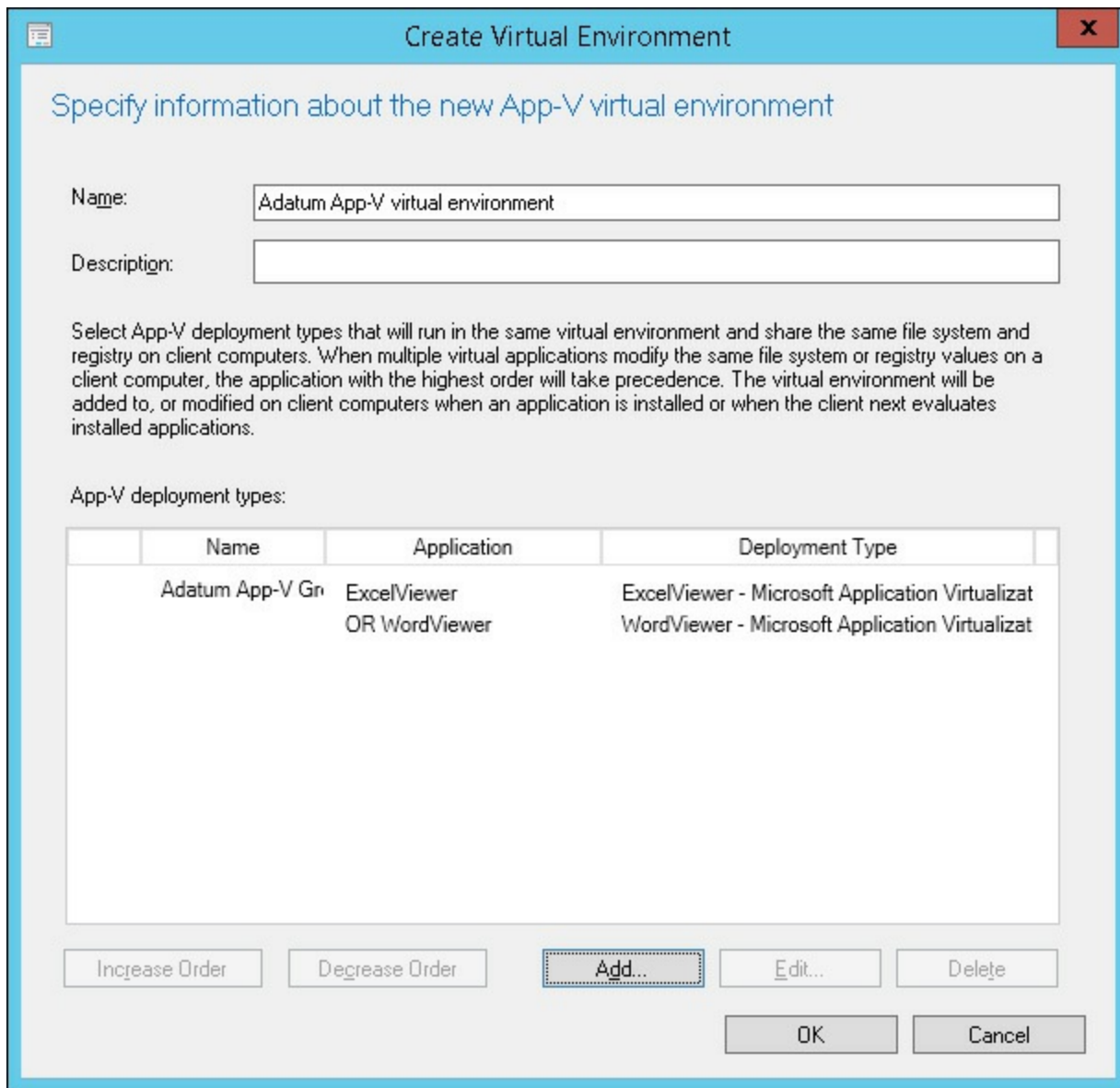
FIGURE 1-4 The Create Virtual Environment dialog box

When migrating existing connection groups from standalone App-V 5.0 virtual environments to virtual environments in which App-V 5.0 is integrated with System Center 2012 R2 Configuration Manager, you must create virtual environments that match the existing connection groups on client computers. You do this so that Configuration Manager manages the clients correctly, and the user's environment within those connection groups remains the same.

The general process for migrating from App-V Connection Groups to a Configuration Manager virtual environment is as follows:

1. Create applications with Application Virtualization 5.0 deployment types for all existing App-V 5.0 packages for the virtual environments that you want to migrate.

2. Deploy the new applications with the purpose of Required.

3. After you deploy the applications, create virtual environments that match the connection groups they are replacing. The virtual environments must have the same App-V 5.0 deployments types in the same order. If the virtual environments do not match the App-V 5.0 Connection Groups, new connection groups will be created, and any user customizations in the shared isolation environment will be lost.

You can create new virtual environments in System Center 2012 R2 Configuration Manager. New

virtual environments must contain at least one App-V deployment. When you deploy an App-V deployment type, the virtual environments associated with the deployment type also are deployed. This enables you to create App-V Connection Groups before all the applications for the new virtual environment are available. To create new App-V virtual environments in the Configuration Manager console, navigate to the Software Library workspace, the Application Management folder, and then the App-V Virtual Environments node. You add App-V deployment types to the virtual environments by using simple rules. An App-V deployment type can belong to more than one virtual environment.

More Info: **App-V Connection Groups**

You can learn more about App-V Connection Groups at *http://technet.microsoft.com/en-us/library/jj713417.aspx*.

Exam Tip

Remember what steps you need to take to allow virtualized applications to share data.

Thought experiment: **Application sequencing at Contoso**

You are preparing to sequence an important application at Contoso. This application has two versions, an x86 version and an x64 version. You intend to deploy the x86 version to computers running an x86 version of Windows 7. You intend to deploy the x64 version to computers running an x64 version of Windows 8.1. With this information in mind, answer the following questions:

1. **How many times should you sequence the application?**
2. **Which services should you disable on the computer running Windows 8.1 x64 prior to sequencing the application?**

Objective summary

- A virtualized application is isolated from the host operating system and interacts indirectly with it through the App-V client.
- You should sequence an application on the same platform as you intend to run it.
- Applications sequenced on x64 platforms cannot run on x86 platforms, but applications sequenced on x86 platforms can run on x64 platforms.
- App-V Connection Groups allow virtualized applications to share data.

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 "" section at the end of the chapter.

1. You use the App-V Sequencer to sequence an x64 application on a computer running Windows 8.1. Which of the following computers can run this application if the App-V client software has been installed? (Choose the best answer.)

    A. The x64 version of Windows 8.1

    B. The x86 version of Windows 8.1

    C. The x64 version of Windows 7

    D. The x86 version of Windows 7

2. You want to allow two virtualized applications, App-A and App-B, to share data when running on the same computer. Which of the following should you configure to allow this to occur? (Choose two. Each answer forms a complete solution.)

    A. App-V Connection Group

    B. App-V virtual environment

    C. Plug-ins

    D. Middleware application

3. You need to sequence an application that is updated on a regular basis. Which of the following should you use with the App-V Sequencer to automate this process?

    A. Connection group

    B. Middleware application

    C. Add-on or plug-in

    D. Package accelerator

Objective 1.2: Manage application virtualization environments

App-V can be run in several ways. You can run an App-V infrastructure with its own servers to stream apps and use a simpler structure by which to virtualize applications but deploy them in a traditional manner. You can also integrate App-V with Configuration Manager. Depending on how you've configured your organization's infrastructure, you can manage App-V apps through Group Policy or through Configuration Manager.

This section covers the following topics:
- App-V infrastructure
- App-V deployment models
- Deploying sequenced applications
- App-V Group Policy

App-V infrastructure

An App-V 5.0 deployment includes several elements, some of which must be present in all App-V 5.0 models and some of which are used only in specific App-V deployments.

These elements are as follows:

- **Management Server** The Management Server hosts a Microsoft Silverlight–enabled web application that App-V administrators use to manage the App-V infrastructure. The Management Server must have a good connection to the Management Server database. You can deploy the Management Server and Management Server database on the same server or on different servers.

- **Publishing Server** The Publishing Server is a web server that deploys applications to App-V clients. In previous versions of App-V, the Publishing Server was known as the streaming server. You deploy App-V applications to the Publishing Server in the App-V full infrastructure model by using the App-V Management Server console. App-V 5.0 applications are streamed from the Publishing Server by using HTTP.

- **Management Server database** The Management Server database stores App-V configuration and settings data. The database is hosted on an SQL instance running SQL Server 2008 SP2, SQL Server 2008 R2, or SQL Server 2012. You can install the Management Server database separately from the Management Server, but if you do, you need to deploy the database first and then specify its location when you deploy the Management Server.

- **Reporting Server** The Reporting Server records the following information: application use, client information, package information, schema changes, and system options. You configure the address of the Reporting Server by using App-V Group Policy settings. Clients forward data to this address, which the Reporting Server then forwards to the Reporting Server database.

- **Reporting Server database** The Reporting Server database stores all the information forwarded to the Reporting Server. The instance that hosts the Reporting Server database must meet the same requirements as the instance that hosts the Management Server database. You can host both databases on the same server. You do not have to install SQL Server Reporting Services to deploy an App-V Reporting Server.

App-V deployment models

App-V has three deployment models, each of which has separate infrastructure requirements. These are the full infrastructure model, the standalone model, and the Configuration Manager integrated model.

> *More Info:* **App-V Deployment Models**
>
> **You can learn more about the full infrastructure model and the standalone model at *http://technet.microsoft.com/en-us/library/dn595131.aspx*.**

Full infrastructure model

The App-V full infrastructure model, also known as the Enterprise model, uses all App-V server elements. It also requires the Sequencer to sequence applications and the App-V client deployed on client computers.

The App-V full infrastructure model provides an organization with all the functions of the Management Server, including authentication, instance limitation, and application metering. These functions have the following properties:

- **Authentication** You can use this to limit applications to specific authorized users. For example, members of the Research department can run a specific application but members of the Management department cannot run the application.

- **Instance limitation** You can use a Management Server to limit the number of execution instances of a specific application to ensure that your organization meets its licensing obligations. Virtualized applications can be streamed to multiple computers, making it more challenging to ensure that instances of the application for which the organization is not licensed are not being run.

- **Application metering** You can generate historical data, recording how often an application is used and by which clients.

When you use the App-V full infrastructure model, you should ensure that Publishing Servers have high-speed connections to the clients that use these applications. This ensures that users who use streaming applications get access to them quickly. Users who access applications from publishing servers located across wide area network (WAN) links have to wait much longer for their applications to open than users who access publishing servers on the local area network (LAN).

The App-V full infrastructure model is appropriate for organizations that:

- Need support for streamed applications.
- Need authentication, instance limitation, and metering.
- Have not already deployed Configuration Manager.

If an organization does not need to support streamed applications and does not require authentication, instance limitation, and metering functionality, it could use the standalone deployment method, which needs less infrastructure investment.

Standalone deployment model

The standalone deployment model is the least infrastructure-intensive version of application virtualization. It needs only a computer configured as an App-V Sequencer and clients with the App-V client installed. The standalone deployment model does not need a Management Server database, Publishing Server, or Management Server.

In the standalone deployment model, you use the App-V Sequencer to create sequenced App-V applications as packages in MSI format. You then deploy those sequenced applications in the same way you would deploy other applications in MSI format—for example, by using Group Policy, Microsoft Intune, System Center 2012 Configuration Manager SP1, or third-party application deployment technologies. The primary difference between deploying a traditional application in MSI format and deploying a sequenced, virtualized application in MSI format is that with the virtualized applications, you have to ensure that the App-V client is installed on the target device.

The standalone deployment model is appropriate for organizations that:

- Want the benefit of virtualized applications but do not need metering or application streaming.
- Want to deploy virtualized applications to clients on the Internet through Intune.
- Need to deploy only a small number of virtualized applications and so do not need to deploy the App-V full infrastructure model Configuration Manager.

Configuration Manager integrated model

The integrated model uses Configuration Manager to manage and measure the deployment of App-V virtualized applications. This deployment model uses the following components:

- **App-V Sequencer** You use this to create sequence App-V applications in App-V 5.0 format. You can also use the Sequencer to sequence applications in MSI format, which you can deploy using Configuration Manager.
- **App-V client** You need to deploy the App-V client to devices that want to access virtualized applications.
- **Configuration Manager** You manage and deploy virtualized applications to collections of computers by using Configuration Manager. Virtualized applications are streamed from Configuration Manager distribution points. To use all the features of App-V 5.0, you must have deployed System Center 2012 Configuration Manager SP1 or System Center 2012 R2 Configuration Manager.

In this integrated model, virtualized applications are deployed as Configuration Manager applications by using the special App-V 5.0 application type rather than from a Publishing Server.

When you use the App-V application type with Configuration Manager, virtualized applications can be streamed from distribution points in the same manner as when you use a Publishing Server in the App-V full infrastructure model. The advantage of the integrated model over the App-V full infrastructure model is that in the integrated model, virtualized applications can stream off any existing Configuration Manager distribution point. Configuration Manager distribution points can also take advantage of BranchCache and Background Intelligent Transfer Service (BITS) functionality.

Another advantage of the integrated model is that its deployment process can automatically determine whether the App-V client is present during application deployment and, if not, deploy the client before deploying the virtualized application. For example, if you deploy a virtualized application to a collection of 10 computers, and 5 of those computers do not have the App-V client installed, Configuration Manager can be set to deploy the App-V client automatically before deploying the virtualized application.

App-V applications can be listed as a deployment type in Configuration Manager. You can choose to deploy an application such as Microsoft Word to a computer and then build logic into the deployment so that, in some cases, the application is installed locally in a traditional manner, and in other cases, the application is installed as an App-V application. For example, Microsoft Word is installed locally if the computer is designated as the user's primary device, but it is installed as an App-V application if the computer is not designated as the user's primary device. The App-V deployment type enables administrators to perform temporary application deployment, which deploys the application to the client but does not make an ongoing configuration change in the client.

Although you can also use sequenced applications in MSI format with Configuration Manager,

these applications will be deployed in their entirety to the target device and will not be streamed to the device through the Configuration Manager distribution point.

The integrated model still requires use of Group Policy if you want to configure App-V client cache settings. You can use this policy to control whether streamed applications will persist in the client cache.

> *More Info:* **Configuration Manager Integrated Model**
>
> **You can learn more about the Configuration Manager integrated model at**
> *http://technet.microsoft.com/en-us/library/jj822982.aspx.*

Deploying sequenced applications

The first decision you need to make when deploying sequenced applications is which type of delivery mechanism you will use. You can stream the applications, install the applications locally, or use a mixture of streaming and local installation. Independent of the method you use, you can run a sequenced application only if the App-V client is present on the client device. When you are deciding which mechanism to use, keep in mind the following information.

Streaming applications

When applications are streamed, the application is available to the user as soon as enough of the application has transferred from the server to the client that the application can start. You can configure streaming so that applications are available only when the client is online. You might want to use this option with sensitive applications to which you want to control access. You can also configure streaming so that applications are available when the client is offline. In this situation, the application is stored in the client's cache. Streaming sequenced applications use the .appv file format.

Local installation of applications

A local installation has the benefits of a virtualized application (such as minimizing compatibility problems with other applications) while also keeping the application available when the client is offline without relying on the application remaining in the client's App-V cache. Locally installed applications are delivered to the client by using local install, Group Policy, Intune, System Center 2012 Configuration Manager SP1 or System Center 2012 R2 Configuration Manager, or another application deployment solution.

When you deploy a sequenced application and locally install it, the entire sequenced application is downloaded to the client before the application is run. The application is always available for offline use—unlike with streamed applications, you cannot ensure that a user will not have access to a sequenced application when that user's computer is not connected to the organizational network.

Locally installed sequenced applications use the .msi format rather than the .appv format. Using the .msi format enables you to treat a sequenced application in the same way that you would treat a traditional local installation. You can deploy a sequenced application by using Intune and Group Policy, an approach that was not possible with earlier versions of App-V. You cannot import sequenced applications to an App-V Publishing Server by using the .msi format.

When you deploy a sequenced application in .msi format, you need to ensure that the App-V client

is present on the target client; if it is not, the application cannot run. You can use Programs And Features on a client to remove a sequenced application deployed in .msi format.

You can use the .msi format with sequenced applications when you create thick images for operating system deployment.

Streaming and local installation of applications combined

You might use a mixture of streaming and local installation. For example, when some applications don't need to be on the client devices permanently but you want the users to have access to them quickly, stream these applications; when other applications need to be on the client devices permanently but need to be isolated from other applications, install these applications locally as App-V applications.

After you decide which delivery mechanism you want to use, you need to select a deployment technology. You can use the following products to deploy sequenced applications:

- **System Center 2012 Configuration Manager SP1 and System Center 2012 R2 Configuration Manager** Configuration Manager supports both streaming and local installation. You can configure a single application to be streamed or locally installed, depending on the conditions that exist on the client. You can configure Configuration Manager to detect whether the App-V client is present on the device. If App-V is not present, Configuration Manager will deploy it before deploying the sequenced application. You can use Configuration Manager reporting functionality to monitor application use.

- **App-V Publishing Server** You can stream applications from App-V Publishing Servers. Use Group Policy to provide clients with the location of publishing servers. Administrators can use App-V Reporting Server functionality to meter application use. If you want to allow application streaming and you are not using System Center 2012 Configuration Manager SP1, you must deploy an App-V Publishing Server.

- **Group Policy deployment** Use Group Policy software deployment to deploy sequenced applications in .msi format locally. You cannot use Group Policy to meter application use.

- **Manual deployment** Use the .msi file to install the sequenced application manually on a computer. Use this method infrequently because it requires substantially more time than an automated deployment method.

- **Logon scripts** Use the Msiexec.exe command to install an .msi file.

- **Microsoft Intune** Use Intune to deploy the .msi file to remote clients that infrequently connect to the organizational network.

Streaming and the App-V application cache

Streamed applications are transferred from App-V Publishing Servers or Configuration Manager distribution points to App-V clients over the HTTPS protocol. Streamed applications start running on the client as soon as enough of the virtualized application has transferred to the client to begin running. For example, rather than downloading an entire 1 GB application before beginning to run, the application might start to run when only some of its files have been transferred. The rest of the application streams to the client as necessary.

The App-V client stores streamed applications in the local App-V cache. As long as a particular

application is in the cache, it will be loaded from there the next time the user wants to run it—the device will not need to reacquire the application from the publishing server or distribution point. As long as an application is in the cache, that application can be used when the device is not connected to the Publishing Server or distribution point.

You can configure the Shared Content Store (SCS) Mode Group Policy item so that sequenced applications can run only when the device is connected to the Publishing Server or distribution point. When you enable this policy, the streamed application will not be stored in the App-V cache and must be reacquired each time the user wants to run it. This policy is only available if the App-V templates are present in Group Policy.

Not all virtualized application deployment methods ensure that the sequenced application can be streamed to the client. Applications can be streamed when you do the following:

- Deploy the application by using the App-V full infrastructure model.
- Deploy the application by using the App-V deployment type in Configuration Manager.

If you are using the App-V full infrastructure model, you need to configure clients with the address of the Publishing Server by using Group Policy. You can configure Group Policy with the address of up to five publishing servers. You use the App-V Management Server web application to import applications in App-V format and publish them to publishing servers. You also use the App-V Management Server web application to configure permissions.

When using App-V sequenced applications with Configuration Manager, clients use Configuration Manager distribution points as the source for streamed applications. These clients use the Configuration Manager client to determine which applications they are eligible to consume.

Configuring dependencies

An advantage of using Configuration Manager as opposed to other deployment methods is that you can configure dependencies. When you configure a dependency, the client checks whether the specified prerequisite software environment is present. In the case of sequenced applications, you can configure Configuration Manager to check whether the App-V software is present on the client. If the App-V software is present, the deployment proceeds as usual. If the App-V software is not present, Configuration Manager will deploy it before deploying the sequenced application.

To configure the App-V client as a dependency for an application, perform the following steps:

1. In the Software Workspace of Configuration Manager, click Software Library.
2. In the Application Management folder, click Applications.
3. Right-click the virtualized application and then click Properties.
4. On the Deployment Types tab, click the deployment associated with App-V 5, as shown in Figure 1-5, and then click Edit.
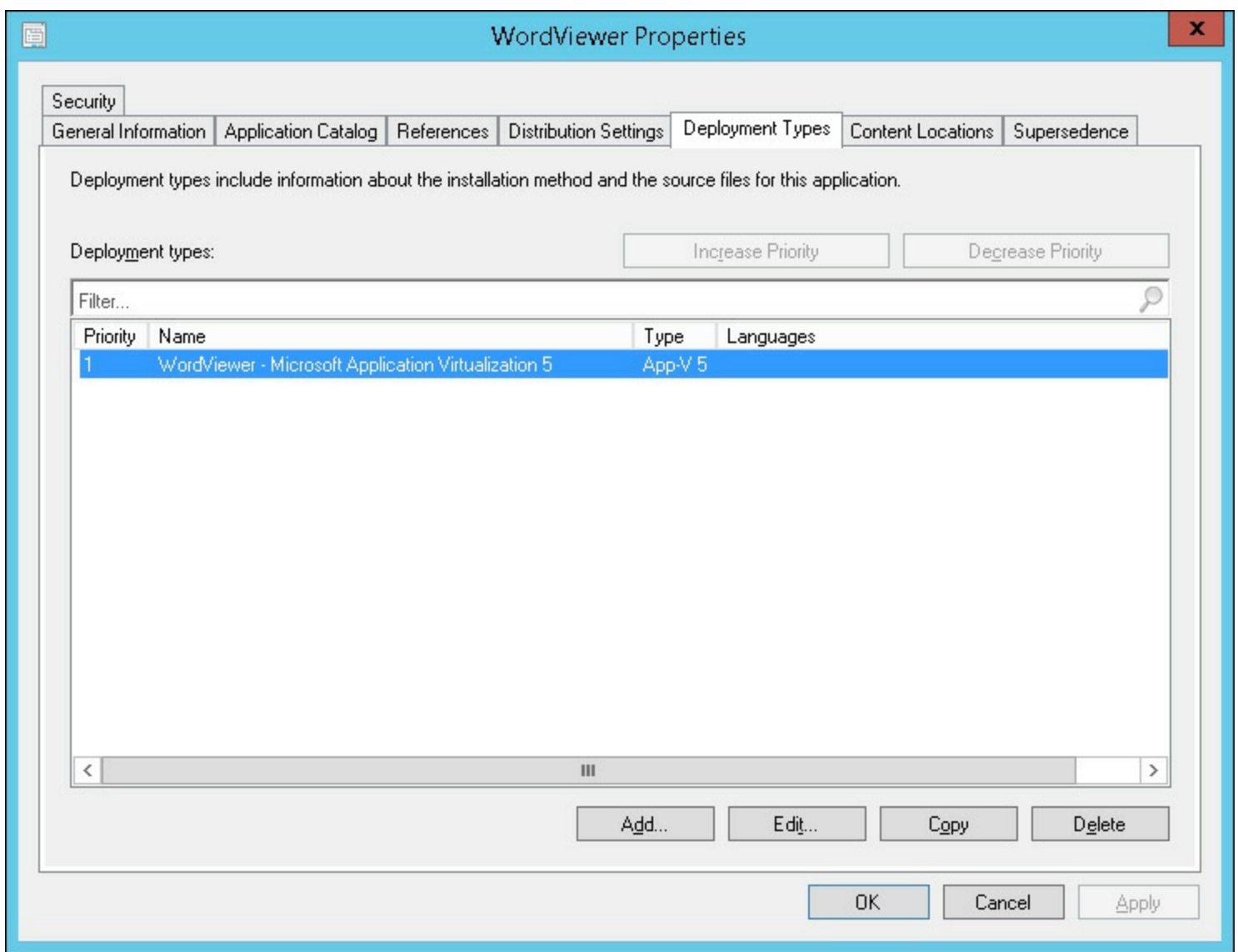
FIGURE 1-5 Deployment types

5. Click the Dependencies tab and then click Add.

6. In the Add Dependency dialog box, click Add.

7. In the Specify Required Application dialog box, click Microsoft Application Virtualization (App-V) Client 5.0. You must have already added Microsoft Application Virtualization (App-V) Client 5.0 to Configuration Manager before you can perform this step.

8. On the Deployment Types page for the selected application, click Microsoft Application Virtualization, as shown in Figure 1-6, and then click OK.
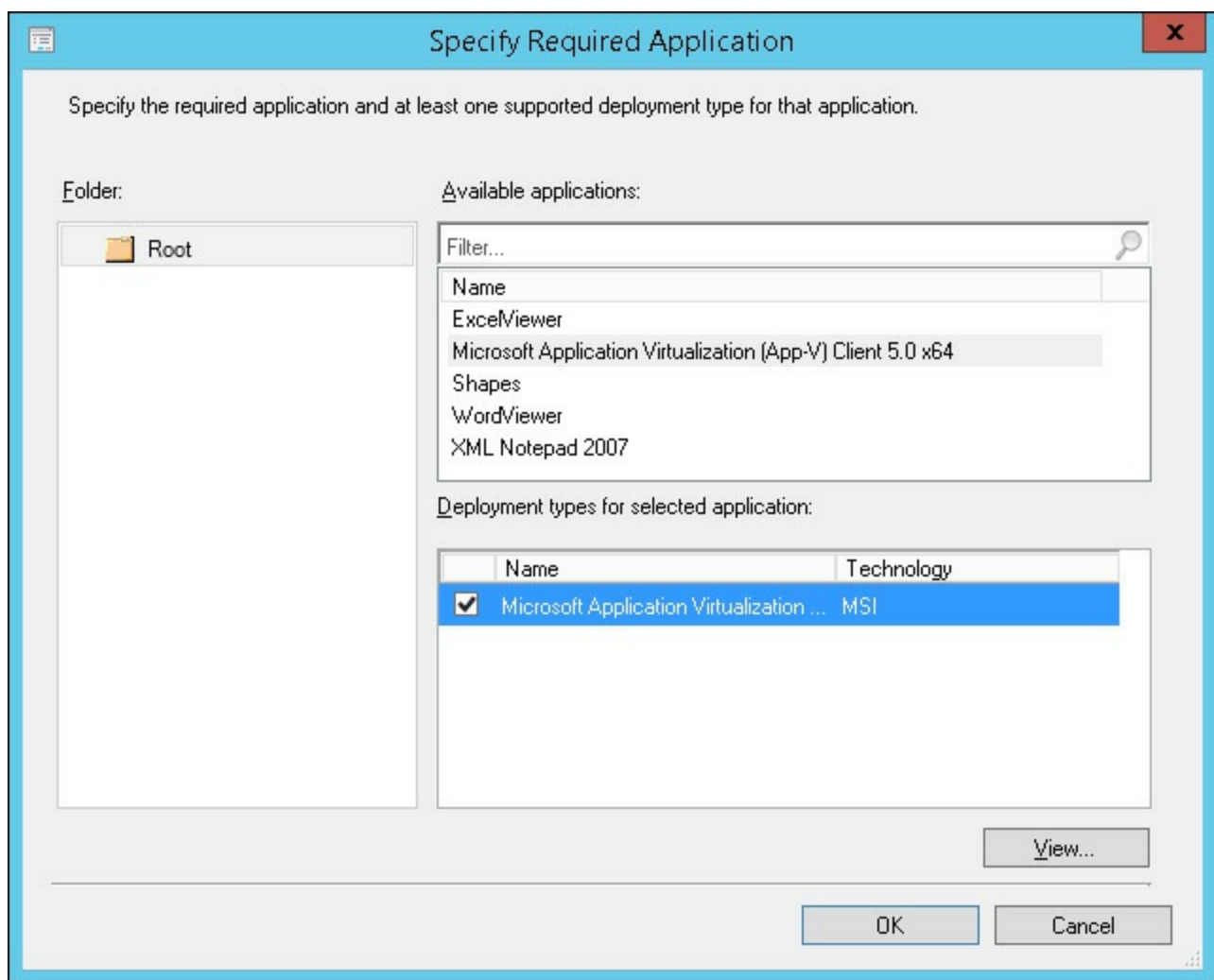
FIGURE 1-6 Specify Required Application dialog box

9. In the Add Dependency dialog box, type **App-V Apps** in the Dependency Group Name box and then click OK.

10. In the Application Properties dialog box, click OK.

App-V Group Policy

When you use the App-V full infrastructure model, you use Group Policy to configure important App-V settings, including the location of publishing servers and the behavior of the client cache. You do not need to use Group Policy to configure App-V if you are using the standalone deployment model.

To configure App-V Group Policy, add the App-V policy template to the Group Policy store on your domain controller. These policies can be downloaded from the Microsoft website.

After you place the templates in the Group Policy store, you can find App-V policies in the Computer Configuration\Policies\Administrative Templates\System\App-V node of a Group Policy Object (GPO). App-V policies are spread across the following six nodes:

- **Client Coexistence** Use the policy in this node to enable automatic migration to App-V 5.0 of packages that were created by using a previous version of App-V.
- **Integration** Use the policies in this node to specify the file paths in a user profile that do not roam with the user profile when used with App-V. Also, use the policies in this node to configure the location of symbolic links to the current version of the published package.
- **Publishing** Use the policies in this node to specify the location of the Publishing Server.

- **Reporting** Use the policy in this node to specify the location of the App-V Reporting Server to client devices.
- **Scripting** Use the policy in this node to configure whether scripts defined in the package manifest configuration files should run.
- **Streaming** Use the policies in this node to configure settings related to package streaming.

Notable policies include the following:

- **Publishing Server 1 Settings** This policy is located in the Publishing node. Use it to specify the location of the first publishing server and the properties of that publishing server. There are five publishing server settings policies, so you can configure up to five publishing servers for each App-V client. In each of these policies, you can configure the following publishing server settings:

  - **Publishing Server Display Name** This is the name of the publishing server shown in the App-V client interface.
  - **Publishing Server URL** This is the URL of the publishing server.
  - **Global Publishing Refresh** Use this setting to enable global publishing refresh. This performs a global refresh to update the list of available published applications.
  - **Global Publishing Refresh On Logon** Use this setting to enable a global publishing refresh at logon.
  - **Global Publishing Refresh Interval** When you enable global publishing refresh, you need to specify a frequency. Use the interval setting to specify the refresh interval for global publishing refresh.
  - **Global Publishing Refresh Interval Unit** When you have set the number of units, you need to set the unit itself. You can select either Hour or Day.
  - **User Publishing Refresh** Use this setting to configure user publishing refresh. This refresh occurs on a user basis for the applications published to the user rather than globally.
  - **User Publishing Refresh On Logon** Use this setting to configure user publishing refresh at logon.
  - **User Publishing Refresh Interval** Use this setting to specify the refresh interval for user publishing refresh.
  - **User Publishing Refresh Interval Unit** Use this setting to specify the interval unit, in either hours or days, for the user publishing refresh cycle.

- **Package Installation Root** Use this policy to specify where all new App-V applications and updates will be installed on the client.

- **Shared Content Store (SCS) mode** Use this policy to specify whether streamed package contents are saved to the local hard disk. This policy is useful when you want to grant access to streamed applications but do not want those applications to be available when the client is offline.

- **Specify what to load in background (that is, Autoload)** This policy enables you to specify which packages App-V acquires automatically on a client computer from a publishing server. The options are Previously Used, None, and All. When enabled, the Previously Used option is

the default; previously used applications will be downloaded automatically from the App-V Publishing Server in the background, which increases the speed at which an application loads.

Depending on security concerns, organizations that use the App-V full Infrastructure model and the integrated model might choose to prevent streamed package contents from being saved to the local hard disk by using the SCS Mode policy. For example, you would use this policy if an application needed to be used on a client in an unsecure location where the application should not be stored locally, or if the application should not be accessible when the device cannot connect to the publishing server.

💡 *Exam Tip*

Remember the different App-V models.

🧪 *Thought experiment:* **App-V deployment planning at Contoso**

You are planning the deployment of App-V at Contoso. Your primary interest is the ability to meter application usage and limit the number of concurrent instances of application execution. Contoso does not have a Configuration Manager deployment. With this information in mind, answer the following questions:

1. Which deployment model is suitable for Contoso?

2. Which protocol will clients use to access streamed applications?

Objective summary

- You can deploy App-V by using the full infrastructure, standalone, or Configuration Manager integrated model.
- App-V applications can run only on computers on which a compatible App-V client is installed.
- App-V applications can stream from an App-V server or a Configuration Manager distribution point. This enables the applications to deploy more quickly.
- When sequenced, App-V applications are available in .msi format. You can deploy App-V applications locally in the same manner as you would deploy any other application in .msi format.
- When deploying App-V applications by using Configuration Manager, you can configure the App-V client as a dependency. This means that the App-V client will be deployed if it is not present on the target computer.
- You can use Group Policy to manage App-V settings, but you must import the App-V–related Group Policy template.

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 "" section at the end of the chapter.

1. You have deployed the Configuration Manager integrated model. You want to deploy App-V applications to some of the computers in your organization; however, the App-V client is not installed on every computer that is a Configuration Manager client. The App-V client should be deployed only to computers that need it to run applications. How can you ensure that computers that are subject to an App-V application deployment are able to run those applications?

   A. Deploy the App-V client to all computers.

   B. Configure the App-V client as a dependency for each App-V application.

   C. Configure each App-V application as a dependency for the App-V client.

   D. Configure each computer to subscribe to the RemoteApp feed.

2. You want to ensure that users with laptop computers have access to App-V applications only when they are on site. Which of the following strategies could you pursue to accomplish this goal? (Choose two. Each correct answer provides a complete solution.)

   A. Use the App-V full infrastructure model.

   B. Use the standalone deployment model.

   C. Use the Configuration Manager integrated model.

   D. Use RD Web Access.

3. Which of the following servers must you deploy to support the App-V full infrastructure model?

   A. Management Server

   B. Publishing Server

   C. Configuration Manager site server

   D. Remote Desktop Session Host server

Objective 1.3: Deploy and manage RemoteApp

Session virtualization is the process by which an application or desktop environment runs remotely, but the display of that application or desktop environment occurs locally. The advantage of this approach is that applications that might otherwise require resources the local device might not have, such as an appropriate processor or enough RAM, can be used locally with the processing, memory, and storage resources the back-end infrastructure provides.

This section covers the following topics:

- Application presentation strategies
- Preparing RemoteApp applications
- Group Policy settings

Application presentation strategies

Remote Desktop Session Host servers provide session virtualization and can exist in the form of either a full desktop session or a remote application. The following sections describe these two application presentation methods.

Remote desktops

Remote Desktop Session Host servers (formerly known as Terminal Servers) provide users with access to a full remote desktop experience. In this scenario, users securely connect to the remote session through their local Remote Desktop Connection (RDC) client. From the users' perspective, their desktop environment appears the same, even though it actually is running on a remote server. Users have access to applications in the same way as if those applications were running locally, even though the applications are running on the Remote Desktop Session Host. Each user establishes his or her own private session that does not affect any other users that are connected to the same Remote Desktop Session Host.

To access a remote desktop, the user account (or domain global group) of the connecting user must be added to the Remote Desktop Users group on the computer to which he or she is connecting. By default, this group has no members.

Installing the Remote Desktop Session Host role on a server automatically enables Remote Desktop connections to the local computer. If you do not install the Remote Desktop Session Host role, you can still enable Remote Desktop access to any Windows-based operating system by modifying the system properties to allow remote connections. You can allow remote connections and select the users who can connect remotely by using System Properties in Control Panel.

Remote Desktop is well suited to single-task workers such as point-of-sale terminals or data entry workers. In such scenarios, it is important to provide a consistent desktop experience for all workers. Remote desktops also perform well over limited bandwidth, making this solution suitable for branch offices where IT support might be limited. Another common use for Remote Desktop is to enable users to access their corporate desktop. For example, users can work from home by connecting to their workstations, or users in bring your own device (BYOD) scenarios can connect to a standard operating system environment from their personal devices.

Remote applications

Users access Remote Application (RemoteApp) programs remotely through Remote Desktop Services, but the programs appear as if they are running on the end user's local computer. These applications can appear on the Start menu like any locally installed application. Users can interact with RemoteApp applications in the same manner that they interact with locally installed applications. Running the application on the server avoids compatibility issues that might prevent you from installing the application locally. RemoteApp is suited to applications that you need to manage centrally or that require higher computing requirements than the users' desktops might have—for example, an application that requires large amounts of RAM or one that requires intensive graphics processing. RemoteApp works with Windows clients that include the Remote Desktop software and Windows RT clients on which the Remote Desktop Connection app is installed.

Remote Desktop Web Access

Remote Desktop Web Access (RD Web Access) allows end users to access applications through a special website. RD Web Access provides a secure way to:

- Present remote applications.
- Provide access to remote virtual desktops.
- Connect to a remote computer.

Users can access a secure site, typically at *https://ServerFQDN/RDWeb*, and establish an SSL session between the client and the RD Web Access server. After authentication, users see a list of any applications or desktops that they have permission to use.

Users also see a link to connect to a remote desktop. This link presents a web-based version of the Remote Desktop Protocol (RDP) client where the users can configure devices, resources, and additional options. Users enter the name of the computer to which they want to connect and configure the options they require. Then they have to sign in to the computer to which they are connecting by using a valid user name and password.

For users who do not need a full desktop or users who are not on the corporate network, RD Web Access is an attractive solution because you need to provide users with only the URL of the RD Web Access server. Applications started from this interface are fully functional and save files back to the company network by default, although users can save files to the local computer if required. RD Web Access is suitable for:

- Users outside the corporate network who need to run corporate applications—for example, users who work from home or use laptops in the field.
- Users in remote offices where no VPN is in place.
- Users who need to access corporate applications from a computer in a public location such as a hotel or an airport.
- Kiosk machines that are locked down so that they grant access to only a limited set of applications through the Internet—for example, public access machines that grant any user access to a certain corporate application.

Preparing RemoteApp applications

Before you can make an application available remotely, you must install it on each Remote Desktop Session Host server that will offer that application. Proper planning and installation of the application ensures that your users can access it in a multiuser environment. You can deploy applications that you want to make remotely available only after you have deployed the Remote Desktop Session Host role.

When you are planning a remote application deployment, consider the following factors:

- **Suitability for multiuser environments** This consideration is the most important. Historically, most end user applications have functioned well in a multiuser environment; however, this is not always the case. You must check with the application vendor to see whether a multiuser configuration is supported. Some vendors can provide fixes that enable you to deploy an application in a multiuser environment. If they cannot, you might have to deploy the application to traditional desktops or find another application that can support a multiuser environment.

- **Application compatibility** You have to investigate whether there are compatibility issues with existing applications on the Remote Desktop Session Host server. Ensure that you thoroughly test the proposed application before putting it into the production environment. You might need multiple Remote Desktop Session Hosts so that incompatible applications can be run separately from each other, and you might need multiple session collections to create silos of applications.

- **Application dependencies** Install, on the same Remote Desktop Session Host server, related applications or applications that have dependencies on other local applications. For example, all the applications of an application suite should be installed on the same Remote Desktop Session Host unless otherwise prescribed by the vendor.

- **Capacity requirements** There are no firm numbers that indicate how many clients a single Remote Desktop Session Host server can support. Resource requirements for remotely delivered applications depend on several factors, including the application requirements, the number of concurrent sessions, and how many applications (and other services) the Remote Desktop Session Host is running. Several tools can provide sizing guidance. Server administrators should monitor their server performance closely in Remote Desktop Session Hosts and listen to the feedback end users provide, adding server resources as required. Microsoft offers white papers to assist in capacity planning.

Installing an application on a Remote Desktop Session Host is not like installing an application on a traditional desktop. Remote Desktop Session Hosts operate in two modes, install mode and execute mode. The server must be placed into install mode to install multiuser applications properly. In install mode, Windows ensures that the appropriate registry entries and initialization (.ini) file settings are configured for the application to function in multiuser environments. After the application is successfully installed, the server must be returned to execute mode. You can change the mode of the server in two ways:

- **Use the command prompt** To use the command prompt, from a command prompt, perform these steps:

  A. Use the change user /install command to place the server into install mode.

  B. Install the application.

  C. Use the change user /execute command to return the server to execute mode so that users can access the application.

- **Use Control Panel** The Programs section of Control Panel lists the Install Application On Remote Desktop applet. This applet starts a wizard that automatically puts the server into install mode and then prompts for the location of the application's installation executable file. The administrator installs the application and completes the wizard. This returns the server to execute mode.

Publishing and configuring RemoteApps

The session collection interface in Remote Desktop Management Service (RDMS) provides a link for you to publish RemoteApp programs, or you can publish from the link on the Tasks drop-down menu. Clicking the Publish RemoteApps Programs link starts the Publish RemoteApp Programs Wizard. The wizard presents a list of all the default applications that are available for publishing. Other applications must be mapped by manually adding the path to the executable file that starts the program.

After the applications are published, you can configure them further by editing the application properties:

- Choose whether to show the remote application in RD Web Access. By default, the setting is Yes.
- Create web folders by typing the name of the folder you want to create.
- Assign command-line parameters.
- Restrict access to the remote application to specific users or groups. By default, all users who can access the collection have access to the application.
- Set file type associations for the remote application. File type associations apply only to users who are connected by the RemoteApp and Desktop Connections feed. Users who are connected by RD Web Access cannot use file type associations.

You can also use the Remote Desktop Services PowerShell module to create, update, and delete RemoteApp applications. To publish a new remote application, use the New RDRemoteApp cmdlet. For example, to publish the Windows PowerPoint Viewer application and have it display in RD Web Access, use the following command:

Click here to view code image

```
New-RDRemoteApp  -Alias PPTViewer  -DisplayName PPTViewer  -FilePath "C:\
Program Files(x86)\Microsoft Office\Office14\PPTVIEW.exe"  -ShowInWebAccess True
-CollectionName RemoteApps  -ConnectionBroker LON-SVR1.Adatum.com
```

Managing connections to RemoteApp applications

After a collection is created and RemoteApp applications are added to the collection, a user can connect to the collection and run RemoteApp applications by using the RDC, by signing in to the RDWeb page, or by subscribing to the RemoteApp feed. If users subscribe to the RemoteApp feed, the applications appear on the Start screen of their computer if it is running Windows 8.1 or Windows 8 or on the Start menu of their Windows 7–based computer.

Connecting with RDC

Users can connect to a remote desktop by using the standard RDP client, Remote Desktop Connection (RDC). The user needs to enter the name of the remote computer in the Computer box and then click Connect. If the computer to which the user is trying to connect allows remote access and if the user is in the Remote Desktop Users group for that computer, the user can sign in to that computer. The user will be presented with a desktop just as if he or she were signing in locally. A user connecting in this fashion has access to all the resources of the remote computer just as if he or she were sitting at the local console.

The RDC client has a number of tabs with options that can be configured to control the user experience. These tabs are as follows:

- **General** Provide the name of the computer to which you want to connect and the user name you are using to connect. You can also save this configuration in an RDP file or open an RDP file that might have been provided to you.

- **Display** Configure the resolution and color depth of the remote session.

- **Local Resources** Specify which local resources will be available to the client computer, such as printers, the Clipboard, local drives, and audio settings.

- **Programs** Configure a specific program to start upon connection.

- **Experience** Choose the level of visual quality to transmit to the client computer from the remote computer based on the available bandwidth of the connection.

- **Advanced** Specify how authentication to the server will occur and configure the Remote Desktop Gateway (RD Gateway) settings.

Connecting with the RemoteApp and Desktop Connections feed

Computers running Windows 8, Windows 8.1, Windows RT, and Windows RT 8.1 can subscribe to the Remote Desktop web feed. With the subscription, applications published to the feed are automatically added to the Start screen on the subscribed device.

After the subscription is established, the Remote Desktop web feed is available from the Start screen or Start menu. Users can manually enter the URL to connect to the feed by using the RemoteApp And Desktop Connections applet in Control Panel, as shown in Figure 1-7, or an administrator can configure the default connection URL with Group Policy.
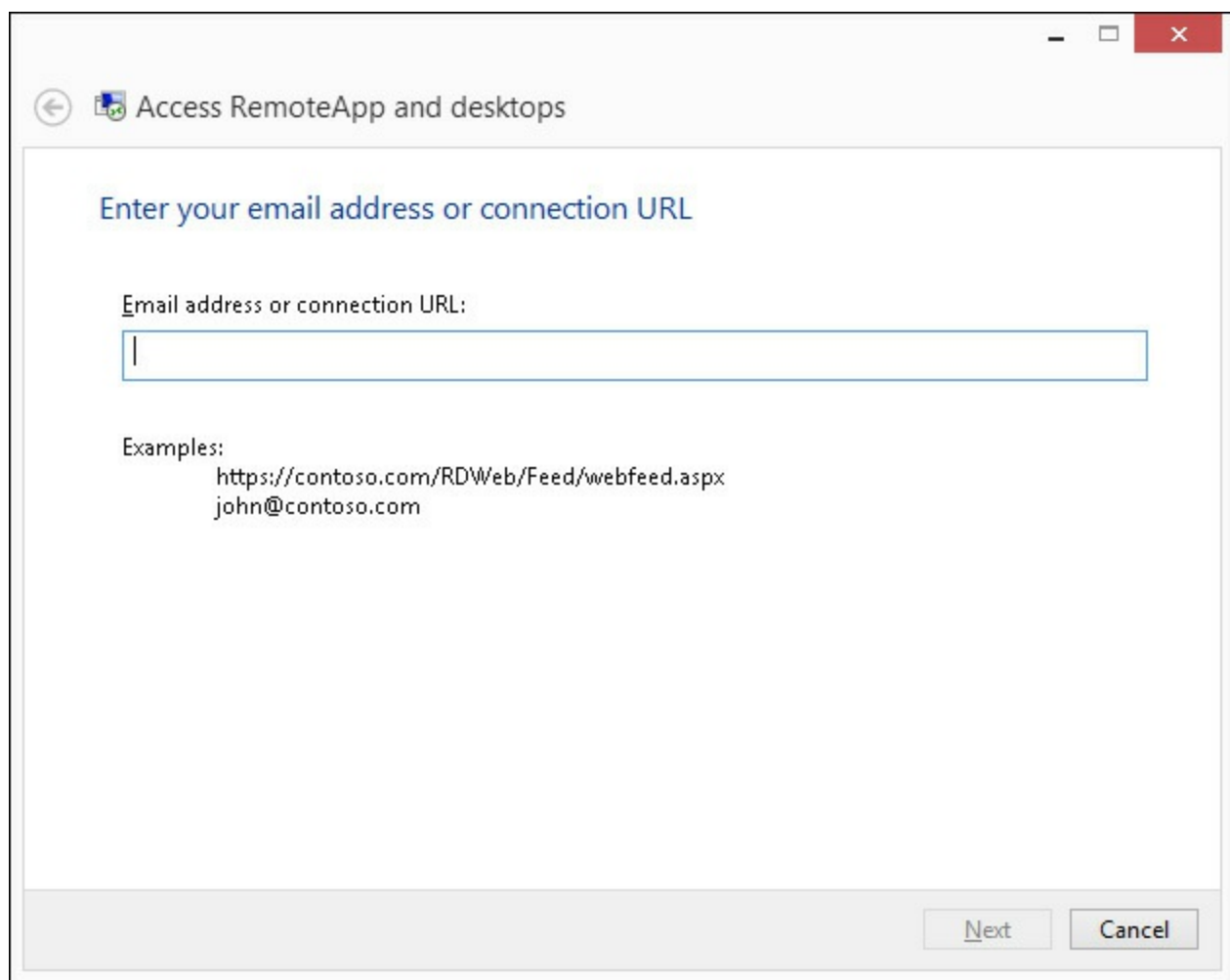
FIGURE 1-7 Access RemoteApp And Desktops dialog box

You can access the feed by using the following URL: *https://<fqdn of rdweb server>/Rdweb/webfeed.aspx*, or users can use their email addresses to subscribe to the feed. If you intend to allow use of an email address to subscribe to the feed, create a TXT record on the DNS server. The record name must be named _msadc, and the text field must contain the URL for the Remote Desktop web feed.

Group Policy settings

In a large organization, it is not practical to configure each remote desktop connection separately. Many Group Policy settings are available to manage the remote desktop or remote application experience for users. After the application presentation method has been determined and the applications have been published, you can use Group Policy to control how the session hosts that house those applications will be accessed. Group Policy enables you to configure settings that can be applied to both users and computers. Many of the same settings appear in both user and computer configurations—for example, session time limits. Typically, if the same settings are configured for both users and computers, the computer setting will override the user setting.

Computer settings

Computer settings affect all users connecting to the remote computer. Computer settings, shown in Figure 1-8, include the following categories:

- **RD Licensing** Control which Remote Desktop Session Host servers are issued Remote Desktop Services client access licenses

- **Remote Desktop Connection Client** Control security aspects of the connection, such as allowing .rdp files or determining whether passwords can be saved
- **Remote Desktop Session Host** Control many aspects of the Remote Desktop Session Host, such as device redirection, limiting the number of connections, user profiles, security, detection of network quality, and session limits
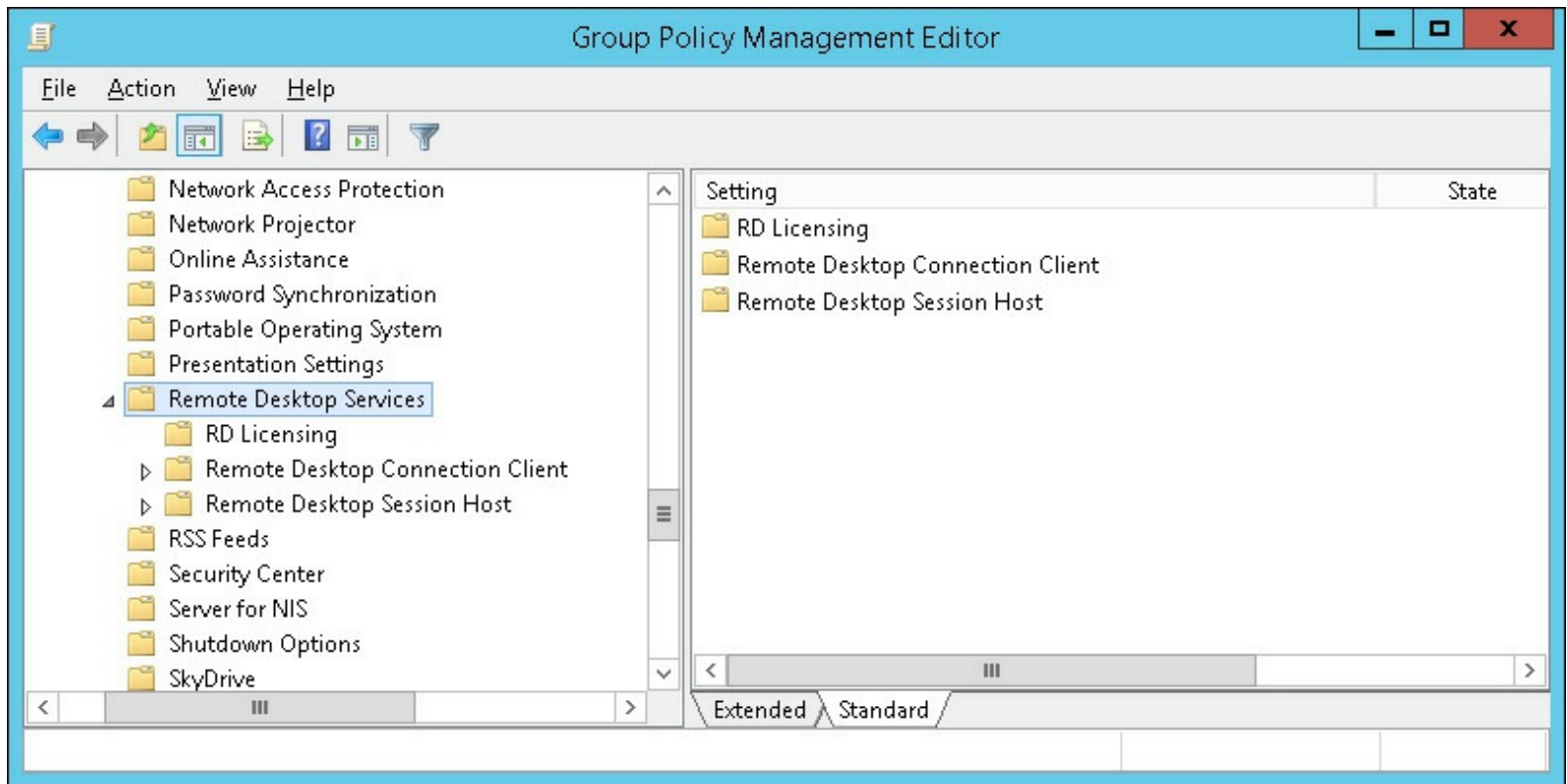
FIGURE 1-8 Remote Desktop Services policies showing computer settings

User settings

User settings are settings for particular groups of users connecting to remote computers. User settings, shown in , include the following categories:

FIGURE 1-9 Remote Desktop Services policies showing user settings

- **RD Gateway** Set the gateway server address and authentication method.

- **Remote Desktop Connection Client** Control .rdp files and the saving of passwords.

- **Remote Desktop Session Host** Control many aspects of the user session, such as device redirection, user profiles, security, and session limits.

- **RemoteApp And Desktop Connections** Specify the default connection URL. This setting is new for Windows Server 2012, and it's particularly useful for distributing the Remote Desktop web feed URL. This Group Policy setting is shown in .
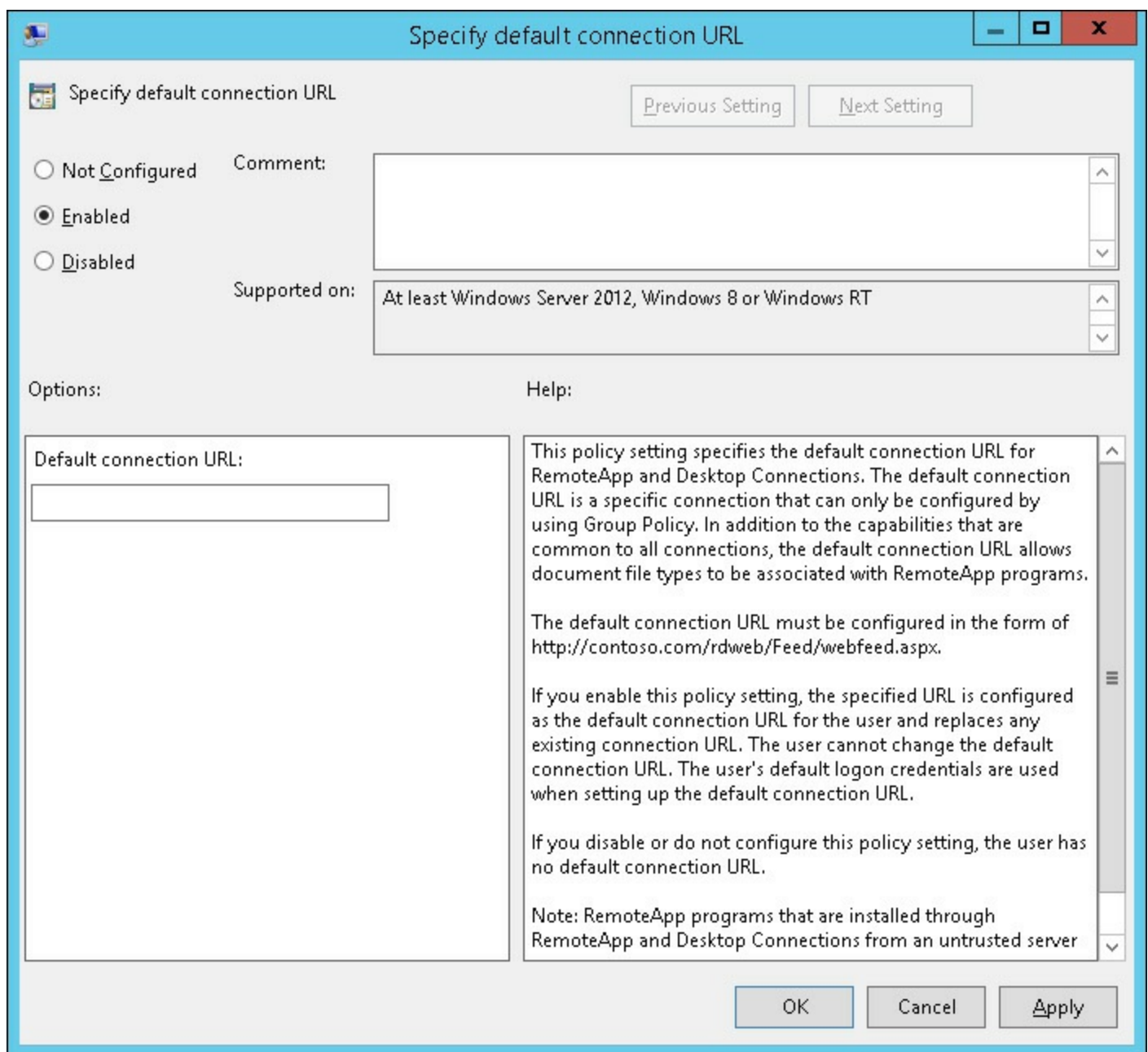
FIGURE 1-10 Specify default connection URL

Remember how to configure a computer running Windows 8.1 or Windows 8 to subscribe to the RemoteApp feed.

> ### Thought experiment: BYOD at Tailspin Toys
>
> **Interns at Tailspin Toys have been given Microsoft Surface 2 devices, which run the Windows RT 8.1 operating system. The Remote Desktop app has been installed on these devices. Interns are to use these devices to run x86 and x64 applications running on a server running Windows Server 2012 R2 with Remote Desktop Services installed.**
>
> 1. **What method could you use to enable an intern to access x86 and x64 RemoteApp applications quickly?**
> 2. **What steps would you take to ensure that RemoteApp applications automatically appeared on the Start screens of the Surface 2 devices the interns use?**

Objective summary

- Remote Desktop enables a user to access a desktop environment remotely that was hosted on another computer where that desktop is displayed on the local device.
- RemoteApp uses the same technology as remote desktop but involves displaying an application that is running on a remote computer on a local device.
- RD Web Access allows users to launch remote desktop sessions and RemoteApp sessions from a specially configured web page.
- Group Policy settings enable you to configure how a remote desktop and RemoteApp are configured.
- Computers running Windows 8.1 and Windows 8 can subscribe to a RemoteApp feed through Group Policy or through an item in Control Panel.

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. What steps can you take to make RemoteApp applications automatically available to users who have computers running Windows 8.1 that are joined to the domain while expending the least amount of administrative effort?

    A. Configure a subscription to the Remote Desktop web feed by using Group Policy.

    B. Configure a subscription to the Remote Desktop web feed by using Control Panel.

    C. Configure the address of the RD Web Access server as the home page in Windows Internet Explorer on each client.

    D. Place shortcuts to each RemoteApp in a shared folder.

2. Which of the following Windows PowerShell cmdlets could you use to create a RemoteApp application?

    A. Remove-RDRemoteApp

B. Get-RDRemoteApp

C. New-RDRemoteApp

D. Set-RDRemoteApp

3. You want to enable users to subscribe to the RemoteApp feed by using their organizational email address from the Control Panel setting on their computers running Windows 8.1. Which of the following steps must you take to prepare DNS to support this configuration?

    A. Create a TXT record named _msadc with the URL for the Remote Desktop web feed in the text field.

    B. Create an MX record with the FQDN for the RD Web Access server

    C. Create an NS record with the FQDN for the RD Web Access server.

    D. Create a CNAME record with the FQDN of the RD Web Access server.

Answers

Objective 1.1

Thought experiment

1. You should sequence the application twice, once for the computers running Windows 7 x86 and once for the computers running Windows 8.1 x64.

2. You should disable the Windows Defender and Windows Search services before sequencing the application on a computer running Windows 8.1 x64.

Objective review

1. **Correct answer:** A

    A. Correct: You should sequence an application on the platform on which you run it. An x64 application can only be sequenced on an x64 version of an operating system.

    B. Incorrect: You cannot use an x86 version of Windows to sequence an x64 application.

    C. Incorrect: You should sequence an application on the platform on which you run it. Even though this might work, it is not the best answer because it is not the platform on which it will be run.

    D. Incorrect: You cannot use an x86 version of Windows to sequence an x64 application.

2. **Correct answers:** A and B

    A. Correct: App-V Connection Groups allow virtualized applications to share data when running on the same computer.

    B. Correct: Virtual environments function in a similar manner to App-V Connection Groups, but they use Configuration Manager rather than an App-V server.

    C. Incorrect: Plug-ins extend the functionality of the application. They don't allow virtualized applications to interact.

    D. Incorrect: A middleware application type enables you to sequence middleware or framework software that another sequenced application package requires.

3. Correct answer: D

    A. Incorrect: You use a connection group when you need applications to share data with each other.

    B. Incorrect: The middleware application type enables you to sequence middleware or framework software that another sequenced application package requires.

    C. Incorrect: You can use the Sequencer to create an add-on or plug-in to extend the functionality of an application.

    D. Correct: Package accelerators automate the sequencing process. They are useful when you need to sequence a particular application frequently.

Objective 1.2

Thought experiment

1. Because you want to use application metering and instance limitation, the full infrastructure model is appropriate.

2. The HTTPS protocol delivers streamed applications to clients.

Objective review

1. Correct answer: B

    A. Incorrect: You should deploy the client only to computers that need it.

    B. Correct: Configuring the App-V client as a dependency will trigger a check to verify that the App-V client is installed before attempting to deploy the application. If the client is not present, it will be installed.

    C. Incorrect: This sequence is reversed. The client should be a dependency for the application.

    D. Incorrect: RemoteApp is not related to the App-V client application.

2. Correct answers: A and C

    A. Correct: You can configure the App-V full infrastructure model so that App-V applications are streamed and not stored in the cache. This means that the application can run only if connectivity can be established.

    B. Incorrect: This model involves local installation and allows offline use.

    C. Correct: You can configure Configuration Manager so that only streaming versions of the app are deployed and configure the cache so that applications are not available offline.

    D. Incorrect: Although it is possible to deploy App-V on a Remote Desktop Session Host server to host virtualized applications, this is not an optimal solution to this situation.

3. Correct answers: A and B

    A. Correct: You need to deploy an App-V Management Server for the App-V full infrastructure model.

    B. Correct: You need to deploy an App-V Publishing Server for the App-V full infrastructure model.

C. Incorrect: You don't need to deploy a Configuration Manager site server for the App-V full infrastructure model.

D. Incorrect: You don't need to deploy a Remote Desktop Session Host server for the App-V full infrastructure model.

Objective 1.3

Thought experiment

1. You could configure RD Web Access. Interns could access the RD Web Access website and use it to launch RemoteApp applications.

2. You would subscribe the Surface 2 devices to the Remote Desktop web feed. RemoteApp applications would automatically be published to the Surface 2 Start screens.

Objective review

1. Correct answer: A

A. Correct: Configuring a subscription to the Remote Desktop web feed by using Group Policy accomplishes the objective with minimum administrative effort.

B. Incorrect: Configuring a subscription to the Remote Desktop web feed by using Control Panel involves substantial administrative effort.

C. Incorrect: Configuring the address of the RD Web Access server as the home page in Windows Internet Explorer on each client involves substantial administrative effort.

D. Incorrect: Placing shortcuts to each RemoteApp in a shared folder involves substantial administrative effort.

2. Correct answer: C

A. Incorrect: The Remove-RDRemoteApp Windows PowerShell cmdlet enables you to remove an existing RemoteApp application.

B. Incorrect: The Get-RDRemoteApp Windows PowerShell cmdlet enables you to view the properties of a RemoteApp application.

C. Correct: The New-RDRemoteApp Windows PowerShell cmdlet enables you to create a RemoteApp application.

D. Incorrect: The Set-RDRemoteApp Windows PowerShell cmdlet enables you to modify an existing RemoteApp application.

3. Correct answer: A

A. Correct: You need to create a TXT record named _msadc with the URL for the Remote Desktop web feed in the text field.

B. Incorrect: You need to create a TXT record named _msadc with the URL for the Remote Desktop web feed in the text field.

C. Incorrect: You need to create a TXT record named _msadc with the URL for the Remote Desktop web feed in the text field.

D. Incorrect: You need to create a TXT record named _msadc with the URL for the Remote

Desktop web feed in the text field.

Chapter 2. Deploy and manage desktop and mobile applications

The ability to manage desktop and mobile applications is one of the main reasons that many organizations deploy System Center 2012 R2 Configuration Manager. Understanding how you deploy and manage software to computers and mobile devices by using Configuration Manager and the cloud-based Microsoft Intune is critical for someone interested in passing the Managing Enterprise Devices and Apps Using System Center Configuration Manager exam.

Objectives in this chapter:

- Objective 2.1: Plan an application distribution strategy.
- Objective 2.2: Deploy applications using Microsoft System Center 2012 Configuration Manager.
- Objective 2.3: Deploy applications using Microsoft Intune.
- Objective 2.4: Plan for application upgrades.
- Objective 2.5: Monitor applications.
- Objective 2.6: Manage content distribution.

Objective 2.1: Plan an application distribution strategy

Configuration Manager provides organizations with a variety of features for comprehensively managing the application life cycle. This includes the ability to manage the process of initial application deployment, application maintenance and monitoring, and application supersedence and removal.

This section covers the following topics:

- Application management by using Configuration Manager
- Applications and packages
- Application management features
- Application management server roles
- Software Center
- Application Catalog

Application management by using Configuration Manager

In System Center 2012 R2 Configuration Manager, you can deploy software by configuring what are termed applications, or you can use the traditional method of configuring what are termed packages and programs. Although they have separate names and function in different ways, both these methods enable you to deploy software to client computers.

Applications contain built-in intelligence, such as the ability to deploy different types of software based on the properties of the client device. Many administrators find packages and programs a more efficient method for running simple commands or running custom scripts on Configuration Manager

clients.

When using packages and programs for software distribution, the process consists of the following elements:

- **Packages** Package objects represent the actual files the targeted client requires to run a program that Configuration Manager deploys. For example, a package could contain the installation files that Configuration Manager uses to install a software application on the client computer. Alternatively, a package might not contain any source files if Configuration Manager only uses it to run an executable that is present on the computers of the members of the targeted collection. When you create a package, you can specify many of its properties, such as the package's name, the location of source files that it contains, and whether it includes one or more programs. For example, you can use the Microsoft PowerPoint Viewer files to create a package.

- **Programs** A program is the command that indicates how to manage the package files. You can create a program only after you create the package in which you define the program. Programs include commands that the client runs during software deployment. For example, a package that you use to install an application will include a program that runs a command, such as Setup.exe, which installs the application. A package must contain at least one program before you can deploy it to clients, but you can create multiple programs for a package. For example, you could create one program that installs an application silently and another program that installs the same application by using an installation wizard. In addition, the program includes information about how the command will run, such as whether user or administrative rights are necessary to run the command, the basic requirements to run the program, and whether another program must be run first.

- **Deployments** Deployments, which are similar to advertisements in prior versions of Configuration Manager, associate a program with a target collection. In addition, deployments specify other options regarding how the source files for a program should be accessed by clients and run. For example, you can configure a software deployment to be available as an optional installation or as a required installation on the client. A deployment also can specify an installation schedule and how a program should run, depending on whether the client's current boundary group has a fast or slow connection to the distribution point. For example, you can specify that the program will not run if the client's boundary group has a slow connection to the selected distribution point. Traditional software distribution uses the following process: packages contain programs, and you use deployments to make the programs available to the collections.

Software deployment also involves a number of other components and concepts:

- **Distribution points** Distribution points are site systems that store the package files, which clients access when running a deployed program. After you create a new package that contains source files, you must distribute the package to at least one distribution point before clients can access it and run any of its programs. Typically, you should place the content on a distribution point that is closest to the clients to which you want to deploy it.

- **Package definition files** You do not always need to create all packages and programs manually. Many software publishers provide package definition files for their applications, which allow for automatic creation of packages and programs. Package definition files specify

a package's properties, such as its name and version, and one or more program definitions. Program definitions in package definition files include the program command and can include other properties such as disk-space requirements and supported client architectures and operating systems.

- **Access accounts** If you need to restrict access to a package, you configure which accounts or groups have permission to access it. By default, administrators have Full permissions, which enable them to perform any action on a package; users have Read permissions.

Applications and packages

Table 2-1 describes the differences between applications and packages based on application management features.

Feature	Application	Package
Basic software information	Options include location of files used in the deployment and some additional deployment settings.	Options include location of files used in the deployment and some additional deployment settings.
Extended software and support information	The application model includes extended information.	This feature is not part of the package model.
Software command options	Deployment types specify: ■ The command to run. ■ The optional Uninstall command. ■ Detection methods. ■ User experience settings. ■ Advanced requirements. ■ Advanced dependency settings.	Programs specify: ■ The command to run. ■ Basic requirements. ■ Basic environment settings. ■ Basic dependency settings. ■ Requirements are contained in query rules for the target collection.
Multiple deployment options	A single application can contain multiple deployment types.	A package can contain multiple programs.
Deployment by	Application.	Package and program.
Deployment option used	The deployment type that Configuration Manager uses is based on requirements, and it determines which to use at run time.	Only one program is available per deployment; all clients in the targeted collection run the same command.
Revision history	Revisions are maintained, and you can revert the application to previous versions.	Revision history is not maintained.
Supersedence	Supersedence enables you to define a replacement relationship between applications.	Packages do not include a similar feature.
Uninstall action	You can deploy applications to install or uninstall an application.	You always deploy packages by using the Install action.
State-based deployment	By using detection methods, the Configuration Manager client can determine the state of an application in relationship to its action and purpose and then perform the appropriate actions if necessary.	Packages do not include a similar feature.

TABLE 2-1 Applications and packages

There is some additional information that you can include in an application and not in a package. This information includes:

■ General information, including administrative categories, date published, owners, and support contacts.

- Application Catalog information, including localization information, keywords, and user categories that help users search in the Application Catalog and user documentation.
- Relationship information between the application and other applications.

You will typically use applications to deploy software because of the advanced deployment options and monitoring features that they provide. Put another way, applications are the method you should use going forward, even though you might still need packages to support the way you performed software deployment in the past. The exception to this generalization is scripts. You are likely to use packages to deploy software when working with:

- Scripts that do not install any software on the computer, such as a script to restart a number of services in a specific order. These scripts typically do not have any detection methods that can determine their state.
- Scripts that will run only once. These scripts will be part of an operating system deployment, and you do not need to monitor them continually.

There are other methods, such as Group Policy Preferences, that you can also use to run scripts on computers, but packages remain the best way to run scripts on a computer if you want to perform that task by using Configuration Manager.

Exam Tip

Using a package is the best way to accomplish the goal of running a script by using Configuration Manager.

Application management features

Application management uses the following Configuration Manager features:

- Requirements
- Global conditions
- Detection methods
- Supersedence
- Deployment action and purpose
- State-based deployment
- User device affinity
- Monitoring

These features are described in the following pages.

Requirements and global conditions

Global conditions enable you to set conditions you can use to create requirements in a deployment type to determine whether the deployment type is suitable for a particular user or client device—for example, whether the computer is the user's primary device. Several global conditions are already defined in Configuration Manager, and you can create more as necessary.

A requirement is a global condition with an operator and a value that is associated with a

deployment type. Configuration Manager evaluates application requirements on a schedule to determine whether the deployment type is applicable to the clients in a targeted collection.

Detection methods

Detection methods enable you to define how Configuration Manager determines an application's installation state. Detection methods can query many aspects of the client operating system, including the file system and registry. For example, a detection method to determine whether an application is installed would involve checking for a specific registry key and value.

Supersedence

Supersedence enables you to configure a relationship between a new application and an existing application that you have deployed. After you configure supersedence, all future deployments and Application Catalog requests receive the new application.

Deployment action and purpose

When you deploy an application in Configuration Manager, you choose a deployment action and a deployment purpose that define what the deployment should do. Together, the deployment action and the deployment purpose represent your intent for the application.

The available deployment actions are:

- **Install** This action specifies that the deployment will install the application.
- **Uninstall** This action specifies that the deployment will uninstall the application.

The possible deployment purposes are:

- **Available** If you deploy the application to a user, the user sees the published application in Application Catalog. If you deploy the application to a device, the user sees it in Software Center.
- **Required** If you deploy the application to either a user or a device, the application is deployed automatically according to the schedule you have configured. However, you can allow a user to install the application before the deadline by using Software Center.

When you specify the user-targeted deployment purpose as available, you can specify whether users need to request approval from an administrator before they can install the application. After an administrator provides approval, which can be done from the Configuration Manager console, the application will install.

State-based deployment

The Configuration Manager client periodically reevaluates the state of deployed applications to verify that the current state matches the deployment purpose. For example, if an application has been deployed as required and the user has uninstalled it, Configuration Manager will reinstall the required application. Similarly, if a required deployment uninstalls an application and the user reinstalls it, Configuration Manager will uninstall the application during the evaluation cycle.

User device affinity

User device affinity enables a user to be associated with one or more specific devices. You can use this feature to deploy applications to the user and ensure that the application is installed on only those specific devices with which the user is associated. For example, you can ensure that an application is installed on the user's primary device rather than on any other device he happens to sign on to. You can use user device affinity to predeploy software on a user's device even when the user is not logged on. You are most likely to use user device affinity as a requirement when configuring a deployment type.

Monitoring

An important aspect of the application management process is to monitor deployments for success or failure. Monitoring can involve several activities, including:

- Examining status in the Monitoring workspace.
- Reviewing application management reports.
- Reviewing status messages.
- Examining log files.

Application management server roles

Server roles that assist in application management include the Application Catalog web service point, Application Catalog website point, and the reporting services point.

Application Catalog

Application Catalog enables users to select and install applications automatically by placing requests in a portal, which administrators can approve for installation, or, if specially configured, allow installation to occur.

You can implement Application Catalog by using the following two site roles:

- **Application Catalog Web Service Point** This role provides software information from the software library. As an administrator, you configure this information for each application that publishes in the catalog.
- **Application Catalog Website Point** This role is the web interface for end users. Users can use this portal to view the list of available applications and request and install applications.

When planning for Application Catalog, you should keep in mind that:

- Application Catalog is a hierarchy-wide role. Typically, in a hierarchy with multiple primary sites, you install one instance of each role in each primary site, although multiple instances are supported.
- You cannot install Application Catalog in a secondary site or on a central administration site, only in a primary site.
- Application Catalog enables users to install deployed applications or request available applications, which deploy after approval.
- Application Catalog enables users to configure some preferences and wipe their mobile devices that are being managed through Configuration Manager.

- You can integrate Application Catalog with Microsoft SharePoint.

Reporting services

The reporting services point is a site system that you install on a server that is running Microsoft SQL Server Reporting Services (SSRS), which provides advanced reporting capabilities and authoring tools for building reports. Use this server role to generate reports related to application management.

You can run reports from the Configuration Manager console or directly from the reporting services point website. You can save reports in a variety of formats. In addition to running reports manually, the reporting services point supports report subscriptions, which are recurring requests to deliver reports at specific times or in response to events. In the subscription, you can specify the application file format of the report.

When you are planning for the reporting services point, consider the following:

- You must install the reporting services point on a computer that is running the same version of SSRS as that of the site database.
- Each SSRS instance can support one site only.
- You can install multiple reporting services points in your hierarchy.
- If you install a reporting services point in a primary site, the reports show the data collected from that site. However, reports that you run on a reporting services point in the central administration site return data collected from the entire hierarchy.

Software Center

Software Center is a tool used for installing and monitoring software deployments targeted to devices. Software Center is installed as part of the Configuration Manager client. Figure 2-1 shows Software Center.
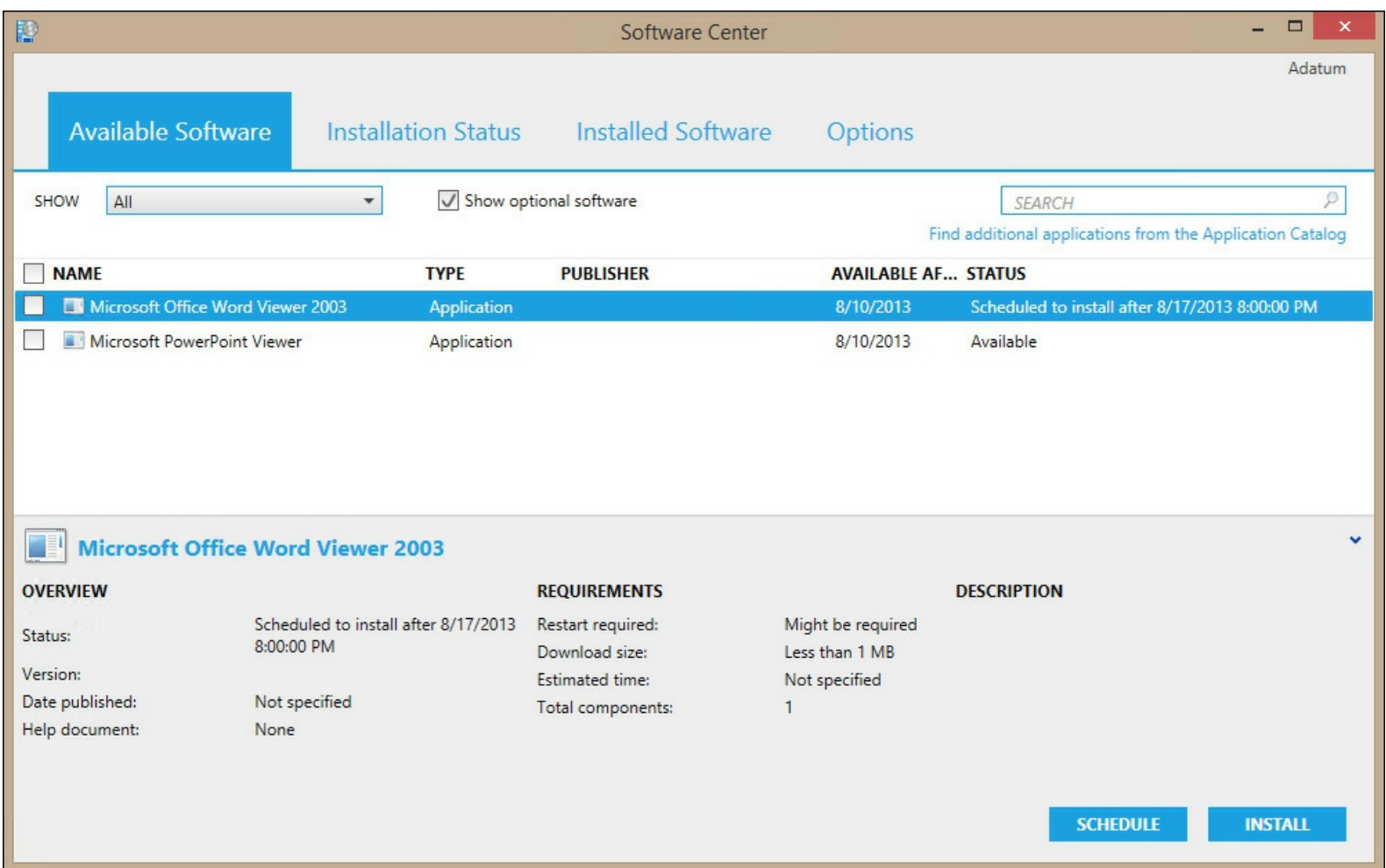
FIGURE 2-1 Software Center showing available software

Software Center provides users with some control over how and when software installs on their devices. Users can perform the following actions by using Software Center:

- Install software that has been deployed as Required to a user collection of which they are members if the deployment deadline has not passed and they are allowed to do so.

- Install software that has been deployed as Available to a device-based collection of which the system is a member.

- Monitor the status of deployed software. The statuses include Available, Install After, Installing, Installed, or Failed.

- Retry an installation that has failed.

- Uninstall installed software if you configure an uninstall command on the application and do not require the software.

- Manage their personal settings. On the Options tab, users can configure the following settings, provided the policies set in the applicable client settings allow them to do so:

  - **Business Hours And Days** Users can configure their business hours and days and configure settings so their systems do not install software during business hours.

  - **Computer Maintenance** Users can configure a setting to allow the required software to deploy only outside their business hours. In addition, they can configure a setting to suspend Software Center activity while in the presentation mode.

  - **Power Management** Users can specify whether this computer will use the power management policies that have been configured through Configuration Manager.

- **Remote Control** Users can specify the level of remote control allowed or whether administrators must ask permission before obtaining remote control or other related settings.

Application Catalog

Application Catalog is an optional component you can install for both intranet-based clients and Internet-based clients. It functions as a self-service catalog from which users can request software for installation.

Application Catalog uses two roles: the Application Catalog Web Service Point and the Application Catalog Website Point roles. The Web Service Point role communicates with the site server to retrieve application information. The Website Point role is the interface for Application Catalog, and this role depends on the Web Service role. When users connect to Application Catalog, the Website Point role passes requests and other communications to the Web Service Point role, which in turn passes those communications to the site server.

You can customize the look of the Application Catalog website by using the Application Catalog website point Properties dialog box. A user can navigate to the Application Catalog website directly. Alternatively, Software Center provides a link to Application Catalog when you configure the Default Application Catalog website point in the applicable client settings.

Users can use the Application Catalog website point to:

- Find available software.
- Specify primary devices.
- Manage available applications. On the Application Catalog tab, users can:
    - Search or browse Application Catalog for available software.
    - Install software available to a user-based collection of which they are members.
    - Request software that requires administrator approval.
- Monitor the status of software requests on the My Application Requests tab.
- Manage their primary devices. On the My Devices tab, users can:
    - Designate the current system as a primary device.
    - Manage their mobile devices. Users can view the status of their mobile devices and wipe them remotely if necessary.

More Info: **Application Catalog and Software Center**

You can learn more about Application Catalog and Software Center at ***http://technet.microsoft.com/en-us/library/hh489603.aspx***.

Software distribution to mobile devices

Integrate Configuration Manager with Microsoft Intune to deploy and manage devices that are running Windows Phone 8, Windows RT, Apple iOS, and Android operating systems. You integrate Configuration Manager with Intune by using the Intune connector, which acts as a gateway between Configuration Manager and Intune. In this method, the mobile devices connect to the cloud to receive configuration information and software. Only System Center 2012 R2 Configuration Manager and System Center 2012 Configuration Manager Service Pack 1 (SP1) support this method.

Users can perform self-enrollment by using Company Portal, which is an app Microsoft publishes and is available in the following locations:

- The Apple App Store for iOS devices
- The Google Play store for Android devices
- The Windows Store for Windows devices

Thought experiment: **Configuration Manager at Wingtip Toys**

You are planning the use of Configuration Manager for software deployment at Tailspin Toys. You want to run a command from the C:\Windows\System32 folder on all of the 15,000 Configuration Manager clients in your organization but to do so only once. You also want to ensure that the App-V version of an application is deployed only on computers that are not a user's primary device. With this information in mind, answer the following questions:

1. **What's the best way to get Configuration Manager to run the command?**
2. **What's the best way to ensure that the App-V version of the application is deployed correctly?**

Objective summary

- In System Center 2012 R2 Configuration Manager, you can choose to deploy software by configuring what are termed applications, or you can use the traditional method of configuring what are termed packages and programs.
- Applications contain built-in intelligence, such as the ability to deploy different types of software based on the properties of the client device.
- Package objects represent the actual files the targeted client requires to run a program that Configuration Manager deploys.
- A program is the command that indicates how to manage the package files.
- Deployments associate a program with a target collection.
- Distribution points are site systems that store the package files, which clients access when running a deployed program.
- Global conditions enable you to set conditions that you can use to create requirements in a deployment type to determine whether the deployment type is suitable for a particular user or

client device.

- Detection methods enable you to define how Configuration Manager determines an application's installation state.
- Supersedence enables you to configure a relationship between a new application and an existing application that you have deployed.
- The available deployment actions are Install and Uninstall.
- The possible deployment purposes are Available and Required.
- User device affinity is the process of associating a user with one or more specific devices.
- Software Center is a tool used for installing and monitoring software deployments targeted to devices.
- Application Catalog functions as a self-service catalog from which users can request software for installation.
- Integrate Configuration Manager with Intune to deploy and manage devices that are running Windows Phone 8, Windows RT, Apple iOS, and Android operating systems.

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 of the following Configuration Manager features is used to determine whether an application has already been installed on a computer?

    A. Detection method

    B. Supersedence

    C. User device affinity

    D. Application Catalog

2. Which of the following Configuration Manager features enables end users to request software they can, after approval, deploy to their computers?

    A. User device affinity

    B. Application Catalog

    C. Supersedence

    D. Detection method

3. Which of the following Configuration Manager features would you use if you wanted to target a deployment so that a particular application was installed only on a user's primary computer?

    A. Detection method

    B. Supersedence

    C. Application Catalog

    D. User device affinity

4. Microsoft Word 2010 is deployed on all computers in your organization. You want this version

of Word to replace Microsoft Word 2013 automatically. Which of the following Configuration Manager features would you employ to accomplish this goal?

- **A.** User device affinity
- **B.** Application Catalog
- **C.** Supersedence
- **D.** Detection method

Objective 2.2: Deploy applications using Microsoft System Center 2012 Configuration Manager

This objective deals with deploying applications to clients by using Configuration Manager. It covers how you can create applications; perform application deployment; and configure detection methods, dependencies, global conditions, requirements, and user device affinity.

This section covers the following topics:
- Application creation
- Application deployment
- Detection methods
- Dependencies
- Global conditions
- Requirements
- User device affinity
- Deploy Software Wizard
- Simulated deployments

Creating applications

You can create applications in Configuration Manager by using the Create Application Wizard. Access this wizard by navigating to the Applications node in the Application Management folder in the Software Library workspace and then clicking Create Application in the shortcut menu or on the ribbon. When creating an application, you can set the wizard to detect settings automatically from the installation files or use the wizard to create the application manually.

When using the Create Application Wizard to create an application from an installation file, the wizard reads the installation files from the standard deployment types and automatically populates several fields for the application. The Create Application Wizard can read the same installation files as the Create Deployment Type Wizard except that it does not display a separate Script Installer option. When creating an application from a script, you select Manually Specify The Application Information in the Create Application Wizard on the Specify Settings For This Application page.

Automatic detection of settings

When you create applications, you select the type of application you will create on the Specify Settings For This Application page of the Create Application Wizard—for example, Windows-based, such as Windows Installer (*.msi file) or Microsoft Application Virtualization 5, or mobile-based, such as the Windows Phone app package. After specifying the type, specify the location of the installation file to be imported.

Depending on the imported file, some of the application information will be read from the file. You can add to or modify the existing information. After completing the wizard, you can customize the application with requirements and other information.

Modifying application settings

Table 2-2 lists application settings that you can modify after creating an .msi-based application.

Tab	Settings
General Information	The settings that you can modify on this tab are: ■ **Name** You can modify the name of the application. ■ **Administrator Comments** You can modify any comments for administrators. ■ **Publisher** You can modify the name of the software manufacturer. ■ **Software Version** You can modify the software version. ■ **Optional Reference** This is an optional field. ■ **Administrative Categories** You can modify these categories that help administrators locate content in the Configuration Manager console. ■ **Date Published** You can use this setting to specify a date on which the application was published. ■ **Allow This Application To Be Installed From The Install Application Task Sequence Action Without Being Deployed** You can select this check box when you want to use the application in a task sequence such as an operating system deployment task sequence. ■ **Owners** You can modify the owners of the application. ■ **Support Contacts** You can modify the support contacts for the application.
Application Catalog	The only setting that you can modify on this tab is Selected Language. The following options are configurable for each language installed and apply to the language selected. (The users can view all these options in Application Catalog.) ■ **Localized Application Name** This option displays the name the users will see. ■ **User Categories** Use this option to specify categories that the user can use to filter applications in Application Catalog. ■ **User Documentation** Use this option to specify a URL for accessing user documentation. ■ **Link Text** Use this option to add a descriptor to the documentation link.

	- **Privacy URL** Use this option to specify a URL to access company-specific privacy information.
	- **Localized Description** Use this option to specify a description for the application.
	- **Keywords** Use this option to add keywords for users to use when searching Application Catalog.
	- **Icon** Use this option to specify an application icon.
	The language in Internet Explorer determines the language displayed when a client connects to Application Catalog.
References	You can use the Relationship Type drop-down list on this tab to view:
	- Applications That Depend On This Application.
	- Applications That Supersede This Application.
	- Virtual Environments That Contain This Application.
Distribution Settings	The settings that you can modify on this tab are:
	- **Distribution Priority** You can use this drop-down list to set the priority for sending the package to other sites and distribution points in the same site.
	- **Distribute The Content For This Package To Preferred Distribution Points** If you select this check box, when a client requests this content and it is not available on any of its preferred distribution points, the content will be distributed automatically to the client's preferred distribution points.
	- **Prestaged Distribution Point Settings** This section provides three options for copying content to distribution points that are configured to support prestaged content:
	- **Automatically Download Content When Packages Are Assigned To Distribution Points** You can use this option for smaller applications, such as Silverlight, that are only a few megabytes in size, where bandwidth limitations will not affect their distribution.

	■ **Download Only Content Changes To The Distribution Point** You can use this option for applications that are quite large but receive small updates. For example, Microsoft Office is an application with an initial size of more than 700 megabytes (MB), and it receives small software updates. ■ **Manually Copy The Content In This Package To The Distribution Point** You can use this option for large packages, such as Office 2013, or for situations in which bandwidth limitations are a concern. With this option, the Configuration Manager distribution manager process will never send the application to the remote distribution point.
Deployment Types	This tab displays the currently configured deployment types and enables you to manage the existing deployment types or add new deployment types.
Content Locations	The Distribution Points or Distribution Point Groups dialog box displays the distribution points and distribution point groups that have the application content.
Supersedence	The Supersedence tab displays the applications that this application supersedes. You can add, edit, or remove supersedence relationships by using this tab.
Security	The Administrative Users section displays the user or groups that have administrative rights to the application.

TABLE 2-2 Application settings

Application deployment

The software deployment process in Configuration Manager consists of determining the users or devices to which you want to deploy the application and the way you want to present the software. The deployment can be deployed automatically (required), presented in Software Center (available to devices), or deployed from Application Catalog (available to users).

You can deploy applications to either user collections or device collections. To deploy an application, select the application and then, on the shortcut menu or ribbon, click Deploy. This launches the Deploy Software Wizard.

By default, the installation behavior on a Windows Installer (*.msi file) deployment type is set according to the information in the .msi file. When using the Install For System If Resource Is Device; Otherwise Install For User Deployment Type on the User Experience tab, there are some differences between deploying to a user and deploying to a device.

Table 2-3 describes these differences.

Install for system if resource is device; otherwise install for user	Deploying to users	Deploying to devices
Software deployed as Required that is at the deadline or beyond	The software is installed automatically and silently.	The software is installed automatically and silently.
Software deployed as Required prior to the deadline	The targeted user can start the installation from Software Center.	Any user of the device can start the installation from Software Center.
Software deployed as Available	The user can request it from Application Catalog. This might require administrator approval.	Any user of the device can start the installation from Software Center.
Deploy software without requiring a user to log on	This option installs the software only on a user's primary device, if present.	You can use this option to install software on any device.
Who can use the software	The user or users to whom the software was deployed can use it.	Everyone using the device can use the software.

TABLE 2-3 Deployment type differences

Software types

The Application Management feature supports different kinds of software, including Windows-based software and mobile device software. You can perform multiple actions with software through System Center 2012 R2 Configuration Manager, including installing standard installations, performing custom installations, installing virtualized applications, and uninstalling software. Each installation method that you define is classified as a deployment type.

Applications contain deployment types, which in turn contain information about the files, commands, and programs used to install or uninstall software by using a particular method or command.

When creating a new deployment type, the Create Deployment Type Wizard reads the installation files from the standard deployment types and automatically populates several fields based on the deployment type. System Center 2012 Configuration Manager and newer versions work with many of the application packages available for installation on computers and mobile devices. The installer files in each of these software packages include all the information required to install the software. Figure 2-2 shows the list of supported automatic installation method detection types.

FIGURE 2-2 Deployment type settings

The Create Deployment Type Wizard uses the following standard installation files to create the application and initial deployment type:

- **Windows Installer (*.msi File)** This deployment type creates an application from a Windows Installer file.

- **Windows App Package** This deployment type uses Windows Store apps (.appx files).

- **Windows App Package (In The Windows Store)** This deployment type enables you to deploy applications directly from the Windows Store. This requires the users to have a valid account for the Windows Store.

- **Script Installer** This deployment type creates custom applications. For example, you use this deployment type for *.exe files or to deploy installation scripts.

- **Microsoft Application Virtualization 4** This deployment type creates an application from a Microsoft Application Virtualization 4 manifest (.xml) file.

- **Microsoft Application Virtualization 5** This deployment type creates an application from a Microsoft Application Virtualization 5 package (.appv) file.

- **Windows Phone App Package (*.xap File)** This deployment type creates an application by using a Windows Phone app package (.xap) file.

- **Windows Phone App Package (In The Windows Phone Store)** This deployment type creates an application deployment based on a link to the application in the Windows Phone Store.

- **Windows Mobile Cabinet** This deployment type creates an application from a Windows Mobile Cabinet (.cab) file for supported Windows-based mobile devices.

- **App Package For iOS (*.ipa File)** This deployment type creates an application from an app package for Apple iOS (.ipa) file.

- **App Package For iOS From App Store** This deployment type creates an application by specifying a link to the app in the App Store.

- **App Package For Android (*.apk File)** This deployment type creates an application from an

app package for an Android (.apk) file.

- **App Package For Android On Google Play** This deployment type creates an application by specifying a link to the app on Google Play.
- **Nokia SIS File** This deployment type creates an application from files that are in Symbian Installation System (sis or sisx) format for supported Nokia Symbian–based mobile devices.
- **Mac OS X** This deployment type creates an application from a Mac OS X Installer (.cmmac) file that was created by using the CMAppUtil tool.
- **Web Application** This deployment type creates a shortcut on a user's device to the web application.

Manual information entry

You can enter information manually into a deployment type or import a file that contains information to the deployment type. A deployment type can include the following information:

- General information about the deployment type, including the name of the deployment type, the technology the deployment type uses, and all the languages the deployment type supports
- Location of any content that the installation requires and the expected behavior when communicating with a distribution point
- Installation commands and uninstall commands
- Detection method used to determine whether the application is installed on a client device
- User experience settings, including installation behavior and visibility
- Requirements that must be met for the deployment type to install
- Return codes used to determine whether a restart is required, the installation is complete, or any other events you want to communicate to the user
- Dependencies—additional deployment types from a separate application—that this deployment type requires

Considerations when deploying to Mac computers

Deploying applications to supported Mac computers is similar to deploying applications to computers that are running Windows operating systems. However, due to the differences in the platforms, consider the following:

- You must package Mac OS X applications by using the CMAppUtil tool on a Mac computer. This renders them in a format that System Center 2012 R2 Configuration Manager can read.
- You can deploy Mac OS X applications only to devices, not to users.
- Mac OS X applications support simulated deployments.
- You cannot deploy Mac OS X applications as Available.
- You cannot send wake-up packets to Mac OS X computers to start a deployment.
- Mac OS X computers do not support Background Intelligent Transfer System (BITS).
- Mac OS X deployments do not support global conditions. However, they do support requirements such as operating system.

Using deployment types

To create a new deployment type in an existing application, open the application's Properties dialog box, click the Deployment Types tab, and then click the Add button. The Create Deployment Type Wizard opens, and you can select the deployment type you are creating. You can choose Automatically Identify Information About This Deployment Type From Installation Files or Manually Specify The Deployment Type Information.

When retrieving the information from an installer file, you import the required information and possibly some optional information. You can edit the deployment type afterward to supply additional optional information or modify the imported information.

When creating a deployment type manually, you must supply all required information in addition to any optional information. For example, when you work with the Windows Installer (*.msi file) deployment type, you can use:

- **Automatic creation** The required fields and some optional fields are populated automatically. They usually include Name, Installation Program, Installation Behavior, Detection Method, and Uninstall Program. The Detection Method and Uninstall Program fields do not appear in the Create Deployment Type Wizard. Additional information that you can provide in the wizard includes Requirements and Dependencies.

- **Manual creation** You must specify Name, Installation Program, and Detection Method. Additional information that you can provide in the wizard includes Uninstall Program, Requirements, Dependencies, and User Experience settings.

The following list describes the sections in the Create Deployment Type Wizard and considerations to keep in mind when configuring them.

- **General** Contains basic information about the deployment type, including the name and type of deployment. You can add additional information as reference information for the Configuration Manager administrators.

- **Content** Contains information about the source files and how this deployment type will use them. If you are creating a deployment type for files that already exist on the client devices, you need not specify the content location.

- **Programs** Contains information about the install and uninstall commands in this deployment type. There are some optional fields to ensure that applications install correctly and enable Windows source management.

- **Detection Method** Contains information about how the success of an installation will be determined. You must specify at least one detection method. For complex installations, you can create a script to detect the installation.

- **User Experience** Contains information about how the user will view and interact with the deployment.

- **Requirements** Contains the conditions that will determine whether to install this deployment type.
- **Return Codes** Contains the codes the program will return when it finishes running. Return codes can indicate successful installation, failed installation, or some other condition such as when the installation process requires a restart.
- **Dependencies** Contains information about the deployment types you must install before you can install this deployment type. You can configure the dependencies to be autoinstalled during a deployment.

Detection methods

A detection method is a procedure that enables the deployment process to determine whether an application is present on a system. Detection occurs before the content is installed and at regular intervals afterward and provides the following functions:

- Preventing Configuration Manager from reinstalling the application needlessly
- Reinstalling a required application that the user has uninstalled, for example, through Control Panel
- Determining whether an application is present before running a deployed uninstall command

When you create an application by using one of the automatic methods, Configuration Manager creates a detection method based on the installer file used to create the application. Generally, this is sufficient for most deployments. However, when you create a deployment type manually or when you need more refinement, you can create enhanced detection methods.

To create a new detection method, open the properties of the deployment type that you wish to modify, click the Detection Methods tab, and then click Add Clause. There are three types of detection rules in the Detection Rule dialog box:

- **File System** You can detect an application based on the existence of a specific file or folder. You can also create a detection method that uses the Date Modified or Date Created properties for either a file or folder, or the Version or Size properties for a file.
- **Registry** You can detect an application by searching in any of the registry hives for the existence of a specific key or value. You can also refine this detection method by specifying a value for comparison.
- **Windows Installer** You can detect an application by using the Windows Installer database of installed applications. You can base this detection method on the existence of a specific product code, or you can specify values for comparison of the Version property or the Upgrade Code property.

You can create multiple detection rules in a single detection method and use either the AND or the OR operator to connect them. In addition, you can group detection methods to make complex detection methods.

Finally, instead of using the detection methods, you can create a Windows PowerShell, Microsoft Visual Basic Scripting Edition (VBScript), or JScript script to detect an installed application.

Dependencies

Dependencies define one or more applications that must be installed before you run a specific deployment type. You can configure dependent applications to install automatically before a deployment type installs.

Dependencies are application deployment types that are added as a prerequisite for another application's deployment type. For example, assume that you have a custom application that requires installation of a particular run time before the application installs. In this case, you would create an application with the appropriate deployment type, which installs the run time as a dependency on the custom application.

When defining a dependency, you create dependency groups. All dependent applications are in one or more dependency groups. When you choose to allow dependent applications to install automatically, each application in the group attempts to install in the order that the group specifies, until one of the dependencies from the group is installed.

When creating a dependency, be careful not to create a circular reference, because then the installation process will not install the applications.

Global conditions

Global conditions define the attributes that Configuration Manager evaluates to determine whether a deployment type applies to a particular user or device. However, they do not define the particular values for which you are checking. You use global conditions to build requirements that will contain the values for which you are checking. You can use the predefined global conditions to define a requirement within any applicable deployment type; however, you cannot modify the predefined global conditions. There are two categories of predefined global conditions for both mobile and Windows-based device types: User and Device.

Table 2-4 lists the predefined global conditions and the requirements for which you should use them.

Category	Predefined global condition	When would you use this?
User	Primary device	Is this device a primary device for the targeted user?
Device	Active Directory site	Does this device belong to one of the listed Active Directory Domain Services (AD DS) sites?
	Operating system	Is this device running one of the listed operating systems?
	Total physical memory	Does this device meet the defined memory requirement?

TABLE 2-4 Global conditions

If the predefined global conditions do not meet your needs, you can create custom global conditions. Administrator-created global conditions allow for a high level of customization. You can create global conditions for Windows-based devices, Windows Mobile–based devices, and Nokia devices. The available settings vary depending on the type of global condition you are creating.

Examples of custom global conditions include:

- Checking for a registry setting on a device.
- Checking for a specific configuration of an application that the registry defines.
- Verifying that a specific .NET assembly is available.
- Verifying an application version for an upgrade.

To create custom global conditions, in the Software Library workspace, in the Global Conditions node, click Create Global Condition.

When you create a Windows-based global condition, you can check several aspects of Windows-based computers. Table 2-5 describes the setting types you can configure for evaluation of applications to Windows-based computers.

Setting type	Description
Active Directory Query	Use this type to construct a query that finds values in AD DS.
Assembly	Use this type to specify an assembly from the global assembly cache to assess as a global condition.
File System	Use this type to specify a file or folder to assess as a global condition.
IIS Metabase	Use this type to specify the Internet Information Services (IIS) metabase setting to assess as a global condition.
Registry Key	Use this type to specify a registry key to assess as a global condition.
Registry Value	Use this type to specify a registry value to assess as a global condition.
Script	Use a discovery script to find and return a value from the target system.
Structured Query Language (SQL) Query	Use this type to specify a Structured Query Language (SQL) query to assess as a global condition.
WQL Query	Use this type to specify a Windows Management Instrumentation (WMI) Query Language (WQL) script to assess as a global condition.
XPath Query	Use this type to specify the XML file path and XML Path Language (XPath) query to assess as a global condition.

TABLE 2-5 Conditions

Requirements

Applications in System Center 2012 R2 Configuration Manager and newer versions support using multiple deployment types in each application. This is similar to a package containing multiple programs. However, there are several differences. When you deploy a package and program to a collection, the program will attempt to run on every member of the collection. Deployment types have intelligence in the form of detection methods, dependencies, and requirements that are not available with programs. This difference means that deployment types run the installation software only on clients whose installation meets all the specified criteria and, therefore, is more likely to be successful.

With applications, you deploy the application and not the deployment types. When clients receive a policy that includes an application deployment, the clients use the requirements in the deployment

types to determine the deployment type, if any, that they will use. You can create multiple deployment types of the same type, such as a suite deploying different combinations of programs, depending on the department to which the user belongs.

When you deploy an application with multiple deployment types, the application-deployment evaluation cycle evaluates requirements for each deployment type for the target device or user. After the target device or user satisfies the requirements for a deployment type, no other deployment types are evaluated, and Configuration Manager uses the satisfying deployment type. If the target device or user cannot satisfy the requirements for any of the deployment types, the application does not attempt to run. When this happens, the status shows that the device has not met the requirements of the application.

When there are multiple deployment types and the target device or user could match the requirements for more than one deployment type, application installation occurs using the highest-priority deployment type. When using multiple deployment types in an application, you must be sure to set the requirements accurately for each deployment type and carefully set the priorities of the deployment types. For example, if the highest-priority deployment type does not have any defined requirements, it will be the only deployment type used for all installations of that application.

Global conditions have three categories that define requirements: User, Device, and Custom. The User and Device categories contain the predefined global conditions that you can use to create requirements. When the existing conditions are not sufficient, you can use the Custom category to create custom global conditions by using the Create button within the Create Requirement dialog box.

When defining requirements, you can use one of two rule types:

- **Value** This condition type compares a value on the client system to the value that you specify. All the predefined requirements are of the Value type. You can create custom global conditions to define value condition types. Each condition has an operator that defines how you are comparing the existing value on the client system to the desired value in the condition. There are many possible operators, including the standard relational operators such as Equals, Not Equal To, Greater Than, Less Than, Between, Greater Than Or Equal To, and Less Than Or Equal To.

- **Existential** This condition type checks whether the condition exists. There are no predefined existential global conditions. You can create custom global conditions to define existential types.

When creating or editing a deployment type manually, you can specify multiple requirements. However, if you specify multiple requirements, all the requirements must be met before deployment occurs.

Table 2-6 lists the categories for requirements.

Category	Conditions	Operators	Possible values
User	Primary device	■ Equals	■ True ■ False
Device	Active Directory site	■ One of ■ None of	■ One or more Active Directory sites
	Configuration Manager site	■ One of ■ None of	■ One or more Configuration Manager sites
	CPU speed	■ Any of the relational operators	■ Any numerical megahertz (MHz) value
	Disk space	■ Any of the relational operators	■ Any numerical megabyte value for any drive, a system drive, or a specific drive
	Number of processors	■ Any of the relational operators	■ Numerical value
	Operating system	■ One of ■ None of	■ Any supported operating system
	Operating system language	■ One of ■ None of	■ Any supported language
	Organizational unit (OU)	■ One of ■ None of	■ One or more Active Directory OUs and child OUs
	Ownership	■ Equals ■ Not equal to	■ Personal ■ Company
	Total physical memory	■ Any of the relational operators	■ Any numerical MB value
	Windows Store inactive	■ Any of the relational operators	■ Any positive integer with 18 digits or fewer
Custom	■ Create a new condition; these become global conditions. ■ Previously created global conditions.	■ Varies	■ Varies

TABLE 2-6 Requirement categories

After creating or adding deployment types, you can adjust the priority with the Increase and Decrease priority buttons on the Deployment Types tab in the application properties.

There are many reasons for creating requirements and as many ways to define them:

- To ensure that the application is installed only on a user's primary device, use the primary device requirement from the User category.

- To ensure that the hardware is capable of supporting the application (such as memory requirements), use the total physical memory requirement from the Device category.

- To ensure that a prerequisite is installed or configured correctly, use a custom requirement to check for a specific file and version or check for registry entries.

More Info: **Chassis Global Condition**

You can learn more about chassis global condition at *http://blogs.technet.com/b/brandonlinton/archive/2013/01/30/configmgr-2012-chassis-type-global-condition.aspx*.

User device affinity

System Center 2012 R2 Configuration Manager and newer versions include a User Device Affinity feature. User device affinity enables a user to associate one or more devices. These devices are the user's primary devices. Similarly, a device can have an affinity with more than one user. You can use user device affinity as a requirement for deployment types to deploy an application to a user-based collection so that the application deploys only to the user's primary devices. However, this requires the user's primary devices to meet the application's other requirements, such as any hardware requirements. Typically, a primary device is the device that the user uses on a daily basis to perform her work.

Using user device affinity as a requirement provides further options for deploying software. For example, a required line-of-business (LOB) application is created with multiple deployment types, such as the Windows Installer (*.msi file) deployment type and the Application Virtualization 5 deployment type. You could configure the requirements for the deployment types to use the Windows Installer (*.msi file) deployment type only for a user's primary device. The application is then deployed as Required for the user. When the user logs on to his primary device, the application is installed locally by using a Windows Installer (*.msi file) deployment type. If the same user accesses a device that is not his primary device, the application is installed by using the Microsoft Application Virtualization 5 deployment type.

In addition, you can deploy an application as Required and then specify to predeploy software to the user's primary device. This allows the application to install before the user logs on so that the user can run the application as soon as she logs on.

Automatically configured affinity

You can configure a site to assign user device affinity automatically based on the usage of the devices. You can control this through Client Settings, either in Default Client Settings in Administration and the Client Settings node or in a custom client setting. There are three settings in the User And Device Affinity group that you can use to control automatic assignment of device affinity:

- **User Device Affinity Usage Threshold (Minutes)** Specify the number of minutes of usage before a user device affinity is created.
- **User Device Affinity Usage Threshold (Days)** Specify the number of days over which the usage-based affinity threshold is measured.
- **Automatically Configure User Device Affinity From Usage Data** In the drop-down list box, click Yes to enable the site to create user device affinities automatically. If you select No, an administrator must approve all user device affinity assignments.

You manage device affinity requests in the Assets And Compliance workspace. Select the Device Collections node and then click Manage Affinity Requests to approve or reject affinity requests. When using automatic affinity assignment, the thresholds are monitored continuously. If a user falls below the specified threshold, the affinity relationship will be removed.

User-defined affinity

You also can enable users to define their own primary devices through Application Catalog. First, configure the Allow User To Define Their Primary Devices user setting either in Default Client Settings or in a custom client setting as shown in Figure 2-3:
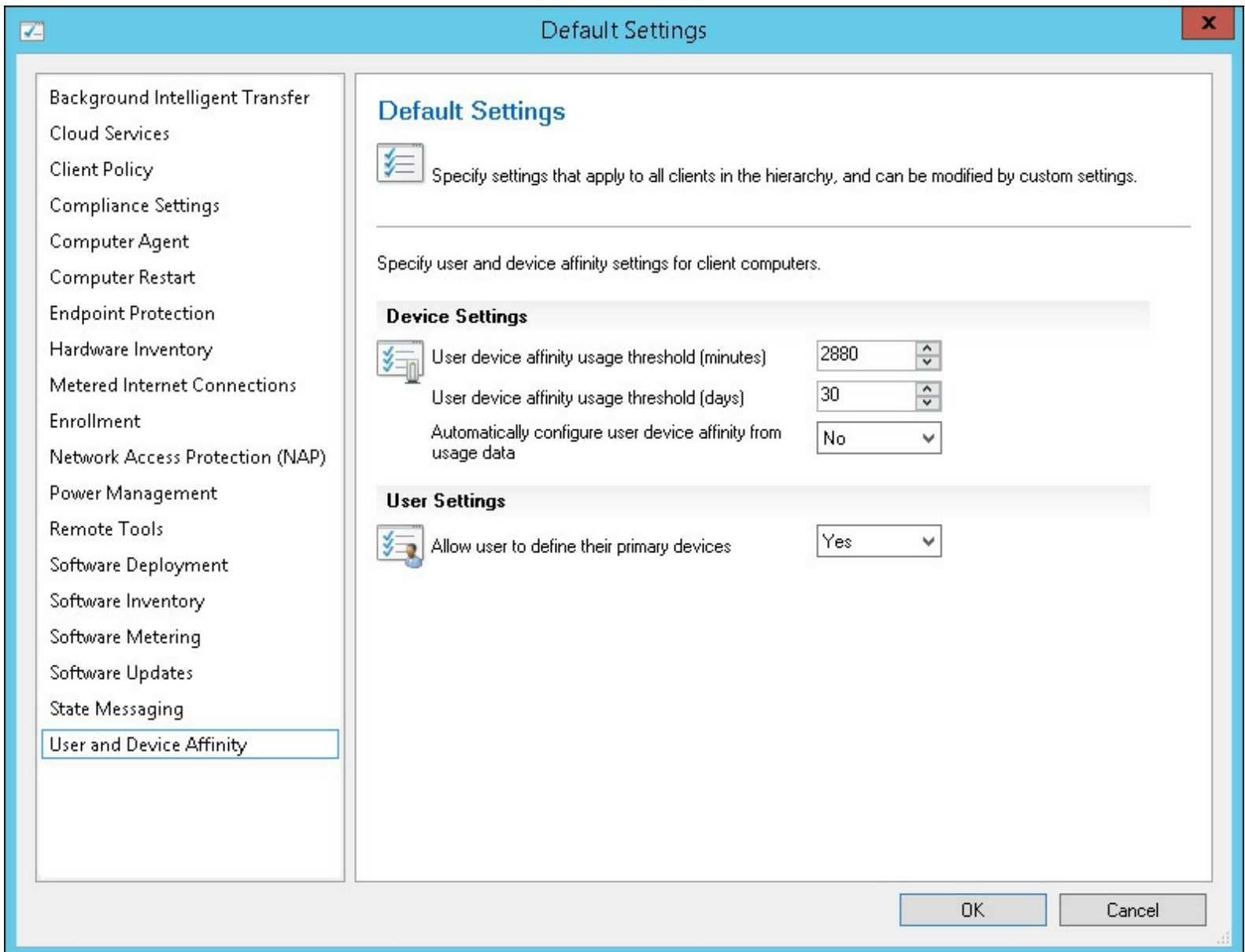
FIGURE 2-3 User device affinity

Users then must start Application Catalog from the device they want to set as a primary device, click the My Devices link, and then select the I Regularly Use This Computer To Do My Work check box.

Administrator-defined affinity

There are three ways for administrators to define user device affinity manually from the Assets And Compliance workspace:

- Select a device and then, on the ribbon, click Edit Primary Users.
- Select a user and then, on the ribbon, click Edit Primary Devices.
- Import a .csv file.

To import a .csv file, select either the Users node or the Devices node and then, on the ribbon, click Import User Device Affinity. Each user and device in the file must already exist in the Configuration Manager database. You must format the file you import in the following manner: *<Domain\user name>,<Device NetBIOS name>*.

Operating system deployment–defined affinity

During operating system deployment, you can use task sequence variables to aid in defining user device affinity:

- **SMSTSAssignUsersMode** There are three options for this variable:
  - **Auto** The Auto setting defines user device affinity automatically.
  - **Pending** The Pending setting creates a user device affinity request that requires administrator approval.
  - **Disabled** The Disabled setting causes the task to skip user device affinity processing.
- **SMSTSUdaUsers** You can assign one or more users to this variable in the format of DOMAIN\Username.

More Info: **Task Sequence Action Variables**

You can learn more about task sequence action variables at
http://technet.microsoft.com/en-us/library/hh273365.aspx.

Deploy software wizard

Before a user or client can run a deployment, you must distribute the appropriate content to one or more distribution points. You can either distribute the content to the distribution points ahead of time or distribute it while completing the Deploy Software Wizard.

After you are ready to deploy an application, you create a deployment that targets either users or devices. The client software checks the management point periodically for changes to user and machine policies. When the client has detected the deployment and reached the scheduled time of the deployment, and there is an applicable deployment type, the client system contacts the management point to locate an available distribution point containing the content. After the client system selects a distribution point with the content, the client system downloads the content and runs the appropriate application deployment type.

You use the Deploy Software Wizard to deploy applications to users and computers. You can launch this wizard either by selecting the application that you want to deploy and then clicking the Deploy button on the ribbon or by selecting Deploy on the shortcut menu.

The following sections describe each page of the Deploy Software Wizard.

General

The Specify General Information For This Deployment page of the Deploy Software Wizard is the General page, shown in [Figure 2-4](#). You can configure the following settings on this page:

- **Software** This setting refers to the name of the application that you are deploying.
- **Collection** This setting refers to the targeted device or user collection.
- **Use Default Distribution Point Groups Associated To This Collection** This check box is cleared by default.
- **Automatically Distribute Content For Dependencies** This check box is selected by default. Typically, you should not change this setting. Selecting it ensures that any dependent content is distributed and available.
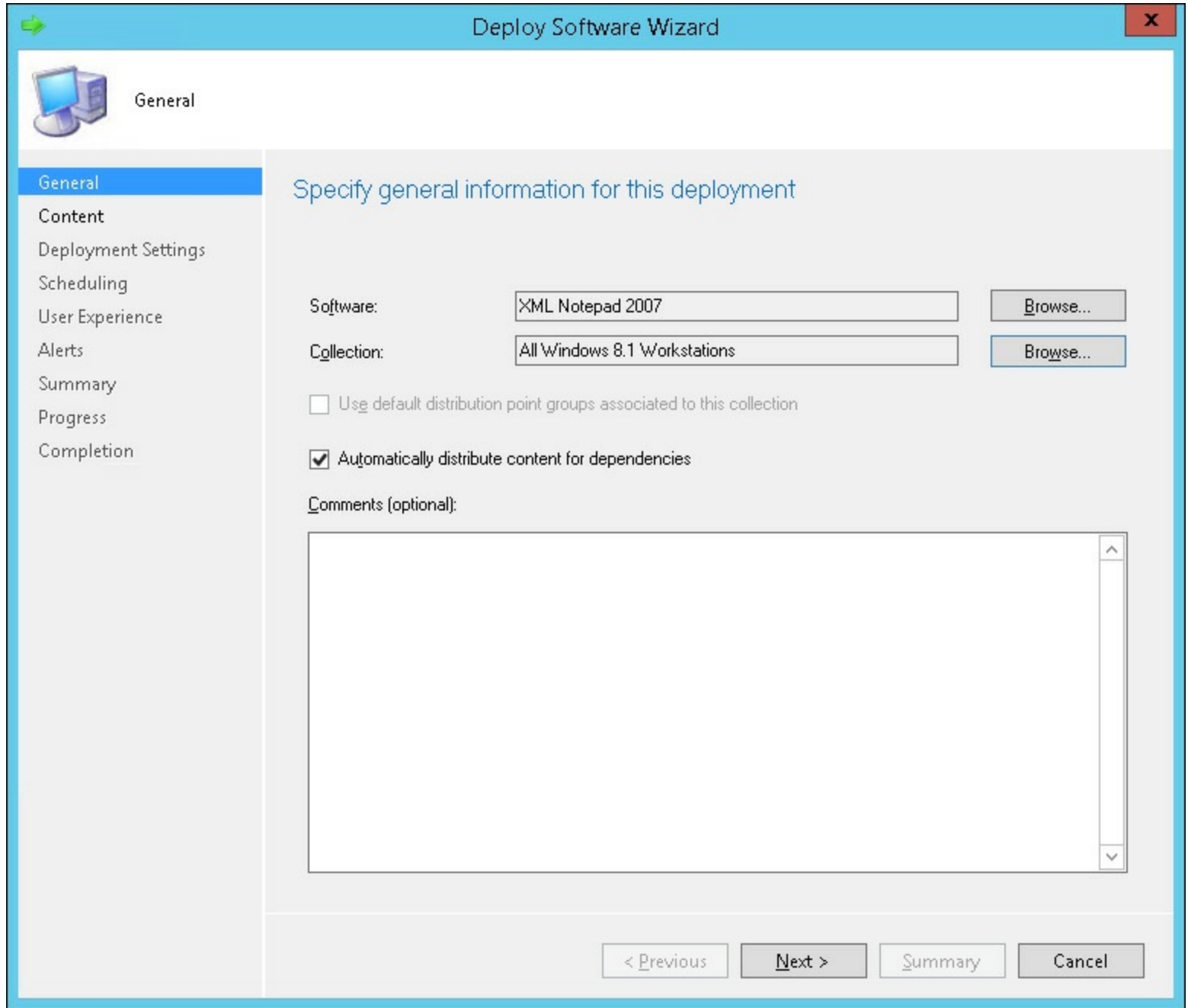
FIGURE 2-4 Deploy Software Wizard

Content

You use the Content page, shown in <u>Figure 2-5</u>, to specify one or more distribution points or distribution point groups that contain the content. If you have not previously distributed the content to at least one distribution point or distribution point group, you must designate the target distribution points or distribution point group at this time.
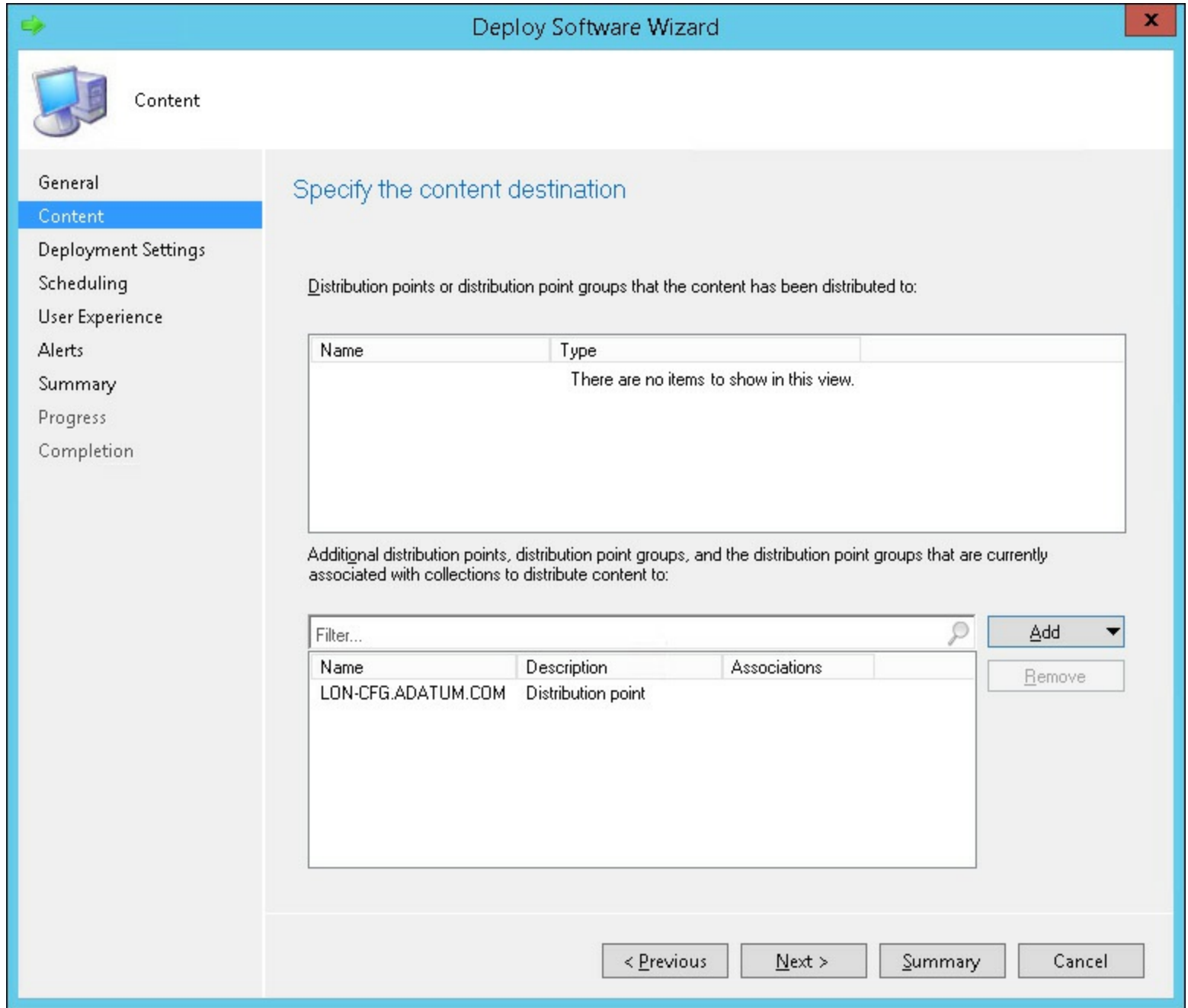
FIGURE 2-5 Specify The Content Destination page

Deployment settings

On the Specify Settings To Control How This Software Is Deployed page, shown in , you can configure the following settings:
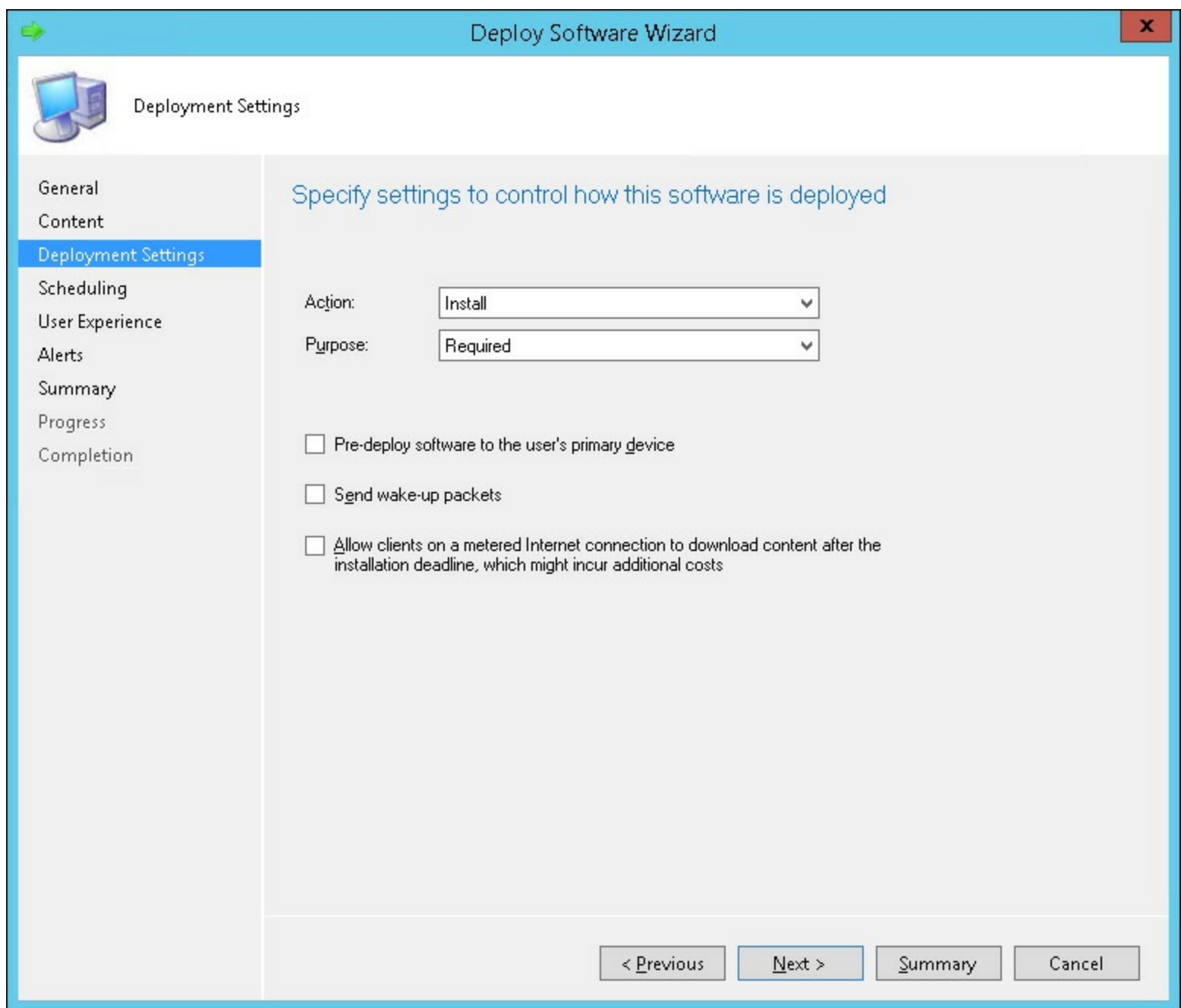
FIGURE 2-6 Deployment Settings

- **Action** This setting has two options: Install and Uninstall.

- **Purpose** When the action is set to Install, this setting has two options: Available and Required. When deploying an Uninstall action, the purpose is always Required.

If you select Required, the following settings are available:
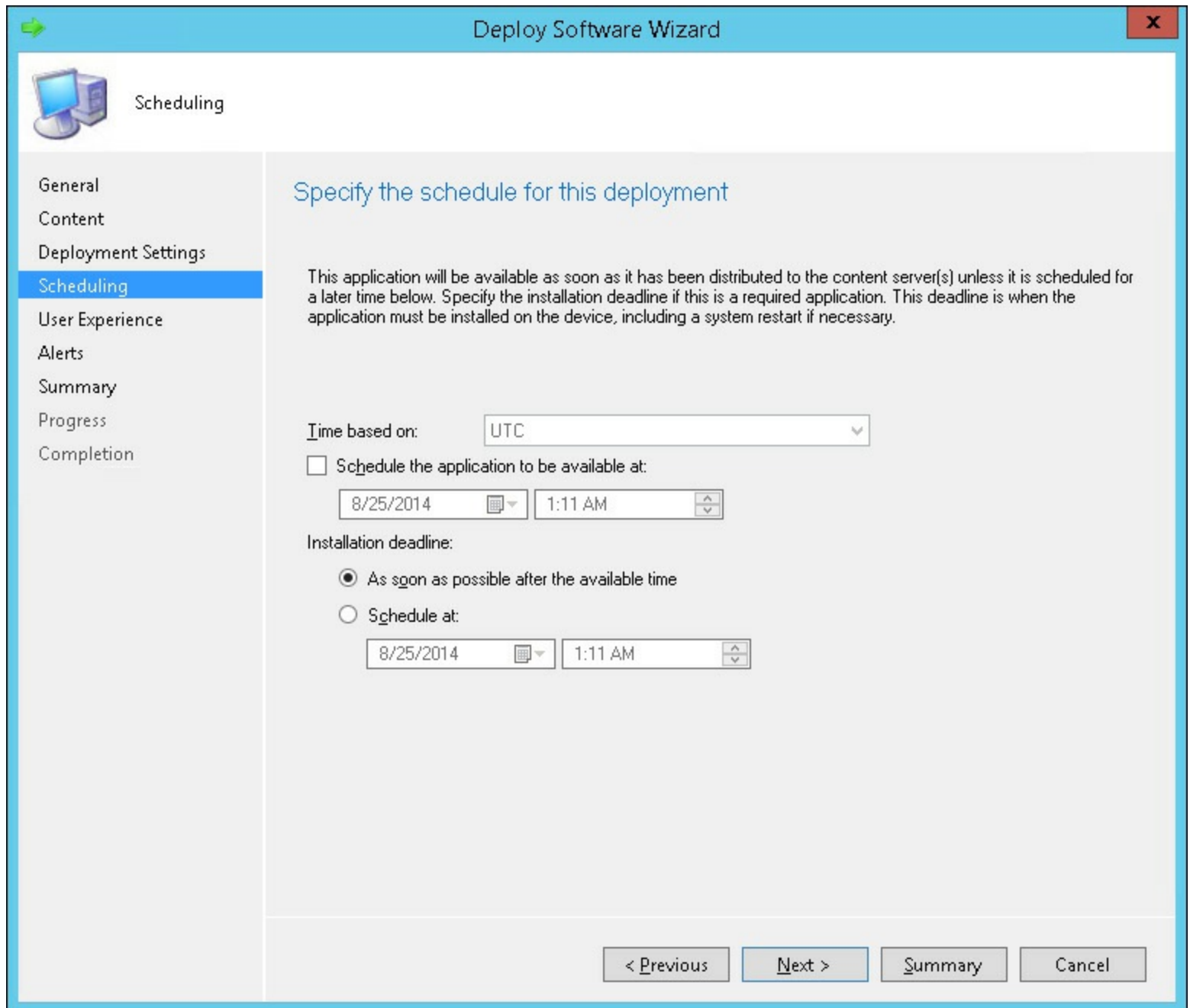
- **Pre-deploy Software To The User's Primary Device** This check box is cleared by default. Selecting this check box allows the software to be installed on a user's primary device without requiring the user to be logged on.

- **Send Wake-up Packets** This check box is cleared by default. Selecting this check box causes a wake-up packet to be sent to devices when the application is scheduled to be deployed. If the device supports Wake On LAN and if the device is turned off, the device is turned on to begin the deployment.

- **Allow Clients On A Metered Internet Connection To Download Content After The Installation Deadline, Which Might Incur Additional Costs** When you enable this option,

clients on metered connections download content automatically when the specified deadline is reached. If the mobile client is on a limited mobile Internet access plan, this could result in many overage minutes.

When deploying to a user, the same settings are available, with one additional option. If the Install action with the Available purpose is selected, the Require Administrator Approval If Users Request This Application check box appears and is cleared by default. If you select this check box, users can request the application from Application Catalog. However, the application will not be deployed until an appropriate Configuration Manager administrator approves it.

Scheduling

On the Specify The Schedule For This Deployment page, shown in Figure 2-7, the options that are visible in this section depend on how you deploy the application. When deploying an application, consider the following scheduling options:

FIGURE 2-7 Specify The Schedule For This Deployment
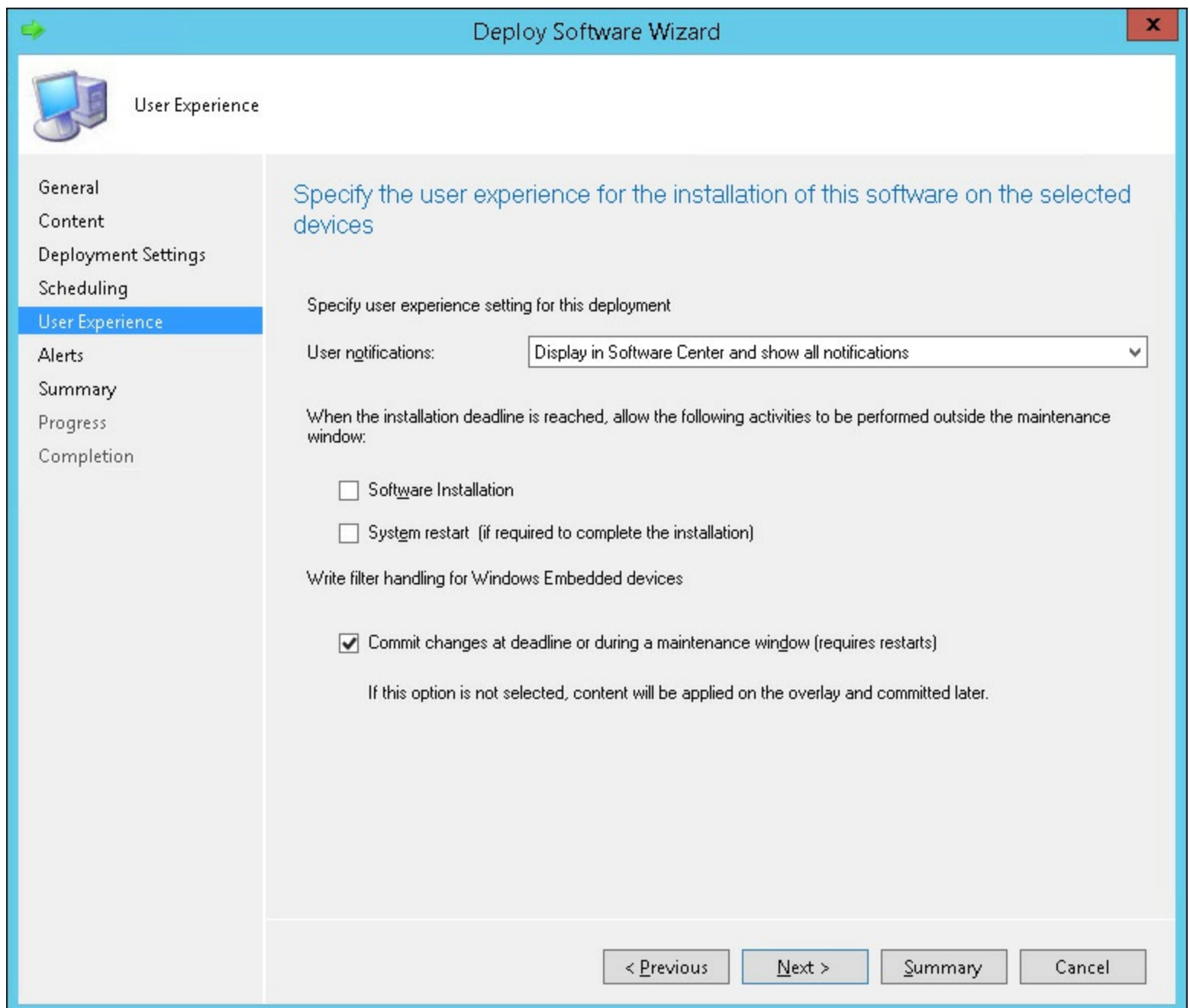
■ The default setting is to make the application available as soon as possible to ensure that

applications are available immediately.

- You can configure the application to be available at a specific time.
- When the application is deployed with the Available purpose, the available time is based on Coordinated Universal Time (UTC).
- When the application is deployed with the Required purpose, the action deadline is As Soon As Possible After The Available Time.
- You can change the action deadline to a specific time. If the action deadline is set to a specific time, you can configure the time to be either UTC or Client Local Time.

User experience

On the Specify The User Experience For The Installation Of This Software On The Selected Devices page, shown in Figure 2-8, you can configure settings related to how end users interact with the application deployment.

FIGURE 2-8 Specify The User Experience For The Installation Of This Software On The Selected Devices

If you deploy the application as Available, you can select one of the following options to determine how users see user notifications:

- Display In Software Center And Show All Notifications
- Display In Software Center, And Only Show Notifications For Computer Restarts

If you deploy the application as Required, an additional user notification option becomes available: Hide In Software Center And All Notifications. In addition, the following two check boxes become available for allowing actions outside a maintenance window when the installation deadline is reached:

- Software Installation or Software Uninstall
- System Restart (If Required To Complete The Installation) or Computer Restart (If Required To Complete The Software Uninstall)

To support the deployment to Windows Embedded devices, System Center 2012 Configuration Manager SP1 introduced the Commit Changes At Deadline Or During A Maintenance Window (Requires Restarts) setting under Write Filter Handling For Windows Embedded Devices.

Alerts

On the Specify Configuration Manager And Operations Manager Alert Options page, you configure what information you get back about deployments. The settings that you configure depend on whether you deploy the software as Available or as Required.

If you deploy the software as Available, you can create a deployment alert when the threshold is higher than a specific value. You can configure the threshold as a percentage of failure; when a certain percentage of deployed clients report a failure, an alert is generated. For example, if you configure the percentage as 10 for a deployment that is targeting 1,000 devices and 100 deployments fail, an alert is generated.

If you also are using System Center 2012 R2 Operations Manager or System Center 2012 Operations Manager, you can specify the following Operations Manager–related settings:

- **Enable System Center Operations Manager Maintenance Mode** This check box is disabled by default. If you enable this setting, the Operations Manager agent on the computer will not generate any alerts during the deployment of the application.

- **Generate System Center Operations Manager Alert When A Software Installation Fails** or **Generate System Center Operations Manager Alert When The Software Removal Fails** This check box is disabled by default. If the Enable System Center Operations Manager maintenance mode is enabled and this setting is not enabled, Operations Manager administrators might not notice failed installations (or uninstallations). This can leave a critical, monitored system in a nonfunctioning state without notifying the Operations Manager administrators.

If you deploy the software as Required, in addition to the options displayed for the Available deployment, the following settings are available:

- **Create A Deployment Alert When The Threshold Is Lower Than The Following** or **Create A Removal Alert When The Threshold Is Lower Than The Following** The following two settings are available under this check box:

- **Percent Success** You can specify a number between 0 and 99.
- **After** You specify a date and time, and, if the specified percentage success is not met at this time, an alert is generated.
- **Create A Deployment Alert When The Threshold Is Higher Than The Following** or **Create A Removal Alert When The Threshold Is Higher Than The Following** The following setting is available under this check box:
  - **Percent Failure** You can specify a number between 0 and 99.

By specifying these settings, you ensure that an alert is generated if the specified percentage of targeted devices has not reported a successful deployment by the specified date and time. For example, you can configure the percent success to 90 by December 12, 2014, for a deployment that is targeting 1,000 devices. On December 13, 2014, if 900 deployments have not been successful, an alert is generated.

Simulated deployment

A simulated deployment is a special deployment in which you can test the evaluation of the requirements in the application's deployment types without distributing any files. You create a simulated deployment by selecting your application and then clicking the Simulate Deployment button on the ribbon. When using simulated deployment, you do not specify a distribution point because target clients do not use content.

A simulated deployment is evaluated like any deployment, and the results are in the Monitoring workspace under the Deployments node along with all the other deployments. When examining the status of the simulated deployment, you see the following results:

- **Success** This includes targets when a deployment type for the application is installed already, including the deployment type with which they comply.
- **Simulate Success** This includes targets that comply with a deployment type in the application, including the deployment type with which they comply.
- **Requirements Not Met** This includes targets that do not comply with any deployment type in the application, including the deployment types with which they do not comply.
- **Unknown** This includes targets that have not yet reported results.

You create a simulated deployment the same way as any other deployment. Therefore, you cannot create a regular deployment for the same application and collection until you delete the simulated deployment.

> ### 🧪 *Thought experiment:* Application deployment at Contoso
>
> **You want to deploy a new application to some of the computers in your organization. A small number of computers in your organization don't have enough memory to run the application, and you want to avoid deploying the application to these computers. You also want to verify that the deployment you have configured will reach all targeted computers. With this information in mind, answer the following questions:**
>
> 1. **What can you do to ensure that the new application is deployed only to computers with enough RAM?**
> 2. **What should you do to verify that the deployment settings are correct?**

Objective summary

- When creating an application, you can either allow the wizard to detect settings automatically from the installation files or use the wizard to create the application manually.
- The software deployment process in Configuration Manager consists of determining the users or devices to which you want to deploy the application and the way in which you want to present the software.
- The deployment can be deployed automatically (required), presented in Software Center (available to devices), or deployed from Application Catalog (available to users).
- You can deploy applications to either user collections or device collections.
- A detection method is a procedure that enables the deployment process to determine whether an application is present on a system.
- Dependencies define one or more applications that must be installed before you run a specific deployment type.
- Global conditions define the attributes that Configuration Manager evaluates to determine whether a deployment type applies to a particular user or device.
- Applications in System Center 2012 R2 Configuration Manager and newer versions support using multiple deployment types in each application.
- Deployment types run the installation software only on clients on which the installation meets all the specified criteria and, therefore, is likely to be successful.
- When there are multiple deployment types and the target device or user could match the requirements for more than one deployment type, application installation occurs using the highest-priority deployment type.
- User device affinity enables a user to associate a primary device with one or more devices. Typically, a primary device is the device the user uses on a daily basis to perform her work.
- You can configure a site to assign user device affinity automatically based on the usage of the devices. You also can allow users to define their own primary devices through Application Catalog.

- Before a user or client can run a deployment, you must distribute the appropriate content to one or more distribution points.
- A simulated deployment is a special deployment in which you can test the evaluation of the requirements in the application's deployment types without distributing any files.

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 want to make an application available to a user through Software Center, but the application should be installed only if the user chooses to install it. Which of the following deployment settings would you configure when running the Deploy Software Wizard? (Choose two. Each correct answer forms part of a complete solution.)

   A. Action: Install

   B. Action: Uninstall

   C. Purpose: Available

   D. Purpose: Required

2. You want to ensure that a particular application is installed on all computers within the scope of the deployment. Deployment of this software is mandatory. Which of the following deployment settings would you configure when running the Deploy Software Wizard? (Choose two. Each correct answer forms part of a complete solution.)

   A. Action: Install

   B. Action: Uninstall

   C. Purpose: Available

   D. Purpose: Required

3. In which of the following situations will software install automatically and silently? (Choose all that apply.)

   A. You deploy the software to a user collection. The software is deployed as Required, and the deadline is set to a point in time prior to the current date.

   B. Software is deployed as Available to a user collection.

   C. Software is deployed as Available to a device collection.

   D. You deploy the software to a device collection. The software is deployed as Required, and the deadline is set to a point in time prior to the current date.

4. In which of the following scenarios will a user be able to request an application from Application Catalog?

   A. You deploy the software to a device collection. The software is deployed as Required, and the deadline is set to a point in time prior to the current date.

   B. Software is deployed as Available to a device collection.

   C. Software is deployed as Available to a user collection.

D. You deploy the software to a user collection. The software is deployed as Required, and the deadline is set to a point in time prior to the current date.

Objective 2.3: Deploy applications using Microsoft Intune

Microsoft Intune is a cloud-based management suite that enables you to perform a variety of client computer and device management and monitoring tasks. Intune is suitable for managing clients that might be located on remote networks on the Internet. You can use Intune to manage the deployment of applications to computers and mobile devices such as those running the Windows Phone, iOS, and Android operating systems.

This section covers the following topics:
- Intune operating system support
- Deploying software to the company portal
- Deploying software for automatic installation
- Windows Intune update policies

Intune operating system support

Intune supports management of clients that are running the following operating systems:
- Windows 8.1, Windows 8, Windows 7, Windows Vista
- Windows RT 8.1, Windows RT
- Windows Phone 8.1, Windows Phone 8
- Apple iOS 7, iOS 6, and iOS 5
- Android (requires Exchange ActiveSync)

Intune can manage mobile devices directly or through Exchange ActiveSync and supports direct management for mobile devices that are running Windows RT, Windows Phone 8, Windows Phone 8.1, and iOS.

To deploy applications directly to mobile devices that are running Windows RT, you must obtain sideloading keys, and you must have a code-signing certificate to sign the applications. The Windows RT or Windows Phone 8 device must trust this code-signing certificate. Furthermore, you can use a process known as deep linking to deploy an application directly from the appropriate Windows Store to mobile devices that are running the Windows RT or Windows Phone 8 mobile operating systems.

You can use Intune to deploy applications to iOS devices by deep linking to the Apple App Store or by sideloading apps, which means you are installing them by using direct access to the source files. To deploy applications to iOS devices, you must obtain the appropriate mobile device management certificates from Apple. You can use a similar process for devices that are running the Android operating system.

Users can enroll devices by downloading the appropriate app from the online store for their mobile device operating system. Alternatively, if they are using a computer running Windows 7 or Windows Vista, they can download and run the Intune client installer.

Certificate requirements

Depending on the mobile device operating system, you need certificates or keys to enroll mobile devices into your organization's Intune subscription.

Table 2-7 details these specifications.

Mobile-device operating system	Certificates or keys	Notes
Windows Phone 8 and Windows Phone 8.1	Code-signing certificate. All side-loaded apps must be code-signed.	Purchase a code-signing certificate from Symantec.
Windows RT 8.1 and Windows RT	■ Sideloading keys allow installation of sideloaded apps. ■ All apps that you sideload must be code-signed.	■ Obtain sideloading keys from Microsoft. ■ Sign apps by using a code-signing certificate that an internal or other trusted certification authority (CA) issues.
iOS5, iOS6, and iOS7	Apple Push Notification service certificate	Obtain certificate from Apple.
Android	Not required	

TABLE 2-7 Intune certificate requirements

Preparing for software deployment

You use the Software workspace of the Intune administrator console to view information about software that has been detected on Intune client computers. Software inventory is only generated for computers, and you can't use this workspace to view the software inventory of managed mobile devices. In the Detected Software section, you can view the properties of detected software and add license agreement information for detected software.

Through the Managed Software page of the Software workspace, you can perform the following tasks:

- View and modify software properties
- Add license agreements to managed software
- Manage software deployments
- Delete software
- Add software

You add software to Intune using the Windows Intune Software Publisher. You can upload software in the form of programs for computers or apps for mobile devices. This software will be stored within Intune's cloud storage. You can also use the Windows Intune Software Publisher to add a link to an app in the Microsoft, Google, or Apple stores and to link to a web application.

Links to an app in the app store are supported by devices running the following operating systems:

- Windows 8
- Windows 8.1
- Windows RT

- Windows Phone 8
- iOS
- Android devices

Links to web apps can be deployed to any device Intune supports.

Deploy software to the company portal

The company portal is a self-service portal that is available to users who have installed the Intune client on their computers or mobile devices. Deploying software to the company portal makes that software optionally available through the company portal on those computers or devices.

To make the software available, you deploy the software package to a particular user group or device group with the deployment action set to Available Install. Members of these groups can then select the software for installation.

Deploy software for automatic installation

You can use Intune to deploy software that will automatically install on computers or devices that are Intune clients. You deploy software for automatic installation by selecting the user or device groups to which you wish to deploy the software and by setting the deployment action to Required Install.

When you set the deployment action to Required Install, you can specify a deadline for the deployment. You can select from among the following deadlines:

- **None** The software will deploy based on agent policy settings.
- **As Soon As Possible** The software will deploy directly after the next synchronization.
- **One Week** The software will deploy one calendar week after the current day.
- **Two Weeks** The software will deploy two calendar weeks after the current day.
- **One Month** The software will deploy one calendar month after the current day.
- **Custom** Use this option to select a specific date and time for software package deployment.

Intune update policies

Intune update policies determine the frequency with which the Intune client checks for and performs the installation of a new application. These are the same settings that are used to control the installation of software updates and are shown in .

FIGURE 2-9 Update policy

The policies related to application installation are as follows:

- **Update And Application Detection Frequency (Hours)** Specify how often the Intune client waits between checking for new updates and applications.

- **Automated Or Prompted Installation Of Updates And Applications** Configure when either automatic or prompted installation of applications or updates will occur.

- **Delay To Restart Windows After Installation Of Scheduled Updates And Applications (Minutes)** Set the length of time the computer will wait before performing a restart after the installation of applications or updates.

- **Delay Following Windows Restart To Begin Installing Missed Scheduled Updates And Applications (Minutes)** Set how long the computer will wait to install applications or updates if a scheduled installation time was missed.

- **Allow Logged On User To Control Windows Restart After Installation Of Scheduled**

Updates And Applications Configure whether a user who is logged on to the computer may control whether the computer restarts after update installation.

- **Delay Between Prompts To Restart Windows After Installation Of Scheduled Updates And Applications (Minutes)** Specify the amount of time that the computer will wait before restart prompts.

More Info: **Intune Installation Policies**

You can learn more about Intune installation polices at *http://blogs.technet.com/b/windowsintune/archive/2013/01/09/policy-settings-for-mandatory-updates.aspx*.

Exam Tip

Remember the differences between deployment actions.

Thought experiment: **Intune at Fabrikam**

Fabrikam has just purchased a large number of Surface 2 devices for remote users. Intune will manage these devices. Users must perform their own enrollment, and then administrators at Fabrikam will deploy an important custom application that runs on Windows RT. With this information in mind, answer the following questions:

1. **How will Surface 2 users enroll in Intune?**
2. **Which keys and certificates are required to deploy custom software to the Surface 2 devices by using Intune?**

Objective summary

- Intune supports managing clients that are running Windows 8.1 (x86, x64), Windows 8 (x86, x64), Windows 7, Windows Vista, Windows RT 8.1, Windows RT, Windows Phone 8, Windows Phone 8.1, Apple iOS 7, iOS 6, iOS5, Android (requires Exchange ActiveSync).
- To deploy applications directly to mobile devices that are running Windows RT, you must obtain sideloading keys, and you must have a code-signing certificate to sign the applications.
- You can use Intune to deploy applications to iOS devices by deep linking to the Apple App Store or by sideloading apps to install them by using direct access to the source files.
- Users can enroll devices by downloading the appropriate app from the online store for their mobile device operating system. Alternatively, if they are using a computer running Windows 7 or Windows Vista, they can download and run the Intune client installer.
- You use the Software workspace of the Intune administrator console to view information about

software that has been detected on Intune client computers.

- To make software available in the company portal, you deploy the software package to a particular user group or device group with the deployment action set to Available Install.
- You deploy software for automatic installation by selecting the user or device groups to which you wish to deploy the software and by setting the deployment action to Required Install.
- Intune update policies determine the frequency with which the Intune client checks for and performs the installation of new applications.

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 of the following Intune policy settings would you configure to set the deployed application installation time to 4 P.M. each weekday?

    A. Update And Application Detection Frequency

    B. Automated Or Prompted Installation Of Updates And Applications

    C. Allow Immediate Installation Of Updates That Do Not Interrupt Windows

    D. Allow Logged On User To Control Windows Restart After Installation Of Scheduled Updates And Applications

2. You want to allow users at your organization to choose when to restart their computers after you deploy an application that requires a restart to complete the installation process. Which of the following Windows Intune policies would you configure to accomplish this goal?

    A. Update And Application Detection Frequency

    B. Allow Logged On User To Control Windows Restart After Installation Of Scheduled Updates And Applications

    C. Allow Immediate Installation Of Updates That Do Not Interrupt Windows

    D. Automated Or Prompted Installation Of Updates And Applications

3. You want to increase the frequency with which applications newly deployed to the company portal become visible to Intune clients. Which of the following Intune policies would you configure to accomplish this goal?

    A. Allow Immediate Installation Of Updates That Do Not Interrupt Windows

    B. Automated Or Prompted Installation Of Updates And Applications

    C. Update And Application Detection Frequency

    D. Allow Logged On User To Control Windows Restart After Installation Of Scheduled Updates And Applications

Objective 2.4: Plan for application upgrades

Applications in Configuration Manager might require ongoing management. Over time, you might modify an application or decide that you no longer need to deploy it. In addition, you might decide to stop deploying an application for a period of time or even uninstall the application from clients. Finally, you likely will upgrade and replace existing applications. In this lesson, you learn about several of the management options that are available for ongoing maintenance of applications.

This section covers the following topics:

- Application supersedence
- Application revision history
- Retiring applications
- Uninstalling applications

Application supersedence

Application management in Configuration Manager enables you to upgrade or replace existing applications by using a supersedence relationship. When you supersede an application, you can specify a new deployment type to replace that of the superseded application. In addition, you can configure whether to uninstall the superseded application.

When you supersede an application, the supersedence applies to all future deployments and Application Catalog requests. The effect on existing deployments depends on the options that you choose. To leave the superseded application in place, you can choose Do Not Replace, or you can specify a new deployment type to replace the old deployment type. If the superseded application has multiple deployment types, you specify a new deployment type for each old deployment type that you want to replace. Whether you choose a new deployment type or not, you can uninstall the application by selecting the Uninstall check box for each old deployment type. Supersedence options are as follows:

- You configure the supersedence to uninstall the old deployment type, and you deploy the application with the required action. When you do this, the existing application is uninstalled, and the new application is installed.

- You specify a new deployment type and do not configure the supersedence to unin-stall the old deployment type. If successful, the existing application will not be unin-stalled, and the new application will perform an in-place upgrade of the old application where possible. If not successful (for example, replacing a software title with a competitor's product), the old application is not removed from the target, and the new application is installed.

You can view the supersedence and dependency relationships between applications, as shown in [Figure 2-10](#), in a variety of ways:

- In the application's Properties dialog box of the superseding application, on the Supersedence tab, you can view the applications this application supersedes.

- In the application's Properties dialog box of the superseded application, on the References tab, you can use these options: Applications That Depend On This Application and Applications That Supersede This Application.

- With a superseding application selected, on the ribbon, you can click View Relationships to view dependencies, supersedence, and global conditions related to the selected application.
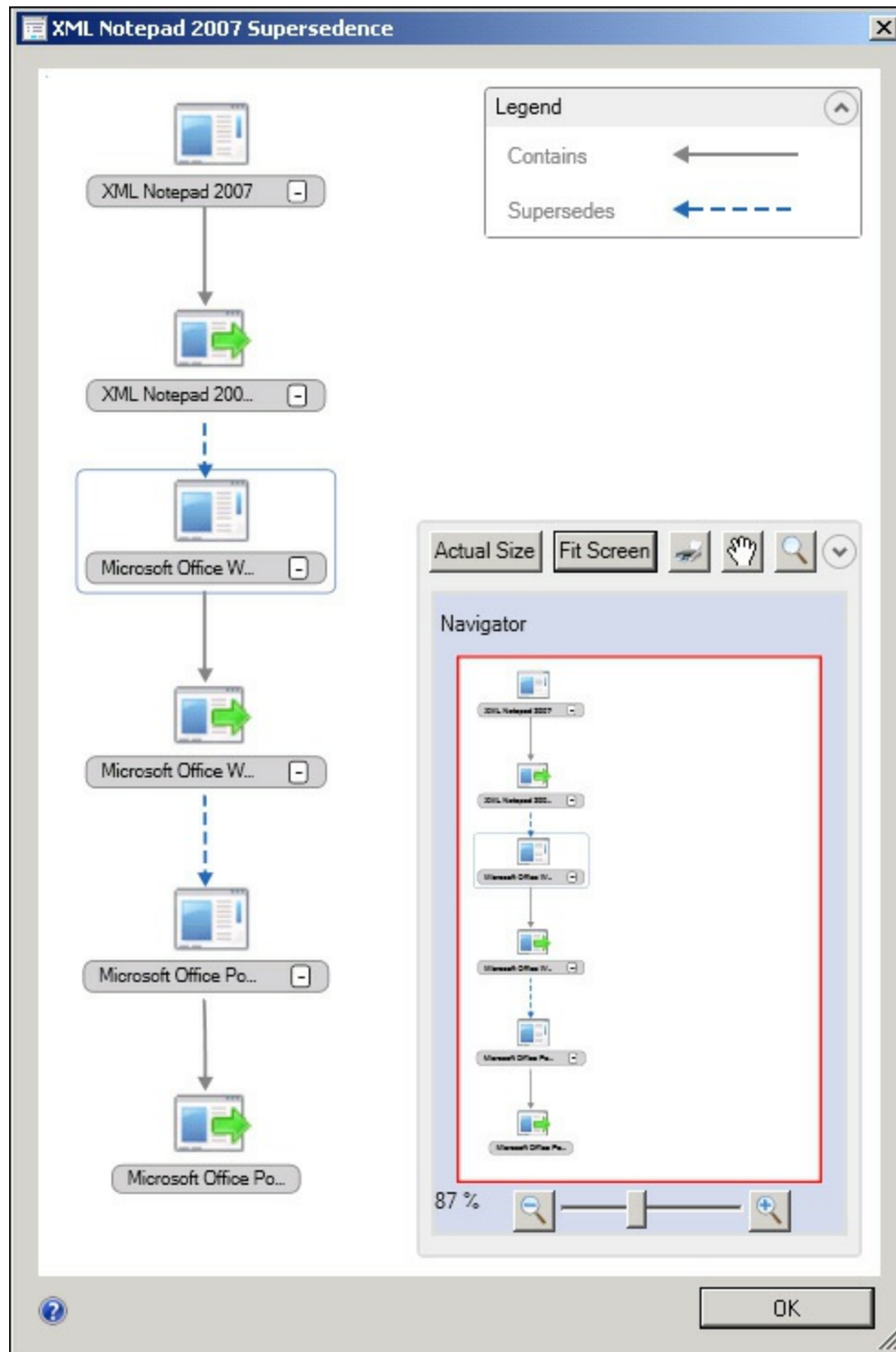
FIGURE 2-10 Supersedence

Application revision history

You can change applications in several ways, including complex tasks such as editing or creating a deployment type and simple tasks such as editing the administrator comments field. When you make any such changes to an application, Configuration Manager creates a new revision of the application. By using the Configuration Manager console, you can access the revision history for each application. After you access the revision history, you can view the properties of each revision, restore a previous revision, or delete an old revision.

To view the revision history of an application, you select the application in Software Library and

then click the Revision History button on the ribbon. shows revision history.
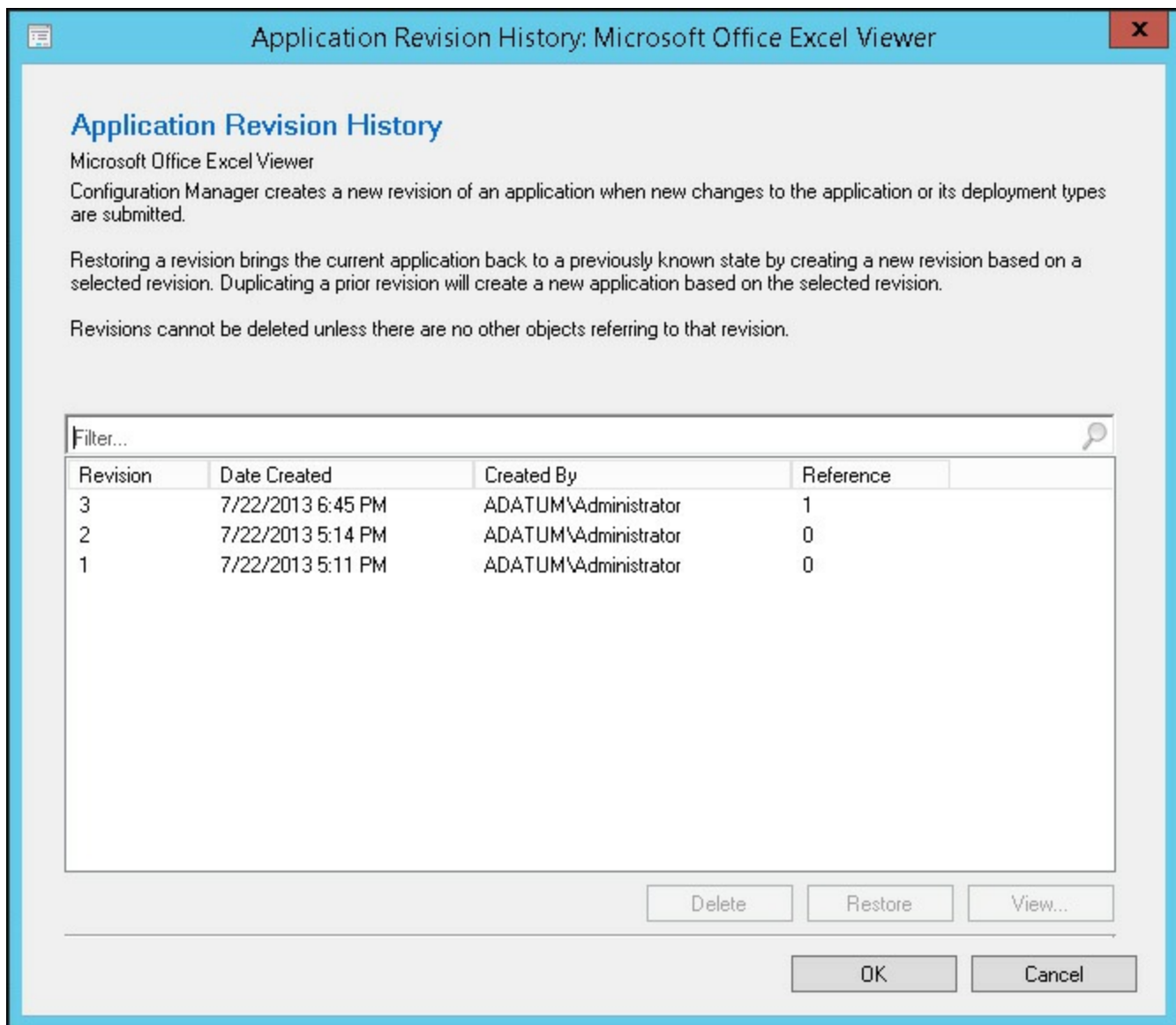
FIGURE 2-11 Revision history

When you view a past revision, you are viewing a read-only copy of it. When you restore a previous version of an application, Configuration Manager creates a new revision.

If you no longer need to maintain a revision, you can delete it by clicking the Delete button. You cannot delete the latest revision. If you do not need the application or any of its revisions, you can delete the application. However, you cannot delete an application if it is:

- Referenced by any deployments.
- Specified as a dependency for another application.
- Referenced in a task sequence.
- Part of a virtual environment.

Retiring applications

You can retire an application at any time. Retiring an application prevents new deployments of the application without uninstalling it. By retiring an application, you save all the work and time you spent creating and customizing the application. Deployments based on retired applications will continue to work as expected; however, you cannot create any new deployments from a retired application.

Although you cannot modify a retired application, you can reinstate the application when desired. After reinstating an application, you can create new deployments of it. If a retired application is not referenced in any deployments, Configuration Manager will delete it automatically after 60 days. However, this will not uninstall the application from any client machines.

Uninstalling applications

If you do not require an application in your environment, you can deploy it with an uninstall action. However, the uninstall deployment will fail if an existing install deployment for the software affects the clients targeted with the uninstall action. Therefore, before deploying an uninstall action, remove the install deployments for the application that you are uninstalling.

You need to remove the install deployments affecting only the clients on which you want to uninstall the application. If the uninstall deployment is in a separate application from the install deployment, you can retire it with the install deployment.

Uninstalling an application will not uninstall any dependent applications. The uninstall action uninstalls all instances of the software regardless of whether the application was installed by Configuration Manager, a manual process, or any other method. However, the software to be uninstalled must be created as an application in Configuration Manager with an appropriate uninstall command.

Thought experiment: **End of application life cycle at Contoso**

An application that is widely deployed on computers will no longer be needed in several months. With this information in mind, you are considering what strategies to pursue when the application is no longer required. As part of the planning process, answer the following questions:

1. **What is the difference between retiring an application and uninstalling an application?**
2. **What might cause an uninstall deployment to fail?**

Objective summary

- Application management in Configuration Manager enables you to upgrade or replace existing applications by using a supersedence relationship.
- When you supersede an application, you can specify a new deployment type to replace that of the superseded application.
- You can configure whether to uninstall the superseded application.

- When you supersede an application, the supersedence applies to all future deployments and Application Catalog requests.
- You can retire an application at any time. Retiring an application prevents new deployments of the application without uninstalling the application.

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. An application has been deployed on 30 percent of the desktop computers at your organization. You want to stop new deployments of this application but don't want to remove existing instances of the application. Which of the following steps could you take to accomplish this goal?

    A. Retire the application.

    B. Uninstall the application.

    C. Supersede the application.

    D. Install the application.

2. An application is deployed on 40 percent of the desktop computers at your organization. Your superiors have chosen not to continue licensing the application, so now you have to make sure that it is removed from these computers. No replacement application has been chosen at this time. Which of the following steps could you take to accomplish this goal?

    A. Install the application.

    B. Supersede the application.

    C. Uninstall the application.

    D. Retire the application.

3. You have decided to switch from one vendor's application to another's. The original vendor's application is present on 80 percent of the desktop computers at your organization. Which of the following steps could you take to replace the original vendor's application with a minimum of administrative effort?

    A. Supersede the application.

    B. Retire the application.

    C. Uninstall the application.

    D. Install the application.

Objective 2.5: Monitor applications

Configuration Manager enables you to monitor the process of application deployment, perform tasks to inventory the applications that are present on Configuration Manager clients, and measure how often users run applications in your organization.

Monitoring application deployment

In the Monitoring workspace of the Configuration Manager console, you can monitor all deployments, including software updates, compliance settings, applications, task sequences, packages, and programs.

Applications in Configuration Manager support state-based monitoring, which you can use to track the last application deployment state for users and devices. These state messages display information about individual devices.

You can view the states on several tabs in the Monitoring workspace. Each tab displays the individual users or devices reporting that state. The compliance states that may be displayed include:

- **Success** The application deployment was successful.

- **In Progress** The application deployment is in progress.

- **Unknown** The state of the application deployment is undetermined, so no state messages have been returned. For example, when a device is turned off for a device-targeted deployment or when a user has not logged on to receive a user-targeted deployment, the state is Unknown.

- **Requirements Not Met** The application did not deploy because it did not comply with a dependency or a requirement.

- **Error** The application failed to deploy because of an error.

Each compliance state includes subcategories that contain additional information on the deployment state and information on the number of users and devices in this category. For example, the Error compliance state contains the following three subcategories:

- Error evaluating policy

- Content related errors

- Installation errors

When more than one compliance state applies for an application deployment to a user who has more than one associated device, the aggregate state that you see is the lowest level of compliance. For example, if a user logs on to two devices, and the application installs successfully on one device but fails to install on the second device, the application's aggregate deployment state for that user displays as Error.

You can use these subcategories to help you quickly identify any important issues with an application deployment. You also can view additional information to determine the devices that fall into a particular subcategory of a compliance state.

Asset Intelligence

Asset Intelligence enhances Configuration Manager's inventory capabilities by extending hardware inventory and adding functionality for license reporting. Enabling additional hardware-inventory Windows Management Instrumentation (WMI) reporting classes helps improve the range of information that Asset Intelligence gathers about software titles in use.

In System Center 2012 R2 Configuration Manager, Asset Intelligence supports the mandatory software identification tags specified in the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 19770-2 standard. These tags include authoritative data that System Center 2012 R2 Configuration Manager can use to identify software installed on client computers. Because a standard defines the tags, an increasing number of software vendors include them in their applications. If you want System Center 2012 R2 Configuration Manager to use mandatory software identification tags, you must enable the SMS_SoftwareTag Asset Intelligence Hardware Inventory Reporting class.

In System Center 2012 R2 Configuration Manager, Asset Intelligence also collects information about Application Virtualization 5 and Application Virtualization 4 applications even though these applications run through the Microsoft Application Virtualization (App-V) client and are not installed on the client computer in a traditional manner.

Asset Intelligence provides organizations with the following benefits over software inventory:

- It provides more accurate representation of software titles that are present on managed computers.

- It provides information about the license usage for specific products rather than just information about the software itself.

- It can be used in conjunction with software metering to rationalize licensing by determining instances when software has deployed but is not being used.

- It uses Software Inventory Agent to detect software titles by scanning client storage. Asset intelligence retrieves information about installed software through the Hardware Inventory Client Agent.

Asset Intelligence has several components, including:

- **The Asset Intelligence catalog** Asset Intelligence relies on a set of database tables, which contain software identification, categorization information, and hardware requirements for software titles. Collectively, these tables are the Asset Intelligence catalog and are stored within the site database. The Asset Intelligence catalog can provide data for reports on installed software titles, organize the information within software categories and families, and provide a predefined set of hardware requirements for the software titles. You also can customize the organization of your information by creating custom software categories and families and adding new user-defined hardware requirements for specific software titles. By using an Asset Intelligence synchronization point, you can download periodic updates dynamically from Microsoft to the Asset Intelligence catalog. These updates contain information about newly released or validated software.

- **Asset Intelligence synchronization point** This is a Configuration Manager site system role that you can use to connect to an online service that Microsoft hosts, known as System Center Online, and then download Asset Intelligence catalog updates. You can either schedule or

manually initiate catalog synchronization. You also can use the Asset Intelligence synchronization point to upload custom software title information to System Center Online. Microsoft will then categorize it.

- **Asset Intelligence home page** The Asset Intelligence node in the Asset And Compliance workspace displays a summary dashboard of Asset Intelligence information. It includes summaries of the Asset Intelligence component status, the catalog synchronization status, and inventoried software status.

- **Asset Intelligence reports** More than 50 reports present Asset Intelligence information in an easy-to-use format. Many of these reports link to more specific reports, which enable you to query for general information and procure detailed information. Report categories include hardware, license management, and software.

More Info: **Asset Intelligence**

You can learn more about Asset Intelligence at *http://technet.microsoft.com/en-us/library/gg681998.aspx*.

Asset Intelligence catalog

The Asset Intelligence catalog contains information for more than 500,000 software titles and versions, representing more than 20 families and 90 specific categories, and includes the following:

- Support for manually importing software license information for software titles in use, including both Microsoft and non-Microsoft titles

- Hardware requirements for many software titles in the catalogSupport for adding custom software categories, families, and software labels

- Support for uploading software title information to the System Center Online service, which then categorizes it

You can review contents of the Asset Intelligence catalog and customize certain elements by clicking the Asset Intelligence node in the Assets And Compliance workspace. The Asset Intelligence folder includes the following nodes:

- Catalog
- Inventoried Software
- Hardware Requirements

Catalog

The catalog includes most of the catalog segments that administrators can update and the following:

- **Software Categories** Asset Intelligence software categories broadly categorize inventoried software titles. By default, there are a number of predefined software categories, such as Line Of Business, Original Equipment Manufacturer (OEM), and Office Suites And Productivity. You can create additional user-defined categories to classify inventoried software further.

- **Software Families** Asset Intelligence software families further define inventoried software titles. By default, the Asset Intelligence catalog includes approximately 20 predefined software families. Some examples of these predefined software families are Components And

Peripherals, Equipment, Home And Entertainment, Industry Specific, Line Of Business, and Productivity And Viewers. You can create additional user-defined software families to classify inventoried software further.

- **Custom Labels** Custom labels enable further classification of inventoried software according to attributes that administrators define. For example, you might create a custom label known as Shareware and associate that label with inventoried shareware titles. You then can run a report to display all software titles with which the custom label Shareware is associated.

Inventoried Software

The list of inventoried software titles includes information about software that the Hardware Inventory Agent reports. This node displays the following information by default for each inventoried software title:

- **Product Name** The name of the inventoried software
- **Publisher** The name of the vendor that developed the software
- **Version** The product version of the software title
- **Category** The currently assigned software category
- **Family** The currently assigned software family
- **Label (1, 2, and 3)** The custom labels that have been assigned with the software title, to a maximum of three
- **Software Count** The number of Configuration Manager clients that have inventoried the software title

Hardware Requirements

You can use Asset Intelligence hardware requirements to provide data to help verify that computers meet hardware requirements for software titles before you target them for deployment. Asset Intelligence retrieves from its catalog the hardware requirements that appear in the Configuration Manager console. The list is not based on inventoried software title information from Configuration Manager clients. You can add, modify, or delete custom hardware requirements for software titles that the Asset Intelligence catalog does not predefine. However, existing, noncustom hardware requirement information that the Asset Intelligence catalog stores is read-only, which means you cannot modify or delete it. The following information appears for each hardware requirement listed:

- **Software Title** The software title name with which the hardware requirement is associated.
- **Minimum CPU (MHz)** The minimum central processing unit (CPU) speed, in megahertz (MHz), that the software title requires.
- **Minimum RAM (KB)** The minimum random access memory (RAM), in KB, that the software title requires.
- **Minimum Disk Space (KB)** The minimum free disk space, in KB, that the software title requires.
- **Minimum Disk Size (KB)** The minimum hard-disk size, in KB, that the software title requires.
- **Validation State** The validation state for the hardware requirement. Valid states include Validated and User Defined.

Asset Intelligence data collection

You must configure several settings and tasks so that Asset Intelligence performs optimally, including the following:

- **Enable Hardware Inventory** Asset Intelligence reports depend on information the Hardware Inventory Agent collects. Ensure that you enable the Hardware Inventory Agent on clients.

- **Enable Software Metering** The software-related Asset Intelligence reports depend on the Software Metering Client Agent to provide data. These reports include the following:

  - Software 07A - Recently used executables by number of computers
  - Software 07B - Computers that recently used a specified executable
  - Software 07C - Recently used executables on a specific computer
  - Software 08A - Recently used executables by number of users
  - Software 08B - Users that recently used a specified executable
  - Software 08C - Recently used executables by a specified user

- **Enable Asset Intelligence Inventory reporting classes** To enable the Asset Intelligence Inventory reporting classes, right-click the Asset Intelligence node and then click Edit Inventory Classes. You can enable the Asset Intelligence reporting classes you need per the type of reporting that you require. Note that from within the Edit Inventory Classes dialog box, as you point to each reporting class, a tooltip displays information about the reports that depend on each reporting class.

- **Enable Windows event log settings** Several Asset Intelligence reports rely on information that Windows security event logs gather on client computers. To support these reports, you must modify the event log settings for Windows security on clients so that it logs all Success logon events. These reports include the following:

  - Hardware 03A - Primary computer users
  - Hardware 03B - Computers for a specific primary console user
  - Hardware 04A - Computers with multiple users (shared)
  - Hardware 05A - Console users on a specific computer

- **Import software license information** Use the Import Software Licenses Wizard to import Microsoft Volume License Statements and General License Statements from non-Microsoft vendors into the Asset Intelligence catalog.

- **Install an Asset Intelligence synchronization point** The site system role for the Asset Intelligence synchronization point connects to System Center Online to download and synchronize Asset Intelligence catalog information. You must install this role on a site system in the central administration site for hierarchy configurations. This requires Internet access by using Transmission Control Protocol (TCP) port 443. You can configure a synchronization schedule, which by default is set to run every seven days.

- **Configure Asset Intelligence maintenance tasks** By default, this Asset Intelligence feature uses two maintenance tasks:

  - **Check Application Title With Inventory Information** Checks that the software title the software inventory reports reconciles with the software title in the Asset Intelligence catalog.

- ■ **Summarize Installed Software Data** Provides information that appears in the Inventoried Software node. This task is available only on primary sites.
- ■ **Configure Asset Intelligence Security** You can use the Asset Manager security role to provide the required permissions to manage the Asset Intelligence synchronization point and modify the Asset Intelligence reporting classes and permissions related to software inventory, hardware inventory, and software metering.

Software metering

Software metering enables you to monitor program usage on Configuration Manager client computers. You can summarize software-metering data to produce useful reports that can help you plan for your organization's software purchases.

Software metering can collect the following information:

- ■ **Program usage information** Includes start time, end time, meter data ID, resource ID, user name, users of Terminal Services sessions, and whether Terminal Services is running
- ■ **File information** Includes file ID, file name, file version, file description, and file size (in KB)
- ■ **Program information** Includes company name, product name, product version, and product language

Software metering uses two main components to perform data-collection tasks: the Software Metering Agent and software-metering rules. When enabled, the Software Metering Agent reports software-metering data based on the site's software-metering rules. You must configure software-metering rules before data collection about a program's usage begins.

The software-metering process includes the following steps:

1. The Software Metering Agent examines each program that runs on the client and determines whether the program file's information matches any software-metering rule. The agent collects usage data each time an actively monitored program runs on the client regardless of whether the client is connected to the network.
2. The agent uploads the data to the management point on its next Software Metering Usage Report Cycle. If the client is not connected to the network, the data remains on the client and then uploads to the management point the next time the client connects to the network.
3. The management point forwards the data to the site server.
4. The site server adds the data to the site database.

Software-metering data is summarized on a specified schedule, and it replicates to the central administration site, which contains usage data from all client computers within the hierarchy.

After the site server summarizes client data, you can view the information by using queries and reports. This data, combined with data from software inventory and Asset Intelligence, can assist your organization in determining its software usage. You can configure three elements of software metering: Software Metering Agent, software-metering rules, and automatic generation of software-metering rules.

Configuring the Software Metering Agent

When enabled, the Software Metering Agent collects usage data for programs specified in software-metering rules. Typically, the agent is enabled by default. However, if the agent has been disabled, you can enable it in Client Settings within the Configuration Manager console. You can also customize the software-metering data collection schedule, which is every seven days by default.

Configuring software-metering rules

After ensuring that the Software Metering Agent is enabled, configure software-metering rules. You must create and configure software-metering rules to specify the applications you want the Software Metering Agent to monitor. The Create Software Metering Rule Wizard leads you through the creation of a new software-metering rule.

Automatic software-metering rules

Configuration Manager enables you to generate software-metering rules automatically, based on recent usage-inventory data. If Configuration Manager automatically generates a software-metering rule, the generated rule will be disabled. You must enable that rule if you want clients to report usage of the software specified in the automatically generated rule. In addition, you might want to disable a software-metering rule but keep it for later use.

You can configure the automatic generation of rules as follows:

1. Open the Software Metering Properties dialog box and then select the Automatically Create Disabled Metering Rules From Recent Usage Inventory Data check box if it is not already selected. This option is selected by default.

2. Specify the percentage of a site's computers that must use a particular program before a software-metering rule for that program is created automatically. The default value is 10 percent.

3. To protect against auto-generating an unmanageable number of disabled rules, specify the number of rules after which no new software-metering rules are created automatically. The default value is 100 rules.

4. Configure the length of time the software-metering data stays stored in the site database. The default value is 90 days.

To enable or disable a software-metering rule, you must perform the following procedure:

1. In the Configuration Manager console, click the Assets And Compliance workspace and then click Software Metering.

2. Select and then right-click one or more software-metering rules and then click either Enable or Disable.

Summarization tasks

The Summarize Software Metering tasks perform data summarization to reduce the amount of data the Configuration Manager site database stores. Data summarization runs daily and only runs against usage data that is older than 12 hours. Data summarization is required for all Configuration Manager software-metering reports to display meaningful data.

You should know when the summarization last occurred if you want to understand what data the

most current set of summary data contains. You can refer to the Software Metering Summarization Progress report in Configuration Manager to determine when the summarization last occurred.

The software-metering summarization tasks are:

- **Summarize Software Metering File Usage Data** The Summarize Software Metering File Usage Data task condenses software-metering file usage data from multiple records into one general record. This record provides information about the program name, version, language, and number of distinct users over intervals of 15 minutes and 1 hour. This process compresses and optimizes the amount of data stored in the Configuration Manager site database. By default, the Summarize Software Metering File Usage Data task runs daily. For every hour, and every 15-minute interval within the hour, the task calculates the total number of distinct user/computer combinations that are running the matching program. Within the 15-minute intervals, this approximates the number of concurrent users. For example:

  - If a single user is using a software program and signs in to three computers simultaneously, this counts as three usages.

  - If three users sign in to a computer that is running Terminal Services or Remote Desktop Services, and all three are running the software program, this counts as three usages.

  - If a single user starts and stops the software program on the same computer three times during the hour, this counts as one usage for that user.

- **Summarize Software Metering Monthly Usage Data** This task condenses detailed software-metering usage data from multiple records into one general record. This record provides information about the program name, program version and language, program running times, number of usages, last usage, user name, and computer name. Data summarization helps compress the amount of data in the Configuration Manager site database. Monthly software usage data replicates to the central administration site. The summarization information includes the number of times each matching software program runs on a particular computer and by a particular user during the month. By default, the task runs daily, and the summarization period is one month.

The following maintenance tasks remove old software-metering data and summarized data from the Configuration Manager site database:

- **Delete Aged Software Metering Data** This task deletes all unsummarized software-metering data that is older than the number of days specified. By default, the task runs every day and deletes software-metering data that is older than five days. You can configure the number of days to be any number from 2 through 255.

- **Delete Aged Software Metering Summary Data** This task deletes summarized software-metering summary data that is older than the number of days specified. By default, the task runs every Sunday to delete software-metering summary data that is older than 270 days.

Exam Tip

Remember the purpose of software-metering rules.

> **Thought experiment:** Contoso Asset Intelligence
>
> **You want to find out more about how applications are being used at Contoso. To accomplish this goal, you have implemented Configuration Manager. After experimenting with the various settings, determine the answers to the following questions:**
>
> 1. **What must you enable to view information about users who have run a specific executable?**
> 2. **You run an Asset Intelligence report to find computers that multiple users are using, but the report displays no records. How can you troubleshoot and correct the issue?**

Objective summary

- In the Monitoring workspace of the Configuration Manager console, you can monitor all deployments, including software updates, compliance settings, applications, task sequences, packages, and programs.
- Applications in Configuration Manager support state-based monitoring, which you can use to track the last application deployment state for users and devices.
- Asset Intelligence enhances Configuration Manager's inventory capabilities by extending hardware inventory and adding functionality for license reporting.
- You can use Asset Intelligence hardware requirements to provide data to help verify that computers meet hardware requirements for software titles before you target them for deployment.
- Software metering enables you to monitor program usage on Configuration Manager client computers.
- The Software Metering Agent reports software-metering data based on the site's software-metering rules.
- The Summarize Software Metering tasks perform data summarization to reduce the amount of data that the Configuration Manager site database stores.

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. By default, what is the maximum number of automatically created Configuration Manager software-metering rules?

    A. 10

    B. 50

    C. 100

    D. 1,000

2. By default, what percentage of a site's computers must use a particular program before a software-metering rule for that program is created automatically?

    A. 5 percent

    B. 10 percent

    C. 15 percent

    D. 20 percent

3. You are monitoring application deployment for computers in a specific collection. Which of the following compliance states indicates that a requirement or dependency wasn't met?

    A. In Progress

    B. Error

    C. Requirements Not Met

    D. Success

Objective 2.6: Manage content distribution

Distribution points store content such as applications, packages, software updates, and operating system images. Configuration Manager clients access this content as instructed by specific deployment tasks. Deploying and managing distribution points requires considering the amount of content on the distribution point, available network bandwidth, and the ability to monitor the status of the distribution point.

This section covers the following topics:

- Content management
- Distribution points
- Network bandwidth considerations
- Content library
- Content management
- Content distribution
- Prestaging content

Content management

Distribution points provide content to Configuration Manager clients. Before you can use Configuration Manager to deploy software to a client device, you must have at least one distribution point that the client can access. Depending on the size of your environment, you can implement additional distribution points as necessary to ensure efficient access to content for Configuration Manager clients.

    Distribution points host content files for:

- Applications.
- Packages.
- Software updates.

- Operating system deployments.

The efficiency of your distribution points depends on two main considerations:

- Managing content distribution to your distribution points in a way that minimizes impact to network bandwidth. You don't want to block clients from accessing content each time you move new data to the distribution point.

- Ensuring that Configuration Manager clients connect to appropriate distribution points to access content for deployments. You want to ensure that clients have access to a local distribution point rather than connecting to one on the other side of the country or even one on another continent.

In Configuration Manager, the distribution point site system role includes a number of features to utilize network bandwidth and store content efficiently. These include:

- **Scheduling and throttling** You can schedule a specific time for availability and limit the transfer rate you use when you distribute content to a distribution point over a network connection. You can restrict rate limits to a percentage of available bandwidth, or you can configure throttling based on the size of data blocks, in kilobytes (KB), and the time delay between sending each data block (in seconds). Note that these options do not apply when the distribution point is on a site server or when you configure it as a pull-distribution point.

- **Content library** The content library is a common repository that stores all content files for packages, applications, software updates, and operating system deployments. Single-instance storage prevents storage of multiple copies of the same content files on the distribution point. This provides a huge benefit by decreasing hard disk space requirements for content. The content library is on the site server and on each distribution point. The Package Transfer Manager site server component transfers content from the site server to a distribution point.

- **Content validation** You can use content validation to ensure the integrity of content that the content library stores. You can run content validation on a schedule that you configure for the distribution point, or you can validate content manually from the properties of any instance of content. You can view the validation status on the Content Status node of the Monitoring workspace.

Distribution points

You can deploy distribution points on computers running server operating systems such as Windows Server 2012 R2, on client operating systems such as Windows 8, and to Microsoft Azure. Before you deploy a new distribution point, consider the following:

- **Association to boundary groups** When you can associate a distribution point with one or more boundary groups, it becomes a preferred distribution point for clients within the boundary group's boundaries. When you associate a distribution point with a boundary group, you configure the connection speed to the distribution point as either Fast (the default) or Slow. Clients that are in an assigned boundary group attempt to use their preferred distribution points for accessing content. For clients outside the assigned boundary groups, you have the option of allowing fallback access to the distribution point. If a preferred distribution point is not available to the client, the client uses an available fallback distribution point.

- **Use of distribution point groups** A distribution point group is a logical grouping of

distribution points that you can use to simplify content distribution to multiple distribution points. For example, if you distribute content to a distribution point group, all distribution points that are group members receive the content. Beginning with System Center 2012 R2 Configuration Manager, if you add a new distribution point to an existing distribution point group, the content hosted on other members of the group will automatically be added to the new distribution point.

You can associate collections with distribution point groups. This enables you to distribute content to collections directly rather than having to specify distribution point groups during deployment. Any distribution points that are members of a distribution point group that you associate with a collection will receive the content that has been distributed to that collection.

- **Support for Internet-based or mobile clients** To support Internet-based clients or mobile clients, you must configure the distribution point to accept HTTPS communication. The distribution point must have a valid public key infrastructure (PKI) web server certificate to use HTTPS communication. In addition, to support client authentication, client computers must have a valid PKI client certificate installed from a trusted certification authority (CA). Internet client support requires additional configuration, such as configuring a fully qualified domain name (FQDN), firewall access rules, and the distribution point to support Internet-based clients. In many scenarios, cloud-based distribution points replicate this functionality without the complexity of configuring communication.

- **Network connection speed to the content source location** By default, all distribution points in a boundary group are configured with a fast connection. When a client is connecting to a fallback distribution point, which is one used when the one to which the client was going to connect is unavailable, Configuration Manager automatically classifies the connection as Slow. You can also specify a distribution point as having a slow connection in relation to a boundary group on which it is a member. It is also possible to configure deployments to behave differently, depending on the connection speed.

- **Content on demand** You can enable the Distribute The Content For This Package To Preferred Distribution Points property for an application or package to enable on-demand content distribution to preferred distribution points. If you enable this setting, when a client requests content that is not available on a preferred distribution point, the content downloads to all preferred distribution points.

- **Scheduling and throttling requirements** You can configure rate limits on distribution points to control the bandwidth used to copy the content from the site server. You can do this on all distribution points with the exception of a distribution point on a site server or a distribution point that you configure as a pull-distribution point. You can configure rate limits by specifying the amount of bandwidth a transfer can use. In addition, you can schedule when the transfer can occur.

- **Prestaged content requirements** When scheduling and throttling do not provide the desired control over the content-transfer process, you can configure the Enable This Distribution Point For Prestaged Content setting in the distribution point properties on the General tab. When you enable this setting, you can control how content is copied to a distribution point on a per-package basis. The following options are available:
  - Automatically Download Content When Packages Are Assigned To Distribution Points

- Download Only Content Changes To The Distribution Point
- Manually Copy The Content In This Package To The Distribution Point

- **Support for operating system deployment** In System Center 2012 R2 Configuration Manager, you can enable distribution points to support Pre-Boot Execution Environment (PXE) and multicast. You can use both of these configurations for operating system deployment tasks. PXE enables distribution points to respond to incoming PXE boot requests by clients on the local network. Multicast enables deploying operating system images by sending data to multiple clients simultaneously instead of by using a separate connection to each client. If you enable PXE or multicast settings on a distribution point, the Windows Deployment Services server role installs automatically on the server. PXE and multicast are not supported on a workstation-based distribution point.

- **BranchCache** System Center 2012 R2 Configuration Manager and newer versions support BranchCache distributed mode. You can configure software deployments to support BranchCache. When a BranchCache-enabled client downloads BranchCache-enabled content from a BranchCache-enabled distribution point, the client caches the software locally. When additional BranchCache-enabled clients on the same subnet need to download the content, they download it from a peer and then cache it. When you use BranchCache in a remote location, only the initial client needs to download the content from a distribution point.

Pull-distribution points

When you assign content to a pull-distribution point, the pull-distribution point copies the content files from the specified distribution point. This reduces the processing usage of the site server when distributing content to a large number of distribution points. Pull-distribution points support the same configurations and functionality as typical Configuration Manager distribution points with the following exceptions:

- You cannot configure a cloud-based distribution point as a pull-distribution point or as a source server for pull distributions.
- You cannot configure a distribution point on a site server as a pull-distribution point.
- Prestaged content distribution settings override pull distribution. If you configure the content for prestaging, a pull-distribution point will not pull it.
- Rate limit configurations do not apply to pull-distribution points.
- Retry settings do not apply to pull-distribution points. The Package Transfer Manager service on the site server does not notify the pull-distribution point to start downloading the content until it has verified that the pull-distribution point is available on a source server.
- If the pull-distribution point is in a remote forest, the Configuration Manager client must be installed on the distribution point, and the Network Access Account must be able to access the source distribution point.

You can configure a distribution point as a pull-distribution point during the creation of the distribution point or after the distribution point is in place. When configuring a distribution point as a pull-distribution point, you must also specify one or more source distribution points. You can use only distribution points that support HTTP as source distribution points if you are using the Configuration Manager console. When configuring multiple source distribution points, you can assign priorities to

each.

Cloud-based distribution points

System Center 2012 Configuration Manager Service Pack 1 (SP1) and later support cloud-based distribution points in Microsoft Azure. You configure cloud-based distribution points in the Cloud services node in the Administration workspace. You must also configure a client settings policy to allow clients to use cloud-based distribution points. Finally, to help control the costs associated with a cloud-based distribution point, you can configure thresholds for the amount of storage the distribution point uses and the amount of client traffic to the distribution point.

Cloud-based distribution points include the following distribution point features:

- Support for individual or group-based management
- A possible fallback distribution point
- Support for intranet and Internet-based clients
- Support for BranchCache-configured systems to download content from the cloud-based distribution point

There are additional features specific to using a cloud-based distribution point in Microsoft Azure. When content is sent to a Microsoft Azure–based distribution point, the content is encrypted while traversing the Internet. In addition, you can quickly scale the size of your distribution points as necessary without investing in additional hardware.

Cloud-based distribution points have the following limitations:

- Cannot host software update packages
- Cannot be configured for PXE or multicast deployments
- Cannot be used with task sequences that use the Download Content Locally When Needed By Running Task Sequence deployment option
- Do not support packages that run from the distribution point
- Do not support streaming packages
- Cannot be configured for prestaged content
- Cannot be configured as pull-distribution points

Network bandwidth considerations

Distributing content in a Configuration Manager infrastructure generates network traffic at various points in the distribution process:

- When content files are copied from the source path to the site server if the source path is on a different server from the site server. For this scenario, files transfers use the Server Message Block (SMB) protocol. The effect of this traffic on the network is usually negligible because it occurs over a high-speed network.

- When content files are copied from the site server to remote distribution points. In this situation, file transfers use the SMB protocol, which can have a significant impact on network usage, especially over low-speed network connections. You can manage this traffic by using content throttling and distribution scheduling except for distribution points that are located on site servers.

Consider the following when configuring content throttling and scheduling:

- Content distribution detects updated files so that only the new or updated files are distributed when content source files are updated.

- You can configure scheduling and set specific throttling settings that determine when and how much bandwidth is consumed during content distribution to remote distribution points. You can configure the throttling settings on the Rate Limits tab and the scheduling settings on the Schedule tab. The Rate Limits and Schedule tabs appear only in the properties for distribution points that are not installed on a site server.

- You can configure remote distribution points with different settings based on the network bandwidth limitations from the site server to the remote distribution point. Each remote distribution point that you configure as a pull-distribution point uses its own throttling settings and schedule to transfer content.

Distribution point priority

Beginning with System Center 2012 R2 Configuration Manager, Configuration Manager assigns a priority to each distribution point. This priority is based on how long content distribution has taken in prior distributions, on average. This priority is evaluated constantly as you distribute content. When you distribute content to multiple distribution points at the same time, the highest-priority distribution point receives content first. The Configuration Manager console does not include any options for managing the distribution point priority settings.

Bandwidth management planning

When planning for network bandwidth management in Configuration Manager, consider how you can reduce the content distribution network traffic:

- Configure scheduling and bandwidth throttling settings on distribution points and senders.

- Use content prestaging to transfer the content offline.

- Place distribution points on the same high-speed networks as clients.

- Install standard applications as part of the operating system images.

- Include standard application installer files in the operating system image and use custom task sequence commands to install those applications from the local source files.

Both senders and the Package Transfer Manager service use file-based replication and the SMB protocol. Any firewalls placed between sites or between the site server and distribution points must allow SMB traffic.

Content library

The content library hosts content files. These files include software updates, operating system deployment images, and files related to packages and applications. Each site server and distribution point hosts a content library. The content library uses a single-instance store for the files it hosts to reduce the amount of disk space that content consumes. Before content files are transferred to a content library, a check is performed to determine whether the file is already present. Files are not added if they are already present in the content library. An association is made between the existing file and the newly transferred application or package.

When you deploy a Configuration Manager distribution point, you can specify the volumes that will host the content library. When you specify multiple volumes, you specify a priority for each volume. Configuration Manager transfers content to volumes based on priority until the highest-priority volume has less than the minimum amount of configured available free space. You must configure these settings when you deploy the distribution point because you cannot alter them after you deploy it.

In environments where site servers and distribution points are hosted on servers running the Windows Server 2012 and Windows Server 2012 R2 operating systems, you can enable deduplication on volumes that store the content library to increase storage efficiency. You should also consider placing the content library on volumes hosted on Storage Spaces. Storage Spaces simplify the process of increasing storage later.

System Center 2012 Configuration Manager SP1 and System Center 2012 R2 Configuration Manager enable you to move content to a different location by using the Content Library Transfer tool, which is available as part of the System Center 2012 Configuration Manager toolkit. You can download this toolkit from the Microsoft Download Center.

Prerequisites for content management

When you deploy a distribution point, Configuration Manager can install and configure Internet Information Services (IIS) automatically. IIS must be present on all distribution points. The only time that you should not have Configuration Manager deploy and configure IIS is when IIS is present already on the distribution point.

When you deploy a distribution point to a site server, you can use only the computer account of the site server as the Site System Installation Account. When you deploy a distribution point to a computer that is a member of the same Active Directory forest, ensure that the site server's computer account is a member of the local Administrators group on a target computer.

If all the management points in the Configuration Manager site are configured for HTTP, you can use self-signed certificates with the distribution point. When all management points in the Configuration Manager site are configured to use HTTPS, you should use a certificate issued by a trusted CA. This certificate must be configured with an intended use that includes client authentication, and it must allow the private key to be exported.

If you use Windows Server 2012 or Windows Server 2012 R2, consider enabling deduplication on the volume that hosts the distribution point. This minimizes the amount of space consumed by content storage.

You can add the Distribution Point Site System role to an existing site system, or you can add a new site system server and then add the Distribution Point Site System role to the new site system server. Before installing the Distribution Point Site System role, ensure that the account you use to install the site system role is a member of the local Administrators group on the site system.

Use the following set of instructions to install and configure a distribution point site system role:

1. In the System Center 2012 R2 Configuration Manager console, click the Administration workspace.

2. Expand Site Configuration and then click the Servers And Site System Roles node.

3. To create a new site system role, right-click Servers And Site System Roles and then click Create Site System Server. To add a new role to an existing site server, in the results pane, right-click the server and then click Add Site System Roles. Both methods open the General page of the Create Site System Server Wizard.

4. On the Select A Server To Use As A Site System page, configure the following options as necessary:

   - **Name** For a new site system server, you must provide either the NetBIOS or FQDN of the computer that will host the system role. If you supply the NetBIOS name, it resolves automatically to the required FQDN for use. For existing site system servers, this value will be configured already.

   - **Site Code** For a new site system server, select the site code that will be associated with this site system. For existing site system servers, this value will be configured already.

   - **Specify An FQDN For This Site System For Use On The Internet** If you use this site system to communicate with Internet-based clients, you need to specify the FQDN that is resolvable from the Internet. This setting is optional, depending on whether you support Internet-based clients.

   - **Require The Site Server To Initiate Connections To This Site System** The default behavior of site systems is to initiate a connection to the site server to send status information. However, in untrusted locations, such as a perimeter network or an untrusted domain, this might not be desirable. The setting ensures that the site server always initiates connections with the site system.

   - **Use The Site Server's Computer Account To Install This Site System** By default, the site server's computer account is used to install the site system. To install the site system successfully, be sure that the site server's computer account is added to the local Administrators group on the computer to which you are adding this site system role.

   - **Use Another Account For Installing This Site System** You may choose to use a specific account for the site system's installation account. If you use a standard user account, make sure that the account is a member of the local Administrators group on the site system.

5. On the Specify Internet Proxy Server page, specify any proxy information required to connect to the Internet.

6. On the Specify Roles For This Server page, select the Distribution Point check box.

7. On the Distribution Point page, configure the following options as necessary:

   - **Install And Configure IIS If Required By Configuration Manager** This option allows Configuration Manager to install and configure IIS on the site system server. If IIS is installed on the site system already, this option ensures that Configuration Manager configures it as necessary during the distribution point site system role-installation process.

   - **Description** This is a text box in which you can provide a brief description of the distribution point.

   - **Specify How Client Computers Communicate With This Distribution Point** Depending on how you configure your site, you might have the option to specify whether clients use HTTP or HTTPS to communicate with the distribution point. If this distribution point is intended to support mobile, Mac OS X, or Internet-based clients, you must configure HTTPS.

   - **Create A Self-signed Certificate Or Import A PKI Client Certificate** By default, a distribution point creates a self-signed certificate to use for PXE communications during operating system deployments. If you use HTTPS for client communication, import a certificate that a trusted CA issues.

   - **Enable This Distribution Point For Prestaged Content** When you enable this option, the site server adheres to the content properties that govern the transfer to prestaged, content-enabled distribution points.

8. On the Drive Settings page, specify the drive settings for the distribution point. Configure the following options as necessary:

   - **Drive Space Reserve (MB)** This setting enables you to specify the amount of space on the drive that should be reserved and the amount that should remain free. Configuration Manager will not use the specified free space for distribution point content storage.

   - **Specify The Locations For The Content Library And Package Share On This Distribution Point** You can specify two disk drives for the content library location and two disk drives for the package share location. By default, Automatic is selected for all options, so the drive with the most available disk space is used. To ensure that you control the content library and package share locations, we recommend specifying a drive letter for primary and secondary locations.

9. If this is a pull-based distribution point, on the Pull Distribution Point page, select the Enable This Distribution Point To Pull Content From Other Distribution Points check box. If you select this option, you must configure the source distribution points.

10. On the PXE Settings page, select the Enable PXE Support For Clients check box if necessary. This setting enables or disables PXE support on the distribution point. If you enable this option, you can configure additional options, such as enabling unknown computer support and requiring a password when computers start by using PXE.

11. On the Multicast page, select the Enable Multicast To Simultaneously Send Data To Multiple Clients check box if necessary. If you enable this option, you can configure additional options such as initiating a Multicast Connection Account, specifying multicast address settings, and enabling scheduled multicast sessions. Furthermore, note that if you select this option, Windows

Deployment Services will be installed if necessary.

12. On the Content Validation page, select the Validate Content On A Schedule check box if necessary. If you enable this option, you can configure a schedule for content validation. Content validation verifies the integrity of the content files that the distribution point stores.

On the Boundary Groups page, you can associate existing boundary groups with the distribution point. This creates a protected distribution point for boundaries that are members of the associated boundary groups. You also can use this page to create new boundary groups as necessary. You can use Allow Fallback Source Location For Content to enable clients outside the boundary groups to use the distribution point when no other distribution point is available.

Distribution point monitoring

In the Monitoring workspace of the Configuration Manager console, you can use the Distribution Status folder to perform monitoring for:

- **Content status** This includes the status of individual packages, applications, and driver packages in relation to their distribution points. When viewing the content status, you can cancel an in-progress distribution.
- **Distribution point group status** This includes the aggregate status of content assigned to a specific distribution point group.
- **Distribution point configuration status** This includes the aggregate status of the content assigned to a distribution point and the status of the optional components (PXE and multicast).

To troubleshoot content distribution, you can use:

- Configuration Manager reports.
- Configuration Manager status messages.
- Configuration Manager logs.

To troubleshoot issues with content management, you can use the following Configuration Manager logs:

- **SMSProv.log** Troubleshoot actions started from the user interface (UI) or the software development kit (SDK).
- **DistMgr.log** Troubleshoot content creation, update, deletion, and start of distribution. You can use this log on the site server from the source site to verify that Distribution Manager processes the content.
- **Scheduler.log** View the current status of the sender job. You can use this log on the site server from the source site to verify that the content was queued for the sender.
- **Sender.log** Troubleshoot the copy of the compressed content to the destination site. You can use this log on the site server from the source site to determine whether the sender has transferred the content to a different site.
- **Despooler.log** Troubleshoot the extraction of the compressed copy to the content library on the destination site. You can use this log file on the site server from the destination site to verify that the despooler received and processed the content.
- **PkgXferMgr.log** Troubleshoot the distribution of content from the site server to the distribution

point. You can use this log on the site server to determine whether the Package Transfer Manager processed the content and transferred it to a distribution point located in the same site as the site server.

- **SMSDPProv.log** Troubleshoot the addition of content to the content library on the distribution point. You can use this log on a distribution point to verify that content was added to the content library.

- **SMSPXE.log** Troubleshoot the PXE provider. You can find this log on a distribution point that is configured to use PXE.

Content distribution

Client computers can access only content that has been distributed to distribution points. Configuration Manager places content files in containers called packages. The distribution process copies these packages to distribution points from the source files in the source path. Packages can host application deployment types, packages, deployment packages, operating system images, driver packages, boot images, and task sequences.

To distribute content to distribution points, perform the following procedure:

1. In the Configuration Manager console, click the Software Library workspace.

2. Expand the appropriate folder (Application Management, Software Updates, or Operating Systems).

3. Access the node for the content that you need to distribute.

4. Select the content and then, on the ribbon, click Distribute Content.

5. In the Distribute Content Wizard, on the Review Selected Content page, verify that the content that is listed is the content you want to distribute. If you are distributing an application, you can select the Detect Associated Content Dependencies And Add Them To This Distribution check box.

6. On the Specify The Content Destination page, click Add. You can add a content destination that is associated with collections, a distribution point, or a distribution point group.

By default, Configuration Manager grants access to the package folder on a distribution account to the Users And Administrators groups. If necessary, you can mediate access to the package folder by configuring access for additional accounts and groups. You do not have to configure the Network Access account as a Package Access account because the Users group already has this account as a member. Mobile devices always access package content anonymously. This means that you cannot use Package Access accounts to mediate access to package content for mobile devices.

Updating content

When you change the source files for specific content, update the copy of the content on the distribution points. When you update content on distribution points, Configuration Manager increments the package version and updates only the files with changes.

To update content on distribution points, perform the following procedure:

1. On the Configuration Manager console, click the Software Library workspace.

2. Expand the appropriate folder: Application Management, Software Updates, or Operating

Systems.

3. Access the node for the content you want to update.

4. Select the content and then, on the ribbon, click Update Distribution Points.

5. In the Configuration Manager message that asks whether you want to refresh the content, click Yes.

Redistributing, validating, or removing content

Sometimes you might need to redistribute content to distribution points, such as when you need to repair corrupted content files. You can use one of the following three methods to perform content redistribution:

- From the Software Library workspace, select the content and then open the Properties dialog box. Click the Content Locations tab, select the distribution point or distribution point group, and then click Redistribute.
- From the Administration workspace, open the Distribution Points node. Right-click a distribution point and then click Properties. On the Content tab, select the content and then click Redistribute.
- From the Administration workspace, open the Distribution Point Groups node. Right-click a distribution point group and then click Properties. On the Content tab, select the content and then click Redistribute.

Managing content in progress

System Center 2012 R2 Configuration Manager introduces the ability to manage content while it is copying to a distribution point. From the Monitoring workspace, you can cancel distributions in progress if necessary. In addition, you can redistribute content that fails to distribute. To cancel content distribution:

1. From the Monitoring workspace, open the Distribution Status node and then select Content Status.

2. Select the distribution that you want to manage and then click the View Status link.

3. On the In Progress tab, in the Asset Details section, right-click the target server and then select Cancel.

Monitoring content status

Configuration Manager provides extensive content monitoring capabilities, including content status, number of failures, pending distributions, and successful distributions. Methods that you can use to monitor content status on distribution points include:

- **Content Status** In the Monitoring workspace, under the Distribution Status folder, click Content Status. When you click this node, the results pane displays a list of all content. You can right-click specific content and then click View Status to display status information that pertains to content distribution and validation.
- **Package Transfer Manager** The Package Transfer Manager component (SMS _PACKAGE_TRANSFER_MANAGER) provides status information that pertains to package transfers to distribution points.

- **Package Transfer Manager component log file (PkgXferMgr.log)** You can find the PkgXferMgr.log file on the primary site server in the *<Configuration Manager Installation Path>*\Logs folder. This log file provides extensive information related to content distribution to remote distribution points.

- **Software Deployment Content reports** System Center 2012 R2 Configuration Manager includes several reports that pertain to content management and distribution. You can find these reports when you expand the Reporting node in the Monitoring workspace.

Prestaging content

Content prestaging enables you to transfer and preload content by using an offline method such as shipping media from a site server to a distribution point. You can use this method instead of file-based replication to reduce network traffic between the site server and the distribution point. Content prestaging:

- Works with all content types.

- Works with content libraries and package shares.

- Registers content availability automatically with the site server upon content extraction on the distribution point.

- Uses a compressed, prestaged content file with the .pkgx extension.

- Can be used to prestage multiple content files in a single operation.

- Offers a conflict detection mechanism as part of the extraction tool to prevent earlier versions of content from being prestaged on a distribution point.

Consider prestaging content for applications and packages when:

- You have limited network bandwidth between the site server and the distribution point. While distributing content over the network to a remote distribution point, and when scheduling and throttling do not reduce network traffic sufficiently, consider prestaging the content on the distribution point.

- You need to restore the content library on a site server. If a site server fails, information about packages and applications in the content library is restored to the site database as part of the restore process. However, the site backup does not include content library files by default. If you do not have a file system backup to restore the content library, you can create a prestaged content file from another site that contains the packages and applications that you need and then extract the prestaged content file on the recovered site server.

Prior to prestaging content, you must perform the following steps on the distribution point that will receive prestaged content:

1. On the General tab of the Distribution Point Properties dialog box, select the Enable This Distribution Point For Prestaged Content check box.

2. On the Distribution Settings tab of the dialog box for content type properties, ensure that you configure the Prestaged Distribution Point settings. These settings include:

   - Automatically Download Content When Packages Are Assigned To Distribution Points.

   - Download Only Content Changes To The Distribution Point.

   - Manually Copy The Content In This Package To The Distribution Point.

To prestage the content, use the following procedure:

1. Create a prestaged content file. You can create a prestaged content file for any type of content. To create the prestaged content file, right-click the content or multiselect two or more instances of content and right-click them and then click Create Prestaged Content File.

2. In the Create Prestaged Content File Wizard, specify the name and location for the content file and then complete the wizard. The Create Prestaged Content File Wizard creates a single file with a .pkgx extension.

3. Distribute the content to the distribution point. You can copy the file to a portable drive or to removable media and then send the drive or media to the location that hosts the distribution point that requires the content.

4. Import the prestaged content file to the distribution point. On the distribution point, open a command prompt and then browse to \SMS_DP$\sms\Tools. At the command prompt, type the following command and then press Enter:

Click here to view code image

```
ExtractContent /P:<PrestagedFileLocation>[\<PrestagedFileName>] /S
```

Exam Tip

Remember the limitations of pull-distribution points.

Thought experiment: **Content distribution at Contoso**

You are reviewing the distribution of content at Contoso. You are particularly concerned about when to prestage content and how to respond to application file corruption. With this information in mind, answer the following questions:

1. **You suspect that the content for a specific software application is corrupt on a distribution point. How can you fix the problem?**

2. **In which scenarios would you prestage content?**

Objective summary

- Before you can use Configuration Manager to deploy software to a client device, you must have at least one distribution point that the client can access.
- When you can associate a distribution point with one or more boundary groups, it becomes a preferred distribution point for clients within the boundary group's boundaries.
- When you associate a distribution point with a boundary group, you configure the connection speed to the distribution point as either Fast (the default) or Slow.
- A distribution point group is a logical grouping of distribution points that you can use to simplify content distribution to multiple distribution points simultaneously.

- Associating a collection with a distribution point group enables you to distribute content to collections directly.
- When you assign content to a pull-distribution point, the pull-distribution point copies the content files from the specified distribution point.
- Beginning with System Center 2012 Configuration Manager SP1, you can use cloud-based distribution points in Microsoft Azure to host a distribution point.
- The content library hosts content files. These files include software updates, operating system deployment images, and files related to packages and applications.
- When you change the source files for specific content, you need to update the copy of the content on the distribution points.
- Content prestaging enables you to transfer and preload content by using an offline method such as shipping media from a site server to a distribution point.

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 of the following cannot be used with cloud distribution points? (Choose all that apply.)

   A. App-V streaming packages

   B. Software update packages

   C. Applications that are installed after being downloaded from the distribution point

   D. Prestaged content

2. Which of the following Configuration Manager log files would you use to troubleshoot the distribution of content from the site server to the distribution point?

   A. Scheduler.log

   B. Sender.log

   C. PkgXferMgr.log

   D. SMSPXE.log

3. Which of the following Configuration Manager log files would you use to view the current status of the sender job to verify that content is queued properly for distribution?

   A. SMSPXE.log

   B. Scheduler.log

   C. Sender.log

   D. PkgXferMgr.log

4. Which of the following Configuration Manager log files would you use to troubleshoot the copying of compressed content to the destination site during content distribution?

   A. PkgXferMgr.log

   B. Scheduler.log

C. Sender.log

D. SMSPXE.log

Answers

Objective 2.1

Thought experiment

1. Configure a program to run the command.

2. Use user device affinity as a requirement when configuring a deployment type.

Objective review

1. **Correct answer:** A

   A. **Correct:** Detection methods enable you to define how Configuration Manager determines an application's installation state.

   B. **Incorrect:** Supersedence enables you to configure a relationship between a new application and an existing application that you have deployed.

   C. **Incorrect:** User device affinity is the process of associating a user with one or more specific devices.

   D. **Incorrect:** Application Catalog functions as a self-service catalog from which users can request software for installation.

2. **Correct answer:** B

   A. **Incorrect:** User device affinity is the process of associating a user with one or more specific devices.

   B. **Correct:** Application Catalog functions as a self-service catalog from which users can request software for installation.

   C. **Incorrect:** Supersedence enables you to configure a relationship between a new application and an existing application that you have deployed.

   D. **Incorrect:** Detection methods enable you to define how Configuration Manager determines an application's installation state.

3. **Correct answer:** D

   A. **Incorrect:** Detection methods enable you to define how Configuration Manager determines an application's installation state.

   B. **Incorrect:** Supersedence enables you to configure a relationship between a new application and an existing application that you have deployed.

   C. **Incorrect:** Application Catalog functions as a self-service catalog from which users can request software for installation.

   D. **Correct:** User device affinity is the process of associating a user with one or more specific devices.

4. **Correct answer:** C

A. **Incorrect:** User device affinity is the process of associating a user with one or more specific devices.

B. **Incorrect:** Application Catalog functions as a self-service catalog from which users can request software for installation.

C. **Correct:** Supersedence enables you to configure a relationship between a new application and an existing application that you have deployed.

D. **Incorrect:** Detection methods enable you to define how Configuration Manager determines an application's installation state.

Objective 2.2

Thought experiment

1. Configure a global condition related to the amount of memory and use it with a requirement so that deployment will occur only if the minimum amount of memory is available.

2. You can perform a simulated deployment to verify that the deployment settings are correct.

Objective review

1. **Correct answers:** A and C

  A. **Correct:** You must choose the Install action to make the application available through Software Center.

  B. **Incorrect:** The Uninstall action removes an application.

  C. **Correct:** The Purpose of Available makes the application available in Software Center.

  D. **Incorrect:** Choosing this option would ensure that the software was deployed, independent of the user's choice.

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

  A. **Correct:** You must choose the Install action to make the application available through Software Center.

  B. **Incorrect:** The Uninstall action removes an application.

  C. **Incorrect:** The Purpose of Available makes the application available in Software Center.

  D. **Correct:** Choosing this option would ensure that the software was deployed, independent of the user's choice.

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

  A. **Correct:** When the software is deployed as Required and the deadline has passed, software will install automatically and silently.

  B. **Incorrect:** In this scenario, the user can request it from Application Catalog.

  C. **Incorrect:** In this scenario, the user can request it from Software Center.

  D. **Correct:** When the software is deployed as Required and the deadline has passed, software will install automatically and silently.

4. **Correct answer:** C

A. **Incorrect:** When the software is deployed as Required and the deadline has passed, software will install automatically and silently.

B. **Incorrect:** In this scenario, the user can request it from Software Center.

C. **Correct:** In this scenario, the user can request it from Application Catalog.

D. **Incorrect:** When the software is deployed as Required and the deadline has passed, software will install automatically and silently.

Objective 2.3

Thought experiment

1. Users will download the Company Portal app from the Windows Store and use it to enroll in Intune.

2. A sideloading key is necessary to sideload software. A code-signing certificate the Surface 2 devices trust is required to sign the custom software digitally.

Objective review

1. **Correct answer:** B

A. **Incorrect:** This policy setting determines the frequency with which new application deployments will be detected.

B. **Correct:** This policy setting determines when updates and applications are installed as scheduled and whether a user is prompted for installation.

C. **Incorrect:** This policy setting determines whether updates that don't require a restart are installed automatically.

D. **Incorrect:** This setting determines whether a logged-on user may control when Windows restarts after the installation of an update or application that requires a restart.

2. **Correct answer:** B

A. **Incorrect:** This policy setting determines the frequency with which new application deployments will be detected.

B. **Correct:** This setting determines whether a logged-on user may control when Windows restarts after the installation of an update or application that requires a restart.

C. **Incorrect:** This policy setting determines whether updates that don't require a restart are installed automatically.

D. **Incorrect:** This policy setting determines when updates and applications are installed as scheduled and whether a user is prompted for installation.

3. **Correct answer:** C

A. **Incorrect:** This policy setting determines whether updates that don't require a restart are installed automatically.

B. **Incorrect:** This policy setting determines when updates and applications are installed as scheduled and whether a user is prompted for installation.

C. **Correct:** This policy setting determines the frequency with which new application

deployments will be detected.

D. **Incorrect:** This setting determines whether a logged-on user may control when Windows restarts after the installation of an update or application that requires a restart.

Objective 2.4

Thought experiment

1. Retiring an application prevents new deployments of the application without uninstalling the application. Uninstalling an application removes the application.

2. Uninstall deployments fail if there is an existing install deployment.

Objective review

1. **Correct answer:** A

   A. **Correct:** Retiring an application blocks new deployments but doesn't remove existing deployed software.

   B. **Incorrect:** Uninstalling an application removes it from computers on which it is installed.

   C. **Incorrect:** Superseding an application replaces one application with another.

   D. **Incorrect:** Installing an application deploys a new application. It does not remove or replace other applications.

2. **Correct answer:** C

   A. **Incorrect:** Installing an application deploys a new application. It does not remove or replace other applications.

   B. **Incorrect:** Superseding an application replaces one application with another. Because no replacement was chosen, you would not select this option.

   C. **Correct:** Uninstalling an application removes it from computers on which it is installed.

   D. **Incorrect:** Retiring an application blocks new deployments but doesn't remove existing deployed software.

3. **Correct answer:** A

   A. **Correct:** Superseding an application replaces one application with another.

   B. **Incorrect:** Retiring an application blocks new deployments but doesn't remove existing deployed software.

   C. **Incorrect:** Uninstalling an application removes it from computers on which it is installed. Although you could uninstall and then configure a new installation, this would require more administrative effort than superseding the application.

   D. **Incorrect:** Installing an application deploys a new application. It does not remove or replace other applications. Although you could uninstall and then configure a new installation, this would require more administrative effort than superseding the application.

Objective 2.5

Thought experiment

1. You must enable Software Metering to view information about users who have run a specific executable.

2. Ensure that all computers are configured to audit logon events. Typically, you would do this by using Group Policy.

Objective review

1. **Correct answer:** C

   A. **Incorrect:** The default maximum number of automatically generated Configuration Manager software-metering rules is 100.

   B. **Incorrect:** The default maximum number of automatically generated Configuration Manager software-metering rules is 100.

   C. **Correct:** The default maximum number of automatically generated Configuration Manager software-metering rules is 100.

   D. **Incorrect:** The default maximum number of automatically generated Configuration Manager software-metering rules is 100.

2. **Correct answer:** B

   A. **Incorrect:** By default, 10 percent of a site's computers must use a particular program to trigger the automatic creation of a software-metering rule.

   B. **Correct:** By default, 10 percent of a site's computers must use a particular program to trigger the automatic creation of a software-metering rule.

   C. **Incorrect:** By default, 10 percent of a site's computers must use a particular program to trigger the automatic creation of a software-metering rule.

   D. **Incorrect:** By default, 10 percent of a site's computers must use a particular program to trigger the automatic creation of a software-metering rule.

3. **Correct answer:** C

   A. **Incorrect:** In Progress status indicates that the application deployment is in progress.

   B. **Incorrect:** Error status indicates that the application failed to deploy because of an error.

   C. **Correct:** Requirements Not Met status indicates that the application did not deploy because it did not comply with a dependency or a requirement.

   D. **Incorrect:** Success status indicates that the application deployment was successful.

Objective 2.6

Thought experiment

1. You can redistribute the content to the distribution point, either from the properties of the software application or package or from the distribution point itself.

2. You would prestage content when you need to distribute large files to remote locations for

which the time or expense required to transfer the content across wide area network (WAN) links is prohibitive.

Objective review

1. **Correct answers:** A, B and D

   A. **Correct:** You can't use App-V streaming packages with cloud-based distribution points.

   B. **Correct:** You can't use software update packages with cloud-based distribution points.

   C. **Incorrect:** You can use applications that are installed after being downloaded from the distribution point with cloud-based distribution points.

   D. **Correct:** You can't use prestaged content with cloud distribution points.

2. **Correct answer:** C

   A. **Incorrect:** You use the Scheduler.log log to view the current status of the sender job. You can use this log on the site server from the source site to verify that the content was queued for the sender.

   B. **Incorrect:** You use the Sender.log log to troubleshoot the copy of the compressed content to the destination site. You can use this log on the site server from the source site to determine whether the sender has transferred the content to a different site.

   C. **Correct:** You use the PkgXferMgr.log log to troubleshoot the distribution of content from the site server to the distribution point. You can use this log on the site server to determine whether the Package Transfer Manager processed the content and transferred it to a distribution point located in the same site as the site server.

   D. **Incorrect:** You use the SMSPXE.log log to troubleshoot the PXE provider. You can find this log on a distribution point that is configured to use PXE.

3. **Correct answer:** B

   A. **Incorrect:** You use the SMSPXE.log log to troubleshoot the PXE provider. You can find this log on a distribution point that is configured to use PXE.

   B. **Correct:** You use the Scheduler.log log to view the current status of the sender job. You can use this log on the site server from the source site to verify that the content was queued for the sender.

   C. **Incorrect:** You use the Sender.log log to troubleshoot the copy of the compressed content to the destination site. You can use this log on the site server from the source site to determine whether the sender has transferred the content to a different site.

   D. **Incorrect:** You use the PkgXferMgr.log log to troubleshoot the distribution of content from the site server to the distribution point. You can use this log on the site server to determine whether the Package Transfer Manager processed the content and transferred it to a distribution point located in the same site as the site server.

4. **Correct answer:** C

   A. **Incorrect:** You use the PkgXferMgr.log log to troubleshoot the distribution of content from the site server to the distribution point. You can use this log on the site server to determine whether the Package Transfer Manager processed the content and transferred it to a

distribution point located in the same site as the site server.

B. Incorrect: You use the Scheduler.log log to view the current status of the sender job. You can use this log on the site server from the source site to verify that the content was queued for the sender.

C. Correct: You use the Sender.log log to troubleshoot the copy of the compressed content to the destination site. You can use this log on the site server from the source site to determine whether the sender has transferred the content to a different site.

D. Incorrect: You use the SMSPXE.log log to troubleshoot the PXE provider. You can find this log on a distribution point that is configured to use PXE.

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.

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.
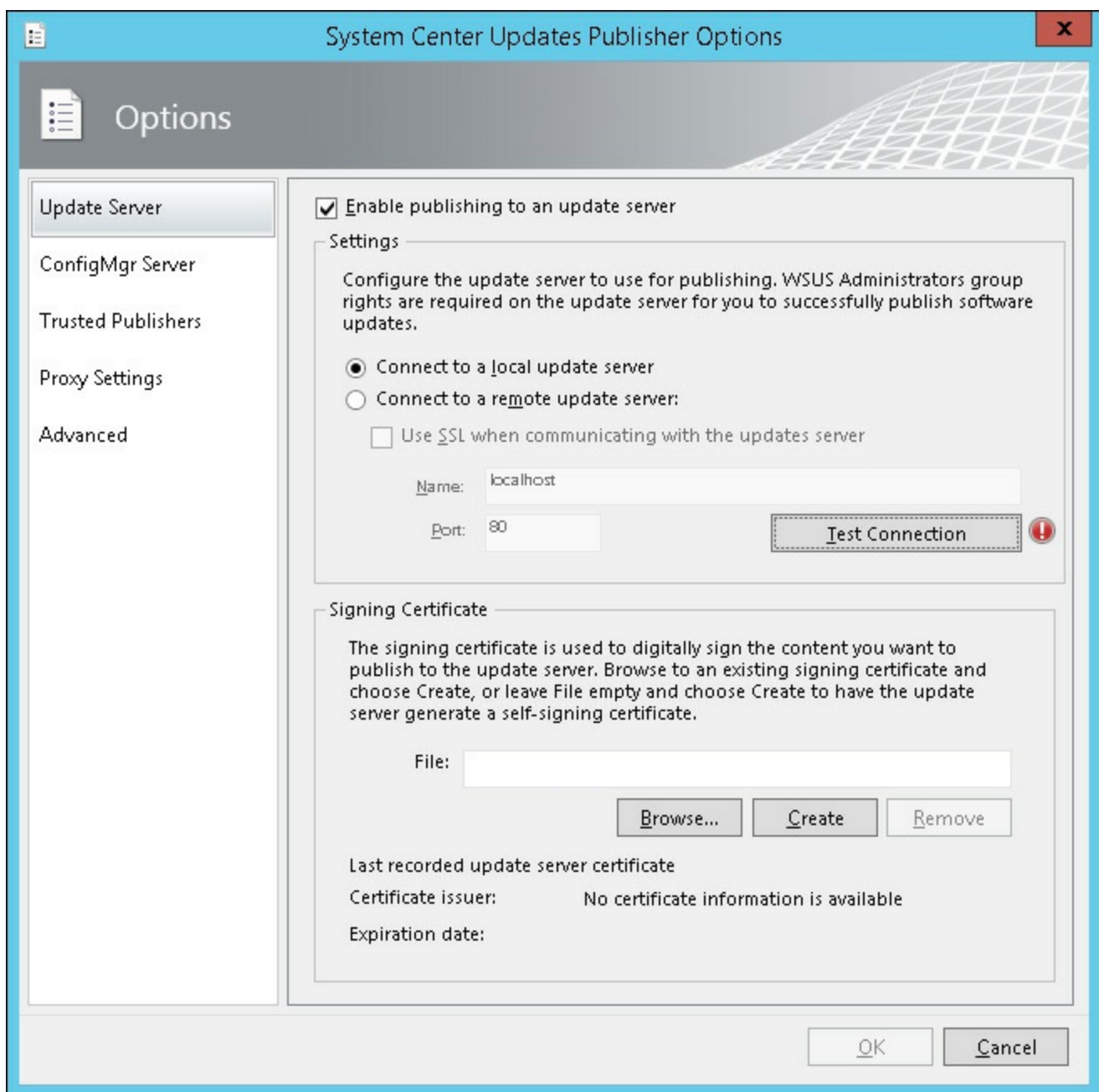
FIGURE 3-1 System Center Updates Publisher Options

ConfigMgr Server options, shown in , 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.
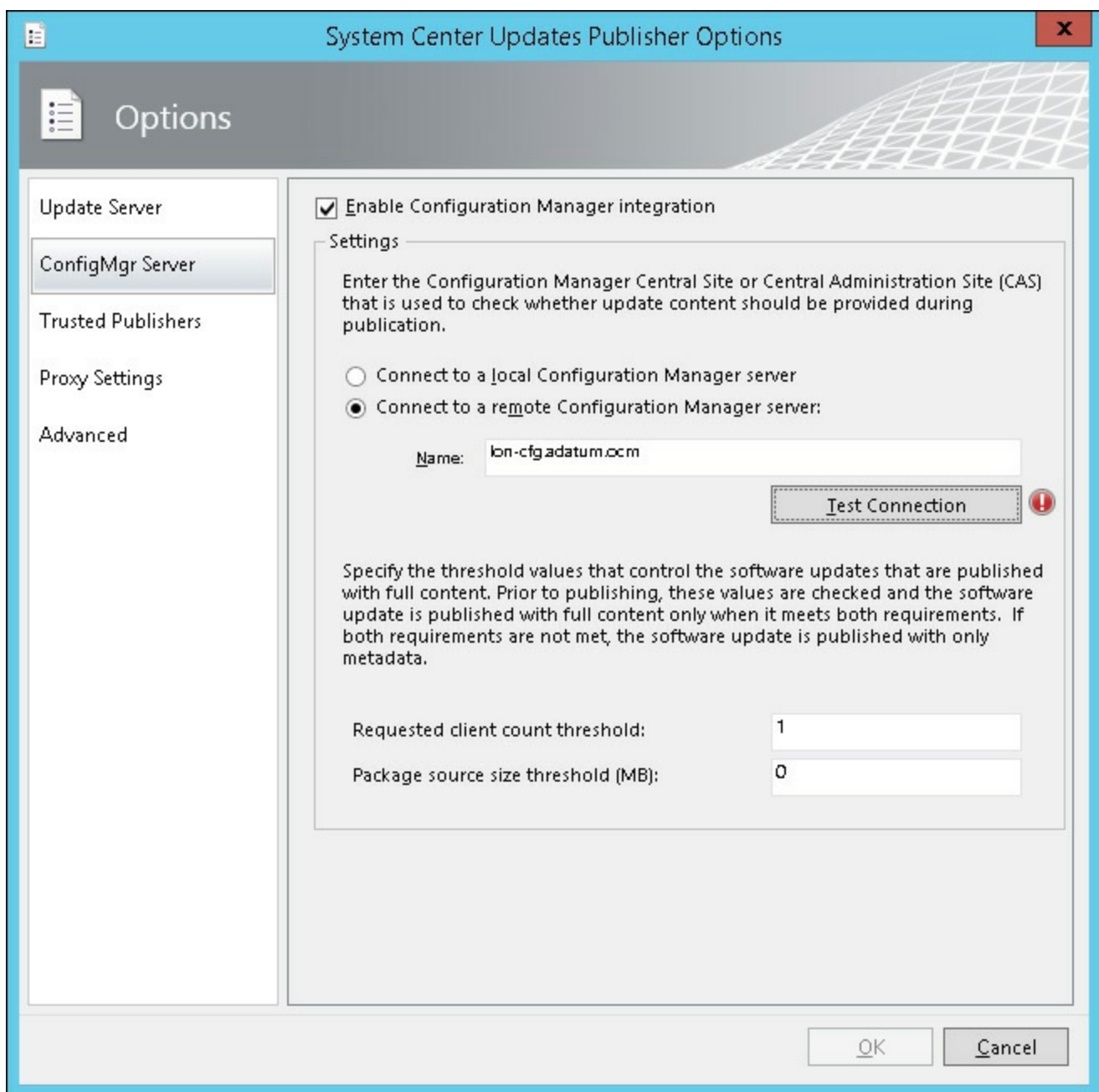
FIGURE 3-2 Configuration Manager integration

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.
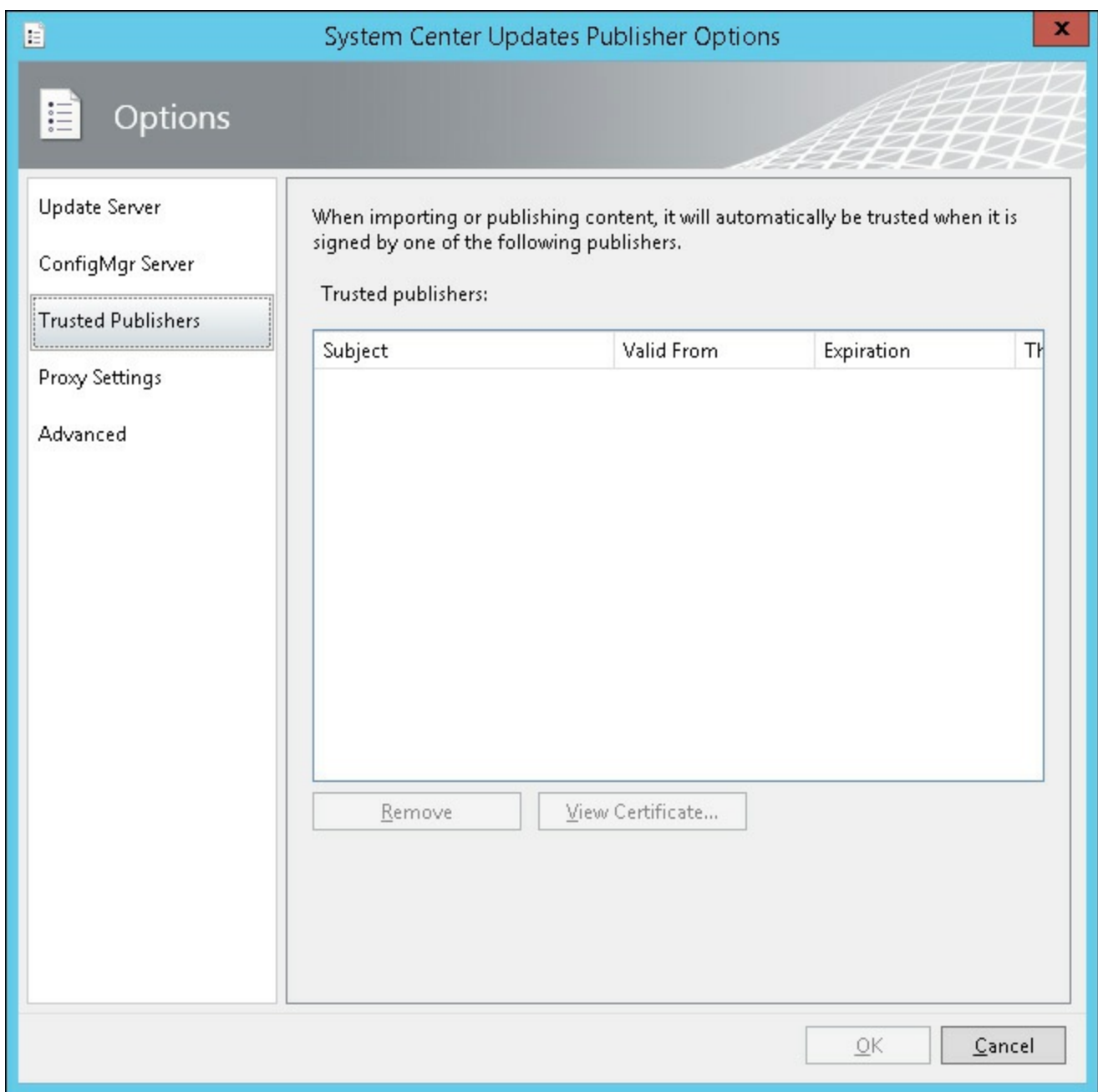
FIGURE 3-3 Trusted Publishers

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.
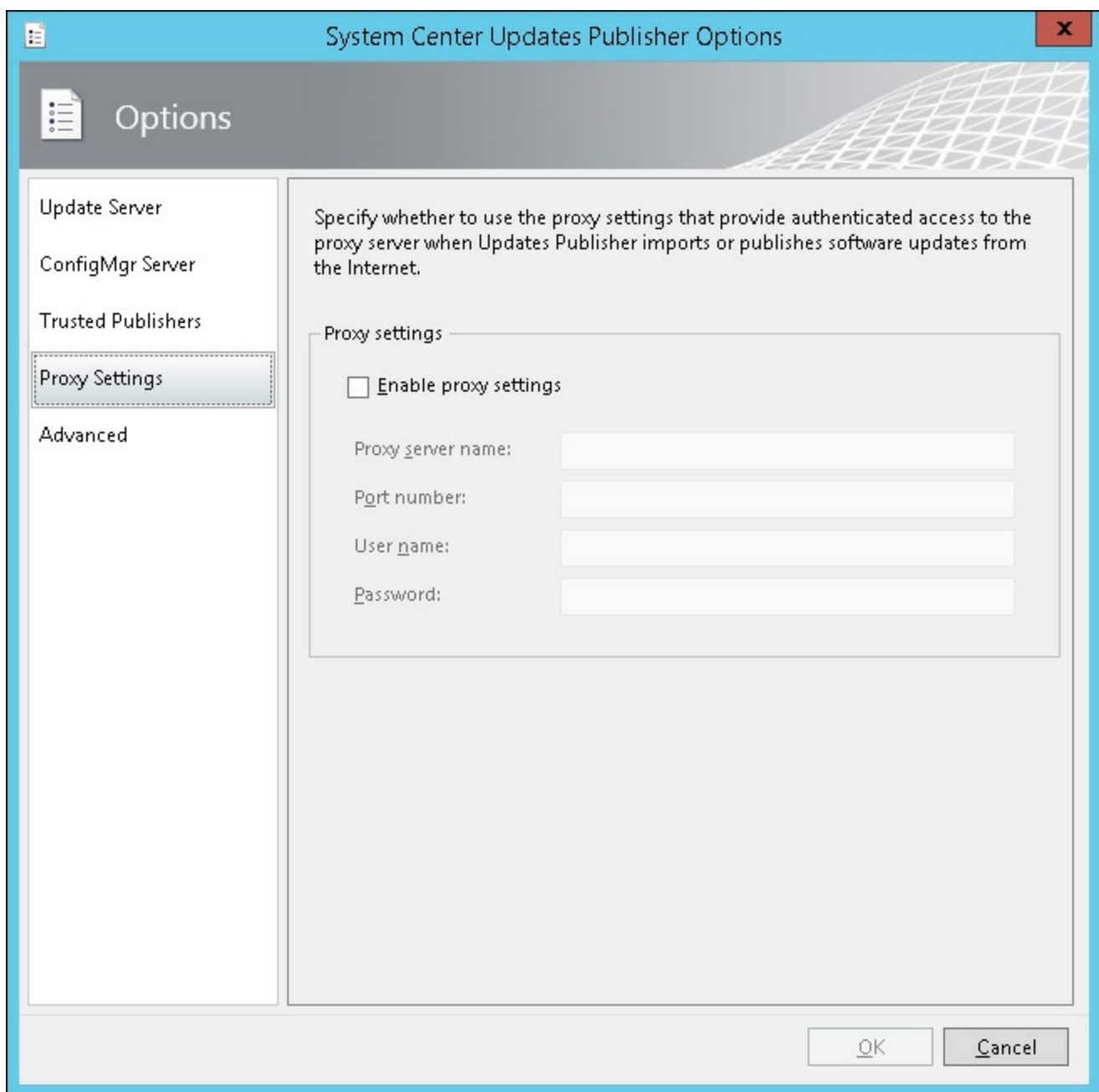
FIGURE 3-4 Proxy Settings

Advanced options, shown in , 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
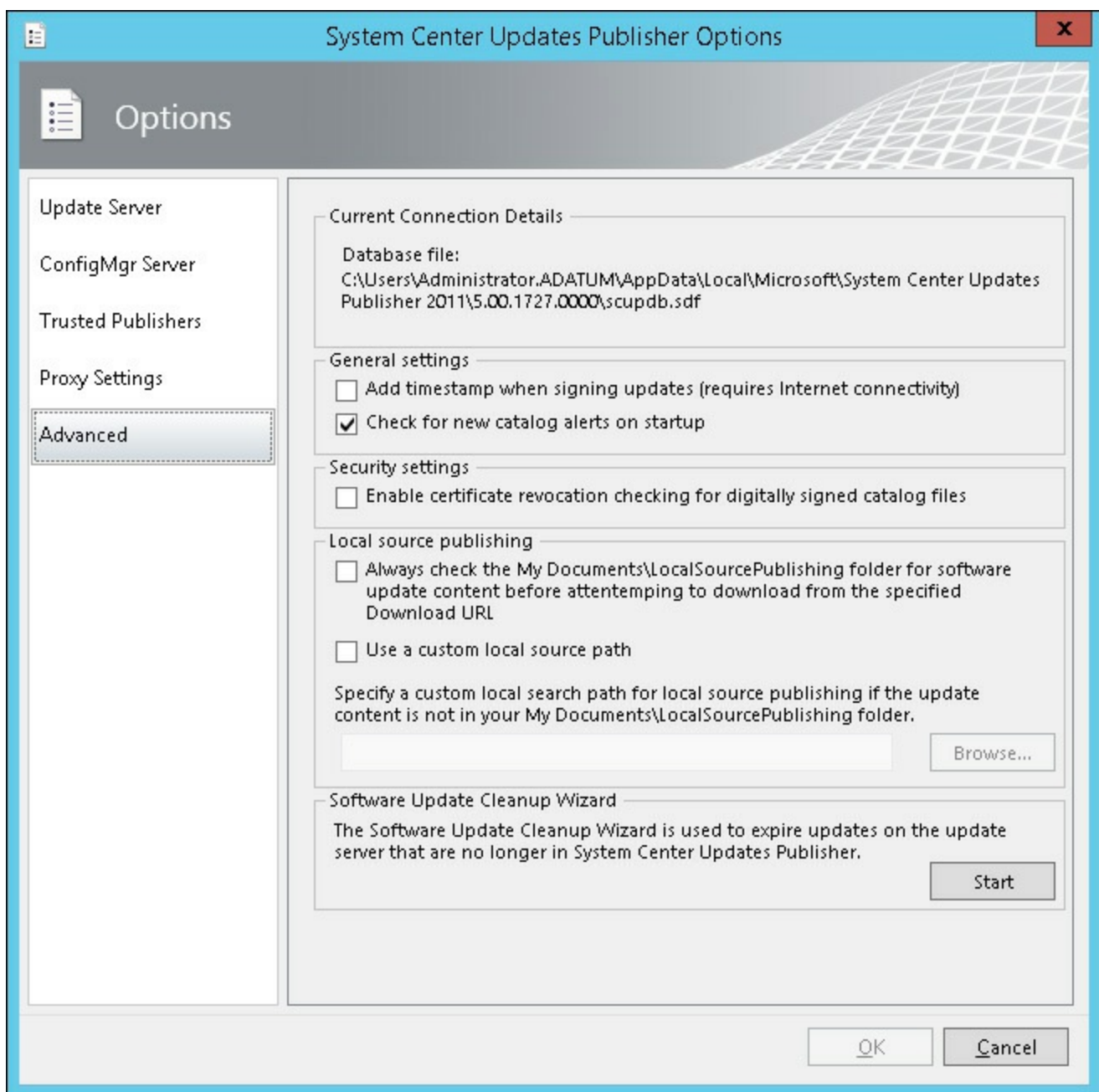
FIGURE 3-5 Advanced options

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.
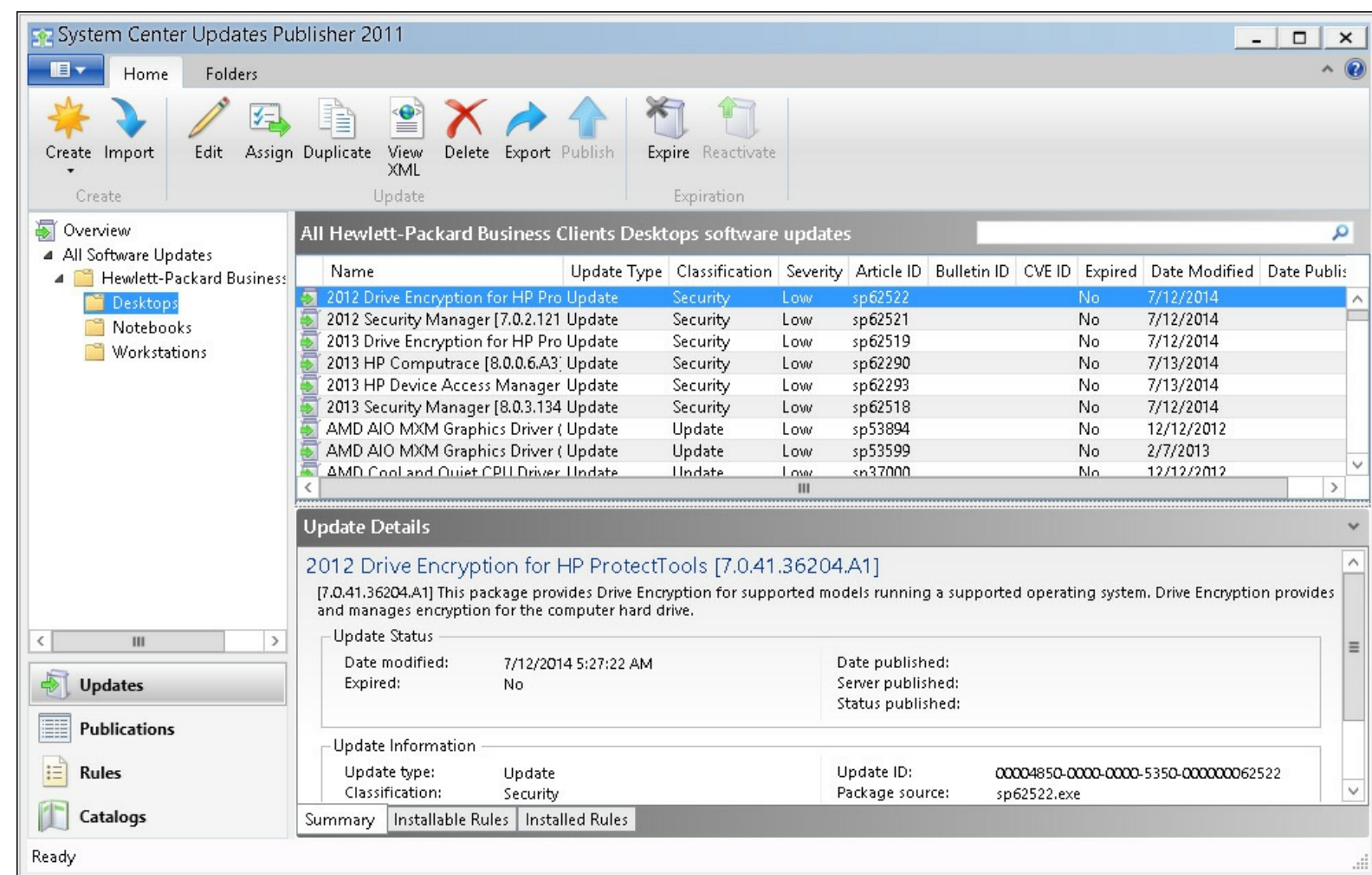
FIGURE 3-6 Updates workspace

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.
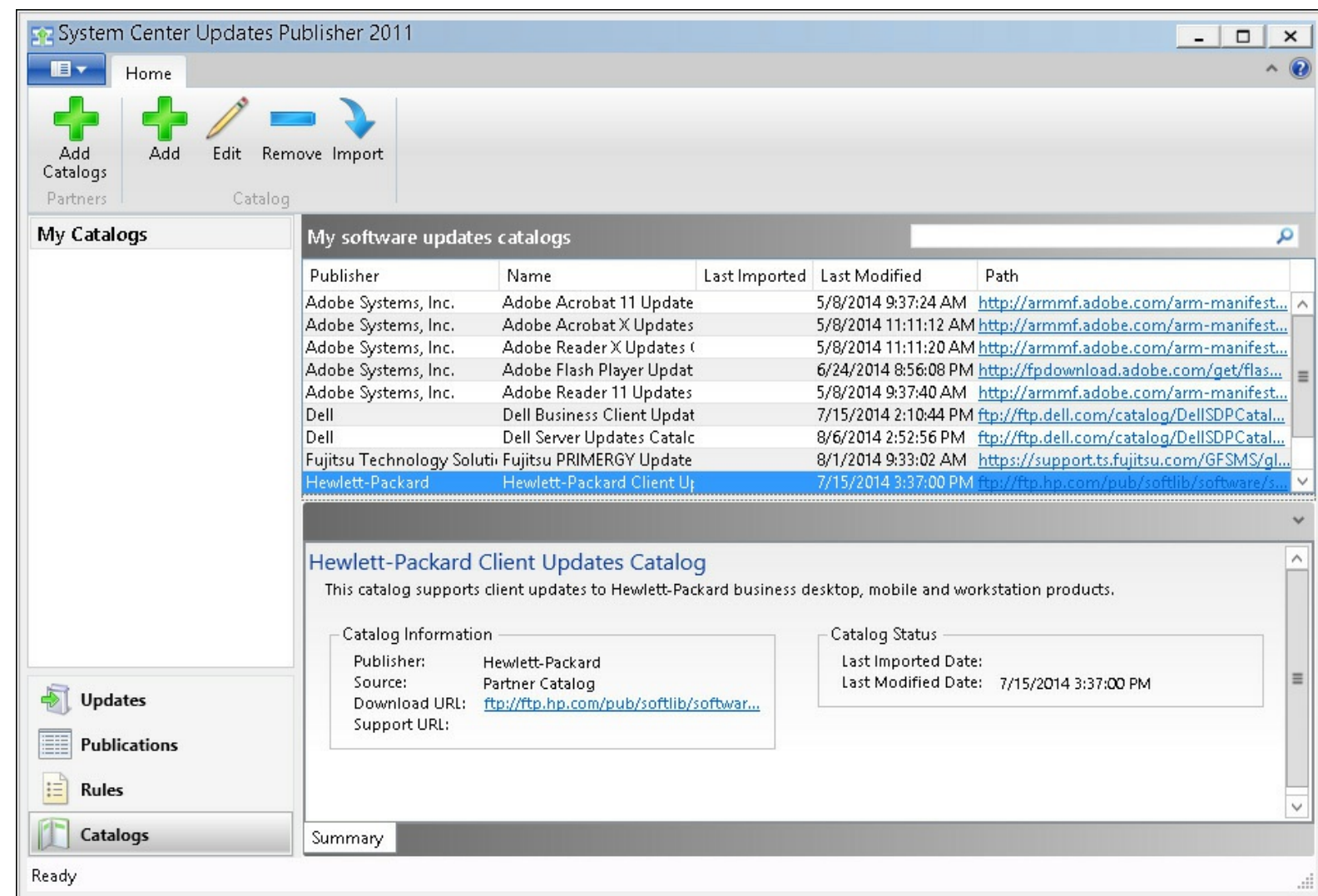
FIGURE 3-7 Catalogs workspace

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 meta-data 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.

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:

[Click here to view code image](#)

```
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 , contains the following settings that configure how client computers deploy software updates:
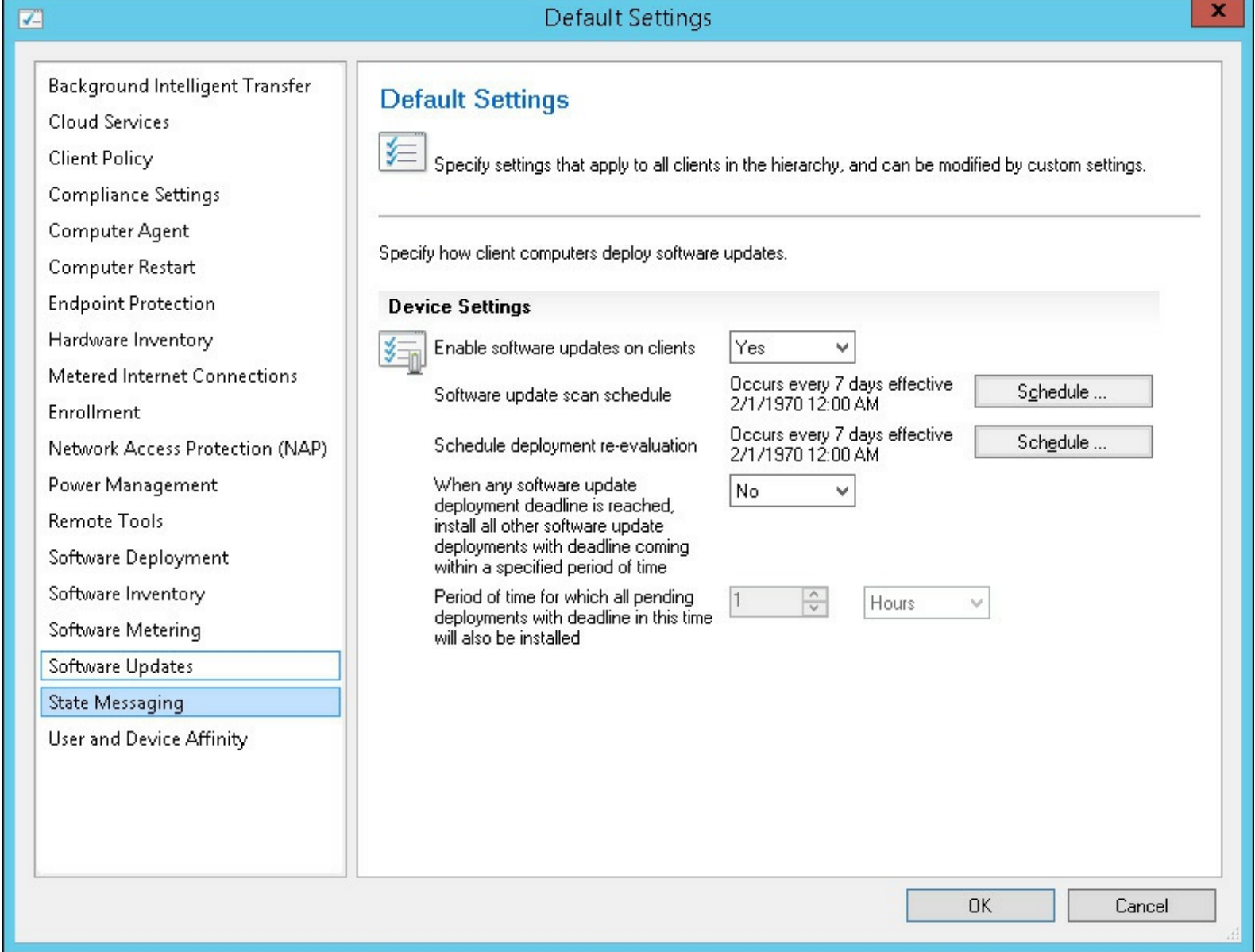
FIGURE 3-9 Software Updates

- **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 <u>Figure 3-10</u>, 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.
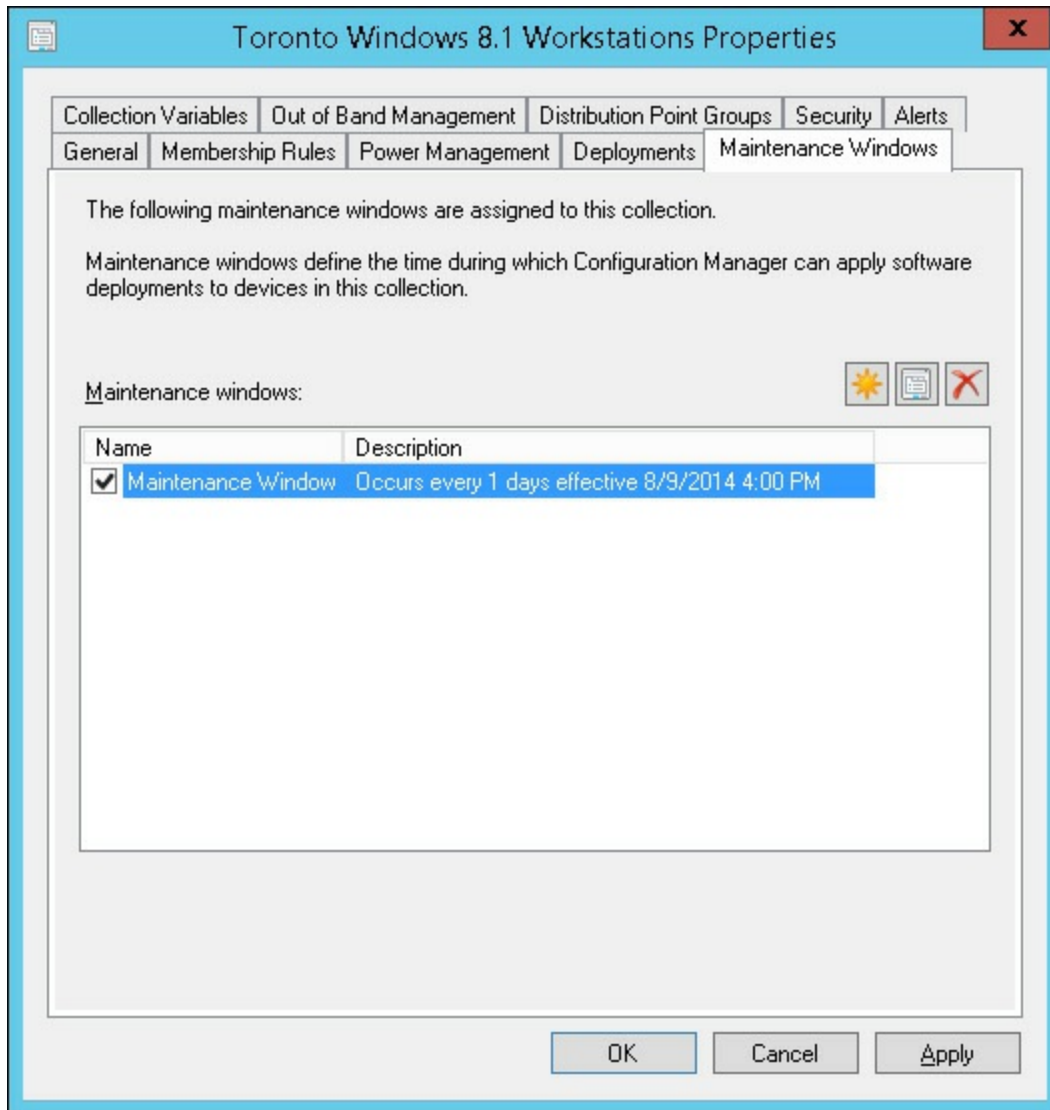
FIGURE 3-10 Maintenance Windows tab

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 . You can use reports to provide information to anyone who has permission to access the reporting feature.
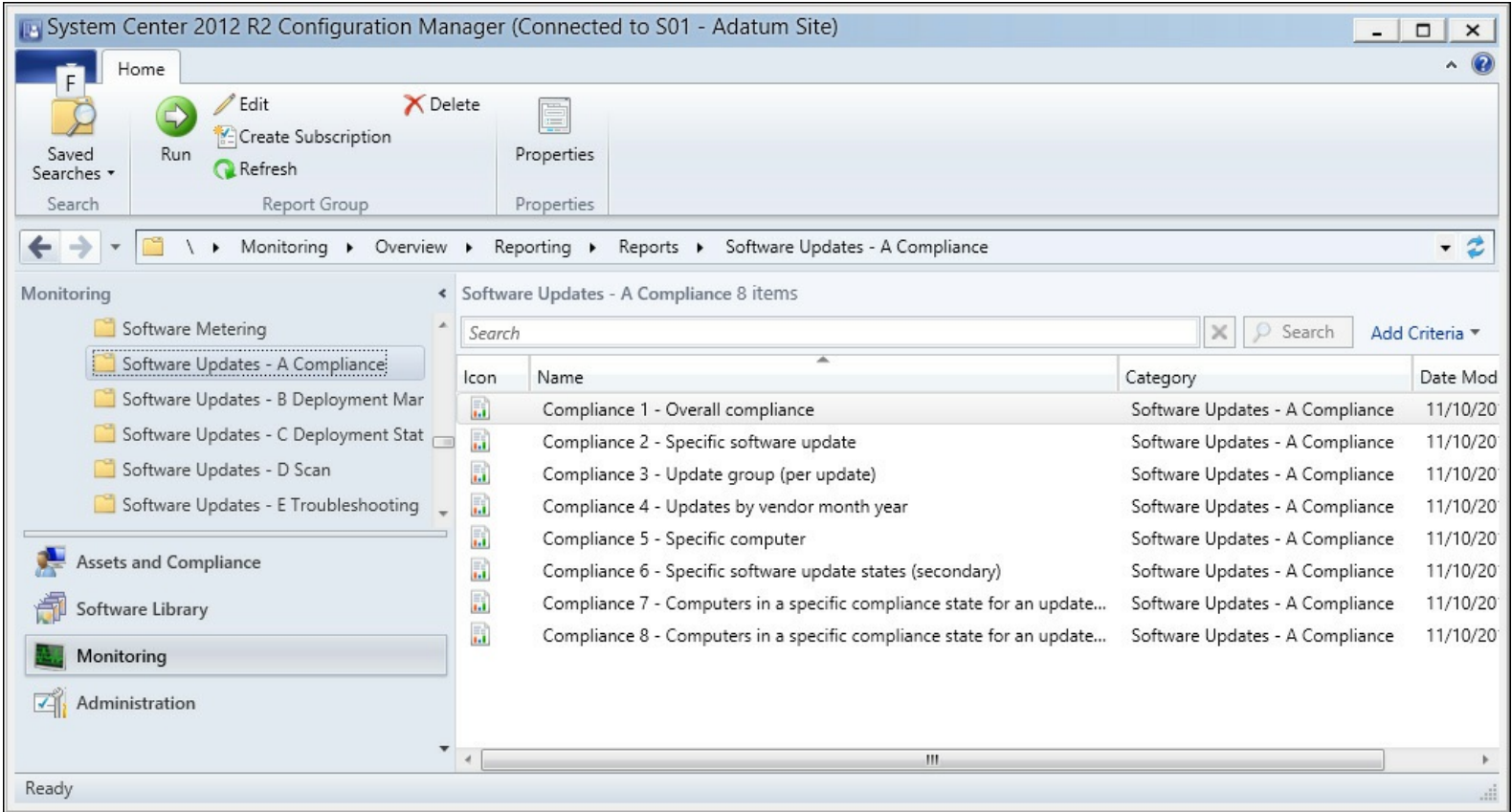
FIGURE 3-11 Software Updates reports

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:

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.
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.
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.

TABLE 3-1 Automatic Deployment Rule Wizard pages and settings

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.
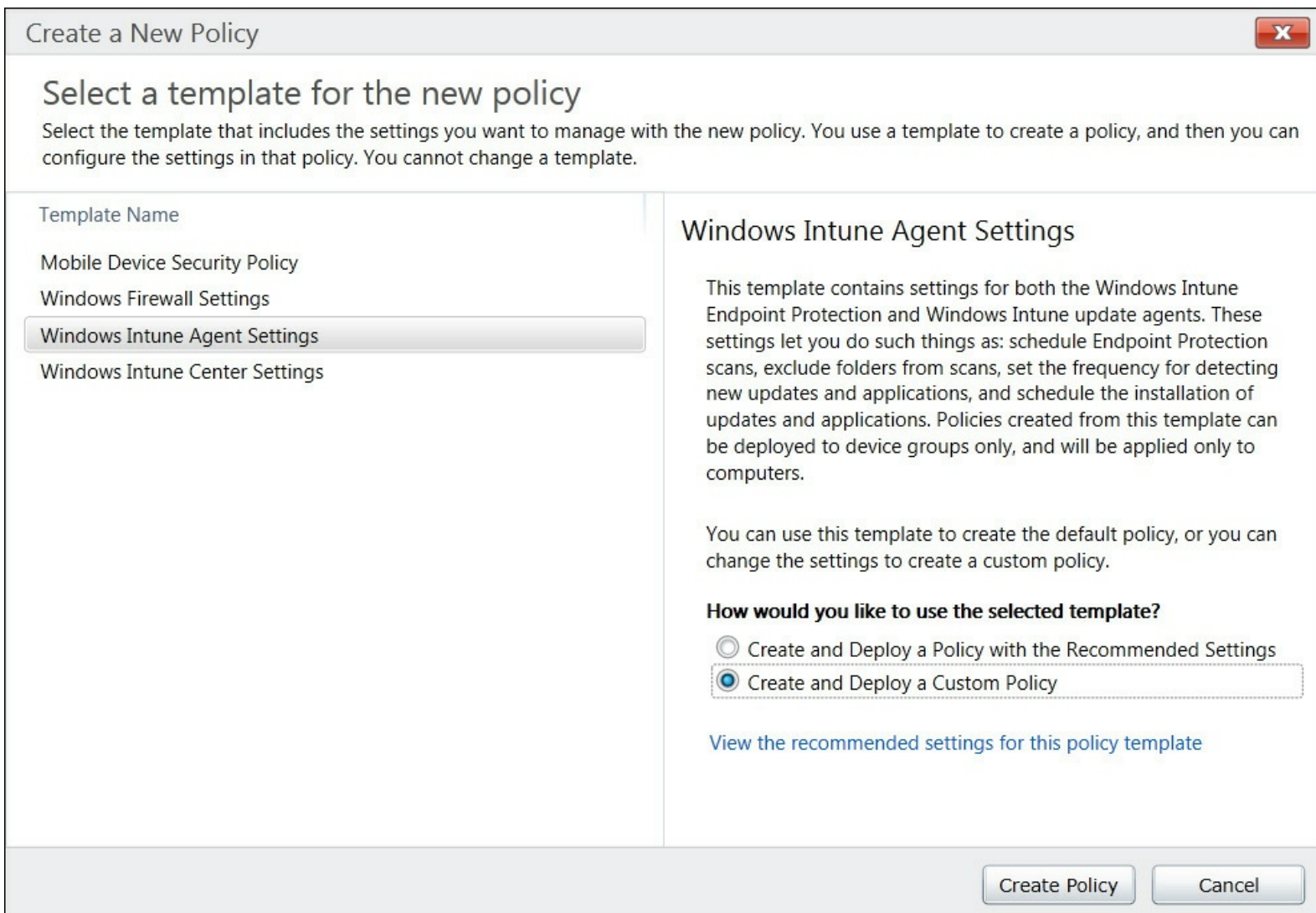
FIGURE 3-12 Creating a policy

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.
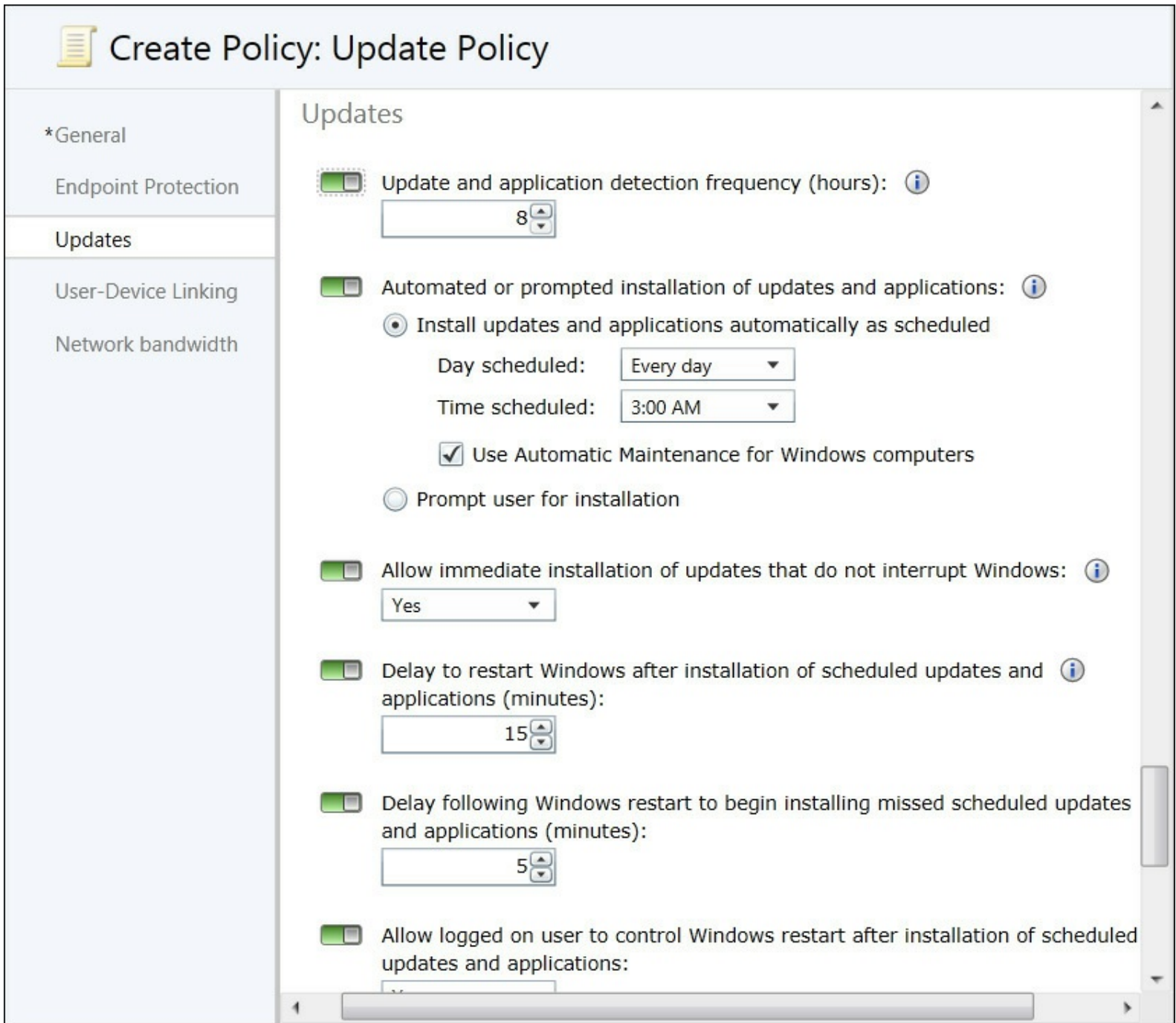
FIGURE 3-13 Updating a policy

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.
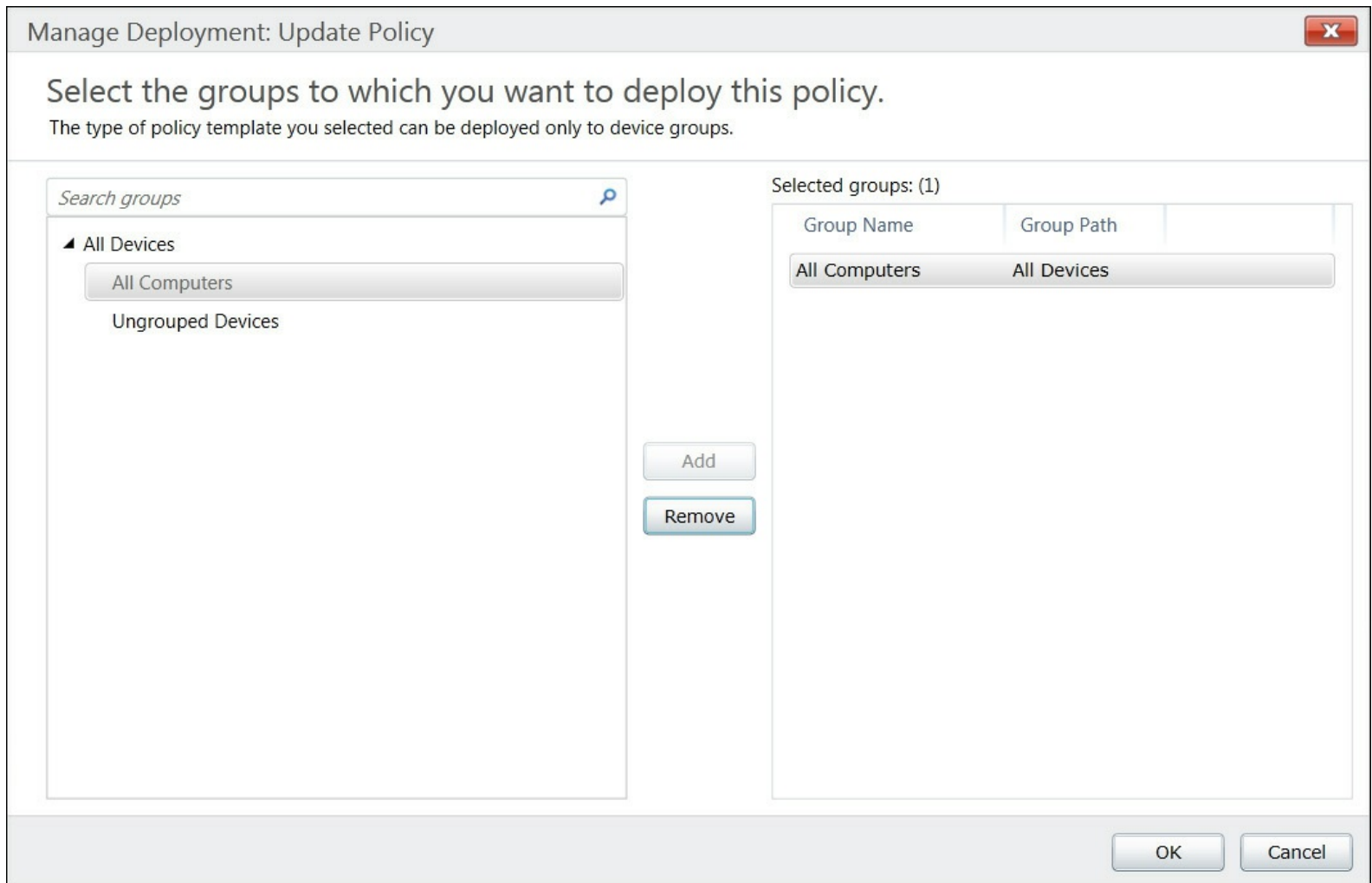
FIGURE 3-14 Selecting groups

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
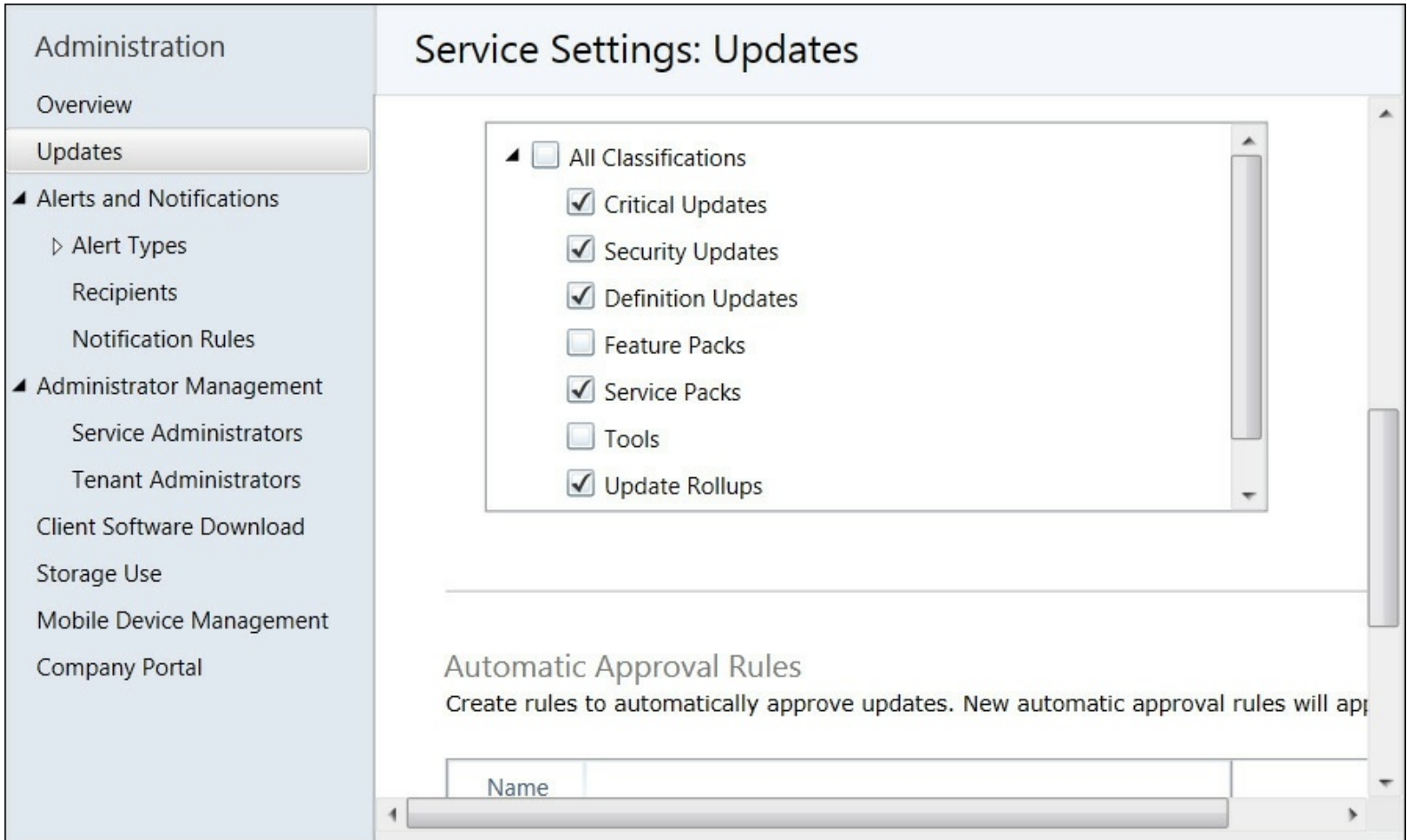
FIGURE 3-15 Service Settings: Updates

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 , select the update that you want to approve and click Approve.

FIGURE 3-16 All Updates

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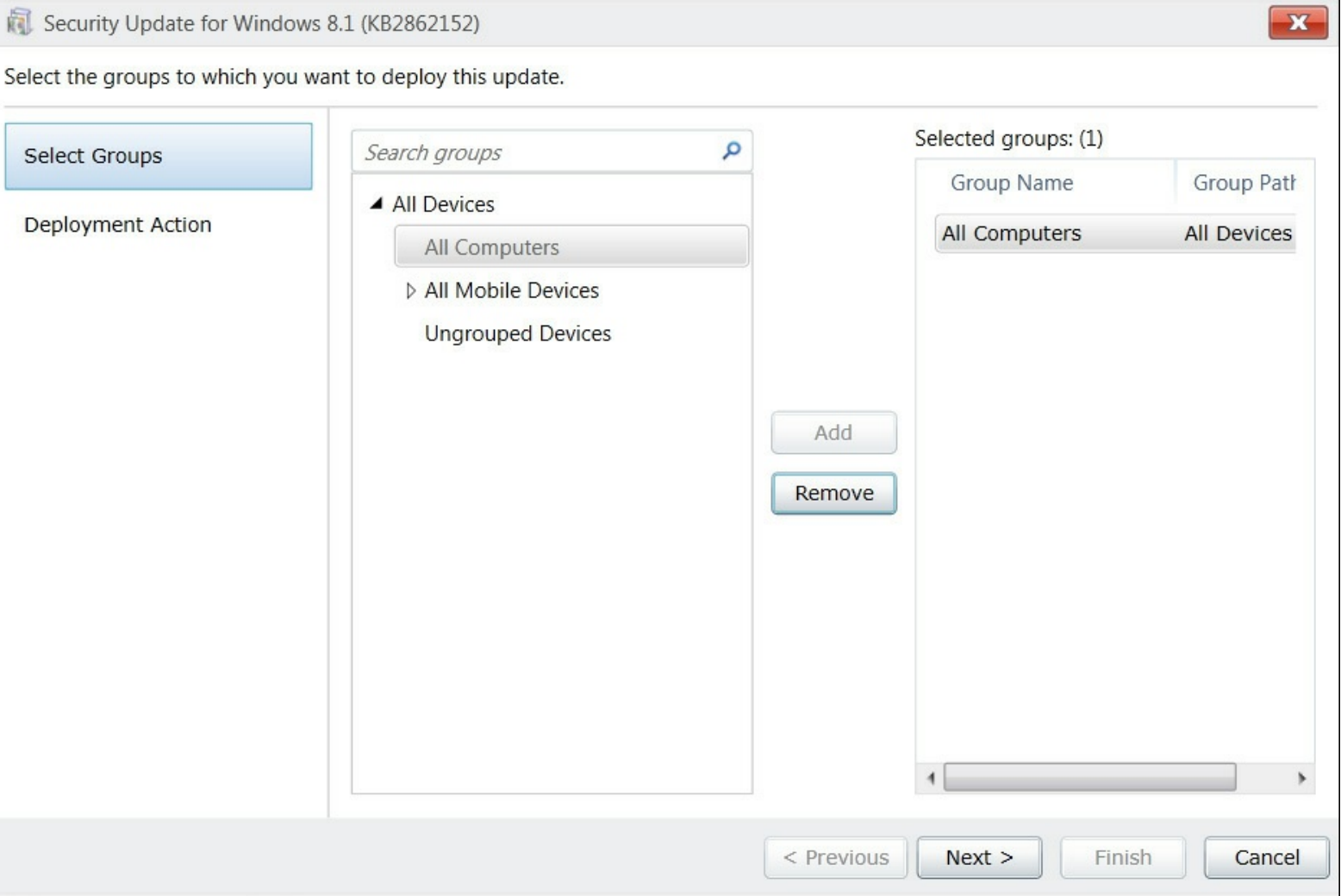
FIGURE 3-17 Select Groups

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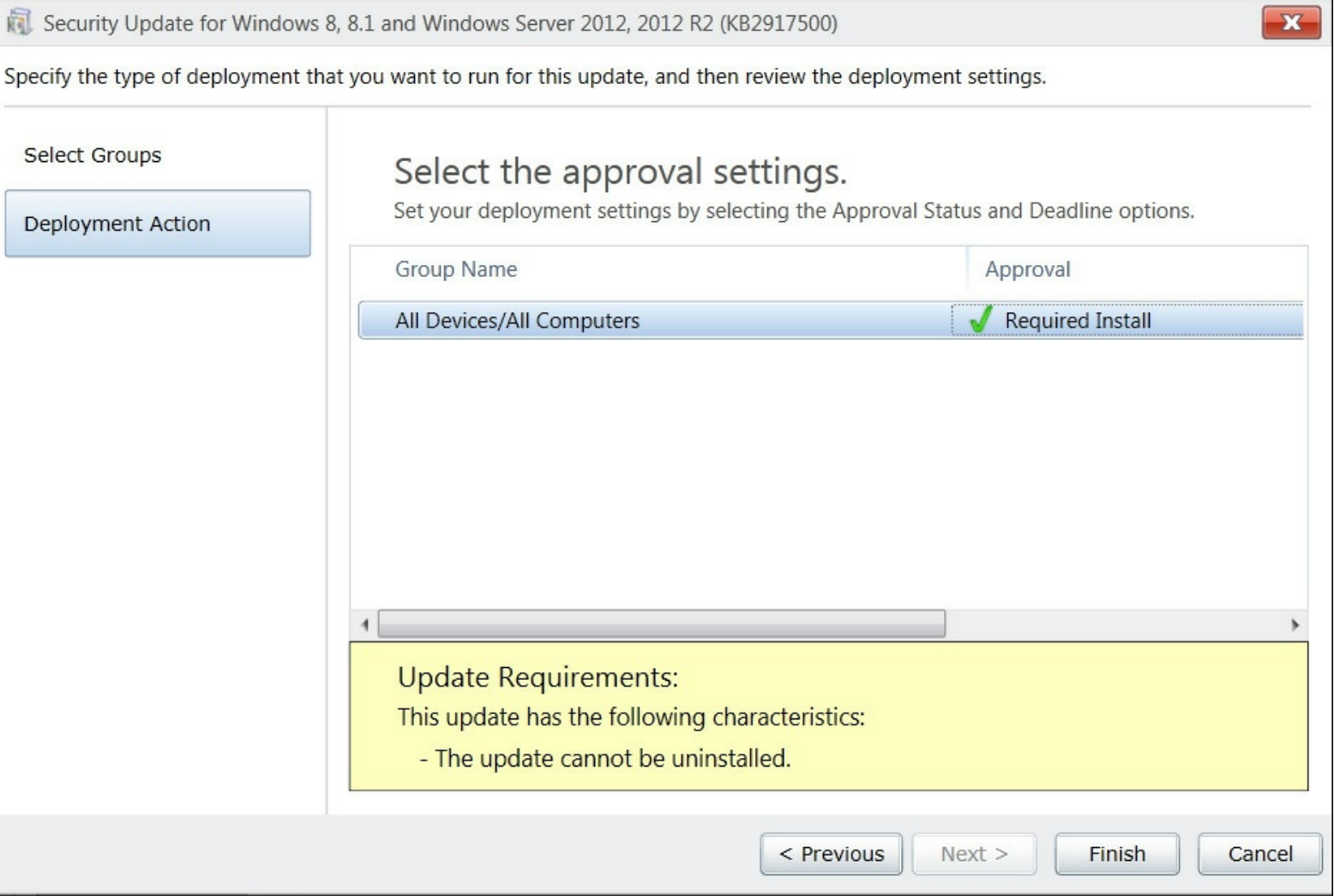
FIGURE 3-18 Deployment Action

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.
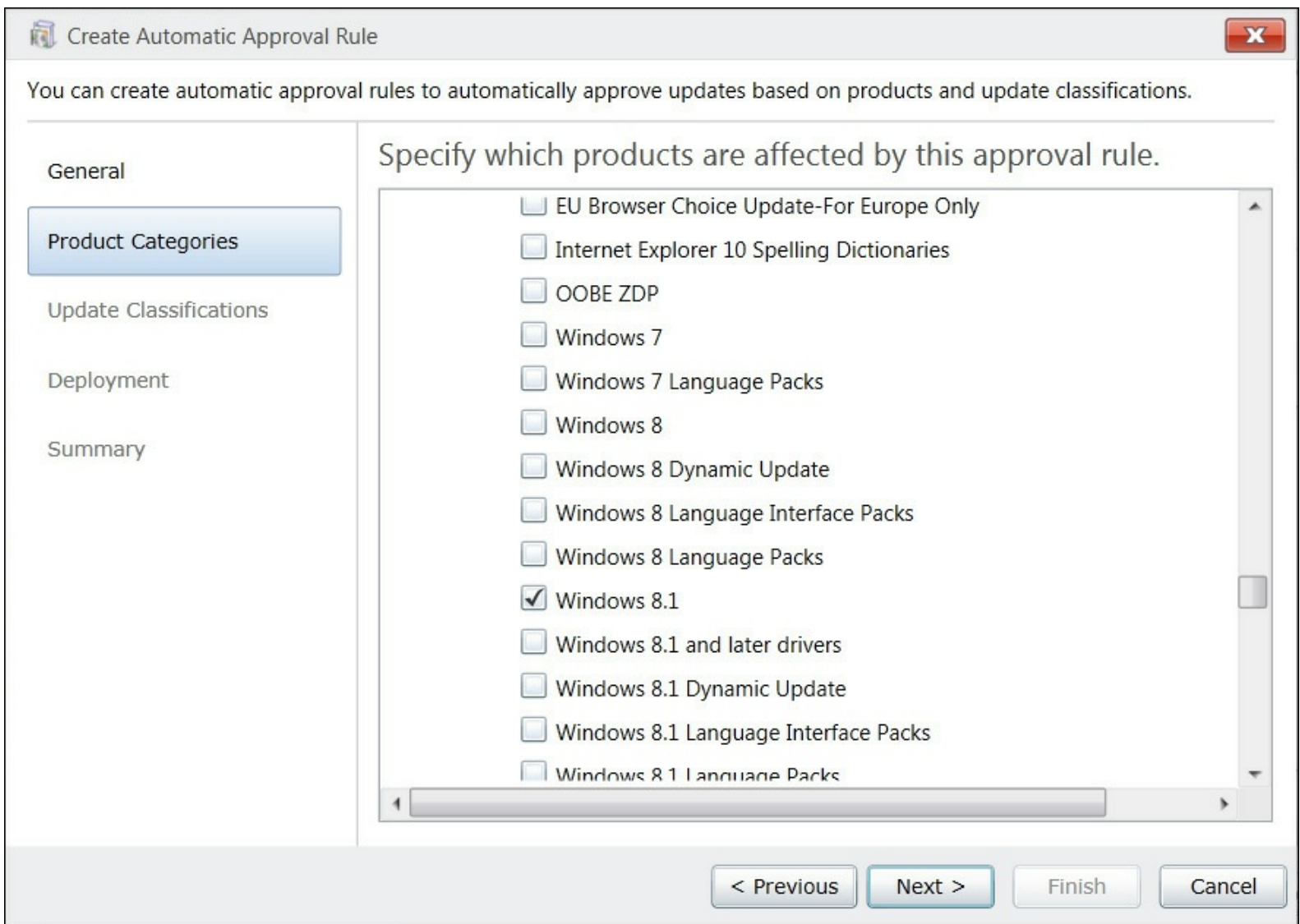
FIGURE 3-19 Product Categories

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.
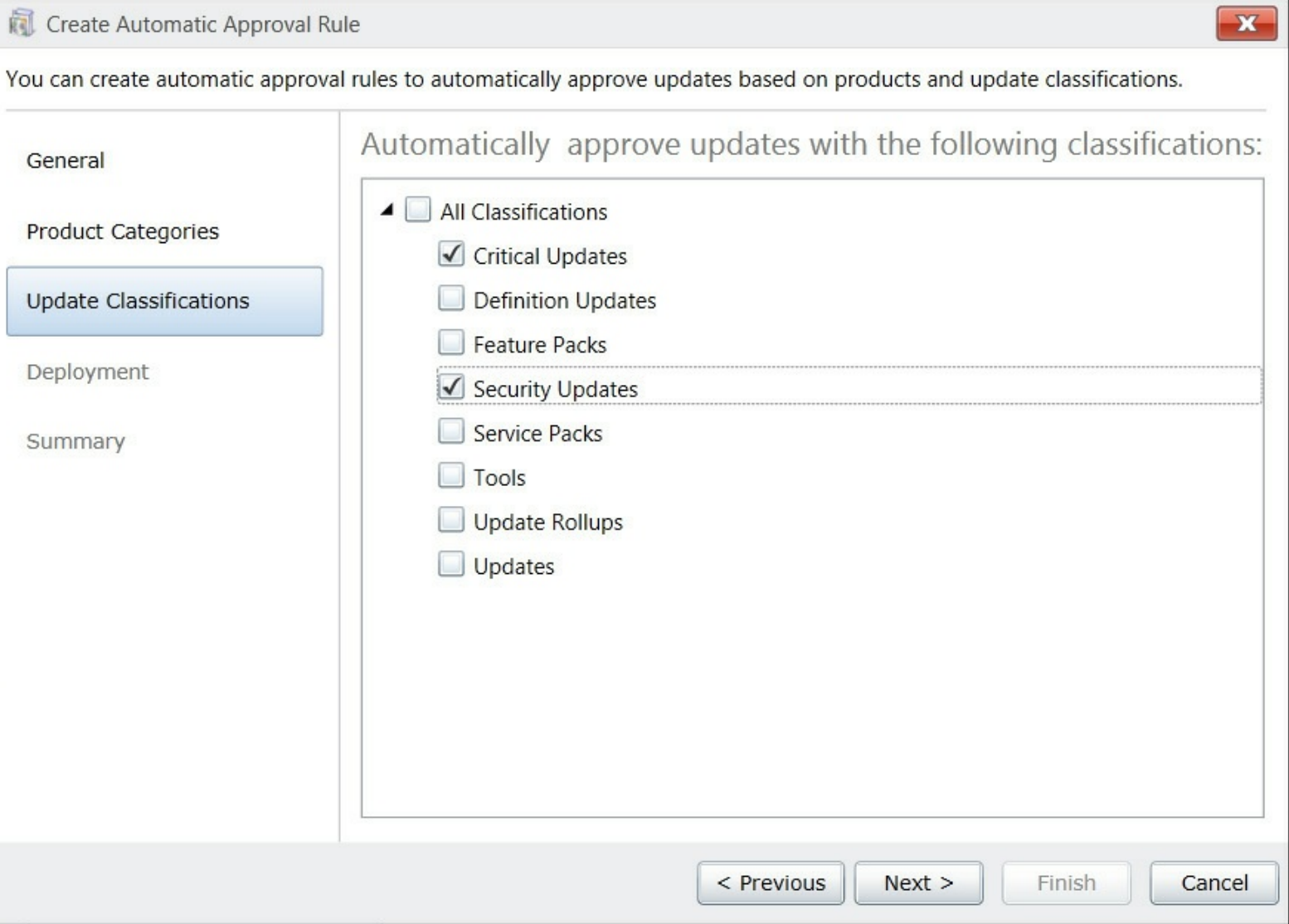
FIGURE 3-20 Update Classifications

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.
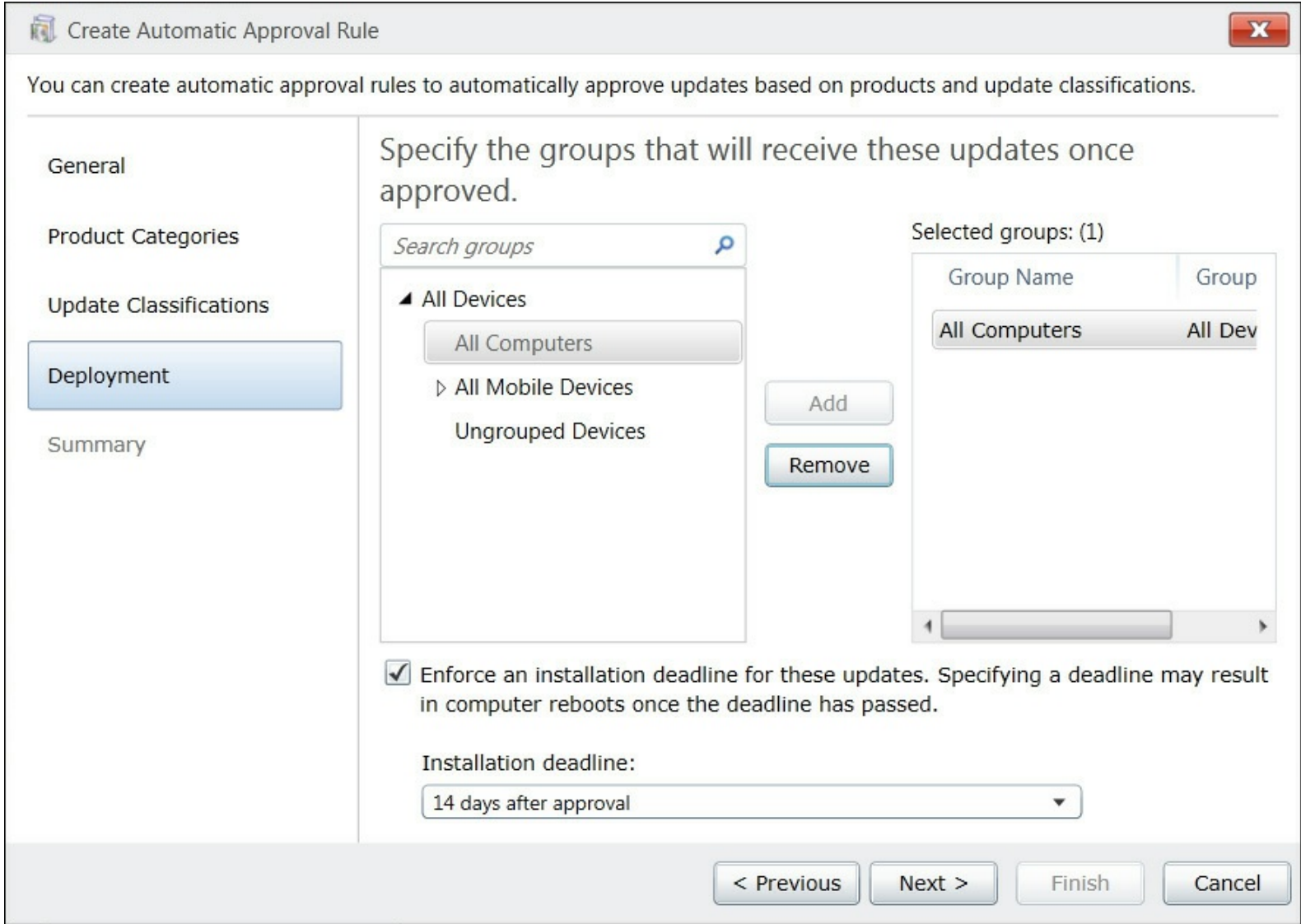
FIGURE 3-21 Deployment

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 "<u>Answers</u>" 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.

Chapter 4. Manage compliance and endpoint protection settings

For many industries, the configuration of computers and devices is subject to compliance legislation. You can use the System Center 2012 R2 Configuration Manager compliance functionality to ensure that your organization's managed devices meet the necessary configuration standards. Configuration Manager also includes antimalware functionality so you can monitor and remediate malware incidents on clients in your organization's environment.

Objectives in this chapter:

- Objective 4.1: Build a configuration item.
- Objective 4.2: Create and monitor a baseline.
- Objective 4.3: Configure Endpoint Protection.

Objective 4.1: Build a configuration item

This objective deals with building configuration items for Configuration Manager. Such items enable you to evaluate the configuration of a Configuration Manager client. You can configure these items for Windows, Mac OS X, and mobile device clients.

This section covers the following topics:

- Overview of compliance settings
- Configuration items
- Creating configuration items
- Configuration item settings
- Remediation

Overview of compliance settings

The Compliance Settings feature in Configuration Manager enables you to assess and manage configuration settings for Windows-based computers, Mac operating system (Mac OS X) computers, and devices running the Windows RT, Windows Phone, Windows Mobile, iOS, and Android mobile operating systems.

You can use compliance settings to:

- Monitor the version of a device's installed operating system.
- Verify whether applications are installed and configured correctly.
- Check for prohibited applications or security settings.
- Check that specific software updates are installed.
- Configure features and security settings on mobile devices.
- Remediate noncompliant settings automatically (when supported).
- Configure user data and profiles settings such as folder redirection, offline files, and roaming

user profiles (applicable for Windows 8.x and newer only).

■ Configure company resource access by using remote connection, virtual private network (VPN), Wi-Fi, and certificate profiles. (This is applicable only for devices running Windows 8.x and newer, iOS, and Android operating systems.)Compliance settings consist of one or more configuration items. Configuration items contain the specific settings and rules that define the requirements necessary to meet compliance. You can group configuration items into configuration baselines. You deploy configuration baselines to client systems to evaluate compliance and, potentially, perform remediation.

More Info: **Compliance Settings Overview**

You can learn more about compliance settings at *http://technet.microsoft.com/en-us/library/gg682139.aspx*.

Configuration items

Configuration items contain one or more unique settings and values that you want to compare for compliance evaluation. For example, does a particular registry key have a particular setting, is a specific software update installed, or is the most recent version of an installed application deployed on the client?

Within a configuration item, you specify the compliance settings you are evaluating and the rules that should take effect based on those settings. You can use a single configuration item to evaluate multiple settings. When configuring a compliance rule as part of a configuration item, you can define the noncompliance severity that the client reports if the evaluation reveals noncompliance. If the configuration item supports remediation, you can specify the setting in the configuration item that you want to remediate—for example, changing a registry key value from 0 to 1.

You can specify configuration items for the following device types:

■ Windows
■ Mobile device
■ Mac OS X

Windows configuration items

You can specify Windows-based configuration items based on values related to the following settings:

■ Active Directory Query
■ Assembly
■ File System
■ IIS Metabase
■ Registry Key
■ Registry Value
■ Script
■ SQL Query

- WQL Query
- XPath Query

Depending on the specific setting, you can configure rules for reporting purposes or for performing remediation tasks.

Mobile device configuration items

Mobile device configuration items enable you to configure settings that you can apply to managed Windows, iOS, and Android devices. Some common settings include the following:

- Password
- Device
- Email management
- Store
- Browser
- Security
- Windows Server work folders

You apply these configuration settings to devices that you manage through the Microsoft Intune connector.

Mac OS X configuration items

Mac OS X configuration items are rules that you want to evaluate for managed Mac OS X computers. Configuration items include:

- Mac OS X Preferences.
- Scripts.

Creating configuration items

You can create a configuration item by using any of the following methods:

- Create a configuration item manually.
- Create a child configuration item from an existing Windows-based configuration item.
- Import configuration data.
- Copy an existing configuration item.

Create a configuration item manually

The most direct way to create a configuration item is to select the Configuration Items node, which is located under Compliance Settings in the Assets And Compliance workspace. Click Create Configuration Item on the ribbon. This starts the Create Configuration Item Wizard.

On the General page of the Create Configuration Item Wizard, shown in Figure 4-1, configure the following basic settings about the configuration item:

- **Name** Provide a name for the configuration item.
- **Description** Provide a description for the configuration item.

- **Type** Specify whether this configuration item is for Windows clients, mobile devices, or Mac OS X clients. When specifying the type as Windows clients, you can specify whether the configuration item is an application. This reveals additional options that you can use for detecting the application.

- **Categories** Provide an administrative category that you can use to tag your configuration items.

FIGURE 4-1 Create Configuration Item Wizard

After completing the General page, the wizard takes different paths, depending on which type of configuration item you are creating. Table 4-1 describes the pages that appear for each of the types.

Type	Wizard page	Description
Windows	Detection Methods	This page appears only if you selected the This Configuration Item Contains Application Settings check box on the General page of the wizard. On the Detection Methods page, you can specify the manner in which the application is detected.
	Supported Platforms	On this page, you can configure the Windows operating systems that will assess this configuration item for compliance. If you selected the This Configuration Item Contains Application Settings check box on the General page, this page appears after the Compliance Rules page.
	Settings	On this page, you can add new settings that you need to monitor.
	Compliance Rules	On this page, you can add new compliance rules used to evaluate the settings based on specified conditions.
Mobile device	Mobile Device Settings	On this page, you select the Mobile Device Settings Groups item that you want to evaluate in this configuration item. For each group that you choose, the wizard adds a page.
	Supported Platforms	On this page, you select the mobile device operating systems that this configuration item can evaluate. The supported platforms include: ■ Windows Mobile 6.1 and 6.5. ■ Nokia Symbian. ■ Windows Phone 8. ■ Windows RT. ■ Windows 8.1. ■ iOS 5, iOS 6, and iOS 7. ■ Android 4, Android 4.1, and 4.2.
	Platform Applicability	This page displays the mobile device settings that do not support all the platforms that you specified on the Supported Platforms page.
Mac OS X	Supported Platforms	On this page, you select the Mac OS X operating systems that this configuration item can evaluate. The supported platforms include Mac OS X 10.6, Mac OS X 10.7, and Mac OS X 10.8.
	Settings	On this page, you can add new settings that you want to monitor.
	Compliance Rules	On this page, you can add new compliance rules to evaluate the settings based on specified conditions.

TABLE 4-1 Create Configuration Item Wizard options

Create a child configuration item

Use the create a child configuration item method to create a configuration item that inherits the properties of an existing configuration item. You then can refine the properties with a more detailed configuration. To create a child configuration item, select the configuration item that you want to use as a parent and then, on the ribbon, click Create Child Configuration Item. This starts the Create Child Configuration Item Wizard.

The Create Child Configuration Item Wizard has the same options as the Create Configuration Item Wizard except that you cannot remove or modify settings inherited from the parent configuration item. You can add settings or compliance rules to refine a configuration item further for a specific baseline. You can create child configuration items only for Windows-based configuration items.

Import configuration data

You can import configuration items that you have:

- Exported from other sites.
- Downloaded as part of configuration packs from the Microsoft website or from other vendors.

To import configuration data, select the Configuration Items node and then, on the ribbon, click the Import Configuration Data button. This starts the Import Configuration Data Wizard. In this wizard, you import one or more cabinet (.cab) files with configuration data, which you can use in Configuration Manager.

Copy existing configuration items

You use the copy existing configuration items method to create a configuration item with the properties of an existing configuration item but for which you want to modify some settings. When you copy a configuration item, you do not maintain a relationship between the new configuration item and the configuration item that you copied. To copy a configuration item, select the configuration item you want to copy and then, on the ribbon, click Copy. This opens the Configuration Item Name dialog box. Provide a name for the copy in the dialog box to create a copy. Then you can edit it as you would edit a configuration item that you created manually.

Configuration item revision history

Configuration Manager maintains a revision history of each configuration item. When you modify a configuration item, you do not lose the previous settings, and you can still use the previous settings in a configuration baseline. When you select the Configuration Items node, you can view in the Revision column the number of times a configuration item has been revised.

To manage revisions, select the configuration item that you want to work with and then, on the ribbon, click the Revision History button. In the Configuration Item Revision History window, the following options are available for you:

- **Show All Revisions or Show Revisions In Use** You can use this drop-down list to switch between all the revisions of the current configuration item and only the revisions that are being used in a configuration baseline.
- **Compare With Current Revision** When you select an older version of the configuration item, you can use this button to view the difference between that revision and the latest revision.

- **Delete** Use this button to delete a particular revision.
- **Export** Use this button to export a particular revision to a .cab file so that you can import the revision into another instance of Configuration Manager.
- **Copy** Use this button to copy a particular revision to create a new configuration item.
- **Restore** Use this button to restore a particular revision. Restoring a revision creates a new revision that is based on the settings of the restored revision.
- **Properties** Use this button to view the properties of a particular revision.

> *More Info:* **Creating Configuration Items**
>
> **You can learn more about creating configuration items at** *http://technet.microsoft.com/en-us/library/gg712331.aspx*.

Configuration item settings

You have several choices for the types of settings to monitor when you create a configuration item for Windows operating systems, mobile device support, or Mac OS X. Each type of configuration setting is evaluated against its own compliance rules and has its own values to monitor.

When configuring compliance rules, the options you have range from simply checking whether a setting exists to comparing it to a specific value. You then specify the severity level if the condition is not met.

Windows settings

When you create a Windows configuration item, you can monitor several aspects of Windows-based computers. The following list describes the setting types that you can monitor for computers running Windows operating systems:

- **Active Directory Query** Use this setting type to construct a query to find values in Active Directory Domain Services (AD DS).
- **Assembly** Use this setting type to specify an assembly from the global assembly cache to assess for compliance on computers.
- **File System** Use this setting type to specify a file or folder to assess for compliance on computers.
- **IIS Metabase** Use this setting type to specify the Internet Information Services (IIS) metabase setting to assess for compliance on computers.
- **Registry Key** Use this setting type to specify a registry key to assess for compliance on computers.
- **Registry Value** Use this setting type to specify a registry value to assess for compliance on computers.
- **Script** Use this setting type to specify two scripts:
  - A discovery script to identify and return a value
  - A remediation script to remediate the noncompliant setting

- **SQL Query** Use this setting type to specify a SQL query to assess for compliance on computers.
- **WQL Query** Use this setting type to specify a Windows Management Instrumentation (WMI) Query Language (WQL) query to assess for compliance on computers.
- **XPath Query** Use this setting type to specify the XML file path and XML Path Language (XPath) query to assess for compliance on computers.

In addition, when using the Windows configuration item type, you can specify that the configuration item must include application settings. Depending on the application settings, the wizard displays detection methods for applications. You have the following options for detecting applications:

- Always Assume Application Is Installed
- Use Windows Installer Detection
- Detect A Specific Application And Deployment Type
- Use A Custom Script To Detect This Application

Mobile device settings

When you create a mobile device configuration item, you can monitor several setting groups for compliance. These setting groups are as follows:

- **Password** This group includes typical password settings such as the password length and password expiration.
- **Device** This group contains device restriction settings.
- **Email Management** This group includes typical settings for email such as allowed protocols, attachments, and archives.
- **Store** This group contains application store settings.
- **Browser** This group contains default web browser settings.
- **Internet Explorer** This group contains Internet Explorer settings for Windows-based clients.
- **Content Rating** This group contains content rating for audio, video, and app content.
- **Cloud** This group enables you to specify cloud restrictions that apply to mobile devices.
- **Security** This group includes typical security settings such as file signing, apps, Bluetooth, and cameras.
- **Peak Synchronization** This group includes settings that control the hours and frequency of mobile device synchronization.
- **Roaming** This group includes settings that configure download options for mobile devices when they are roaming.
- **Encryption** This group includes encryption settings for devices, email, and storage cards.
- **Wireless Communications** This group includes settings to configure wireless network connections for mobile devices.
- **Certificates** This group specifies the certificates to install on mobile devices.
- **System Security** This group includes settings for system security, including firewall, automatic updates, and antimalware protection.

- **Windows Server Work Folders** This group enables you to configure Windows Server work folder settings.

Mac OS X settings

You can monitor the following setting types on Configuration Manager clients running the Mac OS X operating system:

- **Mac OS X Preferences** This setting type includes preferences within Mac OS X that use the following data types on application IDs and keys: string, date and time, integer, floating point, and Boolean.
- **Script** This setting type allows a script to run that returns the value to be assessed for client compliance.

Compliance rules

The simplest compliance rule to configure is an Existential rule. Existential rules test whether a setting exists. You can choose whether the compliance state exists or does not exist. In addition to testing for existence, the File system setting also supports the following compliance rule: File Exists The Following Number Of Times. This rule uses any of the available operators to compare values from *0* through *9999*.

Another type of rule is the Value rule. You use value rules to compare the current value in the configuration item to a specified value by using one of the available operators. Some of the setting types support more than just a simple comparison. For example:

- The value rule for the Registry Key setting enables you to evaluate permissions on a registry key for compliance.
- The value rule for the File System setting enables you to evaluate the following properties:
  - Date Modified
  - Date CreatedSize (Bytes)
  - Product Name
  - File Version
  - Company
  - Secure Hash Algorithm 1 (SHA-1)
  - Attributes
  - Permissions
- The value rule for the Assembly setting enables you to evaluate the following properties: Version, Culture, and Public Key Token.

Depending on the compliance rule you create, you can choose from several relational operators to compare a current value to a desired value. You can use the following operators for this purpose:

- Equals
- Not Equal To
- Greater Than
- Greater Than Or Equal To

- Less Than
- Less Than Or Equal To
- Between
- One Of
- None Of

Severity levels

Computers that do not comply with one or more of the objects or settings in the configuration item send a state message and a status message with one of the following noncompliant severity levels:

- None
- Information
- Warning
- Critical
- Critical With Event

Computers that do not comply with one or more of the objects or settings in the configuration item log a Windows application event message (Event ID: 11857) of the type Error. State messages and status messages the client sends have the noncompliant severity level of Critical With Event.

Remediation

Configuration Manager supports remediation only for the following configuration items:

- Registry values
- Scripts
- WQL query configuration items
- All mobile phone settings
- Mac OS X Preferences

Remediation is available only when the type operator is set to Equals in all cases except for mobile phone settings. During remediation, Configuration Manager performs one of the following actions based on the setting type:

- Create the value if it does not exist (when the rule type is Value and the operator is Equals).
- Set the value if it exists but is not compliant.
- Run a remediation script when using a script-based configuration item.
- Set the value for the mobile device settings if supported by the mobile device operating system. (Not all mobile devices support the same settings.)

The method in which you configure remediation depends on the type of setting:

- For a registry value or WQL query configuration item, in the compliance rule, select the Remediate Noncompliance Rules When Supported check box. If you select this check box, the remediation action will be one of the following:
  - Create The Value If It Does Not Exist.
  - Set The Value If It Exists But Is Not Compliant.

- For a script configuration setting, you need to provide an appropriate remediation script.
- For mobile device configuration settings, on each setting group that you add to the configuration item, you must select the Remediate The Noncompliant Settings check box.

Configuration item remediation occurs only when the item is included in a baseline deployment that you also have configured for remediation. (For remediation to be successful, you must configure remediation both on the compliance rule and in the deployment properties of the configuration baseline in which the configuration item is listed.) Due to the requirement for both the item and deployment to support remediation, you can use the same configuration item in both remediating and nonremediating deployments.

Exam Tip

Remember which configuration item types allow remediation.

Thought experiment: Configuration Items at Contoso

You are testing the compliance functionality of Configuration Manager. Specifically, you are interested in monitoring the configuration of mobile devices and determining whether a prohibited file-sharing application is installed on Configuration Manager clients running the Windows 8.1 operating system. With this information in mind, answer the following questions:

1. **What must you configure in addition to Configuration Manager to manage mobile device configuration item settings?**
2. **Which configuration item type could you use to determine whether a prohibited application is installed on Configuration Manager clients running the Windows 8.1 operating system?**

Objective summary

- The Compliance Settings feature enables you to assess and manage configuration settings for Configuration Manager clients.
- Configuration items contain one or more unique settings and values that you want to compare for compliance evaluation.
- Use the create a child configuration item method to create a configuration item that inherits the properties of an existing configuration item.
- Use the copy existing configuration items method to create a configuration item with the properties of an existing configuration item but for which you want to modify some settings.
- Configuration Manager maintains a revision history of each configuration item. When you modify a configuration item, you do not lose the previous settings, and you can still use the

previous settings in a configuration baseline.

- ■ Configuration Manager supports the following noncompliant severity levels: None, Information, Warning, Critical, and Critical With Event.
- ■ Configuration Manager supports remediation only for the following configuration items: registry values, scripts, WQL query configuration items, all mobile phone settings, and Mac OS X Preferences (where the value type operator is set to Equals).

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 of the following configuration item types supports remediation? (Choose two. Each correct answer provides a complete solution.)

    A. Registry values

    B. Registry keys

    C. WQL query

    D. XPath query

2. Which the following setting types would you use in a configuration item to determine whether a particular file was present on a Configuration Manager client?

    A. Active Directory query

    B. Assembly

    C. File system

    D. Registry value

3. Which of the following setting types would you use in a configuration item to determine whether a specific registry key was present on a Configuration Manager client?

    A. Registry value

    B. WQL query

    C. Script

    D. Registry key

4. Which of the following setting types would you use in a configuration item to run a script to remediate a noncompliant setting?

    A. WQL query

    B. Script

    C. File system

    D. Assembly

5. You have a WMI query language query that determines the amount of free disk space on a computer's operating system volume. Which of the following setting types would you use in a configuration item to determine whether a Configuration Manager client had more than 15 GB

of free space on the operating system volume? (Choose the best answer.)

    A. WQL query

    B. Script

    C. File system

    D. Registry value

Objective 4.2: Create and monitor a baseline

Configuration baselines enable you to collect configuration items, software updates, and even other configuration baselines as a way of determining compliance. You can create your own baselines or import preexisting baselines through configuration packs. You can use the results of a compliance check to create a new collection.

This section covers the following topics:
- Configuration baselines
- Creating configuration baselines
- Deploying configuration baselines
- Configuration packs
- Viewing compliance information

Configuration baselines

A configuration baseline is a group of configuration items, software updates, and other configuration baselines. If a system is noncompliant with one item in a configuration baseline, it is noncompliant with the configuration baseline.

If you include configuration items for multiple products and system settings in a single baseline, you increase the baseline's complexity. This makes managing the baseline more difficult. A simpler approach is to create several single product or system settings baselines and then deploy the baselines to the Configuration Manager collections to which you want to apply them. When you evaluate the baselines, the compliance results are easier for you to analyze. You can use the same configuration item in multiple configuration baselines.

After you create a configuration baseline, you can deploy it to a collection. This enables that collection's devices or primary devices of the collection's users to download the configuration baseline and assess compliance with each of the baseline's configuration items.

Client settings contain the default schedule for running evaluations as shown in . When you deploy a configuration baseline to a collection, you can specify remediation settings, alert settings, and a schedule for that configuration baseline to use for evaluating the client systems.
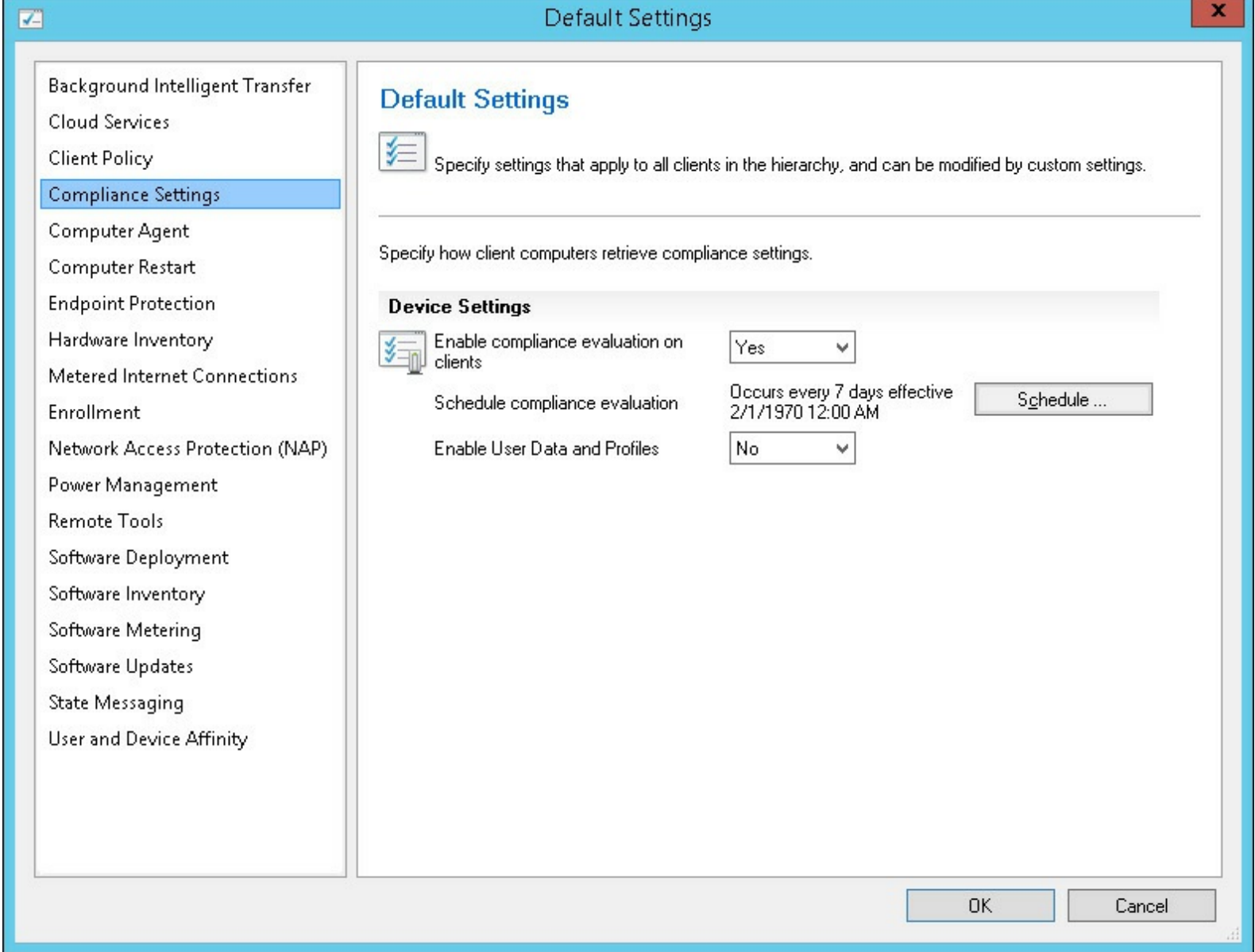
FIGURE 4-2 Compliance Settings

You can use the evaluation results of the configuration baseline to create a collection. If the configuration baseline contains configuration items that do not support automatic remediation, you can use this collection as a target so that an additional task can remediate the issue. For example, you might use the configuration items in a configuration baseline to detect a forbidden application. You then can create a collection based on the configuration baseline and deploy an application or package to uninstall the forbidden application.

You can create collections based on the following compliance states: Compliant, Error, Non-Compliant, and Unknown. You can access the wizard for creating the collection by selecting the configuration baseline and then selecting the Deployment tab. When you select a deployment on the Deployment tab, a Create New Collection menu appears on both the ribbon and the Actions menu. You can use this option to create a query-based collection according to the state you have chosen.

More Info: **Configuration Baselines**

> **You can learn more about configuration baselines at**
> *http://technet.microsoft.com/en-au/library/gg712268.aspx*.

Creating configuration baselines

You can create a configuration baseline in one of the following ways:

- Create a configuration baseline manually, using the Create Configuration Baseline dialog box.
- Import configuration data.
- Copy an existing configuration baseline.

If a configuration item has multiple revisions, you can specify which version of the configuration item is used in the baseline.

Create a configuration baseline manually

The most direct way to create a configuration baseline is to select the Configuration Baselines node, which is located under Compliance Settings in the Assets And Compliance workspace, and then click the Create Configuration Baseline button on the ribbon. This launches the Create Configuration Baseline dialog box, shown in .

FIGURE 4-3 Create Configuration Baseline

Import configuration data

The process to import the configuration baselines is the same as the process to import configuration items. You use the Import Configuration Data Wizard to import one or more .cab files containing configuration baselines, configuration items, or both. Then you can use them in Configuration Manager.

Copy an existing configuration baseline

You use this method to create a configuration baseline when you want a configuration baseline with the properties of an existing configuration baseline. After you make the copy, you can modify the properties to create the configuration baseline you require. When you copy a configuration baseline, you do not maintain a relationship between the new configuration baseline and the configuration baseline that you copied. To copy a configuration baseline, select the configuration baseline that you want to copy and then, on the ribbon, click Copy. This opens the Configuration Baseline Name dialog box.

Deploying configuration baselines

Deploying a configuration baseline to a collection of client devices enables you to perform an evaluation of those devices against the baseline. To deploy a configuration baseline, select an existing configuration baseline and then, on the ribbon, click Deploy. This opens the Deploy Configuration Baselines dialog box shown in Figure 4-4.
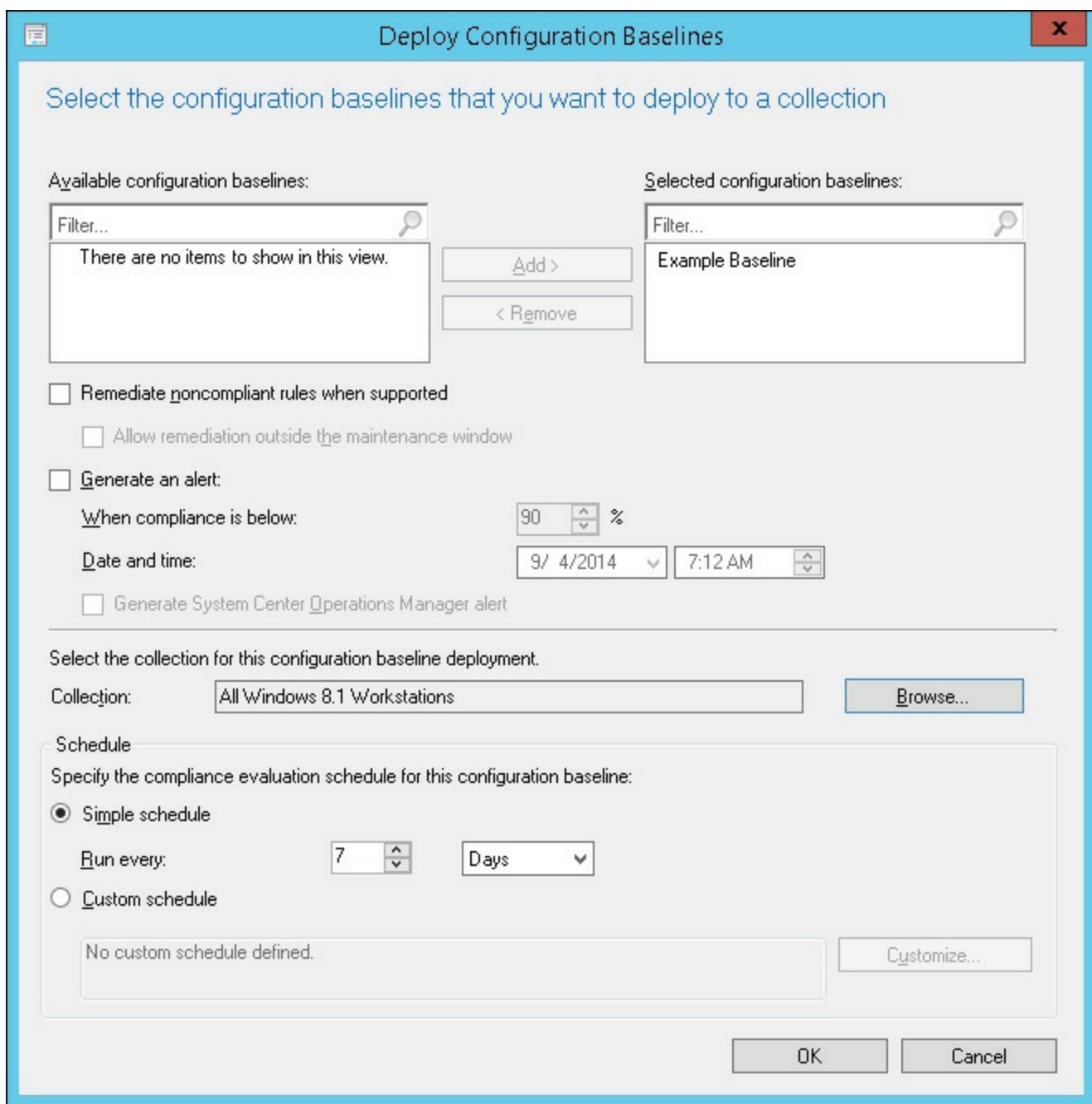
FIGURE 4-4 Deploy Configuration Baselines

The following settings are available in the Deploy Configuration Baselines dialog box:

- **Available Configuration Baselines** Use this list box to select any additional baselines you want to deploy as part of this deployment.

- **Selected Configuration Baselines** This list box displays the baselines that are selected for this deployment.

- **Remediate Noncompliant Rules When Supported** You can configure certain configuration items for automatic remediation. If you enable remediation, you also can allow the remediation process to ignore maintenance windows by selecting the Allow Remediation Outside The Maintenance Window check box.

- **Generate An Alert When Compliance Is Below The Specified Percentage After The Specified Date And Time** When you enable this setting, the compliance percentage check box and the Date And Time check box are also selected. If the specified percentage of systems is not compliant by the specified date and time, Configuration Manager generates an alert. If you are

using System Center 2012 R2 Operations Manager, you can configure Configuration Manager to send the alert to Operations Manager as well, by enabling Generate System Center Operations Manager Alert in this dialog box.

- **Select The Collection For This Configuration Baseline Deployment** Use the Browse button in this option to select the user or device collection to which this baseline will deploy.

- **Specify The Compliance Evaluation Schedule For This Configuration Baseline** Use the default schedule configured on the default client settings or customize the evaluation schedule for the deployment.

More Info: **Deploying Baselines**

You can learn more about deploying baselines at *http://technet.microsoft.com/en-us/library/hh219289.aspx*.

Configuration packs

Configuration packs are predefined configuration items or configuration baselines that Microsoft and other developers provide to organizations. These configuration packs often represent best-practice configurations for common operating systems, server roles, services, and programs. For example, some auditing firms use configuration packs to assess whether an organization complies with specific regulations regarding computer configuration.

You can download Microsoft and some non-Microsoft configuration packs from the Microsoft System Center Marketplace. In addition, you can find configuration packs created by users on several Configuration Manager community support websites. You also can add existing Configuration Manager 2007 configuration packs to System Center 2012 R2 Configuration Manager by using the import functionality.

After you download and import a configuration pack, you can use the configuration items and configuration baselines as they are. Alternatively, you can use them as a starting point for your own configuration settings and then modify the imported configuration packs to meet your requirements.

Viewing compliance information

You can use the Configuration Manager Control Panel item to evaluate the baselines for compliance settings manually or to view the evaluation results for the compliance settings baselines. You require local administrator rights to view a report in the Configuration Manager Control Panel item.

To view compliance on a Configuration Manager client, you can access the Configuration Manager Properties dialog box within Control Panel. The Configurations tab of the Configuration Manager Properties dialog box displays the following basic information:

- A list of all the configuration baselines, including the last version of the baseline that was downloaded

- The last time the evaluation was performed and the results of the evaluation

- The configuration baseline evaluations (if any) that are currently running on this computer

You can use the Configurations tab to perform the following actions:

- **Evaluate** You can select a deployed configuration baseline and then use the Evaluate button to

run the evaluation outside the current schedule.

- ■ **View Report** When you click the View Report button, an Internet Explorer window appears, displaying a report on the selected configuration baseline. The report displays the compliance status of the baseline and all the configuration items that are in the configuration baseline.
- ■ **Refresh** The Refresh button updates the display with current information.

The Configuration Manager site receives the compliance information the client systems generate in the form of state messages. You can use this information to:

- ■ View the compliance of the deployment.
- ■ Create collections based on the state of configuration items.
- ■ Generate and view compliance reports.

Compliance monitoring

Like all deployments, you can monitor the compliance baseline deployments in the Monitoring workspace in the Deployments node. When you select a compliance deployment, the preview pane displays the following:

- ■ **General information** This section includes the name of the deployment and the target collection.
- ■ **Compliance statistics** This section includes a pie chart displaying the relative number of Compliant, Error, Non-Compliant, and Unknown client systems. The total asset count and the time of the summarization appear with a link to a detailed status view.
- ■ **Related objects** This section includes links to the target collection and the deployed baseline.

When you click the View Status link in the preview pane, Configuration Manager displays a more detailed view of the compliance information. The Deployment Status window shows general information similar to the information in the preview pane, including the name of the baseline and target collection and the time the last summarization ran. The Compliant, Error, Non-Compliant, and Unknown tabs display detailed information such as the configuration items, the number of assets, and a list of clients. You can use the More Details link to view the details of a specific asset.

Compliance management reports

The following reports, some of which are listed in Figure 4-5, are available for viewing compliance evaluation results:

- ■ List Of Unknown Assets For A Configuration Baseline
- ■ List Of Rules Conflicting With A Specified Rule For An Asset
- ■ List Of Assets By Compliance State For A Configuration Item In A Configuration Baseline
- ■ Rules And Errors Summary Of Configuration Items In A Configuration Baseline For An Asset
- ■ Summary Compliance Of A Configuration Baseline For A Collection
- ■ Summary Compliance By Configuration Items For A Configuration Baseline
- ■ Summary Compliance By Configuration Baseline
- ■ List Of Assets By Compliance State For A Configuration Baseline
- ■ Details Of Compliant Rules Of Configuration Items In A Configuration Baseline For An Asset

- Compliance History Of A Configuration Item
- Compliance History Of A Configuration Baseline
- Details Of Conflicting Rules Of Configuration Items In A Configuration Baseline For An Asset
- Details Of Remediated Rules Of Configuration Items In A Configuration Baseline For An Asset
- Details Of Noncompliant Rules Of Configuration Items In A Configuration Baseline For An Asset
- Details Of Errors Of Configuration Items In A Configuration Baseline For An Asset
- List Of Unknown Assets For A Configuration Item
- Details Of Conflicting Rules Of Configuration Items In A Configuration Baseline For An Asset
- Details Of Compliant Rules Of Configuration Items In A Configuration Baseline For An Asset
- Summary Compliance By Configuration Policies
- List Of Assets With Certificate Nearing Expiry
- List Of Assets By Certificate Insurance Status
- Certificate Issuance History
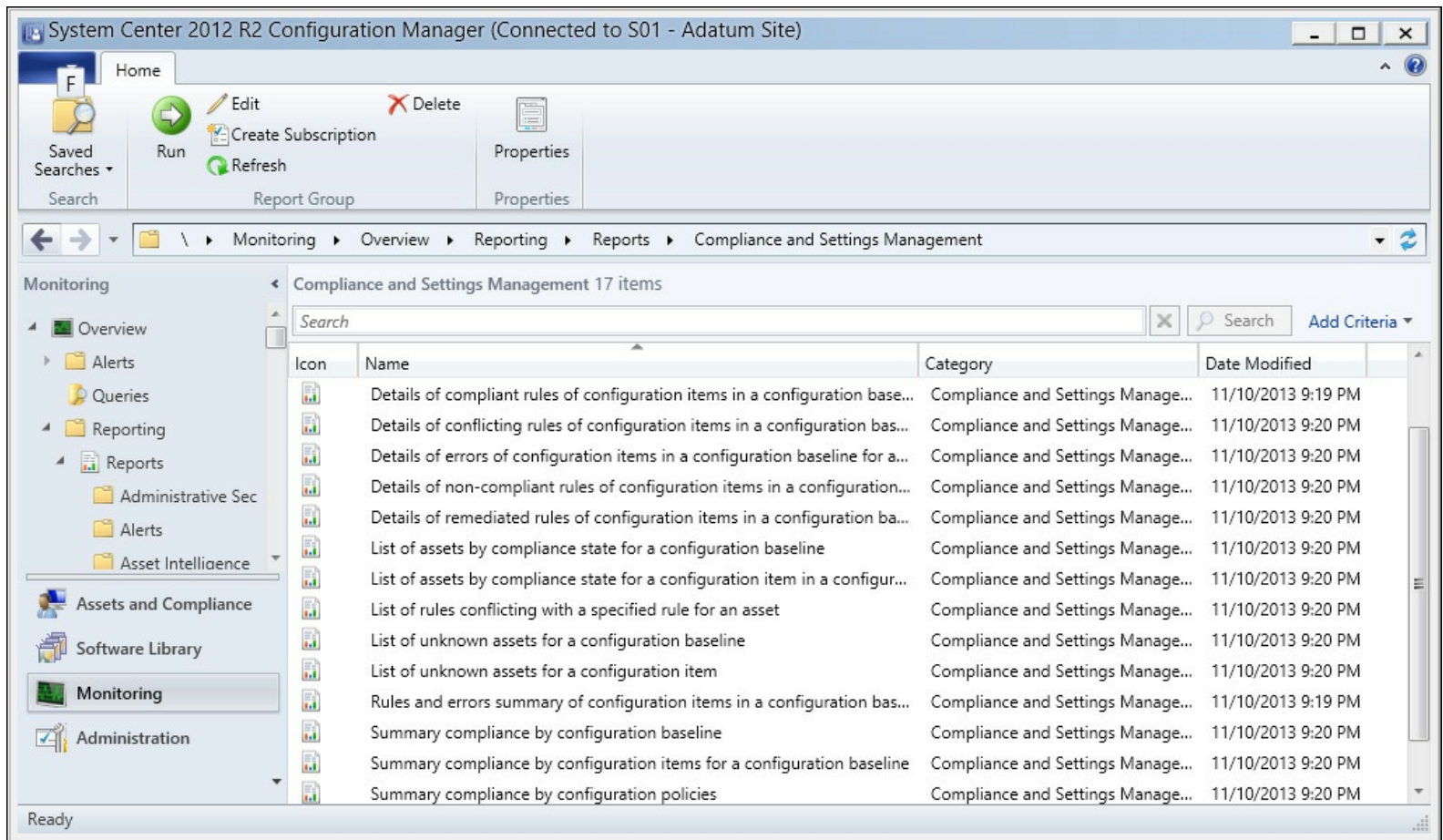
FIGURE 4-5 Compliance reports

More Info: **Monitor Compliance Settings**

You can learn more about monitoring compliance settings at *http://technet.microsoft.com/en-us/library/gg712303.aspx/*.

![Thought experiment icon] *Thought experiment:* **Compliance Monitoring at Fabrikam**

You are using Configuration Manager's compliance functionality to monitor compliance across multiple device collections at your organization. A specific baseline, which includes a large number of configuration items, reports a large percentage of noncompliant clients. You're interested in determining whether a large number of configuration items or just one or two items are causing the noncompliant result. With this information in mind, answer the following questions:

1. **Which report would you use to determine the specific configuration items in a baseline that are triggering noncompliance when applied to a collection?**

2. **Which report would you view to determine the compliance trend for a configuration baseline?**

Objective summary

- A configuration baseline is a group of configuration items, software updates, and other configuration baselines.
- You can group configuration items into configuration baselines.
- You deploy configuration baselines to client systems to evaluate compliance and (potentially) perform remediation.
- You can use the evaluation results of the configuration baseline to create a collection.
- Configuration packs are predefined configuration items or configuration baselines that Microsoft and other developers provide to organizations.

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 of the following can you include in a configuration baseline? (Choose two. Each correct answer provides a complete solution.)

    A. Configuration item

    B. Antimalware policy

    C. Windows Firewall policy

D. Software updates

2. Which of the following options must you select when deploying a configuration baseline so that configuration items are automatically remediated when it is possible to do so? (Choose two. Each correct answer provides a complete solution.)

    A. Select The Collection For This Configuration Baseline Deployment

    B. Select The Compliance Evaluation Schedule For This Configuration Baseline

    C. Generate An Alert When Compliance Is Below The Specified Percentage After The Specified Date And Time

    D. Remediate Noncompliant Rules When Supported

3. You want an alert to be generated if the percentage of computers in a specific collection that isn't compliant after two weeks rises above 25 percent. Which of the following settings must you configure when configuring the deployment of a configuration baseline? (Choose two. Each correct answer provides part of a complete solution.)

    A. Remediate Noncompliant Rules When Supported

    B. Generate An Alert When Compliance Is Below The Specified Percentage After The Specified Date And Time

    C. Select The Compliance Evaluation Schedule For This Configuration Baseline

    D. Select The Collection For This Configuration Baseline Deployment

4. A configuration baseline includes a configuration item that tests for the presence of a particular file on the operating system volume. You want to create a collection of all computers in the Sydney Windows 8.1 Computers collection on which this file is not present on the operating system volume. Which of the following compliance states should you use as the basis for creating a new collection?

    A. Compliant

    B. Non-Compliant

    C. Error

    D. Unknown

Objective 4.3: Configure Endpoint Protection

System Center Endpoint Protection is an antimalware client that you can deploy, manage, and monitor as part of your organization's Configuration Manager deployment. You can also use System Center Endpoint Protection to manage the firewall settings of Configuration Manager clients.

System Center Endpoint Protection

System Center Endpoint Protection is an antimalware client. Prior to the release of System Center 2012, this client was part of the ForeFront suite of products. When you deploy the Configuration Manager Endpoint Protection feature, an Endpoint Protection client installs on Configuration Manager client computers. You can use the Endpoint Protection client to:

- **Detect and remediate malware, rootkit, network, and spyware vulnerabilities** The Endpoint Protection client provides protection by performing scheduled scans on a computer or by enabling real-time protection. Both these methods monitor file and program activity on a computer. The client can use Network Inspection System to inspect network traffic for the most commonly used protocols, such as HTTP, Server Message Block (SMB), and Simple Mail Transfer Protocol (SMTP).

- **Automatically download antimalware definitions and engine updates** You can deploy policies that define how often antimalware definitions are updated and how a client obtains the updates.

- **Manage Windows Firewall settings** Endpoint Protection provides basic management of Windows Firewall for the domain, private, and public profiles. Settings include enabling or disabling the firewall; notifying the user when Windows Firewall blocks a new program; and blocking all incoming connections, including those in the list of allowed programs.

Integrating Endpoint Protection with Configuration Manager provides the following benefits:

- **Flexible source locations for client updates** You can use a variety of source locations for definition updates. You can configure Endpoint Protection to:
  - Obtain updates that Configuration Manager or Windows Server Update Services (WSUS) distributes.
  - Allow direct connection to Microsoft Update and the Microsoft Malware Protection Center.
  - Obtain updates from a Universal Naming Convention (UNC) file share.

- **The ability to take advantage of the management infrastructure** Endpoint Protection uses the existing Configuration Manager infrastructure to communicate policy settings to clients and retrieve status information from clients.

- **Enhanced monitoring and reporting** Configuration Manager provides extensive monitoring capabilities such as email notifications, in-console monitoring, and reports that inform

administrators of malware presence and the security status of client computers.

> *More Info:* **Introduction to Endpoint Protection**
>
> **You can learn more about Endpoint Protection at** *http://technet.microsoft.com/en-us/library/hh508781.aspx.*

Implement Endpoint Protection

Implement Endpoint Protection by performing the following general steps:

1. In the central administration site or a standalone site, install the Endpoint Protection Point Site System role.

2. Create collections as necessary and then configure Endpoint Protection alerts for each collection. Subscribe to alerts as necessary.

3. Determine the source for obtaining updates to malware definitions and the antimalware engine. You must configure additional roles, such as the Software Update Point role, if you plan to use Configuration Manager software updates as the update source.

4. Configure antimalware policies as needed. The Default Antimalware Policy will apply to all Endpoint Protection clients in the hierarchy. You can create and deploy custom antimalware policies that will override the settings in the default policy.

5. Configure client settings for Endpoint Protection. You can use client settings to install and enable Endpoint Protection clients on client computers. As you enable clients, any antimalware policies that you have configured through client settings will come into effect. You can create and deploy custom client settings to target specific collections as needed.

6. Optionally, create and deploy Windows Firewall policies. You can configure Windows Firewall profile settings and then deploy the policy to specific collections.

7. Monitor and manage Endpoint Protection by using the console and alerts.

Prerequisites

To implement Endpoint Protection within your Configuration Manager primary site or hierarchy, you must meet the following prerequisites:

- **Endpoint Protection point** Before you can install the Endpoint Protection client on workstations, you must install and configure an Endpoint Protection Point Site System role at the top site in the hierarchy, whether that is a central administration site or a standalone primary site.

- **Client settings** To install the Endpoint Protection client on workstations, you must configure the appropriate default client settings or create and deploy a custom client setting that targets specific collections.

- **Software update point** If you want to use software updates to deliver antimalware definition and engine updates, you must implement the Software Updates feature of Configuration Manager.

- **Reporting services point** Before you can run reports related to Endpoint Protection, you must

configure a reporting services point site system.

- **Security permissions** The Endpoint Protection Manager security role provides the ability to create and modify antimalware and Windows Firewall policies. This security role also enables you to deploy Endpoint Protection policies to collections, to monitor status, and to create and modify console alerts and reports. You must configure the security role before you implement Endpoint Protection.

You can download specific Endpoint Protection clients to protect Mac computers and Linux clients from the Microsoft Volume Licensing Service Center. You cannot manage these clients from the Configuration Manager console. However, you can use a System Center 2012 Operations Manager management pack to manage Linux clients from Operations Manager.

> *More Info:* **Prerequisites**
>
> **You can learn more about Endpoint Protection prerequisites at** *http://technet.microsoft.com/en-us/library/hh508780.aspx***.**

The Site System role

You must deploy the Endpoint Protection Point Site System role before you can install Endpoint Protection on client computers. Consider the following factors when you deploy this Endpoint Protection role:

- **Deployment within a Configuration Manager hierarchy** You can install the Endpoint Protection point only on a single site system server. You must locate this server within the central administration site for a hierarchy configuration or in the primary site in a standalone primary site configuration. You also must accept the specific Endpoint Protection license agreement when prompted.

- **Microsoft Active Protection Service membership** When you install an Endpoint Protection point, you may specify the default Microsoft Active Protection Service membership setting. If you choose to join the service, Configuration Manager automatically collects information about detected software and sends it to Microsoft. Based on this information, Microsoft creates new antimalware definitions. You can choose from two levels of membership:

  - **Basic membership** If you choose this membership, basic information is sent to Microsoft, which includes information about where the software originated and the actions the user or application performed. This level of membership will not alert the user if the service detects a change by a software program that has not been subject to risk assessment.

  - **Advanced membership** This level of membership will alert the user when the service detects a change by software that has not been subject to risk assessment by Microsoft. In addition to basic information, this membership level will send information such as software location, file names, how the software operates, and the effect that the software has had on the computer.

- **Verification of installation status** You can verify the successful installation of an Endpoint Protection point by monitoring the SMS_ENDPOINT_PROTECTION _MANAGER component for a message with the ID of 500. An ID of 500 indicates that the component has started. The EPSetup.log file also provides details about the installation status.

Client settings

You can use Default Client Settings to apply Endpoint Protection installation settings to all clients within the hierarchy. You would create and configure a Custom Client Device Settings item if you needed to apply unique settings to members of a specific collection. For example, you might want to deploy Endpoint Protection to a small group of computers first to test it before you deploy it to the entire hierarchy. Over time, you can add clients to the target collection to provide a phased deployment.

Figure 4-6 shows the Endpoint Protection settings of Default Client Settings.
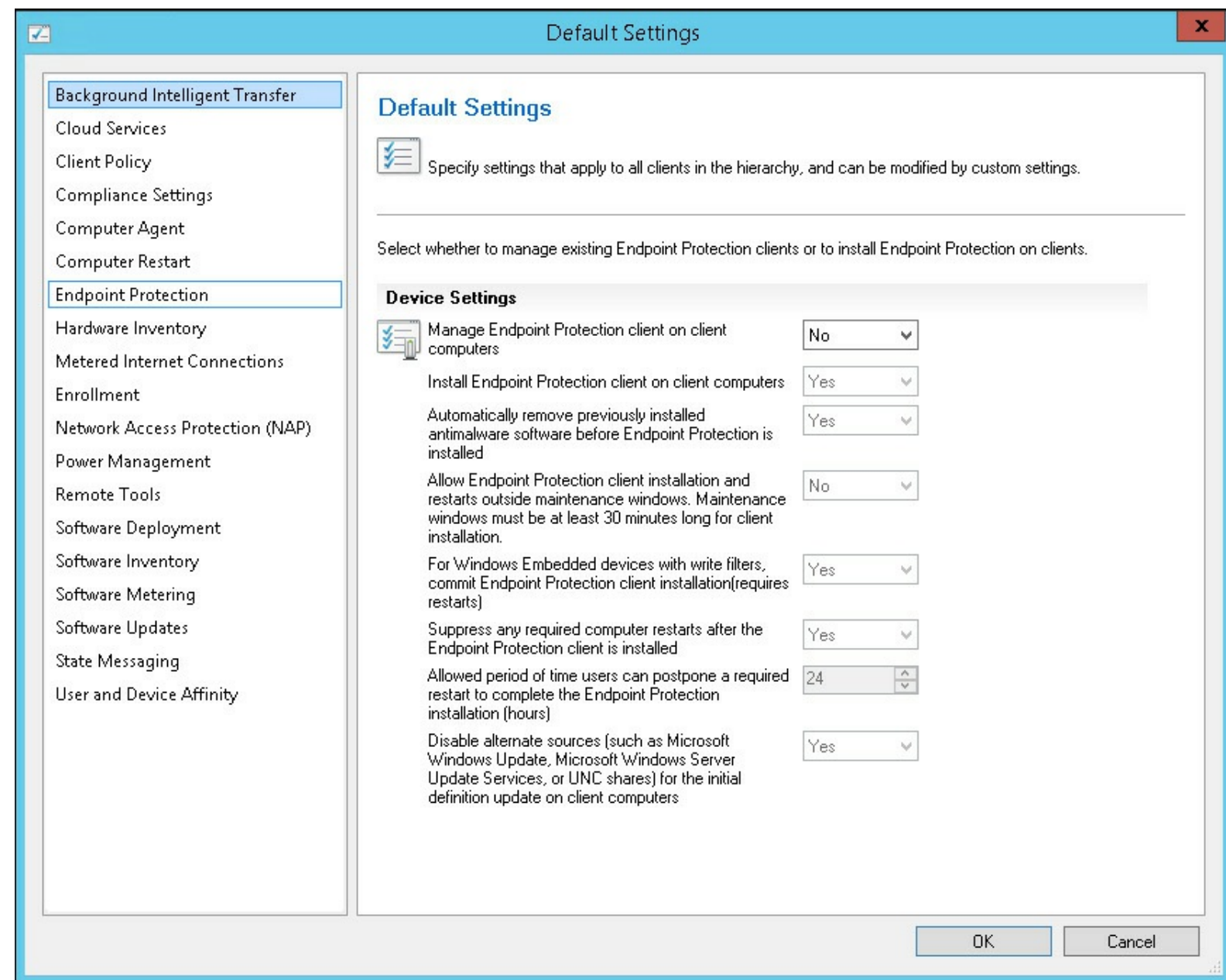
FIGURE 4-6 Endpoint Protection settings

The Endpoint Protection section provides several settings that relate to the installation of the Endpoint Protection client. Table 4-2 describes these settings.

Setting	Description
Manage Endpoint Protection Client On Client Computers	When set to Yes, Configuration Manager manages the existing Endpoint Protection client on client computers. When set to No, Configuration Manager does not manage the Endpoint Protection client. The default setting is No.
Install Endpoint Protection Client On Client Computers	When set to Yes, the Endpoint Protection client installs on client computers. This option is available only if Manage Endpoint Protection Client On Client Computers is set to Yes. When set to No, the Endpoint Protection client will not install on client computers, and all subsequent options are disabled. The default setting is Yes.
Automatically Remove Previously Installed Antimalware Software Before Endpoint Protection Is Installed	When set to Yes, the client installation checks for and uninstalls most third-party antimalware clients. The default setting is Yes. The Endpoint Protection client installation fails if you attempt to install the client on a computer that does not support the uninstallation of an existing antimalware solution. In this case, uninstall the existing antimalware solution before you enable Endpoint Protection.
Allow Endpoint Protection Client Installation And Restart Outside Maintenance Windows. Maintenance Windows Must Be At Least 30 Minutes Long For Client Installation	If set to Yes, the Endpoint Protection client installs outside the specified maintenance window for the device. If set to No, the client installs only during the specified maintenance window. The default setting is No. A maintenance window must be at least 30 minutes long for the Endpoint Protection client to install successfully.
For Windows Embedded Devices With Write Filters, Commit Endpoint Protection Client Installation (Requires Restarts)	This setting specifies how the Endpoint Protection client installs on a Windows Embedded device. If you select Yes, the write filter is disabled, which allows the installation to commit on the device. This also requires a restart of the device. If you select No, the client installs on a temporary overlay and is not committed until another installation commits the changes to the device. The default setting is No.

Suppress Any Required Computer Restarts After The Endpoint Protection Client Is Installed	If set to Yes, after the client installs the client will suppress any required restarts. The default setting is Yes. Consider deploying KB981889 to your Configuration Manager clients before you deploy the Endpoint Protection client. This update requires a client restart, but it can help you prevent restarts during the Endpoint Protection client installation task.
Allowed Period Of Time Users Can Postpone A Required Restart To Complete The Endpoint Protection Installation (Hours)	This setting specifies the number of hours a user can postpone a potential restart after the client installs. The default setting is 24 hours. This option is available only if Suppress Any Required Computer Restarts After The Endpoint Protection Client Is Installed is set to Yes.
Disable Alternate Sources (Such As Microsoft Windows Update, Microsoft Windows Server Update Services, Or UNC Shares) For The Initial Definition Update On Client Computers	After you install the Endpoint Protection client, it will connect immediately to a source and update its antimalware signatures. The default setting is Yes. If you set this to Yes, the initial update of the antimalware signatures from a remote source is disabled. In this case, only Configuration Manager provides the initial update to client computers. This setting helps avoid unnecessary network connections to remote locations such as the Internet and can reduce network bandwidth during the initial installation. Setting this option to No allows the client to update the antimalware signatures from a remote source after initial installation of the client.

TABLE 4-2 Endpoint Protection settings

Antimalware policies

You use an antimalware policy to control configuration settings for the Endpoint Protection client on client computers. When you configure client settings to install Endpoint Protection on client computers, a default client antimalware policy is applied to provide initial protection after the installation.

Figure 4-7 shows the default client antimalware policy.
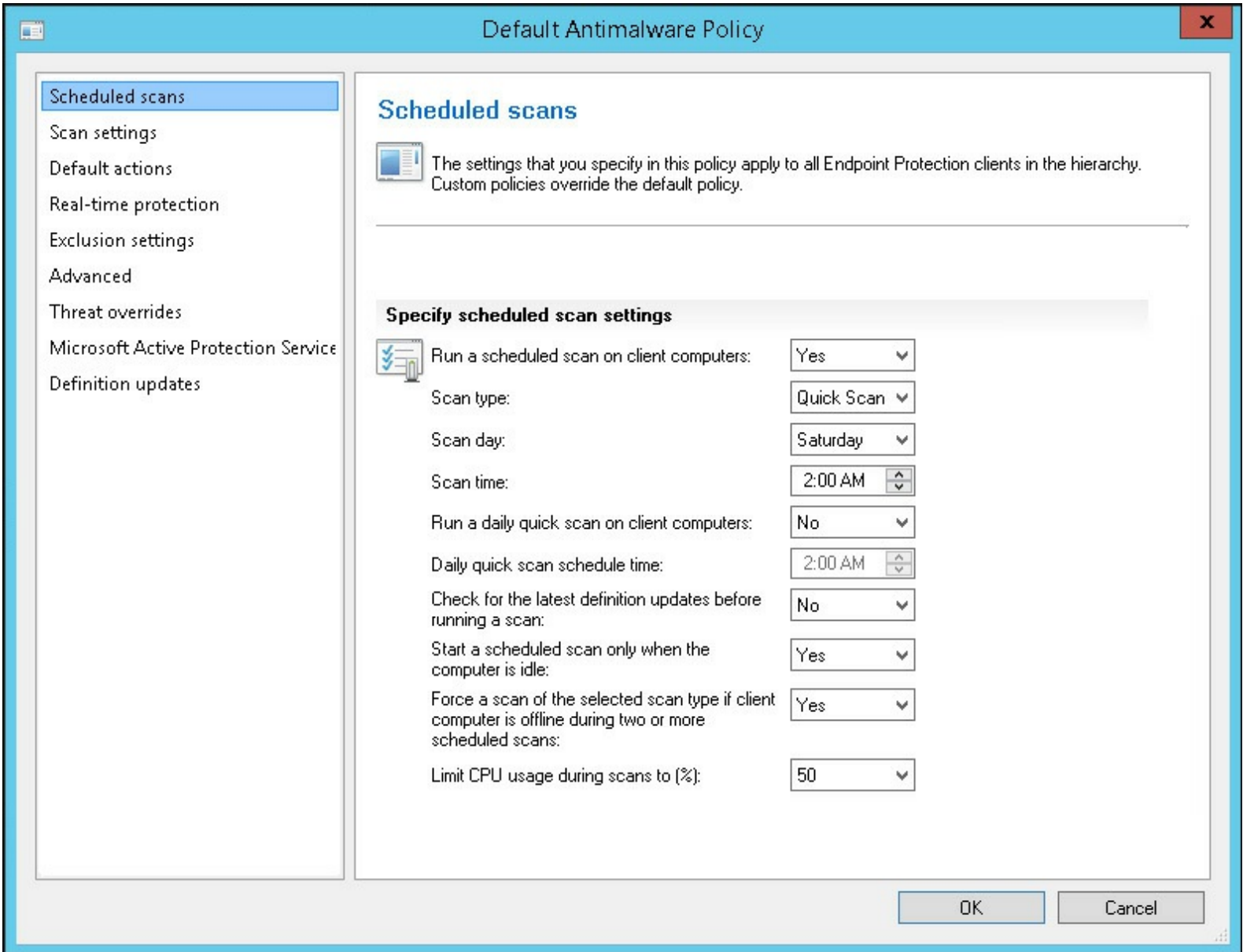
FIGURE 4-7 Scheduled Scans

You can import preconfigured policy templates, or you can create your own custom antimalware policy and deploy the policy to collections. This enables you to provide different Endpoint Protection client settings based on the requirements of the computers contained within a collection. For example, you might have a group of computers in a collection that require specific files or file locations excluded from the malware scan processes. A custom antimalware policy enables you to address this requirement.

If you deploy a custom antimalware policy to a collection, the custom policy settings merge with the default client antimalware policy. A single computer might be a member of multiple collections that have an assigned policy. The client uses priority evaluation to determine which policy to apply. The policy with the highest priority, which is the lowest number displayed in the Priority column, will take precedence. That policy then applies appropriate settings to the Endpoint Protection client software.

To modify the default antimalware policy, perform the following procedure:

1. In the Configuration Manager console, click the Assets And Compliance workspace.

2. Expand the Endpoint Protection node and then click Antimalware Policies.

3. In the results pane, click Default Client Malware Policy.

4. On the ribbon, click Properties.

The Default Antimalware Policy dialog box appears.

Settings that you configure in the Default Antimalware Policy dialog box apply to all computers in the hierarchy on which the Endpoint Protection client is installed unless overridden by a custom malware policy that is assigned to the client.

To create and deploy a custom antimalware policy, perform the following procedure:

1. In the Configuration Manager console, click the Assets And Compliance workspace.

2. Expand the Endpoint Protection node and then click Antimalware Policies.

3. On the ribbon, click Create Antimalware Policy.

The Create Antimalware Policy dialog box appears. In this dialog box, you can provide a name and specify configuration settings.

4. To assign a custom antimalware policy to a collection, choose the policy to deploy and then, on the ribbon, click Deploy.

The Select Collection dialog box appears.

5. In the Select Collection dialog box, select the collection to which you want to deploy this policy and then click OK.

You also can import an existing Endpoint Protection template by selecting the Antimalware Policies node and then clicking Import on the ribbon. Configuration Manager provides several preconfigured antimalware policy settings for high security, standard desktop, server role-based, or performance-optimized scenarios.

Table 4-3 lists the available antimalware policy settings.

Setting	Description
Scheduled Scans	Provides settings to enable or disable a scheduled scan on client computers. When you enable scheduled scans, additional scan options are available, such as the type of scan, the day and time of the scan, and performance options such as starting the scan only when the computer is idle.
Scan Settings	Provides settings that describe what the client should scan—for example, removable storage devices, network drives, and email.
Default Actions	Provides settings to specify how Endpoint Protection should respond to Severe, High, Medium, and Low classified threats. Possible options include Allow, Quarantine, and Remove. For Severe and High threats, you can select an additional option, Recommended, which treats the threat as instructed within the definition files. You cannot select Allow for threats classified as Severe or High.
Real-time Protection	Provides settings to enable real-time protection. If you enable real-time protection, additional options are available to specify whether to scan incoming files, outgoing files, or both. You also can specify whether users can configure real-time protection settings on their computers.
Exclusion Settings	Enables you to specify files, locations, file types, and processes to exclude from the scanning process.
Advanced	Provides settings to specify options such as whether to create a system restore point before cleaning computers, show notification messages to users, delete quarantined files after a specified number of days, and allow users to control exclusions.

Threat Overrides	Enables you to configure a specific action (Allow, Remove, or Quarantine) based on a threat name.
Microsoft Active Protection Service	Enables you to specify whether clients join Microsoft Active Protection Service. You also can specify whether you want to allow end users to modify Microsoft Active Protection Service settings on their client.
Definition Updates	Provides options to specify how often a client will check for definition updates. Settings include specifying the location and order in which the client obtains updated definitions. Possible source options include: ■ Updates Distributed From Configuration Manager. ■ Updates Distributed From WSUS. ■ Updates Distributed From Microsoft Update. ■ Updates Distributed From Microsoft Malware Protection Center. ■ Updates From UNC File Shares. You can define the order in which to contact update sources. If you choose to provide updates from UNC file shares, you must download the updates manually and store them in specific folders on the UNC file share. Files for x64-based computers must be in a folder named x64, and files for x86-based computers must be in a folder named x86. You must share the parent folder that contains the x64 and x86 folders with Read access permissions for the client computers and domain users that connect to the share. During an automatic update, the client computer's computer account is used to authenticate to the share. When a user manually updates the definitions, that user's user account authenticates to the share.

TABLE 4-3 Antimalware policy settings

More Info: **Antimalware Policies**

You can learn more about antimalware policies at *http://technet.microsoft.com/en-us/library/hh508785.aspx***.**

Windows Firewall policies

Endpoint Protection provides you with the ability to control basic settings for Windows Firewall. You can configure a firewall policy to establish the following settings for each type of network profile, including domain, private, and public:

- **Enable Windows Firewall** This setting controls whether Windows Firewall is turned on or off. Options include Yes, No, and Not Configured.

- **Block All Incoming Connections, Including Those In The List Of Allowed Programs** This setting is available only if Enable Windows Firewall is set to Yes for the corresponding network profile. This setting controls whether incoming connections are allowed to the client computers. Options include Yes, No, and Not Configured.

- **Notify The User When Windows Firewall Blocks A New Program** This setting is available only if Enable Windows Firewall is set to Yes for the corresponding network profile. This setting controls whether users are notified when Windows Firewall blocks a program. Options

include Yes, No, and Not Configured.

In a manner similar to how you create a custom antimalware policy, you can create a firewall policy and then deploy the policy to a collection. There is no default Windows Firewall policy. During the policy deployment, you also can configure a schedule to evaluate compliance to the policy. This enables you to view deployment status for the policy to determine which clients are compliant or noncompliant with the Windows Firewall policy.

To create and deploy a firewall policy, perform the following procedure:

1. In the Configuration Manager console, click the Assets And Compliance workspace.

2. Expand the Endpoint Protection node and then click Windows Firewall Policies.

3. On the ribbon, click Create Windows Firewall Policy. The Create Windows Firewall Policy dialog box appears. Provide a name and description and then click Next.

4. On the Profile Settings page, configure settings for each of the network profiles, if required, and then complete the wizard.

To assign a firewall policy to a collection, perform the following procedure:

1. Select the policy you want to deploy and then, on the ribbon, click Deploy.

The Deploy Windows Firewall Policy dialog box appears.

2. Click the Browse button and, in the Select Collection dialog box, select the appropriate device collection. Click OK.

3. Under Specify The Compliance Evaluation Schedule For This Configuration Baseline, specify the schedule to evaluate client compliance with the policy. The default value is to evaluate compliance every seven days. Click OK to close the Deploy Windows Firewall Policy dialog box.

When you deploy a Windows Firewall policy to a device collection, the policy applies to clients in a random order over a two-hour period. This helps decrease the impact on the network.

Policy management

After you deploy antimalware and Windows Firewall policies, you can perform a number of policy management tasks. Table 4-4 provides a summary of them.

Task	Description
Increase priority	If multiple policies are deployed to the same computer, the policies apply in the order shown in the Order column of the Antimalware Policies or Windows Firewall Policies results pane. You can use Increase Priority to increase the priority on a selected policy. This option is available for both antimalware and Windows Firewall policies.
Decrease priority	Similar to Increase Priority, you can use Decrease Priority to decrease the priority of a selected policy. This option is available for both antimalware and Windows Firewall policies.
Merge antimalware policies	This option enables you to merge multiple antimalware policies into a single policy. During the merge, if any policy conflicts occur they are resolved by using the most secure option for the conflicting setting.
Perform an on-demand scan	You might need to perform an on-demand scan of a single computer or a collection of computers outside the scheduled scan. If you select a device collection, the Endpoint Protection button, when clicked, provides options to perform a Full Scan or a Quick Scan on all computers within the collection. If you select a specific computer within a collection, you also can choose to perform a Full Scan or Quick Scan on the selected computer as required. This creates a Configuration Manager client notification, which attempts to initiate the scan as soon as possible.
Force computers to download the latest antimalware definition files	You can force a download of the latest antimalware definition files by performing the following procedure: 1. Select a device collection or a specific computer within a collection. 2. On the Collection tab, click Endpoint Protection. 3. Click Download Definition to open the Download Definition dialog box. 4. In the Download Definition dialog box, select a definition update source: Software Update Deployment or Endpoint Protection Client Source Order. 5. The Download Definition dialog box provides an option to randomize client execution of the download task. Configure the randomization period. The randomization period is set to 120 minutes by default.
Set security scopes	For each antimalware policy, you can define a specific security scope. This enables you to delegate policy management to specific administrative users. For example, you might specify a policy for workstations and configure another policy for servers. You can assign the workstation policy to a scope named Workstations, and you can assign the server policy to a scope named Servers. Then you can assign each scope to appropriate administrative users.

TABLE 4-4 Policy management tasks

Monitoring Endpoint Protection status

Configuration Manager provides extensive functionality, enabling you to monitor the status of the Endpoint Protection client. You can use Configuration Manager to perform the following monitoring tasks:

- Ensure that computers have successfully installed the Endpoint Protection client.
- Determine the status of the antimalware definition files on computers.
- Determine which types of malware have been detected, how many computers have been affected, and the remediation status.

Table 4-5 describes the methods to monitor Endpoint Protection status and compliance.

Method	Description
System Center 2012 R2 Endpoint Protection Status	The Monitoring workspace has a node named Endpoint Protection Status. Under this node is another node, named System Center 2012 R2 Endpoint Protection Status. This node provides information such as: ■ Endpoint Protection client status. ■ Malware remediation status. ■ Top 5 malware by number of computers. ■ Operational status of clients. ■ Definition status on computers.By default, All Systems is selected to show status information. If you want to view the status of other collections, you must select a collection for which you want to view status information. You can select collections that are listed only when: ■ You have deployed an antimalware policy to a collection. ■ You enable View This Collection In The Endpoint Protection Dashboard on the Alerts tab of the device collection's properties.
Malware Detected	The Monitoring workspace also has a node named Malware Detected. This node provides a summary of detected malware, including information such as Collection, Threat Name, Computers Infected, and Computers Remediated.
Antimalware Policies and Malware Detail tabs	In the Assets And Compliance workspace, you can click the Devices node (or expand the Device Collections node) and double-click to view the membership of a device collection. When you select a computer, the preview pane displays an Antimalware Policies tab and a Malware Detail tab. The Antimalware Policies tab shows statistics related to the application state of the policy applied to the client. The Malware Detail tab provides statistics on detected threats and the computer's remediation state.
Reports	The Endpoint Protection report category provides six reports that you can use to classify antimalware activity and infection status. These reports include the following: ■ Antimalware Activity Report ■ Antimalware Overall Status And History ■ Computer Malware Details ■ Infected Computers ■ Top Users By Threats ■ User Threat List

TABLE 4-5 Endpoint Protection monitoring methods
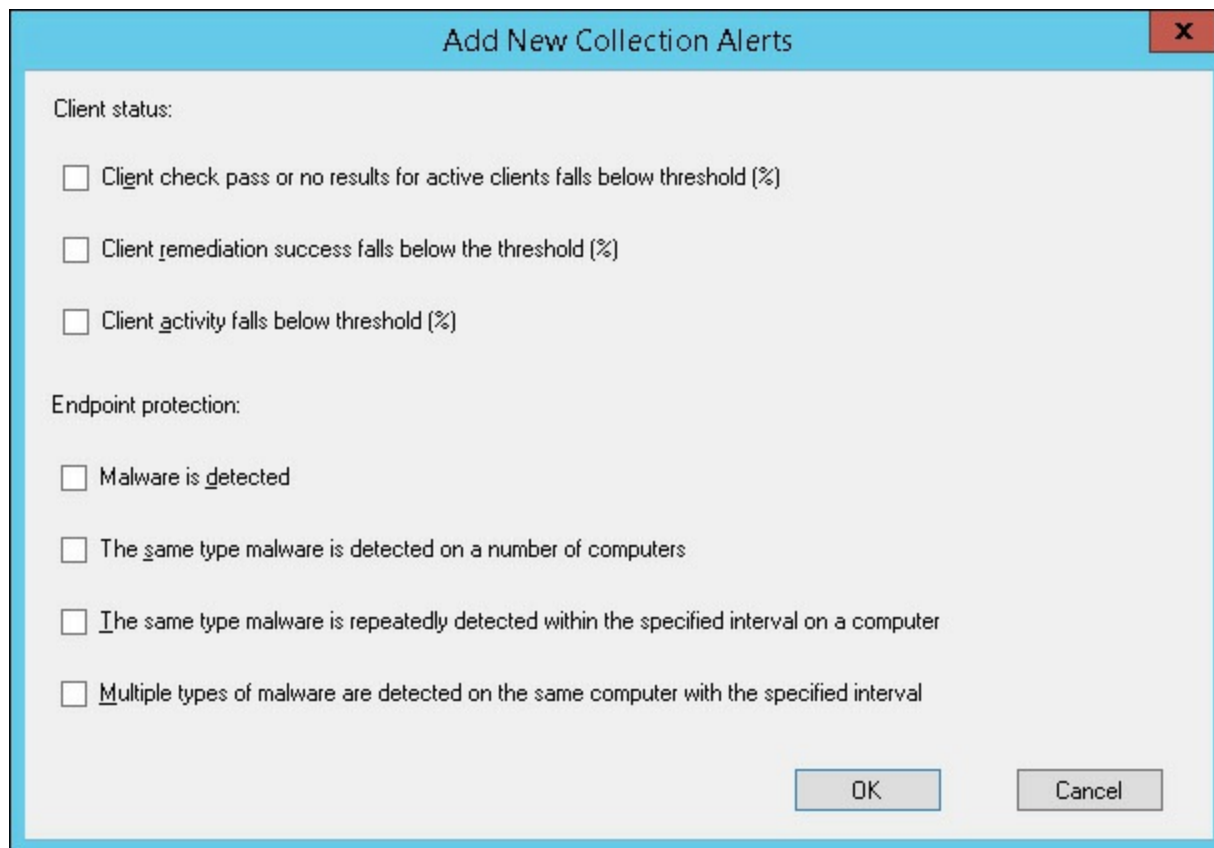
Configuring alerts

You can use Configuration Manager alerts to notify administrative users when specific events have occurred within the hierarchy. You can configure alerts for each collection by opening the Properties dialog box of that collection and then selecting the Alerts tab and clicking Add. This displays the Add New Collection Alerts dialog box, shown in Figure 4-8. Table 4-6 describes the Endpoint Protection events that you can enable to generate alerts.

FIGURE 4-8 Add New Collection Alerts

Event	Description
Malware Is Detected	When you select this event, an alert is generated if malware is detected on any computer within the collection. You can define the malware detection threshold for the alert. Choose from the following options: ■ **High – All Detections** An alert is generated whenever malware is detected, regardless of the action the Endpoint Protection client takes. ■ **Medium – Detected, Pending Action** An alert is generated only if one or more computers require a manual action to complete the malware removal. ■ **Low – Detected, Still Active** An alert is generated when there are one or more computers in the collection on which detected malware is still active.
The Same Type Malware Is Detected On A Number Of Computers	When you select this event, an alert is generated if the same malware has been detected on a specified percentage of computers.
The Same Type Malware Is Repeatedly Detected Within The Specified Interval On A Computer	When you select this event, an alert is generated if specific malware is detected more than a specified number of times over a specified number of hours.
Multiple Types Of Malware Are Detected On The Same Computer With The Specified Interval	When you select this event, an alert is generated if more than a specified number of malware types are detected over a specified number of hours on computers in the monitored collection.

TABLE 4-6 Endpoint Protection alert settings

For each event, you also can specify the severity of the alert itself. Choose Critical, Warning, or Information.

More Info: **Configuring Alerts**

You can learn more about configuring alerts for Endpoint Protection in Configuration Manager at *http://technet.microsoft.com/en-us/library/hh508782.aspx*.

Exam Tip

Remember how antimalware policy priority works.

Objective summary

- System Center Endpoint Protection is an antimalware client that can detect and remediate malware, rootkit, network, and spyware vulnerabilities; automatically download antimalware definitions and engine updates; and manage Windows Firewall settings.
- Endpoint Protection requires a Configuration Manager Endpoint Protection point, which you configure with client settings and, depending on how you want definition updates delivered, a software update point.
- You use an antimalware policy to control configuration settings for the Endpoint Protection client on client computers.
- You can configure a firewall policy to establish settings for each type of network profile, including domain, private, and public.

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 of the following locations can host antimalware definition update files for an Endpoint Protection client? (Choose three. Each correct answer provides a complete solution.)

   A. FTP site

   B. Microsoft Update/Microsoft Malware Protection Center

   C. UNC file share

   D. WSUS server

2. Your organization has a central administration site; the Sydney primary site; the Melbourne primary site; and secondary sites at Canberra, Geelong, and Newcastle. The Geelong site is a secondary site of the Melbourne site. Clients in the Geelong site will be using System Center

Endpoint Protection. In which site should you deploy the Endpoint Protection Point Site System role?

- A. Central administration site
- B. Melbourne
- C. Sydney
- D. Geelong

3. Which of the following would you configure in an antimalware policy to ensure that files on volume E were not scanned for malware by the Endpoint Protection client?

- A. Advanced settings
- B. Real-time protection
- C. Exclusion settings
- D. Threat overrides

4. Which of the following antimalware policy settings would you configure to have a system restore point automatically created by the Endpoint Protection client before cleaning malware from computers?

- A. Real-time protection
- B. Exclusion settings
- C. Advanced settings
- D. Threat overrides

Answers

Objective 4.1

Thought experiment

1. You must configure the Intune connector to manage mobile device configuration item settings.
2. You could look for application-specific registry settings by using Registry Key settings or look for files related to the application by using File System configuration item settings.

Objective review

1. **Correct answers:** A and C

- A. **Correct:** Registry values support remediation.
- B. **Incorrect:** Registry keys do not support remediation. Registry values do.
- C. **Correct:** WQL queries support remediation.
- D. **Incorrect:** XPath queries do not support remediation.

2. **Correct answer:** C

- A. **Incorrect:** You use an Active Directory query setting type to perform an Active Directory query to locate values in Active Directory.

B. **Incorrect:** You use the Assembly setting type to determine whether an assembly from the global assembly cache is present.

C. **Correct:** You can use a File System setting type in a configuration item to determine whether a particular file is present on a Configuration Manager client.

D. **Incorrect:** You use a Registry Value setting type to check for a registry value.

3. **Correct answer:** D

A. **Incorrect:** You use a Registry Value setting type to check for a registry value. You use Registry Key to check for a registry key.

B. **Incorrect:** You use the WQL query setting to determine whether a WQL query run on a Configuration Manager client matches a specific value.

C. **Incorrect:** You can use the Script setting type to run a script that checks for a specific result or runs as a remediation script to remedy a noncompliant setting.

D. **Correct:** You use a Registry Key setting type to check for a registry key.

4. **Correct answer:** B

A. **Incorrect:** You use this setting to determine whether a WQL query run on a Configuration Manager client matches a specific value.

B. **Correct:** You can use the Script setting type to run a script that checks for a specific result or runs as a remediation script to remedy a noncompliant setting.

C. **Incorrect:** You can use a File System setting type in a configuration item to determine whether a particular file is present on a Configuration Manager client.

D. **Incorrect:** You use the Assembly setting type to determine whether an assembly from the global assembly cache is present.

5. **Correct answer:** A

A. **Correct:** You use this setting to determine whether a WQL query run on a Configuration Manager client matches, is greater than, or is less than a specific value.

B. **Incorrect:** Although you could call a script that runs the query, the best answer is to use the WQL query type directly rather than calling a WQL query in a script.

C. **Incorrect:** You can use a File System setting type in a configuration item to determine whether a particular file is present on a Configuration Manager client.

D. **Incorrect:** You use a Registry Value setting type to check for a registry value.

Objective 4.2

Thought experiment

1. You can use the Summary Compliance By Configuration items for a configuration baseline when looking at a collection. You use the detailed report for a specific asset.

2. You would use the compliance history of a configuration baseline report to view configuration baseline compliance trend data.

Objective review

1. Correct answers: A and D

    A. Correct: A configuration baseline is a group of configuration items, software updates, and other configuration baselines.

    B. Incorrect: A configuration baseline is a group of configuration items, software updates, and other configuration baselines.

    C. Incorrect: A configuration baseline is a group of configuration items, software updates, and other configuration baselines.

    D. Correct: A configuration baseline is a group of configuration items, software updates, and other configuration baselines.

2. Correct answers: A and D

    A. Correct: You need to select the collection to which the configuration baseline will be deployed when deploying a baseline.

    B. Incorrect: Although you can specify a schedule, you can use the default schedule, so Select The Compliance Evaluation Schedule For This Configuration Baseline is not mandatory.

    C. Incorrect: You don't need to generate alerts to accomplish this goal.

    D. Correct: You select Remediate Noncompliant Rules When Supported to remediate noncompliant rules when possible.

3. Correct answers: B and D

    A. Incorrect: You select Remediate Noncompliant Rules When Supported to remediate noncompliant rules when possible.

    B. Correct: You need to configure Generate An Alert When Compliance Is Below The Specified Percentage After The Specified Date And Time to accomplish your goal.

    C. Incorrect: Although you can specify a schedule, you can use the default schedule, so Select The Compliance Evaluation Schedule For This Configuration Baseline is not mandatory.

    D. Correct: You need to select the collection to which the configuration baseline will be deployed when deploying a baseline.

4. Correct answer: B

    A. Incorrect: The file will be present on computers that are compliant.

    B. Correct: Computers that are noncompliant do not have the file and will form the basis of the new collection.

    C. Incorrect: The Error state doesn't allow you to determine whether the file is present and should not be used as the basis for the new collection.

    D. Incorrect: The Unknown state doesn't allow you to determine whether the file is present and should not be used as the basis for the new collection.

Objective 4.3

Thought experiment

1. You should configure The Same Type Malware Is Repeatedly Detected Within The Specified Interval On A Computer.

2. You should configure The Same Type Malware Is Detected On A Number Of Computers.

Objective review

1. **Correct answers:** B, C, and D

   A. **Incorrect:** You can't configure the Endpoint Protection client to retrieve antimalware definition updates from an FTP site.

   B. **Correct:** Antimalware definition update files for the Endpoint Protection client can be retrieved from Microsoft Update/Microsoft Malware Protection Center.

   C. **Correct:** Antimalware definition update files for the Endpoint Protection client can be hosted on a UNC file share.

   D. **Correct:** Antimalware definition update files for the Endpoint Protection client can be hosted through WSUS.

2. **Correct answer:** A

   A. **Correct:** You deploy the Endpoint Protection Point Site System role at the top of the Configuration Manager hierarchy.

   B. **Incorrect:** You deploy the Endpoint Protection Point Site System role at the top of the Configuration Manager hierarchy.

   C. **Incorrect:** You deploy the Endpoint Protection Point Site System role at the top of the Configuration Manager hierarchy.

   D. **Incorrect:** You deploy the Endpoint Protection Point Site System role at the top of the Configuration Manager hierarchy.

3. **Correct answer:** C

   A. **Incorrect:** Advanced settings enable you to configure options such as whether to create a system restore point before cleaning computers, show notification messages to users, delete quarantined files after a specified number of days, and allow users to control exclusions.

   B. **Incorrect:** Use real-time protection settings to enable real-time protection. If you enable real-time protection, additional options are available to specify whether to scan incoming files, outgoing files, or both. You also can specify whether users can configure real-time protection settings on their computers.

   C. **Correct:** Exclusion settings enable you to specify files, locations, file types, and processes to exclude from the scanning process.

   D. **Incorrect:** Threat overrides settings enable you to configure a specific action (Allow, Remove, or Quarantine) based on a threat name.

4. **Correct answer:** C

   A. **Incorrect:** Use real-time protection settings to enable real-time protection. If you enable

real-time protection, additional options are available to specify whether to scan incoming files, outgoing files, or both. You also can specify whether users can configure real-time protection settings on their computers.

B. Incorrect: Exclusion settings enable you to specify files, locations, file types, and processes to exclude from the scanning process.

C. Correct: Advanced settings enable you to configure options such as whether to create a system restore point before cleaning computers, show notification messages to users, delete quarantined files after a specified number of days, and allow users to control exclusions.

D. Incorrect: Threat overrides settings enable you to configure a specific action (Allow, Remove, or Quarantine) based on a threat name.

Chapter 5. Manage Configuration Manager clients

The Configuration Manager client is software that you deploy to devices that you intend to manage using System Center 2012 R2 Configuration Manager. The client performs tasks locally, based on the instructions received from Configuration Manager. Collections enable you to group devices or users for performing tasks by using Configuration Manager.

Objectives in this chapter:
- [Objective 5.1: Deploy and manage the client agent](#).
- [Objective 5.2: Manage collections](#).
- [Objective 5.3: Configure and monitor client status](#).

Objective 5.1: Deploy and manage the client agent

This objective deals with how to deploy the Configuration Manager client. It covers the properties of the client itself, the site systems that need to be present within the Configuration Manager hierarchy to support client deployment, the process of installing the client, and the management of client settings.

This section covers the following topics:
- The Configuration Manager client
- Site systems used in client deployment
- Client installation
- Client assignment
- Client settings

The Configuration Manager client

You deploy the Configuration Manager client to devices to perform tasks on behalf of the Configuration Manager server. The Configuration Manager client consists of multiple elements that run in the background. These elements perform tasks based on the site configuration and policy.

On computers running Windows operating systems, the user interface (UI) for the Configuration Manager client consists of two parts: the Configuration Manager control panel and Software Center. If you managed previous versions of Configuration Manager, you are likely familiar with the Configuration Manager control panel. You access it through Control Panel on supported computers running Windows operating systems. You configure and manage the Configuration Manager client software for computers running Mac OS X, Linux, and UNIX operating systems through the command-line interface.

Unlike the Configuration Manager control panel, which is generally used by users with Administrative privileges, Software Center is designed for use by end users. Software Center, shown in [Figure 5-1](#), provides end users with the ability to interact with the app distribution process.
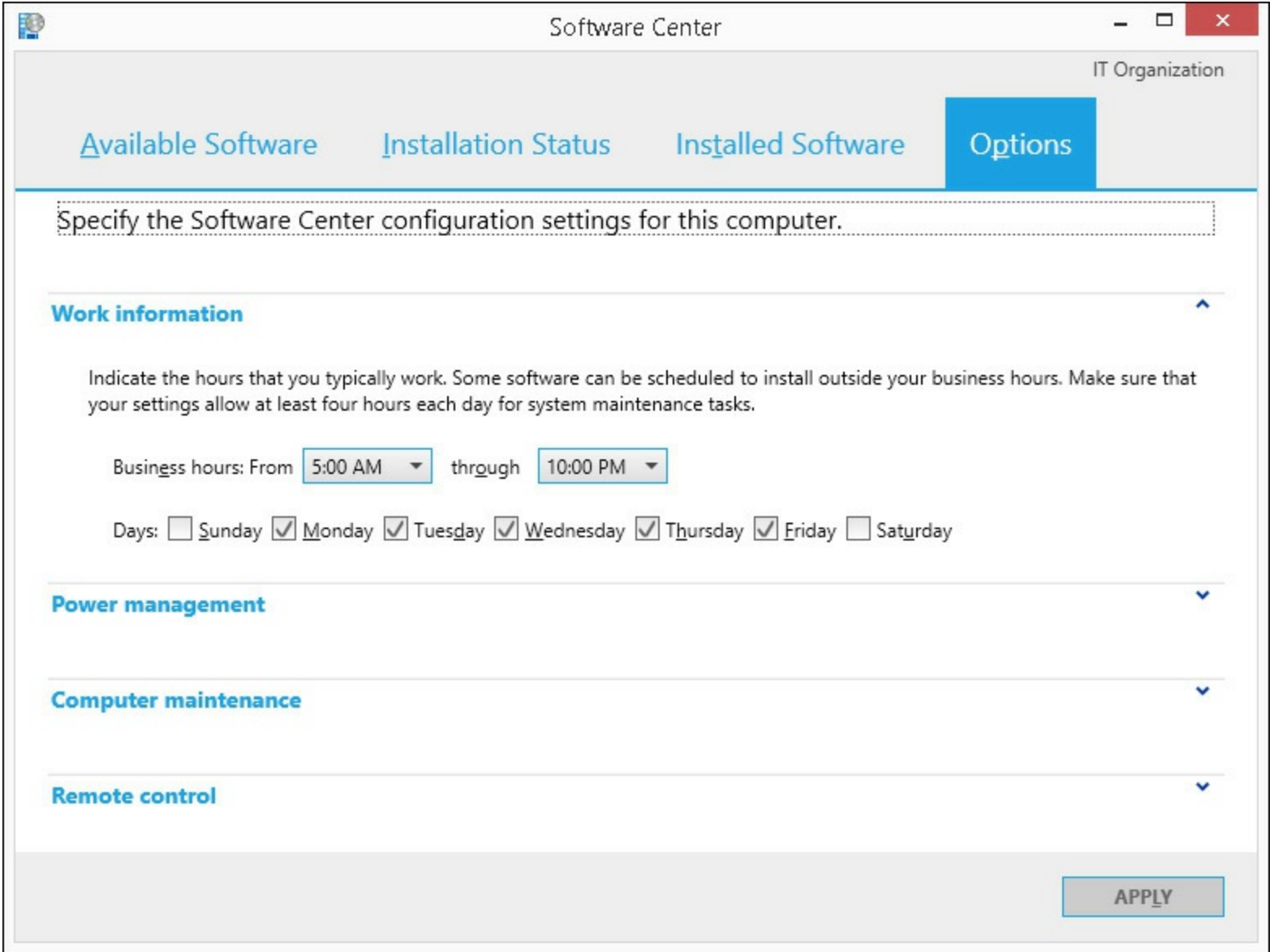
FIGURE 5-1 Software Center Options dialog box

The tabs of the Configuration Manager Properties dialog box are as follows:

- **General** This tab, shown in , enables you to view identifying information about the client. This includes the build number, the assigned site, the type of certificate, and the management point the client is using.
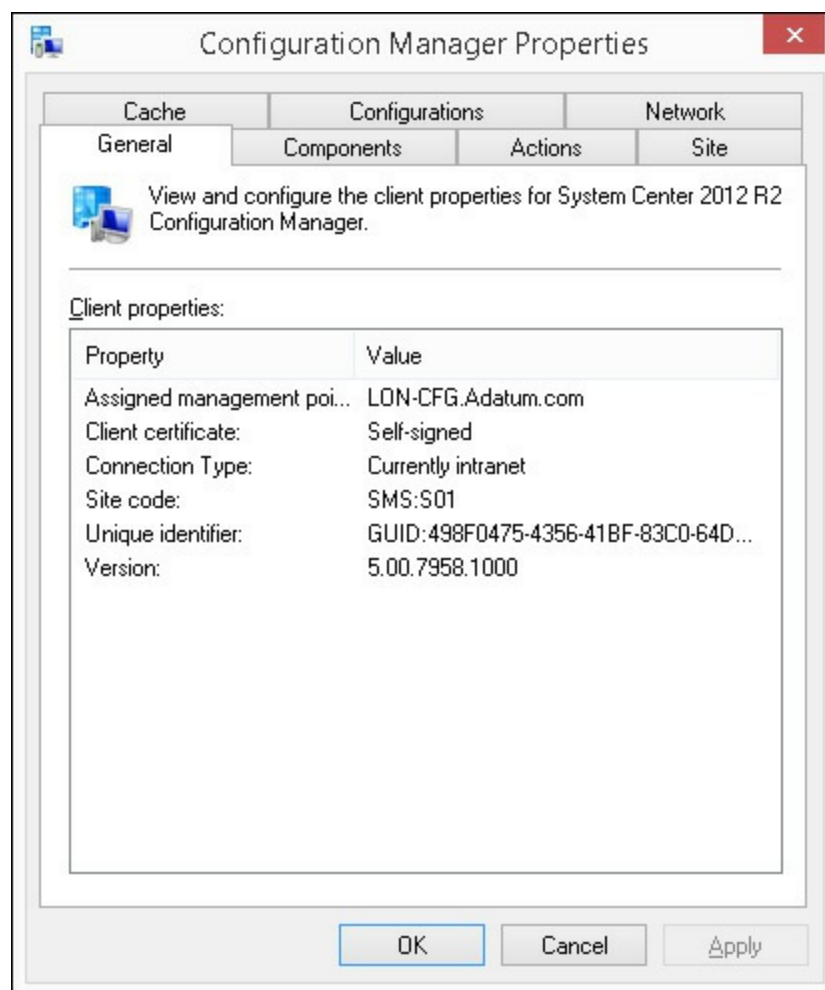
FIGURE 5-2 Configuration Manager Properties General tab

■ **Components** This tab enables you to view information about the installed components and agents. When you install the client, this installs all client components and agents, even if you disable them at the site. On this tab, you can view versions of the individual components and whether they are enabled or disabled. This tab is shown in Figure 5-3.

FIGURE 5-3 Configuration Manager Properties Components tab

■ **Actions** This tab enables you to initiate client actions when you do not want to wait until the scheduled time. Client actions include starting a hardware or software inventory cycle, retrieving user or machine policy updates, and similar actions. Figure 5-4 shows this tab.
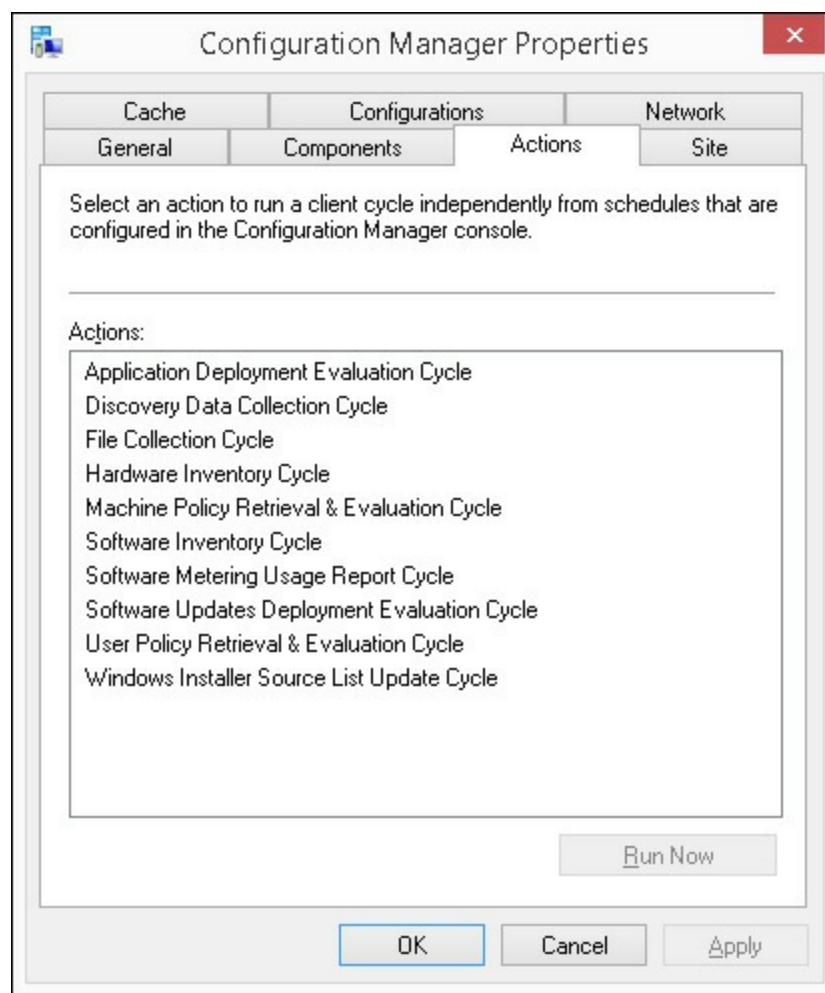
FIGURE 5-4 Configuration Manager Properties Actions tab

- **Site** This tab enables you to assign a client to a site either automatically or manually. Changes to this tab require local administrator rights.
- **Cache** Use this tab to configure the client cache settings. On this tab, you can change the cache location from the default location of %systemroot%\Ccmcache to a different location, or you can delete files from the cache. You also can change the cache's size. Changes to this tab require local administrator rights.
- **Configurations** This tab enables you to view the configuration baselines assigned to this client. You also can run an evaluation and view a local report of the client's compliance. Access to local compliance reports from this tab requires local administrator rights.
- **Network** This tab enables you to configure settings for Internet-based management. Changes to this tab require local administrator rights.

Users can set the following preferences for software delivery or remote control by using Software Center:

- Specify their work information, which includes business hours and days. Users must set aside at least four hours a day for Configuration Manager maintenance tasks.
- Exclude their system from the Configuration Manager Power Management feature if the Configuration Manager policy permits this.
- Specify how software maintenance occurs. Users can specify that their systems install software after business hours or the suspension of Software Center activities while in presentation mode.
- Override remote control settings for their computers if Configuration Manager policy permits

it. Users can specify settings such as the level of remote access and whether permission is required to start a remote control session.

More Info: **Client Settings**

You can learn more about client settings at *http://technet.microsoft.com/en-us/library/gg682067.aspx.*

Workgroup-based clients

You can use Configuration Manager to manage computers that are not part of a domain. These computers, referred to as workgroup-based computers, must meet the following prerequisites:

- You must install the Configuration Manager client software manually on each workgroup-based computer by using an account with local administrator privileges.
- You must configure a network access account to allow access to resources in the site server domain for clients that are not domain members.

There also are features that Configuration Manager does not support for workgroup-based computers, including:

- Using client push installation.
- Targeting users for application deployment.
- Performing global roaming.
- Using Active Directory Domain Services (AD DS) to locate site system servers.
- Using Active Directory discovery.

An alternative to managing nondomain client computers by using Configuration Manager is to manage them by using Microsoft Intune. In this scenario, ensure that you deploy the nondomain-joined client on a network with connectivity to the Internet.

Internet-based clients

You can use Configuration Manager to manage clients on internal networks and clients on external networks with Internet connectivity. Clients on external networks that have Internet connectivity are referred to as Internet-based clients. Configuration Manager uses HTTPS to communicate securely with these clients. To configure a client for Internet-based client management, you must obtain a computer certificate from a trusted certification authority (CA). You must also configure the client with the Internet fully qualified domain name (FQDN) of the management point. After you configure the client, you can manage it as long as the client retains connectivity to the Internet-facing site systems for its assigned Configuration Manager site.

To support HTTPS, you need to deploy a certificate from a trusted CA on the Configuration Manager site systems with which clients communicate. This can be from an internal CA that the client is configured to trust or from an external trusted CA. When using an internal enterprise CA, you can use only version 2 templates because Configuration Manager does not support certificates issued from version 3 and version 4 templates.

Internet-based clients do not support all Configuration Manager features. Specifically, Configuration Manager does not support the following client features on the Internet:

- Client deployment over the Internet, such as client push and software update–based client deployment. Use manual client installation instead.
- Auto-site assignment.
- Network Access Protection (NAP).
- Wake On LAN (WOL).
- Operating system deployment. However, you can deploy task sequences that do not deploy an operating system, such as task sequences that run scripts and maintenance tasks on clients.
- Remote control.
- Out-of-band management, which enables you to manage the computer before the operating system is active.
- Software deployment to users unless the Internet-based management point can authenticate the user in AD DS by using Windows authentication (Kerberos authentication or Windows NT LAN Manager). This is possible when the Internet-based management point trusts the forest in which the user account resides.

An alternative to Internet-based client management is to use DirectAccess, a feature supported for clients running the Enterprise editions of Windows 7, Windows 8, and Windows 8.1 operating systems. DirectAccess enables clients on the Internet to access internal network resources through an always-on, computer-authenticated virtual private network (VPN). DirectAccess has prerequisites, including a requirement that the computers be domain joined and that you deploy a DirectAccess server. A further alternative is to manage Internet-based clients by using Intune.

> *More Info:* **Internet-Based Client Management**
>
> **You can learn more about Internet-based client management at** *http://blogs.technet.com/b/configurationmgr/archive/2013/12/11/a-closer-look-at-internet-based-client-management-in-configmgr-2012.aspx*.

Mac OS X computers

System Center 2012 Configuration Manager Service Pack 1 (SP1) introduced support for Mac OS X computers. Configuration Manager supports the following versions of the Mac operating systems:

- Mac OS X 10.6 (Snow Leopard)
- Mac OS X 10.7 (Lion)
- Mac OS X 10.8 (Mountain Lion)
- Mac OS X 10.9 (System Center R2 Configuration Manager only)

Mac OS X computers are limited to the following Configuration Manager features:

- **Hardware inventory** You can use the hardware inventory data collected from Mac OS X computers in the same way as data collected from Windows-based computers; that is, you can use it to create collections, reports, and queries. You also can use the Configuration Manager console feature Resource Explorer to view hardware inventory data for Mac OS X computers.
- **Software deployment** You can use Configuration Manager to deploy software that is packaged in the following formats to Mac OS X computers:

- Mac OS Installer Package (.pkg)
- Mac OS X Application (.app)
- Apple Disk Image (.dmg)
- Meta Package File (.mpkg)
- **Compliance settings** Configuration Manager supports the use of Mac OS X Preference settings (.plist files) to enforce the configuration of different elements on Mac OS X computers, or shell scripts to monitor and remediate settings.

Configuration Manager client software installation and management for Mac OS X computers requires the use of public key infrastructure (PKI) certificates. The Configuration Manager client software for Mac OS X computers always performs certificate revocation checking, and you cannot disable this functionality. If a Mac OS X computer is unable to perform the check, it will not connect to the Configuration Manager site systems.

Mac OS X computers communicate with Configuration Manager site systems as if they were Internet-based clients. This means that all communication happens by using HTTPS. You must configure management points and distribution points to support Mac OS X computers.

To configure a management point and a distribution point to support Mac OS X computers, perform the following procedure:

1. In the Configuration Manager console, click Administration.

2. In the Administration workspace, expand Site Configuration and then click Servers And Site System Roles.

3. Select the computer that has the management point role assigned. In the details pane, right-click Management Point and then click Properties.

4. In the Management Point Properties dialog box, under Client connections, click HTTPS.

5. Select the Allow Mobile Devices And Mac Computers To Use This Management Point check box and then click OK.

6. Select the computer that has the distribution point role assigned. In the details pane, right-click Distribution Point and then click Properties.

7. In the Distribution Point Properties dialog box, under Specify How Client Computers Communicate With This Distribution Point, select HTTPS.

8. Under Create A Self-Signed Certificate Or Import A PKI Client Certificate, select Import Certificate and then click Browse.

9. Browse to the web server certificate that was created previously for the distribution point and then click OK.

More Info: **Managing Mac OS X**

You can learn more about managing Mac OS X with Configuration Manager at http://blogs.technet.com/b/pauljones/archive/2013/06/02/managing-mac-os-x-with-system-center-2012-configuration-manager.aspx**.**

Linux and UNIX computers

System Center 2012 Configuration Manager SP1 introduced support for computers running the Linux or UNIX computer system. The following versions of Linux and UNIX are supported:

- Oracle Linux 5 and 6
- Red Hat Enterprise Linux 4, 5, and 6
- Solaris 9, 10, and 11
- SUSE Linux Enterprise Server 9, 10, and 11
- Debian 5 and 6
- CentOS-5.0 and CentOS 6
- Ubuntu 12.4 LTS and 10.4 LTS
- IBM AIX 5.3, 6.1, and 7.1
- HP-UX 11i v2 and 11i v3

Configuration Manager supports the following features on Linux-based and UNIX-based computers:

- **Hardware inventory** You can use hardware inventory data collected from Linux and UNIX computers in the same way as data collected from Windows-based computers; that is, you can use it to create collections, reports, and queries. You also can use Resource Explorer to view hardware inventory data for Linux-based and UNIX-based computers.
- **Software deployment** You can use Configuration Manager to deploy software to Linux-based and UNIX-based computers by using packages and programs. Using Configuration Manager for deploying software on Linux-based and UNIX-based computers does not support any kind of user interaction.

Linux-based and UNIX-based computers are also workgroup-based clients and, therefore, have the same prerequisites and limitations of workgroup-based computers. Furthermore, the Configuration Manager client software for Linux and UNIX does not support Server Message Block (SMB) communication, forcing all communication with distribution points to happen over HTTP or HTTPS.

To configure a distribution point to support Linux-based and UNIX-based computers, perform the following steps:

1. In the Configuration Manager console, click Administration.
2. In the Administration workspace, expand Site Configuration and then click Servers And Site System Roles.
3. Select the computer that has the distribution point role assigned. In the details pane, right-click Distribution Point and then click Properties.
4. In the Distribution Point Properties dialog box, under Specify How Client Computers Communicate With This Distribution Point, select either HTTP or HTTPS.
5. If you selected HTTPS in step 4, under Create A Self-Signed Certificate Or Import A PKI Client Certificate, select Import Certificate, click Browse, find a web server certificate that you created previously for the distribution point, and then click OK.

Client installation

To deploy the components of the Configuration Manager client software efficiently to potential resources, you need to decide which deployment method to use. Consider the benefits of each installation method and decide which method suits your environment best. The client deployment methods are as follows:

- **Client push installation** This method pushes the software for the Configuration Manager client software to client computers. You can automate this deployment method so that client installation occurs on systems assigned to the site, or you can manually initiate a client push installation to any discovered system supported for client installation.

- **Group Policy installation** This method uses Group Policy to publish or assign the Configuration Manager client software to computers when the Group Policy Object (GPO) updates on the computer.

- **Software update point installation** Use this method to install the Configuration Manager client software installation program (CCMSetup.exe) as a software update to a software update point. This is useful if Windows Server Update Services (WSUS) is in use in the environment, particularly if you have Windows Firewall enabled and not configured to support other installation methods.

- **Manual installation** In this method, you manually initiate the Configuration Manager client software installation on computers by using CCMSetup.exe. If AD DS contains published information from Configuration Manager, and if you run CCMSetup.exe without any command-line parameters, the client installation process will retrieve the published client installation parameters from AD DS.

- **Logon script installation** This method uses CCMSetup.exe in a logon script to trigger the client installation. This method ensures that the Configuration Manager client software is installed on all computers to which the user has local administrator permissions and that are members of the domain in which the policy that applies the logon script is configured.

- **Upgrade installation (software deployment)** Use this method to upgrade existing client software on computers to newer Configuration Manager versions.

- **Operating system deployment** When using operating system deployment to deploy a new operating system or to upgrade an existing one, you can include the Configuration Manager client software as part of the operating system deployment process.

- **Computer imaging** Use this method to preinstall the Configuration Manager client software on a master image computer that will be used to build your enterprise's computers.

Depending on the client installation method you use, the complexity of configuration can vary significantly. However, all the installation methods use the same files and complete the installation in

essentially the same way. The installation process for the Configuration Manager client software for Windows-based clients uses the following files:

- CCMSetup.exe
- Client.msi
- CCMSetup.msi

CCMSetup.exe

CCMSetup.exe generally begins the client installation process and runs in all client installation methods. CCMSetup performs the following actions:

- Determines the location from which to download client prerequisites and installation files. If you start CCMSetup without command-line options, and if you have extended the AD DS schema for Configuration Manager, the setup process reads the client installation properties from AD DS to find an appropriate management point. If you have not extended the Active Directory schema, CCMSetup searches Domain Name System (DNS) or Windows Internet Naming Service (WINS) for a management point to contact. Alternatively, you can specify a management point by providing the /mp:<*ComputerName*> switch or a specific Universal Naming Convention (UNC) location by using the /source:<*path*> switch.
- Downloads and installs client prerequisite files. Files include the client.msi file and all prerequisite software necessary for install.

CCMSetup copies all the files it needs to the %systemroot%\CCMSetup\Logs folder and creates the Ccmsetup.log file in the same location. Numerous switches are available for modifying the behavior of CCMSetup.exe.

Client.msi

After CCMSetup.exe installs the required prerequisites on the intended client, CCMSetup invokes Client.msi by using MSIExec, a Windows Installer file. MSIExec then installs the client on the system. Client.msi creates the client.msi.log file in the %systemroot%\CCMSetup folder.

You can modify the Client.msi installation behavior by providing specific properties on the CCMSetup.exe command line. Alternatively, you can specify the properties on the Installation Properties tab of the Client Push Installation Properties dialog box. These settings publish to AD DS, and several installation methods use them.

CCMSetup.msi

You also can use GPOs to deploy the Configuration Manager client software. GPOs use the CCMSetup.msi file to initiate the installation process. This file is located in the <*installation directory*>\bin\i386 folder on the Configuration Manager site server.

> *More Info:* **Client Installation Options**
>
> **You can learn more about Configuration Manager client installation options at** *http://technet.microsoft.com/en-us/library/gg699356.aspx*.

Deploying to Mac OS X computers

Because Configuration Manager treats computers running the Mac OS X operating system as Internet-based computers, all communication with the management point and distribution point must happen by using HTTPS. Before deploying the client, you must configure the Configuration Manager environment to support the Mac OS X computers. To ensure that your environment supports Mac OS X computers, perform the following procedure:

1. Deploy certificates and configure the client certificate template for Mac OS X computers:

   A. Deploy a web server certificate to the computers that will run the following site system roles:
      - Management Point
      - Distribution Point
      - Enrollment Point
      - Enrollment Proxy Point

   B. Deploy a client authentication certificate to the computers running the following site system roles:
      - Management Point
      - Distribution Point

   C. Configure the client certificate template in the CA to allow Read And Enroll permission to the account that will be used to enroll the certificate on the Mac OS X computers.

2. Configure the following Configuration Manager site system roles that Mac OS X computers use:

   A. Management Point. Configure the following settings:
      - HTTPS Communication
      - Allow Client Connections From The Internet
      - Allow Mobile Devices And Mac Computers To Use The Management Point

   B. Distribution Point. Configure the following settings:
      - HTTPS Communication
      - Allow Client Connections From The Internet

   C. Install an enrollment point and an enrollment proxy point.

3. Configure Default Client Settings to support Mac OS X computers:

   A. Set Allow Users To Enroll Mobile Devices And Mac Computers to Yes.

   B. Create a new profile to assign clients to a Configuration Manager site by using a CA and the certification template that you changed in step 1.

After you configure the environment correctly to support Mac OS X computers, you can download and install the Configuration Manager client software on existing Mac OS X computers. To install the client on Mac OS X computers, perform the following procedure:

1. Download and extract the client source files for Mac OS X clients. You do this by downloading the ConfigmgrMacClient.msi file from the Microsoft Download Center to a Windows-based computer and then running the ConfigmgrMacClient.msi file to extract the Mac

client package, named Macclient.dmg. Copy the Macclient.dmg file to the Mac OS X computer on which you want to install the client and run the file to extract its contents to a local disk.

2. Install the client on the Mac OS X computer and enroll it as a client. You do this by running the following commands:

```
sudo ./ccmsetup

sudo ./CMEnroll –s <enrollment_proxy_server_name> -ignorecertchainvalidation -u
<'username'>
```

3. Restart the Mac OS X computer.

In organizations that use System Center 2012 R2 Configuration Manager only, the Enrollment Wizard starts after you install the client on the computer running Mac OS X. It enables you to enroll the computer by specifying domain credentials and the name of the enrollment proxy point server.

> *More Info:* **Install Mac OS X Client**
>
> **You can learn more about installing the Mac OS X client at** http://technet.microsoft.com/en-us/library/jj591553.aspx**.**

Deploying to Linux-based and UNIX-based computers

Cumulative update 1 for System Center 2012 Configuration Manager SP1 and later provides a universal installer that you can use to deploy the Configuration Manager client to any supported version of Linux or UNIX. Prior to the cumulative update 1 for System Center 2012 Configuration Manager SP1, each Linux or UNIX version had its own install package that had to be downloaded and installed on the client computer to make it a Configuration Manager client.

To install the client by using the universal installer, perform the following procedure:

1. Copy the install script and the client installation (.tar) file to the Linux-based or UNIX-based computer. The name of the .tar file will be Ccm-universal-x86.<*build*>.tar or ccm-universal-x64.<*build*>.tar, where x86 is for use on 32-bit clients, x64 is for use on 64-bits, and build represents the build number for the installer.

2. On the Linux-based or UNIX-based computer, run the following command:

```
./install –mp <FQDN of management point> -sitecode <site_code> ccm-universal-<x86
or x64>.<build>.tar
```

3. Review the contents of Scxcm.log in the /V/Opt/Microsoft folder to confirm that the installation occurred.

> *More Info:* **Installing the Client on Linux and UNIX Computers**
>
> **You can learn more about installing the client on Linux and UNIX computers at** http://technet.microsoft.com/en-us/library/jj573939.aspx**.**

Extending the schema

Although it is not mandatory, extending the AD DS schema and publishing Configuration Manager information in AD DS helps simplify the client deployment process and site management. When you extend the AD DS schema and publish Configuration Manager information in AD DS, this simplifies the client installation process by storing Configuration Manager– related information in Active Directory, which enables clients to retrieve the data during installation. You can use AD DS publishing with any installation method on domain-joined Windows clients to enable automatic site assignment. AD DS publishing also enables you to provide the client with the name of the management point with which to communicate, in addition to other information.

Configuration Manager publishes the following client installation properties to AD DS:

- The default management point used to download content for the client installation.
- The Configuration Manager site code.
- The HTTP port used for client communication.
- The HTTPS port used for client communication.
- A setting indicating that the client must communicate using HTTPS.
- The fallback status point. If the site has multiple fallback status points, the first to be installed is the only one published to AD DS.
- The selection criteria for certificate selection. This might be required when the client has more than one valid certificate.Installation properties specified on the Installation Properties tab of the Client Push Installation Properties dialog box.
- Automatic updates when alterations are made to default ports for site systems.

Only a member of the Schema Admins group, or an enterprise administrator who has sufficient permissions to modify the schema, can extend it. If you extend the schema prior to installation, Configuration Manager configures the site automatically to publish site information during installation. At the end of the installation, the Configuration Manager site server publishes site information to AD DS. However, you can extend the schema after installing Configuration Manager and configure the site manually to publish to AD DS.

You can extend the Active Directory schema by using either of the following methods:

- The LDIFDE command-line tool (Ldifde.exe) and the ConfigMgr_ad_schema.ldf file. You must modify the ConfigMgr_ad_schema.ldf file to include the name of the Active Directory forest prior to modifying the schema.
- The ExtADSch.exe tool. ExtADsch.exe creates a log file in the root of the system drive called Extadsch.log.

You can find both the executable files in either the \SMSSETUP\BIN\i386 folder or the \SMSSETUP\BIN\x64 folder on the installation media. ExtADSch.exe is a standalone executable file; however, the ConfigMgr_ad_schema.ldf file requires you to run the following command to use it.

[Click here to view code image](#)

```
ldifde -i -f ConfigMgr_ad_schema.ldf -v -j <location to store log file>
```

Site systems used in client deployment

The process of installing the Configuration Manager client software uses several site systems. In addition to the site systems that play a direct role in client deployment, several site systems might participate in client deployment.

The following site system roles are involved directly with installing client devices:

- Management point
- Fallback status point
- Software update point
- Enrollment point and enrollment proxy point
- Distribution point
- Reporting services point

Management point

A management point is usually required to complete the client installation process because the client might need to contact a distribution point to download necessary prerequisite software. The installation process is complete when the client has registered with a primary site, receives its initial policy assignment, and then retrieves the policy. This initial policy sets the components to their desired state. In most installation methods, the client downloads CCMSetup.exe and Client.msi files from a management point and any other prerequisites from a distribution point. After the installation program is complete, the client contacts the management point to register itself and obtains its site assignment. It then reports the state of the installation. If the client cannot contact the management point, all the client components will show as Installed instead of Enabled or Disabled.

The client software follows several methods to locate the management point and uses the methods in the following order:

1. **Setup parameters** As part of the installation command, you can specify a management point.
2. **AD DS** The client software will query AD DS for an appropriate management point.
3. **Domain Name System (DNS)** The client will search for a service (SRV) resource record type for a management point. To find the right SRV record in DNS, you must configure clients with their site code.
4. **Windows Internet Naming Service (WINS)** A management point will update its WINS record with appropriate information automatically. If a client is a WINS client, WINS is the last resource the client software uses to locate a management point.

Automatic client assignment is determined using boundaries that are members of a boundary group, where that boundary group has automatic assignment enabled. In previous versions of Configuration Manager, automatic site assignment would fail, and Configuration Manager would not manage clients if they fell outside all boundaries. With System Center 2012 Configuration Manager, you can

configure a fallback site for client assignment at the hierarchy level. If you install a client that is outside any of the configured boundary groups, the automatic site assignment process will use this site, and the installation process will complete successfully.

Fallback status point

The fallback status point is an optional site system that you can use during the client installation process. A fallback status point monitors client deployment and identifies unmanaged clients because unmanaged clients cannot communicate with a management point. The fall-back status point relies on unauthenticated connections from clients over HTTP. You should use a dedicated system for the fallback status point so that if a site system is not available, the client can contact the fallback status point to report the error. You cannot configure the fallback status point as a highly available role.

The reports that the Configuration Manager client software produces use data sent by clients through the fallback status point. Mobile devices that are enrolled by Configuration Manager and mobile devices that are managed by using the Exchange Server connector do not use a fallback status point.

Software update point

You can install the Configuration Manager client software by using software update point push installations. If you choose to use this method, configure the software update point on a WSUS server to install the client when computers scan for applicable software updates.

Enrollment point and enrollment proxy point

Mobile devices use the enrollment point for enrollment with Configuration Manager, and the enrollment proxy point manages the enrollment requests from the mobile devices. These site system roles are not required if you plan to manage mobile devices by using only the Exchange connector.

Distribution point

Most client installation methods copy the necessary installation files from a management point. In certain circumstances, the installation process uses a distribution point instead. When you deploy an operating system by using the Configuration Manager Operating System Deployment feature, the task sequence action that installs the client software downloads the operating system from a distribution point. If you use Pre-Boot Execution Environment (PXE) boot in conjunction with operating system deployment, Configuration Manager installs the Windows Deployment Services PXE server on the distribution point.

Reporting services point

In addition to the required and optional roles that client installation uses directly, you might find it useful to install a reporting services point. This will enable you to view any reports about the client installation process or the status of the clients.

More Info: **Site System Roles Used For Client Deployment**

You can learn more about site system roles used for client deployment at
http://technet.microsoft.com/en-au/library/gg681976.aspx.

Client assignment

You cannot manage a client until it is assigned to a site. After client installation is complete, the client is assigned automatically to a site so that the client can be managed. You can assign client devices to any primary site; however, you cannot assign client devices either to a secondary site or to a central administration site.

Most clients will reside within site-assignment boundary groups and will be assigned automatically to a site based on the boundary definition. You can configure a fallback site for clients that might be outside the configured boundaries of any site. You also can assign a client to a site through a client.msi property either directly or through the Installation Properties tab of the Client Push Installation Properties dialog box.

If you have not extended AD DS, you have two options for site assignment. You can specify a site code by using the Client.msi property SMSSITECODE=site code, or you can assign a group of clients to a site manually by using Group Policy. You also can choose to install a client offline instead of installing it immediately to a site.

If the client automatic assignment fails, the client software remains installed, but Configuration Manager will not manage it until you assign the client to a site. If the client is unassigned, it will attempt to perform automatic assignment each time the CCMExec process starts.

After the client is assigned to a site, it remains assigned to that site even if the client changes its IP address and roams to another site. A client can move to another site only when an administrator reassigns it manually.

> *More Info:* **Client Site Assignment**
>
> **You can learn more about client site assignment at *http://technet.microsoft.com/en-us/library/gg682060.aspx*.**

Client settings

You can configure client software in the Administration workspace in the Client Settings node of the Configuration Manager console. You configure the Default Client Settings object with settings that will apply to all clients. The Default Client Settings object always has a priority of 10,000, and you cannot change this setting. Therefore, the Default Client Settings object is applied first, and custom settings will override the default settings when you assign them to collections. You can configure custom settings for any of the categories or a combination of categories found in the Default Client Settings object.

Client settings are hierarchy-wide settings that, by default, affect all clients in the hierarchy. Because Configuration Manager considers these settings as global data, modifications that you make to Default Client Settings at one site replicate to all other primary sites in the hierarchy and to the central administration site.

Custom settings

In the Administration workspace, in the Client Settings node of the Configuration Manager console, you can create custom client settings. The Default Client Settings object applies to all clients, and if you want to configure a setting for all devices or users, you can modify the Default Client Settings option. However, if you need to change some settings for a specific collection of users or devices, you will need to create a custom setting.

Reasons for creating custom client settings include:

- Creating a custom client setting for a group of systems on which software metering should be disabled.
- Creating a custom client setting for a group of systems to increase or decrease the frequency of status messages.
- Creating a custom client setting for a group of servers to prevent them from configuring an affinity with a user automatically.

After creating a custom client setting object, deploy it to one or more collections to apply it. To deploy a custom client setting to a collection, right-click the custom client setting and then click Deploy. You can then choose the collections to which you want to deploy the custom client setting.

Note that you cannot configure certain settings through a custom client device policy. Table 5-1 lists the settings that you can configure only in the Default Client Settings object.

Policy	Setting
Compliance Settings	Schedule Compliance Evaluation
Hardware Inventory	The settings in this policy include: ■ Maximum Custom Management Information Format (MIF) File Size In Kilobytes (KB). ■ Collect MIF Files.
Mobile Devices	Polling Interval
Software Inventory	Configure The Display Names For Manufacturer Or Product

TABLE 5-1 Default client settings policy settings

Multiple client device settings

Assigning multiple client device settings to a collection enables you to create different client device-settings objects for separate Configuration Manager feature sets. For example, you might have a client device-settings object for software deployment and another client device-settings object for hardware inventory.

All client setting objects are assigned a priority level. Configuration Manager processes each setting object in order, with lower numerical values overriding higher numerical values. When you create a new custom client setting, it receives the next available priority. When you delete a custom client settings object, the priority on all client settings that have a higher priority reduces by one. For example, consider when you have four custom client settings: ClientSetting1, ClientSetting2, ClientSetting3, and ClientSetting4. ClientSetting1 was created first and has a priority of one. ClientSetting2 was created second and has a priority of two. ClientSetting3 has a priority of three,

and ClientSetting4 has a priority of four. If you delete ClientSetting2, ClientSetting1 will retain its priority of one, the priority of ClientSetting3 will be adjusted to two, and the priority of ClientSetting4 will be adjusted to three.

You can use the Configuration Manager console's Resultant Client Settings functionality to determine the resultant client settings when multiple client settings are applied. In the Assets And Compliance workspace, right-click the device, user, or user collection for which you want to see resultant client settings, click Client Settings, and then click Resultant Client Settings.

More Info: **Client Settings**

You can learn more about client settings at _http://technet.microsoft.com/en-au/library/gg682109.aspx_.

Exam Tip

Remember how settings are resolved when multiple client settings apply through collection membership.

Thought experiment: **Configuration Manager client deployment**

You are planning the deployment of the Configuration Manager client at Contoso. As part of the planning process, you need to determine how to handle computers that are not joined to the domain and computers that are running the Mac OS X operating system. With this information in mind, answer the following questions:

1. **What steps do you need to take to install the Configuration Manager client on nondomain-joined Windows-based computers?**

2. **Which site system roles require web server certificates when you use Configuration Manager to manage computers running Mac OS X?**

3. **Which site system roles require client authentication certificates when you use Configuration Manager to manage computers running Mac OS X?**

Objective summary

- On computers running Windows operating systems, the UI for the Configuration Manager client consists of two parts: the Configuration Manager control panel and Software Center.
- Users can set the preferences for software delivery or remote control by using Software Center.
- You must manually install the Configuration Manager client software on workgroup-based computers and configure a network access account to allow access to resources in the site server domain for clients that are not domain members.

- To configure a client for Internet-based client management, obtain a computer certificate from a trusted certification authority (CA). You must configure the client with the Internet fully qualified domain name (FQDN) of the management point.

- Extending the schema simplifies the client installation process by storing Configuration Manager–related information in Active Directory.

- You can assign client devices to any primary site but cannot assign client devices either to a secondary site or to a central administration site.

- The Default Client Settings object is applied first, and custom settings will override the default settings when you assign them to collections.

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. Of which domain security group must a user account be a member if it will be used to extend the schema with information about Configuration Manager?

   A. Domain Admins

   B. Schema Admins

   C. Enterprise Admins

   D. Protected Users

2. You are working with a Configuration Manager deployment in which the Active Directory schema has not been extended. Which of the following methods can you use to assign a site code to clients? (Choose two. Each correct answer provides a complete solution.)

   A. Use the Client.msi property SMSSITECODE=site code.

   B. Configure an answers.txt file.

   C. Configure Group Policy.

   D. Configure an unattend.xml file.

3. What is the priority of the Default Client Settings object?

   A. 1

   B. 100

   C. 1,000

   D. 10,000

4. Which of the following settings cannot be configured through a custom client device policy? (Choose three. Each correct answer provides a complete solution.)

   A. Software Inventory: Configure The Display Names For Manufacturer Or Product

   B. Compliance Settings: Schedule Compliance Evaluation

   C. Mobile Devices: Polling Interval

   D. Cloud Services: Allow Access To Cloud Distribution Point

Objective 5.2: Manage collections

You can use collections to manage and organize groups of computers, mobile devices, users, and security groups throughout your Configuration Manager environment. You also can use collections to help accomplish many Configuration Manager management tasks. In this section, you learn about the various types of collections, the methods to create collections, and the process of monitoring collections.

This section covers the following topics:

- Collections
- Collection rules
- Maintenance windows
- Power management
- Monitoring collections

Collections

Collections represent resource groups that consist of devices such as computers and mobile devices or users and user groups from all of the hierarchy's sites. You can use collections to accomplish several management and configuration tasks, including:

- Organizing resources into manageable units to create an organized and logical structure of resources.
- Organizing collections of target resources to perform Configuration Manager operations on multiple resources simultaneously. Configuration Manager operations can include operations such as application deployments and installation of software updates.
- Targeting groups of computers with specific configurations, such as:
  - Client settings.
  - Power-management settings.
  - Maintenance-window settings.
- Organizing computers based on their compliance status, with a specific baseline.
- Integrating with role-based administration to specify collections that a specific administrative user can access.

You can view or modify collections by using the User Collections and Device Collections nodes found in the Assets And Compliance workspace. User collections can contain Users and User Groups. Device collections can contain devices managed by Configuration Manager.

Configuration Manager includes seven predefined user and device collections as described in Table 5-2.

Collection	Location	Description
All User Groups	User Collections	This collection displays all security groups that the Active Directory Group Discovery method discovers.
All Users	User Collections	This collection displays all users that the Active Directory User Discovery method discovers.
All Users And User Groups	User Collections	This collection contains all users and user groups that the Active Directory User Discovery method discovers.
All Desktop And Server Clients	Device Collections	This collection displays all desktop computers and servers that are Configuration Manager clients and that have communicated with the site by using Heartbeat Discovery.
All Mobile Devices	Device Collections	This collection displays mobile devices that Configuration Manager manages and that satisfy one of the following conditions: ■ The mobile device is assigned to a site. ■ The Exchange Server connector has discovered the mobile device.
All Systems	Device Collections	This collection contains all systems and all unknown computers. This collection also displays devices that have been discovered by using Active Directory System Discovery, Network Discovery, and Heartbeat Discovery.
All Unknown Computers	Device Collections	This collection contains x64 and x86 placeholder entries for the unknown computer support features that Operating System Deployment uses.

TABLE 5-2 Predefined collections

> *More Info:* **Configuration Manager Collections**
>
> **You can learn more about Configuration Manager collections at**
> *http://technet.microsoft.com/en-us/library/gg682177.aspx*.

Collection rules

You can use rules to manage the membership of Configuration Manager collections. Table 5-3 describes the different rule types you can use to manage the membership of Configuration Manager collections.

Rule	Description
Direct rule	You can use a direct rule to add a specific resource to a collection. If you add a resource to a collection by using a direct rule, the resource will remain in the collection until manually removed. You can create or manage direct membership rules for a collection by using either of the following methods: ■ Use the Create Direct Membership Rule Wizard. This wizard opens when you select Direct Rule in the Create Device Collection Wizard or in the Create User Collection Wizard. ■ Add the selected items to an existing collection. You can select existing resources and add these resources to existing user collections by using the Users node and the Devices node located in the Assets And Compliance workspace. This creates a direct membership rule for the target collection that contains the selected resources.
Query rule	You can use a query rule to add members to a collection based on their attributes. For example, you can create a collection that contains devices that are within a specific Active Directory organizational unit (OU), or you can create a collection that contains devices on which a specific software version is installed. In both cases, collection membership is updated dynamically based on the query rule's results. You can configure collection membership to be reevaluated according to a schedule.
Include collections	You can use the include collections rule type to include the members of another collection in the membership evaluation for the current collection.
Exclude collections	You can use the exclude collections rule type to exclude the members of another collection in the membership evaluation for the current collection.

TABLE 5-3 Collection rule types

When you create a new collection, you specify a base collection called a limiting collection. The limiting collection becomes a foundation for resources that can be added to the new collection. You can use limiting collections along with role-based access control to ensure that delegated administrators can see only objects that are relevant for their administrative tasks.

Configuration Manager reevaluates all of a collection's rules on a specified schedule. You can also trigger on-demand reevaluation of collection membership. The default schedule to evaluate the membership of custom collections is once every seven days.

Configuration Manager supports incremental evaluation of members of a collection. This feature runs separately from the full update cycle, and it scans periodically for new resources or resources that have changed since the previous collection evaluation. If you enable incremental evaluation, incremental collection member evaluation runs every five minutes. Figure 5-5 shows enabling incremental updates during collection creation.
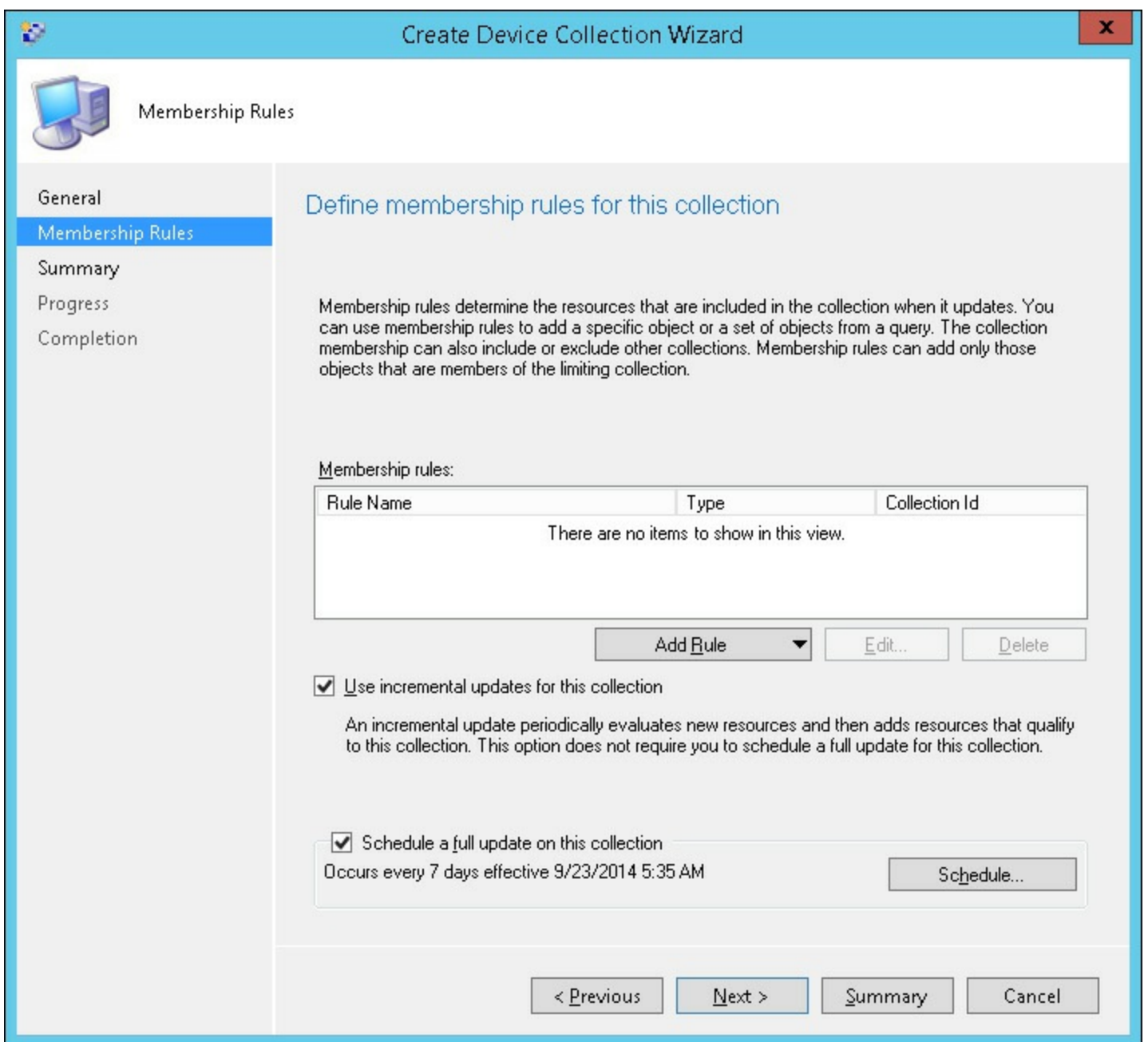
FIGURE 5-5 Membership Rules page of the Create Device Collection Wizard, showing options for incremental updates and scheduling full updates

Maintenance windows

Maintenance windows enable you to configure a specific period during which required deployments, software-update installations, configuration-item remediation, and task sequences can run on a client. Assigning a specific start time for a program deployment does not ensure that the program runs at that time. However, you can configure maintenance windows to ensure that the assigned program installations and the restarts that Configuration Manager triggers do not occur at inconvenient or undesirable times.

For example, you might configure a required application deployment that installs a large application and then restarts the computer. To avoid running this during normal business hours, you might configure the deployment to run at 2:00 A.M. on a specific day. However, an executive might have taken a portable computer on a business trip before you deployed the program. When the executive returns to the office after the scheduled start time, the portable computer would start to install the application a few minutes after the computer connects to the office network. This could

affect the system performance of the computer and, after installation, force a restart at the very time the executive wants to check an important email message or make a presentation. To avoid this scenario, configure an overnight maintenance window for a collection of which the executive's computer is a member. This ensures that the installation and restarts do not occur during normal business hours.

You can configure maintenance windows by opening the Properties dialog box of a specific collection and then selecting the Maintenance Windows tab as shown in .
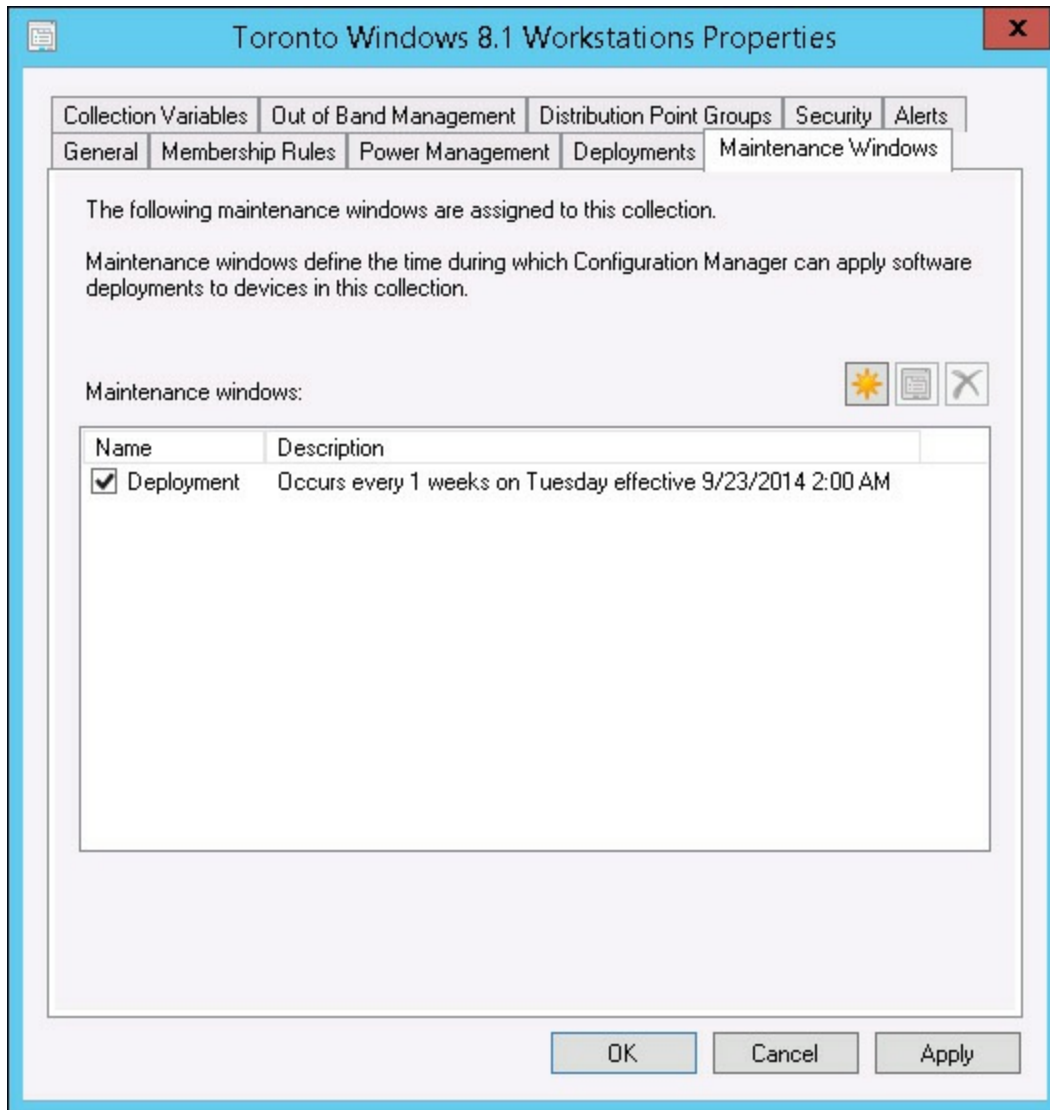
FIGURE 5-6 Maintenance Windows tab

Maintenance windows do not affect the following configuration management processes:

- Policy download and evaluation
- Data collection and reporting of inventory and metering data
- Remediation for Network Access Protection (NAP)
- Transmission of Wake On LAN wake-up packets
- Out-of-band management
- Application deployment content downloads
- Deployments, software-update deployments, configuration-item remediation, or task sequences that are optional or specifically configured to ignore maintenance windows
- User-initiated deployments

Changes to maintenance windows that occur during a maintenance window do not take effect while the current maintenance window is in effect.

A required deployment does not run during a maintenance window that is shorter or has less time remaining than the deployed software's configured maximum run time. For example, a deployment that has a run time of 45 minutes does not run if only 30 minutes remain in the maintenance window. In addition, if you configure the maximum run time of deployed software as unknown, the software might run past the end of a maintenance window.

A client computer can be a member of more than one collection with maintenance windows. When a client computer is a member of two or more collections with maintenance windows, that computer's maintenance windows will be a combination of the defined collections' maintenance windows.

For example, PC1 is a member of Collection A, Collection B, and Collection C. The maintenance windows for each of the collections are as follows:

- Collection A's maintenance window is from 5 P.M. to 8 P.M.
- Collection B's maintenance window is from 4 A.M. to 7 A.M.
- Collection C's maintenance window is from 7 P.M. to 11 P.M.

Therefore, PC1's maintenance windows will be from 4 A.M. to 7 A.M. and from 5 P.M. to 11 P.M. When using maintenance windows, consider the following best practices:

- When you use maintenance windows to restrict system changes, you should create collections specifically for this purpose instead of using the default collections or other custom collections.
- When you configure maintenance windows, include a description of the maintenance window in the collection's name for easy identification.

> *More Info:* **Maintenance Windows**
>
> **You can learn more about maintenance windows at http://technet.microsoft.com/en-us/library/hh508762.aspx.**

Power management

Use Configuration Manager to configure and monitor standard Windows power options throughout the managed environment. Configuration Manager power management enables you to apply a power plan to managed computers and monitor power consumption to minimize costs and provide environmental benefits for your organization.

Table 5-4 describes the external dependency for implementing power management by using Configuration Manager.

Dependency	Description
Client computer support for the intended power state	Client computers need to be able to support the following states: ■ Sleep ■ Hibernate ■ Wake from sleep ■ Wake from hibernate Clients with Windows 7 and later provide the best platform for power management. However, you can also use power management with Windows Vista. You can use the Power Management: Power Capabilities report to verify the hardware capabilities of computers in a specific collection.
Correct display adapter driver	Make sure that client computers are using the correct display adapter driver. If they are using the wrong display adapter driver, the sleep states might be disabled, and power-monitoring data might not be available.

TABLE 5-4 Power management dependencies

Table 5-5 lists the prerequisites for implementing power management by using Configuration Manager.

Dependency	Description
Configuration Manager client software	All client computers that you intend to manage with a power management policy must be Configuration Manager clients.
Hardware Inventory	To use power management, you must enable Hardware Inventory. Power management uses information that the hardware inventory process collects.
Power Management Client Settings	To use power management, you must enable Power Management Client Settings. You can configure this option in Default Client Settings to apply to the entire hierarchy, or you can create a custom client device setting to deploy to a specific collection. By default, Power Management Client Settings is enabled. You can also allow users to exclude their devices from power management. If you enable this option, users can then use Software Center to exclude their own computers from power management plans. This option is disabled by default.
Reporting services point	The power management reports require you to configure a reporting services point within the site.

TABLE 5-5 Power management prerequisites

To implement an enterprise-wide power management solution, you must:

1. Monitor the current power state and usage.

Your first step to effective power management is to collect data and analyze reports that outline current power settings and consumption. Power management uses hardware inventory to collect data. You can view the hardware inventory by using reports and graphs to determine optimal power management settings for your environment. During your monitoring stage, you can use a number of reports that provide information related to current power settings on computers in a collection; power management capabilities of a computer; and current computer, monitor, and user activity over a period of time. You can also use the reports to provide information related

to current power consumption for a specified collection over a period of time, current power consumption costs for a specified collection over a period of time, and computers not capable of power management.

2. Plan power management plans.

   After monitoring and collecting baseline data, you can use the gathered information to decide on the types of power management settings you want to deploy. It is important to determine specific settings that you want to enable or disable to meet your organizational requirements.

3. Apply power management policies.

   After carefully planning your power management settings, you can configure and apply the required plan settings to a specific collection. Depending on the settings required, you can specify default power plans, or you can create your own customized power plan.

4. Check compliance and reports.

   As the power management settings take effect, you can track ongoing power consumption and settings on all managed computers and troubleshoot any problems. Various reports provide details about power usage, costs, and environmental impact.

Power management plan settings

When you are ready to apply power management settings, you can choose to implement a default power plan or customize your own plan for both peak and nonpeak time intervals. Default power plans include:

- Balanced.
- High Performance.
- Power Saver.

Depending on the power plan that you use and the peak or nonpeak configuration, various power management settings might or might not be applied. You cannot modify default plans. However, if you choose to create a customized power plan, you can modify and apply your own settings to match specific requirements. Figure 5-7 shows the Balanced power plan.
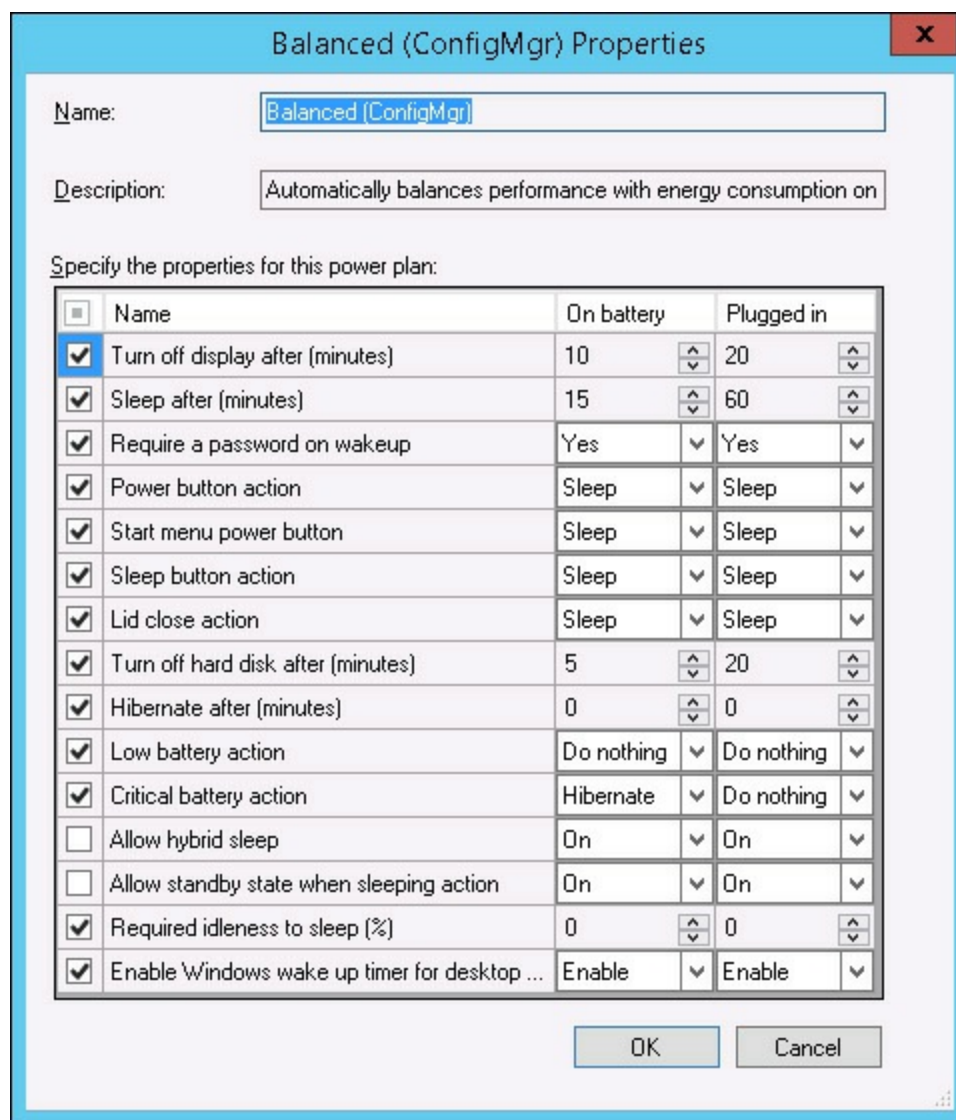
FIGURE 5-7 Power plan settings

Table 5-6 describes the available power management settings.

Setting	Description
Turn Off Display After (Minutes)	This setting specifies the amount of time that a computer must be inactive before turning off the monitor. Setting a value of zero prevents power management from turning off the display.
Sleep After (Minutes)	This setting specifies the amount of time that a computer must be inactive before going into a sleep state.
Hibernate After (Minutes)	This setting specifies the amount of time that a computer must be inactive before going into a hibernation state.
Require A Password On Wakeup	This setting specifies whether unlocking the computer requires a password after it comes out of a sleep state.
Power Button Action	This setting specifies the action that occurs when you press the power-on button on the computer. Values include the following: ■ Do nothing ■ Sleep ■ Hibernate ■ Shut down
Start Menu Power Button	This setting specifies the action that occurs when you click the Start menu power button. Values include the following: ■ Sleep ■ Hibernate ■ Shut down
Sleep Button Action	This setting specifies the action that occurs when you press the Sleep button. Values include the following: ■ Do nothing ■ Sleep ■ Hibernate ■ Shut down

Lid Close Action	This setting specifies the action that occurs when you close the lid on a portable computer. Values include the following: ■ Do nothing ■ Sleep ■ Hibernate ■ Shut down
Turn Off Hard Disk After (Minutes)	This setting specifies the amount of time that a computer's hard disk must be idle before it turns off.
Hibernate After (Minutes)	This setting specifies the amount of time that a computer must be inactive before it goes into a hibernation state.
Low Battery Action	This setting specifies the action that occurs when the battery reaches a low-threshold setting on a portable computer. Values include the following: ■ Do nothing ■ Sleep ■ Hibernate ■ Shut down
Critical Battery Action	This setting specifies the action that occurs when the battery reaches a critical-threshold setting on a portable computer. Values include the following: ■ Do nothing ■ Sleep ■ Hibernate ■ Shut down
Allow Hybrid Sleep	This setting specifies whether Windows should save a hibernation file when the computer enters a sleep state. You can use the hibernation file to restore the computer's state in the event of a power loss while in the sleep state.
Allow Standby State When Sleeping Action	This setting enables the computer to be in standby mode, which enables it to wake up faster. Note that this mode still consumes some power.
Required Idleness To Sleep (%)	This setting specifies a percentage of idle time for the computer processor to go into a sleep state.
Enable Windows Wake-Up Timer For Desktop Computers	This setting enables the built-in Windows wake-up timer that power management can use to wake a desktop computer. This setting is not available for portable computers.

TABLE 5-6 Power management settings

You can configure each of the power management settings twice: once for on-battery systems and once for plugged-in systems. To apply a power plan to a collection of computers, perform the following procedure:

1. Right-click the collection that is to have the power management policy and then click Properties.

2. Click the Power Management tab and then select Specify Power Management Settings For This Collection.

Figure 5-8 shows this for the Toronto Windows 8.1 Workstations collection.
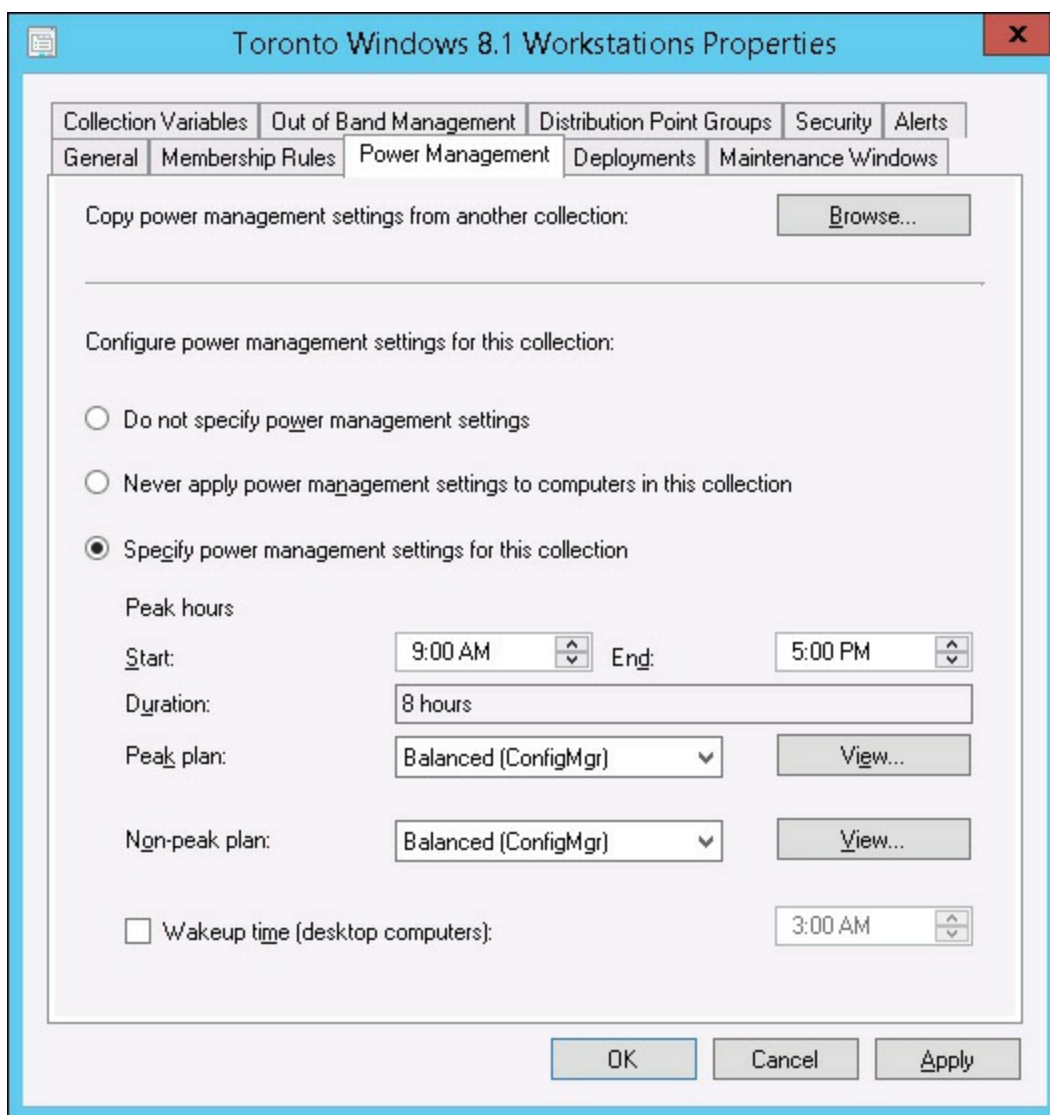
FIGURE 5-8 Power Management tab

3. Specify a power plan for both peak and nonpeak times.

If you are creating a customized power plan, the Edit button is available for editing specific power management settings.

Power management reports

You can view and analyze various reports related to power consumption, environmental impact, and power management settings in your Configuration Manager environment. The site database retains power management data used by daily reports for 31 days. The site database retains data used by monthly reports for 13 months. You might consider saving or exporting the results from critical reports if you want to be able to perform long-term analysis.

To view power management reports, perform the following procedure:

1. In the Monitoring workspace, expand the Reporting node and then expand the Reports node.

2. Click the Power Management folder.

3. In the results pane, shown in Figure 5-9, select the report to view and then, on the ribbon, click Run.
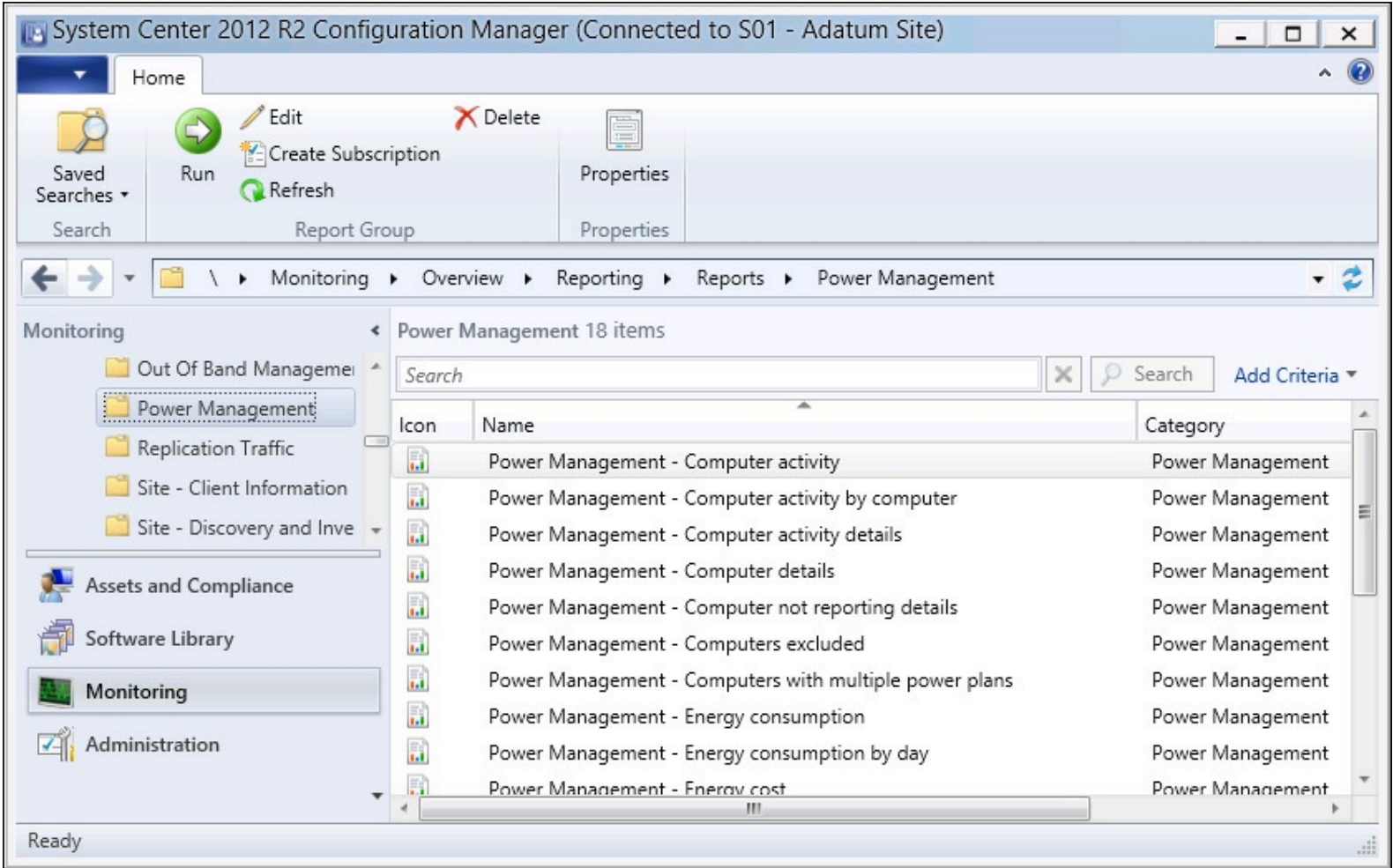
FIGURE 5-9 Power management reports

Depending on the report, you might need to provide additional criteria to view the data results.

> *More Info:* **Power Management**
>
> **You can learn more about power management at** *http://technet.microsoft.com/en-us/library/gg699392.aspx*.

Monitoring collections

Because several Configuration Manager features are based on collections, you should know how to monitor the collections. You might want to know when the collections are created, modified, or deleted. You also might want to view status messages that pertain to members of a specific collection. You can monitor collection-based tasks by using the following methods:

- **Component Status** The Component Status node, under the System Status node in the Monitoring workspace, contains the SMS_COLLECTION_EVALUATOR component. This component provides status information related to collections.

- **Log files** The Colleval.log file is associated with the SMS_COLLECTION_EVALUATOR component and provides detailed status information related to collection evaluation and management. This log file is located in the c:\Program Files\Microsoft Configuration Manager\Logs folder.

- **Status Message Queries** The Status Message Queries node, under the System node in the Monitoring workspace, provides the following status-message queries to assist in collection

monitoring:

- All Status Messages For A Specific Collection At A Specific Site
- Collection Member Resources Manually Deleted
- Collections Created, Modified, And Deleted

- **Reports** The Reports node includes several reports that pertain to collection-based tasks. The reports include:

- All Collections.
- All Resources In A Specific Collection.
- All Package And Program Deployments To A Specified Collection.
- Inventory Classes Assigned To A Specific Collection.
- Issues by incidence detail for a specified collection.

To view all reports that pertain to collections, you can perform a search on the Reports node for Collections. Figure 5-10 shows the results of this search.

FIGURE 5-10 Collection-related reports

Exam Tip

Remember the default evaluation schedule period for rule-based collections.

Objective summary

- Collections represent resource groups that consist of devices such as computers and mobile devices or users and user groups from all of the hierarchy's sites.
- You can use a direct rule to add a specific resource to a collection. If you add a resource to a collection by using a direct rule, the resource will remain in the collection until manually removed.
- You can use a query rule to add members to a collection based on their attributes.
- The default schedule to evaluate the membership of custom collections is once every seven days; incremental collection member evaluation runs every five minutes.
- Maintenance windows enable you to configure a specific period during which required deployments, software-update installations, configuration-item remediation, and task sequences can run on a client.
- Configuration Manager power management enables you to apply a power plan to managed computers.

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 of the following can you add to a collection by using a direct membership rule? (Choose two. Each correct answer provides a complete solution.)

    A. Router

    B. Switch

    C. Active Directory security group

    D. User account

2. You have created a collection by using a query rule. You have not enabled incremental updates. How often will the membership of the collection be updated by default?

    A. Once an hour

B. Once a day

C. Once every 7 days

D. Once every 10 days

3. Which of the following activities are not affected by maintenance windows? (Choose three. Each correct answer provides a complete solution.)

A. Configuration item remediation

B. User-initiated software deployment

C. Policy download and evaluation

D. Centralized software deployments

4. Which of the following client settings must be enabled if you want to use Configuration Manager to manage power settings for computers running Windows 8.1?

A. Hardware Inventory

B. Remote Tools

C. Software Inventory

D. Compliance Settings

Objective 5.3: Configure and monitor client status

System Center 2012 R2 Configuration Manager includes the Client Status feature that you can use to monitor client health and activity. The client health evaluator works outside the normal client processes to enable an administrator to discover issues with the clients, particularly issues that clients would be unable to report. This section describes how to use the Client Status feature and how to use the Configuration Manager console to monitor and evaluate client health.

This section covers the following topics:
- Verifying client installation
- Client status
- Client health evaluation and remediation
- Client health reports
- Client health alerts

Verifying client installation

You can verify the Configuration Manager client software's installation success in a number of ways, from both the server side and the client side. To verify that the Configuration Manager client software installed successfully, you can examine client log files, Control Panel in the client computer, and current information in collections and status reports.

Table 5-7 describes methods for verifying a successful client installation.

Verification method	Description
Client status column within the collection	Collection status displays information about the client's status, including: ■ Client Type (Computer). ■ Client (Yes/No). ■ Site Code. ■ Client Activity (Active/Inactive).
Configuration Manager reports	Configuration Manager reports provide client deployment and assignment status. All of the client deployment and assignment reports require you to deploy a fallback status point system role in the environment and configure the client to report state messages to the fallback status point during client installation. Useful Configuration Manager reports include the following: ■ Client Assignment Detailed Status Report ■ Client Assignment Failure Details ■ Client Assignment Status Details ■ Client Assignment Success Details ■ Client Deployment Status Details ■ Client Deployment Success Report ■ Client Deployment Failure Report ■ Computers Assigned But Not Installed For A Particular Site ■ Count Of Clients For Each Site ■ Count Of Configuration Manager Clients By Client Versions
Configuration Manager properties	On each client, you can confirm the client's status from the General tab of the Configuration Manager Properties dialog box.

Client logs	You can use several log files to verify client installation. Examples include:
	■ **CCMSetup.log** This log records setup tasks that CCMSetup.exe performs. You use this log to help troubleshoot client installation problems. CCMSetup.log is stored at %Windir%\CCMSetup\Logs.
	■ **Client.msi.log** This log records setup tasks that Client.msi performs. You use this log to help troubleshoot client installation problems. Client.msi.log is stored at %Windir%\CCMSetup\Logs.
	■ **ClientLocation.log** This log records site assignment tasks. You use this log to help troubleshoot when the client is not assigned to a Configuration Manager site. ClientLocation.log is stored at %Windir%\CCM\Logs.
	■ **ClientIDManagerStartup.log** This log records when the client has registered in the site successfully. No other client processes will complete until after registration of the client. This log is stored at %Windir%\CCM\Logs.
	■ **DataTransferService.log** This log records all BITS communication for policy or package access. You should check this log when troubleshooting components that cannot download. This log is stored at %Windir%\CCM\Logs.
	■ **PolicyAgent.log** This log records policies by using the Data Transfer service. You should check this log when troubleshooting the policy that cannot update. This log is stored at %Windir%\CCM\Logs.

TABLE 5-7 Verifying client installation

Client status

The System Center 2012 R2 Configuration Manager client agent runs a scheduled task to evaluate its client health status. The health status of a client enables you to determine the answers to the following questions:

■ How many clients are healthy in the hierarchy?

■ How many clients are inactive in the hierarchy because they have been powered off for a long time or because the Configuration Manager client agent is not installed?

■ What is the main cause of unhealthy clients in the hierarchy?

The task runs daily between midnight and 1:00 A.M. by default. Then, the client sends the evaluation results to a management point as a status message. Similar to the initial installation process, if the client fails to send its status message to a management point, it will then send the status message to a fallback status point if one exists in your hierarchy. If you have not installed a fallback status point in your hierarchy, the site server might not receive some evaluation results. The site server summarizes the evaluation results and activities of the client's health and then displays them in the Configuration Manager console in the Client Status folder located in the Monitoring workspace.

When you click the Client Status node, the results pane displays some statistics and the Recent Alerts section. The statistics have links showing the percentage of clients that are healthy, unhealthy,

or unknown, and active or inactive. Recent Alerts shows the alerts the Client Health feature generates because of meeting defined thresholds for client health and activity.

If you click the different links, this creates a temporary node under the Devices node in the Assets And Compliance workspace, and the console changes automatically to the newly created temporary node. Temporary nodes remain in the Configuration Manager console until you remove them manually or close the console. For example, when you click the Active Clients That Failed Client Check link—which denotes the clients that failed the client health checks—a temporary node for these unhealthy clients is created and selected automatically.

More Info: **Client Status**

You can learn more about client status at *http://technet.microsoft.com/en-us/library/hh338432.aspx*.

Client health evaluation and remediation

Client Status in the Configuration Manager console receives its information from the Client Health evaluation engine running on each client. The Client Health evaluation engine is an executable file named CCMEval.exe. This engine can perform health checks by using rules and can automatically rectify some configuration problems through a process termed *remediation*.

CCMEval.exe is installed with the Configuration Manager client agent and runs on computers. However, it is not part of the mobile device client. When you install the Configuration Manager client agent, the install process creates a scheduled task named Configuration Manager Health Evaluation. This task runs Ccmeval.exe at a time between midnight and 1:00 A.M. The client reports the results as a state message to the client's management point or a fallback status point if the management point is unavailable.

You can run the Configuration Manager Health Evaluation process on demand by running CCMEval.exe as required. Client health evaluation and remediation is only available to Windows-based computers. To view the client health rules that the Client Health evaluation engine is using, you can look in the *<client location>*\ccmeval.xml file. You can disable remediation of a client system by setting the following registry value to *True*: HKLM \Software\Microsoft\CCM\CCMEval\NotifyOnly.

If the computer is not running when the scheduled Configuration Manager Health Evaluation task is due to run, the task will run automatically as soon as it can, such as when you load the operating system or bring the computer out of sleep mode. Table 5-8 lists the health evaluation rules and remediation actions.

Health check	Remediation
Verify WMI Service Exists	No automatic remediation
Verify/Remediate WMI Service Startup Type	Set service startup to automatic
Verify/Remediate WMI Service Status	Start service
Wmi Repository Integrity Test	Reinstall client
Wmi Repository Read/Write Test	Reset WMI Repository and reinstall client
Verify BITS Exists	No automatic remediation
Verify/Remediate BITS Startup Type	Set service startup to automatic
Verify/Remediate Client And Client Prerequisites Installation	Reinstall client
Verify SMS Agent Host Service Exists	No automatic remediation
Verify/Remediate SMS Agent Host Service Startup Type	Set service startup to automatic
Verify/Remediate SMS Agent Host Service Status	Start service
Verify/Remediate Lantern Service Startup Type	Set service startup to manual
Verify/Remediate Antimalware Service Startup Type	Set service startup to automatic
Verify/Remediate Antimalware Service Status	Start service
Verify/Remediate Network Inspection Service Startup Type	Set service startup to manual
Verify/Remediate Windows Update Service Startup Type	Set service startup to automatic
Verify/Remediate Windows Update Service Status	Start service
Verify/Remediate Configuration Manager Remote Control Service Startup Type	Set service startup to automatic
Verify/Remediate Configuration Manager Remote Control Service Status	Start service
Verify/Remediate SQL CE Database Is Healthy	Set the database to ccmstore.sdf

TABLE 5-8 Health evaluation rules

Client health reports

In addition to the Client Check and Client Activity information in the Configuration Manager console, you can use the Client Status reports. After you have installed and configured a reporting services point role, the Client Status reports are located in the Client Status folder in the Configuration Manager console or the ConfigMgr_<*site code*>\Client Status path in the reporting website.

lists the available reports.

Report	Description
Client Remediation Details	This report provides client remediation details for a given collection.
Client Remediation Summary	This report provides remediation summary information for a given collection.
Client Status History	This report provides a historical view of the overall client status in the environment.
Client Status Summary	This report provides administrators with the current percentages of healthy and active clients for a given collection.
Client Time To Request Policy	This report shows the percentage of clients that have requested policy at least once in the past 30 days. Each day represents a percentage of total clients that have requested policy since day one in the cycle. This is useful for determining the time it would take to distribute a policy update to your client population. Client deployments or changes in client count can affect the accuracy of the report.
Clients With Failed Client Check Details	This report displays details about clients in a specific collection that have failed a client check.
Inactive Clients Details	This report provides a detailed list of inactive clients for a given collection.

TABLE 5-9 Client health reports

Client health alerts

The Alerts feature can use data from the Client Status feature to generate alerts in the Configuration Manager console. To configure alerts for Client Status, open the Properties dialog box for any collection. On the Alerts tab, click Add. You can add the following alert conditions:

- Client Check Pass Or No Results For Active Clients Falls Below Threshold (%)
- Client Remediation Success Falls Below The Threshold (%)
- Client Activity Falls Below Threshold (%)

After you have configured the alerts, the alerts that generate appear in the Alerts node of the Monitoring workspace and in the Client Status node. You also can subscribe to alerts to receive email notifications if you require email in addition to the in-console alert feature.

Exam Tip

Remember that not all health issues can be remediated.

Thought experiment: Client monitoring at Contoso

You are the Configuration Manager administrator at Contoso. You are concerned that a number of client computers that Configuration Manager manages at your organization are either inactive or regularly failing client health checks. With this information in mind, answer the following questions:

1. How can you determine which clients have failed client health checks?

2. How can you determine which clients in a collection are inactive?

Objective summary

- The System Center 2012 R2 Configuration Manager client agent runs a scheduled task to evaluate its client health status.
- If the client fails to send its status message to a management point, it will then send the status message to a fallback status point if one exists in your hierarchy.
- The Client Health evaluation engine is an executable file named CCMEval.exe. This engine can perform health checks by using rules and can automatically rectify some configuration problems through a process termed *remediation*.
- You can run the Configuration Manager Health Evaluation process on demand by running CCMEval.exe as required. Client health evaluation and remediation is only available to Windows-based computers.

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 want to run Configuration Manager Health Evaluation immediately rather than waiting for it to occur at the scheduled time. Which of the following files would you run to accomplish this task?

   A. CCMEval.exe

   B. CCMSetup.exe

   C. CMTrace.exe

   D. CCMSetup.msi

2. Which of the following health evaluation rules supports remediation?

   A. Verify BITS Exists

   B. Verify/Remediate Windows Update Service Status

   C. Verify SMS Agent Host Service Exists

   D. Verify File Exists

3. Which of the following reports would you run to view remediation details for a given collection?

    A. Client Status History

    B. Client Remediation Details

    C. Client Status Summary

    D. Inactive Clients Details

Answers

Objective 5.1

Thought experiment

1. You must install the client manually, using an account with local administrator privileges. You also must configure a network access account to allow access to resources in the site server domain for clients that are not domain members.

2. The computers running the Management Point, Distribution Point, Enrollment Point, and Enrollment Proxy Point roles require web server certificates when you want to use Configuration Manager to manage computers running Mac OS X.

3. The computers running the Management Point and Distribution Point roles require client authentication certificates when you want to use Configuration Manager to manage computers running Mac OS X.

Objective review

1. Correct answer: B

    A. Incorrect: The user account used to extend the schema must be a member of the Schema Admins domain security group.

    B. Correct: The user account used to extend the schema must be a member of the Schema Admins domain security group.

    C. Incorrect: The user account used to extend the schema must be a member of the Schema Admins domain security group.

    D. Incorrect: The user account used to extend the schema must be a member of the Schema Admins domain security group.

2. Correct answers: A and C

    A. Correct: You can assign a site code to a Configuration Manager client by using the Client.msi property SMSSITECODE=site code.

    B. Incorrect: You cannot assign a site code to a Configuration Manager client by using an answers.txt file.

    C. Correct: You can assign a site code to a Configuration Manager client by using Group Policy.

    D. Incorrect: You cannot assign a site code to a Configuration Manager client by using an

unattend.xml file.

3. **Correct answer:** D

    A. **Incorrect:** The Default Client Settings object has a default priority of 10,000.

    B. **Incorrect:** The Default Client Settings object has a default priority of 10,000.

    C. **Incorrect:** The Default Client Settings object has a default priority of 10,000.

    D. **Correct:** The Default Client Settings object has a default priority of 10,000.

4. **Correct answers:** A, B, and C

    A. **Correct:** You can cannot configure the Software Inventory: Configure The Display Names For Manufacturer Or Product setting through a custom client policy.

    B. **Correct:** You cannot configure the Compliance Settings: Schedule Compliance Evaluation setting through a custom client policy.

    C. **Correct:** You cannot configure the Mobile Devices: Polling Interval setting through a custom client policy.

    D. **Incorrect:** You can configure the Cloud Services: Allow Access To Cloud Distribution Point setting through a custom client policy.

Objective 5.2

Thought experiment

    1. Configure the Critical Battery Action power management setting.

    2. Configure the Lid Close Action power management setting.

Objective review

    1. **Correct answers:** C and D

        A. **Incorrect:** You cannot add a router to a collection because a router cannot be managed by Configuration Manager.

        B. **Incorrect:** You cannot add a switch to a collection because a switch cannot be managed by Configuration Manager.

        C. **Correct:** You can add an Active Directory security group to a collection by using a direct membership rule.

        D. **Correct:** You can add a user account to a collection by using a direct membership rule.

    2. **Correct answer:** C

        A. **Incorrect:** By default, collection membership is reevaluated once every 7 days.

        B. **Incorrect:** By default, collection membership is reevaluated once every 7 days.

        C. **Correct:** By default, collection membership is reevaluated once every 7 days.

        D. **Incorrect:** By default, collection membership is reevaluated once every 7 days.

    3. **Correct answers:** A, B, and C

        A. **Correct:** Configuration item remediation is not affected by maintenance windows.

B. Correct: User-initiated software deployment is not affected by maintenance windows.

C. Correct: Policy download and evaluation are not affected by maintenance windows.

D. Incorrect: Although it is possible to configure a centralized software deployment specifically to ignore maintenance windows, by default, centralized software deployment only occurs during the times specified in the maintenance window.

4. **Correct answer:** A

A. Correct: You must enable Hardware Inventory to be able to use Configuration Manager to manage power settings for computers running Windows 8.1.

B. Incorrect: You do not need to enable Remote Tools to be able to use Configuration Manager to manage power settings for computers running Windows 8.1.

C. Incorrect: You do not need to enable Software Inventory to be able to use Configuration Manager to manage power settings for computers running Windows 8.1.

D. Incorrect: You do not need to enable Compliance Settings to be able to use Configuration Manager to manage power settings for computers running Windows 8.1.

Objective 5.3

Thought experiment

1. Run the Clients With Failed Client Check Details report.
2. Run the Inactive Clients Details report to determine which clients are no longer active in a collection.

Objective review

1. **Correct answer:** A

A. Correct: You run CCMEval.exe to trigger the health evaluation process.

B. Incorrect: CCMSetup.exe is used in the client deployment process.

C. Incorrect: CMTrace.exe is used to view log files.

D. Incorrect: CCMSetup.msi is used in the Configuration Manager setup process.

2. **Correct answer:** B

A. Incorrect: The Verify BITS Exists health check does not support automatic remediation.

B. Correct: The Verify/Remediate Windows Update Service Status health check supports automatic remediation.

C. Incorrect: The Verify SMS Agent Host Service Exists health check does not support automatic remediation.

D. Incorrect: The Verify File Exists health check does not support automatic remediation.

3. **Correct answer:** B

A. Incorrect: The Client Status History report provides a historical view of the overall client status in the environment.

B. Correct: You would run the Client Remediation Details report to view remediation details

for a given collection.

C. Incorrect: The Client Status Summary report provides the current percentages of healthy and active clients for a given collection.

D. Incorrect: The Inactive Clients Details report provides a detailed list of inactive clients for a given collection.

Chapter 6. Manage inventory using Configuration Manager

As the name of the product suggests, Configuration Manager enables you to inventory and manage the configuration of managed client devices. Hardware and software inventory allow you to generate a detailed picture of the hardware and software configurations of the client devices that Configuration Manager manages. Software Metering is a feature that enables you to track how applications on managed clients are being utilized. You can then use the reporting functionality in Configuration Manager to generate detailed reports using the information that has been collected.

Objectives in this chapter:
- Objective 6.1: Manage hardware and software inventory.
- Objective 6.2: Manage software metering.
- Objective 6.3: Create reports.

Objective 6.1: Manage hardware and software inventory

Configuration Manager enables you to configure the collection of hardware and software inventory and, thus, to generate detailed information about the configuration of client devices in your organization. You can use this detailed information as the basis for creating Configuration Manager collections or use it to generate reports about the configuration of managed devices.

This section covers the following topics:
- Inventory collection
- Hardware inventory collection
- Extending hardware inventory
- Software inventory collection
- File collection
- Managing inventory collection

Inventory collection

Inventory collection involves gathering information about a client computer's hardware and software. You can collect inventory information through three primary methods:

- **Hardware inventory** Collects information about the hardware configuration of client computers. Configuration Manager supports hardware inventory collection for computers that are running supported Windows operating systems, Mac OS X, Linux, and UNIX operating systems.

- **Software inventory** Collects information about files on client devices. Operating systems that are not Windows-based do not support software inventory.

- **Asset Intelligence** Use in conjunction with and in addition to hardware inventory to report software installations on client computers.

If you want to configure hardware and software inventory options that apply to the entire hierarchy, do so using Default Client Settings. If you want to configure hardware and software inventory options that only apply to a small number of computers, create custom client settings and then assign them to specific collections.

Exam Tip

Custom client settings override any settings that you configure within Default Client Settings.

Inventory collection isn't limited to Configuration Manager. Microsoft Intune (formerly Windows Intune) can collect hardware inventory from its clients. Integrating Intune with Configuration Manager enables you to use the inventory information that Intune collects in Configuration Manager.

When you integrate Intune with Configuration Manager, there are some differences between what Intune inventories for personal devices and what it inventories for company-owned devices. The following table illustrates the software inventory capability of Intune when integrated with Configuration Manager.

Platform	Personal devices	Company devices
Windows Phone 8/Windows Phone 8.1	Only managed apps	Only managed apps
Windows RT/Windows RT 8.1	Only managed apps	Only managed apps
Windows 8/Windows 8.1	Only managed apps	Only managed apps
iOS	Only managed apps	All installed apps
Android	Only managed apps	All installed apps

TABLE 6-1 Intune inventory information

More Info: **Intune Inventory**

You can learn more about Microsoft Intune inventory at *http://blogs.technet.com/b/tune_in_to_windows_intune/archive/2014/03/24/windows-intune-mobile-device-inventory-information-faq.aspx*.

You can use the results of inventory collection with other Configuration Manager features. For example, you can:

- Build queries that include or exclude computers based on their hardware configuration or installed software. For example, you can create a query that displays all computers with less than 5 gigabytes of space left on their operating system volume.
- Build collections by using queries that include or exclude computers based on their hardware configuration or the type of installed software—for example, that have a specific model of graphics adapter or that are running a specific application.
- Generate reports based on hardware configuration or installed software.

- Use queries and reports to find computers that do not meet corporate standards. For example, you can maintain information about current hardware and software installations to ensure that all computers meet the current compliance requirements.
- Use Resource Explorer, which is the Configuration Manager console that displays the complete inventory data that Configuration Manager collects for individual computers.
- Collect copies of files from client computers by using software inventory. Configuration Manager then stores these files on the site server. One example is if you need to collect a specific configuration file from computers within a specific site.

By default, the hardware inventory and software inventory collection runs every seven days, though by configuring default or custom client settings, you can modify this schedule to meet your organization's requirements. Computer hardware and software configuration changes slowly, so it is rarely necessary to schedule aggressive inventory collection. Figure 6-1 shows a schedule configured to run once every 14 days.
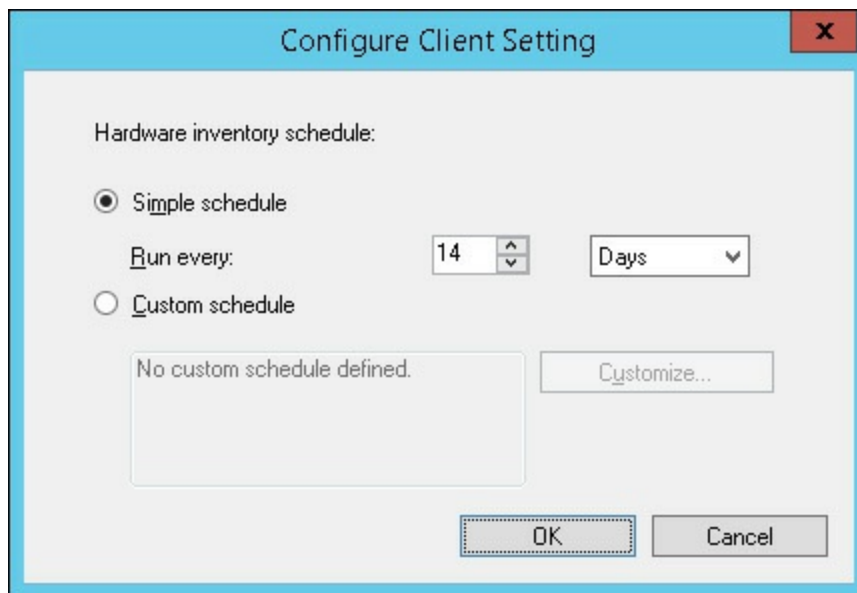
FIGURE 6-1 Inventory schedule

Inventory collection runs automatically based on the schedule you configure. The key phases in the inventory collection process are as follows:

1. Inventory agents create inventory data files that contain the collected data.
2. Client sends inventory data files to the management point.
3. Management point forwards data to the site server.
4. Update the site database. Configuration Manager updates the database.
5. Replicate to the central administration site.

The primary site servers add the inventory data to the Configuration Manager site database. The site database stores hardware inventory history for each client. Configuration Manager retains only the current software inventory data for each client and does not store historical data. Inventory data is site data, and site data will not replicate to any other primary sites in the hierarchy, only to the central site.

Hardware inventory collection

The Configuration Manager hardware inventory agent discovers information about computers by querying the Windows Management Instrumentation (WMI) database on the client computer. The hardware inventory agent is enabled by default and runs every seven days. By default, hardware inventory has a built-in random delay, which ranges from 60 to 240 minutes. This helps alleviate contention issues for specific scenarios, such as Virtual Desktop Infrastructure (VDI) environments.

WMI is the Microsoft implementation of Web-Based Enterprise Management (WBEM). WBEM allows access to data from a variety of underlying technologies, including the Win32 class, WMI, the Desktop Management Interface (DMI), and the Simple Network Management Protocol (SNMP). WBEM is based on the Common Information Model (CIM) schema. WMI uses Managed Object Format (MOF) files to determine what information to load into the CIM repository. WMI can also use providers to access the CIM repository.

Clients running OS X, Linux, or UNIX use an open source Open Management Infrastructure (OMI) implementation of the CIM and WBEM standards to gather hardware inventory information. OMI includes rules for gathering information about installed applications because it is not possible to obtain this information through a software inventory.

With Configuration Manager 2007, you used the SMS_DEF.MOF file to customize hardware inventory classes. With Configuration Manager 2012 and Configuration Manager 2012 R2, you customize the hardware inventory classes that the hardware inventory agent collects by modifying the hardware inventory client settings.

The first time the hardware inventory agent runs, it collects and returns a full hardware inventory. This full inventory establishes a baseline for future inventory collections. Subsequent inventory data contains only the information that has changed since the previous inventory collection. Another term for this changed information is delta information. Because delta information is typically a fraction of a complete inventory collection, the network traffic that client inventory generates after initial inventory collection is much smaller.

Certain events can cause a client to again collect and report a full hardware inventory:

- The client attempts to update inventory data that does not exist in the site database.
- The delta inventory information becomes corrupt.
- You upgrade the Configuration Manager client software to a new version.
- An administrator assigns the client to a new site.

You can modify the hardware inventory collection by configuring the client settings for the hardware inventory agent. You configure the hardware inventory agent in the Administration workspace, Client Settings node, in either Default Client Settings or a custom client settings object. Figure 6-2 shows enabling hardware inventory.
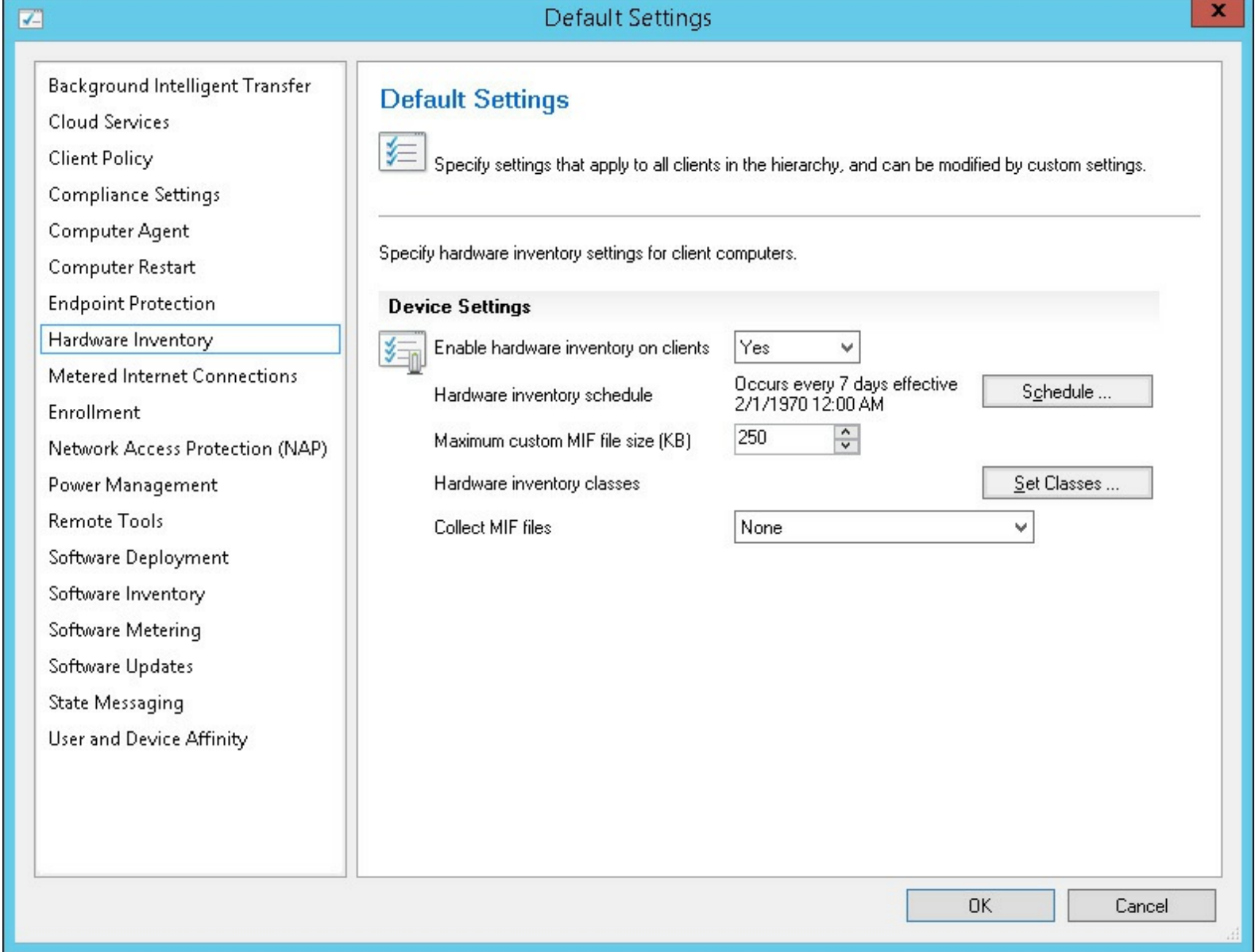
FIGURE 6-2 Hardware Inventory client settings

If you want the hardware inventory settings to apply to specific computers only, create a custom client setting that deploys to a collection that contains the computers you want to inventory. If a computer receives settings from both the default and custom client settings, the hardware inventory agent merges the hardware inventory classes from each of the settings when the client reports its hardware inventory.

You can configure several options for hardware inventory as described in .

Option	Use
Enable Hardware Inventory On Clients	Enable or disable a hardware inventory collection. This option is enabled by default. Disabling hardware inventory in custom settings disables hardware inventory on clients.
Hardware Inventory Schedule	Specify the start time and interval for which the client's hardware inventory agent collects hardware inventory. By default, hardware inventory collection runs every seven days.
Maximum Custom MIF File Size (KB)	Specify the maximum size for custom Managed Information Format (MIF) files that you want to collect from a client. You can configure this option by using the Collect MIF Files setting. The hardware inventory agent does not collect or process any MIF files that exceed the maximum custom MIF file size. The default value is 250 kilobytes (KB).
Hardware Inventory Classes	Customize which WMI classes and attributes you use to collect hardware information from Configuration Manager clients. You can modify the default classes and attributes, or you can import custom Managed Object Format (MOF) files to allow for vendor-specific classes and attributes.
Collect MIF Files	Specify the custom MIF file types that you want to collect. You can choose to collect custom IDMIF and NOIDMIF files, or you can collect both types. The default option is no collection of any custom MIF files.

TABLE 6-2 Hardware inventory options

More Info: **Hardware Inventory**

You can learn more about hardware inventory at *http://technet.microsoft.com/en-us/library/hh301103.aspx*.

Extending hardware inventory

You can extend the hardware inventory for Windows-based clients by using the following methods for Default Client Settings or for a custom client-device setting configuration:

- Enable or disable existing inventory classes. To display a list of default inventory classes, click the Set Classes button, which opens the Hardware Inventory Classes dialog box shown in Figure 6-3. From this dialog box, you can enable or disable the classes and class properties that you want the hardware inventory agent to collect. You can use either the Search For Inventory Classes field or the Filter buttons that are at the top of the Hardware Inventory Classes dialog box to search for and view individual classes.
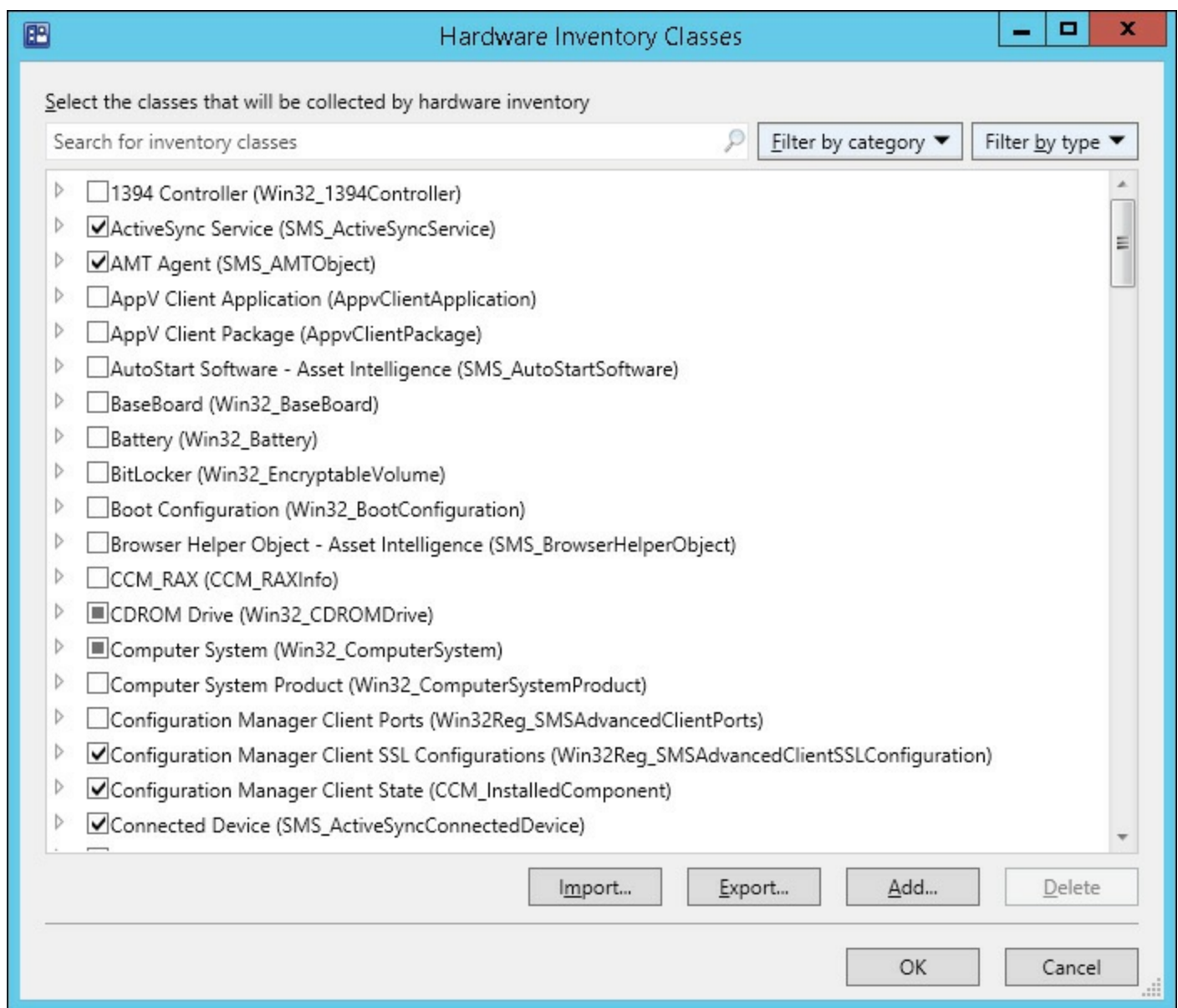
FIGURE 6-3 Hardware Inventory Classes

- Add a new hardware inventory class. You can connect to another computer to retrieve specific inventory classes and then add the new inventory class to the set of default classes. For example, you might use a client computer to test a hardware vendor–specific MOF file. After you verify that the specific MOF file collects the custom information properly, you can connect to the computer from the Configuration Manager console to import the vendor-specific classes.

If you have a custom MOF file that contains hardware inventory class settings that you used in a prior version of Configuration Manager or an MOF file that a vendor provides, you can use the Import and Export features to import or export custom MOF files and their associated settings.

The Configuration.mof file is a text file you can edit with a text editor such as Notepad .exe, which defines the data classes for the hardware inventory agent. Configuration.mof also defines and registers the providers that the hardware inventory agent uses during data collection. To extend the hardware inventory that Configuration Manager collects, you edit the Configuration.mof file to use a registered inventory data provider. For example, if you want to collect additional information from specific registry keys on the client computer, you modify the registry property provider to collect the specific registry key information that you require.

When clients request computer policies as part of their normal policy-polling interval,

Configuration Manager attaches the Configuration.mof content to the policy body that clients download and compile. When you add, modify, or delete data classes from the Configuration .mof file, the next time that clients receive an updated computer policy, they automatically compile changes that have occurred to inventory-related data classes.

The Configuration.mof file is located on the site server in the ConfigMgr install directory \Inboxes\Clifiles.src\Hinv folder.

Software inventory collection

Software inventory collection enables you to inventory specific file types, such as .exe files, located on Configuration Manager client devices. Software inventory provides some details about a file by inventorying file header information. If the file does not have a file header, or if the software inventory agent cannot read the header file, the file is inventoried as an unknown file type. Inventory results include a report on any file that matches the requested file type and might include file-system details that you configure in the software inventory agent settings. You can also use software inventory to collect copies of files that are transferred to the site server. The default inventory settings are shown in Figure 6-4.
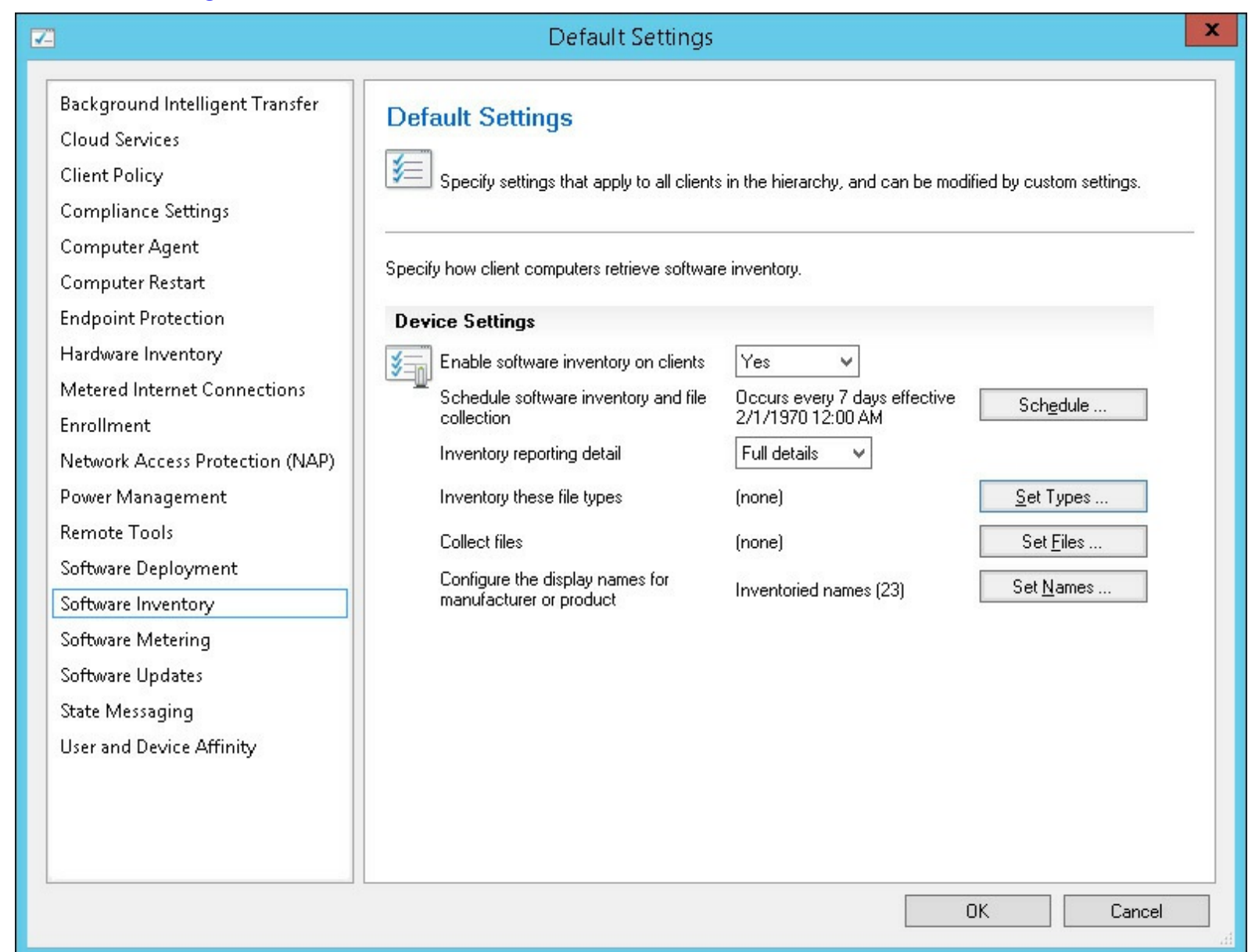
FIGURE 6-4 Software Inventory

Similar to hardware inventory, software inventory initially reports a full inventory soon after you enable the software inventory agent. Subsequent inventory reports only contain changes to inventory information. The site server processes delta inventory information but rejects it if information is missing or corrupt. If the site server rejects the delta inventory, it instructs the client to run and report a full inventory cycle.

You can use Resource Explorer to view inventory information for client software, or you can view software-inventory information in reports. Configuration Manager clients that are running OS X, Linux, or UNIX do not support the software inventory feature.

By default, the software inventory agent is enabled and configured to run every seven days using the simple schedule option. However, no file types are specified. You can modify this setting to configure file types, as shown in Figure 6-5, and a custom schedule as necessary.
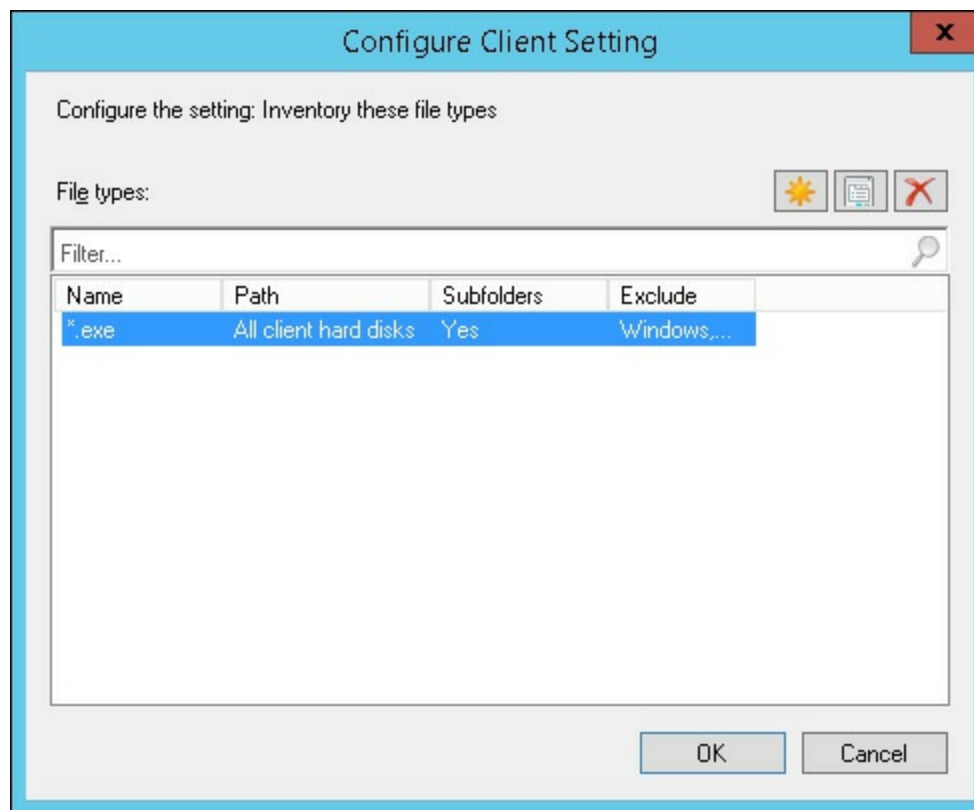
FIGURE 6-5 File Types

The information that Configuration Manager gathers can include data related to the operating system, installed programs, and any files that you want to inventory. Configuration Manager stores this data in the site database, where you can use the information in queries to generate and view reports or to build software-specific collections. For example, you can create a collection of all computers that have specific versions of files, or you can find all clients with an old version of a file and replace it with a newer version.

Although software inventory can provide a list of installed application files, such as .exe files, you should not use it for identifying installed software. Instead, you should use Asset Intelligence, which provides details about installed applications beyond a simple list of file names. For example, software inventory might find a file named Game.exe but not be able to find information beyond that name. Asset Intelligence, however, will allow you to identify which application it actually is.

By default, software inventory is enabled on clients, but no file types are defined for inventory. To inventory specific file types, you need to configure software inventory rules by using the following settings:

- **Name** You can list a specific file, or you can specify a file type by using wildcard characters. For example, you could specify *.ps1 to inventory Windows PowerShell command-line interface scripts.

- **Path** You can configure the agent to search for the specified file on all of the clients' hard disks or in a specific path. The path can be explicit or based on a variable such as *%ProgramFiles%*.

- **Exclude Encrypted And Compressed Files** This option is enabled by default and specifies that Configuration Manager does not inventory any file that has the encryption or compression attribute set.

- **Exclude Files In The Windows Folder** This option is enabled by default and specifies that Configuration Manager will not inventory any files that are in the %SystemRoot% folder.

In addition, you can configure reporting detail for software inventory to specify whether software inventory collects file system full details, details for inventoried files, or product details from file header information. These options apply to all software inventory rules.

Collecting software inventory of encrypted and compressed files might cause the inventory process to run more slowly. To inventory an encrypted file, the software inventory agent must create a decompressed copy of the file. Furthermore, if the client computer is running antivirus software, the antivirus software rescans every file that the inventory process opens.

You can exclude some folders or entire volumes from a client's software inventory. To exclude a folder, create a hidden file named Skpswi.dat in that folder. Note that excluding a folder from software inventory also excludes any subfolders. To exclude an entire hard disk, create the hidden Skpswi.dat file in the volume's root. You also might decide to use the Skpswi.dat file to exclude specific folders that you do not want to inventory on a file server or distribution point.

Software inventory retrieves manufacturer and product names from file header information. If any inconsistencies are in the way, these names are entered in the header information; multiple variations of the manufacturer and product names also appear both in Resource Explorer and in any query results based on inventoried file display names.

For example, files created by A. Datum Corporation might enter the manufacturer name in various forms, such as A. Datum; A. Datum, Corp; A. Datum, corp; or Adatum. Such inconsistencies can make it more difficult to read and query against software inventory information because the data appears under multiple manufacturer names rather than under a single name.

To resolve this problem, you can set custom display names for manufacturers or products. For example, you can map all variations of A. Datum to A. Datum Corporation for display and query purposes.

More Info: **Software Inventory**

You can learn more about software inventory at *http://technet.microsoft.com/en-us/library/hh509028.aspx*.

File collection

File collection allows files to be collected from Configuration Manager clients. When you specify a file for collection, the software inventory agent runs a file collection cycle on each Configuration Manager client. If the software inventory agent finds a file to collect, it attaches the file to the inventory report and then forwards it to the site server. On the client, the file collection cycle is a separate action from the software inventory cycle. By default, software inventory does not collect any files.

The site server stores up to five versions of each file that the software inventory agent collects from each client. The site server does not delete any files that the software inventory agent collects. Therefore, you should use file collection only in very specific circumstances and configure the agent to collect only files that are small and do not change often. Consider enabling deduplication on the volume that hosts collected files.

Exam Tip

File collection is not enabled by default. Up to five versions of each file are stored.

To configure file collection by software inventory, you must perform the following procedure:

1. To create a new file entry, under Client Settings, in the Software Inventory section, click Set Files and then click New (which appears as a star).

2. In the Collected File Properties dialog box, shown in , specify the name of the files that you want to collect or use wildcard characters to specify the file types that you want to collect. An example is *.ini.

FIGURE 6-6 Collected File Properties

3. Specify the location in which you want the agent to search for files. You can configure the agent to search for a specific file on all of the client's hard disks or in a specific path only. The path can be explicit or based on a variable such as *%windir%*.

4. Specify whether to exclude encrypted and compressed files.

5. Specify the maximum total file size of files collected for this entry.

The site server stores each collected file in the ConfigMgr installation directory\Inboxes \Sinv.box\Filecol folder. If a file has not changed since the last collection, the agent will not collect it again. You can use Resource Explorer to view or save files that the agent collects from a client.

Managing inventory collection

You may have situations in which you need hardware or software inventory to run immediately on a single client. For example, when a client has received an upgrade, you may want it reported as soon as possible.

You can initiate certain client actions (such as policy retrieval and inventory collection) on demand, independent of scheduled intervals. You can initiate these client actions on the Actions tab of the Configuration Manager Properties dialog box in Control Panel on the client.

To initiate off-cycle inventory collection and reporting, you must complete the following procedure:

1. On the client computer, open Control Panel.

2. In Control Panel, in System And Security, start Configuration Manager.

3. In the Configuration Manager Properties dialog box, click the Actions tab.

4. Under Actions, select the inventory action that you want to initiate, such as the Hardware Inventory Cycle shown in <u>Figure 6-7</u>, and then click Run Now.
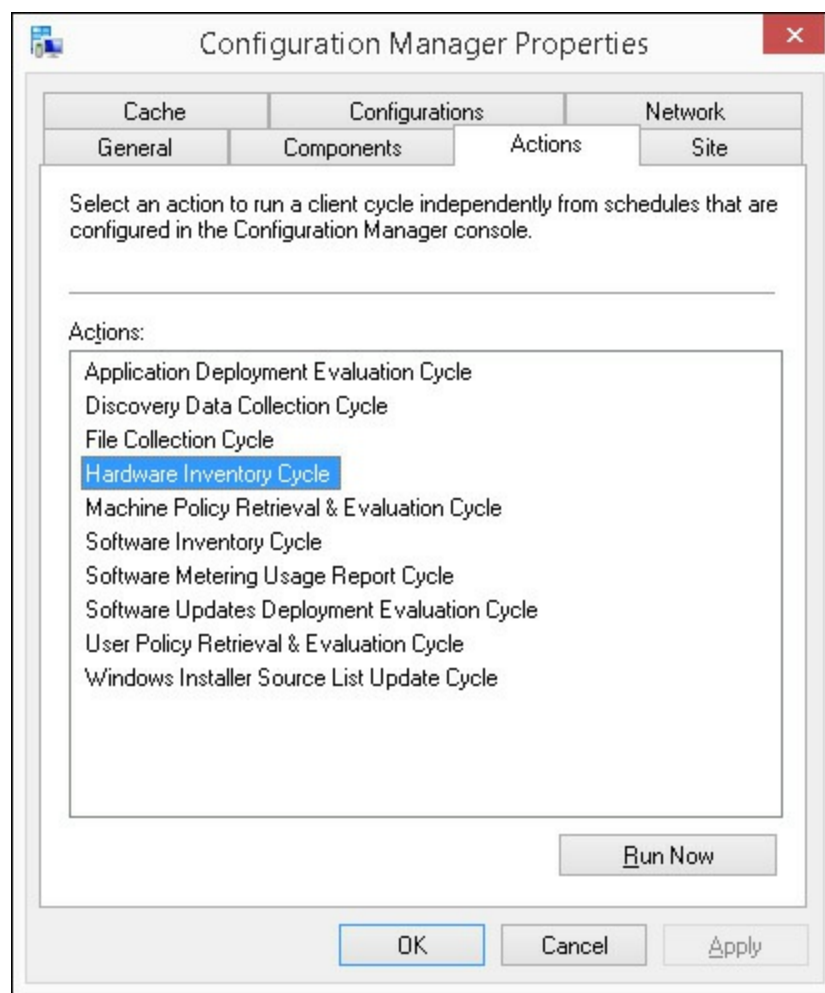
FIGURE 6-7 Hardware Inventory Cycle

After agents collect hardware or software inventory information from Configuration Manager client computers, you can view the results by using either Resource Explorer or inventory reports. You also can obtain results by creating custom queries from within the Configuration Manager console.

You can use Resource Explorer to display inventory information for one client at a time. To start Resource Explorer, you must complete the following procedure:

1. From the Configuration Manager console, click the Assets And Compliance workspace.

2. Click the Devices node. Note that you also can click Device Collections, right-click a device collection that contains the client device that you want to view, and then click Show Members.

3. In the list view, right-click a client device, point to Start, and then click Resource Explorer.

You also can use the reporting feature to view various types of reports pertaining to hardware and software inventory. To access reports, complete the following procedure:

1. In the Configuration Manager console, click the Monitoring workspace.

2. Expand the Reporting node and then click and expand the Reports node. Notice that reports are organized into category-based folders, enabling you to locate common reports quickly.

You also can access reporting by using Internet Explorer to open the Report Manager URL. By default, the URL for the Report Manager is *http://servername/Reports*.

If you configure management points to use HTTPS for client communication, all data transmitted to the server is protected using Secure Sockets Layer (SSL). However, you can opt to use HTTP to communicate with management points within your internal network. In this case, HTTP sends client inventory data and collected files unencrypted and unsigned. As a result, your organization would be

exposed to threats such as someone intentionally sending invalid data or excessively large data as a form of denial-of-service attack. In addition, because the data is unencrypted, it is possible for someone to capture and read the collected inventory in transit. As a best practice, consider implementing security measures to protect the inventory process and data communication by using the following methods:

- **Enable Signing And Encryption** To provide more secure communication between client computers and the site, you can configure several signing and encryption options, including:

  - **Require Signing** This option ensures that all data that is sent from the client to the management point is signed.

  - **Require Secure Hash Algorithm 256 (SHA-256)** This option ensures that when a client is communicating by using HTTP, the communication uses the SHA-256 hash algorithm to sign the data. Note that only System Center 2012 Configuration Manager client and newer Configuration Manager versions support SHA-256.

  - **Use Encryption** This option ensures that all inventory data and state messages are encrypted by using the Triple Data Encryption Standard (3DES) encryption algorithm when sent to the management points. You can use this option for environments in which inventory data might contain sensitive information.

To enable signing and encryption for the site, complete the following procedure:

1. In the Configuration Manager console, click the Administration workspace.
2. Expand the Site Configuration node and then click Sites.
3. In the list view, right-click the site and then click Properties.
4. In the Site Properties dialog box, click the Signing And Encryption tab.
5. Select the signing and encryption options as needed.

   - **Disable Any Custom MIF File Collections** Although you can extend inventory by collecting IDMIF and NOIDMIF files, the MIF files that the hardware inventory agent collects are not validated. As a result, a malicious user could use the MIF files to alter your site's database by overwriting valid data with invalid data.

   - **Do Not Collect Critical Or Sensitive Files** The inventory client agent runs with the rights of the LocalSystem account. This account can collect copies of critical system files, such as the registry or security account database. When these files are available at the site server, someone with permission to read the collected files could analyze their contents and potentially discern important client details that could enable him or her to compromise its security.

   - **Use An Appropriate Deletion Interval For Aged Inventory Data And Collected Files** You can ensure the encryption of data that is sent from the client to the management point, but the data that the site database stores is not encrypted. Therefore, you should determine how long you want the database to retain the inventory information and collected files and configure the Delete Aged Inventory History and Delete Aged Collected Files site maintenance tasks as appropriate.

To configure the deletion interval for the Delete Aged Inventory History and Delete Aged Collected Files site maintenance tasks, complete the following procedure:

1. In the Configuration Manager console, click the Administration workspace.
2. Expand the Site Configuration node and then click Sites.
3. In the list view, right-click the site and then click Site Maintenance.
4. Modify the properties for the Delete Aged Inventory History and Delete Aged Collected Files site maintenance tasks as required. This dialog box is shown in Figure 6-8.
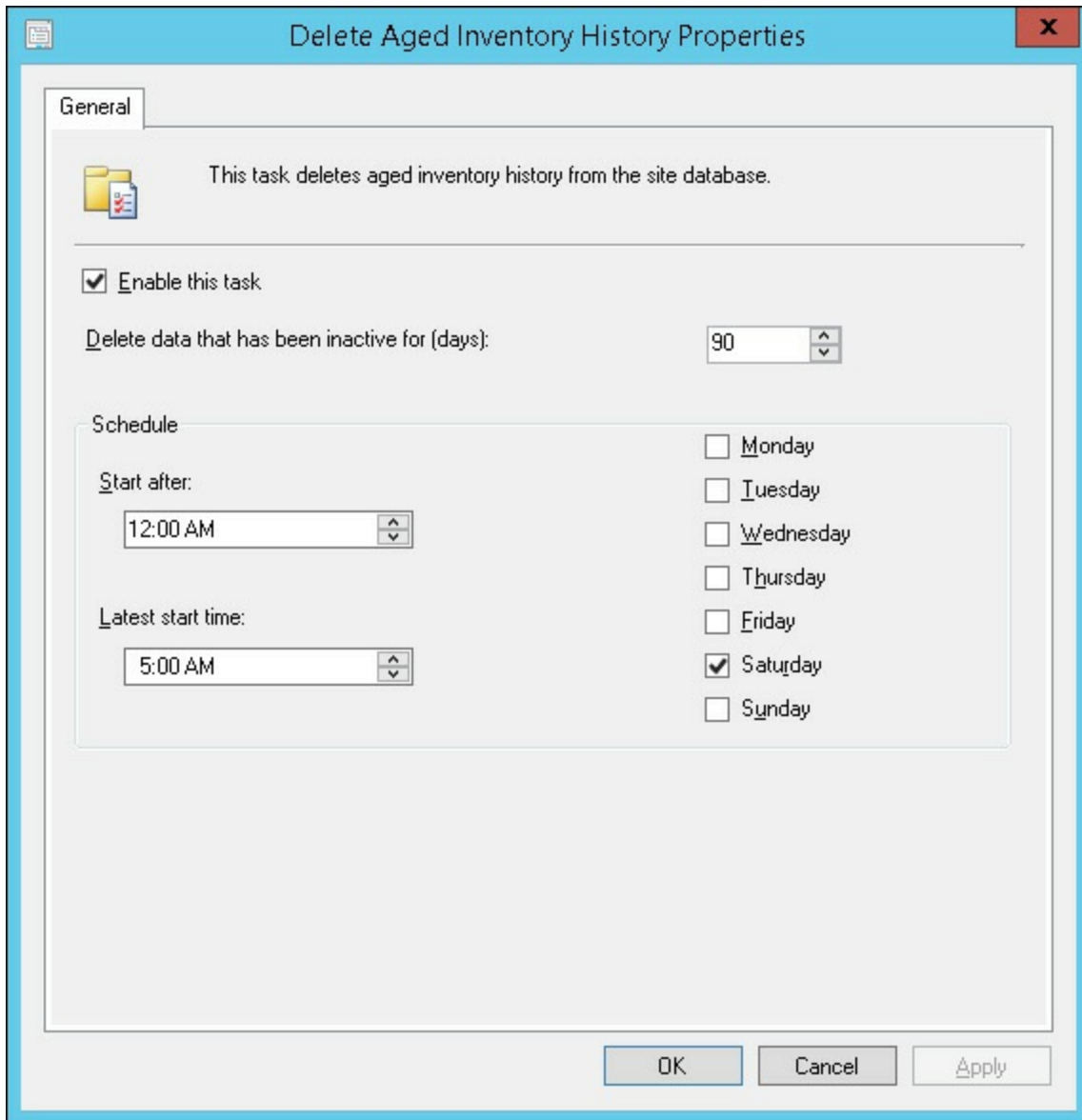
FIGURE 6-8 Delete Aged Inventory History Properties

Several methods are available to troubleshoot the causes of problems with inventory collection. These methods include:

- **Reviewing the client log files** A client's log files can help you identify inventory problems that are affecting that client. The client log files that pertain directly to inventory are as follows:
  - **InventoryAgent.log** Records activities of the inventory agent, including creation of discovery data records (DDRs) and inventory reports.
  - **CcmExec.log** Records activities of the client of the Short Message Service (SMS) Agent Host service. For inventory, this includes high-level events such as initialization of the inventory agent queue.
  - **Policyagent.log** Records policy updates on the client, including updates that enable the

inventory agent and configure the hardware inventory collection.

- **FileSystemFile.log** Records scanning events by the inventory agent file system for software inventory when you enable and configure it.
- **Mifprovider.log** Records events related to MIF file reporting.

- **Reviewing the management point log files** You can use log files on the management point to help identify inventory problems that relate to inventory processing. The management point log files that pertain to inventory are as follows:

  - **MP_Hinv.log** Provides details on hardware inventory that client computers report.
  - **MP_Relay.log** Provides details on how inventory information maps to specific inbox folders.
  - **MP_Retry.log** Provides information on the retry states of inventory collection.

- **Reviewing the site-server log files** You can use log files on the server to help identify inventory problems that affect more than one client. The following are log files of the site server that relate directly to inventory:

  - **Dataldr.log** Records processing of MIF files and hardware inventory data into the site database.
  - **Sinvproc.log** Records processing of software inventory data into the site database.

- **Reviewing status message queries** Configuration Manager status messages report information about Configuration Manager component behavior and data flow. Status messages can be helpful when you are troubleshooting Configuration Manager issues because many status messages include possible cause and resolution information. Status message queries related to inventory include the following:

  - Clients That Reported Errors Or Warnings During Inventory File Collection
  - Clients That Reported Errors Or Warnings While Creating A Hardware Inventory File
  - Clients That Reported Errors Or Warnings While Creating A Software Inventory File

---

Thought experiment: **Inventory collection at Contoso**

You are the Configuration Manager administrator at Contoso. Contoso has a heterogeneous environment, with computers that run Windows, Mac OS X, Linux, and UNIX operating systems. You are interested in collecting hardware and software inventory information. With this in mind, answer the following questions:

1. **Which operating systems support the collection of hardware inventory?**
2. **Which operating systems support the collection of software inventory?**

Objective summary

- Inventory collection involves gathering information about a client computer's hardware and software.

- Hardware inventory collects information about the hardware configuration of client computers.
- Configuration Manager supports hardware inventory collection for computers that are running supported Windows operating systems, Mac OS X, Linux, and UNIX operating systems.
- Software inventory collects information about files on client devices. Operating systems not based on Windows do not support software inventory.
- Custom client settings override any settings that you configure within Default Client Settings.
- The Configuration.mof file is a text file that defines the data classes for the hardware inventory agent.
- File collection allows files to be collected from Configuration Manager 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. Which of the following Configuration Manager features can you use to determine whether a specific graphics card is being used on a Configuration Manager client?

    A. Hardware inventory

    B. Software inventory

    C. File collection

    D. Software metering

2. You want to collect all .ini files stored in a specific folder on each Configuration Manager client. Which of the following Configuration Manager features would you use to accomplish this goal?

    A. Software metering

    B. Asset Intelligence

    C. Hardware inventory

    D. File collection

3. You have configured software inventory to inventory all files that use the .docx extension. If you don't change any other settings, which of the following file types will not be collected by software inventory by default? (Choose all that apply.)

    A. Files with the encryption attribute set

    B. Files with the compression attribute set

    C. Files with the hidden attribute set

    D. Files with the archive attribute set

Objective 6.2: Manage software metering

Software metering enables you to track how often a particular application is used. This is extremely useful if you want to determine which applications are, and are not, being used in your organization.

This section covers the following topics:

- Software metering
- Software-metering rules
- Manage software-metering tasks

Software metering

You use software metering to monitor application usage on Configuration Manager client computers. You can summarize software-metering data to produce useful reports that can help you plan for your organization's software purchases.

Software metering can be useful when you need to know:

- How many instances of a particular software program users are using.
- How many licenses of a particular software program you need to purchase when you renew your license agreement with the software vendor.
- Whether any users are still running a particular software program. If users are no longer using the program, you could consider retiring it.
- What times of the day users most frequently use a software program.

Software metering can collect detailed information, such as the information listed in Table 6-3.

Collected information	Included values
Program usage information	■ Start time ■ End time ■ Meter data ID ■ Resource ID ■ User name ■ Users of Terminal/Remote Desktop Services sessions ■ Whether Terminal/Remote Desktop Services is still running
File information	■ File ID ■ File name ■ File version ■ File description ■ File size (in KB)
Program information	■ Company name ■ Product name ■ Product version ■ Product language

TABLE 6-3 Information collected by the software-metering process

Software metering uses two main components to perform data collection tasks: the Software Metering Agent and software-metering rules. When enabled, the Software Metering Agent reports software-metering data based on the site's software-metering rules. You must configure software-

metering rules prior to beginning data collection about a program's usage.

Default Client Settings enables the Software Metering Agent by default and is configured to send software-metering data to the management point every seven days. Rules are created automatically, based on usage. However, no rules are enabled by default. If you want to enable software metering for a specific group of computers, you can create a custom client setting configuration that targets a specific collection of devices, and then you can disable the Software Metering Agent in default client agent settings. shows the Software Metering settings section of the Default Client Settings object.
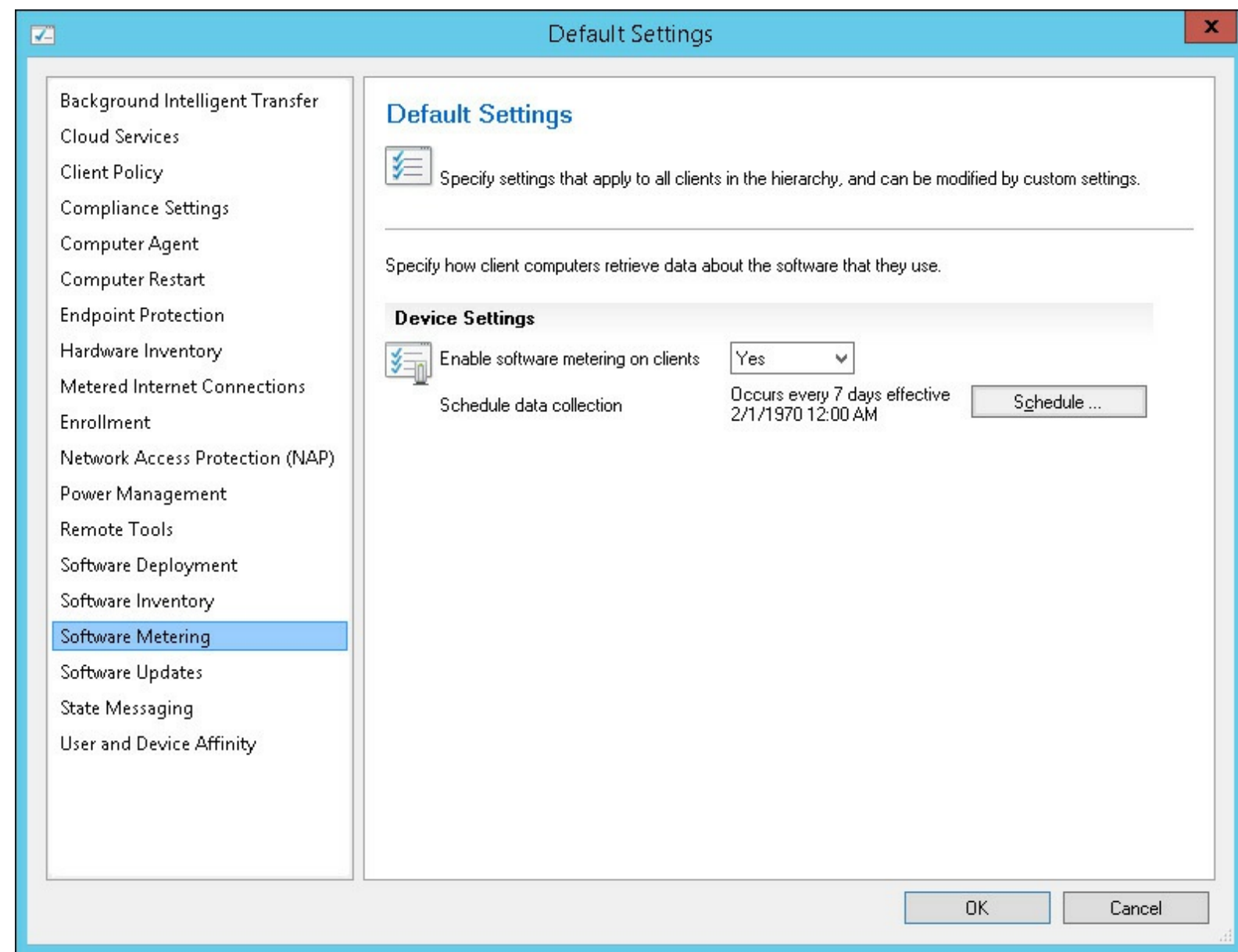
FIGURE 6-9 Software Metering

The software-metering process includes the following steps:

1. The Software Metering Agent examines each program that runs on the client and determines whether the program file's information matches any software-metering rule. The agent collects usage data every time an actively monitored program runs on the client, regardless of whether the client is connected to the network.

2. The agent uploads the data to the management point on its next software metering usage report cycle. If the client is not connected to the network, the data remains on the client and then uploads to the management point the next time the client connects to the network.

3. The management point forwards the data to the site server.

4. The site server adds the data to the site database.

> *More Info:* **Software Metering**
>
> **You can learn more about software metering at _http://technet.microsoft.com/en-us/library/gg682205.aspx_.**

Software-metering rules

When you create a new rule, you can specify the site to which the rule applies and whether the rule should affect only the specified site or all clients in the hierarchy. By default, rules apply either to the site in which you define them or to all sites if you define them in the central administration site.

To create a software-metering rule, perform the following steps:

1. In the Configuration Manager console, click the Software Metering node of the Assets And Compliance workspace.

2. On the ribbon, click Create Software Metering Rule.

3. On the General page of the Create Software Metering Rule Wizard, specify the details of the application you wish to meter. Figure 6-10 shows a metering rule configured for Notepad.exe. You can browse to the application location to have these properties populated automatically.
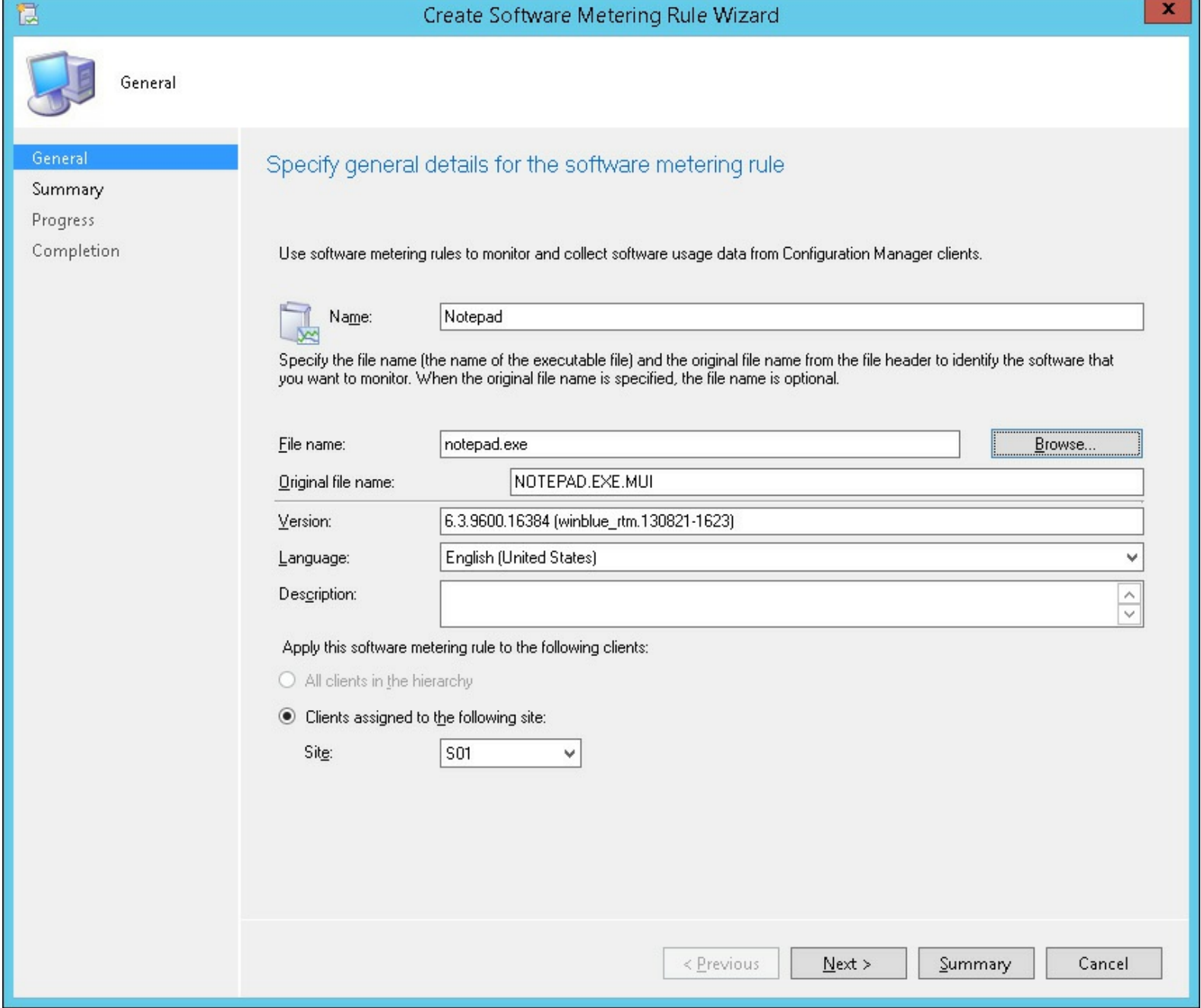
FIGURE 6-10 Create Software Metering Rule Wizard

    4. Complete the wizard to create the rule.

    Automatic software-metering rule creation enables you to specify the percentage of client computers in the hierarchy that must have the application installed before a rule is automatically created. The default value is 10 percent. You can configure a maximum number of software-metering rules that can be automatically created; the default is 100. You can configure automatic software-metering rule creation in the Software Metering Properties dialog box, which is accessible through the Assets And Compliance workspace of the Configuration Manager console. shows the Software Metering Properties dialog box.
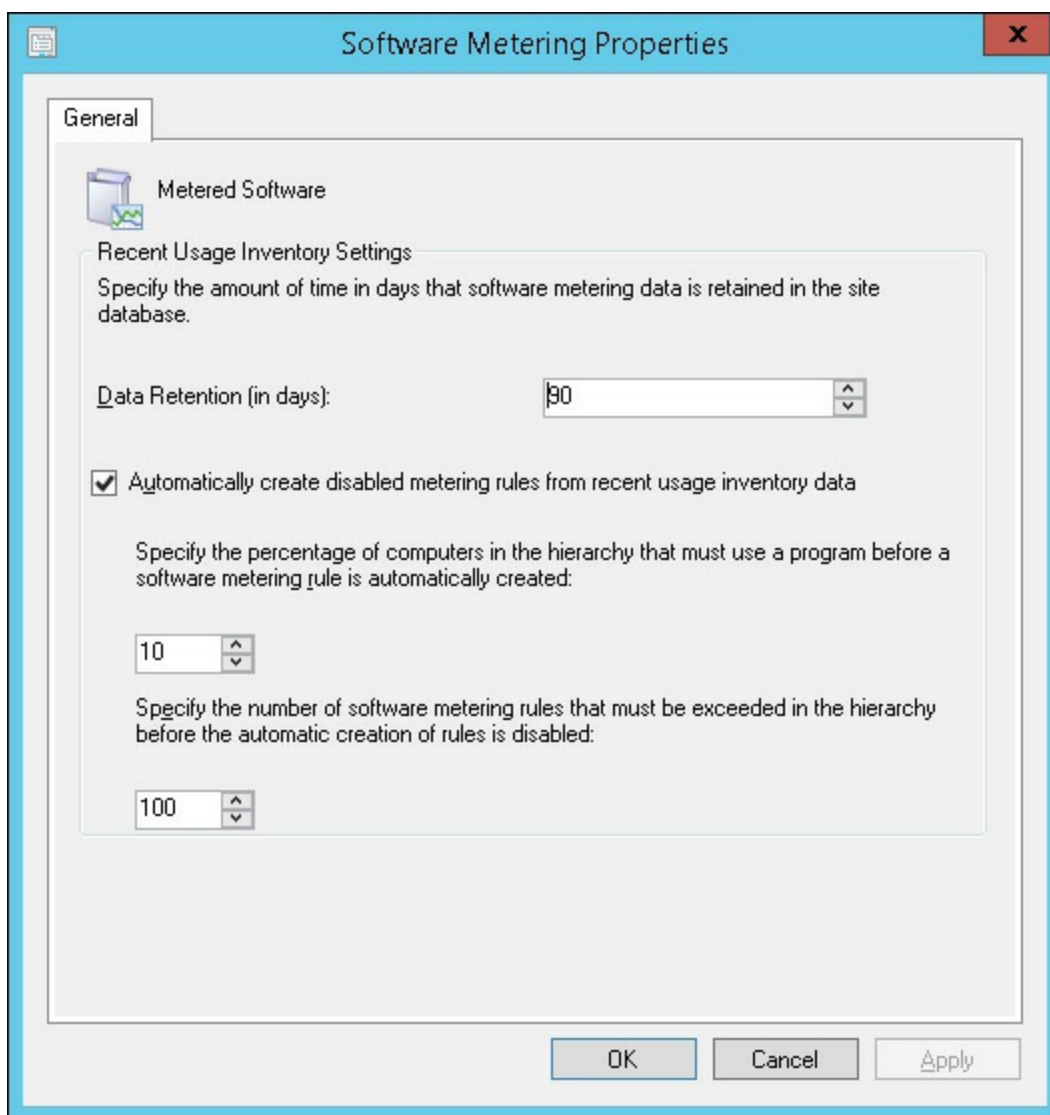
FIGURE 6-11 Software Metering Properties

More Info: **Automatic Rule Creation**

You can learn more about automatic software-metering rule creation at
http://technet.microsoft.com/en-us/library/hh427343.aspx.

Exam Tip

Remember how to configure automatic rule creation.

Manage software-metering tasks

Software-metering data is summarized on a specified schedule and then replicates to the central
administration site, which contains usage data from all client computers within the hierarchy. After
the site server summarizes client data, you can view the information by using queries and reports.
This data, combined with data from software inventory and Asset Intelligence, can assist your
organization in determining its software usage.

Configuration Manager includes a number of site-maintenance tasks to help you manage the usage

data that software metering collects. These tasks are responsible for summarizing software-metering data and deleting aged software-metering data. These summarization tasks summarize data to reduce the amount of data that the Configuration Manager site database stores.

Data summarization runs daily and only runs against usage data that is older than 12 hours. Data summarization is required for all Configuration Manager software-metering reports to display meaningful data.

You can use the RunMeterSumm.exe tool to initiate an off-cycle summarization of software-metering data. You can obtain this tool from the Configuration Manager toolkit.

If you want to understand what data the most current set of summary data contains, you should know when the summarization last occurred. You can refer to the software-metering summarization progress report in Configuration Manager to determine when summarization last occurred.

The software-metering summarization tasks are:

- **Summarize Software Metering File Usage Data** The Summarize Software Metering File Usage Data task condenses software-metering file usage data from multiple records into one general record. This record provides information about the program name, version, language, and number of distinct users over intervals of 15 minutes and 1 hour. This process compresses and optimizes the amount of data stored in the Configuration Manager site database. By default, the Summarize Software Metering File Usage Data task runs daily. For every hour and every 15-minute interval within the hour, the task calculates the total number of distinct user/computer combinations that are running the matching program. Within the 15-minute intervals, this approximates the number of concurrent users. For example:

  - If a single user is using a software program and signs in to three computers simultaneously, this counts as three usages.

  - If three users sign in to a computer that is running Terminal Services or Remote Desktop Services, and all three are running the software program, this counts as three usages.

  - If a single user starts and stops the software program on the same computer three times during the hour, this counts as one usage for that user.

- **Summarize Software Metering Monthly Usage Data** This task condenses detailed software-metering usage data from multiple records into one general record. This record provides information about the program name, program version and language, program running times, number of usages, last usage, user name, and computer name. Data summarization helps compress the amount of data in the Configuration Manager site database. Monthly software usage data replicates to the central administration site. The summarization information includes the number of times each matching software program runs on a particular computer and by a particular user during the month. By default, the task runs daily, and the summarization period is one month.

The following maintenance tasks remove old software-metering data and summarized data from the Configuration Manager site database:

- **Delete Aged Software Metering Data** This task deletes all unsummarized software-metering data that is older than the number of days specified. By default, the task runs every day and deletes software-metering data that is older than five days. You can configure the number of days to be anywhere from 2 to 255 days.

- **Delete Aged Software Metering Summary Data** This task deletes summarized software-metering summary data that is older than the number of days specified. By default, the task runs every Sunday to delete software-metering summary data that is older than 270 days.

Thought experiment: **Software metering at Fabrikam**

You are the Configuration Manager administrator at Fabrikam. You've been trialing Configuration Manager's software-metering functionality, but you've found that the default configuration does not suit your needs. Specifically, you want to use it to find out how many people are running a specific graphics application that you want to retire. You also want to reduce the number of automatically created rules so that they are only generated if a substantial number of people are using an application. With this in mind, answer the following questions:

1. **How can you determine the number of people who are running the graphics application, given that it's likely to be used by less than 10 percent of people in the organization?**

2. **What steps can you take to reduce the number of automatically created rules and limit rule creation to when more than 30 percent of client computers in your organization use an application?**

Objective summary

- Software metering records how many instances of a particular software program users are using.
- Software metering records when the application was run, who ran it, and how long they were running it.
- Maintenance tasks remove software-metering data and summary data after specified periods.

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 want to ensure that aged software-metering summary data is stored for 365 days. Which of the following tasks would you modify to accomplish this goal?

   A. Summarize Software Metering File Usage Data

   B. Summarize Software Metering Monthly Usage Data

   C. Delete Aged Software Metering Data

   D. Delete Aged Software Metering Summary Data

2. You want to ensure that software-metering data is deleted only after 28 days. Which of the following tasks would you modify to accomplish this goal?

A. Delete Aged Software Metering Summary Data

B. Delete Aged Software Metering Data

C. Summarize Software Metering Monthly Usage Data

D. Summarize Software Metering File Usage Data

3. You want to track which users are running a specific application and how often they are running that application. Which of the following Configuration Manager features would you take advantage of to accomplish this goal?

A. Software inventory

B. Software metering

C. File collection

D. Asset Intelligence

4. By default, on what percentage of Configuration Manager client computers in the hierarchy must an application be launched before a software-metering rule is automatically created to track its use?

A. 5 percent

B. 10 percent

C. 20 percent

D. 25 percent

Objective 6.3: Create reports

The reporting functionality in Configuration Manager enables you to view and manipulate the information that it has collected about client devices in your organization. The Asset Intelligence functionality of Configuration Manager enables you to identify precisely which software is running on managed client devices.

This section covers the following topics:
- Queries
- Configuration Manager reporting
- Managing reports
- Asset Intelligence

Queries

A query is a specific set of instructions that extract information about a defined set of objects. You can use a query in Configuration Manager to obtain almost any information from the site database. This includes items such as specific types of computers, user groups, sites, collections, and applications. You also can query your database for information such as the number of clients that have free space of less than 5 GB and the number of clients in a particular site. One caveat is that the inventory information in the database is as current as the last inventory cycle. You might run a particular query to locate a computer that could have changed since the last inventory. Therefore, because the computer no longer meets the criteria of the query, it will not appear in the query results.

You build queries in Configuration Manager in the WMI Query Language (WQL), which is based on Windows Management Instrumentation (WMI). WMI is similar to Structured Query Language (SQL). You can use preconfigured queries or create your own custom queries to search the site database. When creating custom queries in Configuration Manager, you can use the Query Statement Properties in the Create Query Wizard in design mode to choose the components of your query, or you can use Query Statement Properties in the query language mode to type your own WQL queries.

Although design mode provides an easier interface to use when creating queries, you cannot create all queries by using design mode. For instance, when using aggregation commands in WQL, you can view and manage the query only in query language mode.

You can perform two types of queries in Configuration Manager:

- **Data queries** You can use data queries for extracting information that relates to resource discovery or inventory data. In general, the primary purpose of data queries is to build collections.
- **Status message queries** This type of query has a very specific use. The Site Status and Component Status nodes show you status messages that relate to a specific site system or component. Although there are some filtering options, these might not be sufficient when troubleshooting an issue. Therefore, you can use status message queries to create custom queries that return status messages, including from clients. The primary purpose of status message queries is to locate stored status messages.

You can use queries in Configuration Manager to search the site database for any object. All objects have attributes and values that you can query. However, not all objects have the same attributes and values. For example, both user resources and system resources have a name; however, user resources do not have installed software.

Every object type is defined by a set of attribute classes, which are further defined by individual attributes. For example, the System Resource object type is defined by attribute classes such as processor, disk drives, and installed software. Together, these characterize the discovery data and inventory data of a system resource. These attribute classes have their own unique attributes. The attributes define the values stored in the database, such as current clock speed for processors or partitions for disk drives.

Most object types, such as the Site object type, have only one attribute class and few attributes, whereas the System Resource object type has more than 200 attribute classes and thousands of attributes. Attribute classes are directly related to SQL Server tables and Web-Based Enterprise Management (WBEM) classes. In database terms, the attribute class represents a table, the attributes represent the column headers, and the actual data collected is stored in the rows.

Queries search against only one object type at a time. By default, Configuration Manager queries the System Resource object type.

Configuration Manager has 28 object types, as shown in Table 6-4.

Configuration Manager Object Types

■ Application Conflicts Data	■ Application Dependency Data	■ Application Deployment Asset Details
■ Application Deployment Error Asset Details	■ Application Deployment Error Status	■ Application Deployment Requirement Not Met Asset Details
■ Application Deployment Status	■ Application Requirement Not Met Status	■ Application Requirement Data
■ Collection Data Point	■ Deployment	■ Deployment Asset Details
■ Deployment Summary Per Collection	■ Endpoint Protection Dash Board Data Point	■ Failed VE Data
■ IP Network	■ Package	■ Program
■ Program Deployment Asset Details	■ Program Deployment Status	■ Security Roles
■ Security Scopes	■ Site	■ Software Metering Rule
■ System Resource	■ Unknown Computer	■ User Group Resource
■ User Resource		

TABLE 6-4 Configuration Manager object types

In addition, there is an Unknown Computer object for the All Unknown Computers collection that is used in operating system deployment. You can create queries by using the Unknown Computer object type; however, you must write out the query in WQL.

A valid query includes the following elements:

■ A unique query name that identifies the query

■ Object type

■ Attribute class

■ Attribute

When you create a query, the only requirement is that you specify a unique name for your query. The object type is set to the System Resource object type by default, and all attribute classes and attributes have default values. However, by including specific object types, attribute classes, and attributes, you can ensure that you do not have an overly large number of results, which can be unwieldy.

If you use the default values and your default query returns a large number of attributes, you can limit the number of attributes that appear. To do this, perform the following steps:

1. In the Query Properties dialog box, click Edit Query Statement.

2. In the Query Statement Properties dialog box, on the General tab, configure the attributes that you want to view in the results.

If you want to restrict the results that are returned to only attributes with specific values, use the Criteria tab to specify the attribute class and attribute along with the value that you want to find. You do not need to use the same attributes on the General tab that you use on the Criteria tab. For example, on the General tab, you might include attributes such as Computer Name or IP Address to identify specific computers. However, your criteria could be to restrict the results to a specific driver version.

If your query includes attributes from more than one attribute class, you can join or link the attribute classes so the displayed data for each accurately relates to that for the other. When you select an attribute on either the General tab or the Criteria tab, Configuration Manager creates a suitable join for the attribute class automatically. For example, if you build a query to display all computers with 4 gigabytes (GB) of random access memory (RAM) and with Microsoft Office installed, the data is joined automatically because both tables have a key field that identifies the device from which the data was collected. For advanced queries, you can use the Joins tab to link attributes manually from multiple attribute classes.

Configuration Manager reporting

For reporting to function in Configuration Manager, you must install a SQL Server Reporting Services (SSRS) server that is running the same version of SQL Server as the site database server. You can use any supported version of SQL Server:

- SQL Server 2008 Service Pack 2 (SP2) with cumulative update (CU) 9 or newer
- SQL Server 2008 SP3 with CU 4 or newer
- SQL Server 2008 R2 with SP1 and CU 6 or newer
- SQL Server 2008 R2 with SP2
- SQL Server 2012 with CU 2 or newer
- SQL Server 2012 SP1
- SQL Server 2014

You can install SSRS on the site server or on a remote site system. However, for optimal performance, you should install SSRS on a remote site system server.

There are prerequisites before you can install SSRS:

- The user account that you use to run setup must be a member of the local Administrators group and have rights to create databases on the server running SQL Server that is hosting the SSRS databases.
- The computer account for the Configuration Manager server must be in the local Administrators group on the SSRS server. Configuration Manager connects to Reporting Services to configure security rights for users. You should not configure SQL Server security rights when you integrate Configuration Manager reports with SSRS.
- When installing SSRS, you must have a SQL Server database engine installed in the same instance.
- Check for interoperability issues. To use the default configuration for SSRS Native Mode, setup must be able to use the following default settings:
  - Port 80

- Virtual directory names ReportServer_instance_name and Reports_instance_name
- Default databases named ReportServer and ReportServerTempDB

After you install SSRS, you can configure a reporting services point. To configure SSRS, the simplest option is to install SSRS by using the default configuration for native mode. When you use this option, the SSRS server is ready to use after installation. Default installation configures the following:

- Service account for the Report Server service
- Report Server Web service URL
- Report Manager URL
- Report Server database
- Service account access to the report server databases
- Data source name (DSN) connection for the report server databases

Default installation does not configure the unattended execution account, report server email settings, or scale-out deployment settings. You should back up the encryption keys after you have completed the installation.

If you choose to install in the files-only mode, then before you can use the reporting services point, you first must manually configure SSRS. After installing SSRS, you would configure it by using the Reporting Services Configuration Manager, shown in Figure 6-12.
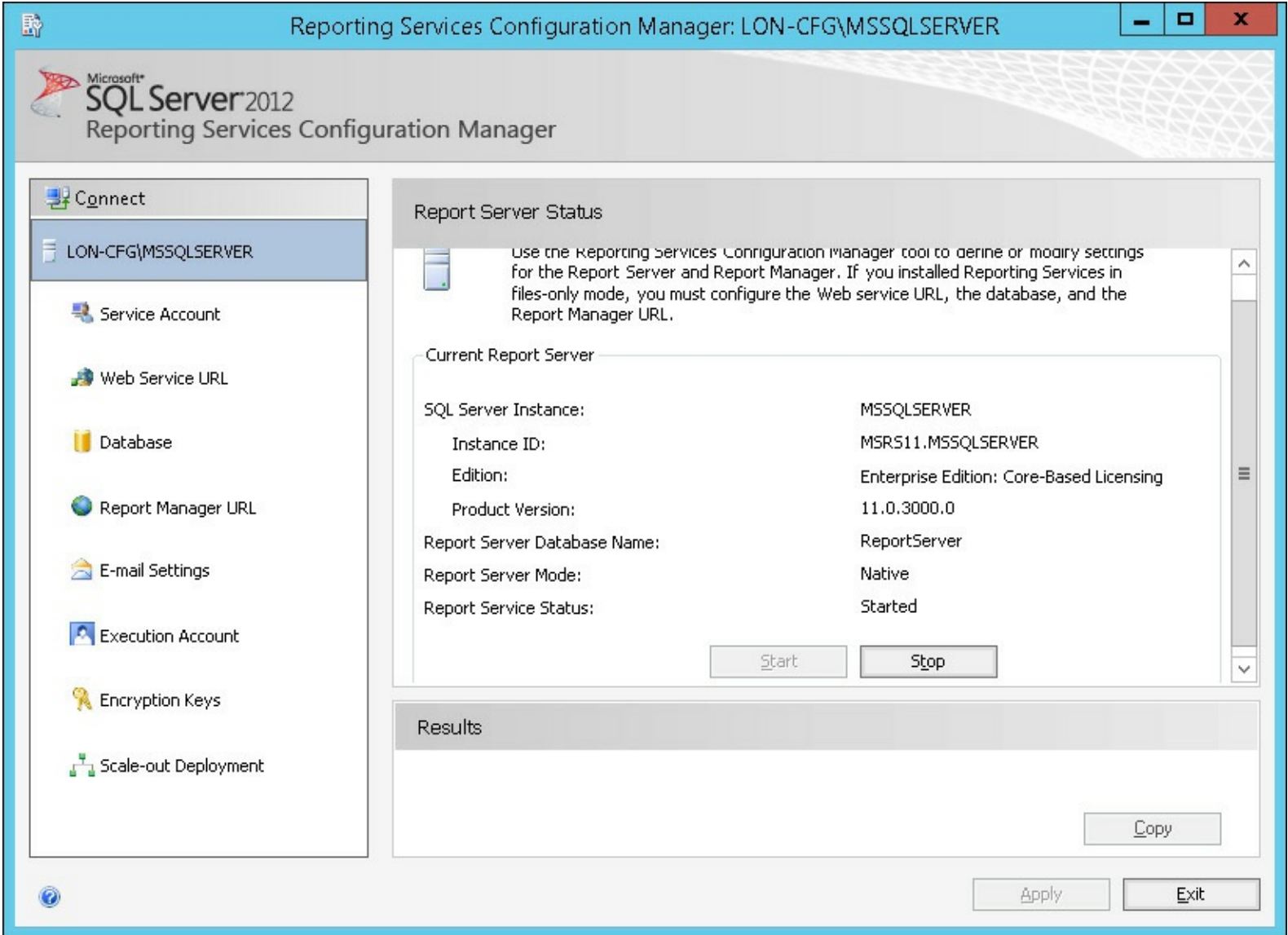
FIGURE 6-12 Reporting Services Configuration Manager

When running the Reporting Services Configuration Manager, you first must specify the server name and instance that you are managing. After you connect to the server, you must configure the nodes as described in .

Node	Description
\<Server Name\> \\\<Instance Name\>	This node displays a summary of the current configuration and the status of the service.
Service Account	This node enables you to change the service account that was set during SSRS installation.
Web Service URL	During the initial configuration, you click the Apply button to accept the default settings, or you can change the default settings before clicking Apply.
Database	In this node, you click the Change Database button to specify the database that SSRS should use.
Report Manager URL	During the initial configuration, you click the Apply button to accept the default settings, or you can change the default settings prior to clicking Apply.
Email Settings	This is an optional setting. If you will use report subscriptions through email, you must configure a sender address and a Simple Mail Transfer Protocol (SMTP) server.
Execution Account	This account enables you to use report-data sources that require credentials or to connect to remote servers that store external images such as custom icons.
Encryption Keys	This node enables you to back up or restore the encryption keys that SSRS uses.
Scale-out Deployment	This node displays the status of a scale-out deployment of SSRS in which multiple SSRS servers share a common reporting database.

TABLE 6-5 Reporting services configuration

More Info: **SQL Server Reporting Services**

You can learn more about SQL Server Reporting Services at *http://technet.microsoft.com/en-us/library/bb934490(v=sql.110).aspx* and *http://technet.microsoft.com/en-us/library/ms156305(v=sql.110).aspx*.

Managing reports

Configuration Manager includes more than 400 reports. They are displayed in the Configuration Manager console as shown in Figure 6-13 and are organized into more than 50 subfolders based on the category of the report.
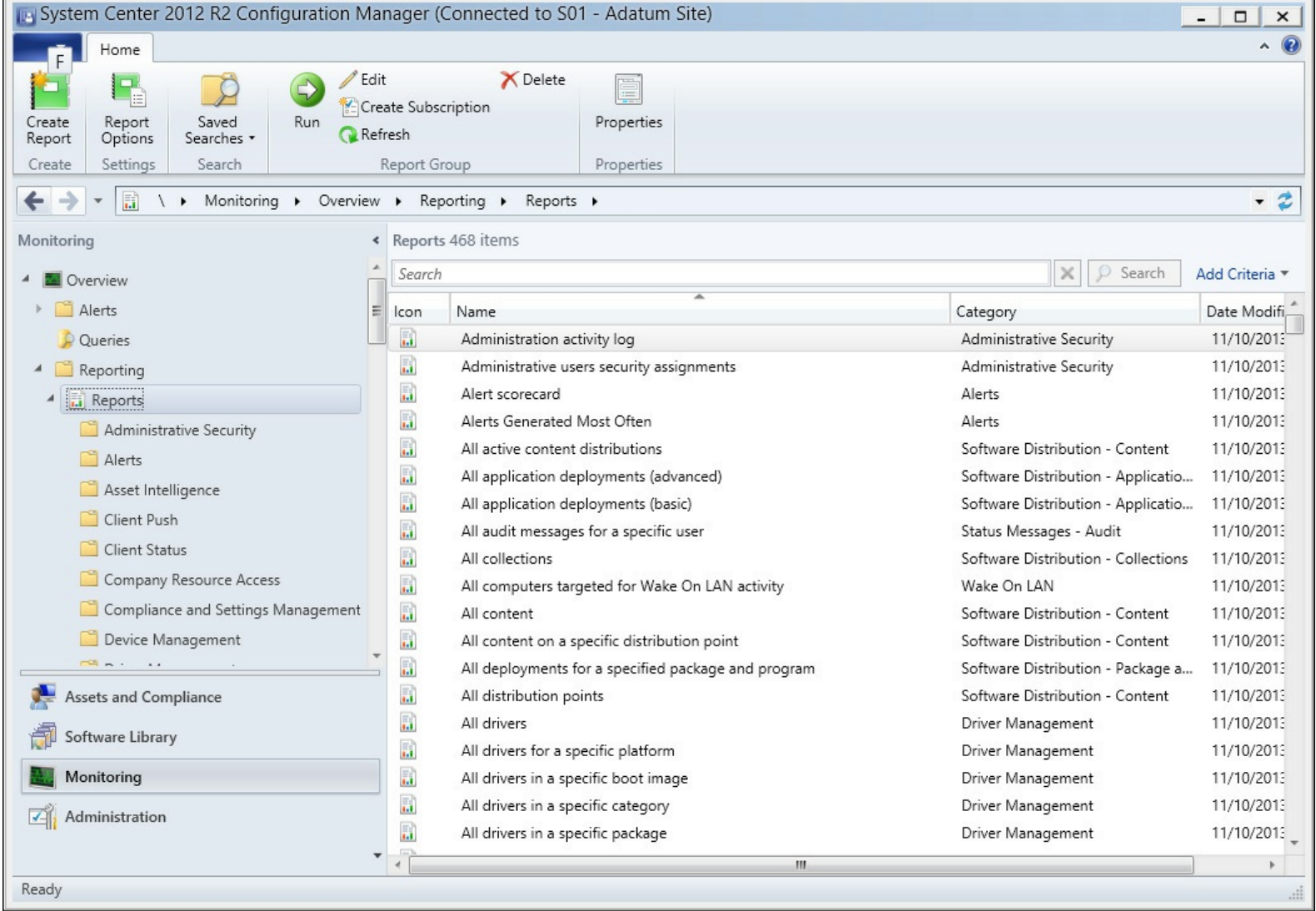
FIGURE 6-13 Configuration Manager Reports node

When you run the Create Report Wizard, you select whether you want to create a Model-Based Report or an SQL-Based Report. Figure 6-14 shows the Create Report Wizard.
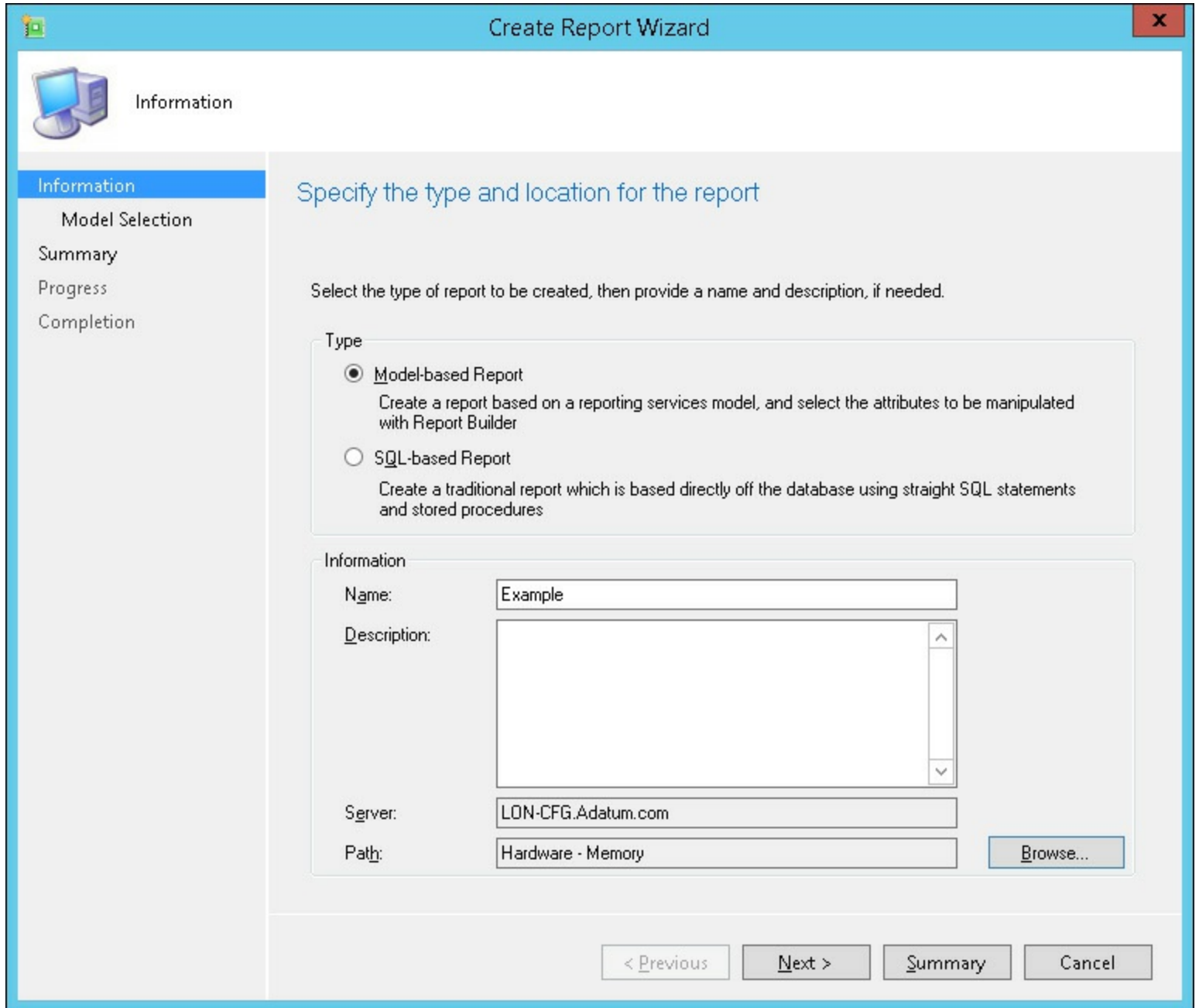
FIGURE 6-14 Create Report Wizard

If you select Model-Based Report, you will be asked to select the reporting services model on which to base the report, and the Microsoft SQL Server Report Builder will run as shown in . If you choose SQL-Based Report, the report builder is launched without selecting a model.
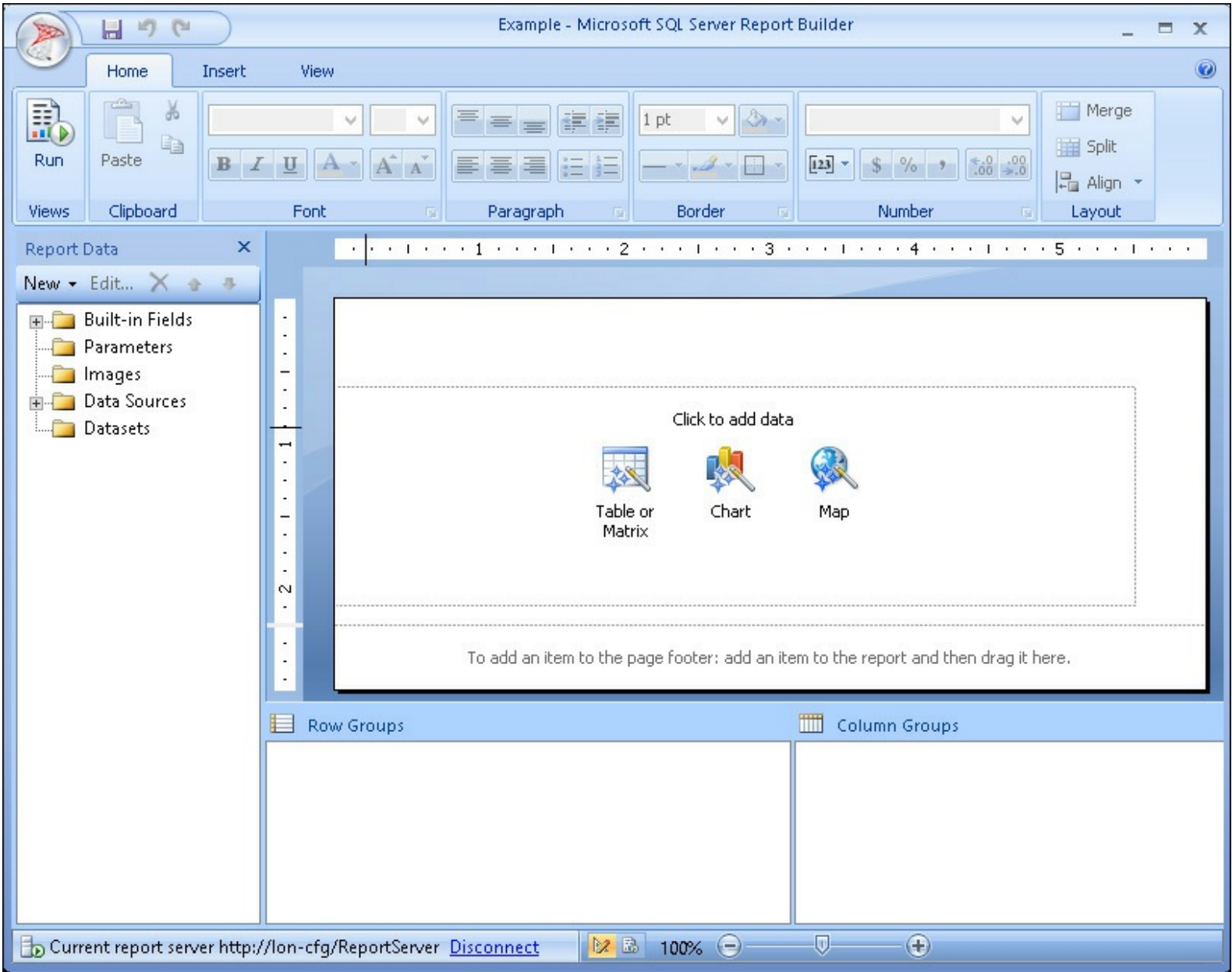
FIGURE 6-15 SQL Server Report Builder

SQL Server Report Builder also runs if you choose to edit an existing report. You can edit a report by selecting it within the Configuration Manager console and clicking Edit on the console ribbon. You can create a clone of a report by editing the report and then saving it with a new name by using SQL Server Report Builder. You also can use Save As functionality to export an existing report.

To import a report, navigate to the Reporting Services webpage, which is located at *http://server/reports*, using an account that has permission to edit reports. Navigate to the folder into which you want to upload the report and then click Upload File. On the Upload File page, shown in Figure 6-16, browse to the report file in .rdl format and click OK. You also can use the Reporting Services webpage to add folders in which to store Configuration Manager reports.
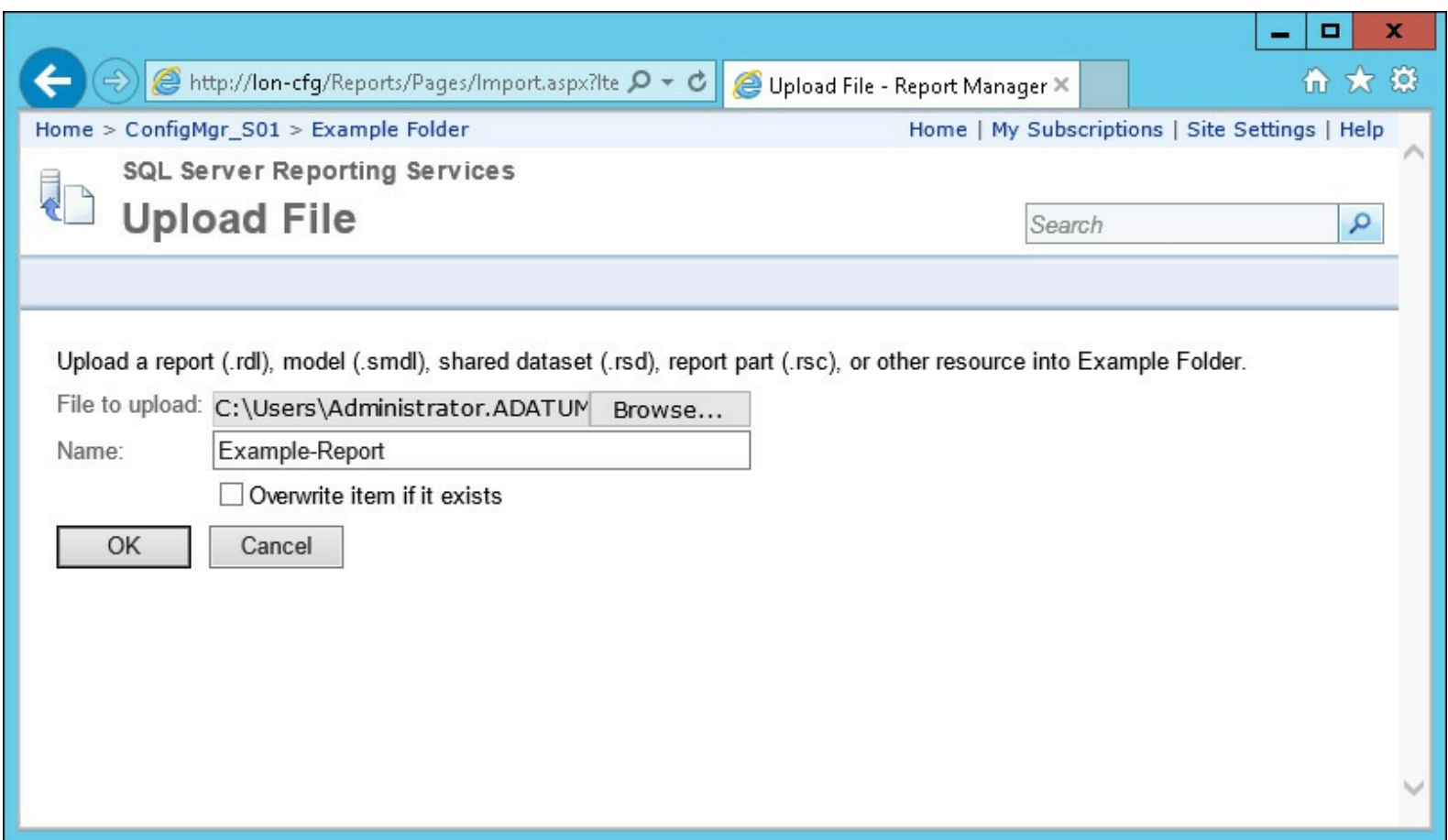
FIGURE 6-16 Upload report

More Info: **Managing Reports**

You can learn more about managing Configuration Manager reports at
http://technet.microsoft.com/en-us/library/dn581948.aspx.

 Exam Tip

Remember what steps you need to take to clone and import a report.

Asset Intelligence

Asset Intelligence enhances the inventory capabilities of Configuration Manager by extending hardware inventory and adding functionality for license reporting. By enabling additional hardware-inventory WMI reporting classes, Asset Intelligence helps improve the range of information that it gathers about software titles in use.

Asset Intelligence offers the following benefits over software inventory:

- Enables more accurate representation of software titles that are present on managed computers
- Provides information about the license usage for specific products rather than just information about the software itself
- Can be used in conjunction with software metering to rationalize licensing by determining instances when software has deployed but is not being used

■ Retrieves information about installed software through the hardware inventory client agent after the software inventory agent detects software titles by scanning client storage

Asset Intelligence reports are divided into three main areas: hardware, license, and software. Asset Intelligence presents a picture of how software is used in your environment, for example, by finding which systems cannot upgrade a software package and finding installed software that is not being used.

Table 6-6 lists some of the Asset Intelligence reports.

Name	Inputs	Description
Hardware 04A – Shared (multi-user) Computers	■ Collection	This report lists computers that do not seem to have a primary user because no one user has a percentage of console logon time greater than 66 percent.
Hardware 08A – Hardware That Is Not Ready For A Software Upgrade	■ Collection ■ Product	This report displays hardware that does not meet the minimum hardware requirements.
Hardware 10A – Computers In A Specified Collection That Have Changed During A Specified Timeframe	■ Collection ■ Name of the changed class (All = All classes) ■ Objects added to the database ■ Objects deleted from the database ■ Objects updated in the database ■ Start date of the change window ■ End date of the change window	This report displays a list of computers in a specified collection in which a hardware class has changed during a specified timeframe. The objects added/deleted/updated inputs are set to either yes or no to include or exclude those objects from the report.
License 01A – Microsoft Volume License Ledger For Microsoft License Statements	■ Collection ■ Channel Code	This report displays an inventory of all Microsoft software titles that are available from the Microsoft Volume Licensing program.
License 03A – Count Of Licenses By License Status	■ Collection ■ Product Name	This report lists the products whose licenses are managed by the Software Licensing Service.
License 15A – General License Reconciliation Report	■ Collection	This report provides reconciliation of general software licenses purchased and the actual inventory count.
Software 01A – Summary Of Installed Software In A Specific Collection	■ Collection ■ Publisher ■ Maximum rows to return	This report provides a summary of installed software, which is ordered by the number of instances found from inventory.
Software 03A – Uncategorized Software	■ Collection	This report lists the software that either is categorized as unknown or has no categorization.
Software 09A – Infrequently Used Software	■ Collection ■ Days not used	This report displays software titles that have not been used during a specified period of time.

TABLE 6-6 Important Asset Intelligence reports

Asset Intelligence components include:

■ **The Asset Intelligence catalog** Asset Intelligence relies on a set of database tables, which

contain software identification, categorization information, and hardware requirements for software titles. Collectively, these tables are the Asset Intelligence catalog and are stored within the site database. The Asset Intelligence catalog can provide data for reports on installed software titles, organize the information within software categories and families, and provide a predefined set of hardware requirements for the software titles. You also can customize the organization of your information by creating custom software categories and families and adding new user-defined hardware requirements for specific software titles. By using an Asset Intelligence synchronization point, you can download periodic updates dynamically from Microsoft to the Asset Intelligence catalog. These updates contain information about newly released or validated software.

- **Asset Intelligence synchronization point** This is a Configuration Manager site system role that you can use to connect to System Center Online, an online service that Microsoft hosts. From there, you can download Asset Intelligence catalog updates. You can either schedule or manually initiate catalog synchronization. You also can use the Asset Intelligence synchronization point to upload custom software title information to System Center Online. Microsoft then categorizes it.

- **Asset Intelligence home page** The Asset Intelligence node in the Asset And Compliance workspace displays a summary dashboard of Asset Intelligence information. It includes summaries of the Asset Intelligence component status, the catalog synchronization status, and inventoried software status.

- **Asset Intelligence reports** More than 50 reports present Asset Intelligence information in a simplified format. Many of these reports link to more specific reports, which enable you to query for general information and procure detailed information. Report categories include hardware, license management, and software.

The Asset Intelligence catalog contains information for more than 500,000 software titles and versions, representing more than 20 families and 90 specific categories. The Asset Intelligence catalog includes the following:

- Support for manually importing software license information for software titles in use, including both Microsoft and non-Microsoft titles
- Hardware requirements for many software titles in the catalog
- Support for adding custom software categories, families, and software labels
- Support for uploading software title information to the System Center Online service, which then categorizes it

You can review contents of the Asset Intelligence catalog and customize certain elements by clicking the Asset Intelligence folder in the Assets And Compliance workspace of the Configuration Manager console. The Asset Intelligence folder includes the following nodes:

- **Catalog** Includes most of the catalog segments that administrators can update:
  - **Software Categories** Asset Intelligence software categories broadly classify inventoried software titles. By default, there are a number of predefined software categories, including line-of-business (LOB), original equipment manufacturer (OEM), and Office Suites And Productivity. You can create additional user-defined categories to classify inventoried software further.

- **Software Families** Asset Intelligence software families further define inventoried software titles. By default, the Asset Intelligence catalog includes approximately 20 predefined software families. Some examples of these predefined software families are Components And Peripherals, Equipment, Home And Entertainment, Industry Specific, Line Of Business, and Productivity And Viewers. You can create additional user-defined software families to classify inventoried software further.
- **Custom Labels** Custom labels enable further classification of inventoried software according to attributes that administrators define. For example, you might create a custom label known as Shareware and associate that label with inventoried shareware titles. You then can run a report to display all software titles that have the custom label Shareware associated with them.

- **Inventoried Software** The list of inventoried software titles includes information about software that the hardware inventory agent reports. This node displays the following information by default for each inventoried software title:
  - **Product Name** The name of the inventoried software
  - **Publisher** The name of the vendor that developed the software
  - **Version** The product version of the software title
  - **Category** The currently assigned software category
  - **Family** The currently assigned software family
  - **Label (1, 2, and 3)** The custom labels that have been assigned with the software title, to a maximum of three
  - **Software Count** The number of Configuration Manager clients that have inventoried the software title
  - **State** The validation state for the software title

- **Hardware Requirements** You can use Asset Intelligence hardware requirements to help verify that computers meet hardware requirements for software titles before you target the computers for deployment. Asset Intelligence retrieves from its catalog the hardware requirements that display in the Configuration Manager console. The list is not based on inventoried software title information from Configuration Manager clients. You can add, modify, or delete custom hardware requirements for software titles that the Asset Intelligence catalog does not predefine. However, existing noncustom hardware requirement information that the Asset Intelligence catalog stores is read-only, which means you cannot modify or delete it. The following information appears for each listed hardware requirement:
  - **Software Title** The software title name with which the hardware requirement is associated.
  - **Minimum CPU (MHz)** The minimum central processing unit (CPU) speed, in megahertz (MHz), that the software title requires.
  - **Minimum RAM (KB)** The minimum random access memory (RAM), in KB, that the software title requires.
  - **Minimum Disk Space (KB)** The minimum free disk space, in KB, that the software title requires.

- **Minimum Disk Size (KB)** The minimum hard-disk size, in KB, that the software title requires.
- **Validation State** The validation state for the hardware requirement. Valid states include Validated and User defined.

In System Center 2012 R2 Configuration Manager, Asset Intelligence supports the mandatory software identification tags specified in the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 19770-2 standard. These tags include authoritative data that Configuration Manager can use to identify software installed on client computers. Because the tags are standardized, an increasing number of software vendors include them in their applications. If you want Configuration Manager to use mandatory software identification tags, you must enable the SMS_SoftwareTag Asset Intelligence Hardware Inventory reporting class.

In System Center 2012 R2 Configuration Manager, Asset Intelligence collects information about Microsoft Application Virtualization 5.0 and Application Virtualization 4.0 applications even though these applications run through the Microsoft Application Virtualization (App-V) client and are not installed on the client computer in a traditional manner.

You must configure several settings and tasks so that Asset Intelligence performs optimally. These settings include:

- **Enable Hardware Inventory** Asset Intelligence reports depend on information that the hardware inventory agent collects. Ensure that you enable the hardware inventory agent on clients.
- **Enable Software Metering** The following Asset Intelligence reports depend on the Software Metering Client Agent to provide the following data:
  - Software 07A - Recently used executables by number of computers
  - Software 07B - Computers that recently used a specified executable
  - Software 07C - Recently used executables on a specific computer
  - Software 08A - Recently used executables by number of users
  - Software 08B - Users who recently used a specified executable
  - Software 08C - Recently used executables by a specified user
- **Enable Asset Intelligence Inventory Reporting Classes** To enable the Asset Intelligence Inventory reporting classes, right-click the Asset Intelligence node and then click Edit Inventory Classes. You can enable the Asset Intelligence reporting classes that you need per the type of reporting that you require. Note that from within the Edit Inventory Classes dialog box, as you point to each reporting class, a tooltip displays information about the reports that depend on each reporting class.
- **Enable Windows Event Log Settings** Several Asset Intelligence reports rely on information that Windows security event logs gather on client computers. To support these reports, you must modify the event-log settings for Windows security on clients so that it logs all Success logon events. These reports include:
  - Hardware 03A - Primary computer users
  - Hardware 03B - Computers for a specific primary console user
  - Hardware 04A - Computers with multiple users (shared)

■ Hardware 05A - Console users on a specific computer

■ **Import Software License Information** Use the Import Software Licenses Wizard to import Microsoft Volume License Statements and General License Statements from non-Microsoft vendors into the Asset Intelligence catalog.

■ **Install An Asset Intelligence Synchronization Point** The site system role for the Asset Intelligence synchronization point connects to System Center Online to download and synchronize Asset Intelligence catalog information. You must install this role on a site system in the central administration site for hierarchy configurations. This requires Internet access using Transmission Control Protocol (TCP) port 443. You can configure a synchronization schedule, which by default is set to run every seven days.

■ **Configure Asset Intelligence Maintenance Tasks** By default, the Asset Intelligence feature uses two maintenance tasks:

   ■ **Check Application Title With Inventory Information** This task reconciles the software title in the software inventory reports with the software title in the Asset Intelligence catalog.

   ■ **Summarize Installed Software Data** This task provides information that displays in the Inventoried Software node. This task is available only on primary sites.

■ **Configure Asset Intelligence Security** You can use the Asset Manager Security role to provide the required permissions to manage the Asset Intelligence synchronization point and to modify the Asset Intelligence reporting classes and permissions related to software inventory, hardware inventory, and software metering.

Maintaining and managing Asset Intelligence involves a number of tasks, including:

■ **Viewing Asset Intelligence information that Asset Intelligence reports collect from clients** You can run Asset Intelligence reports to view the most detailed information that the Asset Intelligence feature collects. Asset Intelligence reports are as follows:

   ■ **Hardware reports** Provide information about hardware assets within your organization, including age and upgrade readiness

   ■ **License management reports** Provide information about licensing, including number of licenses in use, sales channels, and time until expiration

   ■ **Software reports** Provide information about software families, categories, and specific software titles installed on your organization's computers

■ **Updating the Asset Intelligence catalog** To request synchronization manually, in the Configuration Manager console, click the Assets And Compliance workspace and then click Asset Intelligence. Right-click Asset Intelligence, point to Synchronize, and then click Synchronize Asset Intelligence Catalog. You may request manual synchronization only once every 12 hours.

■ **Requesting software categorization** You can submit uncategorized software title information for research and categorization. After you submit an uncategorized software title, Microsoft researchers identify, categorize, and then make the software title categorization information available to all customers who are using the System Center Online service. The following information applies to software title information that is submitted for categorization:

   ■ System Center Online receives only basic software title information. You can review the

software title information before Microsoft researchers categorize and submit it.

- Submitting software titles for categorization does not transmit any license information.
- Software title information that you upload becomes available publicly as part of the Microsoft System Center Online Services catalog. Other customers then can download it.
- Microsoft System Center Online Services does not record the source of the submitted software. However, you should not submit application titles for categorization that contain confidential or proprietary information.

- **Resolving software details conflicts** If an Asset Intelligence catalog categorization value conflicts with information downloaded from System Center Online, a software details conflict occurs. You can use the Asset Intelligence Software Details Conflict Resolution dialog box to select a conflict resolution action.

More Info: **Asset Intelligence**

You can learn more about Asset Intelligence at *http://technet.microsoft.com/en-us/library/gg699382.aspx*.

Thought experiment: **Asset Intelligence at Adatum**

You are piloting the Configuration Manager Asset Intelligence feature at Adatum. You are interested in going beyond the reports that are included in the product by default. You also have some concerns about some data from System Center Online, which you want to correct for your local deployment. With this information in mind, answer the following questions:

1. **Which tool can you use to create a brand new report based on Asset Intelligence data?**
2. **An Asset Intelligence catalog categorization value conflicts with information downloaded from System Center Online. What can you do to resolve this issue?**

Objective summary

- Software metering enables you to track how often a particular application is used.
- Automatic software metering rule creation enables you to specify the percentage of client computers in the hierarchy that must have the application installed before a rule is automatically created.
- Software-metering data is summarized on a specified schedule and then replicates to the central administration site, which contains usage data from all client computers within the hierarchy.
- Data summarization runs daily and only against usage data that is older than 12 hours.

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 of the following tools could you use to import a report in RDL format so that it can be used in Configuration Manager?

   A. Configuration Manager console

   B. Internet Explorer

   C. SQL Server Report Builder

   D. Reporting Server Configuration Manager

2. Which of the following tools could you use to clone an existing Configuration Manager report?

   A. Reporting Server Configuration Manager

   B. SQL Server Report Builder

   C. Internet Explorer

   D. Configuration Manager console

3. You want to edit the properties of an existing Configuration Manager report. Which of the following tools could you use to accomplish this goal?

   A. Configuration Manager console

   B. Internet Explorer

   C. SQL Server Report Builder

   D. Reporting Server Configuration Manager

4. Which of the following Configuration Manager features would you use to determine software license usage information?

   A. Hardware inventory

   B. Software inventory

   C. File collection

   D. Asset Intelligence

Answers

Objective 6.1

Thought experiment

1. Windows, Mac OS X, Linux, and supported UNIX operating systems support the collection of hardware inventory.

2. Only Configuration Manager clients running Windows operating systems support the collection of software inventory.

Objective review

1. **Correct answer:** A

   A. **Correct:** You can use hardware inventory to determine whether a specific graphics card is being used on a Configuration Manager client.

   B. **Incorrect:** Software inventory enables you to inventory software, not hardware.

   C. **Incorrect:** You can't use file collection to determine which hardware is installed on a computer.

   D. **Incorrect:** Software metering tracks how often an application is run.

2. **Correct answer:** D

   A. **Incorrect:** Software metering tracks how often an application is run.

   B. **Incorrect:** Asset Intelligence enables you to identify software on a computer.

   C. **Incorrect:** Hardware inventory enables you to collect hardware information, not files.

   D. **Correct:** You would use file collection to collect all .ini files stored in a specific folder on a Configuration Manager client.

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

   A. **Correct:** Software inventory does not collect files with the encryption attribute set by default.

   B. **Correct:** Software inventory does not collect files with the compression attribute set by default.

   C. **Incorrect:** Software inventory will inventory files with the hidden attribute set by default.

   D. **Incorrect:** Software inventory will inventory files with the archive attribute set by default.

Objective 6.2

Thought experiment

1. Because the graphics application is likely to be used by less than 10 percent of people in the organization, you'll need to create a software-metering rule rather than letting one be created automatically.

2. You can modify Software Metering Properties to change the threshold for rule creation and the maximum number of automatically created rules.

Objective review

1. **Correct answer:** D

   A. **Incorrect:** The Summarize Software Metering File Usage Data task condenses software-metering file usage data from multiple records into one general record.

   B. **Incorrect:** The Summarize Software Metering Monthly Usage Data task condenses detailed software-metering usage data from multiple records into one general record.

   C. **Incorrect:** The Delete Aged Software Metering Data task deletes all unsummarized software-metering data that is older than the number of days specified.

D. Correct: The Delete Aged Software Metering Summary Data task deletes summarized software-metering summary data that is older than the number of days specified. By default, the task runs every Sunday to delete software-metering summary data that is older than 270 days.

2. **Correct answer:** B

 A. **Incorrect:** The Delete Aged Software Metering Summary Data task deletes summarized software-metering summary data that is older than the number of days specified. By default, the task runs every Sunday to delete software-metering summary data that is older than 270 days.

 B. **Correct:** The Delete Aged Software Metering Data task deletes all unsummarized software-metering data that is older than the number of days specified. By default, the task runs every day and deletes software-metering data that is older than five days.

 C. **Incorrect:** The Summarize Software Metering Monthly Usage Data task condenses detailed software-metering usage data from multiple records into one general record.

 D. **Incorrect:** The Summarize Software Metering File Usage Data task condenses software-metering file usage data from multiple records into one general record.

3. **Correct answer:** B

 A. **Incorrect:** You cannot use software inventory to determine which user has been running an application and how often the user does so.

 B. **Correct:** You can use software metering to determine which user has been running an application and how often the user does so.

 C. **Incorrect:** You cannot use file collection to determine which user has been running an application and how often the user does so.

 D. **Incorrect:** You cannot use Asset Intelligence to determine which user has been running an application and how often the user does so.

4. **Correct answer:** B

 A. **Incorrect:** By default, a software-metering rule is created when an application is launched on 10 percent of Configuration Manager client computers in a hierarchy.

 B. **Correct:** By default, a software-metering rule is created when an application is launched on 10 percent of Configuration Manager client computers in a hierarchy.

 C. **Incorrect:** By default, a software-metering rule is created when an application is launched on 10 percent of Configuration Manager client computers in a hierarchy.

 D. **Incorrect:** By default, a software-metering rule is created when an application is launched on 10 percent of Configuration Manager client computers in a hierarchy.

Objective 6.3

Thought experiment

 1. You can use SQL Server Report Builder to create a report based on information in the Configuration Manager database.

2. You can use the Asset Intelligence Software Details Conflict Resolution dialog box to resolve conflicts between categorization and information in System Center Online.

Objective review

1. Correct answer: B

A. Incorrect: You cannot use the Configuration Manager console to import reports in RDL format.

B. Correct: You use Internet Explorer, or another browser, to connect to *http://server/reports* to upload reports in RDL format.

C. Incorrect: You can use SQL Server Report Builder to clone and edit reports, but you need to use Internet Explorer, or another browser, to upload a report to a Report Server instance.

D. Incorrect: You use Reporting Server Configuration Manager to configure the Reporting Server instance.

2. Correct answer: B

A. Incorrect: You use Reporting Server Configuration Manager to configure the Reporting Server instance.

B. Correct: You can use SQL Server Report Builder to clone and edit reports.

C. Incorrect: You use Internet Explorer, or another browser, to connect to *http://server/reports* to upload reports in RDL format. You can't use Internet Explorer to clone a report.

D. Incorrect: You cannot use the Configuration Manager console to clone a report.

3. Correct answer: C

A. Incorrect: You cannot use the Configuration Manager console to edit the properties of an existing Configuration Manager report.

B. Incorrect: You cannot use Internet Explorer to edit the properties of an existing Configuration Manager report.

C. Correct: You can use SQL Server Report Builder to clone and edit reports.

D. Incorrect: You use Reporting Server Configuration Manager to configure the Reporting Server instance.

4. Correct answer: D

A. Incorrect: You can't use hardware inventory to determine software license usage information.

B. Incorrect: Although software inventory can identify some files, it is not as reliable as Asset Intelligence for determining software licensing information.

C. Incorrect: You can't use file collection to determine software license usage information.

D. Correct: Because Asset Intelligence provides a more accurate report about which software is present on Configuration Manager clients, it is the best tool for determining software license usage information.

Chapter 7. Provision and manage mobile devices

Mobile devices, whether laptops, tablets, or smartphones, make up an increasing percentage of the devices used to perform work-related activities in organizations. Mobile device management (MDM) enables the organization to manage those devices. You can perform MDM through Microsoft Exchange Server by using Configuration Manager, through Microsoft Intune, or through a combination of Exchange and Microsoft Intune.

Objectives in this chapter:

- Objective 7.1: Integrate Configuration Manager with the Microsoft Exchange ActiveSync Connector.
- Objective 7.2: Manage devices with Microsoft Intune.
- Objective 7.3: Manage connection profiles by using Configuration Manager.

Objective 7.1: Integrate Configuration Manager with the Microsoft Exchange ActiveSync Connector

In many organizations, mobile devices already connect to a Microsoft Exchange deployment by using ActiveSync. Although it's possible to apply mobile device policies directly through Exchange to apply configuration settings to these devices, this requires Exchange administrators to perform MDM tasks. Configuration Manager provides the option of configuring a connector between a Configuration Manager deployment and Microsoft Exchange so that MDM policies set in Configuration Manager are applied through the mobile device's ActiveSync connection to Exchange Server.

This section covers the following topics:

- Exchange Server connector
- Connector settings
- Connector configuration

Exchange Server connector

In many organizations, mobile devices connect to an organization's infrastructure through Microsoft Exchange. Users of mobile devices that are running the iOS, Android, Windows Phone, and Windows Mobile operating systems already synchronize their email messages. The Exchange Server connector for System Center 2012 R2 Configuration Manager enables you to manage mobile devices remotely that connect to an Exchange Server deployment, without requiring Configuration Manager to enroll these devices directly.

The Exchange Server connector enables you to manage mobile devices by using the Configuration Manager console instead of Exchange ActiveSync mailbox policies. You can use the Exchange Server connector with an on-premises deployment of Exchange and a cloud-based Exchange deployment.

The Exchange Server connector enables you to perform the following mobile device–management tasks:

- **Discovery** Enables Configuration Manager to discover any mobile device that has registered with the Exchange Server environment.
- **Hardware inventory** Enables Configuration Manager to perform hardware inventory only based on the information that it receives from Exchange. This is not as comprehensive as a hardware inventory that is available to mobile devices that you manage through the Intune connector for Configuration Manager.
- **Settings management** Enables you to override default Exchange ActiveSync mailbox policy settings with settings that you configure through the Exchange Server connector for Configuration Manager.
- **Quarantine and block from Exchange Server** Enables you to block a mobile device from the Exchange Server organization and from Configuration Manager.
- **Remote wipe** Enables Exchange Server administrators, the device user, and Configuration Manager administrators to wipe devices remotely.
- **Reporting** Enables basic mobile device–management reports but does not provide all the reports that are available when you manage the device by using the Intune connector for Configuration Manager.

When you configure the Exchange Server connector, you determine whether Configuration Manager or Exchange ActiveSync mailbox policies are responsible for managing specific settings, including the following groups:

- General
- Password
- Email Management
- Security
- Applications

The important thing to remember is that after you configure any setting in a group, Configuration Manager is responsible for managing all of that group's settings. If you do not configure any settings in a group, the applicable Exchange ActiveSync policy remains in effect. When planning to use the Exchange Server connector, remember that responsibility for managing mobile devices will shift from the Exchange administrators to the Configuration Manager administrators.

General settings

The General Settings group of policies, shown in Figure 7-1, enables you to configure the following settings:

- **Internet Sharing From Mobile Devices** Whether the device allows tethering
- **Computer Synchronization** Whether the device can be synchronized with a computer
- **Allow mobile devices that cannot be provisioned** Whether mobile devices that cannot be managed completely by Exchange can make connection
- **Refresh Interval (Hours)** How often the mobile device policy is refreshed
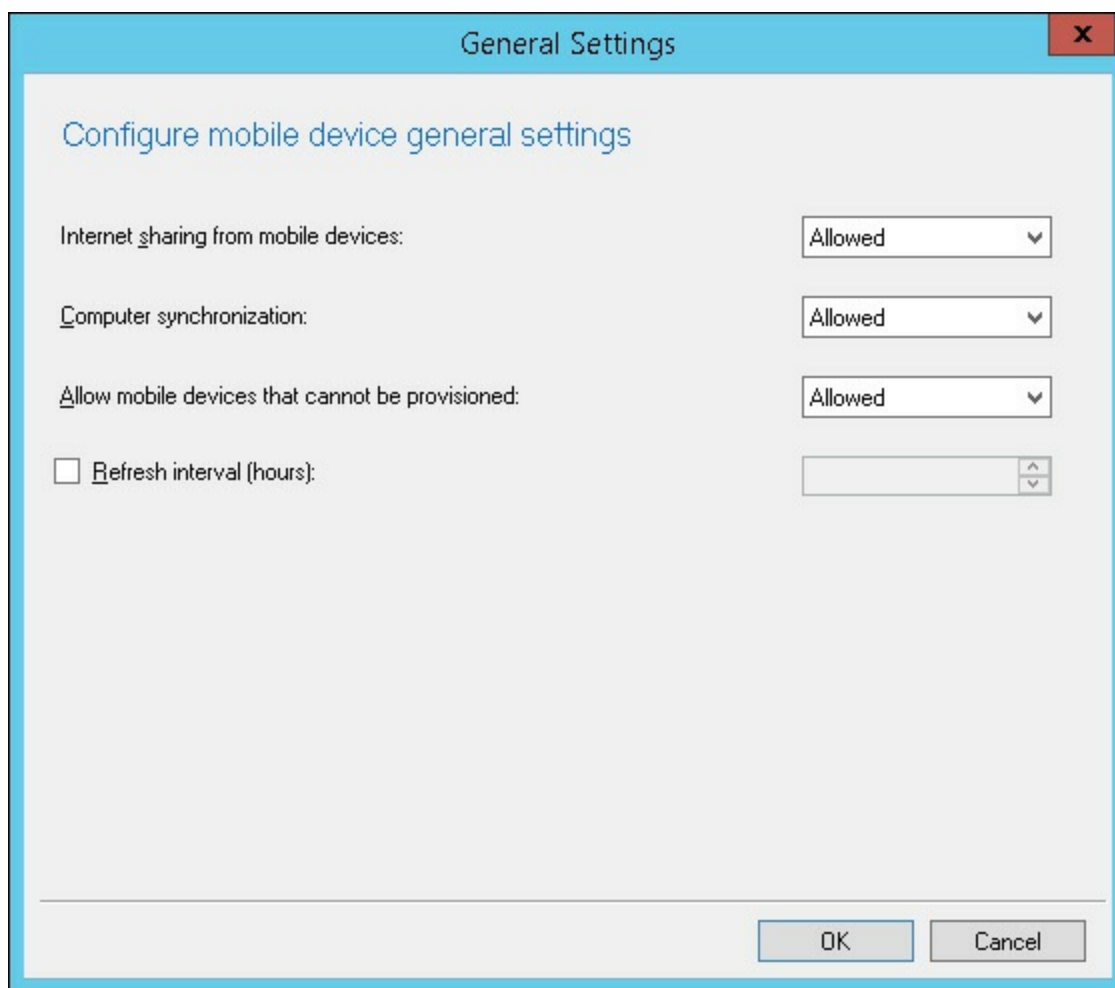
FIGURE 7-1 General Settings

Password settings

The Password Settings group, shown in , enables you to configure the following settings:

- **Require Password Settings On Mobile Devices** Whether to require a password to unlock the mobile device
- **Minimum Password Length (Characters)** Minimum required password length
- **Password Expiration In Days** Maximum password age
- **Number Of Passwords Remembered** How many unique passwords are stored before one can be reused
- **Number Of Failed Logon Attempts Before Device Is Wiped** Number of incorrect password entries that can be made before the device wipes
- **Idle Time In Minutes Before Mobile Device Is Locked** Number of minutes of inactivity before the device locks
- **Password Complexity** Whether complex passwords are required
- **Minimum Number Of Complex Characters** Number of character types required in a complex password (uppercase/lowercase/symbol/number)
- **Allow Simple Password** Whether to allow a simple password
- **Allow Password Recovery** Whether to allow passwords to be recovered by administrators
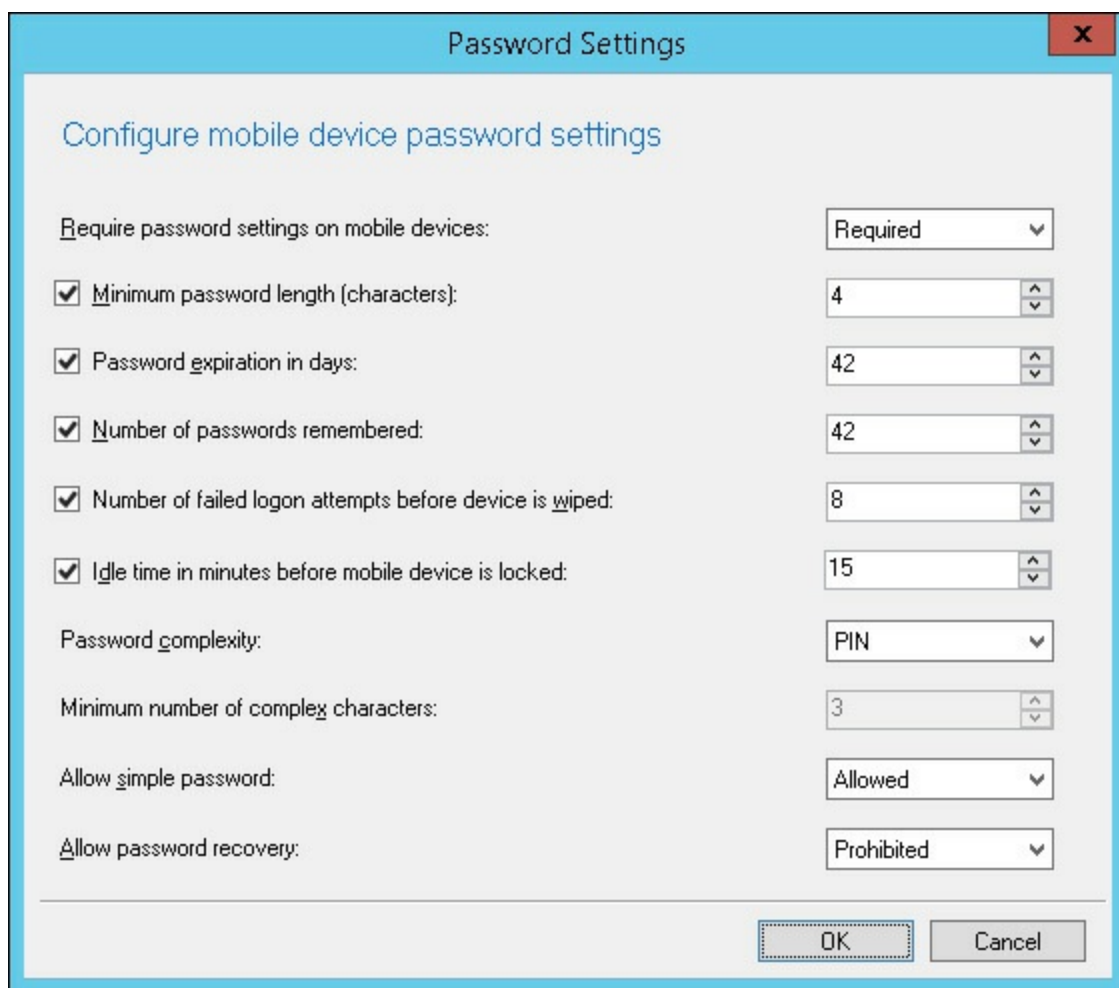
FIGURE 7-2 Password Settings

Email management

The Email Management Settings group, shown in , enables you to configure the following settings:

- **POP And IMAP Email** Whether to allow POP and IMAP protocol email
- **Maximum Time To Keep Email** How long email will be stored
- **Maximum Time To Keep Calendar Entries** How long calendar entries can be stored
- **Direct Push When Roaming** Whether to allow Direct Push when the mobile device is on a roaming network
- **Allowed Message Formats** Whether to allow HTML and/or plaintext messaging formats
- **Size Limit In Kilobytes (KB) For Plain Text Email (Automatically Downloaded)** Maximum size of plaintext messages that will be automatically downloaded
- **Size Limit In KB For HTML Email (Automatically Downloaded)** Maximum size for HTML format messages that will be downloaded
- **Email Attachments** Whether to allow email attachments to be downloaded
- **Size Limit In KB For Email Attachments (Automatically Downloaded)** Maximum size for automatically downloaded email attachments
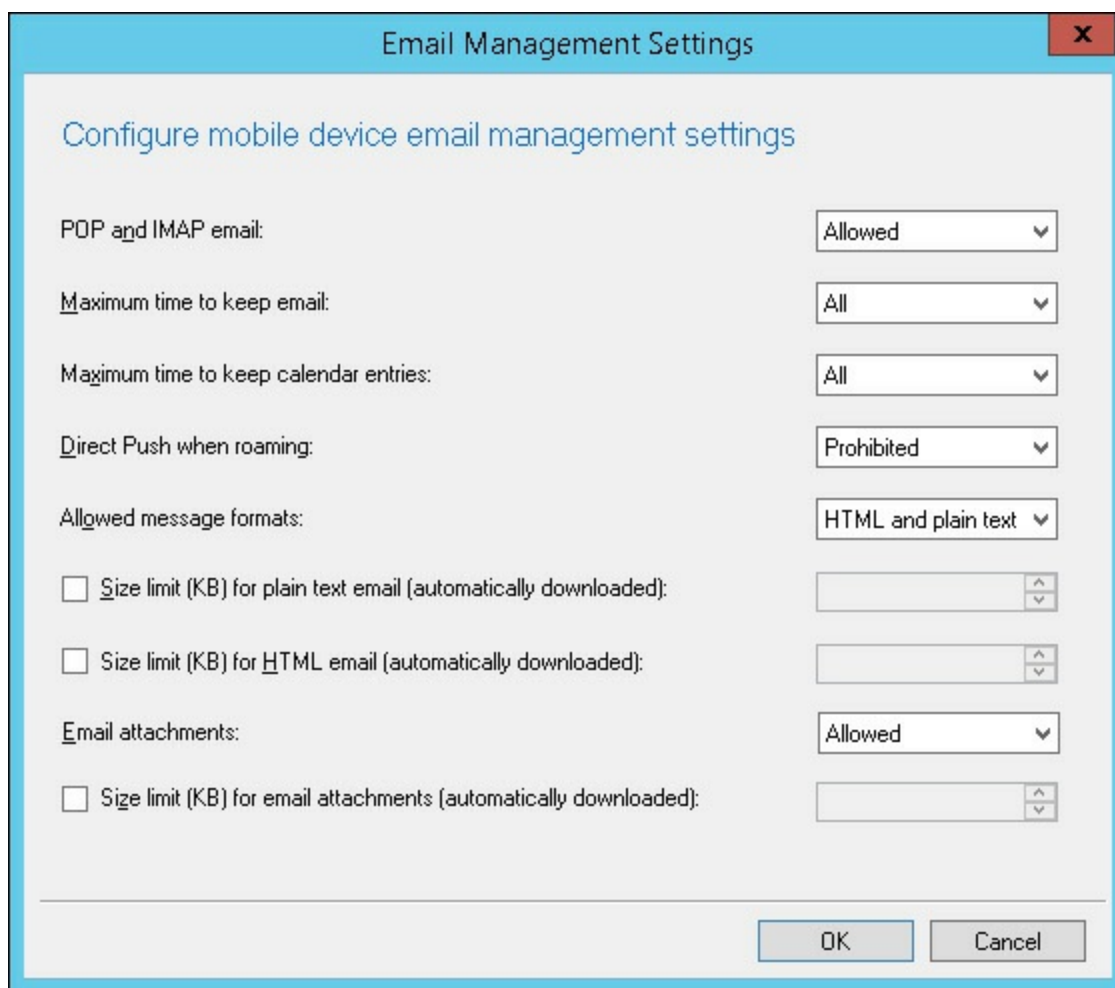
FIGURE 7-3 Email Management Settings

Security

The Security Settings group, shown in [Figure 7-4](#), enables you to configure the following settings:

- **Remote Desktop** Whether the device supports Remote Desktop
- **Removable Storage** Whether the device supports removable storage
- **Camera** Whether the device's camera can be used
- **Bluetooth** Whether Bluetooth functionality can be used
- **Wireless Network Connections** Whether to allow connections to a wireless network
- **Infrared** Whether to allow infrared connections
- **Browser** Whether to allow use of the mobile device's browser
- **Storage Card Encryption** Whether to enforce encryption on any storage card
- **File Encryption On Mobile Device** Whether to require encryption on the mobile device itself
- **Short Message Service (SMS) And Multimedia Messaging Service (MMS) Messaging** Whether to allow SMS/MMS functionality on the device
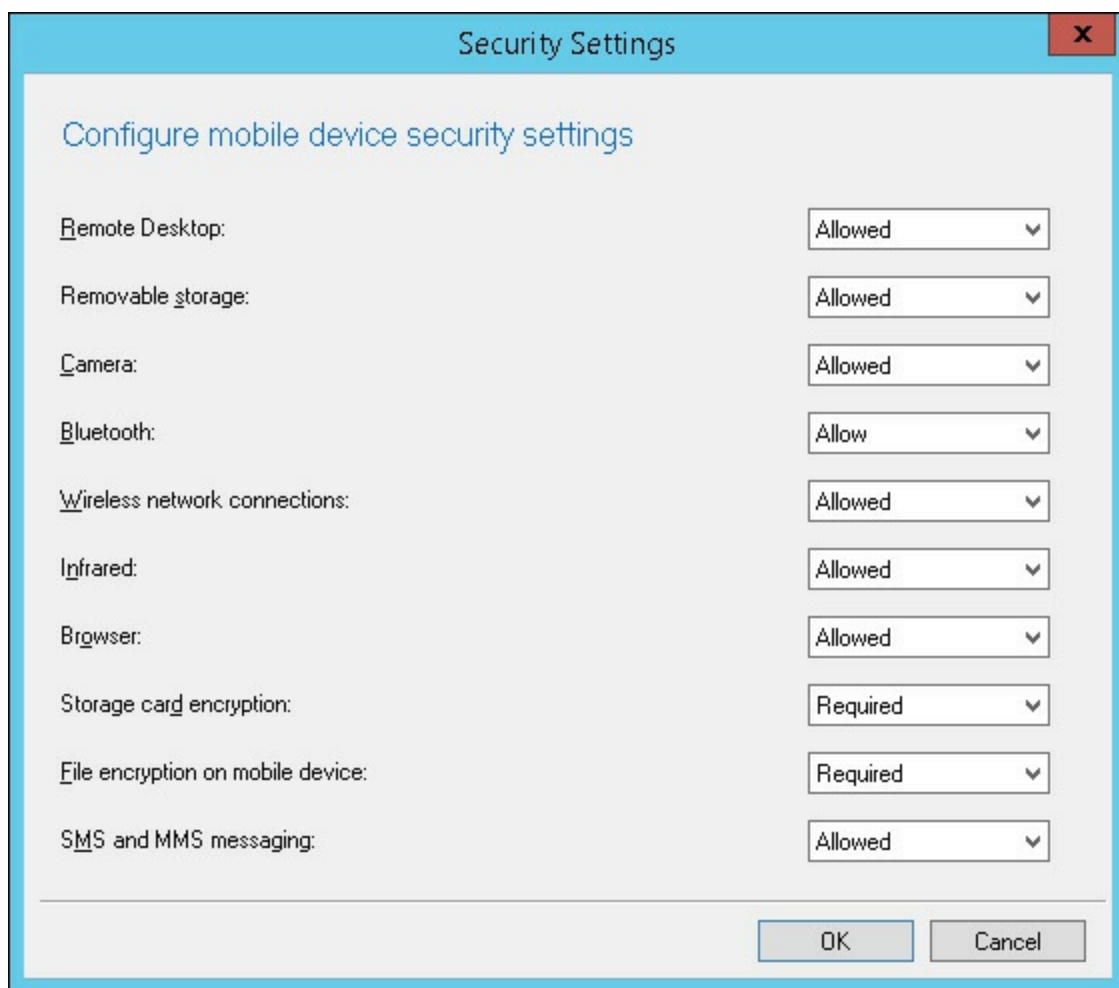
FIGURE 7-4 Security Settings

Applications

The Applications Settings group, shown in , enables you to configure the following settings:

- **Unsigned File Installation** Whether to allow the installation of unsigned files
- **Unsigned Applications** Whether to allow the installation of unsigned applications
- **Block The Following Applications In ROM** A list of specifically blocked applications
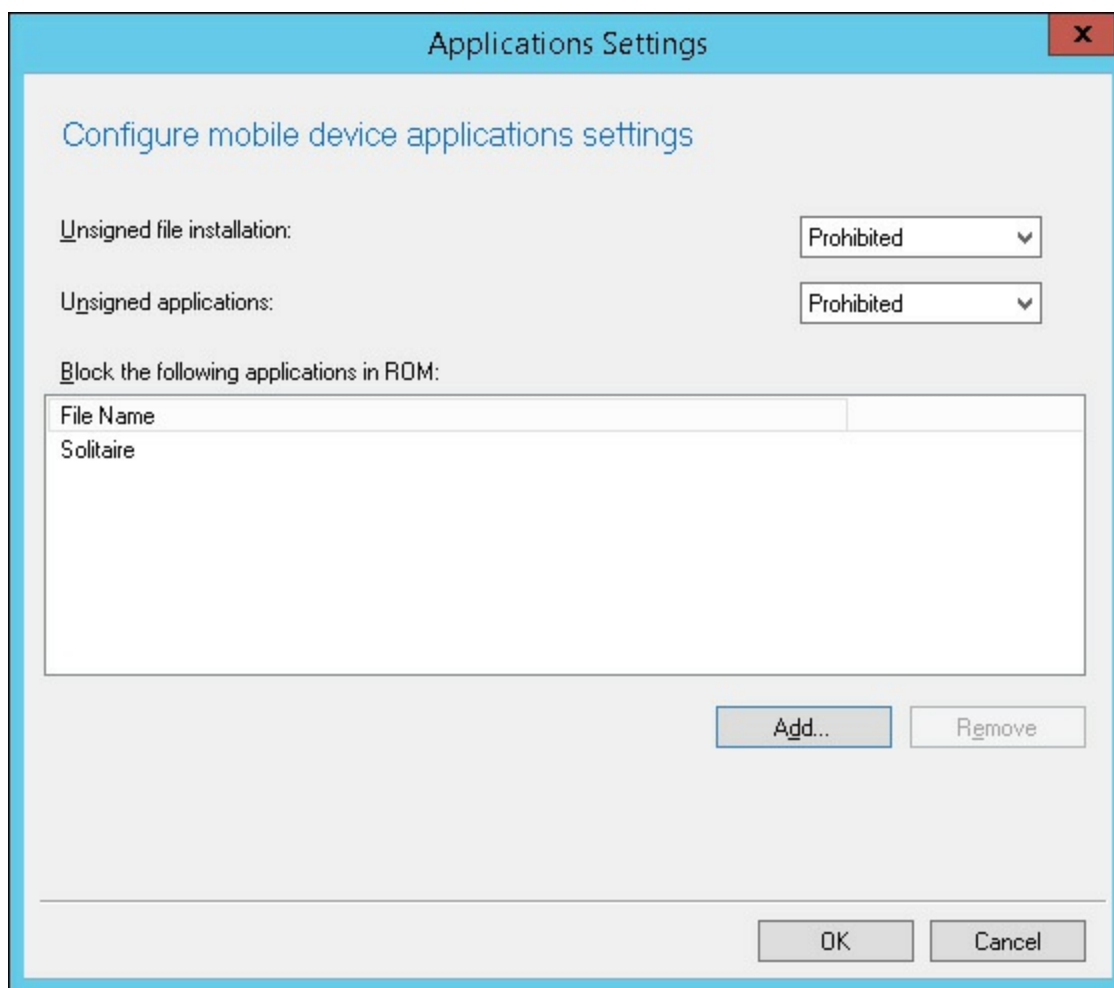
FIGURE 7-5 Applications Settings

Connector configuration

You should configure the account that you want to use when you set up an Exchange Server connector to be a member of the following Exchange management roles:

- Recipient Management
- View Only Organization Management
- Server Management

The Exchange Server connector enables you to manage any device that supports Exchange ActiveSync, although not all devices that use Exchange ActiveSync support all Exchange ActiveSync management functionality. The Exchange Server connector does not install a client on the mobile device that you are managing. This means that using the Exchange Server connector provides only a subset of the functionality available for mobile device management when compared to managing the same devices through the Configuration Manager Intune connector.

When you configure the Exchange Server connector, you specify the address of a Client Access server as shown in . When configuring the address of the client access server, specify one that is in the same Active Directory Domain Services (AD DS) site as the Configuration Manager site system server.
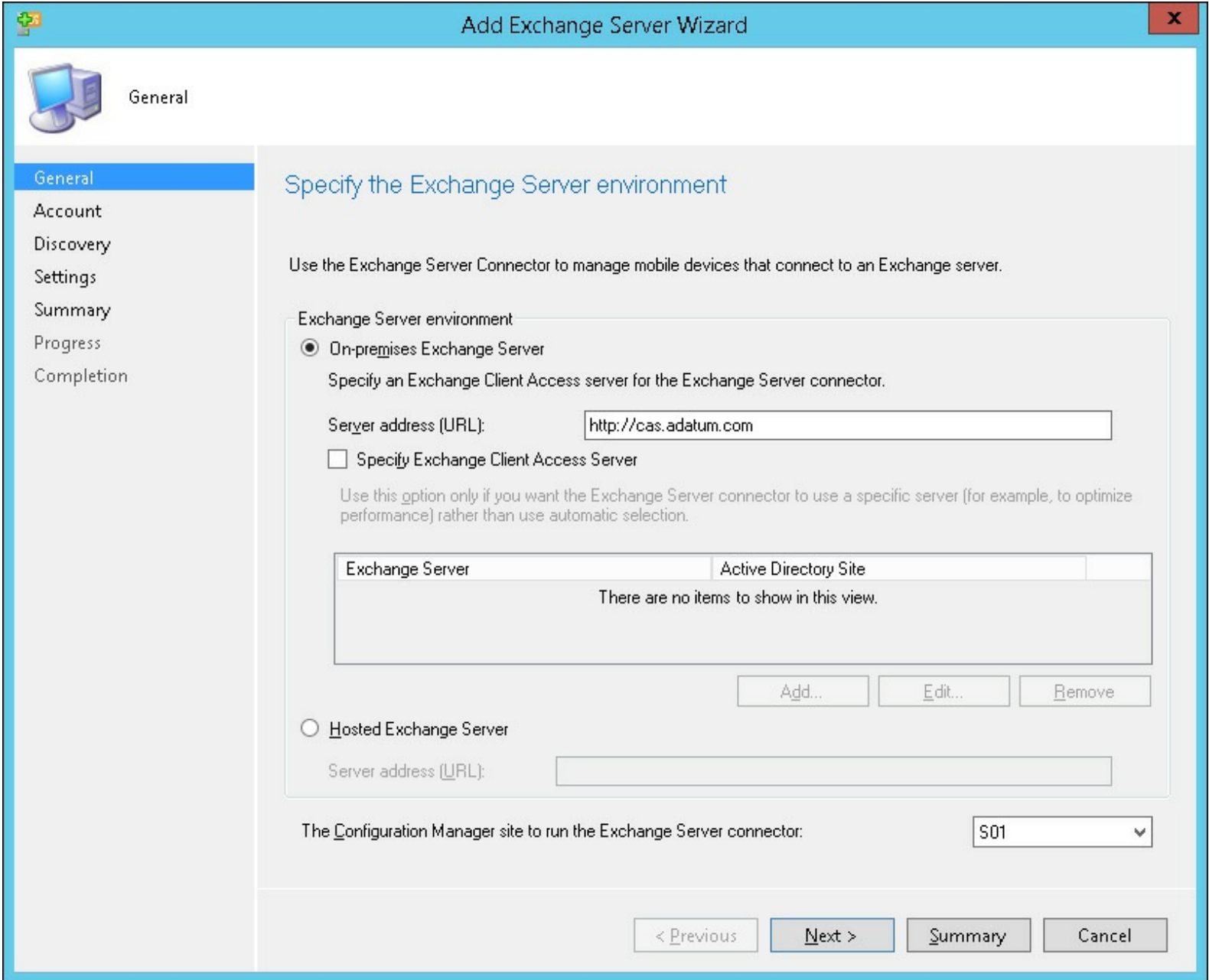
FIGURE 7-6 Add Exchange Server Wizard

The Exchange Server connector connects through the client access server to configure the default Exchange ActiveSync mailbox policy on the mailbox server. Even though the mailbox server is used to interact with the policy, the policy itself is stored within Active Directory Domain Services.

The first time a mobile device connects to the client access server, it retrieves the policy. Every subsequent time that the device connects to the client access server, it checks to see whether there are updates to the policy. If the policy has been updated, the mobile device downloads and applies the new policy.

More Info: **Configuration Manager and Activesync**

You can learn more about Configuration Manager and ActiveSync at *http://technet.microsoft.com/en-us/library/gg682001.aspx*.

Exam Tip

Remember which type of Exchange Server you specify when creating the connection between Configuration Manager and Exchange.

Thought experiment: ActiveSync MDM at Fabrikam

You are responsible for MDM at Fabrikam, a manufacturer of surveillance drones. You have configured the Configuration Manager ActiveSync connector for Exchange and will be managing MDM policies from Configuration Manager. You will be implementing policies as required. Because of the secure nature of Fabrikam's facilities, you need to ensure that the cameras on any mobile phones brought into the facilities are disabled. In addition, because several Fabrikam executives travel extensively overseas, you want to ensure that Direct Push functionality is disabled when their mobile phones are connected to roaming networks. With this in mind, answer the following questions:

1. Which settings group would you configure to ensure that mobile device cameras cannot be used on mobile devices managed at Fabrikam?

2. Which settings group would you configure to block Direct Push notifications when a mobile device is connected to a roaming network?

Objective summary

- The Exchange Server connector enables you to configure mobile device policies applied through ActiveSync to devices that connect to an Exchange deployment.
- After you configure one setting in a settings group, all settings in that group will be managed through Configuration Manager rather than through Exchange.
- When configuring the Exchange Server connector on the Configuration Manager server, specify the address of the client access server.
- The Exchange Server connector enables you to perform Discovery, Hardware Inventory, Settings Management, Remote Wipe, Reporting, and Quarantine And Block from Exchange Server.

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 "" section at the end of the chapter.

1. You are configuring the Configuration Manager Exchange Server connector. Your organization has an Exchange Server 2010 deployment. Each Exchange Server role is located on a separate server. Which of the following server addresses should you specify when creating the connector?

    A. The address of the Hub Transport server

    B. The address of the mailbox server

    C. The address of the client access server

    D. The address of the Edge Transport server

2. Which of the following Exchange Server ActiveSync connector settings would you configure to ensure that a person must change her mobile device password every five weeks?

    A. Minimum Password Length

    B. Password Expiration In Days

    C. Number Of Passwords Remembered

    D. Number Of Failed Logon Attempts Before The Device Is Wiped

3. Which of the following Exchange Server ActiveSync connector settings would you configure to ensure that a person cannot use one of his 20 previously used passwords the next time he has to change his mobile device password?

    A. Number Of Failed Logon Attempts Before The Device Is Wiped

    B. Number Of Passwords Remembered

    C. Password Expiration In Days

    D. Minimum Password Length

4. You work at a secure facility. You want to ensure that people cannot unlock a stolen mobile device by randomly attempting to guess the password. Which of the following Exchange Server ActiveSync connector settings would you configure to ensure that the device is wiped if such an attempt is made?

    A. Password Expiration In Days

    B. Minimum Password Length

    C. Number Of Failed Logon Attempts Before The Device Is Wiped

    D. Number Of Passwords Remembered

Objective 7.2: Manage devices with Microsoft Intune

Microsoft Intune (formerly Windows Intune) is a cloud-based management service. You can use it to manage enrolled mobile devices through a web portal. You can also configure a connector between Intune and an on-premises Configuration Manager deployment. When you do this, Intune functions as a conduit through which Configuration Manager policies are applied.

Microsoft Intune

Microsoft Intune is a cloud-based management service that enables you to manage client computers and mobile devices. You can use Intune to perform the following tasks:

- Deploy and manage software updates
- Deploy and manage applications
- Inventory hardware and software
- Manage endpoint protection
- Perform remote assistance
- Manage mobile devices
- Manage software licensing
- Configure Windows Firewall policy

You can use Intune to perform management tasks on computers that rarely connect to an organizational network. You can also use Intune to perform management tasks on a device that is not joined to an Active Directory domain. Intune also enables you to manage software deployment for computers that are running Windows, Android, and Apple iOS operating systems.

You do not need a Configuration Manager deployment to use Intune, but you can integrate Intune into a Configuration Manager deployment. Using Configuration Manager with Intune enables you to manage all of your organization's devices, both mobile devices and traditional computers, using a single console.

Intune supports management of clients on the following operating systems:

- Windows 8.1 (x86, x64), Windows 8 (x86, x64), Windows 7, and Windows Vista
- Windows RT 8.1 and Windows RT
- Windows Phone 8 and Windows Phone 8.1
- Apple iOS 6, iOS 7, and iOS 8
- Android 4

> *More Info:* **Set Up Intune**
>
> **You can learn more about setting up Intune at *http://technet.microsoft.com/en-us/library/dn646960.aspx*.**

Application deployment with Microsoft Intune

Each operating system Intune manages has different requirements according to what is needed to perform application deployment.

To deploy applications directly to mobile devices that are running Windows RT, you must obtain sideloading keys, and you must have a code-signing certificate to sign the applications. The Windows RT or Windows Phone 8 device must trust this code-signing certificate. In addition, you can use deep linking to deploy an application from the appropriate Windows App store directly to mobile devices that are running the Windows RT, Windows RT 8.1, Windows Phone 8, or Windows Phone 8.1 operating systems.

You can use Intune to deploy applications to iOS devices by deep linking to the Apple Store or by sideloading apps, which means you are installing them by using direct access to the source files. To deploy applications to iOS devices, you must obtain the appropriate mobile device management certificates from Apple. You can use a similar process for devices running the Android operating system.

More Info: **Intune Application Deployment**

You can learn more about Intune application deployment at *http://technet.microsoft.com/en-us/library/dn646955.aspx*.

Integrating Microsoft Intune with Configuration Manager

To configure the connector between Intune and System Center 2012 R2 Configuration Manager or System Center 2012 Configuration Manager with SP1, you must create the connector and deploy the Intune connector site system role.

Prior to configuring the Intune connector, you should ensure that you perform the following tasks:

- Sign up for an Intune organizational account. Before you can configure the connector, you must have Intune administrator credentials for the organizationname.onmicrosoft. com domain. Do not use the account that you used to sign up for Intune (the Outlook.com, Hotmail.com, or live.com Microsoft account) to configure the connector.

- Add a public company domain to Intune. You should have a public company domain for which you can create Domain Name System (DNS) resource records, and you must configure this domain within Intune. This isn't a requirement, but it is highly recommended.

- If you have a public domain name that you will be using with Intune, configure user account, or user principal name (UPN), suffixes. You must configure user accounts with UPNs for the public company domain.

- Configure directory synchronization. You must configure Active Directory synchronization between your on-premises Active Directory and the Microsoft Azure Active Directory that you are using with the Intune organizationname.onmicrosoft.com domain.

- Create a DNS alias. Create a canonical name (CNAME) record in DNS that maps enterpriseenrollment.organizationname.com (where organizationname.com is your organization's DNS suffix) to manage.microsoft.com.

- Obtain relevant certificates or keys. Depending on the mobile devices that you will be managing through Intune, you need the certificates or keys that are listed in the following table.

Depending on the mobile device operating system, you will need certificates or keys to enroll mobile devices through the Intune with Configuration Manager connector. Table 7-1 details those

specifications.

Mobile-device operating system	Certificates or keys	Notes
Windows Phone 8 and Windows Phone 8.1	Code-signing certificate. All side-loaded apps must be code-signed.	Purchase a code-signing certificate from Symantec.
Windows RT 8.1 and Windows RT	Sideloading keys to allow installation of sideloaded apps. All apps that you sideload must be code-signed.	Obtain sideloading keys from Microsoft. Sign apps by using a code-signing certificate that an internal or third-party trusted certification authority (CA) issues.
iOS 6, iOS 7, iOS 8	Apple Push Notification service certificate.	Obtain from Apple.
Android	Not required.	

TABLE 7-1 Mobile device operating system requirements

To create the Intune connector, you must perform the following procedure:

1. In the Administration workspace, expand the Hierarchy Configuration folder and then click Microsoft Intune Subscriptions.

2. On the ribbon, click Add Microsoft Intune Subscription.

3. On the Introduction page, click Next.

4. On the Subscription page, sign in by using an account configured as an administrator for your Intune organization. Select the Allow The Configuration Manager Console To Manage This Subscription check box.

5. Review the privacy links.

6. On the General page, specify the following settings:

   - Collection: Specify which user collection contains users who will enroll their mobile devices.
   - Company name: Specify your organization name.
   - URL to company privacy information: Provide privacy information (optional).
   - Color scheme for company portal: Change the color of the company portal if desired.
   - Configuration Manager site code: Specify the primary site for mobile devices.

7. On the Platforms page, choose the device types you want to manage and then review the platform requirements. For each device type that you select, you need to configure additional settings. You can configure these settings on a per-device basis when necessary.

When you enable Allow The Configuration Manager Console To Manage This Subscription, Configuration Manager takes control of the Intune subscription for mobile device management. You cannot undo this step. If you later decide that you do not want to manage Intune by using Configuration Manager, you must create a new Intune subscription.

To deploy the site system role for the Intune connector, perform the following procedure on a site system server that communicates with the Intune servers that manage.microsoft.com hosts:

1. In the Administration workspace, expand the Site Configuration folder and then click Servers

And Site System Roles.

2. Select the site system server and then click Add Site System Roles on the ribbon.

3. On the System Role Selection page, select Microsoft Intune Connector and then click Next.

4. Complete the wizard.

Device enrollment

Each mobile device operating system uses a different method to enable users to self-enroll their mobile devices, with the method sometimes different depending on whether you are using Intune as a standalone product or have configured integration with Configuration Manager. You can use the following method:

- **Windows Phone 8 and Windows Phone 8.1** To enroll a Windows Phone 8 device, users select Company Apps or Workplace from their phones' Settings screen. They then provide their domain credentials in the form of their UPN and password. The user is then prompted to install the company app or hub, which installs the company portal. The device collects inventory and applies management settings. Users then can access any available apps.

- **Windows RT 8.1 and Windows RT** To enroll a Windows RT 8 device, go to the Workspace section of settings and provide the organizational credentials as shown in Figure 7-7. This enrolls the Windows RT device in Configuration Manager. If your organization has System Center 2012 R2 Configuration Manager, you also can download the Company Portal App from the Windows Store and then provide your user credentials.
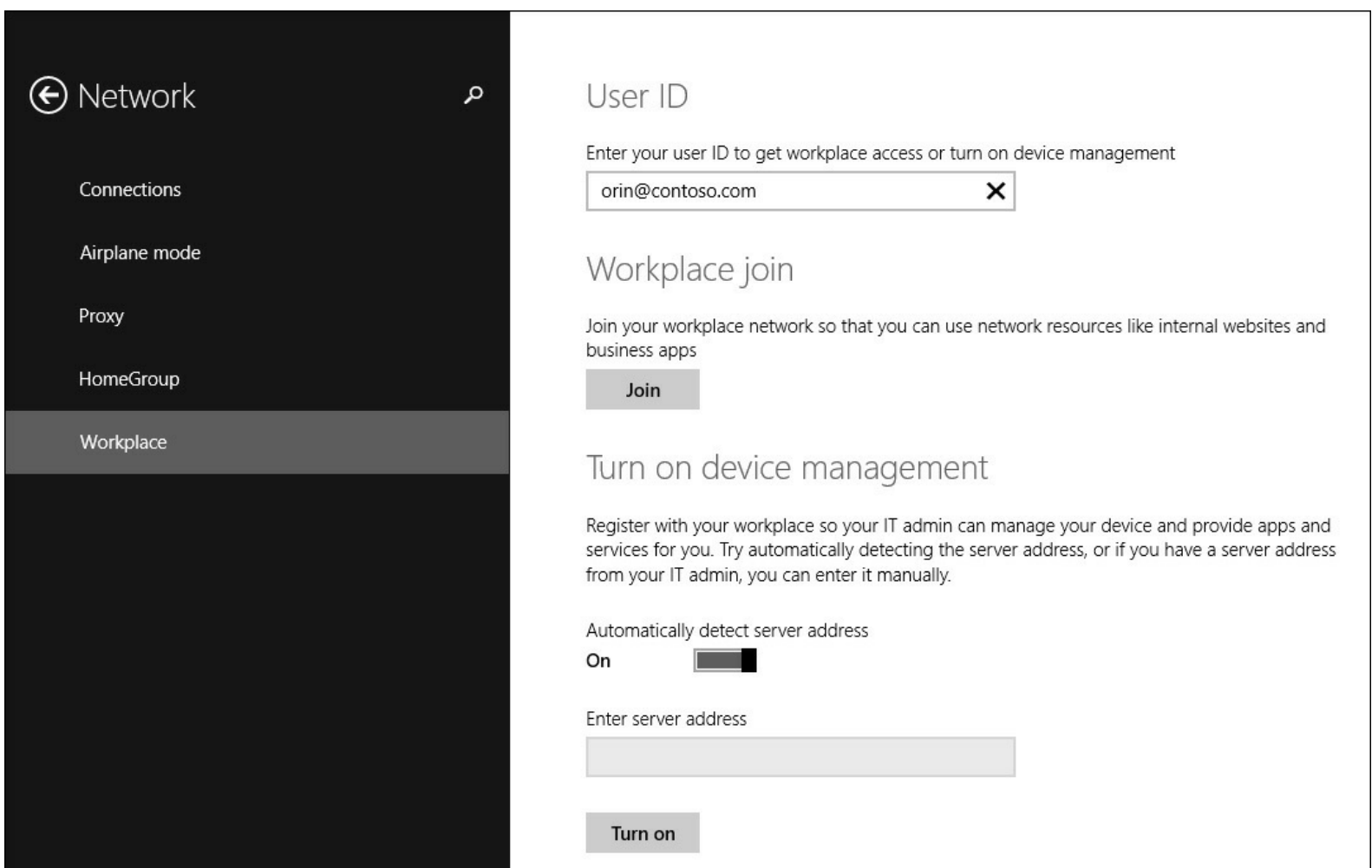
FIGURE 7-7 Workplace join

- **iOS** To enroll an iOS device, use the device's browser to navigate to manage.microsoft.com and then provide credentials. If your organization has integrated System Center 2012 R2 Configuration Manager, you can obtain the Company Portal app through the Apple App Store.

- **Android** Users can enroll mobile devices that are running the Android operating system by acquiring the Company Portal App, without charge, from the Google Play store. They then can provide their credentials in the app to enroll in the Configuration Manager infrastructure. Only System Center 2012 R2 Configuration Manager supports this method.

- **Windows** To enroll a computer running Windows 8.1, go to the Workplace settings control panel shown in Figure 7-8 and click Join. You'll need to be signed on with an appropriate set of credentials. You also can download the Company Portal App from the Windows Store and then provide your user credentials.

FIGURE 7-8 Workplace join

Exam Tip

Remember that an Apple Push Notification Service certificate is required to manage devices running iOS. No such certificate is required to manage devices running Android.

Thought experiment: **Intune connector configuration at Tailspin Toys**

You are preparing to deploy an Intune connector between the Tailspin Toys Configuration Manager deployment and a recently activated Intune subscription.

1. **With which hostname on the Internet must the site server on which you will deploy the Intune connector be able to communicate?**
2. **Which account should you specify when configuring the Intune connector on the Configuration Manager site server?**

Objective summary

- You can use Intune to manage hardware inventory, software inventory, endpoint protection, remote assistance settings, software licensing, and firewall policy.
- You can use Intune to deploy and manage software updates and applications.
- You can use Intune separately from Configuration Manager, or you can integrate it with Configuration Manager.
- You can deploy apps to mobile devices by deep linking to the app in the appropriate vendor's store.
- You need to have an Apple Push Notification Service certificate from Apple if you want to manage and deploy applications to devices running the iOS operating system.
- Devices running the Android operating system do not require special certificates to be managed through Intune.
- You need to configure directory synchronization between Microsoft Azure Active Directory and on-premises Active Directory if you intend to integrate Intune with Configuration Manager.
- The site server that hosts the Intune connector must be able to communicate with manage.microsoft.com on the Internet.

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 of the following device management tasks can you perform using Intune on a computer running Windows 8.1? (Choose all that apply.)

    A. Operating system upgrade

    B. BitLocker unlock

    C. Application deployment

    D. Hardware inventory

2. You work for adatum.com. You are preparing to integrate your on-premises Configuration Manager 2012 R2 deployment with a newly configured Intune subscription. Which of the following DNS configuration changes must you make?

    A. Create a CNAME record named enterpriseenrollment.adatum.com that maps to manage.microsoft.com.

    B. Create an MX record named enterpriseenrollment.adatum.com that maps to manage.microsoft.com.

    C. Create an NS record named enterpriseenrollment.adatum.com that maps to manage.microsoft.com.

    D. Create an SRV record named enterpriseenrollment.adatum.com that maps to manage.microsoft.com.

3. Which of the following are necessary if you want to deploy an in-house application by using Intune to 150 tablets running the Windows RT 8.1 operating system? (Choose two. Each correct

answer forms part of a complete solution.)

    A. Code-signing certificate trusted by the Windows RT 8.1 devices

    B. Encryption certificate trusted by the Windows RT 8.1 devices

    C. Sideloading keys

    D. Activation keys

Objective 7.3: Manage connection profiles by using Configuration Manager

Connection profiles enable you to provision managed devices automatically with settings, including Wi-Fi access point authentication information, virtual private network (VPN) configuration, email account setup, and digital certificate provisioning.

This section covers the following topics:
- Remote connection profiles
- VPN profiles
- Certificate profiles
- Email profiles
- Wi-Fi profiles

Remote connection profiles

You use remote connection profiles to configure Configuration Manager clients so that they can establish remote connections across the Internet to their work computers. This saves you from needing to provide instructions to end users on how they can perform these steps manually. For example, you can use remote connection profiles to configure a collection of desktop computers in the office so that it is possible for appropriately authenticated users on the Internet to establish remote desktop connection sessions. Through these sessions, these users would be able to interact with their office desktop computers directly, allowing access to files, shared folders, and resources such as printers.

    You can configure remote connection profiles to:

- Force the use of a known Remote Desktop Gateway (RD Gateway) server. Incoming connections will only be allowed if they are initiated from this address. You can configure RD Gateway servers with secure authentication policies so that connections from external clients are appropriately vetted before being forwarded to computers that can host remote desktop connection sessions on protected networks.

- Configure a collection of computers to allow inbound Remote Desktop connection sessions.

- Limit inbound Remote Desktop connection sessions to users who are listed as primary users of a computer.

- Configure Windows Firewall with advanced security rules so that inbound connections are possible if the computer connects to a domain or private network.

    Figure 7-9 shows the creation of a remote connection profile in which an RD Gateway server has been specified and settings allowing connections from primary users are enabled.
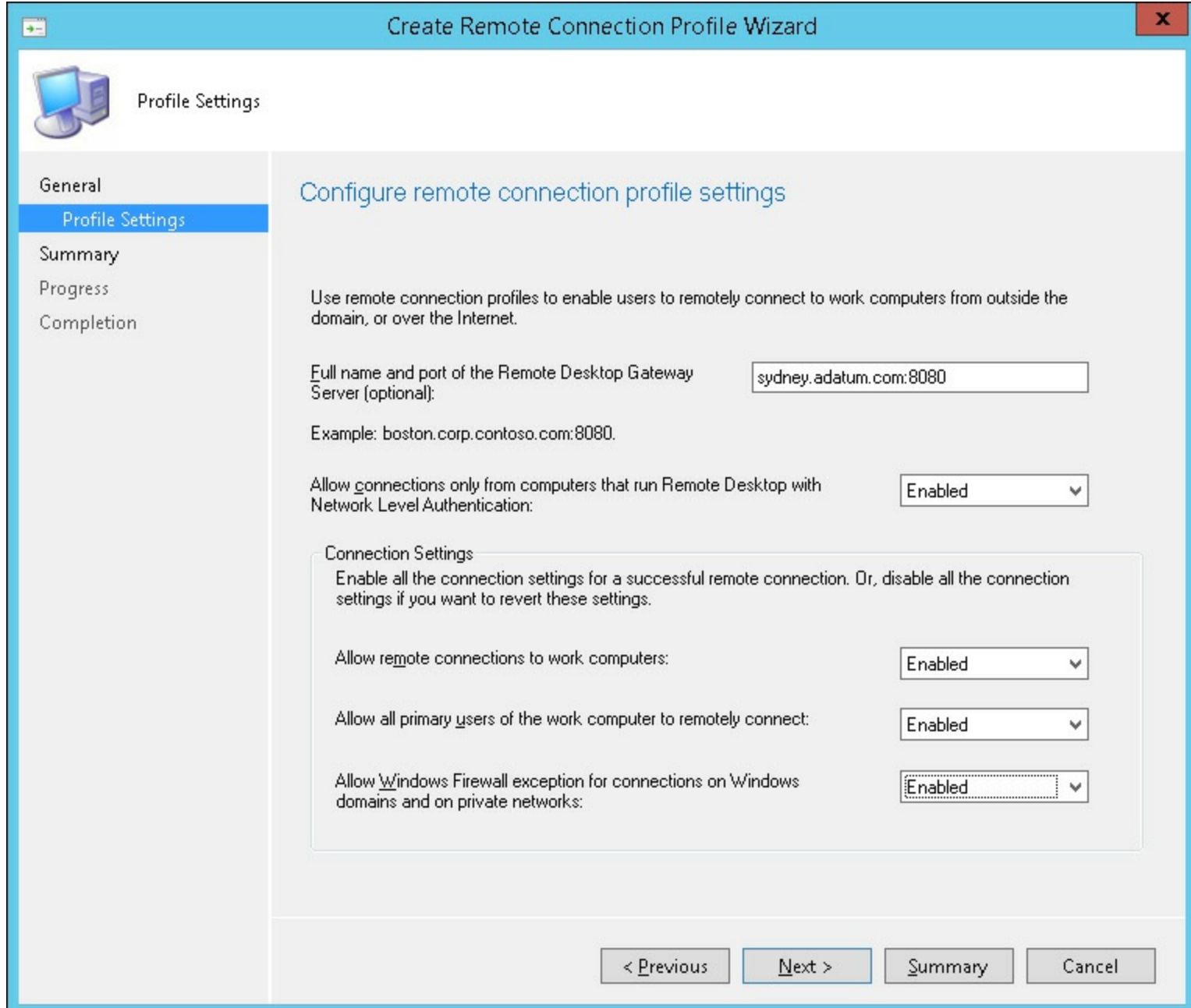
FIGURE 7-9 Create Remote Connection Profile Wizard

VPN profiles

You can use VPN profiles to deploy VPN connection configuration information to Configuration Manager clients that are running Windows 8.1 and Windows RT 8.1 or to iPhone and iPad devices that are running iOS 5, iOS 6, and iOS 7. You can use VPN profiles to deploy VPN connections that use the following connection types:

- Cisco AnyConnect
- Juniper Pulse
- F5 Edge Client

- Dell SonicWALL Mobile Connect
- Check Point Mobile VPN
- Microsoft SSL (SSTP)
- Microsoft Automatic
- IKEv2
- PPTP
- L2TP

The advantage of doing this is that by deploying the profiles to devices, end users will be able to make VPN connections without having to configure them themselves. Figure 7-10 shows the configuration of an IKEv2-based VPN profile.
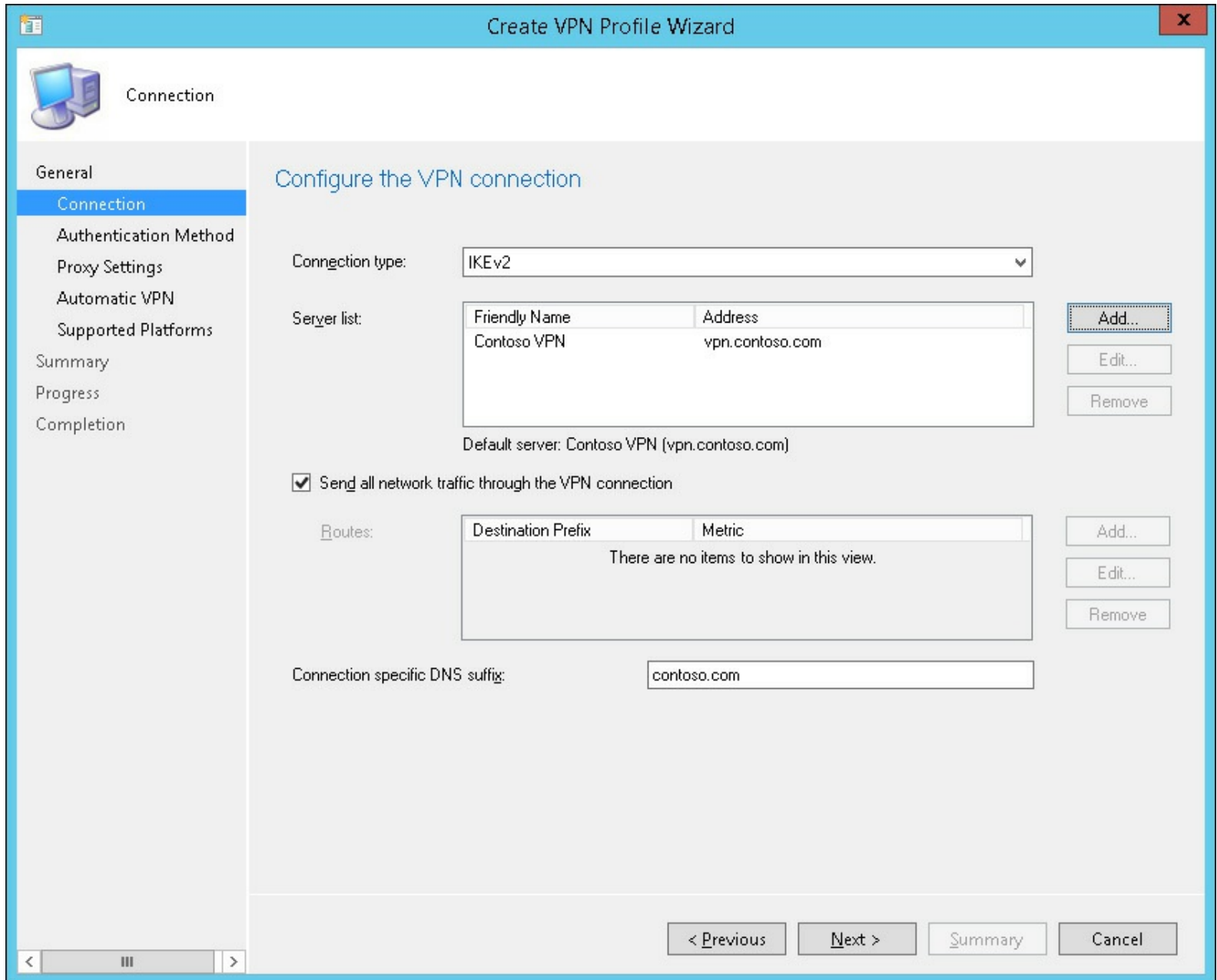
FIGURE 7-10 Create VPN Profile Wizard

Certificate profiles

You can use certificate profiles to deploy certificates to Configuration Manager clients. Certificate profiles enable you to configure automatic certificate deployment to clients that cannot participate in the Active Directory Certificate Services (AD CS) autoenrollment process because they are not members of the organization's AD DS. The Windows RT 8.1, Windows 8.1, iOS, and Android operating systems support certificate profiles, which in turn support the following functionality:

- Certificate enrollment and renewal from enterprise or standalone certification authorities (CAs)
- Deployment of trusted CA certificates to compatible Configuration Manager clients
- Monitoring of and reporting on installed certificates

To use certificate profiles, you must deploy the certificate registration point on a site system server either in the central administration site or in a primary site. You cannot deploy this role in a secondary site.

Figure 7-11 shows the configuration of a certificate profile.
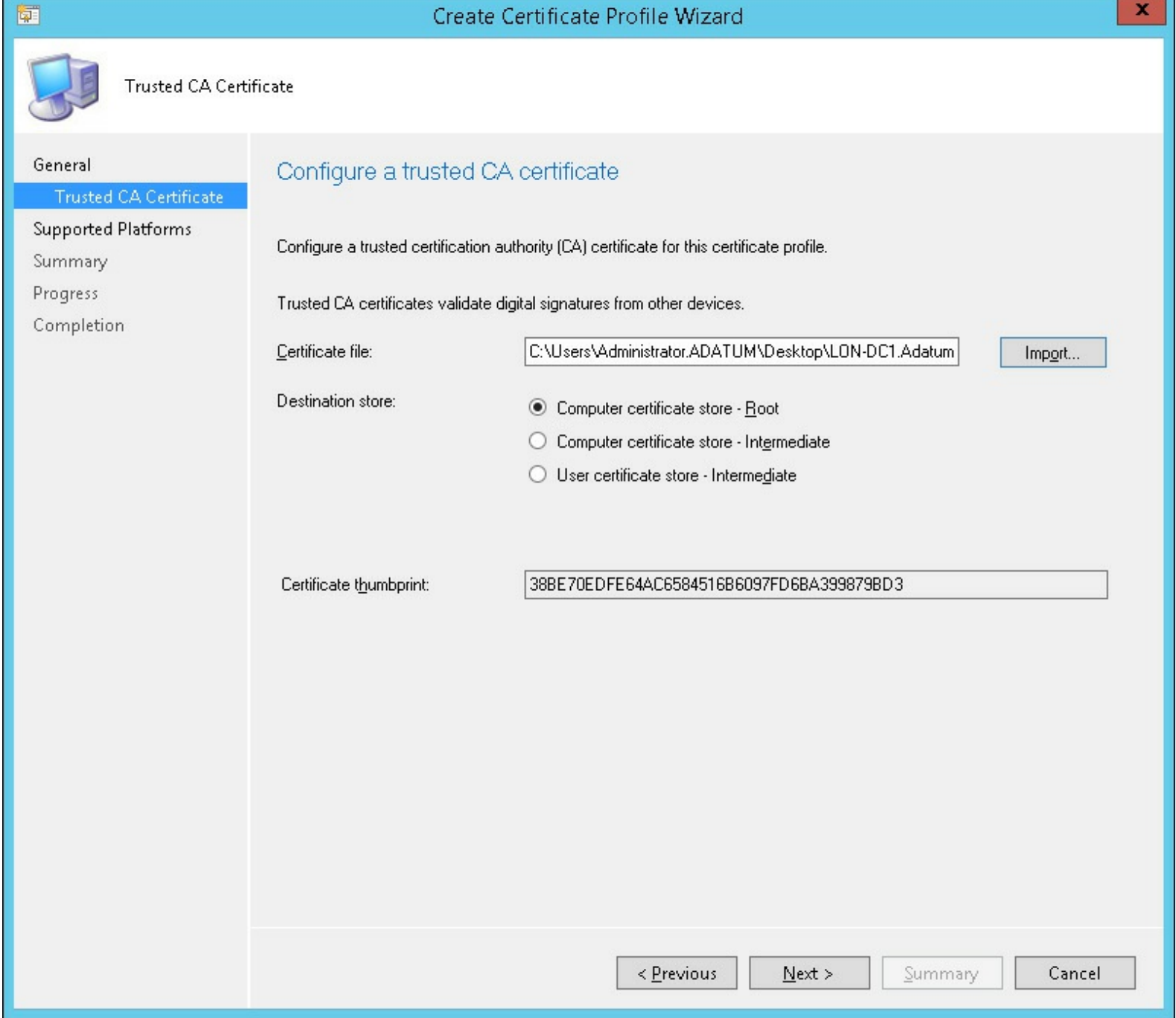
FIGURE 7-11 Create Certificate Profile Wizard

More Info: **Certificate Profiles**

You can learn more about certificate profiles at _http://technet.microsoft.com/en-us/library/dn261202.aspx_.

Email profiles

Email profiles are an optional feature in Configuration Manager 2012 R2. They enable you to provision managed devices running Windows Phone 8 and Windows Phone 8.1 or devices running iOS 5, iOS 6, iOS 7, and iOS 8 with profile information for organizational email accounts through Exchange ActiveSync. This minimizes the amount of effort required for a user to provision a connection to his organizational email account. In addition to email settings, an email profile configures synchronization settings for contacts, calendars, and tasks. Before it is possible to configure an email profile, it is necessary to install the Email Profiles Extension for Intune in the Configuration Manager site.

> *More Info:* **Email Profiles**
>
> **You can learn more about email profiles at _http://technet.microsoft.com/en-au/library/dn554226.aspx_.**

Wi-Fi profiles

You can use Wi-Fi profiles to deploy wireless network settings so that devices will connect automatically to preconfigured wireless networks without requiring the user to perform the operation manually. When you deploy Wi-Fi profiles, computers and mobile devices will connect to networks automatically without requiring direct user intervention.

You can use Wi-Fi profiles with devices running the following operating systems:

- Windows 8.1 (x86 and x64)
- Windows RT 8.1
- iOS 5
- iOS 6
- iOS 7
- iOS 8
- Android

Figure 7-12 shows a Wi-Fi profile for a wireless network with the SSID Contoso.
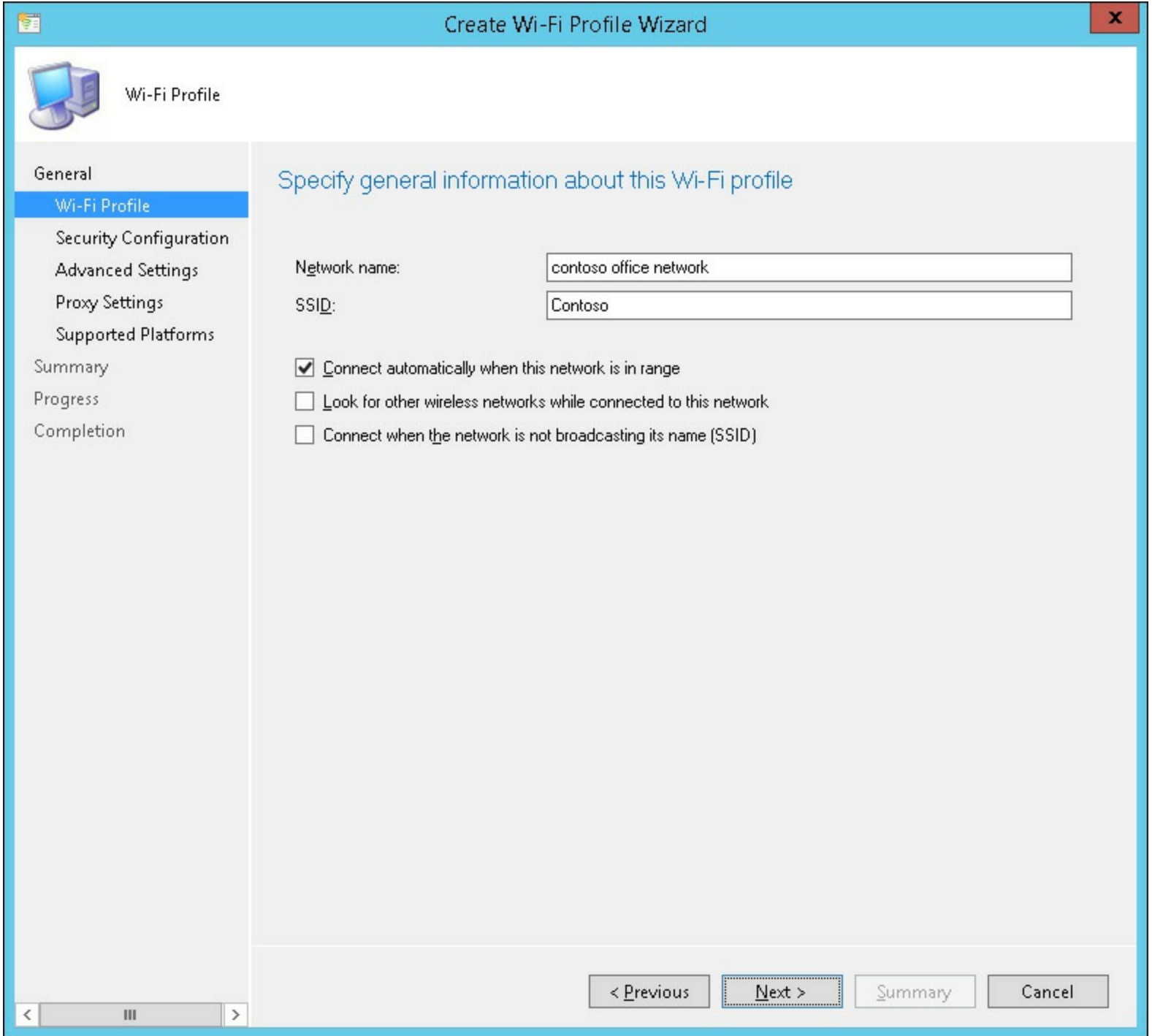
FIGURE 7-12 Create Wi-Fi Profile Wizard

More Info: **Wi-Fi Profiles**

You can learn more about Wi-Fi profiles at *http://technet.microsoft.com/en-us/library/dn261221.aspx*.

Exam Tip

Remember which items can be provisioned using profiles.

Objective summary

- Remote connection profiles enable you to deploy Remote Desktop connection configuration information to managed computers, allowing remote access to those computers using a Remote Desktop Protocol (RDP) client.
- VPN profiles enable you to deploy VPN connection configuration information to managed devices.
- Certificate profiles enable you to deploy certificates to managed devices.
- Email profiles enable you to deploy email, calendar, contacts, and tasks configuration information to managed devices.
- Wi-Fi profiles enable you to deploy wireless network configuration information to managed devices.

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 want to allow people to connect using Remote Desktop connection from their home computers, through an RD Gateway server deployed on your organization's perimeter network, to their work desktop computers on your organization's internal network. Which of the following profiles should you deploy to accomplish this goal?

   A. Email profile

   B. Certificate profile

   C. VPN profile

   D. Remote connection profile

2. You are testing a new device that uses a self-signed certificate to encrypt communication. You

want to configure 30 Configuration Manager clients so that they trust this self-signed certificate. Which of the following profiles would you deploy to accomplish this goal?

A. Email profile

B. Certificate profile

C. VPN profile

D. Remote connection profile

3. You are switching your remote access service from an SSTP VPN to an IKEv2 VPN because this allows automatic reconnection without requiring user reauthentication. Which of the following profiles would you deploy to mobile computers so that they are updated with this new VPN connection information?

A. Remote connection profile

B. Certificate profile

C. VPN profile

D. Email profile

4. Which of the following can you use to configure nondomain-joined computers running the Windows 8.1 operating system with the appropriate settings that allow them to connect to your organization's Exchange deployment?

A. Email profile

B. Certificate profile

C. VPN profile

D. Remote connection profile

Answers

Objective 7.1

Thought experiment

1. You would configure the Security Settings group to ensure that mobile device cameras cannot be used at Fabrikam.

2. You would configure the Email Management Settings group to block Direct Push notifications when a mobile device is connected to a roaming network.

Objective review

1. **Correct Answer:** C

A. **Incorrect:** When configuring the connector, you have to provide the address of the client access server.

B. **Incorrect:** When configuring the connector, you have to provide the address of the client access server.

C. **Correct:** When configuring the connector, you have to provide the address of the client

access server.

    D. Incorrect: When configuring the connector, you have to provide the address of the client access server.

2. Correct Answer: B

    A. Incorrect: The Minimum Password Length setting configures minimum password length.

    B. Correct: You would configure the Password Expiration In Days setting and set the value to 35 days if you wanted people to change their mobile device's password every five weeks.

    C. Incorrect: Use the Number Of Passwords Remembered setting to ensure that passwords cannot be reused.

    D. Incorrect: Use the Number Of Failed Logon Attempts Before The Device Is Wiped setting to ensure that a device is wiped if a password is incorrectly entered a number of times in succession.

3. Correct Answer: B

    A. Incorrect: Use the Number Of Failed Logon Attempts Before The Device Is Wiped setting to ensure that a device is wiped if a password is incorrectly entered a number of times in succession.

    B. Correct: Use the Number Of Passwords Remembered setting to ensure that passwords cannot be reused.

    C. Incorrect: The Password Expiration In Days setting determines how often a person must change her mobile device password.

    D. Incorrect: The Minimum Password Length setting configures minimum password length.

4. Correct Answer: C

    A. Incorrect: The Password Expiration In Days setting determines how often a person must change his mobile device password.

    B. Incorrect: The Minimum Password Length setting configures minimum password length.

    C. Correct: Use the Number Of Failed Logon Attempts Before The Device Is Wiped setting to ensure that a device is wiped if a password is incorrectly entered a number of times in succession.

    D. Incorrect: Use the Number Of Passwords Remembered setting to ensure that passwords cannot be reused.

Objective 7.2

Thought experiment

1. The site server on which you deploy the Intune connector must be able to communicate with the manage.microsoft.com hostname.

2. You must configure an Intune administrator account. You should not use the account that you used to sign up for Intune (the Outlook.com, Hotmail.com, or live.com Microsoft account) to configure the connector.

Objective review

1. **Correct Answers:** C and D

   A. **Incorrect:** You cannot perform an operating system upgrade by using Intune.

   B. **Incorrect:** You cannot perform BitLocker unlock by using Intune.

   C. **Correct:** You can perform application deployment by using Intune.

   D. **Correct:** You can perform hardware inventory by using Intune.

2. **Correct Answer:** A

   A. **Correct:** Prior to configuring a connection between an on-premises Configuration Manager deployment and Intune, you must create a canonical name (CNAME) record in DNS that maps enterpriseenrollment.organizationame.com (where organizationname.com is your organization's DNS suffix) to manage.microsoft.com.

   B. **Incorrect:** You must create a CNAME record. MX records are used to locate mail servers.

   C. **Incorrect:** You must create a CNAME record. NS records are used to locate name servers.

   D. **Incorrect:** You must create a CNAME record. SRV records are used to locate services.

3. **Correct Answers:** A and C

   A. **Correct:** To deploy an application to computers running Windows RT 8.1 through Intune, you must obtain sideloading keys, and you must have a code-signing certificate to sign the applications.

   B. **Incorrect:** You need a code-signing certificate

   C. **Correct:** To deploy an application to computers running Windows RT 8.1 through Intune, you must obtain sideloading keys, and you must have a code-signing certificate to sign the applications.

   D. **Incorrect:** You need sideloading keys.

Objective 7.3

Thought experiment

1. You can configure a certificate profile to deploy the CA certificate of the standalone CA on the perimeter network to managed devices. This will ensure that the managed iOS devices trust certificates issued by the standalone CA.

2. You can configure a Wi-Fi profile with the authentication details of Wi-Fi networks at Contoso. This will ensure that managed iOS devices can automatically connect to wireless networks.

Objective review

1. **Correct Answer:** D

   A. **Incorrect:** You use an email profile to provision a device with email, calendar, task, and contacts settings.

B. Incorrect: You can use a certificate profile to deploy a certificate, including a root certificate or a self-signed certificate, to a managed device. This certificate will be trusted.

C. Incorrect: You can use a VPN profile to deploy VPN connection information automatically to managed devices.

D. Correct: You can use a remote connection profile to configure computers so that they will accept inbound Remote Desktop connection requests if specific conditions are met.

2. **Correct Answer:** B

A. Incorrect: You use an email profile to provision a device with email, calendar, task, and contacts settings.

B. Correct: You can use a certificate profile to deploy a certificate, including a root certificate or a self-signed certificate, to a managed device. This certificate will be trusted.

C. Incorrect: You can use a VPN profile to deploy VPN connection information automatically to managed devices.

D. Incorrect: You can use a remote connection profile to configure computers so that they will accept inbound Remote Desktop connection requests if specific conditions are met.

3. **Correct Answer:** C

A. Incorrect: You can use a remote connection profile to configure computers so that they will accept inbound Remote Desktop connection requests if specific conditions are met.

B. Incorrect: You can use a certificate profile to deploy a certificate, including a root certificate or a self-signed certificate, to a managed device. This certificate will be trusted.

C. Correct: You can use a VPN profile to deploy VPN connection information automatically to managed devices.

D. Incorrect: You use an email profile to provision a device with email, calendar, task, and contacts settings.

4. **Correct Answer:** A

A. Correct: You use an email profile to provision a device with email, calendar, task, and contacts settings.

B. Incorrect: You can use a certificate profile to deploy a certificate, including a root certificate or a self-signed certificate, to a managed device. This certificate will be trusted.

C. Incorrect: You can use a VPN profile to deploy VPN connection information automatically to managed devices.

D. Incorrect: You can use a remote connection profile to configure computers so that they will accept inbound remote desktop connection requests if specific conditions are met.

Index

Numbers and Symbols

3DES (Triple Data Encryption Standard) encryption algorithm, 282

A

access accounts, 41

Access RemoteApp And Desktops dialog box, 29

Active Directory Certificate Services (AD CS), 335

Active Directory Domain Services (AD DS)

    authenticating users, 226

    Configuration Manager clients, 230–231

    Exchange Server connector, 321

    extending schema, 234–236

ActiveSync

    Configuration Manager and, 315–324

    Intune and, 76

AD CS (Active Directory Certificate Services), 335

AD DS (Active Directory Domain Services)

    authenticating users, 226

    Configuration Manager clients, 230–231

    Exchange Server connector, 321

    extending schema, 234–236

Add Applications dialog box, 8–9

Add Dependency dialog box, 19–20

Add Exchange Server Wizard, 322

Add New Collection Alerts dialog box, 211

add-ons, 5

Advanced antimalware policy setting, 206

alerts

    client health, 262

    Endpoint Protection, 211–212

    software update, 148–149, 155

All Desktop And Server Clients collection, 243

All Mobile Devices collection, 243

All Systems collection, 243

All Unknown Computers collection, 243

All User Groups collection, 243

All Users And User Groups collection, 243

All Users collection, 243

D

S

About the author

ORIN THOMAS is an MVP, an MCT, and has a string of Microsoft MCSE and MCITP certifications. He has written more than 30 books for Microsoft Press and is a contributing editor at Windows IT Pro magazine. He has been working in IT since the early 1990s. He regularly speaks at events such as TechEd in Australia and around the world on Windows Server, Windows Client, System Center, and security topics. Orin founded and runs the Melbourne System Center, Security, and Infrastructure Group. You can follow him on Twitter at *http://twitter.com/orinthomas*.

Free ebooks

From technical overviews to drilldowns on special topics, get *free* ebooks from Microsoft Press at:

www.microsoftvirtualacademy.com/ebooks

Download your free ebooks in PDF, EPUB, and/or Mobi for Kindle formats.

Look for other great resources at Microsoft Virtual Academy, where you can learn new skills and help advance your career with free Microsoft training delivered by experts.

Microsoft Press

Now that you've read the book...

Tell us what you think!

Was it useful?
Did it teach you what you wanted to learn?
Was there room for improvement?

Let us know at http://aka.ms/tellpress

Your feedback goes directly to the staff at Microsoft Press,
and we read every one of your responses. Thanks in advance!

Microsoft

Code Snippets

Many titles include programming code or configuration examples. To optimize the presentation of these elements, view the eBook in single-column, landscape mode and adjust the font size to the smallest setting. In addition to presenting code and configurations in the reflowable text format, we have included images of the code that mimic the presentation found in the print book; therefore, where the reflowable format may compromise the presentation of the code listing, you will see a "Click here to view code image" link. Click the link to view the print-fidelity code image. To return to the previous page viewed, click the Back button on your device or app.

```
New-RDRemoteApp  -Alias PPTViewer  -DisplayName PPTViewer  -FilePath "C:\
Program Files(x86)\Microsoft Office\Office14\PPTVIEW.exe"  -ShowInWebAccess True
-CollectionName RemoteApps  -ConnectionBroker LON-SVR1.Adatum.com
```

```
ExtractContent /P:<PrestagedFileLocation>[\<PrestagedFileName>] /S
```

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

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

```
sudo ./ccmsetup

sudo ./CMEnroll -s <enrollment_proxy_server_name> -ignorecertchainvalidation -u
<'username'>
```

```
./install -mp <FQDN of management point> -sitecode <site_code> ccm-universal-<x86
or x64>.<build>.tar
```

```
ldifde -i -f ConfigMgr_ad_schema.ldf -v -j <location to store log file>
```