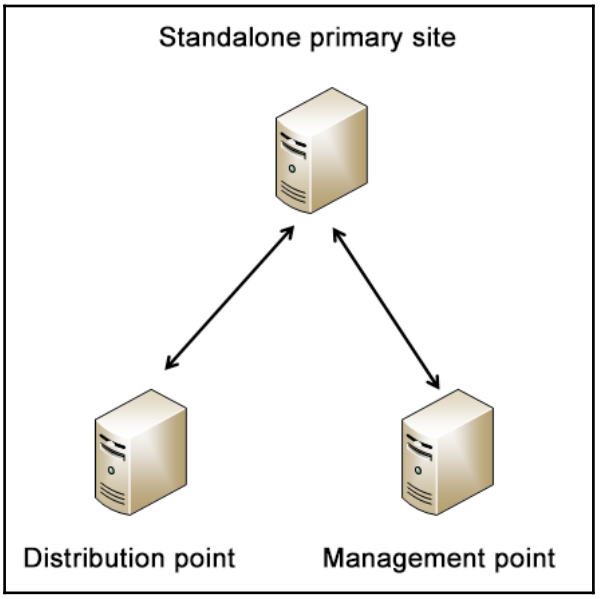
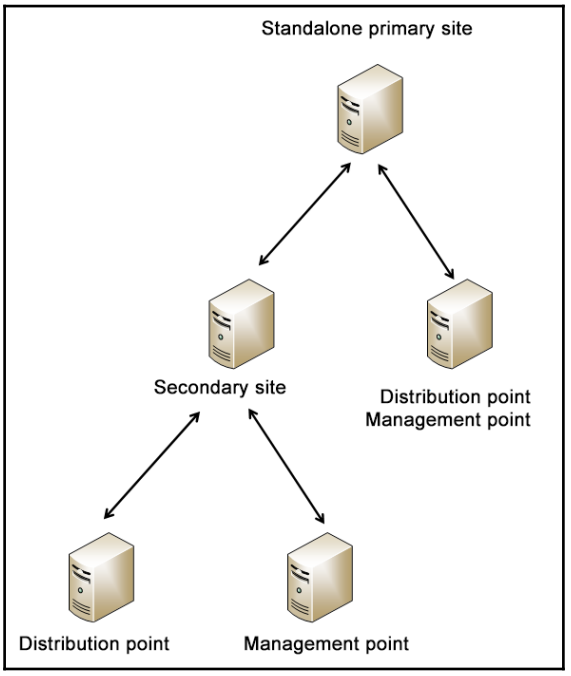
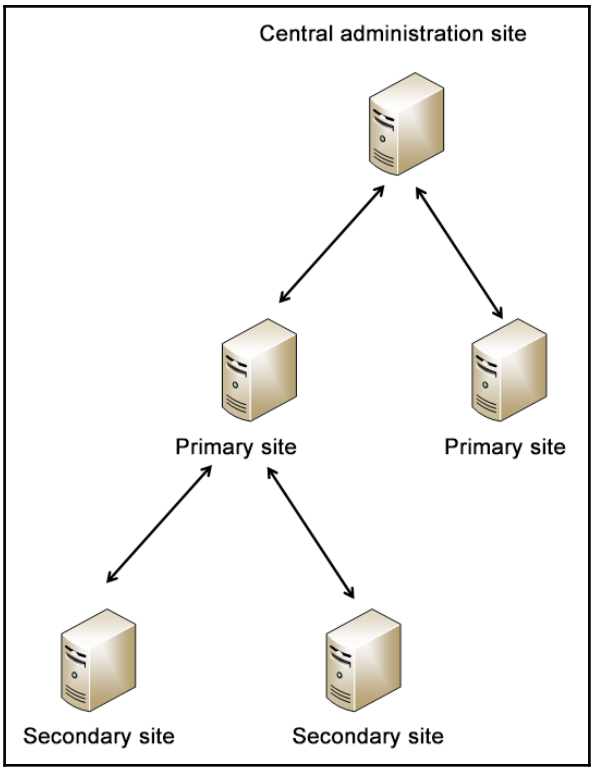
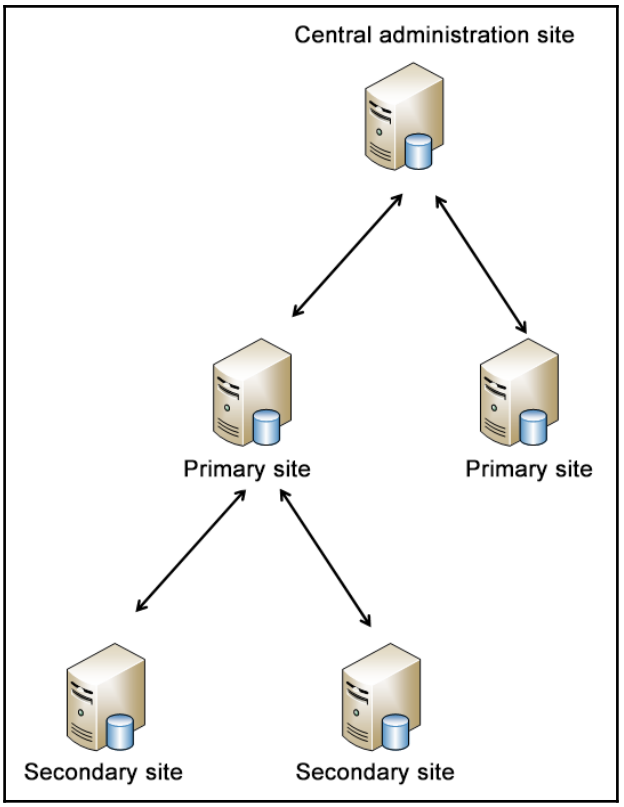
# Chapter 1: Design Planning

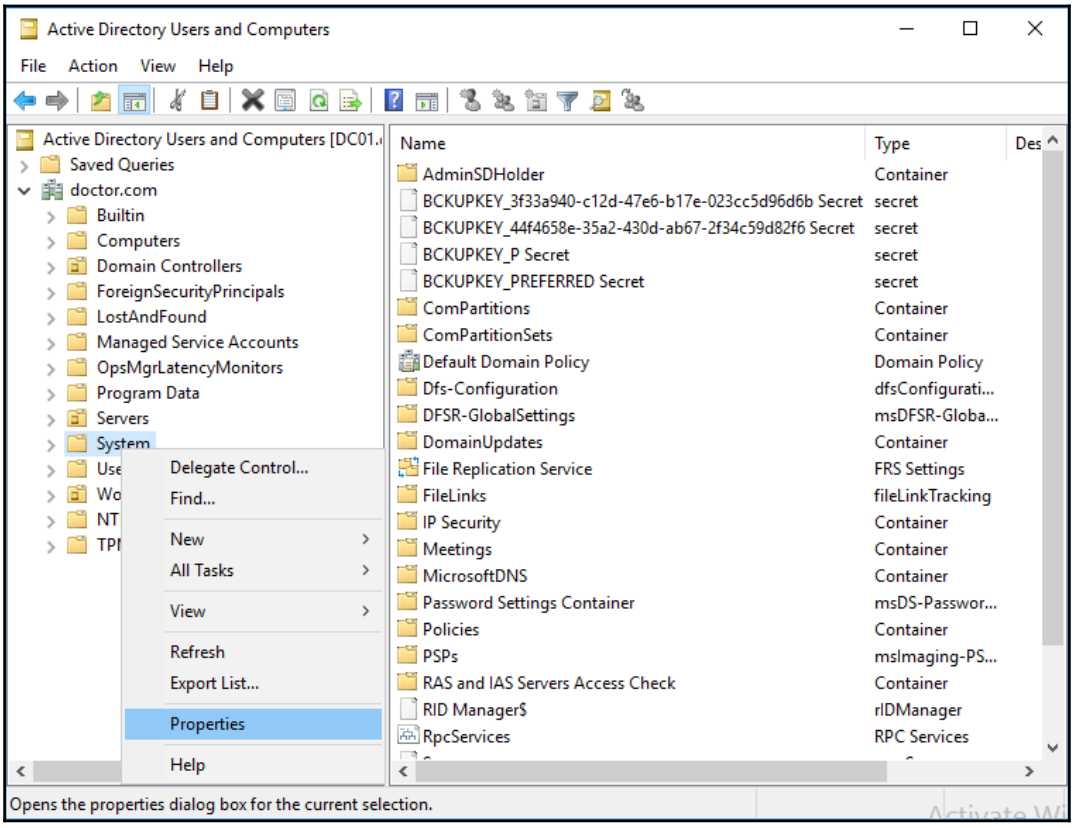


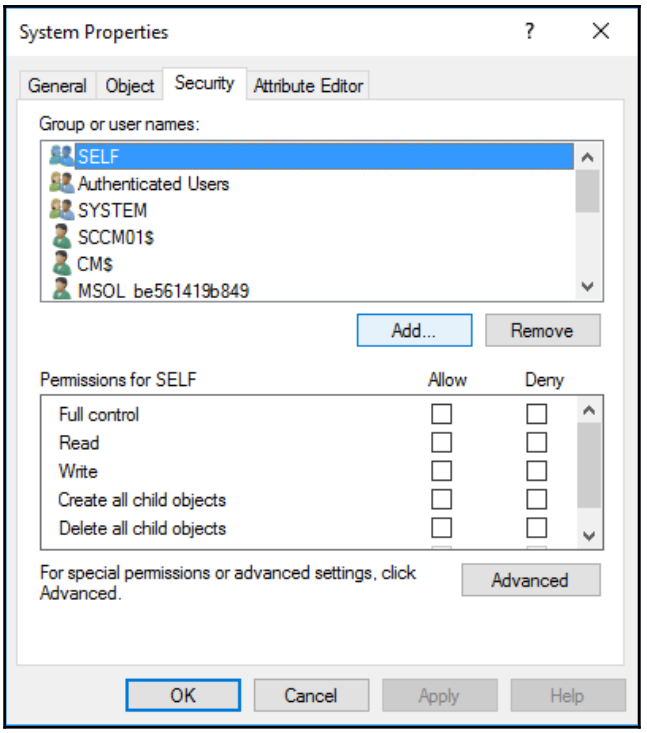



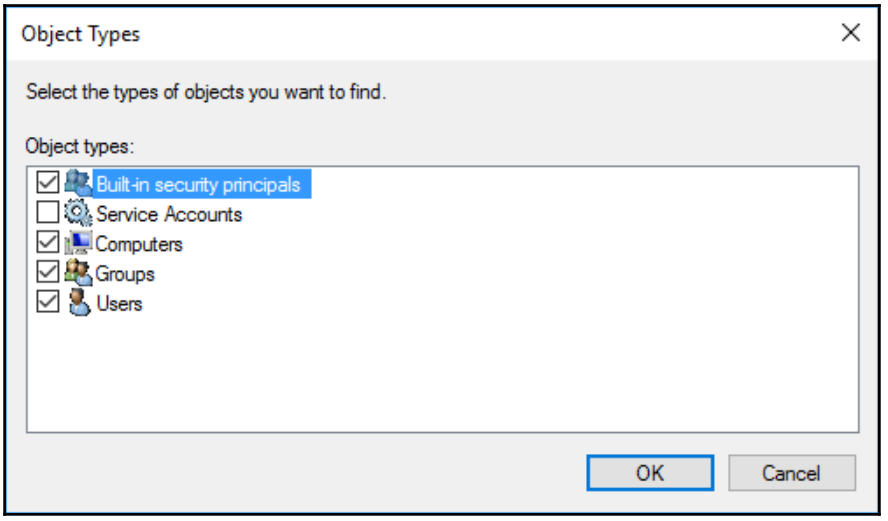

Central administration site
Primary site
Primary site
Secondary site
Secondary site

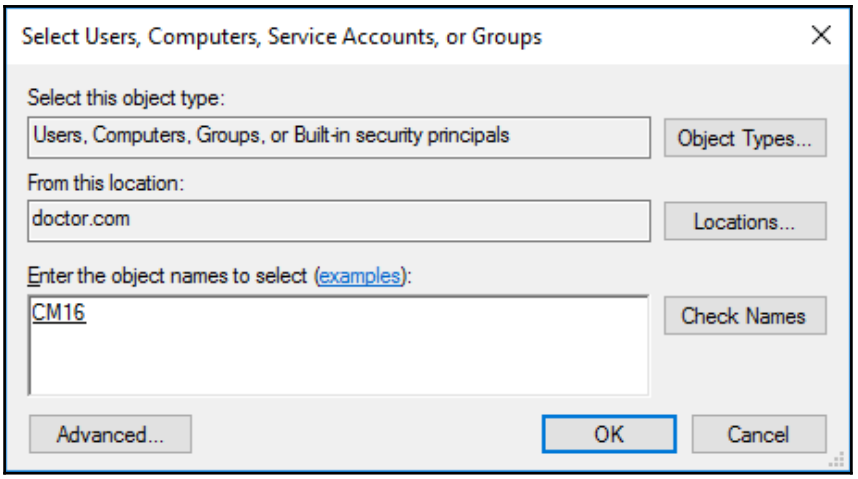

Central administration site
Primary site
Primary site
Secondary site
Secondary site

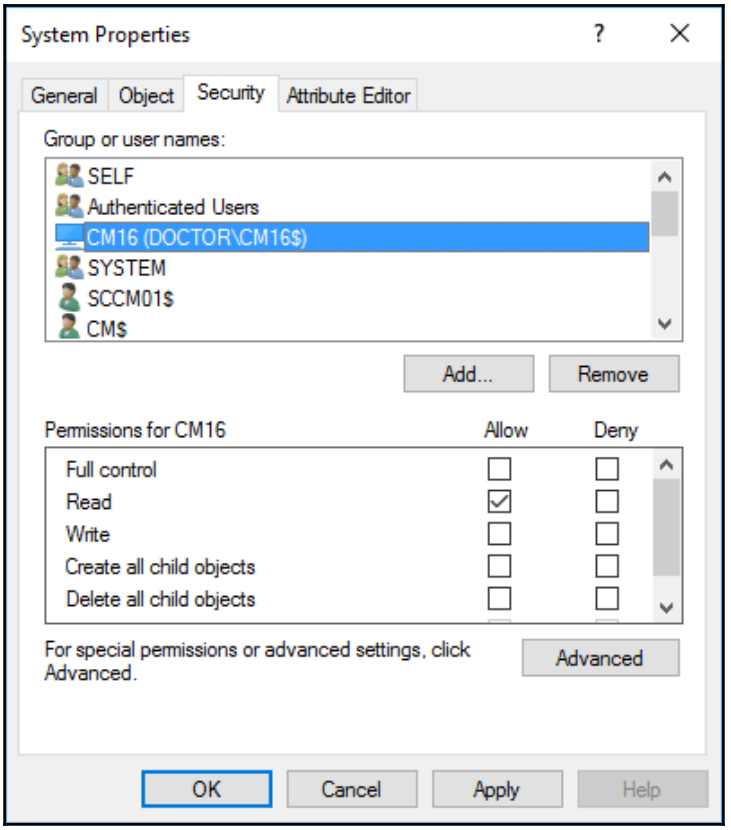
# Chapter 2: Installing Configuration Manager

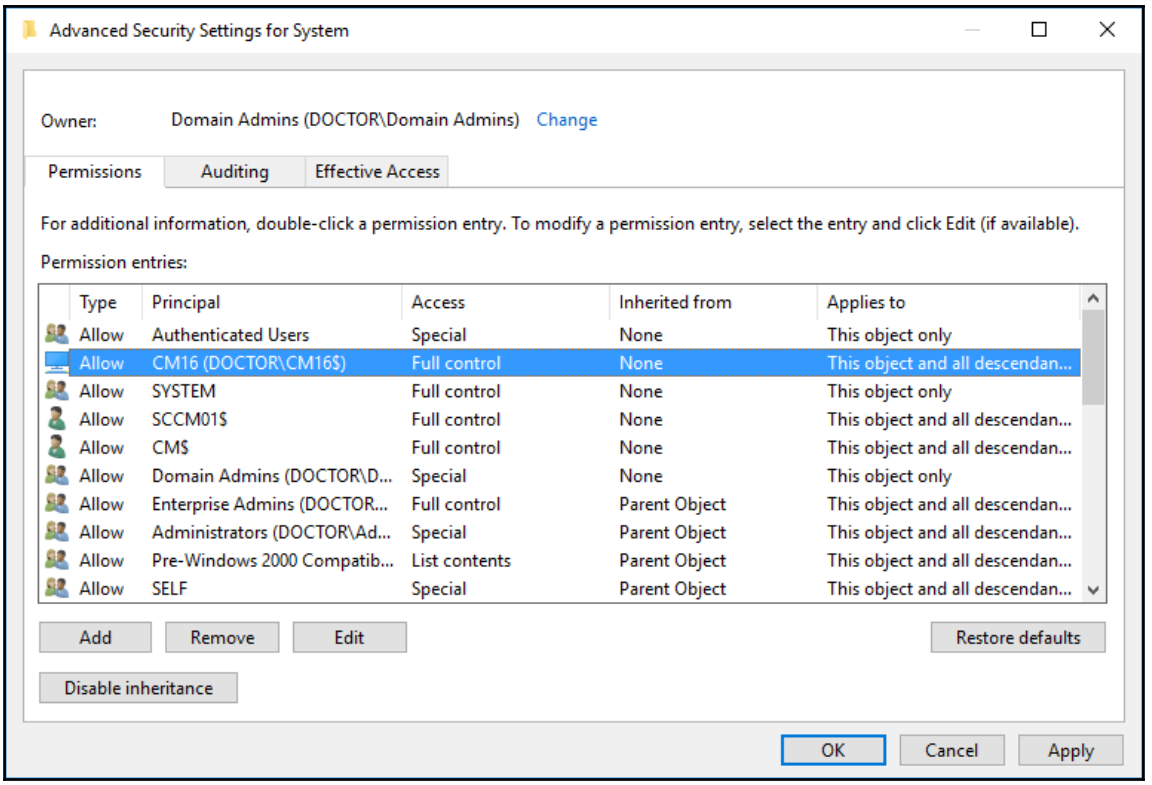


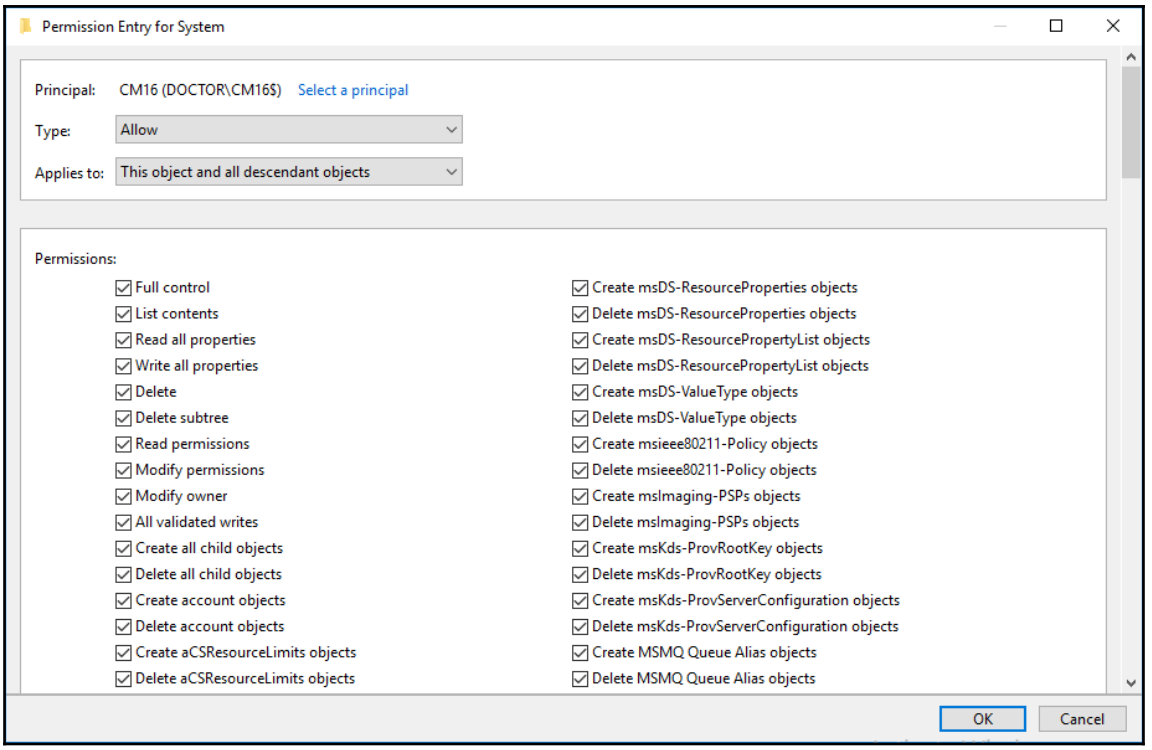

System Properties
General
Object
Security
Attribute Editor
Group or user names:
SELF
Authenticated Users
SYSTEM
SCCM01$
CM$
MSOL_be561419b849
Add...
Remove
Permissions for SELF
Allow
Deny
Full control
Read
Write
Create all child objects
Delete all child objects
For special permissions or advanced settings, click Advanced.
Advanced
OK
Cancel
Apply
Help

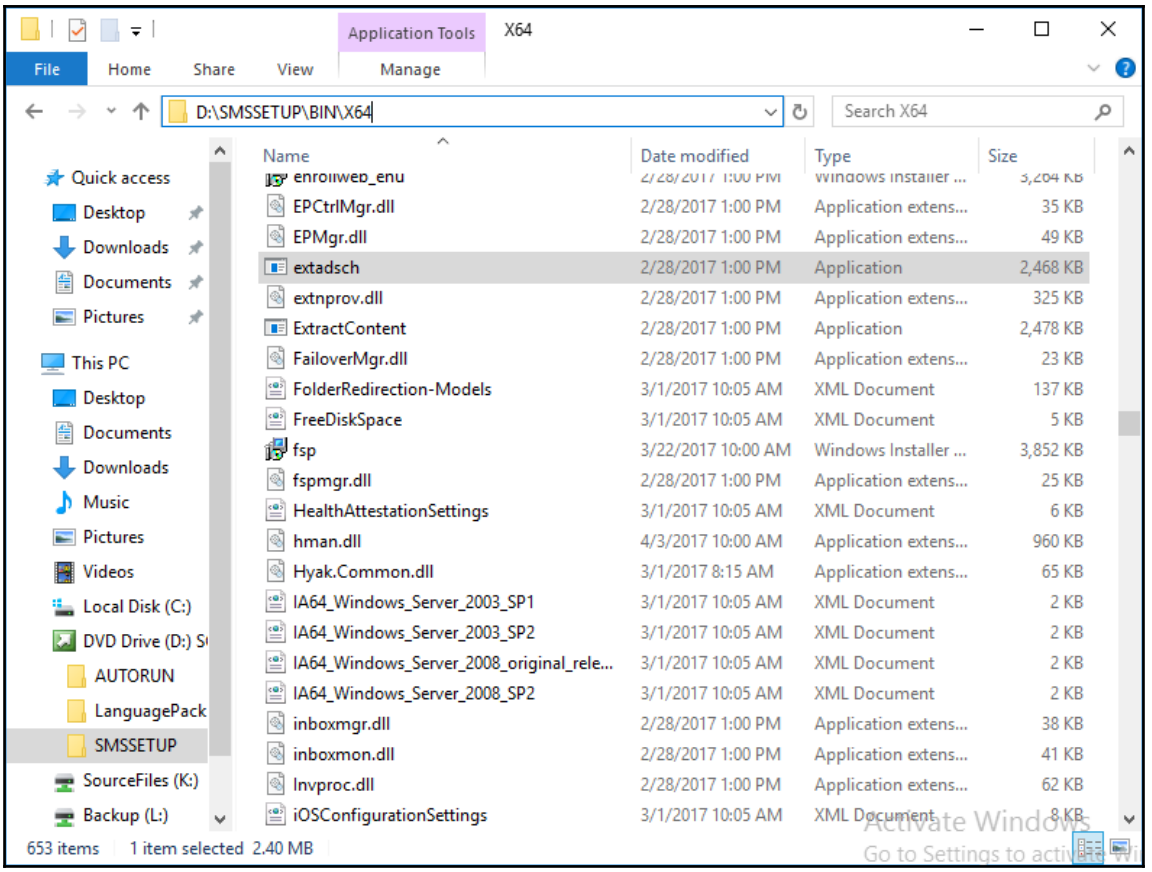

Object Types
Select the types of objects you want to find.
Object types:
Built-in security principals
Service Accounts
Computers
Groups
Users
OK
Cancel

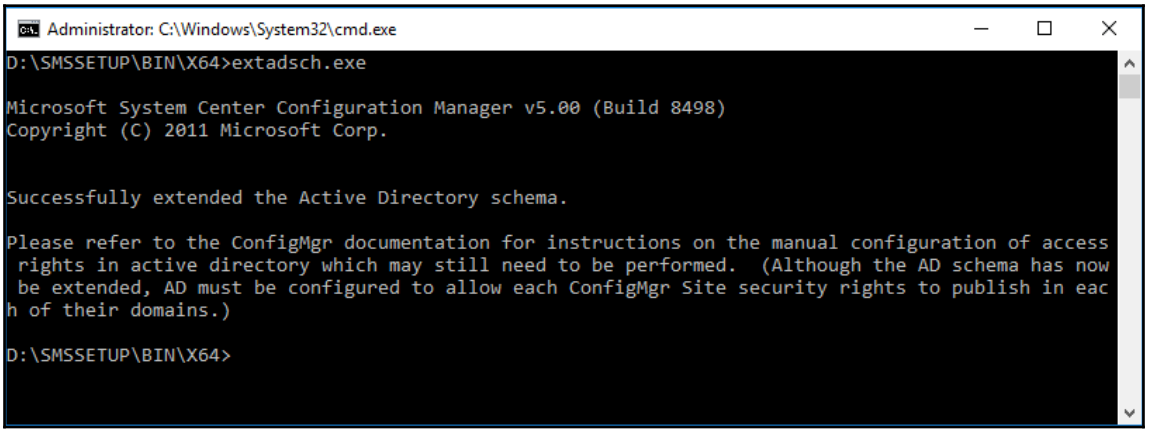

Select Users, Computers, Service Accounts, or Groups
Select this object type:
Users, Computers, Groups, or Built-in security principals
Object Types...
From this location:
doctor.com
Locations...
Enter the object names to select (examples):
CM16
Check Names
Advanced...
OK
Cancel

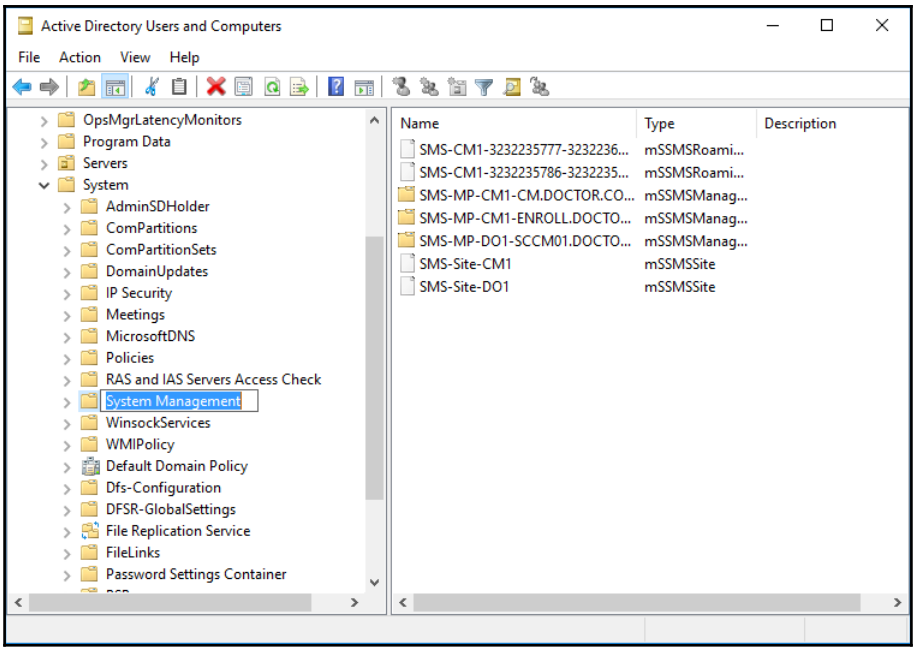

System Properties
General
Object
Security
Attribute Editor
Group or user names:
SELF
Authenticated Users
CM16 (DOCTOR\CM16$)
SYSTEM
SCCM01$
CM$
Add...
Remove
Permissions for CM16
Allow
Deny
Full control
Read
Write
Create all child objects
Delete all child objects
For special permissions or advanced settings, click Advanced.
Advanced
OK
Cancel
Apply
Help

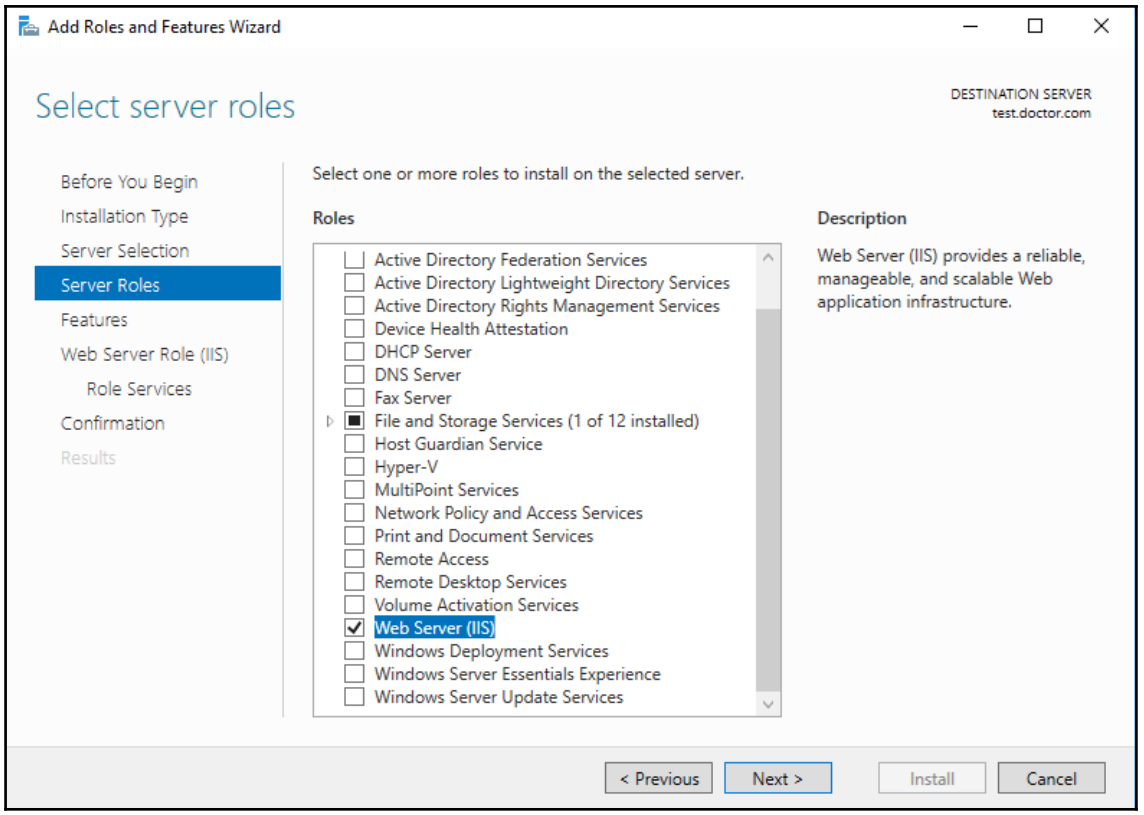

Advanced Security Settings for System
Owner: Domain Admins (DOCTOR\Domain Admins) Change
Permissions
Auditing
Effective Access
For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).
Permission entries:
Type Principal Access Inherited from Applies to
Allow Authenticated Users Special None This object only
Allow CM16 (DOCTOR\CM16$) Full control None This object and all descendan...
Allow SYSTEM Full control None This object only
Allow SCCM01$ Full control None This object and all descendan...
Allow CM$ Full control None This object and all descendan...
Allow Domain Admins (DOCTOR\D... Special None This object only
Allow Enterprise Admins (DOCTOR... Full control Parent Object This object and all descendan...
Allow Administrators (DOCTOR\Ad... Special Parent Object This object and all descendan...
Allow Pre-Windows 2000 Compatib... List contents Parent Object This object and all descendan...
Allow SELF Special Parent Object This object and all descendan...
Add
Remove
Edit
Restore defaults
Disable inheritance
OK
Cancel
Apply

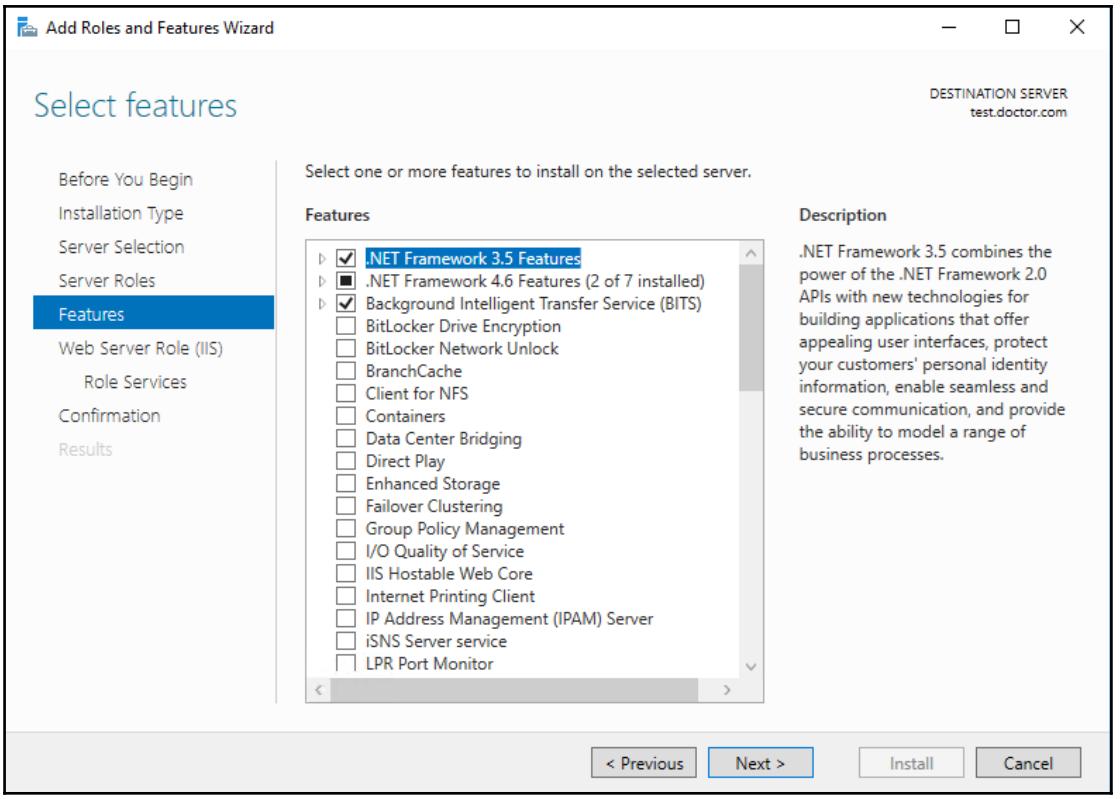

Permission Entry for System
Principal: CM16 (DOCTOR\CM16$) Select a principal
Type: Allow
Applies to: This object and all descendant objects
Permissions:
Full control
List contents
Read all properties
Write all properties
Delete
Delete subtree
Read permissions
Modify permissions
Modify owner
All validated writes
Create all child objects
Delete all child objects
Create account objects
Delete account objects
Create aCSResourceLimits objects
Delete aCSResourceLimits objects
Create msDS-ResourceProperties objects
Delete msDS-ResourceProperties objects
Create msDS-ResourcePropertyList objects
Delete msDS-ResourcePropertyList objects
Create msDS-ValueType objects
Delete msDS-ValueType objects
Create msieee80211-Policy objects
Delete msieee80211-Policy objects
Create mslmaging-PSPs objects
Delete mslmaging-PSPs objects
Create msKds-ProvRootKey objects
Delete msKds-ProvRootKey objects
Create msKds-ProvServerConfiguration objects
Delete msKds-ProvServerConfiguration objects
Create MSMQ Queue Alias objects
Delete MSMQ Queue Alias objects
OK
Cancel

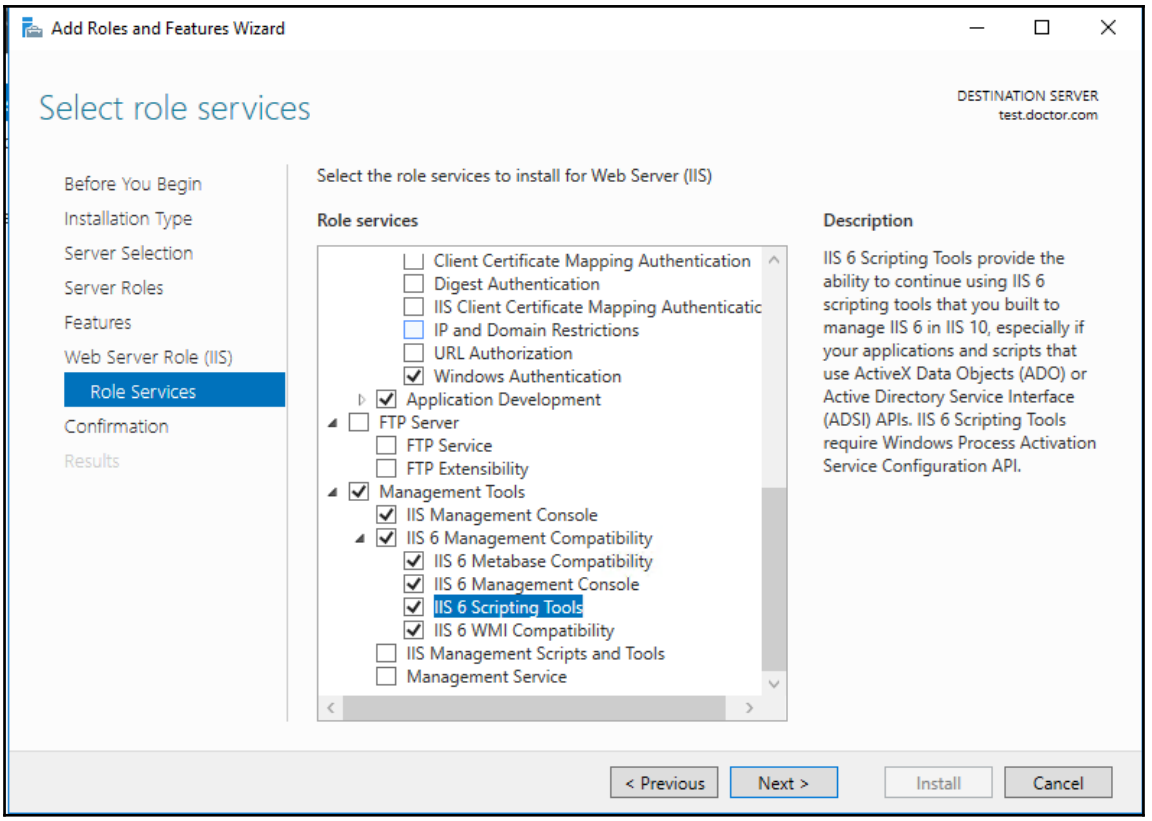

Application Tools
X64
File
Home
Share
View
Manage
D:\SMSSETUP\BIN\X64
Search X64
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
DVD Drive (D:) S
AUTORUN
LanguagePack
SMSSETUP
SourceFiles (K:)
Backup (L:)
Name
Date modified
Type
Size
EPCtrlMgr.dll 2/28/2017 1:00 PM Application extens... 35 KB
EPMgr.dll 2/28/2017 1:00 PM Application extens... 49 KB
extadsch 2/28/2017 1:00 PM Application 2,468 KB
extnprov.dll 2/28/2017 1:00 PM Application extens... 325 KB
ExtractContent 2/28/2017 1:00 PM Application 2,478 KB
FailoverMgr.dll 2/28/2017 1:00 PM Application extens... 23 KB
FolderRedirection-Models 3/1/2017 10:05 AM XML Document 137 KB
FreeDiskSpace 3/1/2017 10:05 AM XML Document 5 KB
fsp 3/22/2017 10:00 AM Windows Installer ... 3,852 KB
fspmgr.dll 2/28/2017 1:00 PM Application extens... 25 KB
HealthAttestationSettings 3/1/2017 10:05 AM XML Document 6 KB
hman.dll 4/3/2017 10:00 AM Application extens... 960 KB
Hyak.Common.dll 3/1/2017 8:15 AM Application extens... 65 KB
IA64_Windows_Server_2003_SP1 3/1/2017 10:05 AM XML Document 2 KB
IA64_Windows_Server_2003_SP2 3/1/2017 10:05 AM XML Document 2 KB
IA64_Windows_Server_2008_original_rele... 3/1/2017 10:05 AM XML Document 2 KB
IA64_Windows_Server_2008_SP2 3/1/2017 10:05 AM XML Document 2 KB
inboxmgr.dll 2/28/2017 1:00 PM Application extens... 38 KB
inboxmon.dll 2/28/2017 1:00 PM Application extens... 41 KB
Invproc.dll 2/28/2017 1:00 PM Application extens... 62 KB
iOSConfigurationSettings 3/1/2017 10:05 AM XML Document 8 KB
653 items
1 item selected 2.40 MB
Activate Windows
Go to Settings to activate Wi

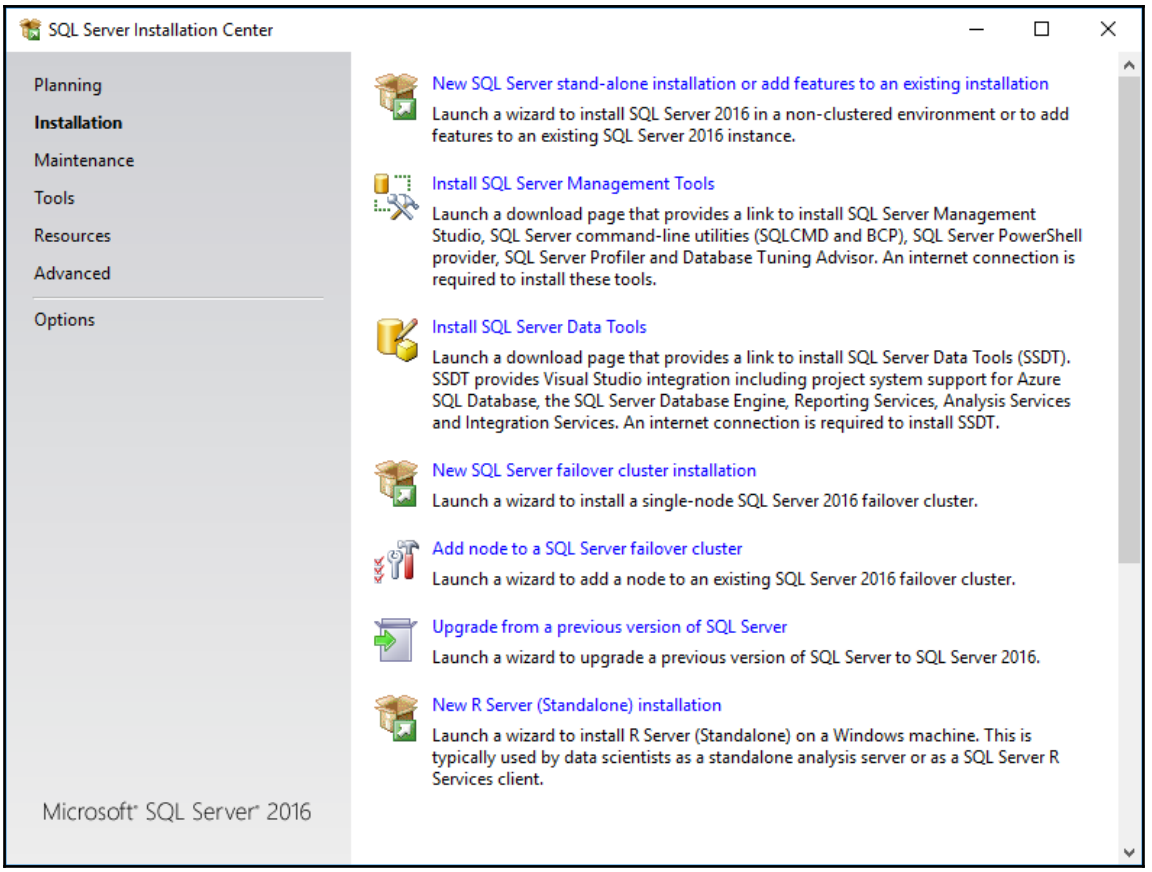

Administrator: C:\Windows\System32\cmd.exe
D:\SMSSETUP\BIN\X64>extadsch.exe
Microsoft System Center Configuration Manager v5.00 (Build 8498)
Copyright (C) 2011 Microsoft Corp.
Successfully extended the Active Directory schema.
Please refer to the ConfigMgr documentation for instructions on the manual configuration of access
rights in active directory which may still need to be performed. (Although the AD schema has now
be extended, AD must be configured to allow each ConfigMgr Site security rights to publish in eac
h of their domains.)
D:\SMSSETUP\BIN\X64>

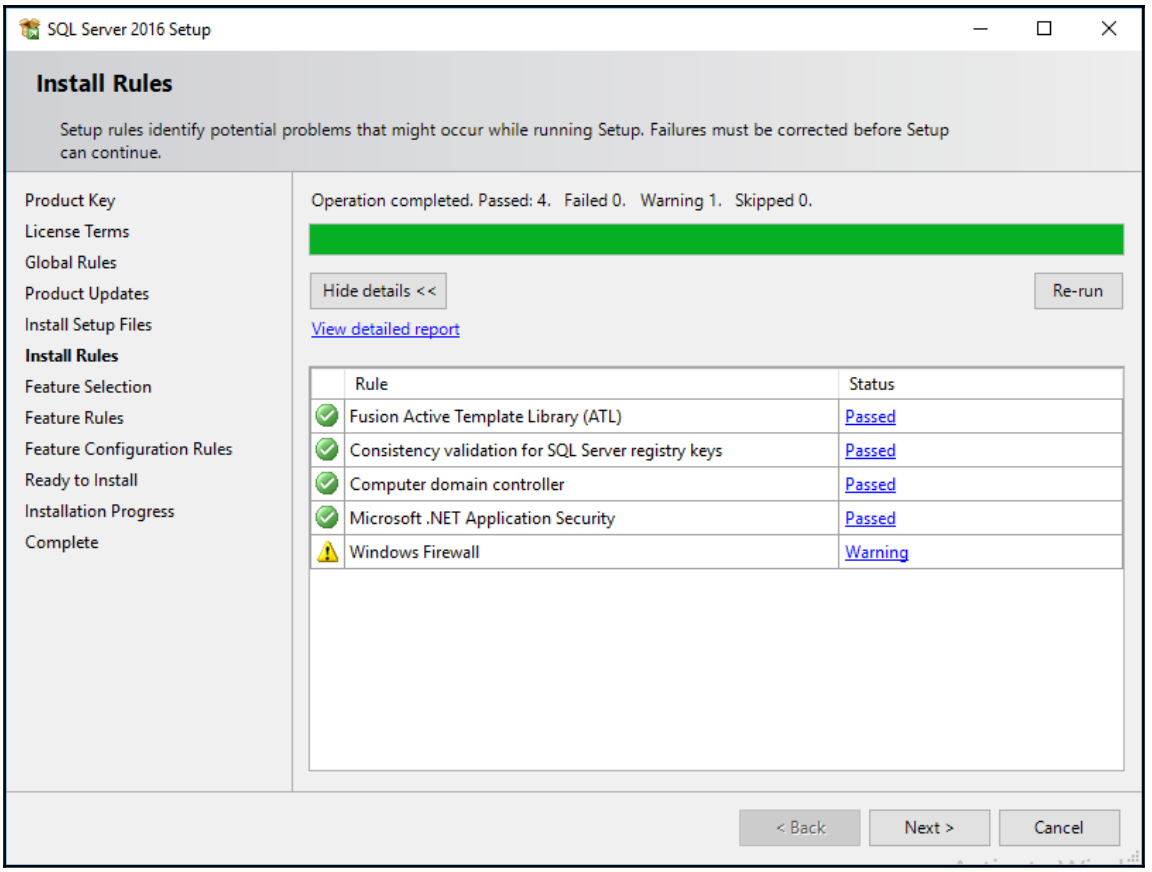

Active Directory Users and Computers
File
Action
View
Help
OpsMgrLatencyMonitors
Program Data
Servers
System
AdminSDHolder
ComPartitions
ComPartitionSets
DomainUpdates
IP Security
Meetings
MicrosoftDNS
Policies
RAS and IAS Servers Access Check
System Management
WinsockServices
WMIPolicy
Default Domain Policy
Dfs-Configuration
DFSR-GlobalSettings
File Replication Service
FileLinks
Password Settings Container
Name
Type
Description
SMS-CM1-3232235777-3232236...
mSSMSRoami...
SMS-CM1-3232235786-3232235...
mSSMSRoami...
SMS-MP-CM1-CM.DOCTOR.CO...
mSSMSManag...
SMS-MP-CM1-ENROLL.DOCTO...
mSSMSManag...
SMS-MP-DO1-SCCM01.DOCTO...
mSSMSManag...
SMS-Site-CM1
mSSMSSite
SMS-Site-DO1
mSSMSSite

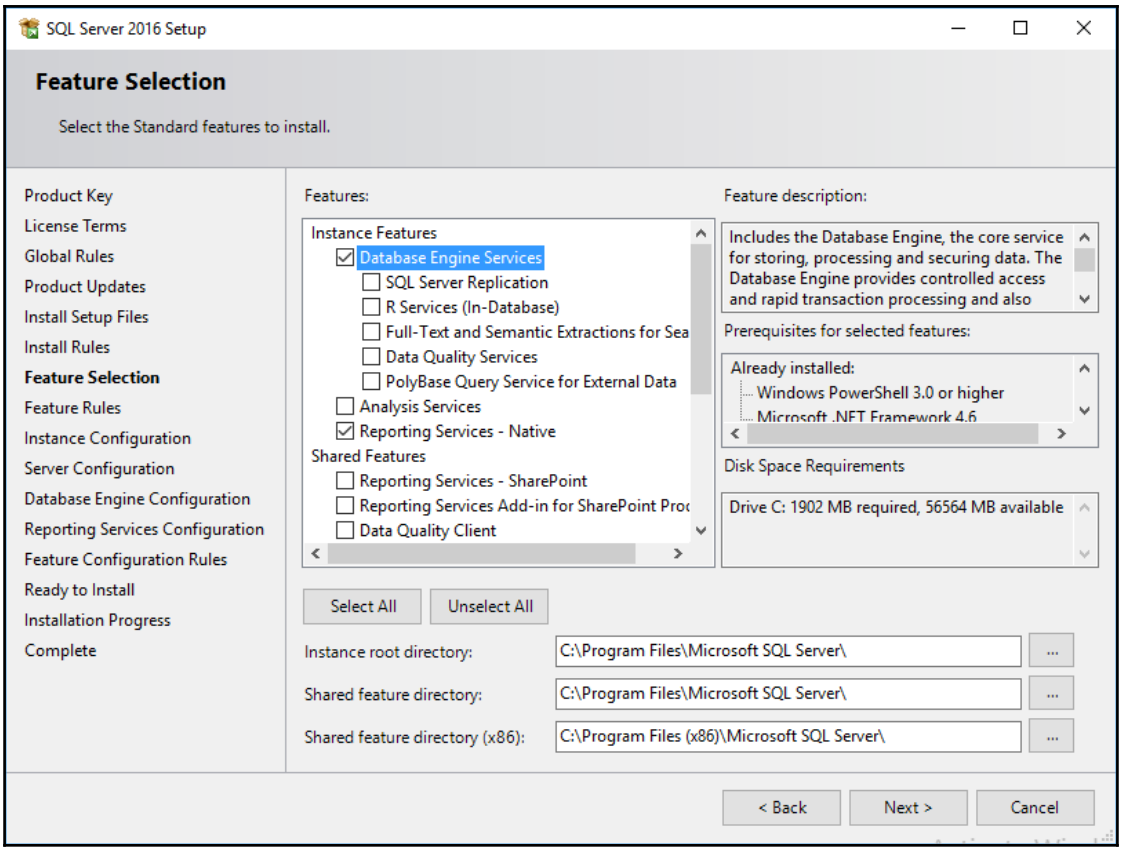

Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
test.doctor.com
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Web Server Role (IIS)
Role Services
Confirmation
Results
Select one or more roles to install on the selected server.
Roles
Active Directory Federation Services
Active Directory Lightweight Directory Services
Active Directory Rights Management Services
Device Health Attestation
DHCP Server
DNS Server
Fax Server
File and Storage Services (1 of 12 installed)
Host Guardian Service
Hyper-V
MultiPoint Services
Network Policy and Access Services
Print and Document Services
Remote Access
Remote Desktop Services
Volume Activation Services
Web Server (IIS)
Windows Deployment Services
Windows Server Essentials Experience
Windows Server Update Services
Description
Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.
< Previous
Next >
Install
Cancel

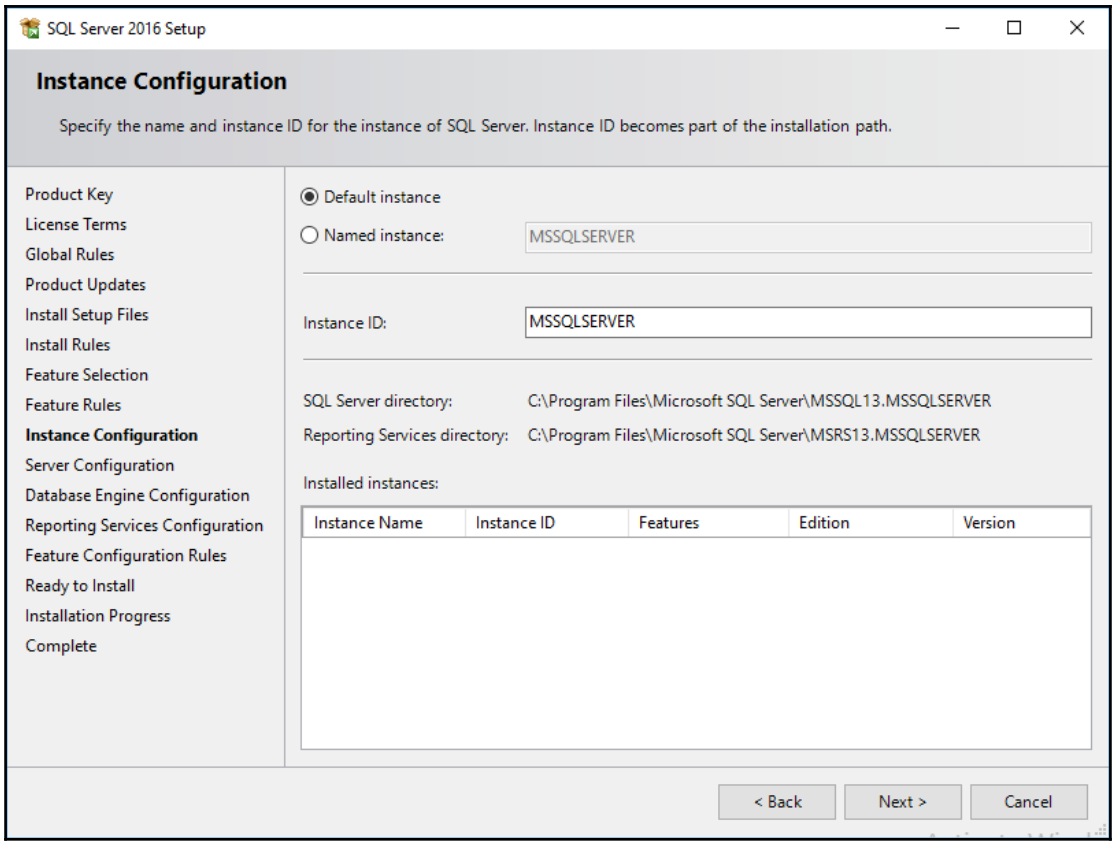

Add Roles and Features Wizard
Select features
DESTINATION SERVER
test.doctor.com
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Web Server Role (IIS)
Role Services
Confirmation
Results
Select one or more features to install on the selected server.
Features
.NET Framework 3.5 Features
.NET Framework 4.6 Features (2 of 7 installed)
Background Intelligent Transfer Service (BITS)
BitLocker Drive Encryption
BitLocker Network Unlock
BranchCache
Client for NFS
Containers
Data Center Bridging
Direct Play
Enhanced Storage
Failover Clustering
Group Policy Management
I/O Quality of Service
IIS Hostable Web Core
Internet Printing Client
IP Address Management (IPAM) Server
iSNS Server service
LPR Port Monitor
Description
.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.
< Previous
Next >
Install
Cancel

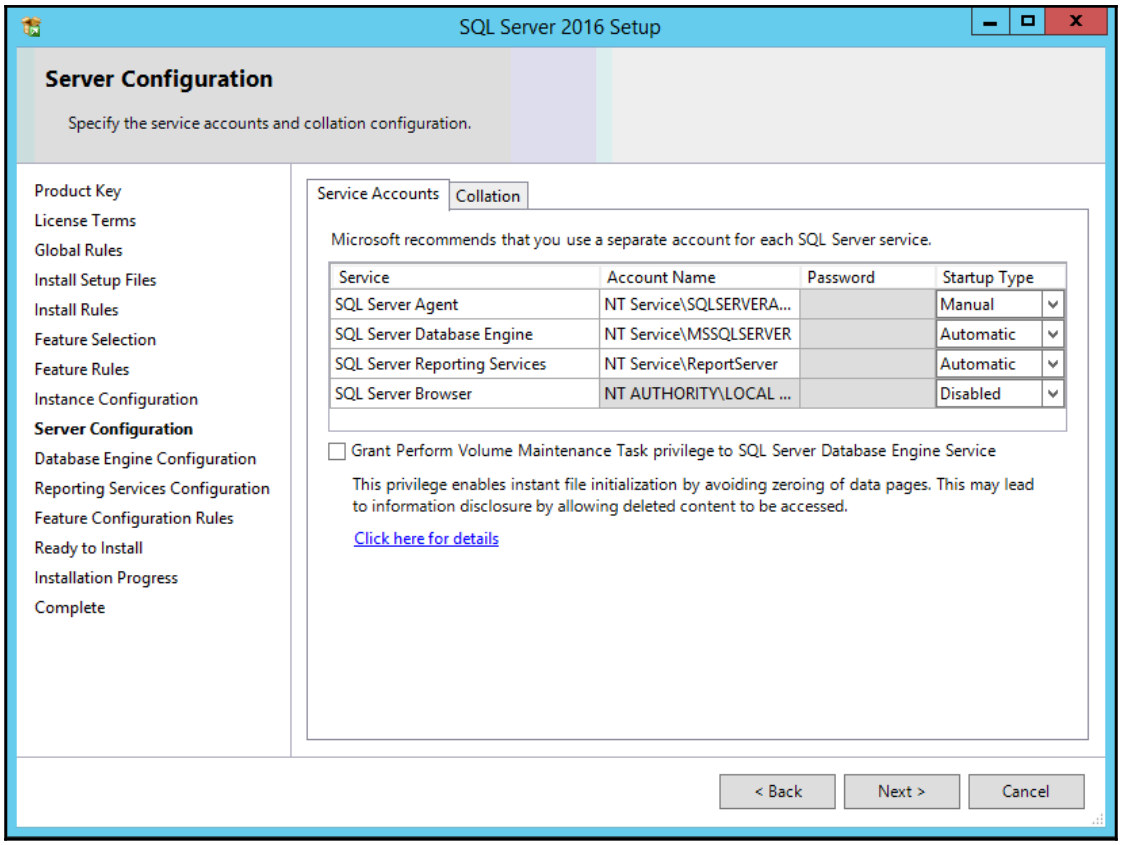

Add Roles and Features Wizard
Select role services
DESTINATION SERVER
test.doctor.com
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Web Server Role (IIS)
Role Services
Confirmation
Results
Select the role services to install for Web Server (IIS)
Role services
Client Certificate Mapping Authentication
Digest Authentication
IIS Client Certificate Mapping Authenticatic
IP and Domain Restrictions
URL Authorization
Windows Authentication
Application Development
FTP Server
FTP Service
FTP Extensibility
Management Tools
IIS Management Console
IIS 6 Management Compatibility
IIS 6 Metabase Compatibility
IIS 6 Management Console
IIS 6 Scripting Tools
IIS 6 WMI Compatibility
IIS Management Scripts and Tools
Management Service
Description
IIS 6 Scripting Tools provide the ability to continue using IIS 6 scripting tools that you built to manage IIS 6 in IIS 10, especially if your applications and scripts that use ActiveX Data Objects (ADO) or Active Directory Service Interface (ADSI) APIs. IIS 6 Scripting Tools require Windows Process Activation Service Configuration API.
< Previous
Next >
Install
Cancel

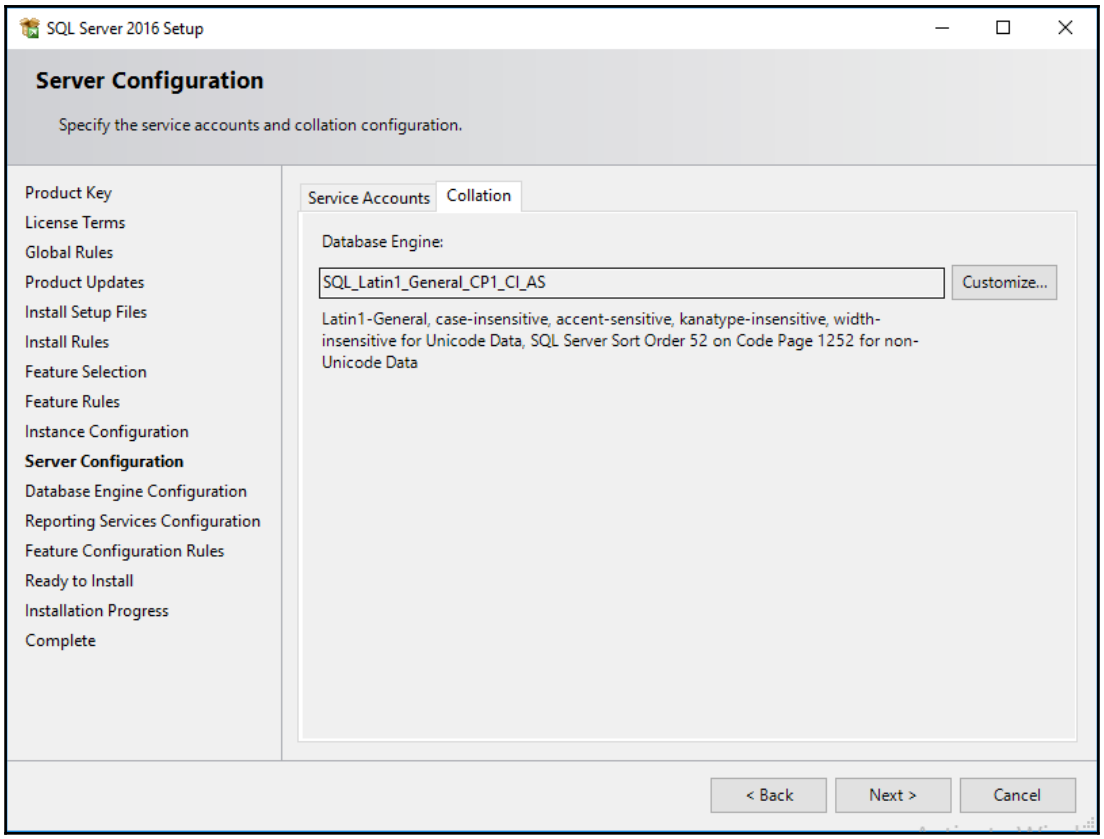

SQL Server Installation Center
Planning
Installation
Maintenance
Tools
Resources
Advanced
Options
Microsoft SQL Server 2016
New SQL Server stand-alone installation or add features to an existing installation
Launch a wizard to install SQL Server 2016 in a non-clustered environment or to add features to an existing SQL Server 2016 instance.
Install SQL Server Management Tools
Launch a download page that provides a link to install SQL Server Management Studio, SQL Server command-line utilities (SQLCMD and BCP), SQL Server PowerShell provider, SQL Server Profiler and Database Tuning Advisor. An internet connection is required to install these tools.
Install SQL Server Data Tools
Launch a download page that provides a link to install SQL Server Data Tools (SSDT). SSDT provides Visual Studio integration including project system support for Azure SQL Database, the SQL Server Database Engine, Reporting Services, Analysis Services and Integration Services. An internet connection is required to install SSDT.
New SQL Server failover cluster installation
Launch a wizard to install a single-node SQL Server 2016 failover cluster.
Add node to a SQL Server failover cluster
Launch a wizard to add a node to an existing SQL Server 2016 failover cluster.
Upgrade from a previous version of SQL Server
Launch a wizard to upgrade a previous version of SQL Server to SQL Server 2016.
New R Server (Standalone) installation
Launch a wizard to install R Server (Standalone) on a Windows machine. This is typically used by data scientists as a standalone analysis server or as a SQL Server R Services client.

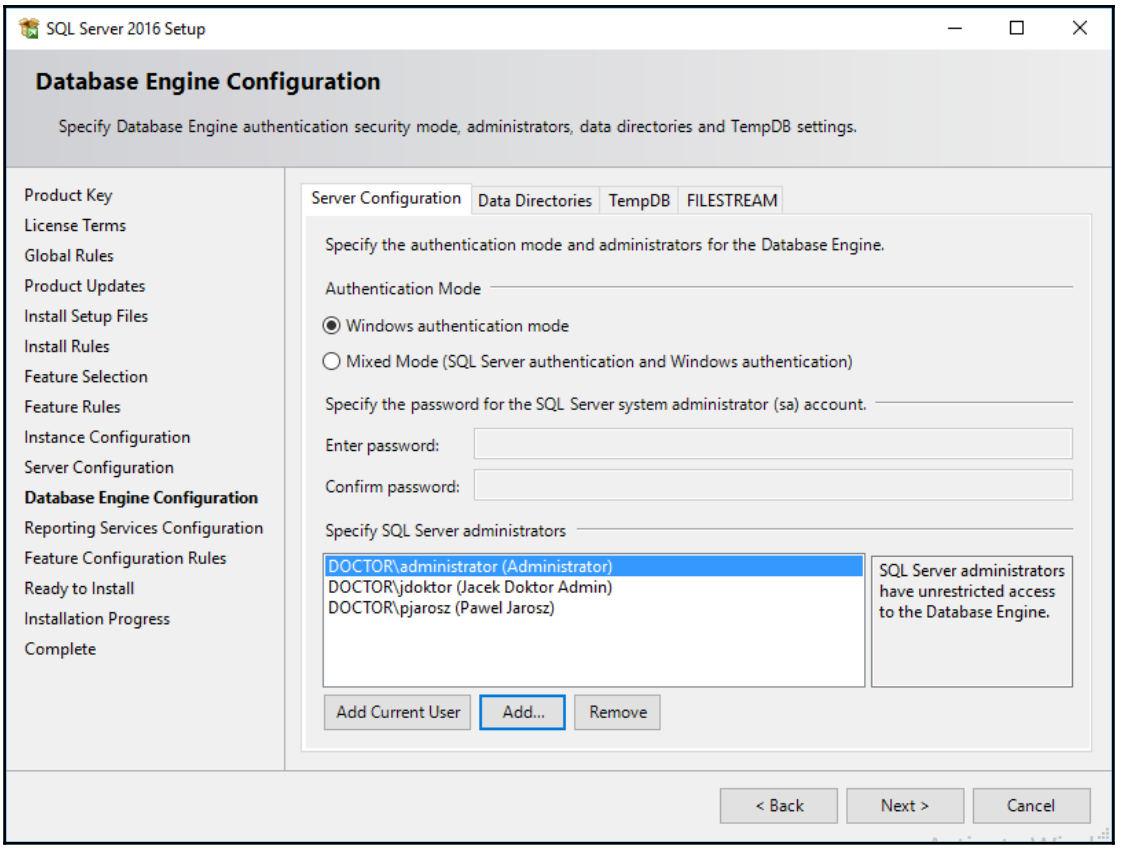

SQL Server 2016 Setup
Install Rules
Setup rules identify potential problems that might occur while running Setup. Failures must be corrected before Setup can continue.
Product Key
License Terms
Global Rules
Product Updates
Install Setup Files
Install Rules
Feature Selection
Feature Rules
Feature Configuration Rules
Ready to Install
Installation Progress
Complete
Operation completed. Passed: 4. Failed 0. Warning 1. Skipped 0.
Hide details <<
Re-run
View detailed report
Rule
Status
Fusion Active Template Library (ATL)
Passed
Consistency validation for SQL Server registry keys
Passed
Computer domain controller
Passed
Microsoft .NET Application Security
Passed
Windows Firewall
Warning
< Back
Next >
Cancel

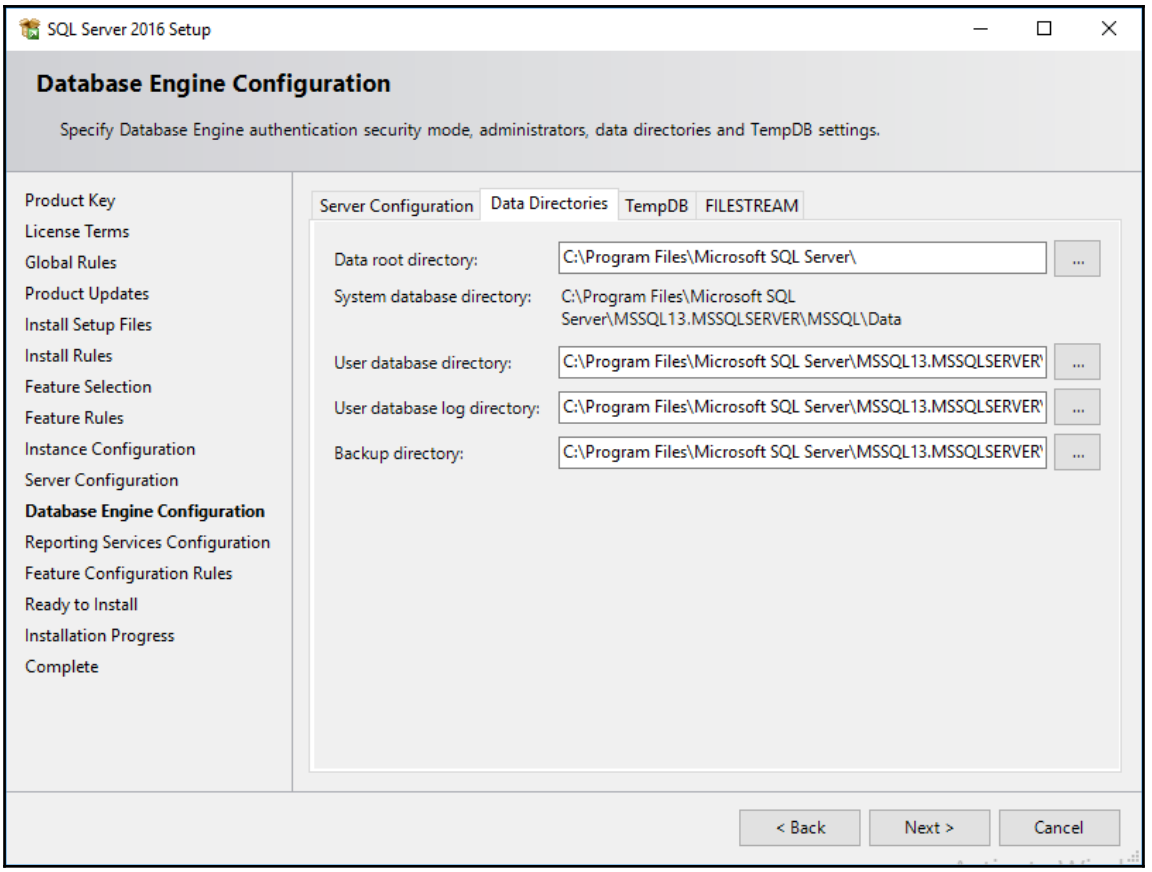

SQL Server 2016 Setup
Feature Selection
Select the Standard features to install.
Product Key
License Terms
Global Rules
Product Updates
Install Setup Files
Install Rules
Feature Selection
Feature Rules
Instance Configuration
Server Configuration
Database Engine Configuration
Reporting Services Configuration
Feature Configuration Rules
Ready to Install
Installation Progress
Complete
Features:
Instance Features
Database Engine Services
SQL Server Replication
R Services (In-Database)
Full-Text and Semantic Extractions for Sea
Data Quality Services
PolyBase Query Service for External Data
Analysis Services
Reporting Services - Native
Shared Features
Reporting Services - SharePoint
Reporting Services Add-in for SharePoint Proc
Data Quality Client
Feature description:
Includes the Database Engine, the core service for storing, processing and securing data. The Database Engine provides controlled access and rapid transaction processing and also
Prerequisites for selected features:
Already installed:
Windows PowerShell 3.0 or higher
Microsoft .NET Framework 4.6
Disk Space Requirements
Drive C: 1902 MB required, 56564 MB available
Select All
Unselect All
Instance root directory:
C:\Program Files\Microsoft SQL Server\
Shared feature directory:
C:\Program Files\Microsoft SQL Server\
Shared feature directory (x86):
C:\Program Files (x86)\Microsoft SQL Server\
< Back
Next >
Cancel

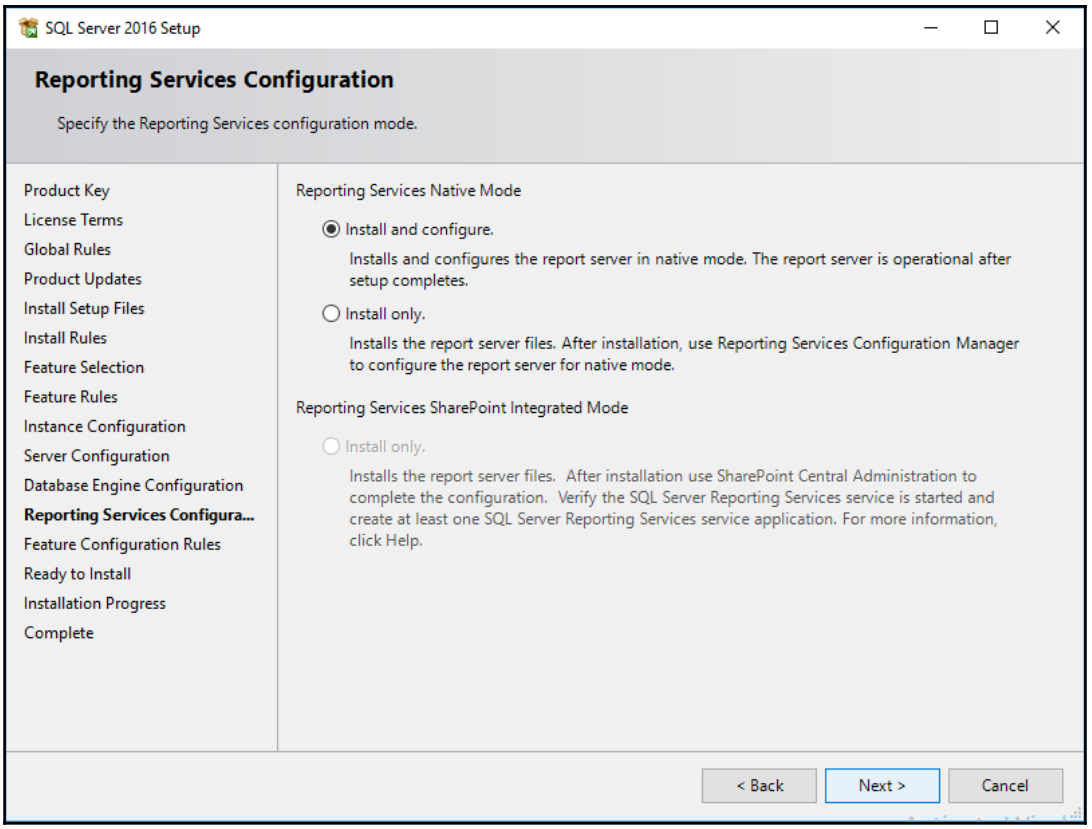

SQL Server 2016 Setup
Instance Configuration
Specify the name and instance ID for the instance of SQL Server. Instance ID becomes part of the installation path.
Product Key
License Terms
Global Rules
Product Updates
Install Setup Files
Install Rules
Feature Selection
Feature Rules
Instance Configuration
Server Configuration
Database Engine Configuration
Reporting Services Configuration
Feature Configuration Rules
Ready to Install
Installation Progress
Complete
Default instance
Named instance:
MSSQLSERVER
Instance ID:
MSSQLSERVER
SQL Server directory:
C:\Program Files\Microsoft SQL Server\MSSQL13.MSSQLSERVER
Reporting Services directory:
C:\Program Files\Microsoft SQL Server\MSRS13.MSSQLSERVER
Installed instances:
Instance Name
Instance ID
Features
Edition
Version
< Back
Next >
Cancel

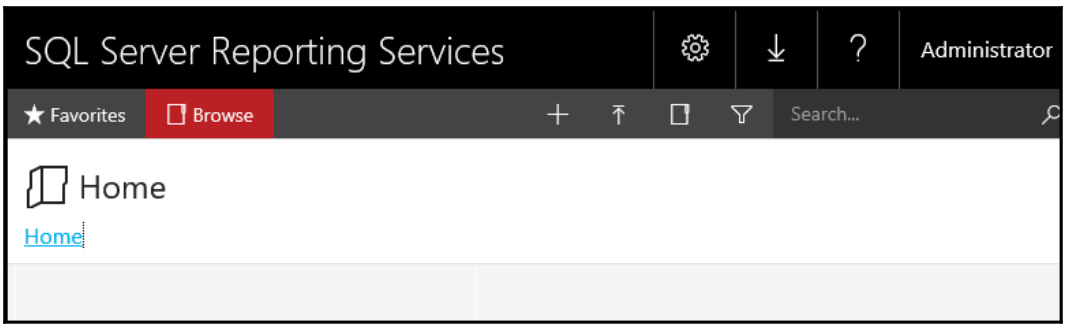

SQL Server 2016 Setup
Server Configuration
Specify the service accounts and collation configuration.
Product Key
License Terms
Global Rules
Install Setup Files
Install Rules
Feature Selection
Feature Rules
Instance Configuration
Server Configuration
Database Engine Configuration
Reporting Services Configuration
Feature Configuration Rules
Ready to Install
Installation Progress
Complete
Service Accounts
Collation
Microsoft recommends that you use a separate account for each SQL Server service.
Service
Account Name
Password
Startup Type
SQL Server Agent
NT Service\SQLSERVERA...
Manual
SQL Server Database Engine
NT Service\MSSQLSERVER
Automatic
SQL Server Reporting Services
NT Service\ReportServer
Automatic
SQL Server Browser
NT AUTHORITY\LOCAL ...
Disabled
Grant Perform Volume Maintenance Task privilege to SQL Server Database Engine Service
This privilege enables instant file initialization by avoiding zeroing of data pages. This may lead to information disclosure by allowing deleted content to be accessed.
Click here for details
< Back
Next >
Cancel

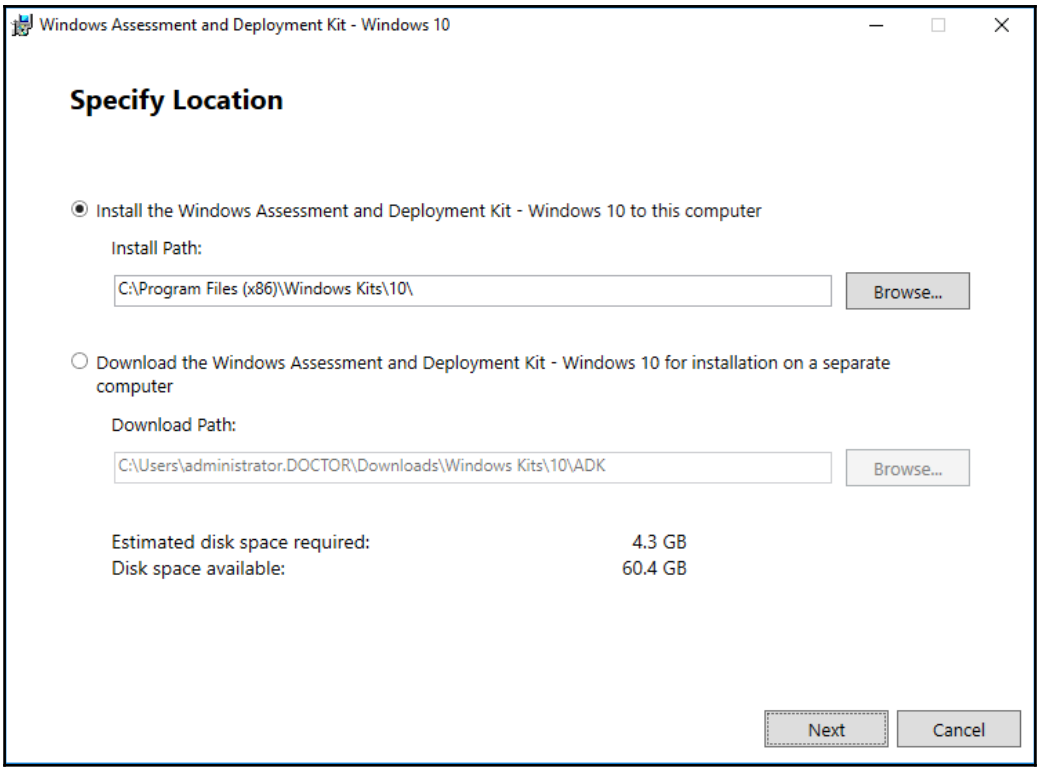

SQL Server 2016 Setup
Server Configuration
Specify the service accounts and collation configuration.
Product Key
License Terms
Global Rules
Product Updates
Install Setup Files
Install Rules
Feature Selection
Feature Rules
Instance Configuration
Server Configuration
Database Engine Configuration
Reporting Services Configuration
Feature Configuration Rules
Ready to Install
Installation Progress
Complete
Service Accounts
Collation
Database Engine:
SQL_Latin1_General_CP1_CI_AS
Customize...
Latin1-General, case-insensitive, accent-sensitive, kanatype-insensitive, width-insensitive for Unicode Data, SQL Server Sort Order 52 on Code Page 1252 for non-Unicode Data
< Back
Next >
Cancel

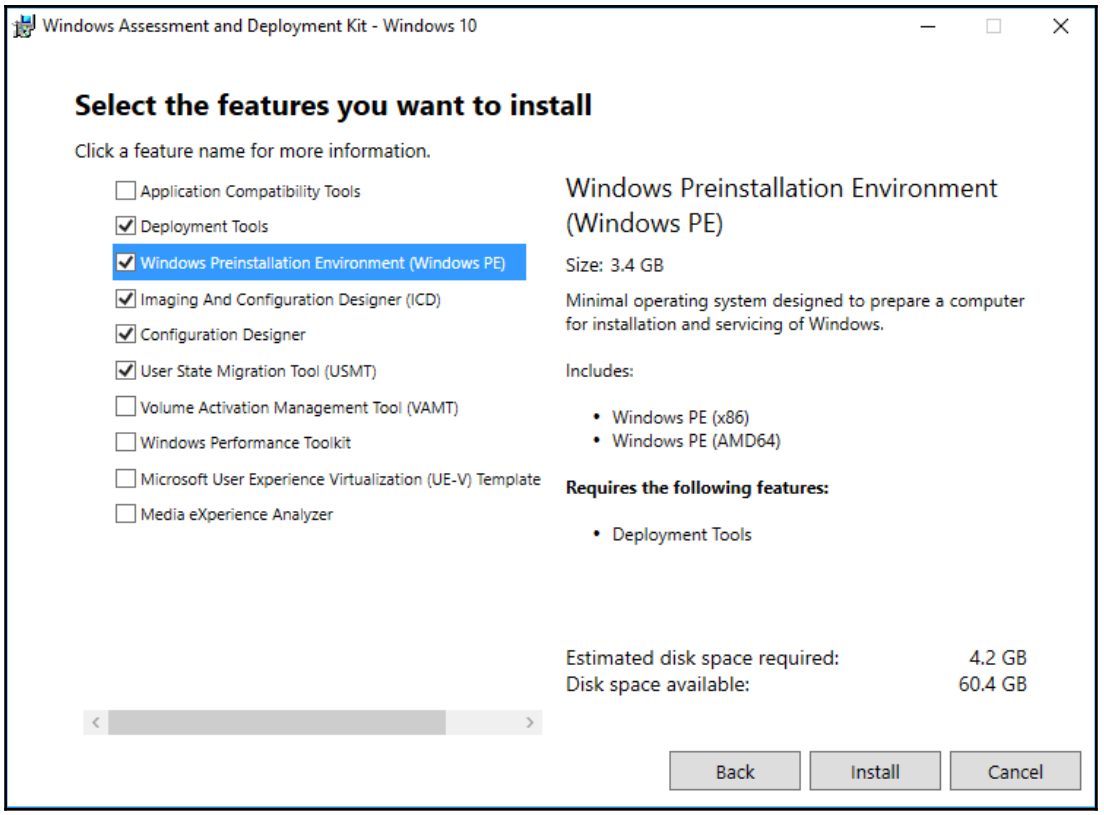

SQL Server 2016 Setup
Database Engine Configuration
Specify Database Engine authentication security mode, administrators, data directories and TempDB settings.
Product Key
License Terms
Global Rules
Product Updates
Install Setup Files
Install Rules
Feature Selection
Feature Rules
Instance Configuration
Server Configuration
Database Engine Configuration
Reporting Services Configuration
Feature Configuration Rules
Ready to Install
Installation Progress
Complete
Server Configuration
Data Directories
TempDB
FILESTREAM
Specify the authentication mode and administrators for the Database Engine.
Authentication Mode
Windows authentication mode
Mixed Mode (SQL Server authentication and Windows authentication)
Specify the password for the SQL Server system administrator (sa) account.
Enter password:
Confirm password:
Specify SQL Server administrators
DOCTOR\administrator (Administrator)
DOCTOR\jdoktor (Jacek Doktor Admin)
DOCTOR\pjarosz (Pawel Jarosz)
SQL Server administrators have unrestricted access to the Database Engine.
Add Current User
Add...
Remove
< Back
Next >
Cancel

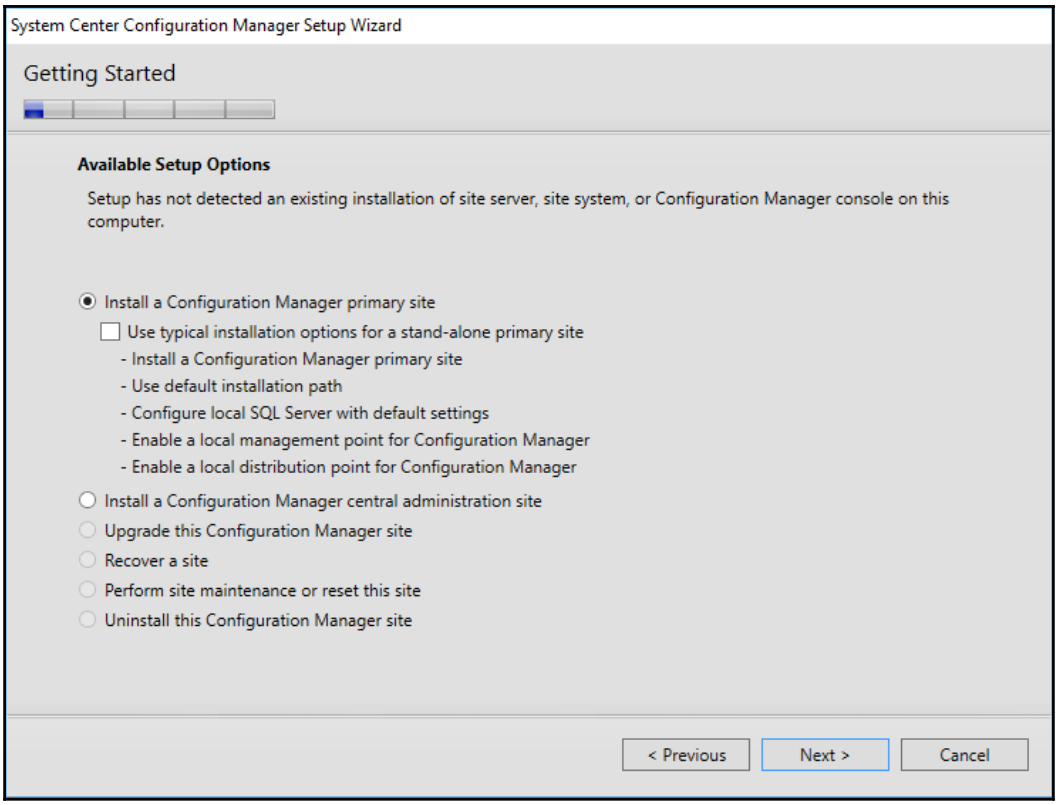

SQL Server 2016 Setup
Database Engine Configuration
Specify Database Engine authentication security mode, administrators, data directories and TempDB settings.
Product Key
License Terms
Global Rules
Product Updates
Install Setup Files
Install Rules
Feature Selection
Feature Rules
Instance Configuration
Server Configuration
Database Engine Configuration
Reporting Services Configuration
Feature Configuration Rules
Ready to Install
Installation Progress
Complete
Server Configuration
Data Directories
TempDB
FILESTREAM
Data root directory:
C:\Program Files\Microsoft SQL Server\
System database directory:
C:\Program Files\Microsoft SQL Server\MSSQL13.MSSQLSERVER\MSSQL\Data
User database directory:
C:\Program Files\Microsoft SQL Server\MSSQL13.MSSQLSERVER\
User database log directory:
C:\Program Files\Microsoft SQL Server\MSSQL13.MSSQLSERVER\
Backup directory:
C:\Program Files\Microsoft SQL Server\MSSQL13.MSSQLSERVER\
< Back
Next >
Cancel

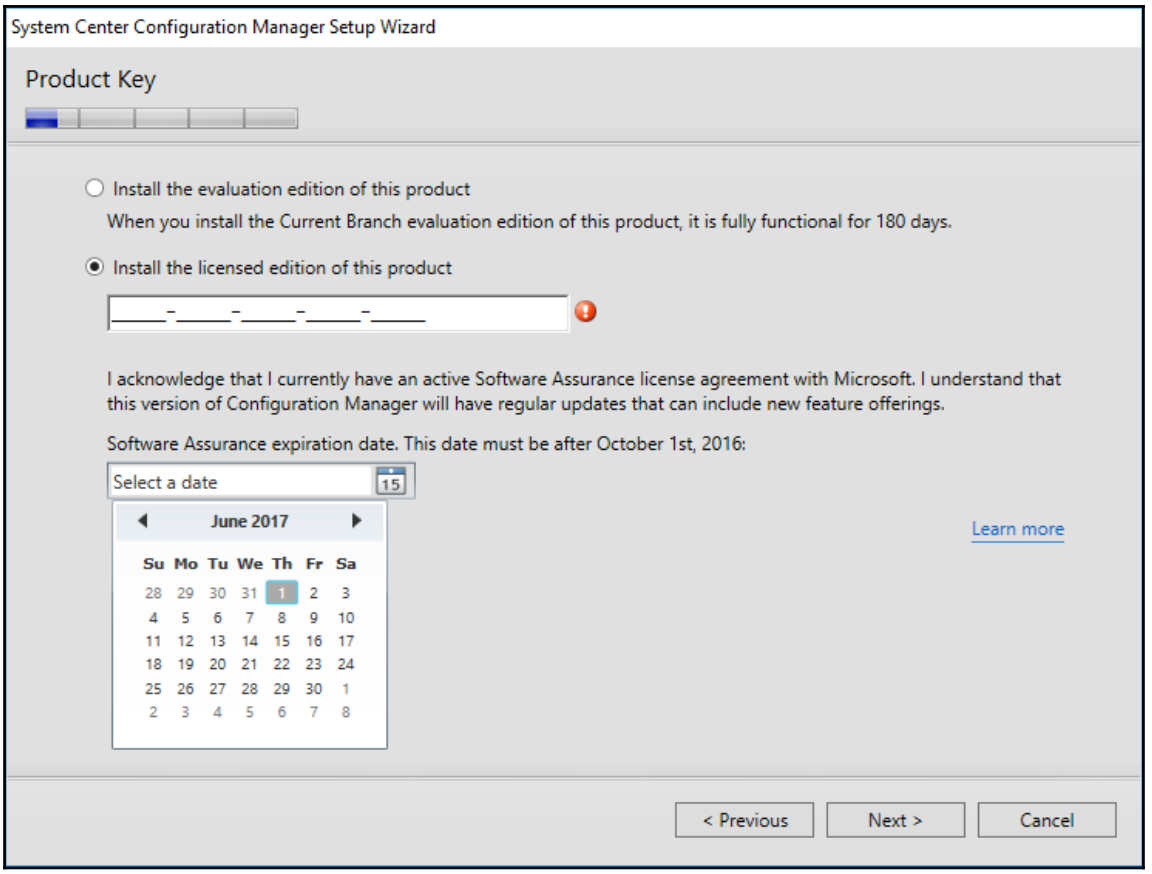

SQL Server 2016 Setup
Reporting Services Configuration
Specify the Reporting Services configuration mode.
Product Key
License Terms
Global Rules
Product Updates
Install Setup Files
Install Rules
Feature Selection
Feature Rules
Instance Configuration
Server Configuration
Database Engine Configuration
Reporting Services Configura...
Feature Configuration Rules
Ready to Install
Installation Progress
Complete
Reporting Services Native Mode
Install and configure.
Installs and configures the report server in native mode. The report server is operational after setup completes.
Install only.
Installs the report server files. After installation, use Reporting Services Configuration Manager to configure the report server for native mode.
Reporting Services SharePoint Integrated Mode
Install only.
Installs the report server files. After installation use SharePoint Central Administration to complete the configuration. Verify the SQL Server Reporting Services service is started and create at least one SQL Server Reporting Services service application. For more information, click Help.
< Back
Next >
Cancel

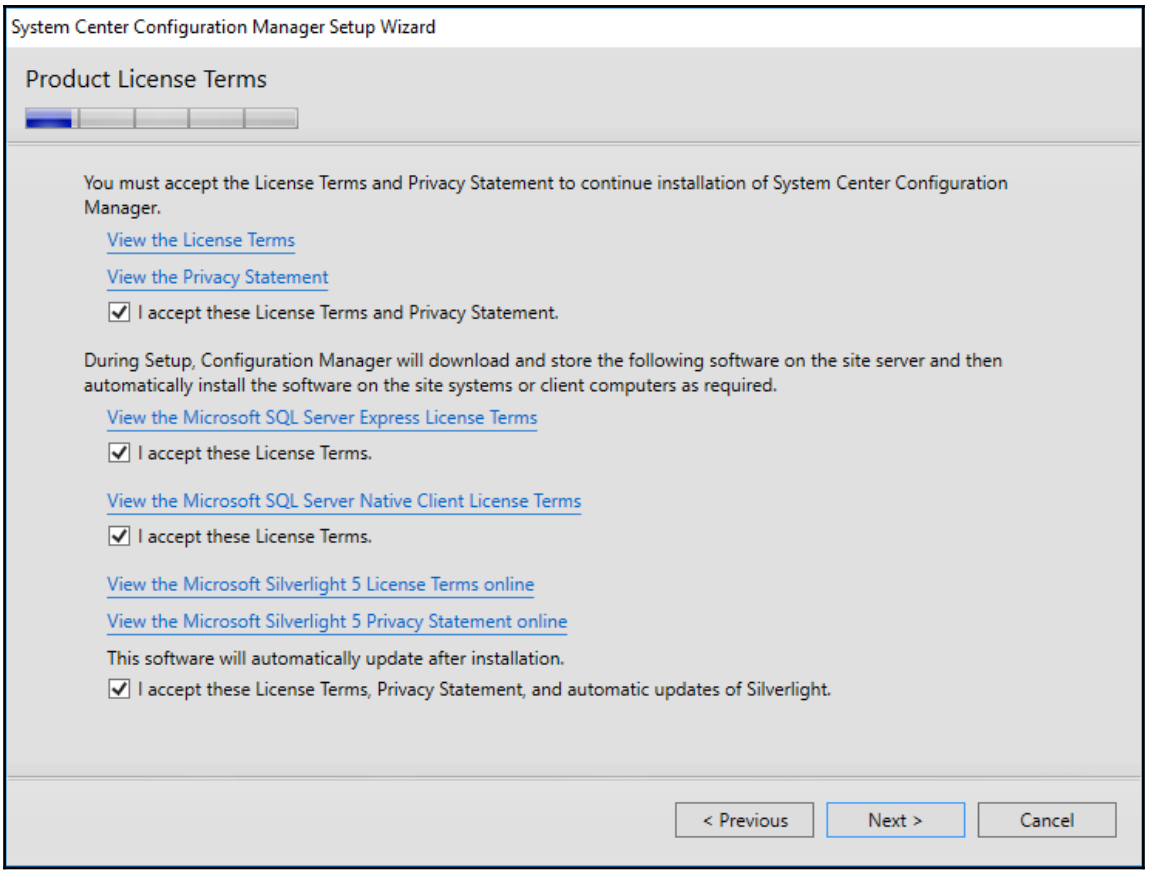

SQL Server Reporting Services
Administrator
Favorites
Browse
Search...
Home
Home

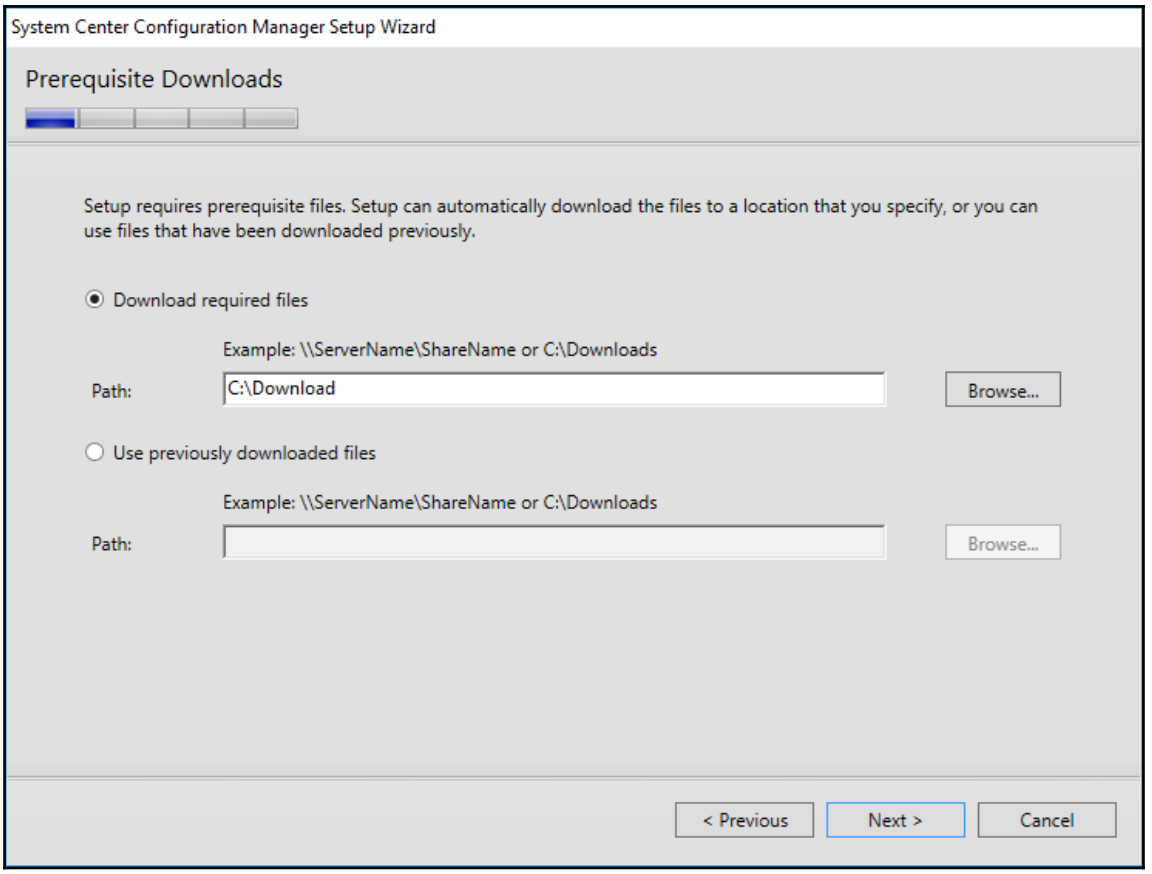

Windows Assessment and Deployment Kit - Windows 10
Specify Location
Install the Windows Assessment and Deployment Kit - Windows 10 to this computer
Install Path:
C:\Program Files (x86)\Windows Kits\10\
Browse...
Download the Windows Assessment and Deployment Kit - Windows 10 for installation on a separate computer
Download Path:
C:\Users\administrator.DOCTOR\Downloads\Windows Kits\10\ADK
Browse...
Estimated disk space required: 4.3 GB
Disk space available: 60.4 GB
Next
Cancel

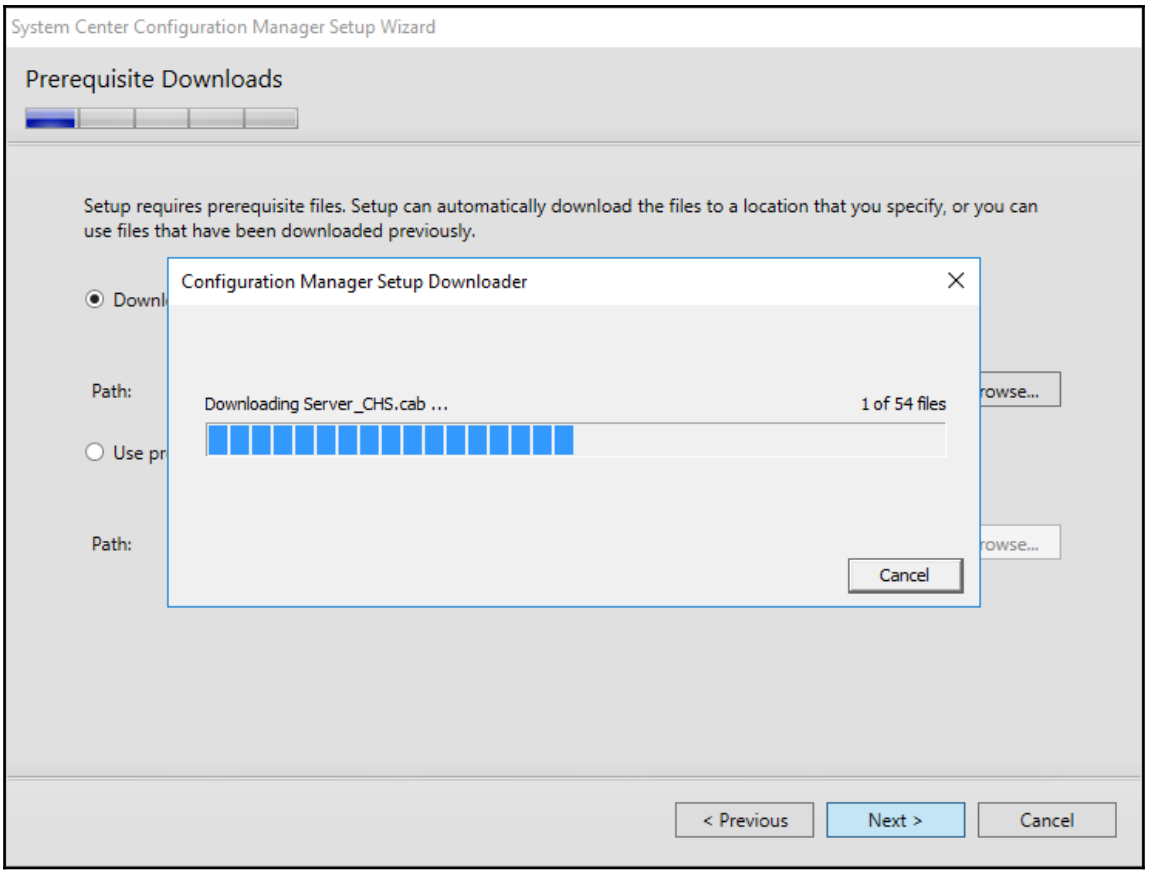

Windows Assessment and Deployment Kit - Windows 10
Select the features you want to install
Click a feature name for more information.
Application Compatibility Tools
Deployment Tools
Windows Preinstallation Environment (Windows PE)
Imaging And Configuration Designer (ICD)
Configuration Designer
User State Migration Tool (USMT)
Volume Activation Management Tool (VAMT)
Windows Performance Toolkit
Microsoft User Experience Virtualization (UE-V) Template
Media eXperience Analyzer
Windows Preinstallation Environment (Windows PE)
Size: 3.4 GB
Minimal operating system designed to prepare a computer for installation and servicing of Windows.
Includes:
Windows PE (x86)
Windows PE (AMD64)
Requires the following features:
Deployment Tools
Estimated disk space required: 4.2 GB
Disk space available: 60.4 GB
Back
Install
Cancel

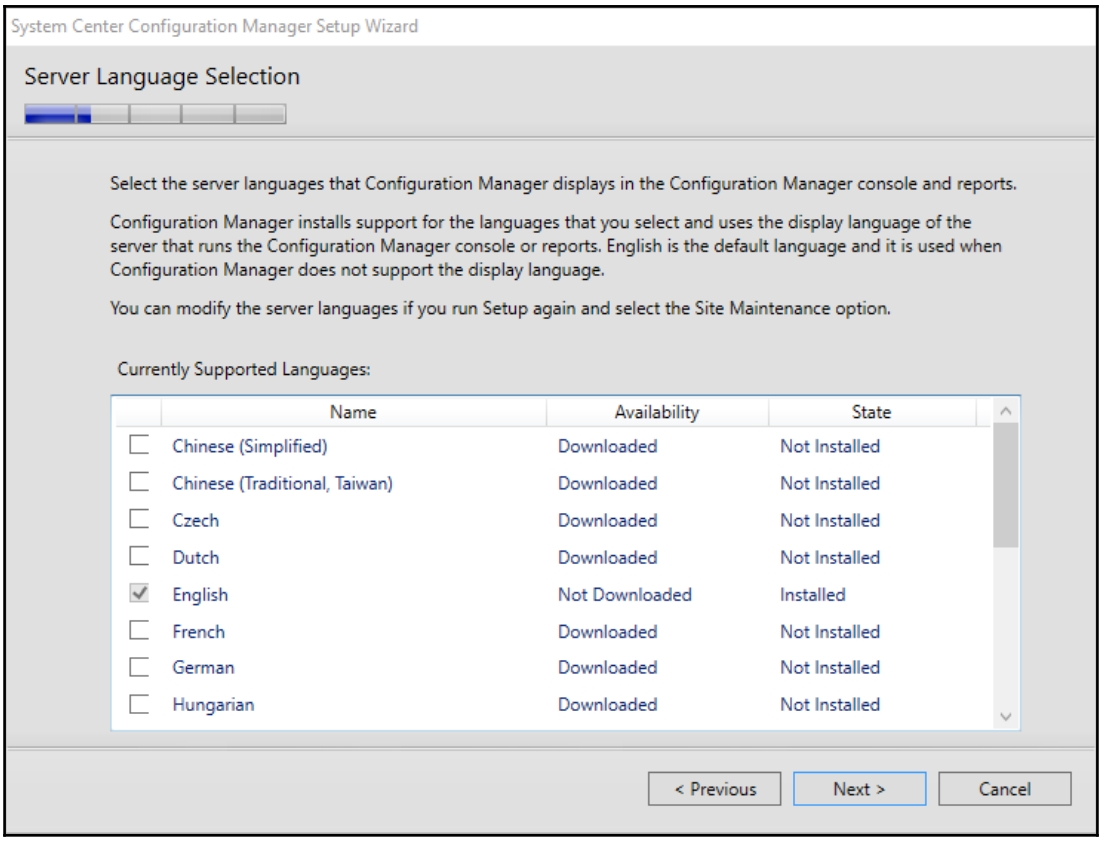

System Center Configuration Manager Setup Wizard
Getting Started
Available Setup Options
Setup has not detected an existing installation of site server, site system, or Configuration Manager console on this computer.
Install a Configuration Manager primary site
Use typical installation options for a stand-alone primary site
- Install a Configuration Manager primary site
- Use default installation path
- Configure local SQL Server with default settings
- Enable a local management point for Configuration Manager
- Enable a local distribution point for Configuration Manager
Install a Configuration Manager central administration site
Upgrade this Configuration Manager site
Recover a site
Perform site maintenance or reset this site
Uninstall this Configuration Manager site
< Previous
Next >
Cancel

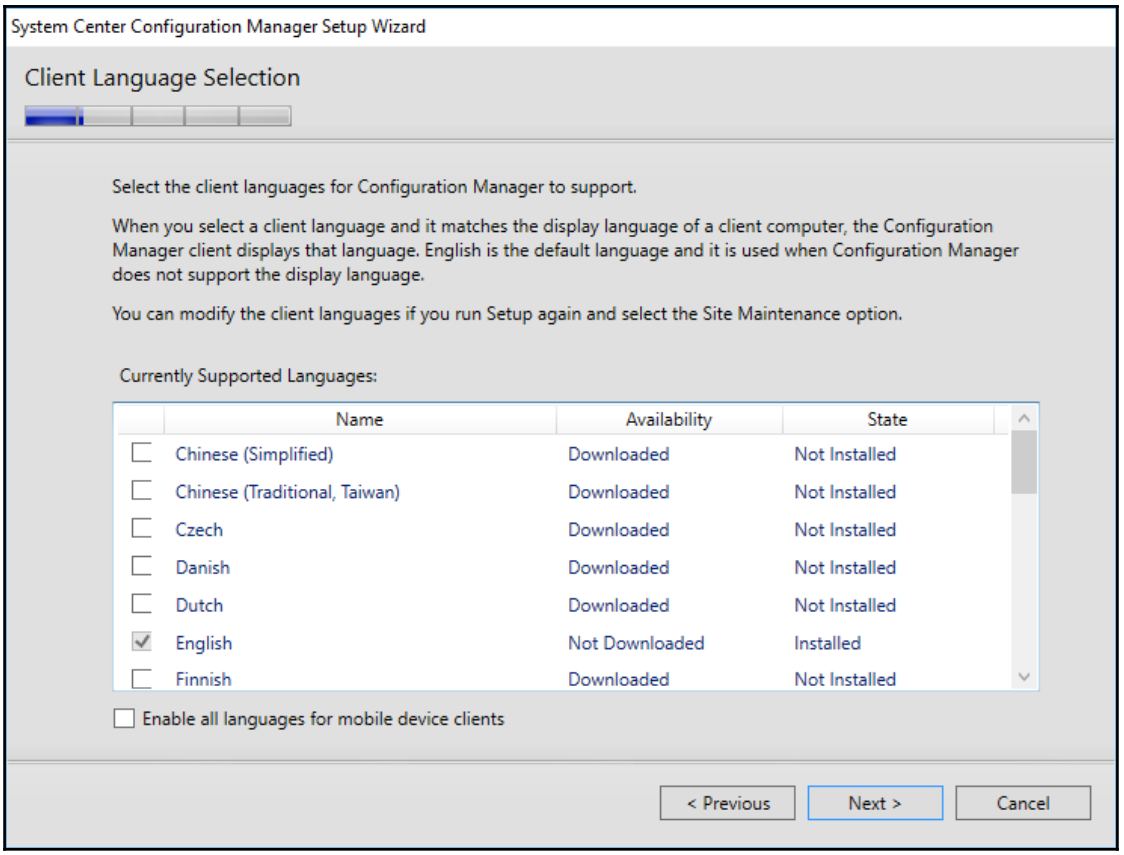

System Center Configuration Manager Setup Wizard
Product Key
Install the evaluation edition of this product
When you install the Current Branch evaluation edition of this product, it is fully functional for 180 days.
Install the licensed edition of this product
I acknowledge that I currently have an active Software Assurance license agreement with Microsoft. I understand that this version of Configuration Manager will have regular updates that can include new feature offerings.
Software Assurance expiration date. This date must be after October 1st, 2016:
Select a date
June 2017
Su Mo Tu We Th Fr Sa
28 29 30 31 1 2 3
4 5 6 7 8 9 10
11 12 13 14 15 16 17
18 19 20 21 22 23 24
25 26 27 28 29 30 1
2 3 4 5 6 7 8
Learn more
< Previous
Next >
Cancel

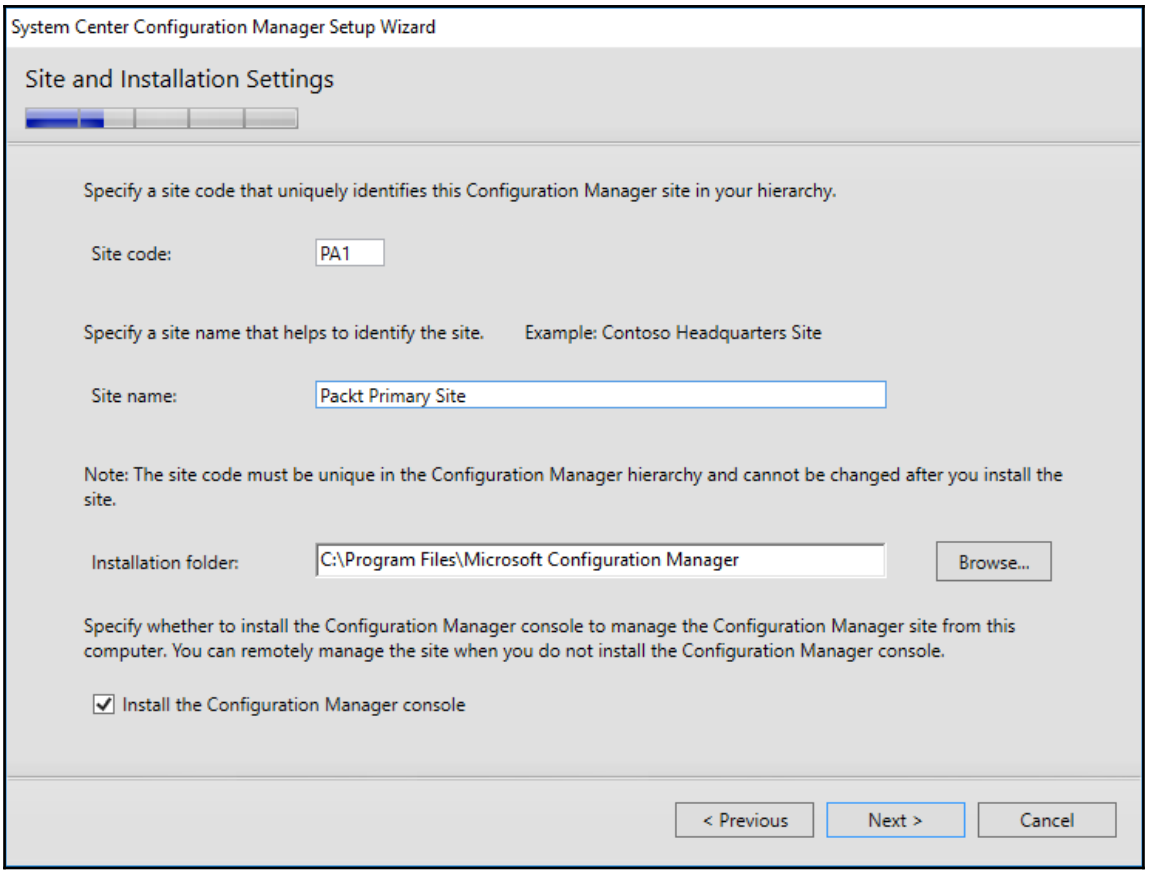

System Center Configuration Manager Setup Wizard
Product License Terms
You must accept the License Terms and Privacy Statement to continue installation of System Center Configuration Manager.
View the License Terms
View the Privacy Statement
I accept these License Terms and Privacy Statement.
During Setup, Configuration Manager will download and store the following software on the site server and then automatically install the software on the site systems or client computers as required.
View the Microsoft SQL Server Express License Terms
I accept these License Terms.
View the Microsoft SQL Server Native Client License Terms
I accept these License Terms.
View the Microsoft Silverlight 5 License Terms online
View the Microsoft Silverlight 5 Privacy Statement online
This software will automatically update after installation.
I accept these License Terms, Privacy Statement, and automatic updates of Silverlight.
< Previous
Next >
Cancel

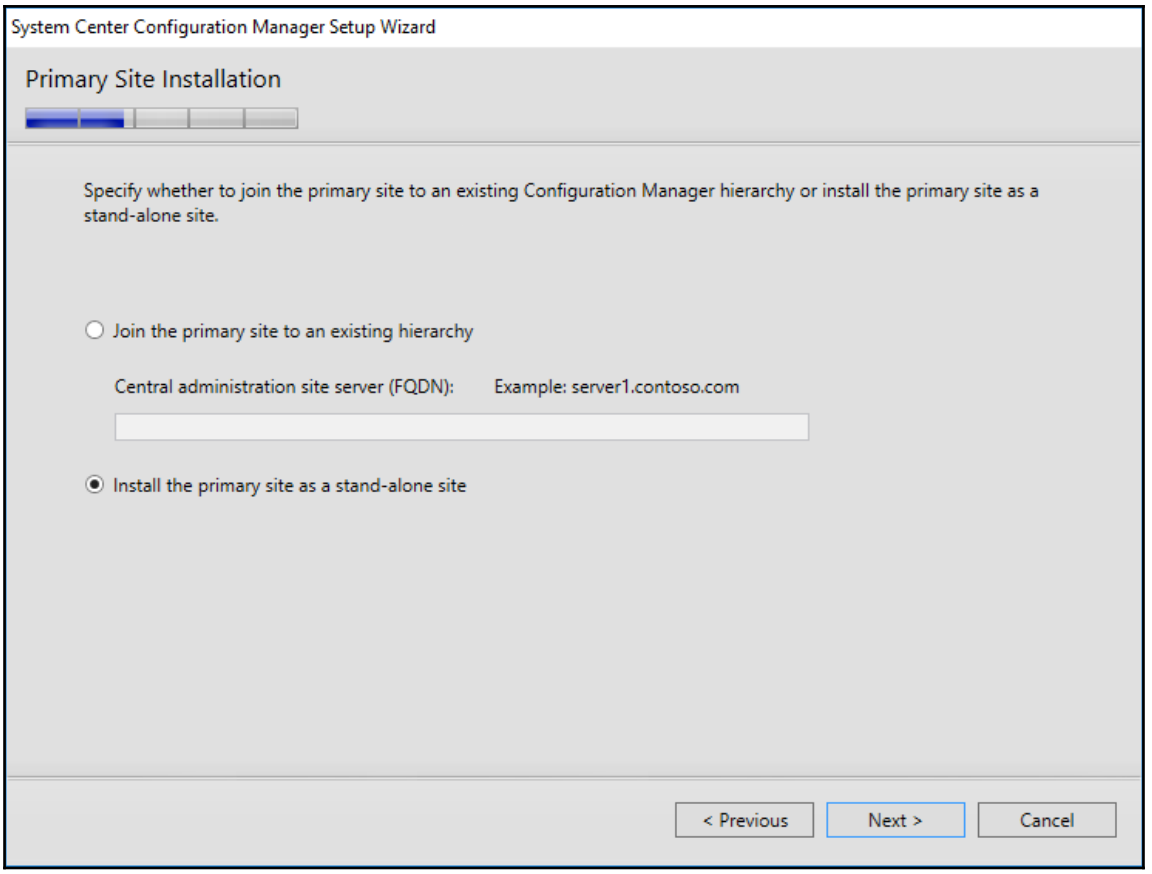

System Center Configuration Manager Setup Wizard
Prerequisite Downloads
Setup requires prerequisite files. Setup can automatically download the files to a location that you specify, or you can use files that have been downloaded previously.
Download required files
Example: \\ServerName\ShareName or C:\Downloads
Path:
C:\Download
Browse...
Use previously downloaded files
Example: \\ServerName\ShareName or C:\Downloads
Path:
Browse...
< Previous
Next >
Cancel

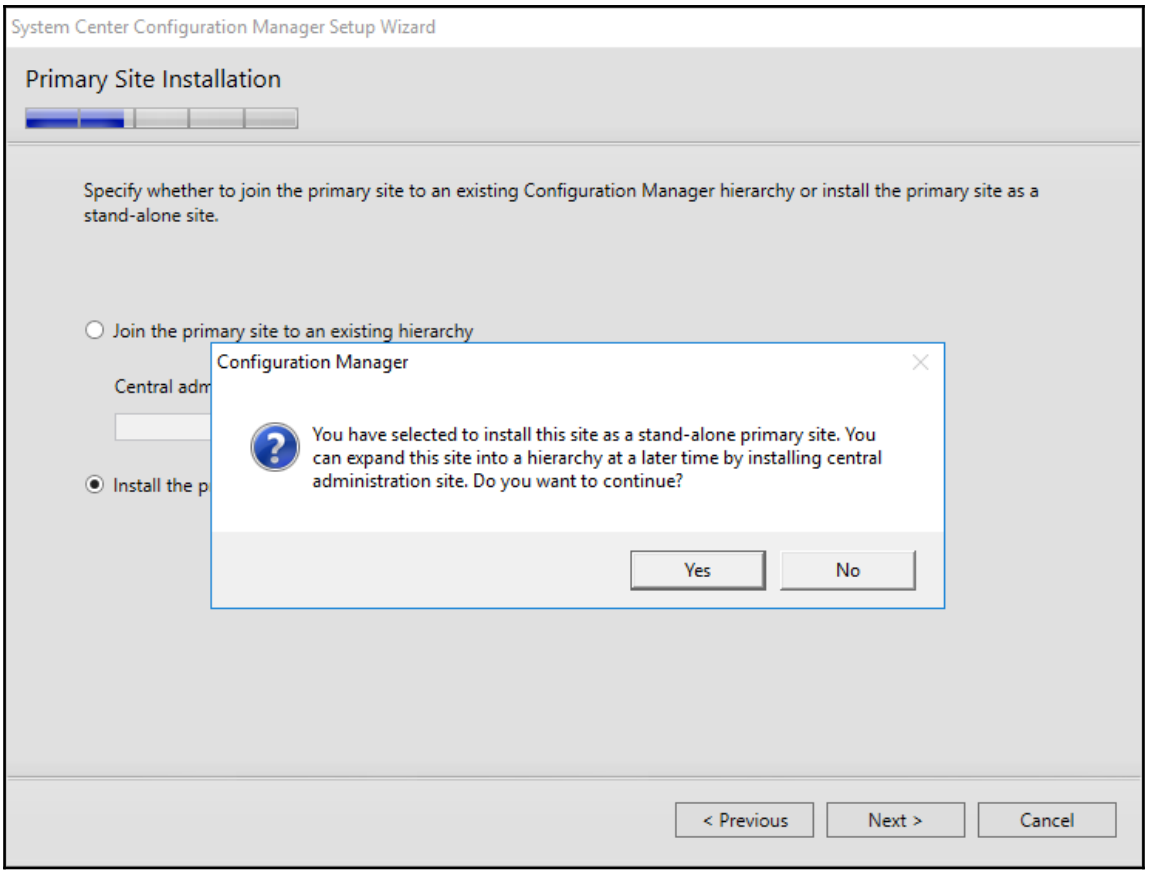

System Center Configuration Manager Setup Wizard
Prerequisite Downloads
Setup requires prerequisite files. Setup can automatically download the files to a location that you specify, or you can use files that have been downloaded previously.
Path:
Use pr
Path:
Configuration Manager Setup Downloader
Downloading Server_CHS.cab ...
1 of 54 files
Cancel
< Previous
Next >
Cancel

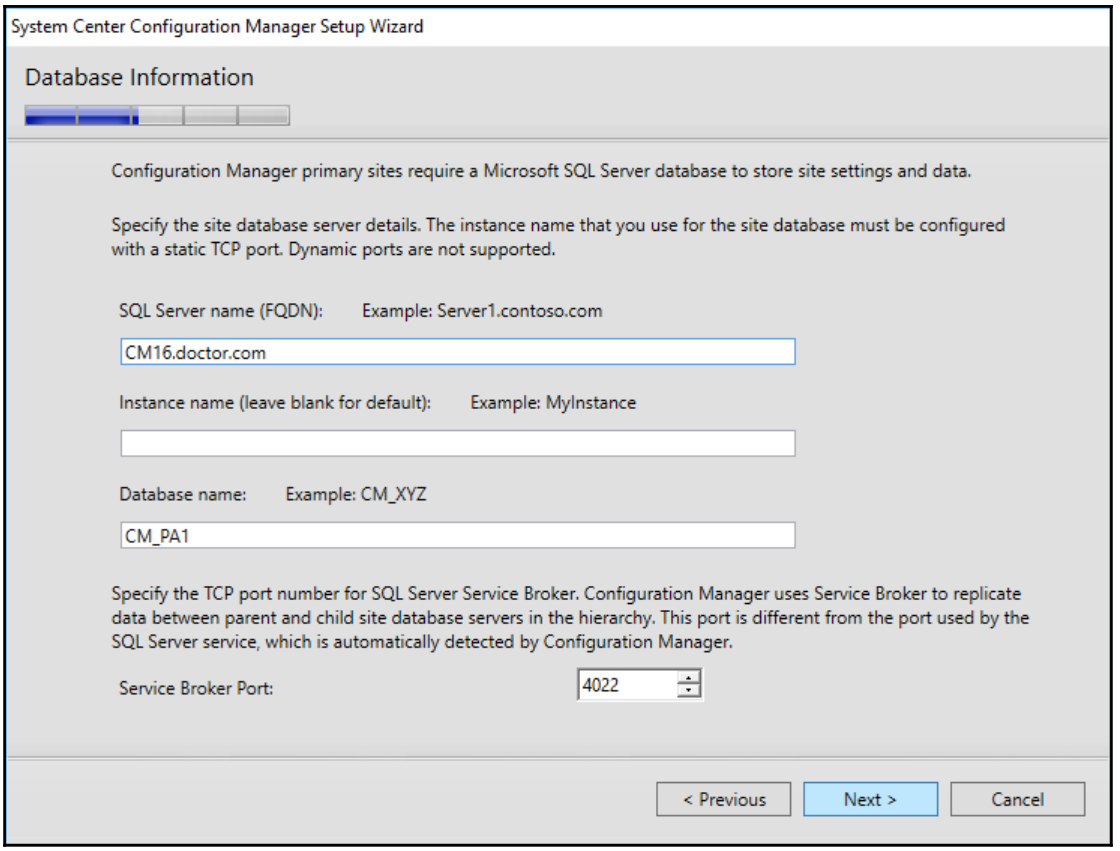

System Center Configuration Manager Setup Wizard
Server Language Selection
Select the server languages that Configuration Manager displays in the Configuration Manager console and reports.
Configuration Manager installs support for the languages that you select and uses the display language of the server that runs the Configuration Manager console or reports. English is the default language and it is used when Configuration Manager does not support the display language.
You can modify the server languages if you run Setup again and select the Site Maintenance option.
Currently Supported Languages:
Name
Availability
State
Chinese (Simplified)
Downloaded
Not Installed
Chinese (Traditional, Taiwan)
Downloaded
Not Installed
Czech
Downloaded
Not Installed
Dutch
Downloaded
Not Installed
English
Not Downloaded
Installed
French
Downloaded
Not Installed
German
Downloaded
Not Installed
Hungarian
Downloaded
Not Installed
< Previous
Next >
Cancel

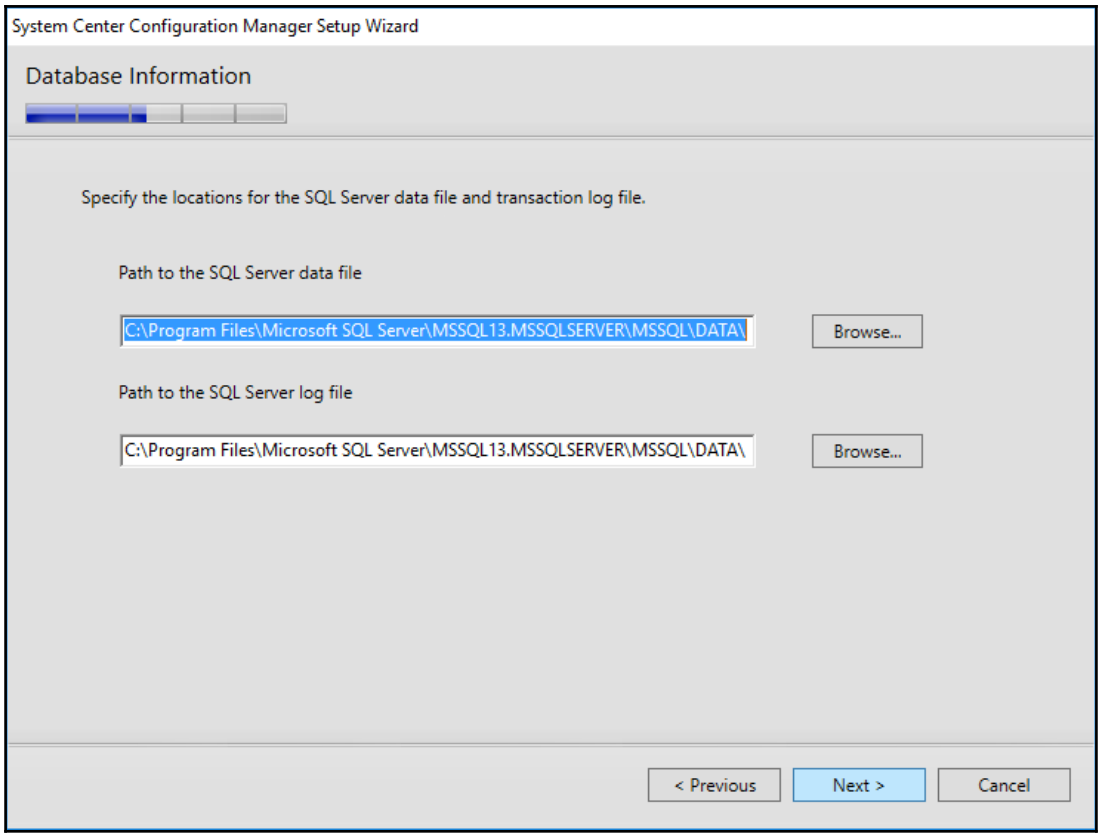

System Center Configuration Manager Setup Wizard
Client Language Selection
Select the client languages for Configuration Manager to support.
When you select a client language and it matches the display language of a client computer, the Configuration Manager client displays that language. English is the default language and it is used when Configuration Manager does not support the display language.
You can modify the client languages if you run Setup again and select the Site Maintenance option.
Currently Supported Languages:
Name
Availability
State
Chinese (Simplified)
Downloaded
Not Installed
Chinese (Traditional, Taiwan)
Downloaded
Not Installed
Czech
Downloaded
Not Installed
Danish
Downloaded
Not Installed
Dutch
Downloaded
Not Installed
English
Not Downloaded
Installed
Finnish
Downloaded
Not Installed
Enable all languages for mobile device clients
< Previous
Next >
Cancel

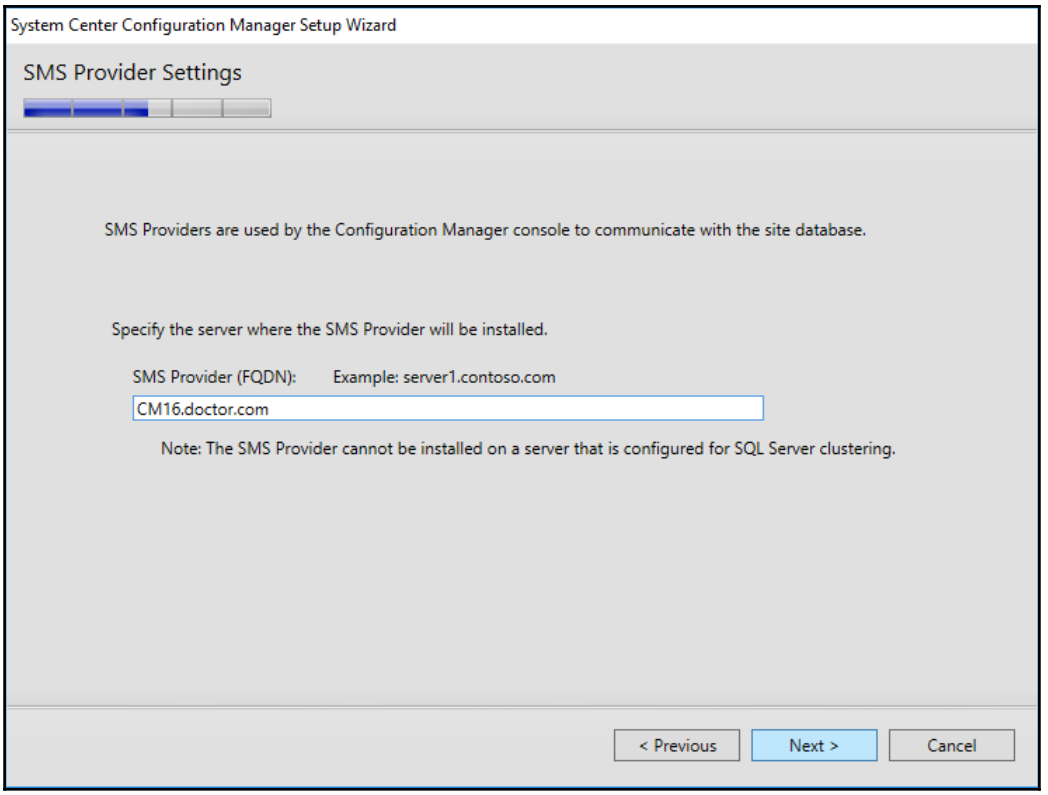

System Center Configuration Manager Setup Wizard
Site and Installation Settings
Specify a site code that uniquely identifies this Configuration Manager site in your hierarchy.
Site code:
PA1
Specify a site name that helps to identify the site.
Example: Contoso Headquarters Site
Site name:
Packt Primary Site
Note: The site code must be unique in the Configuration Manager hierarchy and cannot be changed after you install the site.
Installation folder:
C:\Program Files\Microsoft Configuration Manager
Browse...
Specify whether to install the Configuration Manager console to manage the Configuration Manager site from this computer. You can remotely manage the site when you do not install the Configuration Manager console.
Install the Configuration Manager console
< Previous
Next >
Cancel

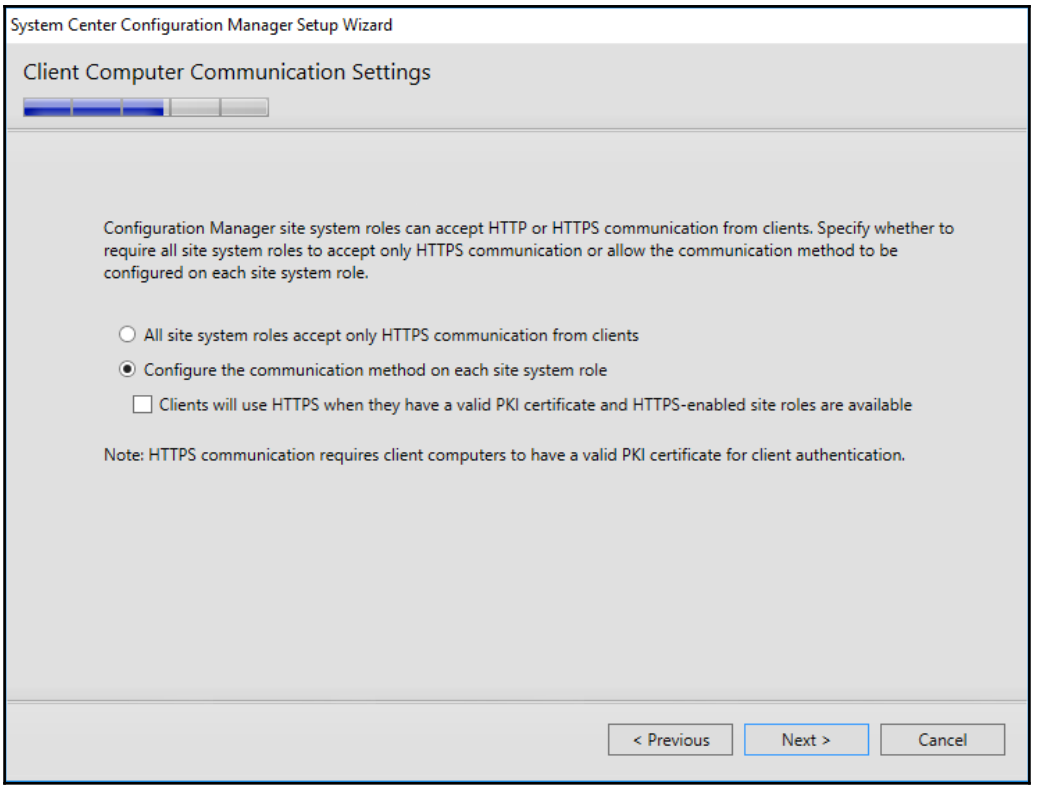

System Center Configuration Manager Setup Wizard
Primary Site Installation
Specify whether to join the primary site to an existing Configuration Manager hierarchy or install the primary site as a stand-alone site.
Join the primary site to an existing hierarchy
Central administration site server (FQDN):
Example: server1.contoso.com
Install the primary site as a stand-alone site
< Previous
Next >
Cancel

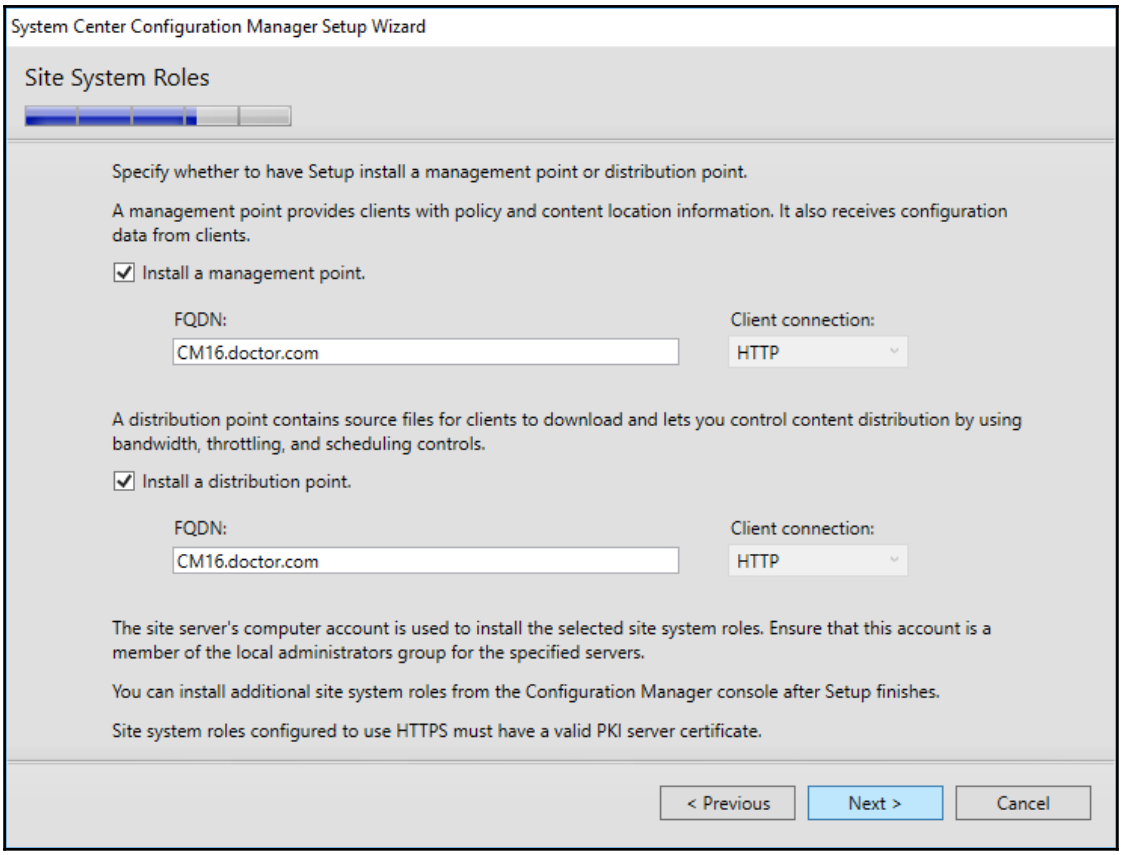

System Center Configuration Manager Setup Wizard
Primary Site Installation
Specify whether to join the primary site to an existing Configuration Manager hierarchy or install the primary site as a stand-alone site.
Join the primary site to an existing hierarchy
Central adm
Install the p
Configuration Manager
You have selected to install this site as a stand-alone primary site. You can expand this site into a hierarchy at a later time by installing central administration site. Do you want to continue?
Yes
No
< Previous
Next >
Cancel

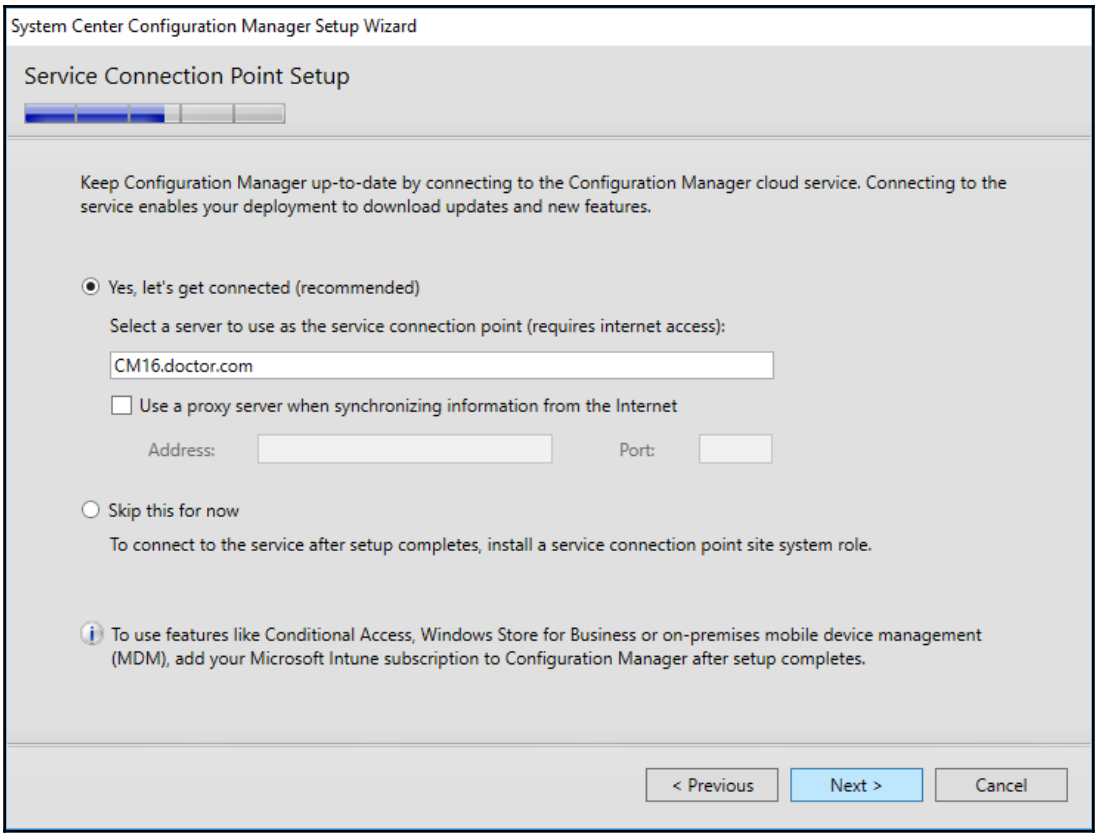

System Center Configuration Manager Setup Wizard
Database Information
Configuration Manager primary sites require a Microsoft SQL Server database to store site settings and data.
Specify the site database server details. The instance name that you use for the site database must be configured with a static TCP port. Dynamic ports are not supported.
SQL Server name (FQDN): Example: Server1.contoso.com
CM16.doctor.com
Instance name (leave blank for default): Example: MyInstance
Database name: Example: CM_XYZ
CM_PA1
Specify the TCP port number for SQL Server Service Broker. Configuration Manager uses Service Broker to replicate data between parent and child site database servers in the hierarchy. This port is different from the port used by the SQL Server service, which is automatically detected by Configuration Manager.
Service Broker Port:
4022
< Previous
Next >
Cancel

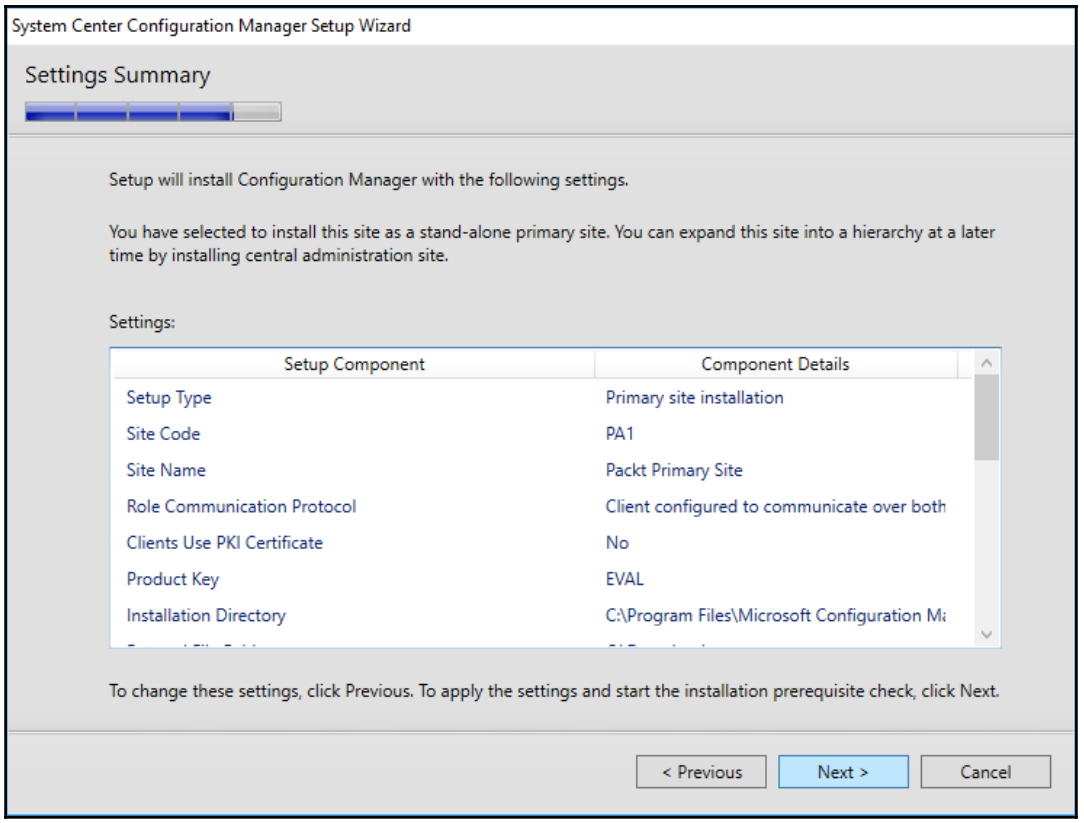

System Center Configuration Manager Setup Wizard
Database Information
Specify the locations for the SQL Server data file and transaction log file.
Path to the SQL Server data file
C:\Program Files\Microsoft SQL Server\MSSQL13.MSSQLSERVER\MSSQL\DATA\
Browse...
Path to the SQL Server log file
C:\Program Files\Microsoft SQL Server\MSSQL13.MSSQLSERVER\MSSQL\DATA\
Browse...
< Previous
Next >
Cancel

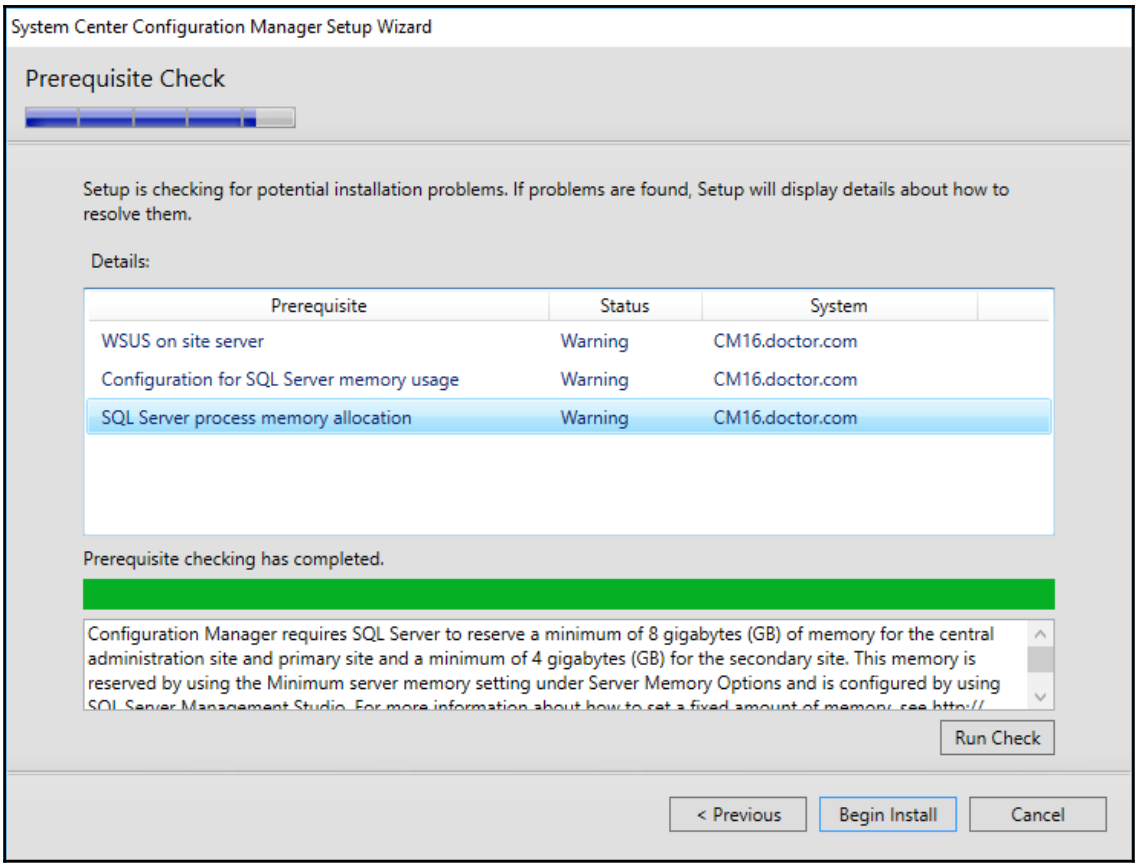

System Center Configuration Manager Setup Wizard
SMS Provider Settings
SMS Providers are used by the Configuration Manager console to communicate with the site database.
Specify the server where the SMS Provider will be installed.
SMS Provider (FQDN):
Example: server1.contoso.com
CM16.doctor.com
Note: The SMS Provider cannot be installed on a server that is configured for SQL Server clustering.
< Previous
Next >
Cancel

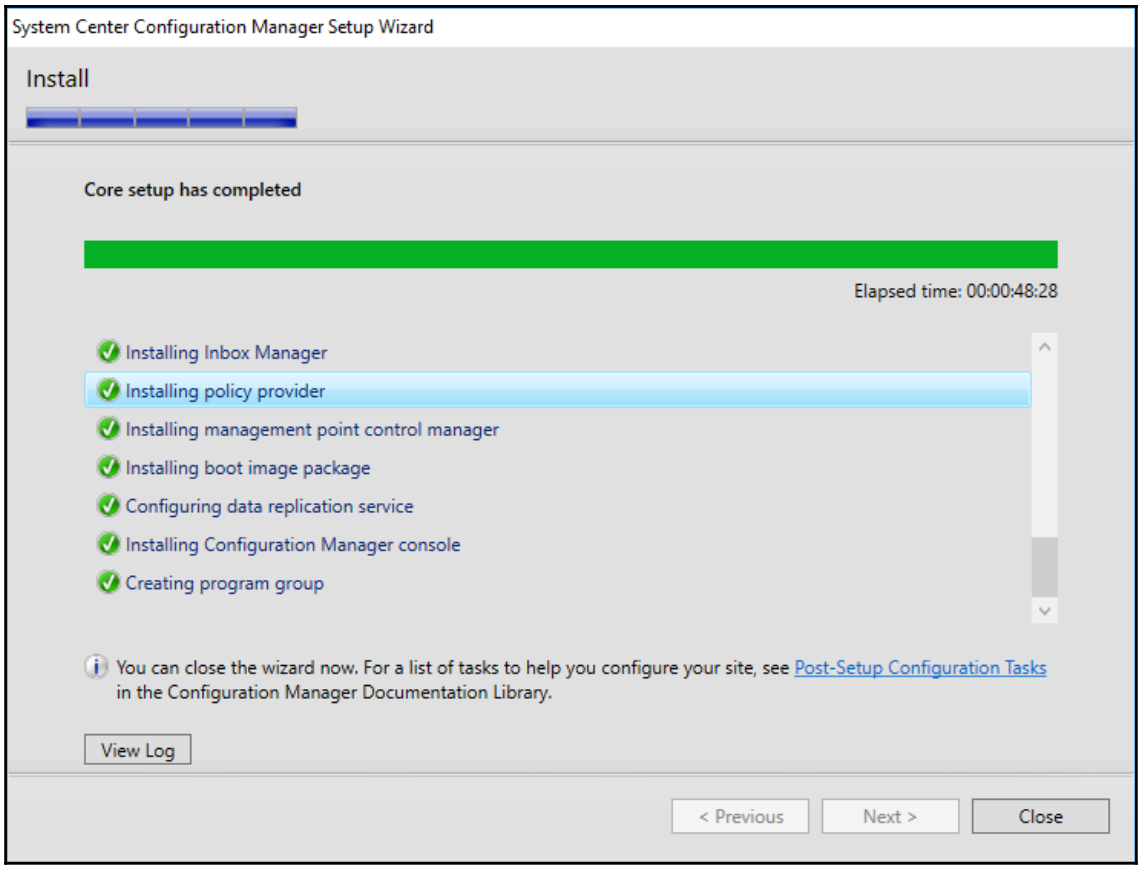

System Center Configuration Manager Setup Wizard
Client Computer Communication Settings
Configuration Manager site system roles can accept HTTP or HTTPS communication from clients. Specify whether to require all site system roles to accept only HTTPS communication or allow the communication method to be configured on each site system role.
All site system roles accept only HTTPS communication from clients
Configure the communication method on each site system role
Clients will use HTTPS when they have a valid PKI certificate and HTTPS-enabled site roles are available
Note: HTTPS communication requires client computers to have a valid PKI certificate for client authentication.
< Previous
Next >
Cancel

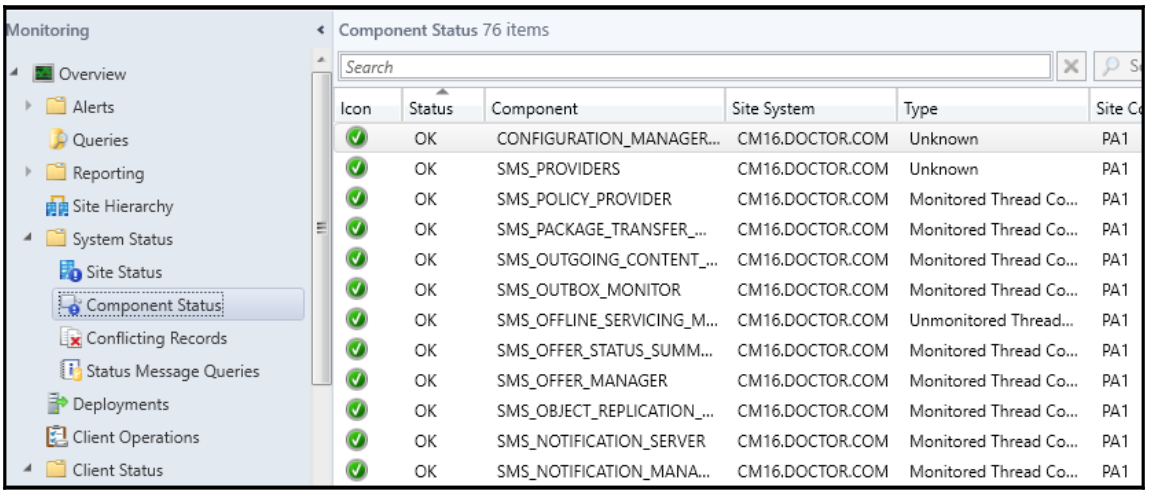

System Center Configuration Manager Setup Wizard
Site System Roles
Specify whether to have Setup install a management point or distribution point.
A management point provides clients with policy and content location information. It also receives configuration data from clients.
Install a management point.
FQDN:
CM16.doctor.com
Client connection:
HTTP
A distribution point contains source files for clients to download and lets you control content distribution by using bandwidth, throttling, and scheduling controls.
Install a distribution point.
FQDN:
CM16.doctor.com
Client connection:
HTTP
The site server's computer account is used to install the selected site system roles. Ensure that this account is a member of the local administrators group for the specified servers.
You can install additional site system roles from the Configuration Manager console after Setup finishes.
Site system roles configured to use HTTPS must have a valid PKI server certificate.
< Previous
Next >
Cancel

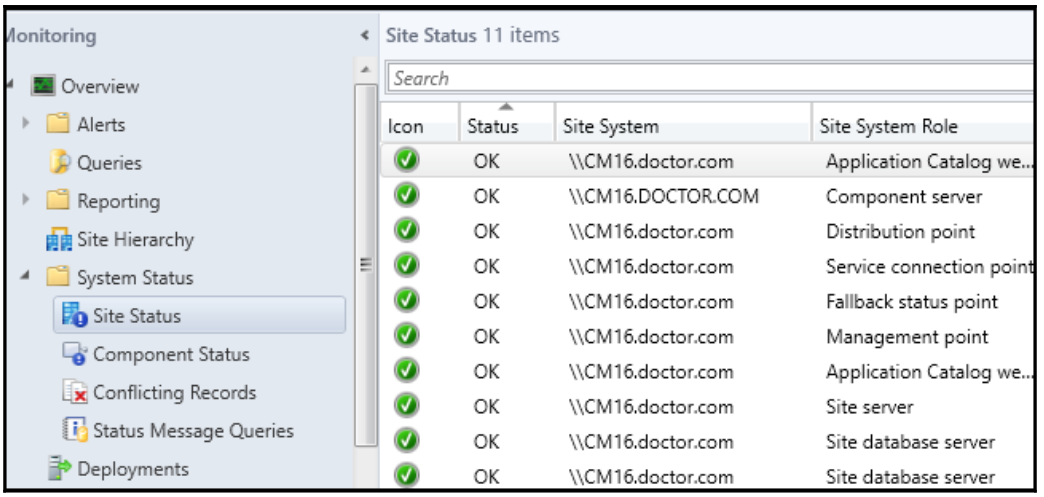

System Center Configuration Manager Setup Wizard
Service Connection Point Setup
Keep Configuration Manager up-to-date by connecting to the Configuration Manager cloud service. Connecting to the service enables your deployment to download updates and new features.
Yes, let's get connected (recommended)
Select a server to use as the service connection point (requires internet access):
CM16.doctor.com
Use a proxy server when synchronizing information from the Internet
Address:
Port:
Skip this for now
To connect to the service after setup completes, install a service connection point site system role.
To use features like Conditional Access, Windows Store for Business or on-premises mobile device management (MDM), add your Microsoft Intune subscription to Configuration Manager after setup completes.
< Previous
Next >
Cancel


System Center Configuration Manager Setup Wizard
Settings Summary
Setup will install Configuration Manager with the following settings.
You have selected to install this site as a stand-alone primary site. You can expand this site into a hierarchy at a later time by installing central administration site.
Settings:
Setup Component
Component Details
Setup Type
Primary site installation
Site Code
PA1
Site Name
Packt Primary Site
Role Communication Protocol
Client configured to communicate over both
Clients Use PKI Certificate
No
Product Key
EVAL
Installation Directory
C:\Program Files\Microsoft Configuration M
To change these settings, click Previous. To apply the settings and start the installation prerequisite check, click Next.
< Previous
Next >
Cancel

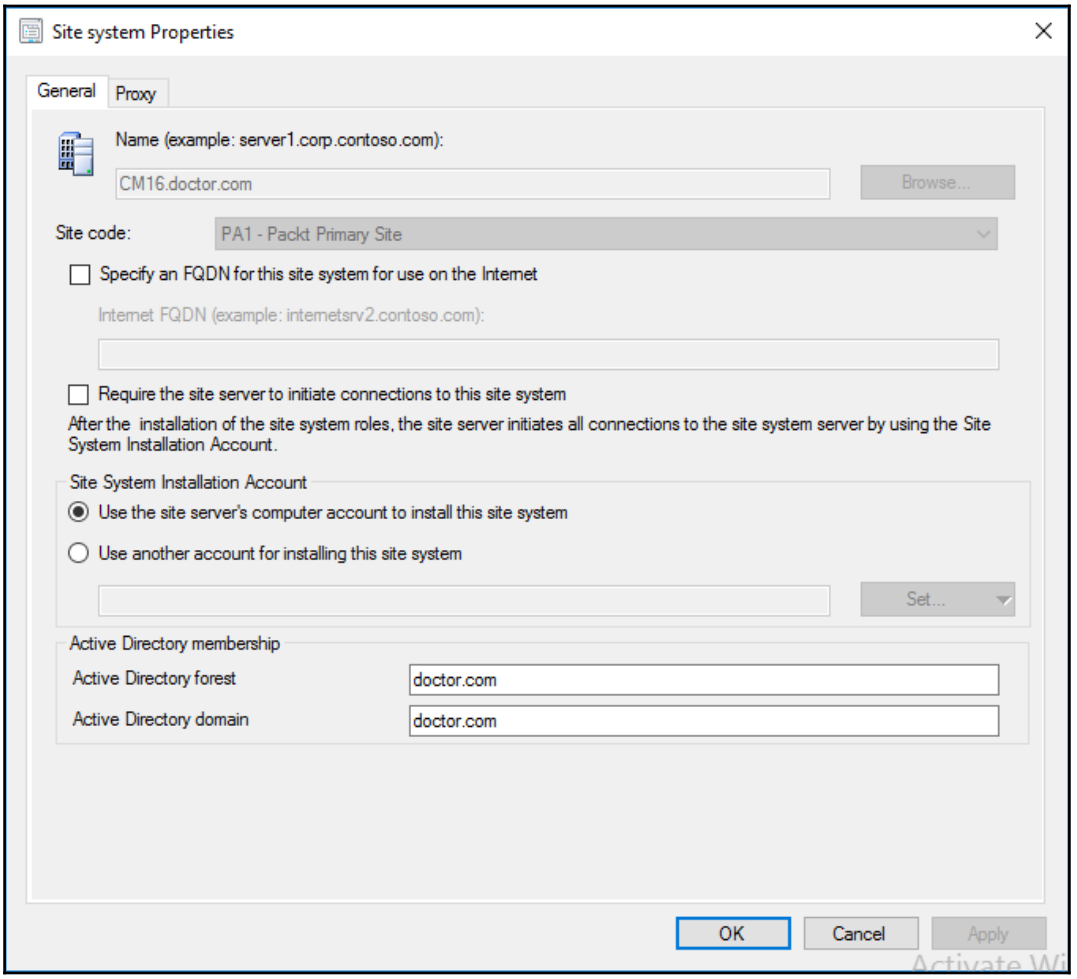

System Center Configuration Manager Setup Wizard
Prerequisite Check
Setup is checking for potential installation problems. If problems are found, Setup will display details about how to resolve them.
Details:
Prerequisite
Status
System
WSUS on site server
Warning
CM16.doctor.com
Configuration for SQL Server memory usage
Warning
CM16.doctor.com
SQL Server process memory allocation
Warning
CM16.doctor.com
Prerequisite checking has completed.
Configuration Manager requires SQL Server to reserve a minimum of 8 gigabytes (GB) of memory for the central administration site and primary site and a minimum of 4 gigabytes (GB) for the secondary site. This memory is reserved by using the Minimum server memory setting under Server Memory Options and is configured by using
Run Check
< Previous
Begin Install
Cancel

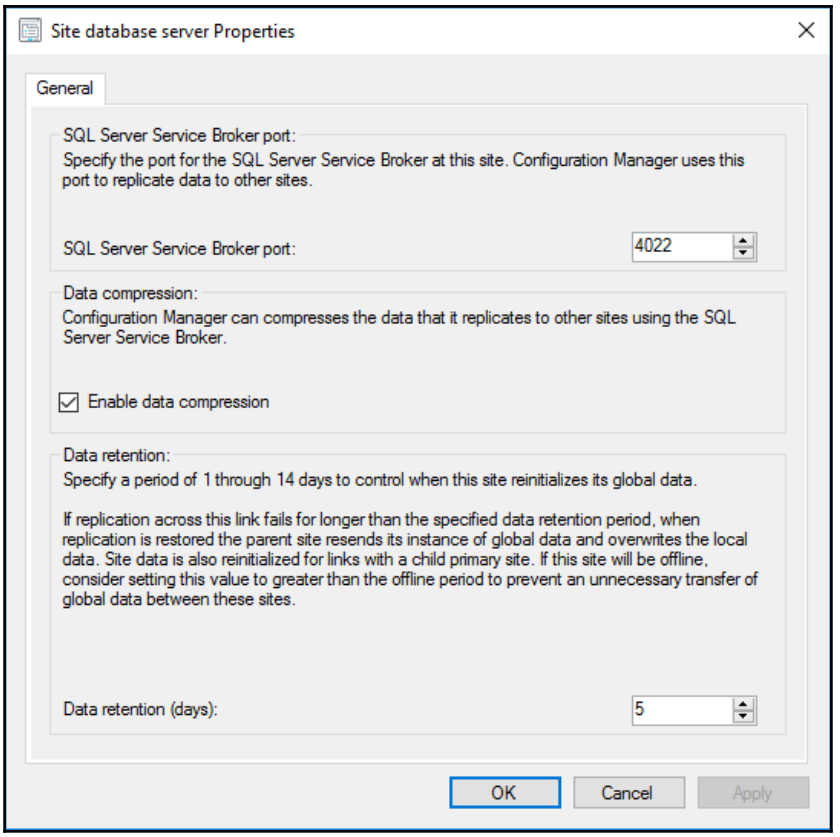

System Center Configuration Manager Setup Wizard
Install
Core setup has completed
Elapsed time: 00:00:48:28
Installing Inbox Manager
Installing policy provider
Installing management point control manager
Installing boot image package
Configuring data replication service
Installing Configuration Manager console
Creating program group
You can close the wizard now. For a list of tasks to help you configure your site, see Post-Setup Configuration Tasks in the Configuration Manager Documentation Library.
View Log
< Previous
Next >
Close

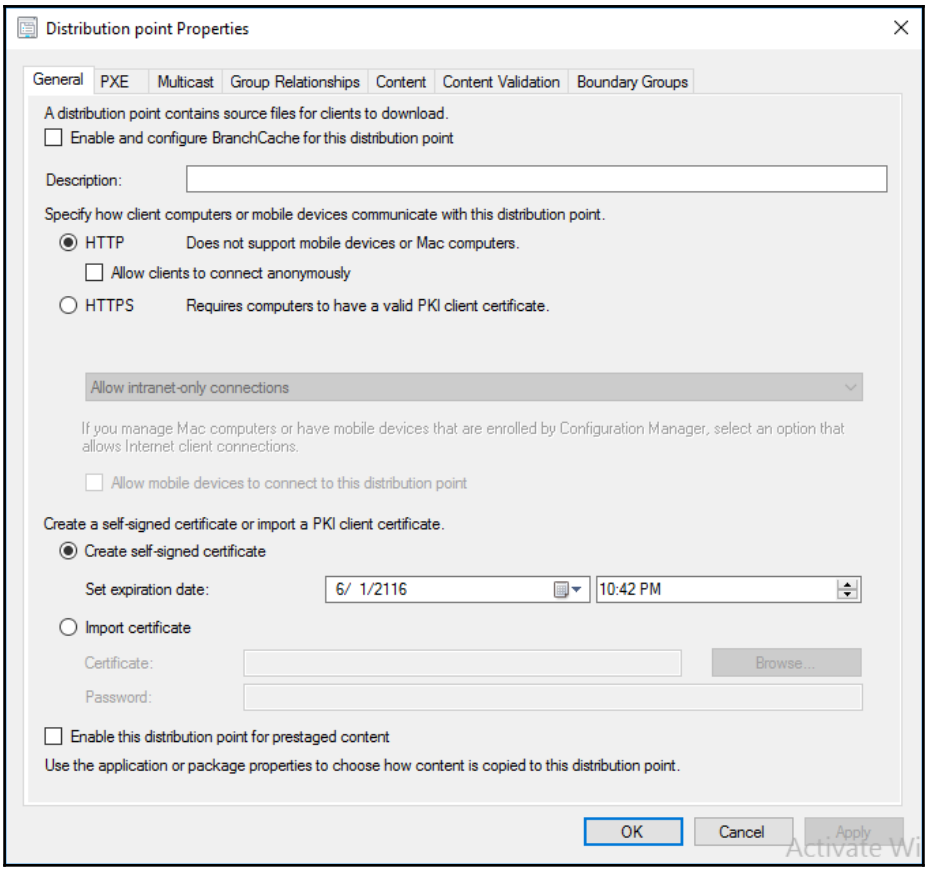

Monitoring
Overview
Alerts
Queries
Reporting
Site Hierarchy
System Status
Site Status
Component Status
Conflicting Records
Status Message Queries
Deployments
Client Operations
Client Status
Component Status 76 items
Search
Icon
Status
Component
Site System
Type
Site Co
OK CONFIGURATION_MANAGER... CM16.DOCTOR.COM Unknown PA1
OK SMS_PROVIDERS CM16.DOCTOR.COM Unknown PA1
OK SMS_POLICY_PROVIDER CM16.DOCTOR.COM Monitored Thread Co... PA1
OK SMS_PACKAGE_TRANSFER_... CM16.DOCTOR.COM Monitored Thread Co... PA1
OK SMS_OUTGOING_CONTENT_... CM16.DOCTOR.COM Monitored Thread Co... PA1
OK SMS_OUTBOX_MONITOR CM16.DOCTOR.COM Monitored Thread Co... PA1
OK SMS_OFFLINE_SERVICING_M... CM16.DOCTOR.COM Unmonitored Thread... PA1
OK SMS_OFFER_STATUS_SUMM... CM16.DOCTOR.COM Monitored Thread Co... PA1
OK SMS_OFFER_MANAGER CM16.DOCTOR.COM Monitored Thread Co... PA1
OK SMS_OBJECT_REPLICATION_... CM16.DOCTOR.COM Monitored Thread Co... PA1
OK SMS_NOTIFICATION_SERVER CM16.DOCTOR.COM Monitored Thread Co... PA1
OK SMS_NOTIFICATION_MANA... CM16.DOCTOR.COM Monitored Thread Co... PA1

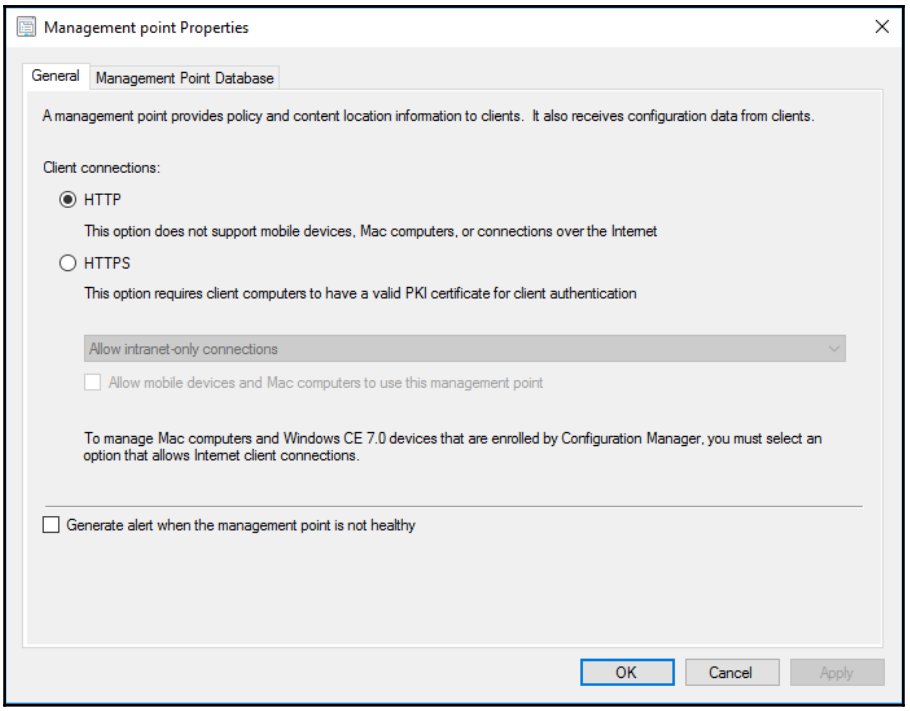

Monitoring
Overview
Alerts
Queries
Reporting
Site Hierarchy
System Status
Site Status
Component Status
Conflicting Records
Status Message Queries
Deployments
Site Status 11 items
Search
Icon
Status
Site System
Site System Role
OK \\CM16.doctor.com Application Catalog we...
OK \\CM16.DOCTOR.COM Component server
OK \\CM16.doctor.com Distribution point
OK \\CM16.doctor.com Service connection point
OK \\CM16.doctor.com Fallback status point
OK \\CM16.doctor.com Management point
OK \\CM16.doctor.com Application Catalog we...
OK \\CM16.doctor.com Site server
OK \\CM16.doctor.com Site database server
OK \\CM16.doctor.com Site database server

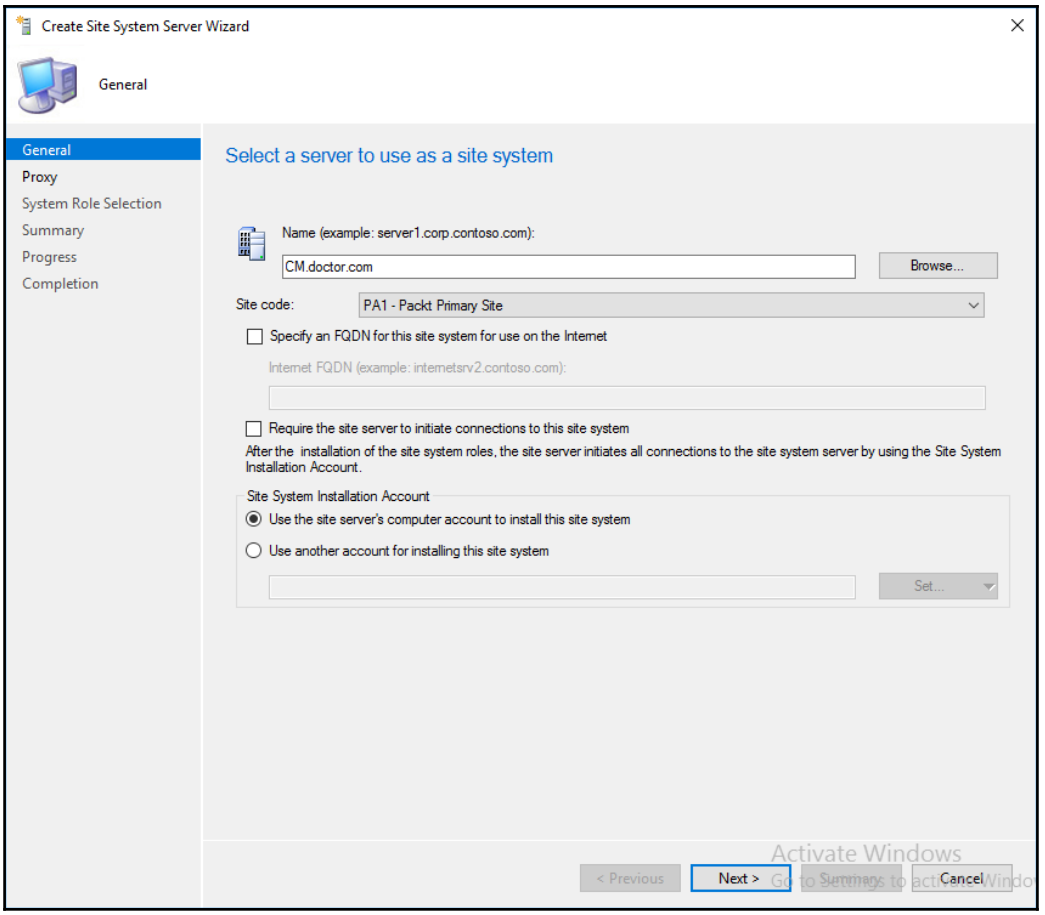
# Chapter 3: Configure Sites and Boundaries

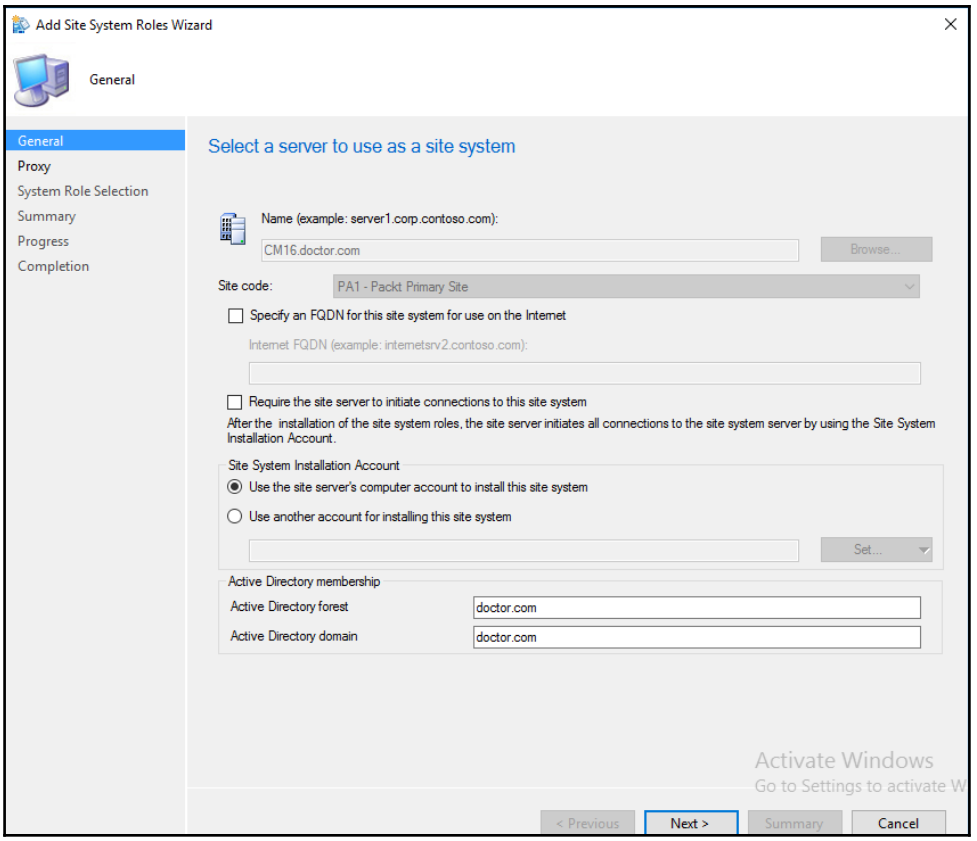


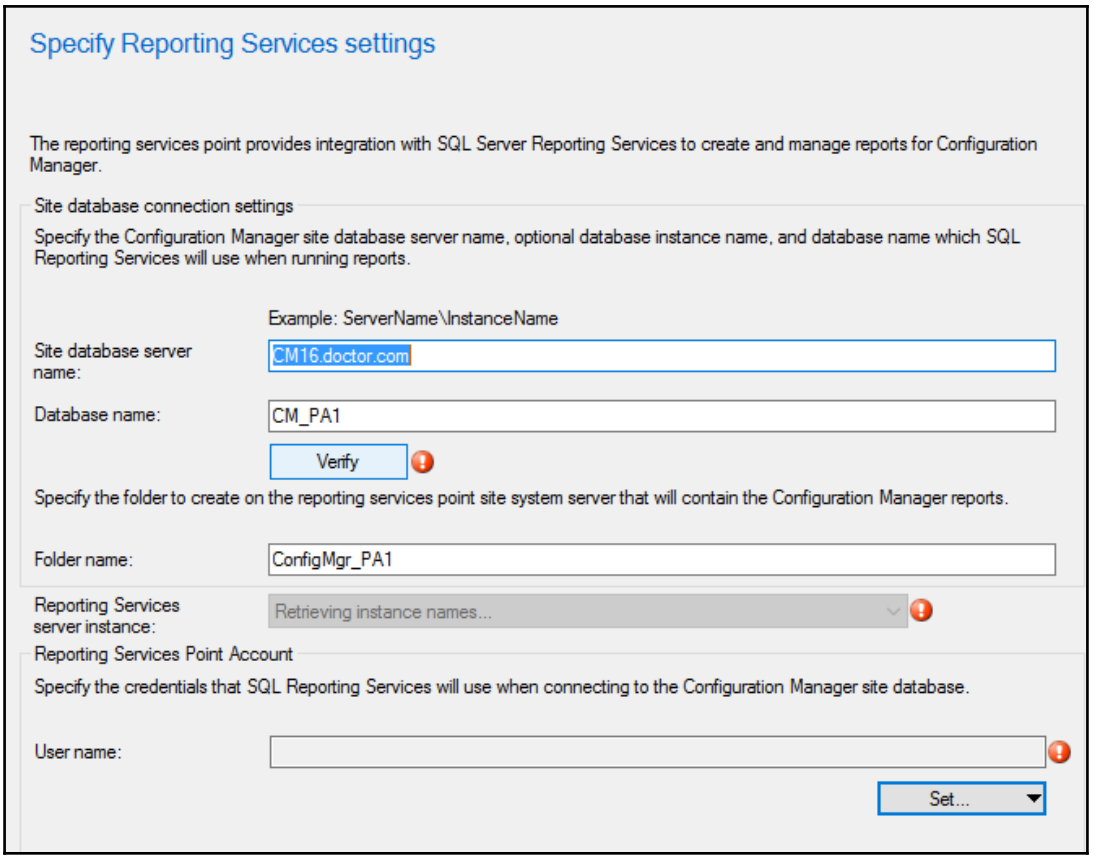

Site database server Properties
General
SQL Server Service Broker port:
Specify the port for the SQL Server Service Broker at this site. Configuration Manager uses this port to replicate data to other sites.
SQL Server Service Broker port:
4022
Data compression:
Configuration Manager can compresses the data that it replicates to other sites using the SQL Server Service Broker.
Enable data compression
Data retention:
Specify a period of 1 through 14 days to control when this site reinitializes its global data.
If replication across this link fails for longer than the specified data retention period, when replication is restored the parent site resends its instance of global data and overwrites the local data. Site data is also reinitialized for links with a child primary site. If this site will be offline, consider setting this value to greater than the offline period to prevent an unnecessary transfer of global data between these sites.
Data retention (days):
5
OK
Cancel
Apply

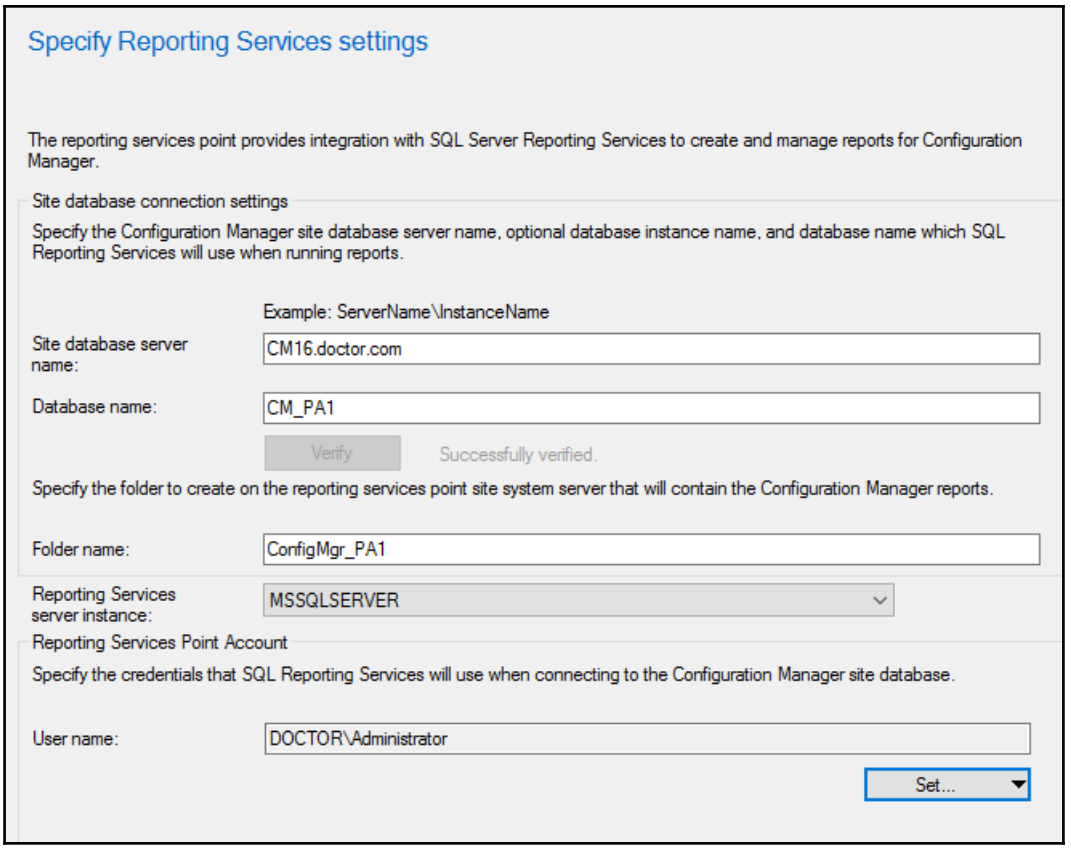

Distribution point Properties
General
PXE
Multicast
Group Relationships
Content
Content Validation
Boundary Groups
A distribution point contains source files for clients to download.
Enable and configure BranchCache for this distribution point
Description:
Specify how client computers or mobile devices communicate with this distribution point.
HTTP
Does not support mobile devices or Mac computers.
Allow clients to connect anonymously
HTTPS
Requires computers to have a valid PKI client certificate.
Allow intranet-only connections
If you manage Mac computers or have mobile devices that are enrolled by Configuration Manager, select an option that allows Internet client connections.
Allow mobile devices to connect to this distribution point
Create a self-signed certificate or import a PKI client certificate.
Create self-signed certificate
Set expiration date:
6/ 1/2116
10:42 PM
Import certificate
Certificate:
Browse...
Password:
Enable this distribution point for prestaged content
Use the application or package properties to choose how content is copied to this distribution point.
OK
Cancel
Apply

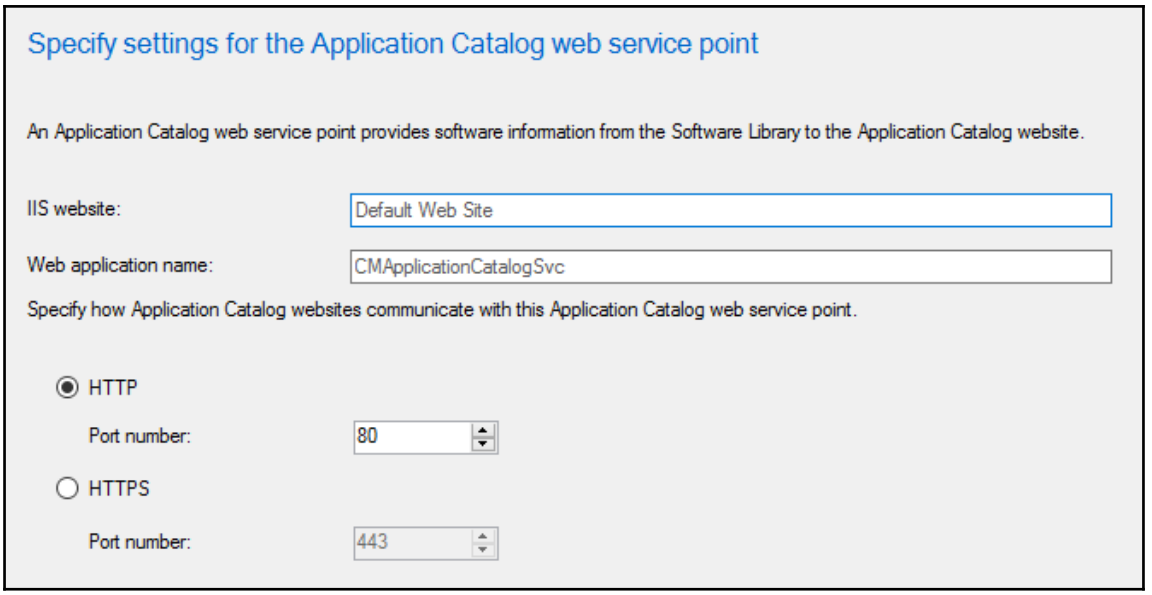

Management point Properties
General
Management Point Database
A management point provides policy and content location information to clients. It also receives configuration data from clients.
Client connections:
HTTP
This option does not support mobile devices, Mac computers, or connections over the Internet
HTTPS
This option requires client computers to have a valid PKI certificate for client authentication
Allow intranet-only connections
Allow mobile devices and Mac computers to use this management point
To manage Mac computers and Windows CE 7.0 devices that are enrolled by Configuration Manager, you must select an option that allows Internet client connections.
Generate alert when the management point is not healthy
OK
Cancel
Apply

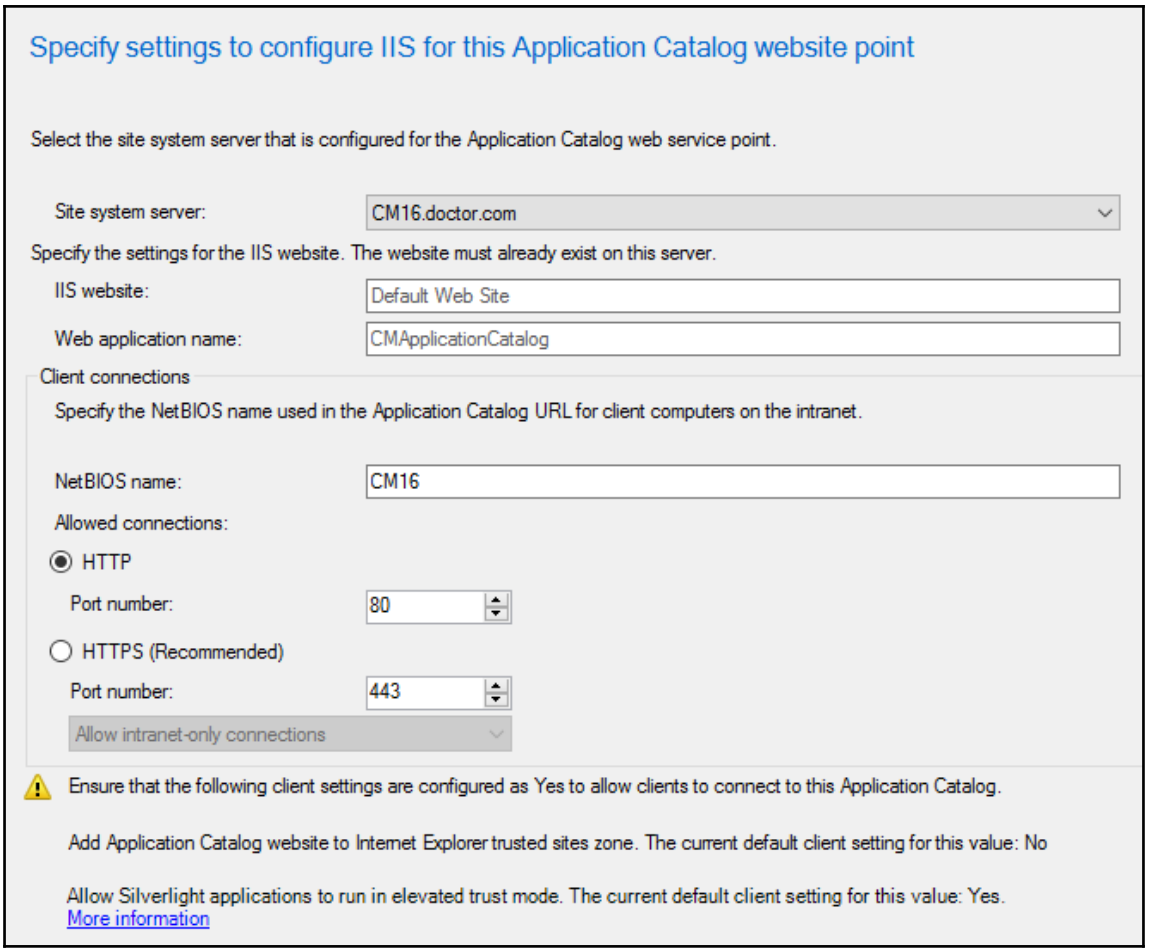

Create Site System Server Wizard
General
General
Proxy
System Role Selection
Summary
Progress
Completion
Select a server to use as a site system
Name (example: server1.corp.contoso.com):
CM.doctor.com
Browse...
Site code:
PA1 - Packt Primary Site
Specify an FQDN for this site system for use on the Internet
Internet FQDN (example: internetsrv2.contoso.com):
Require the site server to initiate connections to this site system
After the installation of the site system roles, the site server initiates all connections to the site system server by using the Site System Installation Account.
Site System Installation Account
Use the site server's computer account to install this site system
Use another account for installing this site system
Set...
Activate Windows
< Previous
Next >
Summary
Cancel

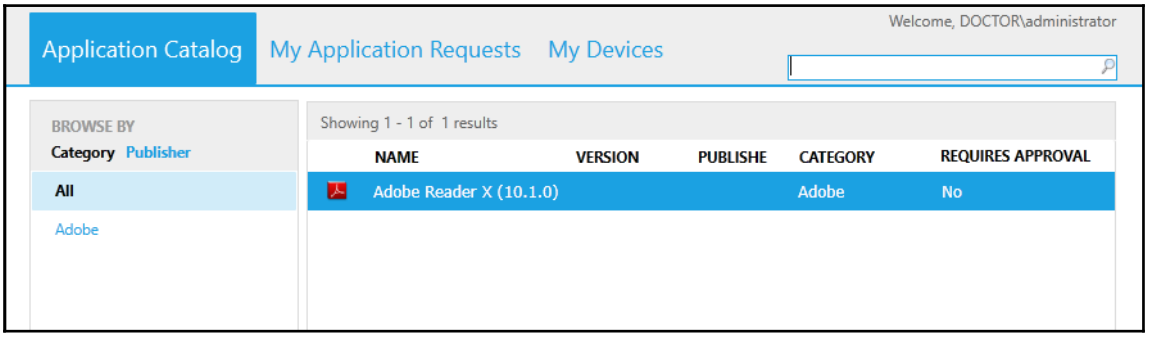

Add Site System Roles Wizard
General
General
Proxy
System Role Selection
Summary
Progress
Completion
Select a server to use as a site system
Name (example: server1.corp.contoso.com):
CM16.doctor.com
Browse...
Site code:
PA1 - Packt Primary Site
Specify an FQDN for this site system for use on the Internet
Internet FQDN (example: internetsrv2.contoso.com):
Require the site server to initiate connections to this site system
After the installation of the site system roles, the site server initiates all connections to the site system server by using the Site System Installation Account.
Site System Installation Account
Use the site server's computer account to install this site system
Use another account for installing this site system
Set...
Active Directory membership
Active Directory forest
doctor.com
Active Directory domain
doctor.com
Activate Windows
Go to Settings to activate W
< Previous
Next >
Summary
Cancel

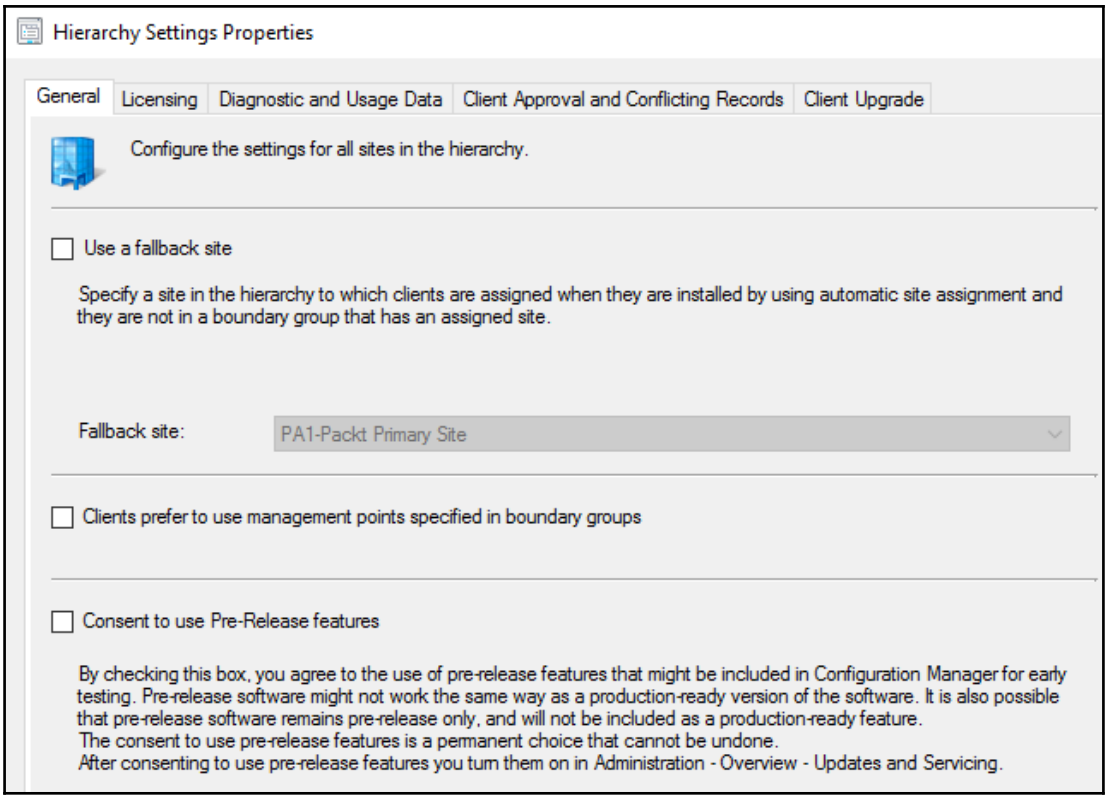

Specify Reporting Services settings
The reporting services point provides integration with SQL Server Reporting Services to create and manage reports for Configuration Manager.
Site database connection settings
Specify the Configuration Manager site database server name, optional database instance name, and database name which SQL Reporting Services will use when running reports.
Example: ServerName\InstanceName
Site database server name:
CM16.doctor.com
Database name:
CM_PA1
Verify
Specify the folder to create on the reporting services point site system server that will contain the Configuration Manager reports.
Folder name:
ConfigMgr_PA1
Reporting Services server instance:
Retrieving instance names...
Reporting Services Point Account
Specify the credentials that SQL Reporting Services will use when connecting to the Configuration Manager site database.
User name:
Set...

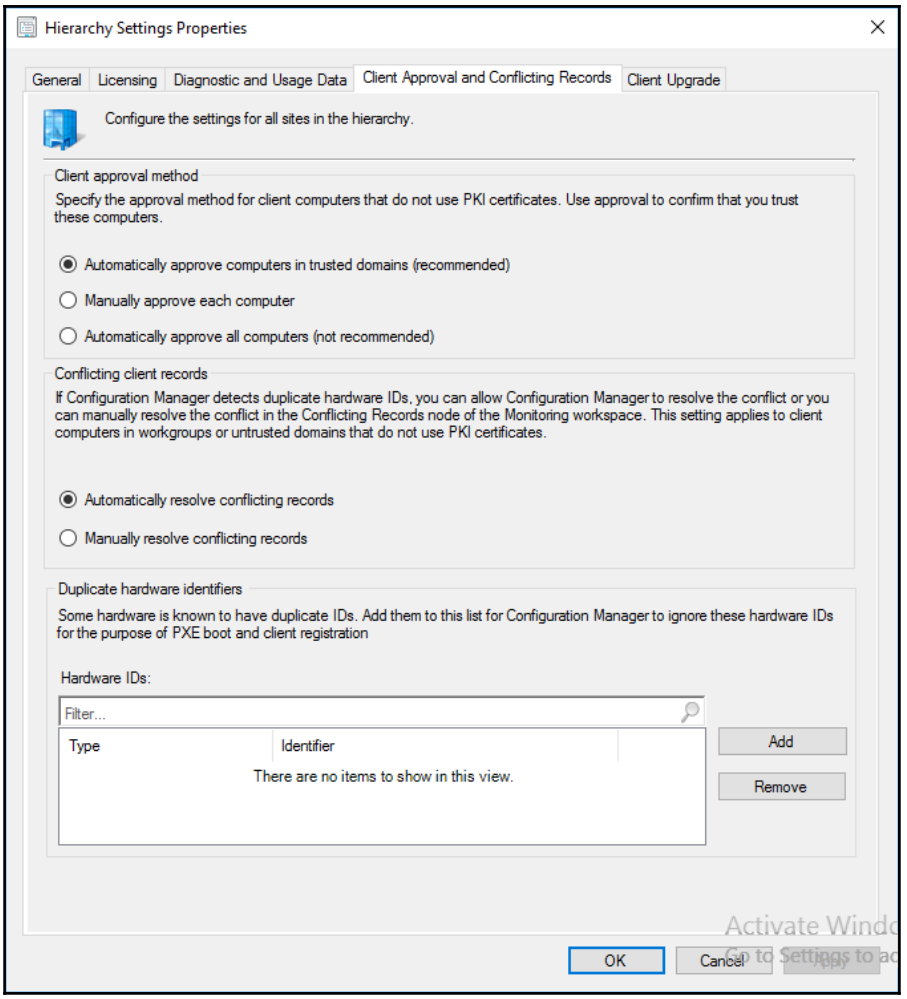

Specify Reporting Services settings
The reporting services point provides integration with SQL Server Reporting Services to create and manage reports for Configuration Manager.
Site database connection settings
Specify the Configuration Manager site database server name, optional database instance name, and database name which SQL Reporting Services will use when running reports.
Example: ServerName\InstanceName
Site database server name:
CM16.doctor.com
Database name:
CM_PA1
Verify
Successfully verified.
Specify the folder to create on the reporting services point site system server that will contain the Configuration Manager reports.
Folder name:
ConfigMgr_PA1
Reporting Services server instance:
MSSQLSERVER
Reporting Services Point Account
Specify the credentials that SQL Reporting Services will use when connecting to the Configuration Manager site database.
User name:
DOCTOR\Administrator
Set...

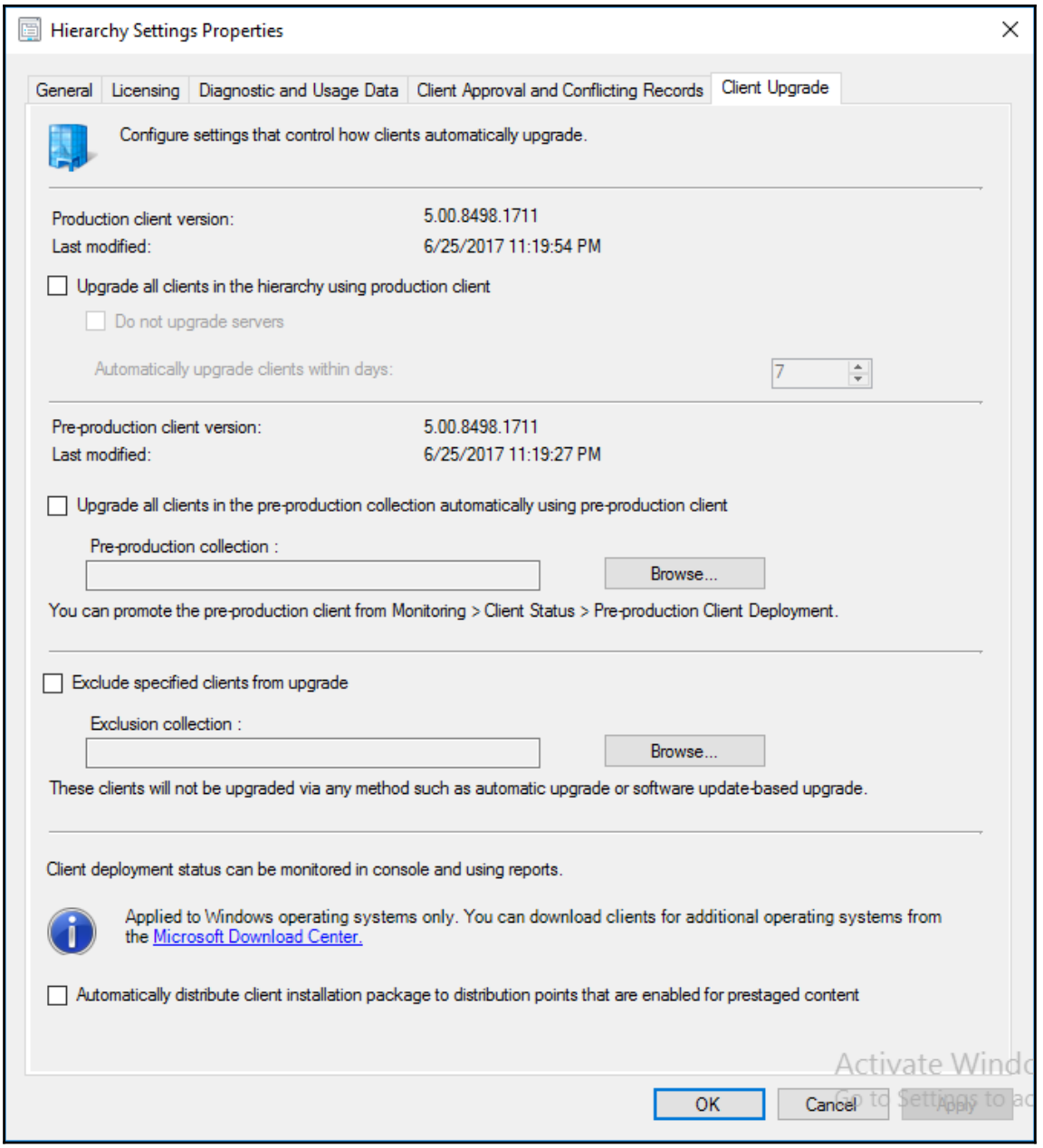

Specify settings for the Application Catalog web service point
An Application Catalog web service point provides software information from the Software Library to the Application Catalog website.
IIS website:
Default Web Site
Web application name:
CMApplicationCatalogSvc
Specify how Application Catalog websites communicate with this Application Catalog web service point.
HTTP
Port number:
80
HTTPS
Port number:
443

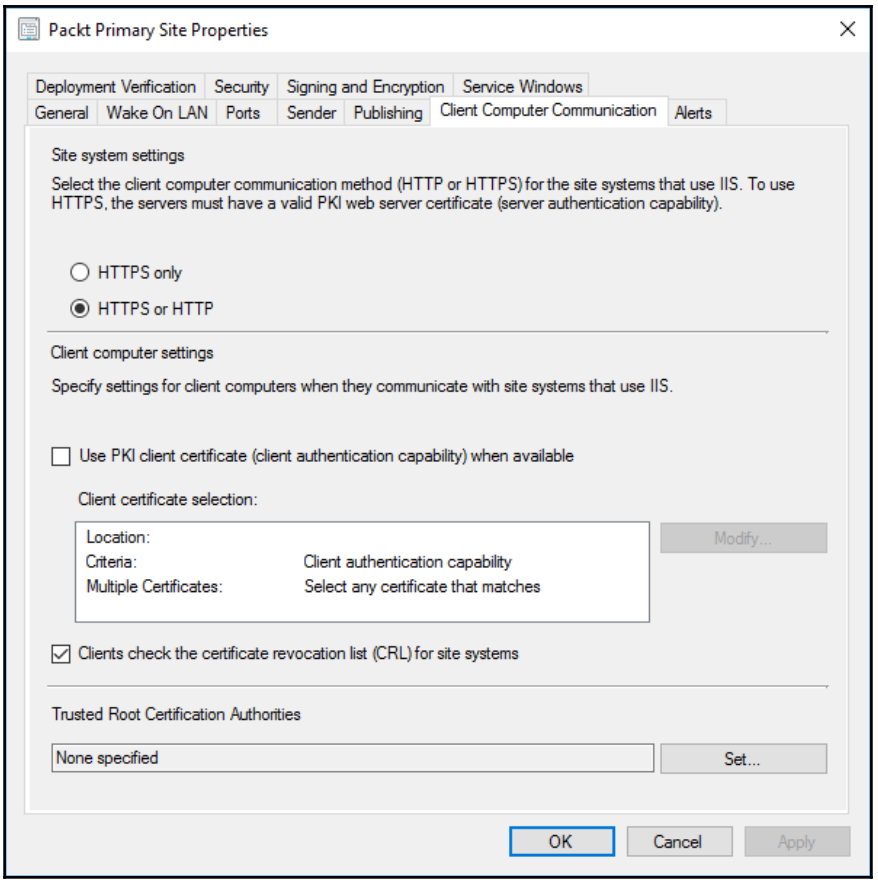

Specify settings to configure IIS for this Application Catalog website point
Select the site system server that is configured for the Application Catalog web service point.
Site system server:
CM16.doctor.com
Specify the settings for the IIS website. The website must already exist on this server.
IIS website:
Default Web Site
Web application name:
CMApplicationCatalog
Client connections
Specify the NetBIOS name used in the Application Catalog URL for client computers on the intranet.
NetBIOS name:
CM16
Allowed connections:
HTTP
Port number:
80
HTTPS (Recommended)
Port number:
443
Allow intranet-only connections
Ensure that the following client settings are configured as Yes to allow clients to connect to this Application Catalog.
Add Application Catalog website to Internet Explorer trusted sites zone. The current default client setting for this value: No
Allow Silverlight applications to run in elevated trust mode. The current default client setting for this value: Yes.
More information

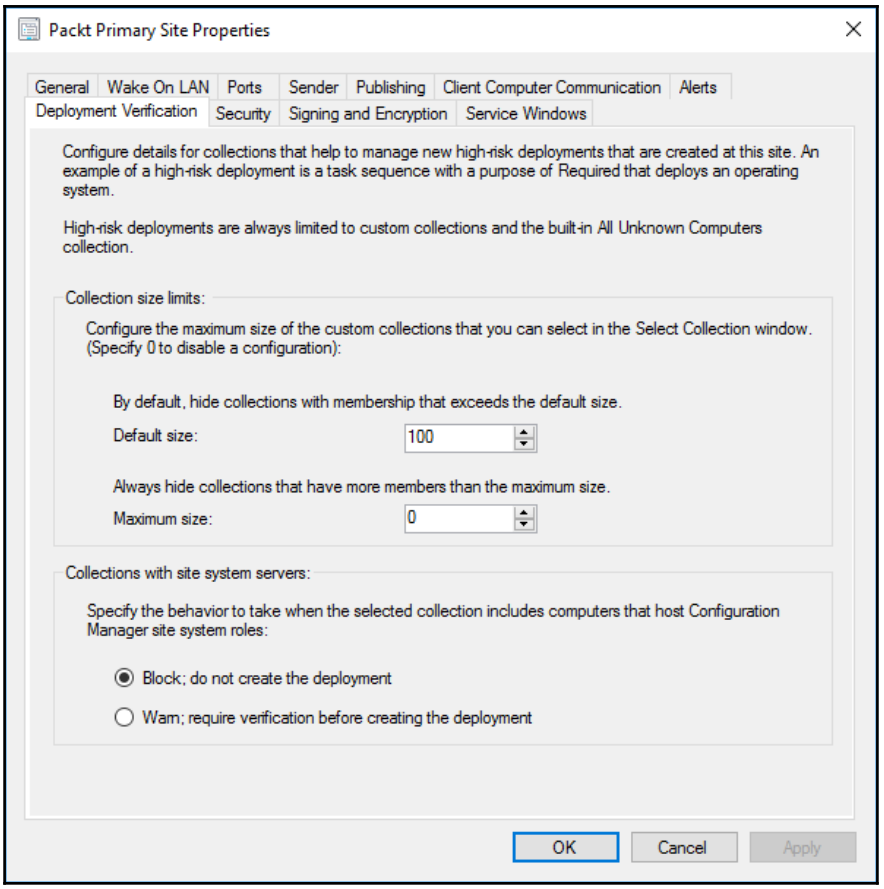

Application Catalog
My Application Requests
My Devices
Welcome, DOCTOR\administrator
BROWSE BY
Category Publisher
All
Adobe
Showing 1 - 1 of 1 results
NAME
VERSION
PUBLISHE
CATEGORY
REQUIRES APPROVAL
Adobe Reader X (10.1.0)
Adobe
No

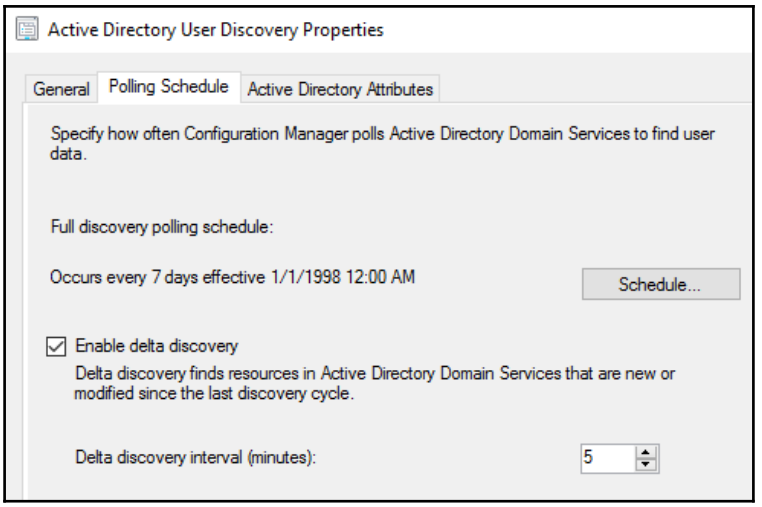

Hierarchy Settings Properties
General
Licensing
Diagnostic and Usage Data
Client Approval and Conflicting Records
Client Upgrade
Configure the settings for all sites in the hierarchy.
Use a fallback site
Specify a site in the hierarchy to which clients are assigned when they are installed by using automatic site assignment and they are not in a boundary group that has an assigned site.
Fallback site:
PA1-Packt Primary Site
Clients prefer to use management points specified in boundary groups
Consent to use Pre-Release features
By checking this box, you agree to the use of pre-release features that might be included in Configuration Manager for early testing. Pre-release software might not work the same way as a production-ready version of the software. It is also possible that pre-release software remains pre-release only, and will not be included as a production-ready feature.
The consent to use pre-release features is a permanent choice that cannot be undone.
After consenting to use pre-release features you turn them on in Administration - Overview - Updates and Servicing.

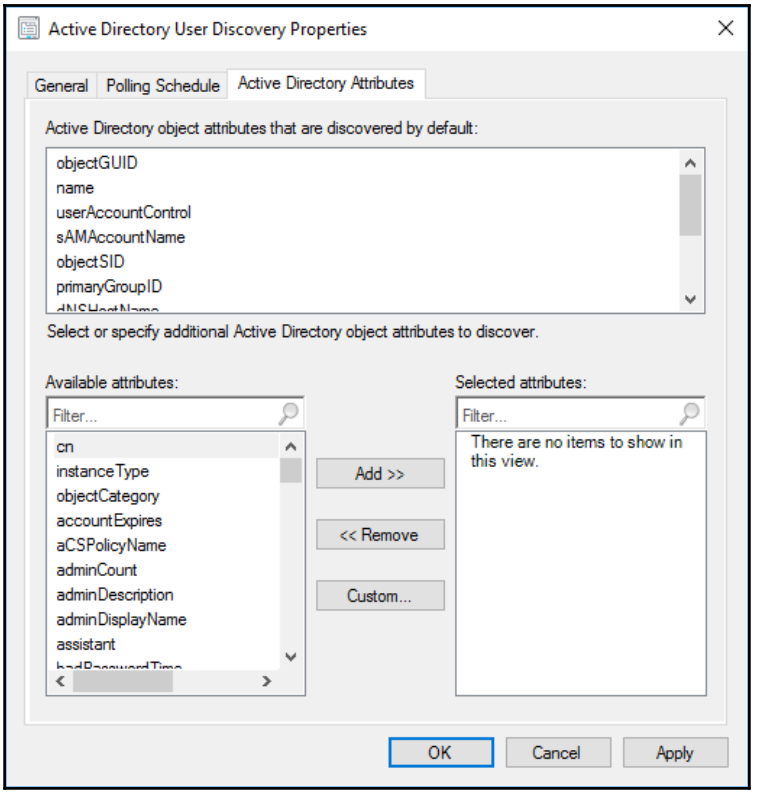

Hierarchy Settings Properties
General
Licensing
Diagnostic and Usage Data
Client Approval and Conflicting Records
Client Upgrade
Configure the settings for all sites in the hierarchy.
Client approval method
Specify the approval method for client computers that do not use PKI certificates. Use approval to confirm that you trust these computers.
Automatically approve computers in trusted domains (recommended)
Manually approve each computer
Automatically approve all computers (not recommended)
Conflicting client records
If Configuration Manager detects duplicate hardware IDs, you can allow Configuration Manager to resolve the conflict or you can manually resolve the conflict in the Conflicting Records node of the Monitoring workspace. This setting applies to client computers in workgroups or untrusted domains that do not use PKI certificates.
Automatically resolve conflicting records
Manually resolve conflicting records
Duplicate hardware identifiers
Some hardware is known to have duplicate IDs. Add them to this list for Configuration Manager to ignore these hardware IDs for the purpose of PXE boot and client registration
Hardware IDs:
Filter...
Type
Identifier
There are no items to show in this view.
Add
Remove
OK
Cancel
Apply

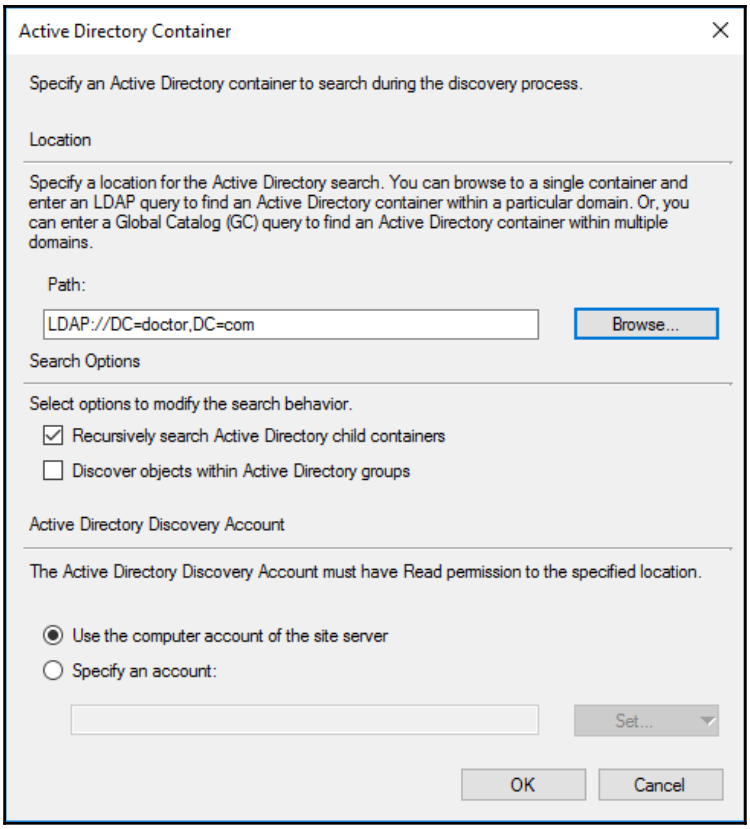

Hierarchy Settings Properties
General
Licensing
Diagnostic and Usage Data
Client Approval and Conflicting Records
Client Upgrade
Configure settings that control how clients automatically upgrade.
Production client version:
5.00.8498.1711
Last modified:
6/25/2017 11:19:54 PM
Upgrade all clients in the hierarchy using production client
Do not upgrade servers
Automatically upgrade clients within days:
7
Pre-production client version:
5.00.8498.1711
Last modified:
6/25/2017 11:19:27 PM
Upgrade all clients in the pre-production collection automatically using pre-production client
Pre-production collection :
Browse...
You can promote the pre-production client from Monitoring > Client Status > Pre-production Client Deployment.
Exclude specified clients from upgrade
Exclusion collection :
Browse...
These clients will not be upgraded via any method such as automatic upgrade or software update-based upgrade.
Client deployment status can be monitored in console and using reports.
Applied to Windows operating systems only. You can download clients for additional operating systems from the Microsoft Download Center.
Automatically distribute client installation package to distribution points that are enabled for prestaged content
Activate Windo
Go to Settings to ac
OK
Cancel
Apply

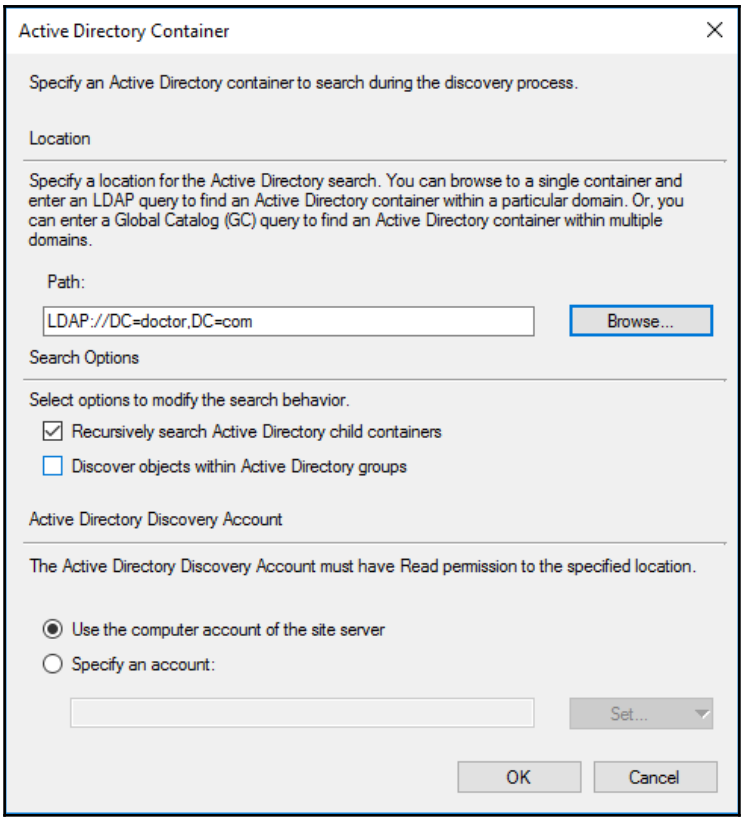

Packt Primary Site Properties
Deployment Verification
Security
Signing and Encryption
Service Windows
General
Wake On LAN
Ports
Sender
Publishing
Client Computer Communication
Alerts
Site system settings
Select the client computer communication method (HTTP or HTTPS) for the site systems that use IIS. To use HTTPS, the servers must have a valid PKI web server certificate (server authentication capability).
HTTPS only
HTTPS or HTTP
Client computer settings
Specify settings for client computers when they communicate with site systems that use IIS.
Use PKI client certificate (client authentication capability) when available
Client certificate selection:
Location:
Criteria:
Client authentication capability
Multiple Certificates:
Select any certificate that matches
Modify...
Clients check the certificate revocation list (CRL) for site systems
Trusted Root Certification Authorities
None specified
Set...
OK
Cancel
Apply

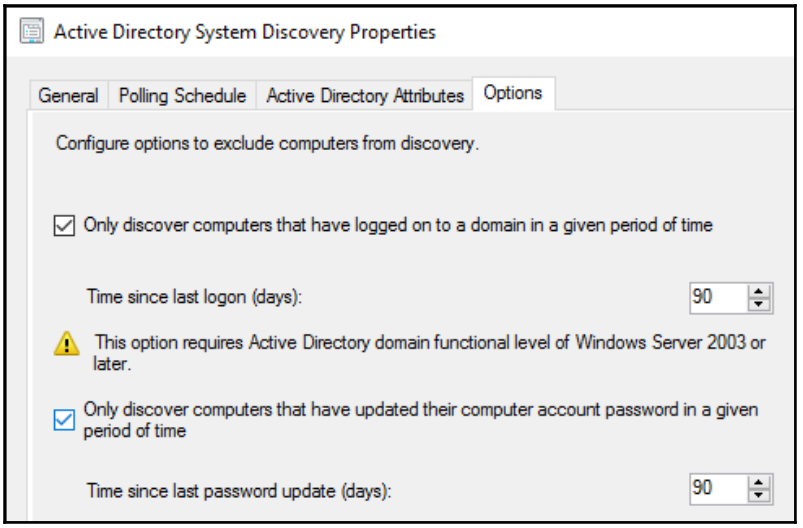

Packt Primary Site Properties
General
Wake On LAN
Ports
Sender
Publishing
Client Computer Communication
Alerts
Deployment Verification
Security
Signing and Encryption
Service Windows
Configure details for collections that help to manage new high-risk deployments that are created at this site. An example of a high-risk deployment is a task sequence with a purpose of Required that deploys an operating system.
High-risk deployments are always limited to custom collections and the built-in All Unknown Computers collection.
Collection size limits:
Configure the maximum size of the custom collections that you can select in the Select Collection window. (Specify 0 to disable a configuration):
By default, hide collections with membership that exceeds the default size.
Default size:
100
Always hide collections that have more members than the maximum size.
Maximum size:
0
Collections with site system servers:
Specify the behavior to take when the selected collection includes computers that host Configuration Manager site system roles:
Block; do not create the deployment
Warn; require verification before creating the deployment
OK
Cancel
Apply

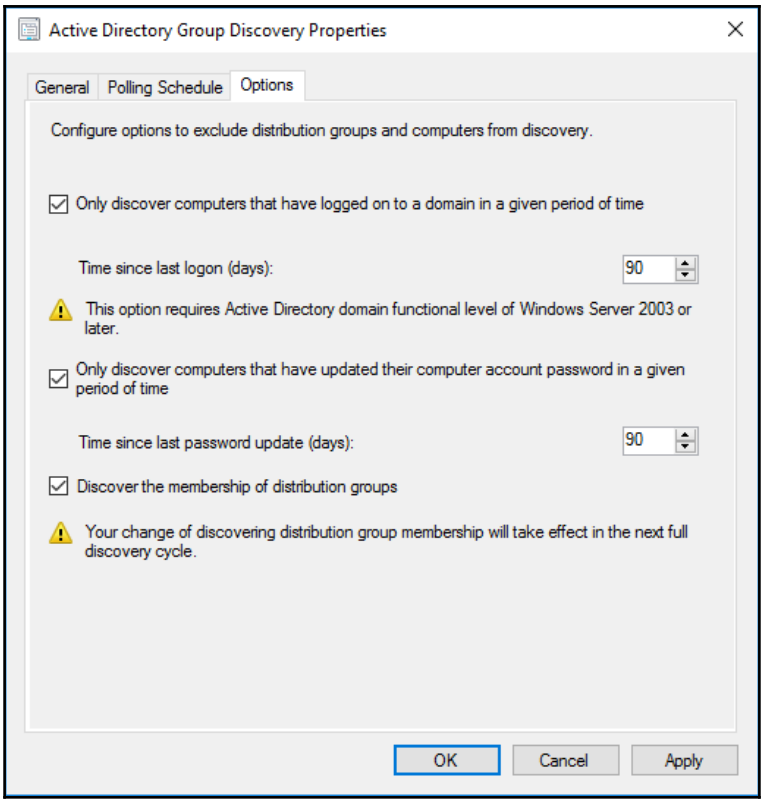

Active Directory User Discovery Properties
General
Polling Schedule
Active Directory Attributes
Specify how often Configuration Manager polls Active Directory Domain Services to find user data.
Full discovery polling schedule:
Occurs every 7 days effective 1/1/1998 12:00 AM
Schedule...
Enable delta discovery
Delta discovery finds resources in Active Directory Domain Services that are new or modified since the last discovery cycle.
Delta discovery interval (minutes):
5

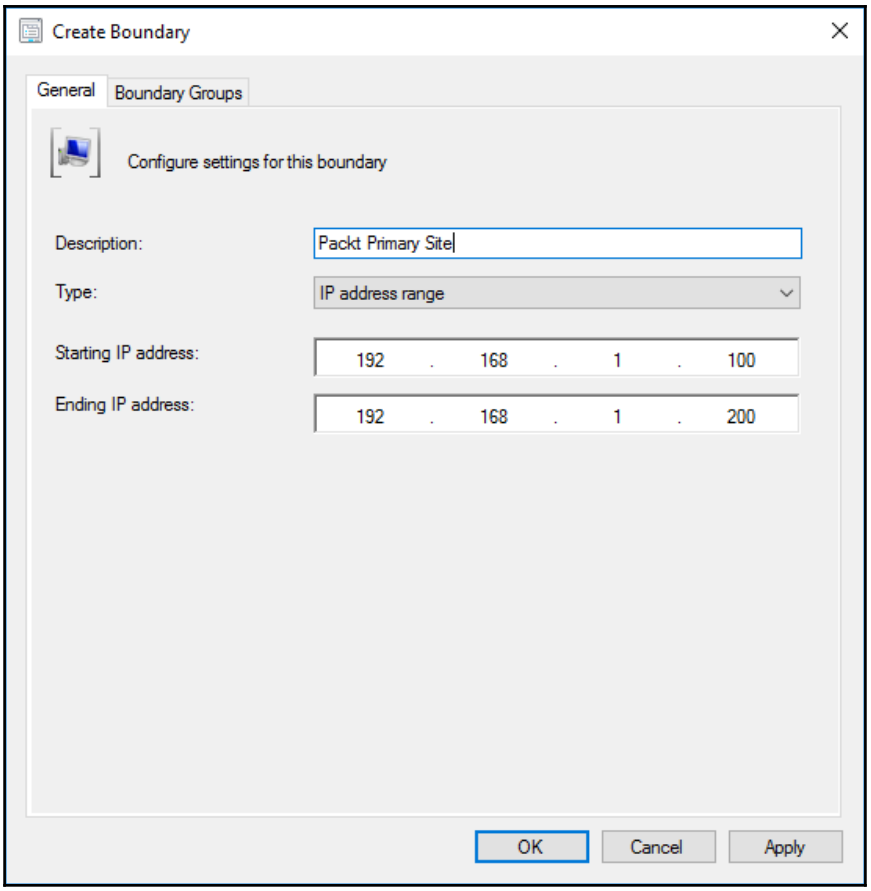

Active Directory User Discovery Properties
General
Polling Schedule
Active Directory Attributes
Active Directory object attributes that are discovered by default:
objectGUID
name
userAccountControl
sAMAccountName
objectSID
primaryGroupID
Select or specify additional Active Directory object attributes to discover.
Available attributes:
Filter...
cn
instanceType
objectCategory
accountExpires
aCSPolicyName
adminCount
adminDescription
adminDisplayName
assistant
Add >>
<< Remove
Custom...
Selected attributes:
Filter...
There are no items to show in this view.
OK
Cancel
Apply

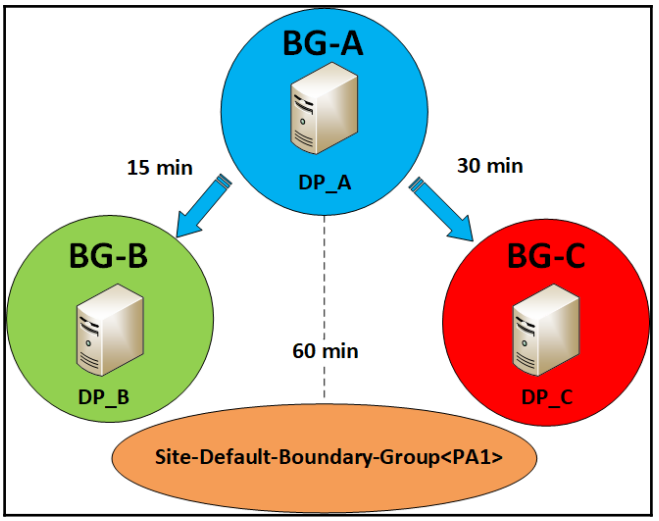

Active Directory Container
Specify an Active Directory container to search during the discovery process.
Location
Specify a location for the Active Directory search. You can browse to a single container and enter an LDAP query to find an Active Directory container within a particular domain. Or, you can enter a Global Catalog (GC) query to find an Active Directory container within multiple domains.
Path:
LDAP://DC=doctor,DC=com
Browse...
Search Options
Select options to modify the search behavior.
Recursively search Active Directory child containers
Discover objects within Active Directory groups
Active Directory Discovery Account
The Active Directory Discovery Account must have Read permission to the specified location.
Use the computer account of the site server
Specify an account:
Set...
OK
Cancel

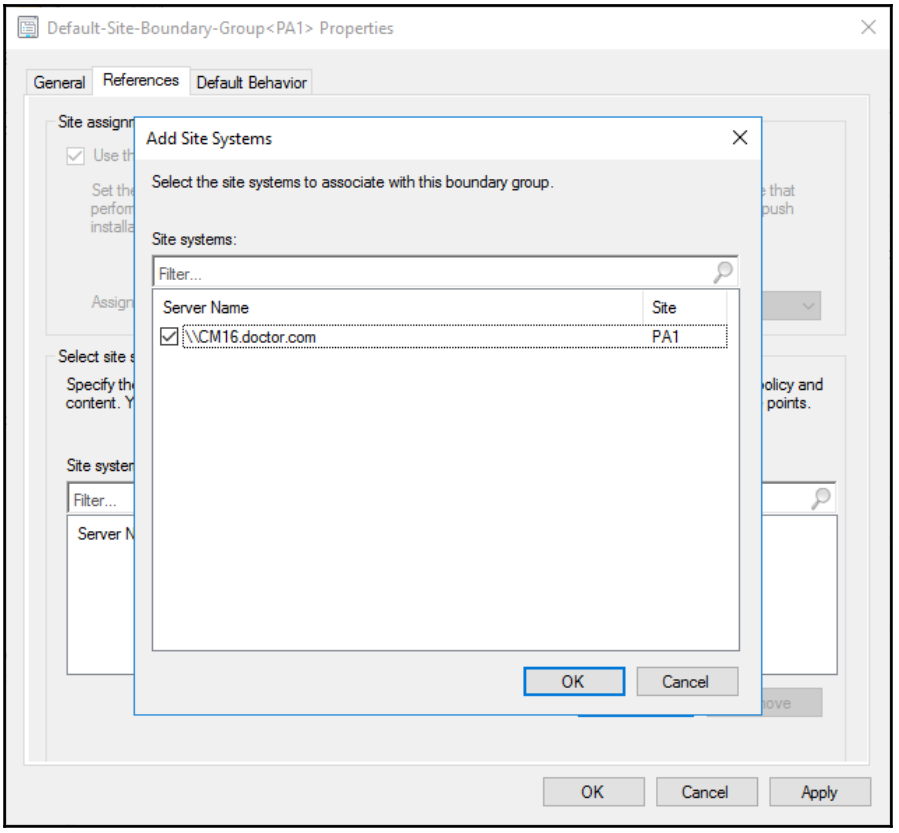

Active Directory Container
Specify an Active Directory container to search during the discovery process.
Location
Specify a location for the Active Directory search. You can browse to a single container and enter an LDAP query to find an Active Directory container within a particular domain. Or, you can enter a Global Catalog (GC) query to find an Active Directory container within multiple domains.
Path:
LDAP://DC=doctor,DC=com
Browse...
Search Options
Select options to modify the search behavior.
Recursively search Active Directory child containers
Discover objects within Active Directory groups
Active Directory Discovery Account
The Active Directory Discovery Account must have Read permission to the specified location.
Use the computer account of the site server
Specify an account:
Set...
OK
Cancel

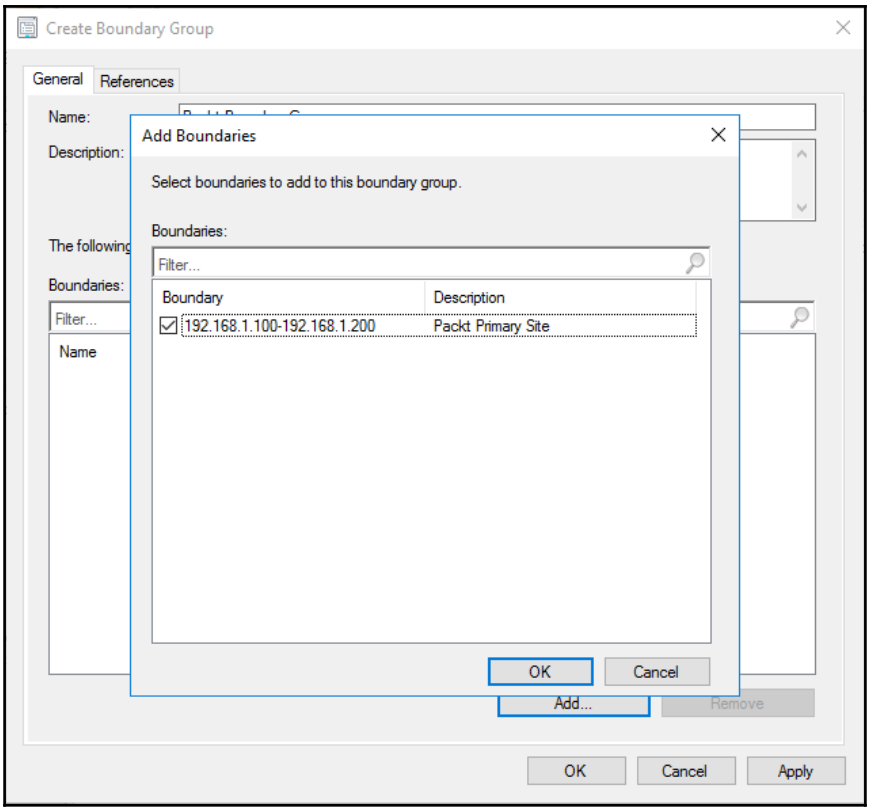

Active Directory System Discovery Properties
General
Polling Schedule
Active Directory Attributes
Options
Configure options to exclude computers from discovery.
Only discover computers that have logged on to a domain in a given period of time
Time since last logon (days):
90
This option requires Active Directory domain functional level of Windows Server 2003 or later.
Only discover computers that have updated their computer account password in a given period of time
Time since last password update (days):
90

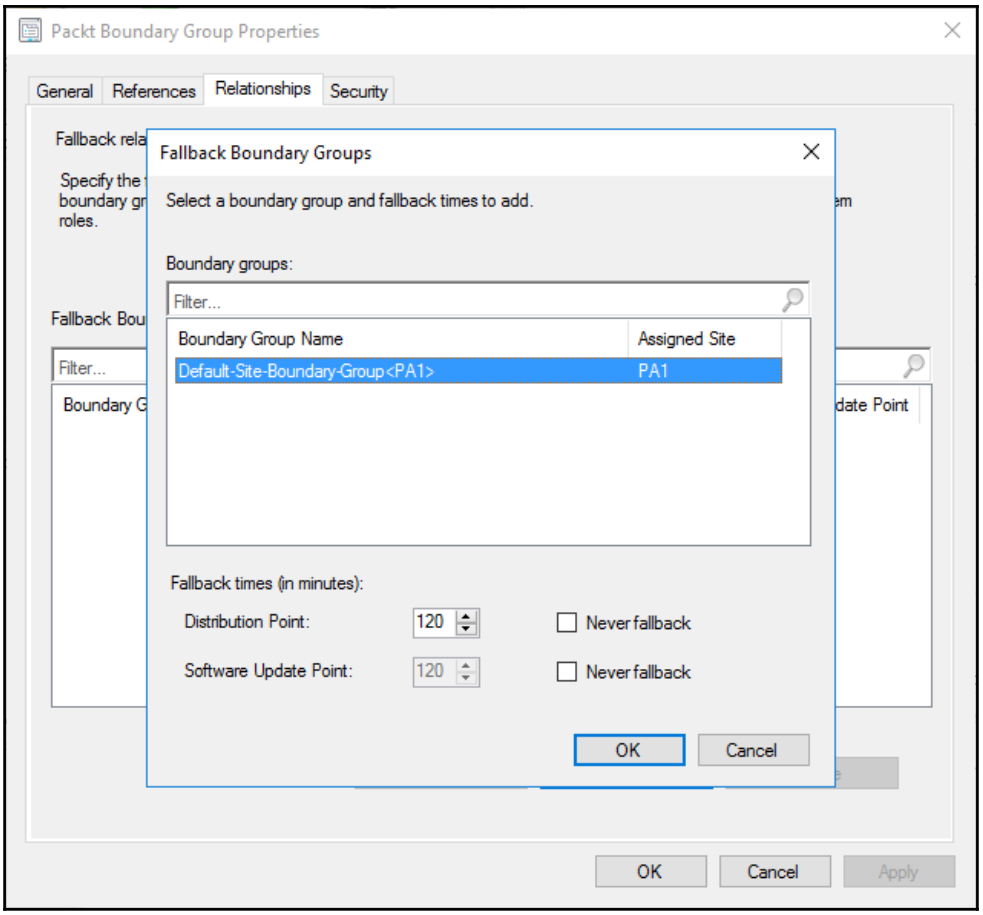

Active Directory Group Discovery Properties
General
Polling Schedule
Options
Configure options to exclude distribution groups and computers from discovery.
Only discover computers that have logged on to a domain in a given period of time
Time since last logon (days):
90
This option requires Active Directory domain functional level of Windows Server 2003 or later.
Only discover computers that have updated their computer account password in a given period of time
Time since last password update (days):
90
Discover the membership of distribution groups
Your change of discovering distribution group membership will take effect in the next full discovery cycle.
OK
Cancel
Apply


Create Boundary
General
Boundary Groups
Configure settings for this boundary
Description:
Packt Primary Site
Type:
IP address range
Starting IP address:
192 . 168 . 1 . 100
Ending IP address:
192 . 168 . 1 . 200
OK
Cancel
Apply

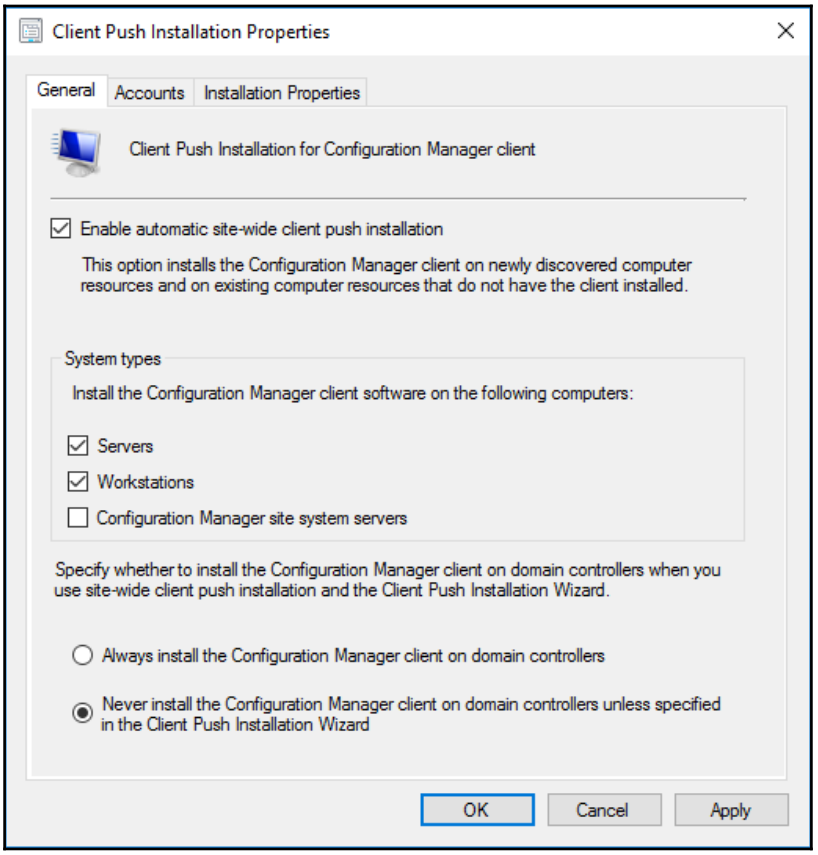

BG-A
DP_A
15 min
30 min
BG-B
DP_B
60 min
BG-C
DP_C
Site-Default-Boundary-Group<PA1>

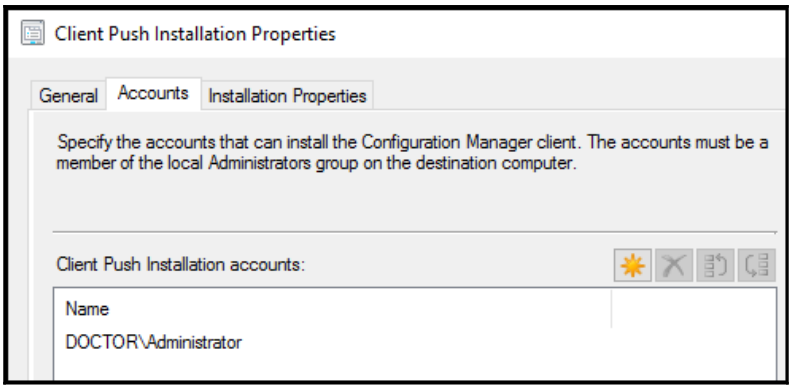

Default-Site-Boundary-Group<PA1> Properties
General
References
Default Behavior
Add Site Systems
Select the site systems to associate with this boundary group.
Site systems:
Filter...
Server Name
Site
\\CM16.doctor.com
PA1
OK
Cancel
OK
Cancel
Apply


Create Boundary Group
General
References
Name:
Description:
The following
Boundaries:
Filter...
Name
Add Boundaries
Select boundaries to add to this boundary group.
Boundaries:
Filter...
Boundary
Description
192.168.1.100-192.168.1.200
Packt Primary Site
OK
Cancel
Add...
Remove
OK
Cancel
Apply

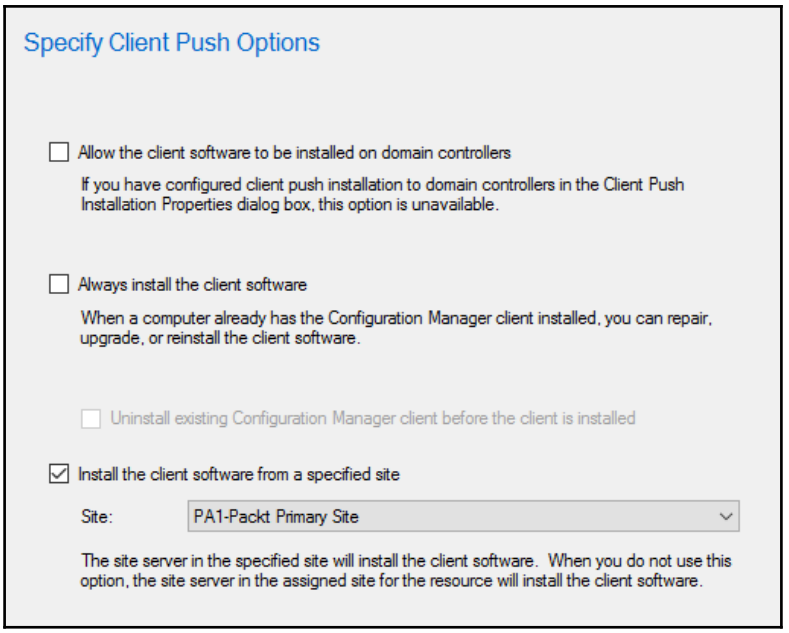

Packt Boundary Group Properties
General
References
Relationships
Security
Fallback rela
Specify the
boundary gr
roles.
Fallback Bou
Filter...
Boundary G
Fallback Boundary Groups
Select a boundary group and fallback times to add.
Boundary groups:
Filter...
Boundary Group Name
Assigned Site
Default-Site-Boundary-Group<PA1>
PA1
Fallback times (in minutes):
Distribution Point:
120
Never fallback
Software Update Point:
120
Never fallback
OK
Cancel
date Point
OK
Cancel
Apply

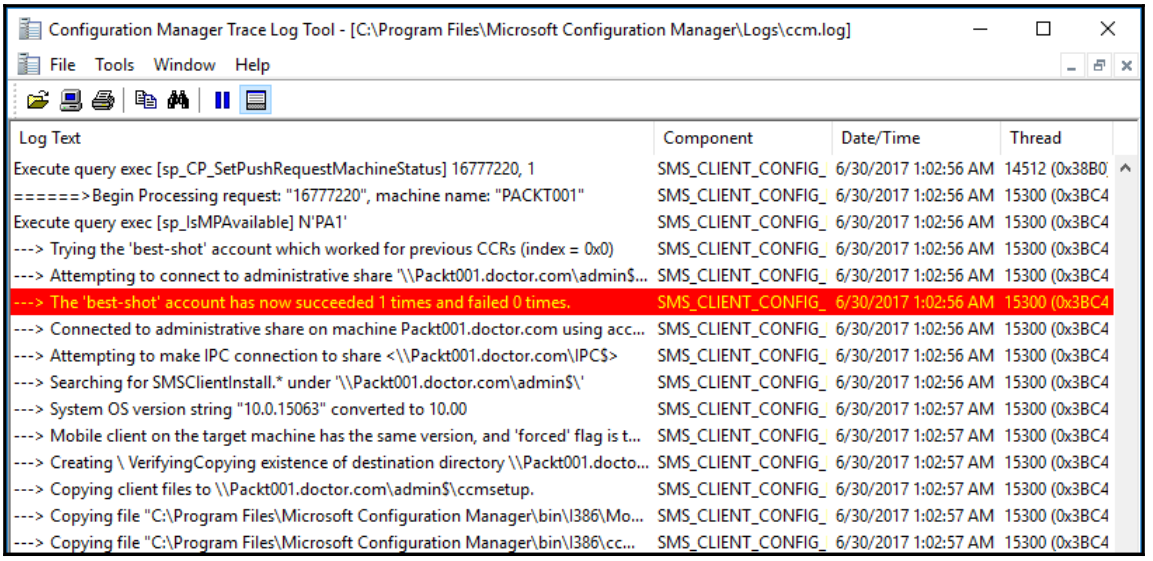
# Chapter 4: Configuration Manager Agent Installation

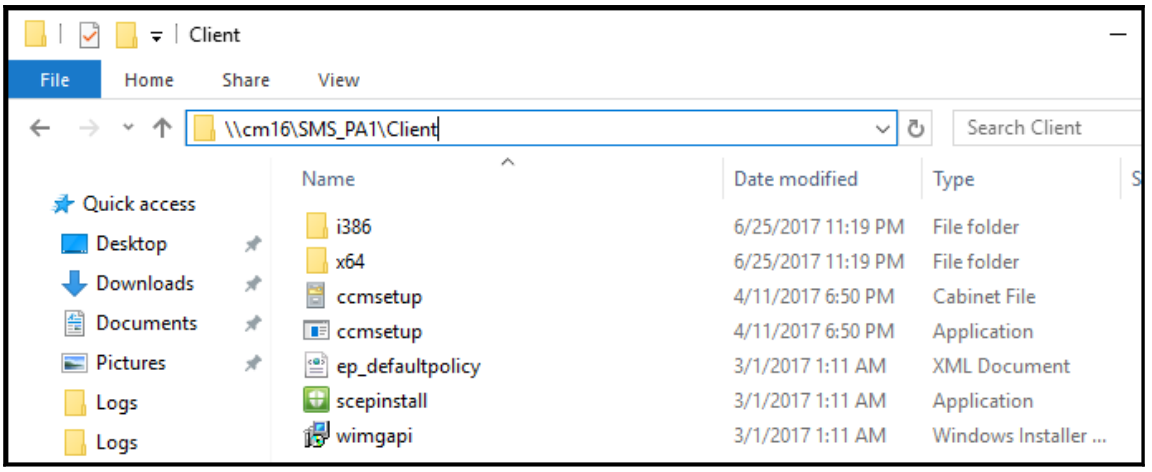


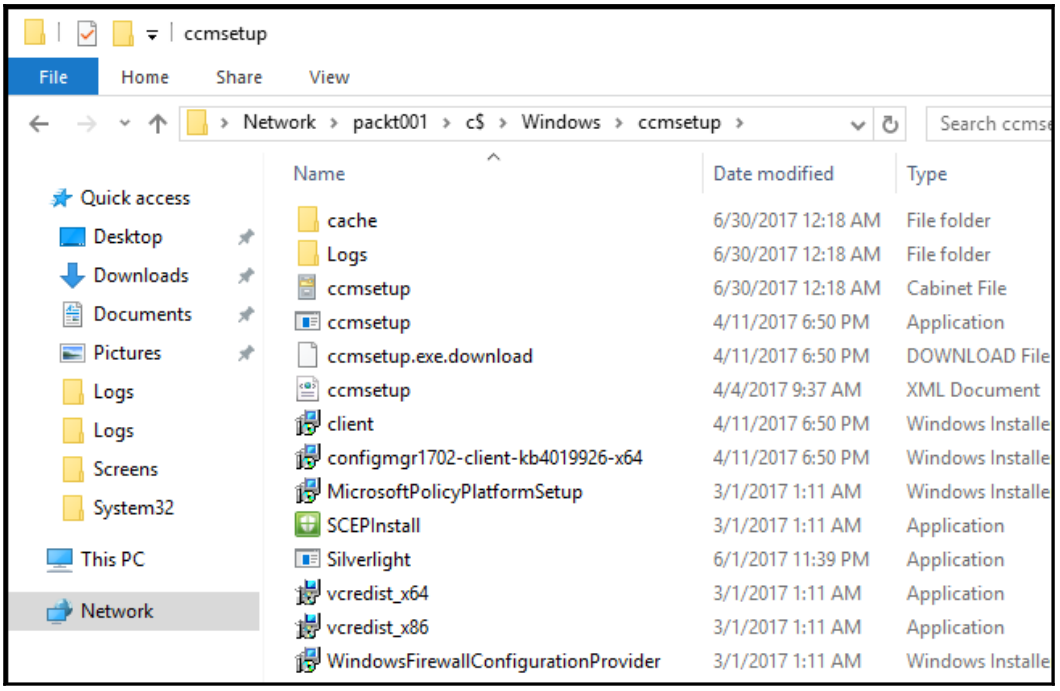

Client Push Installation Properties
General
Accounts
Installation Properties
Specify the accounts that can install the Configuration Manager client. The accounts must be a member of the local Administrators group on the destination computer.
Client Push Installation accounts:
Name
DOCTOR\Administrator

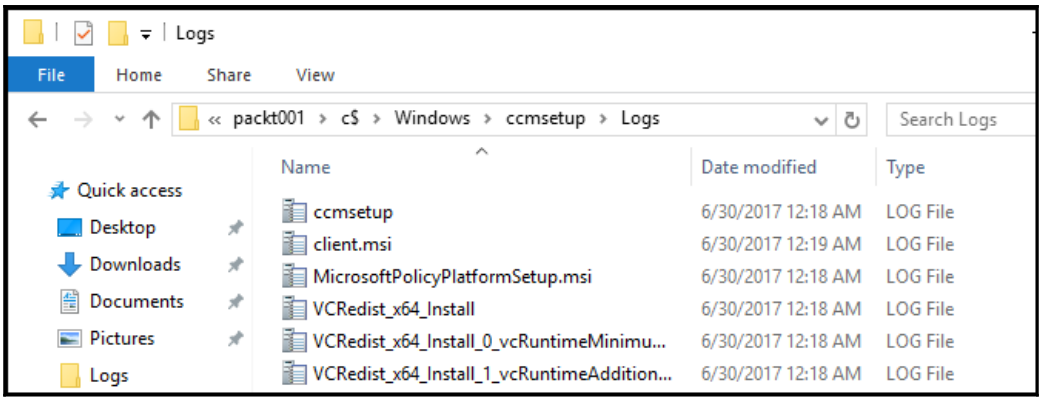

Client Push Installation Properties
General
Accounts
Installation Properties
Specify any client.msi installation properties that you require when you install the Configuration Manager client software. Do not specify installation properties for CCMSetup.exe.
Installation properties:
SMSSITECODE=PA1 SMSFPS=CM12.DOCTOR.COM

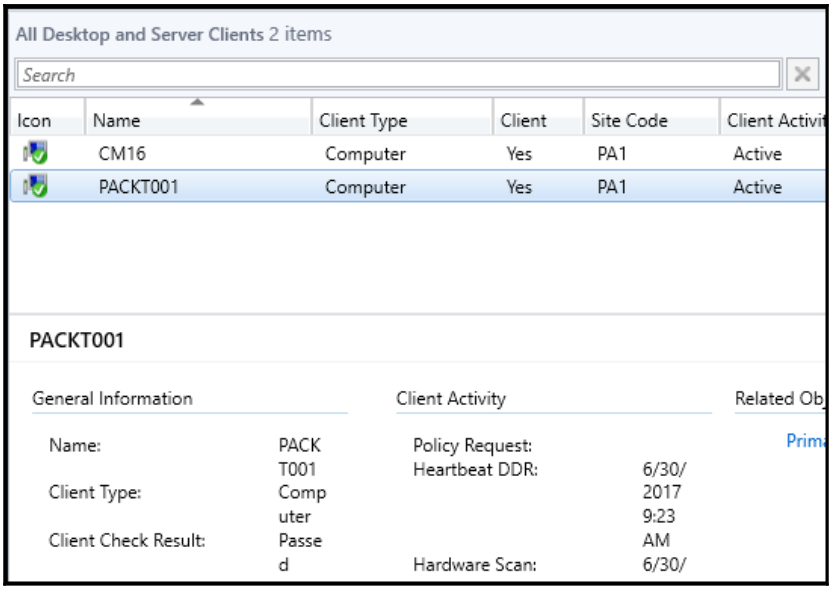

Specify Client Push Options
Allow the client software to be installed on domain controllers
If you have configured client push installation to domain controllers in the Client Push Installation Properties dialog box, this option is unavailable.
Always install the client software
When a computer already has the Configuration Manager client installed, you can repair, upgrade, or reinstall the client software.
Uninstall existing Configuration Manager client before the client is installed
Install the client software from a specified site
Site:
PA1-Packt Primary Site
The site server in the specified site will install the client software. When you do not use this option, the site server in the assigned site for the resource will install the client software.

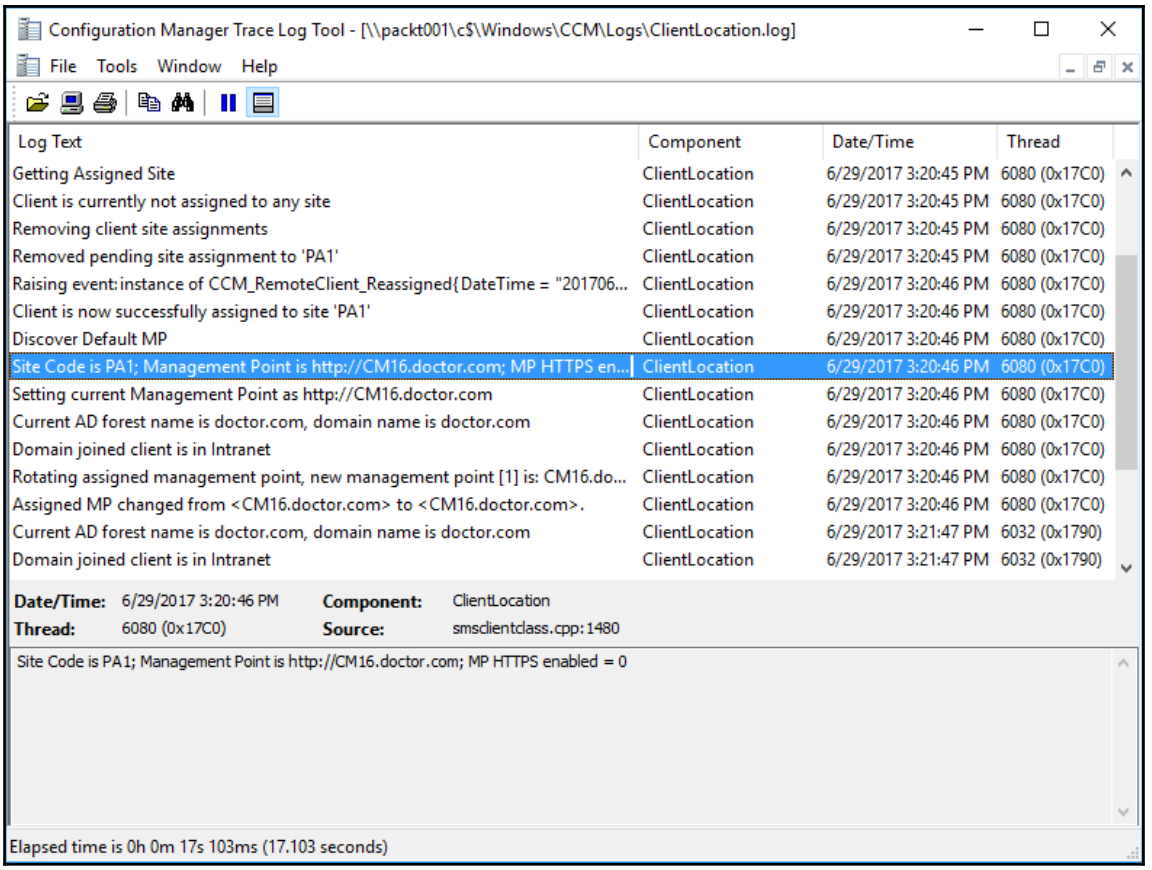

Configuration Manager Trace Log Tool - [C:\Program Files\Microsoft Configuration Manager\Logs\ccm.log]
File Tools Window Help
Log Text Component Date/Time Thread
Execute query exec [sp_CP_SetPushRequestMachineStatus] 16777220, 1 SMS_CLIENT_CONFIG_ 6/30/2017 1:02:56 AM 14512 (0x38B0
======>Begin Processing request: "16777220", machine name: "PACKT001" SMS_CLIENT_CONFIG_ 6/30/2017 1:02:56 AM 15300 (0x3BC4
Execute query exec [sp_IsMPAvailable] N'PA1' SMS_CLIENT_CONFIG_ 6/30/2017 1:02:56 AM 15300 (0x3BC4
---> Trying the 'best-shot' account which worked for previous CCRs (index = 0x0) SMS_CLIENT_CONFIG_ 6/30/2017 1:02:56 AM 15300 (0x3BC4
---> Attempting to connect to administrative share '\\Packt001.doctor.com\admin$... SMS_CLIENT_CONFIG_ 6/30/2017 1:02:56 AM 15300 (0x3BC4
---> The 'best-shot' account has now succeeded 1 times and failed 0 times. SMS_CLIENT_CONFIG_ 6/30/2017 1:02:56 AM 15300 (0x3BC4
---> Connected to administrative share on machine Packt001.doctor.com using acc... SMS_CLIENT_CONFIG_ 6/30/2017 1:02:56 AM 15300 (0x3BC4
---> Attempting to make IPC connection to share <\\Packt001.doctor.com\IPC$> SMS_CLIENT_CONFIG_ 6/30/2017 1:02:56 AM 15300 (0x3BC4
---> Searching for SMSClientInstall.* under '\\Packt001.doctor.com\admin$\' SMS_CLIENT_CONFIG_ 6/30/2017 1:02:56 AM 15300 (0x3BC4
---> System OS version string "10.0.15063" converted to 10.00 SMS_CLIENT_CONFIG_ 6/30/2017 1:02:57 AM 15300 (0x3BC4
---> Mobile client on the target machine has the same version, and 'forced' flag is t... SMS_CLIENT_CONFIG_ 6/30/2017 1:02:57 AM 15300 (0x3BC4
---> Creating \ VerifyingCopying existence of destination directory \\Packt001.docto... SMS_CLIENT_CONFIG_ 6/30/2017 1:02:57 AM 15300 (0x3BC4
---> Copying client files to \\Packt001.doctor.com\admin$\ccmsetup. SMS_CLIENT_CONFIG_ 6/30/2017 1:02:57 AM 15300 (0x3BC4
---> Copying file "C:\Program Files\Microsoft Configuration Manager\bin\I386\Mo... SMS_CLIENT_CONFIG_ 6/30/2017 1:02:57 AM 15300 (0x3BC4
---> Copying file "C:\Program Files\Microsoft Configuration Manager\bin\I386\cc... SMS_CLIENT_CONFIG_ 6/30/2017 1:02:57 AM 15300 (0x3BC4

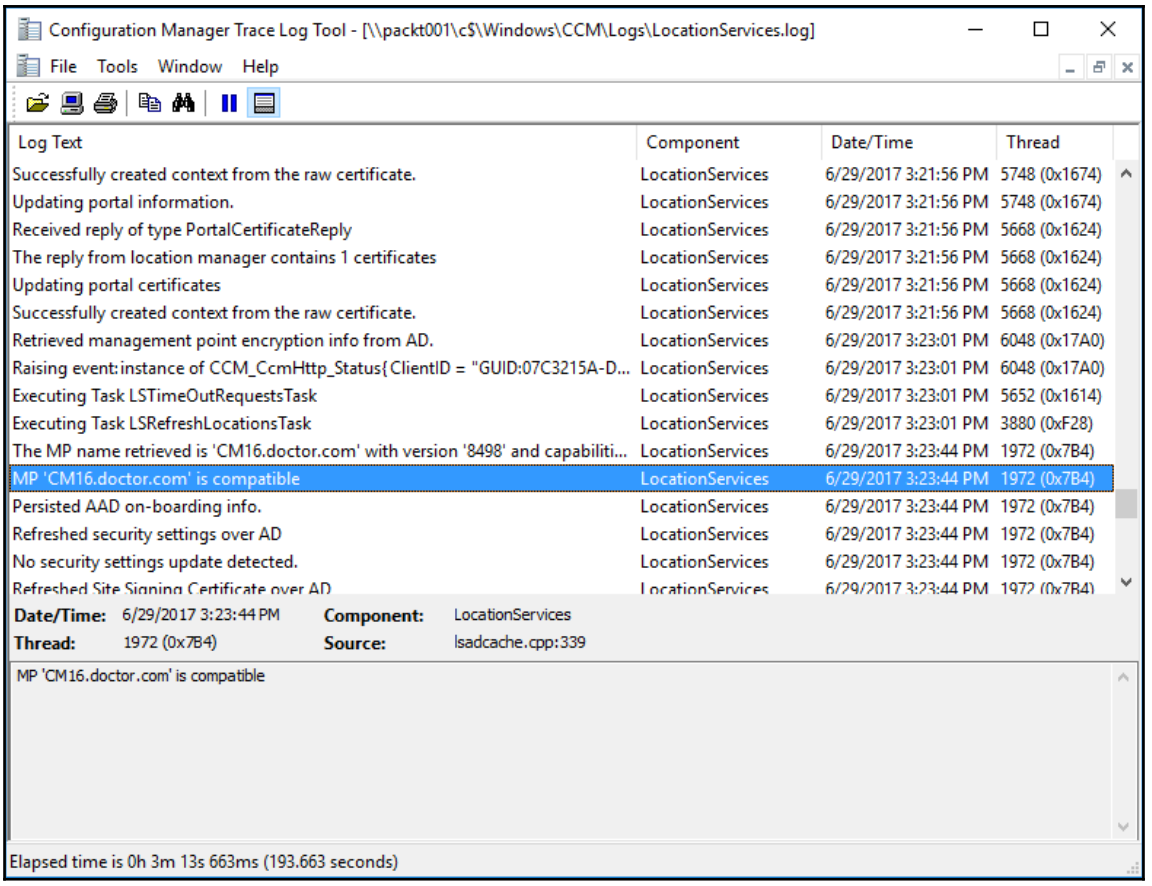

Client
File
Home
Share
View
\\cm16\SMS_PA1\Client
Search Client
Quick access
Desktop
Downloads
Documents
Pictures
Logs
Logs
Name
Date modified
Type
i386
6/25/2017 11:19 PM
File folder
x64
6/25/2017 11:19 PM
File folder
ccmsetup
4/11/2017 6:50 PM
Cabinet File
ccmsetup
4/11/2017 6:50 PM
Application
ep_defaultpolicy
3/1/2017 1:11 AM
XML Document
scepinstall
3/1/2017 1:11 AM
Application
wimgapi
3/1/2017 1:11 AM
Windows Installer ...

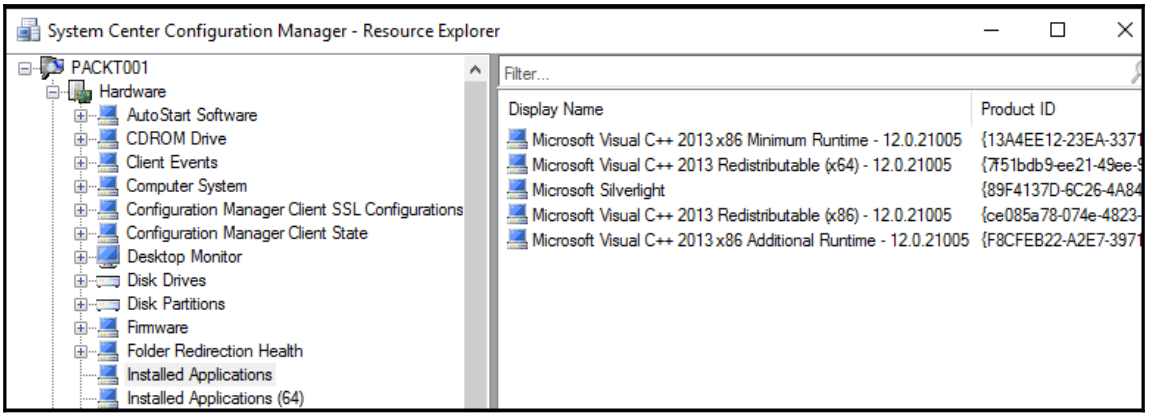

ccmsetup
File
Home
Share
View
Network
packt001
c$
Windows
ccmsetup
Search ccmse
Quick access
Desktop
Downloads
Documents
Pictures
Logs
Logs
Screens
System32
This PC
Network
Name
Date modified
Type
cache
6/30/2017 12:18 AM
File folder
Logs
6/30/2017 12:18 AM
File folder
ccmsetup
6/30/2017 12:18 AM
Cabinet File
ccmsetup
4/11/2017 6:50 PM
Application
ccmsetup.exe.download
4/11/2017 6:50 PM
DOWNLOAD File
ccmsetup
4/4/2017 9:37 AM
XML Document
client
4/11/2017 6:50 PM
Windows Installe
configmgr1702-client-kb4019926-x64
4/11/2017 6:50 PM
Windows Installe
MicrosoftPolicyPlatformSetup
3/1/2017 1:11 AM
Windows Installe
SCEPInstall
3/1/2017 1:11 AM
Application
Silverlight
6/1/2017 11:39 PM
Application
vcredist_x64
3/1/2017 1:11 AM
Application
vcredist_x86
3/1/2017 1:11 AM
Application
WindowsFirewallConfigurationProvider
3/1/2017 1:11 AM
Windows Installe

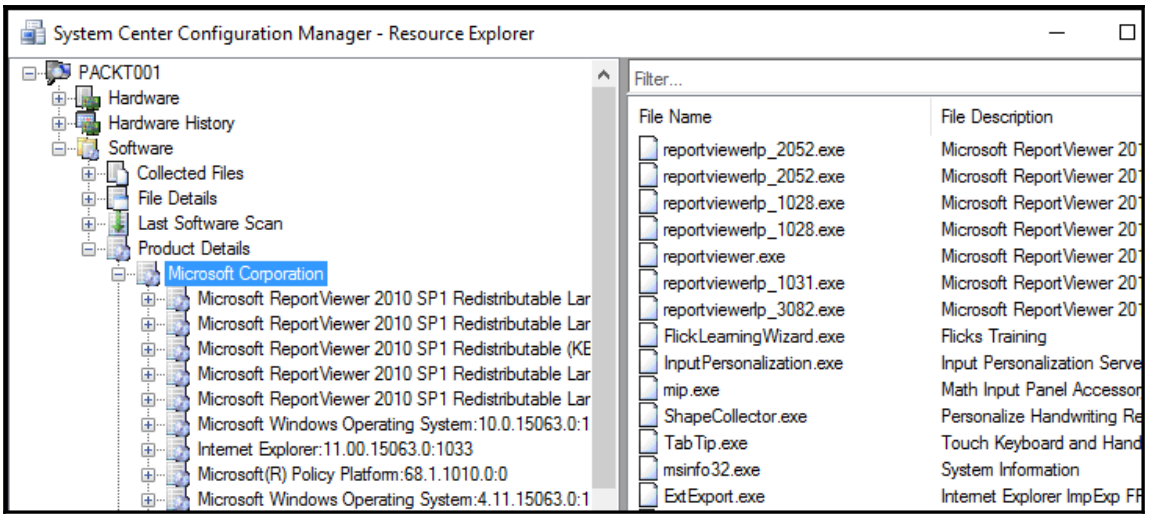

Logs
File
Home
Share
View
« packt001 › c$ › Windows › ccmsetup › Logs
Search Logs
Quick access
Desktop
Downloads
Documents
Pictures
Logs
Name
Date modified
Type
ccmsetup 6/30/2017 12:18 AM LOG File
client.msi 6/30/2017 12:19 AM LOG File
MicrosoftPolicyPlatformSetup.msi 6/30/2017 12:18 AM LOG File
VCRedist_x64_Install 6/30/2017 12:18 AM LOG File
VCRedist_x64_Install_0_vcRuntimeMinimu... 6/30/2017 12:18 AM LOG File
VCRedist_x64_Install_1_vcRuntimeAddition... 6/30/2017 12:18 AM LOG File


All Desktop and Server Clients 2 items
Search
Icon
Name
Client Type
Client
Site Code
Client Activi
CM16 Computer Yes PA1 Active
PACKT001 Computer Yes PA1 Active
PACKT001
General Information
Name: PACKT001
Client Type: Computer
Client Check Result: Passed
Client Activity
Policy Request:
Heartbeat DDR: 6/30/2017 9:23 AM
Hardware Scan: 6/30/
Related Ob
Prima

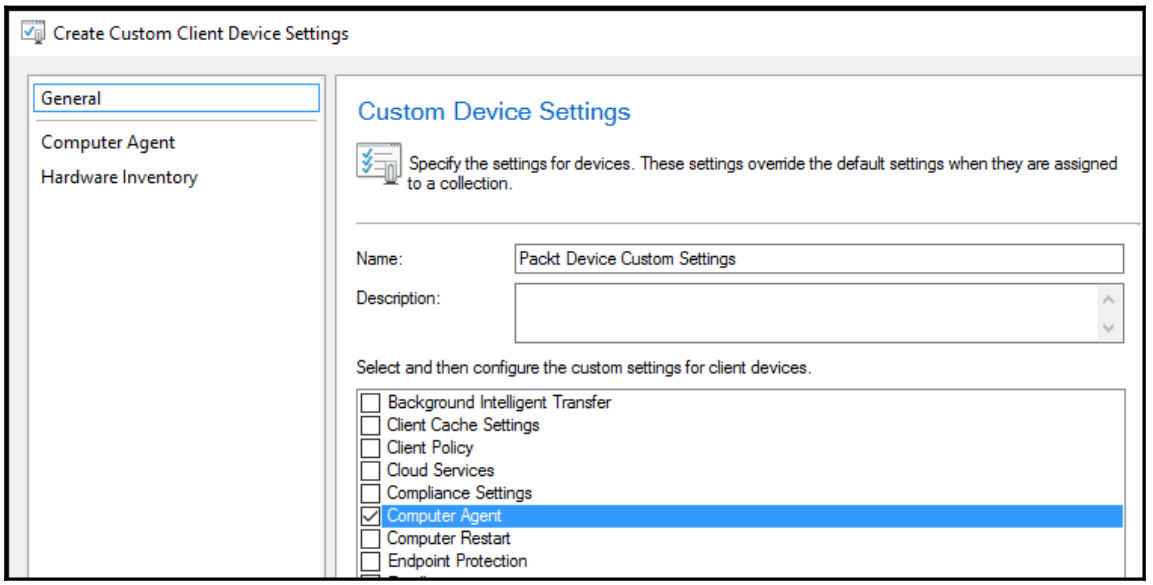

Configuration Manager Trace Log Tool - [\\packt001\c$\Windows\CCM\Logs\ClientLocation.log]
File Tools Window Help
Log Text Component Date/Time Thread
Getting Assigned Site ClientLocation 6/29/2017 3:20:45 PM 6080 (0x17C0)
Client is currently not assigned to any site ClientLocation 6/29/2017 3:20:45 PM 6080 (0x17C0)
Removing client site assignments ClientLocation 6/29/2017 3:20:45 PM 6080 (0x17C0)
Removed pending site assignment to 'PA1' ClientLocation 6/29/2017 3:20:45 PM 6080 (0x17C0)
Raising event:instance of CCM_RemoteClient_Reassigned{DateTime = "201706... ClientLocation 6/29/2017 3:20:46 PM 6080 (0x17C0)
Client is now successfully assigned to site 'PA1' ClientLocation 6/29/2017 3:20:46 PM 6080 (0x17C0)
Discover Default MP ClientLocation 6/29/2017 3:20:46 PM 6080 (0x17C0)
Site Code is PA1; Management Point is http://CM16.doctor.com; MP HTTPS en... ClientLocation 6/29/2017 3:20:46 PM 6080 (0x17C0)
Setting current Management Point as http://CM16.doctor.com ClientLocation 6/29/2017 3:20:46 PM 6080 (0x17C0)
Current AD forest name is doctor.com, domain name is doctor.com ClientLocation 6/29/2017 3:20:46 PM 6080 (0x17C0)
Domain joined client is in Intranet ClientLocation 6/29/2017 3:20:46 PM 6080 (0x17C0)
Rotating assigned management point, new management point [1] is: CM16.do... ClientLocation 6/29/2017 3:20:46 PM 6080 (0x17C0)
Assigned MP changed from <CM16.doctor.com> to <CM16.doctor.com>. ClientLocation 6/29/2017 3:20:46 PM 6080 (0x17C0)
Current AD forest name is doctor.com, domain name is doctor.com ClientLocation 6/29/2017 3:21:47 PM 6032 (0x1790)
Domain joined client is in Intranet ClientLocation 6/29/2017 3:21:47 PM 6032 (0x1790)
Date/Time: 6/29/2017 3:20:46 PM Component: ClientLocation
Thread: 6080 (0x17C0) Source: smsclientclass.cpp:1480
Site Code is PA1; Management Point is http://CM16.doctor.com; MP HTTPS enabled = 0
Elapsed time is 0h 0m 17s 103ms (17.103 seconds)

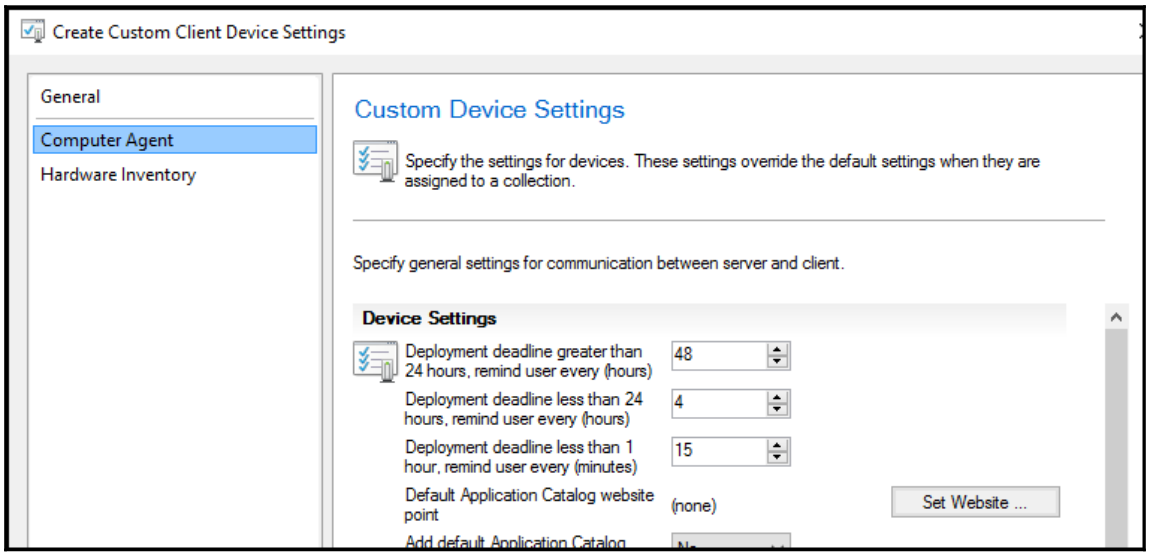

Configuration Manager Trace Log Tool - [\\packt001\c$\Windows\CCM\Logs\LocationServices.log]
File Tools Window Help
Log Text Component Date/Time Thread
Successfully created context from the raw certificate. LocationServices 6/29/2017 3:21:56 PM 5748 (0x1674)
Updating portal information. LocationServices 6/29/2017 3:21:56 PM 5748 (0x1674)
Received reply of type PortalCertificateReply LocationServices 6/29/2017 3:21:56 PM 5668 (0x1624)
The reply from location manager contains 1 certificates LocationServices 6/29/2017 3:21:56 PM 5668 (0x1624)
Updating portal certificates LocationServices 6/29/2017 3:21:56 PM 5668 (0x1624)
Successfully created context from the raw certificate. LocationServices 6/29/2017 3:21:56 PM 5668 (0x1624)
Retrieved management point encryption info from AD. LocationServices 6/29/2017 3:23:01 PM 6048 (0x17A0)
Raising event:instance of CCM_CcmHttp_Status{ClientID = "GUID:07C3215A-D... LocationServices 6/29/2017 3:23:01 PM 6048 (0x17A0)
Executing Task LSTimeOutRequestsTask LocationServices 6/29/2017 3:23:01 PM 5652 (0x1614)
Executing Task LSRefreshLocationsTask LocationServices 6/29/2017 3:23:01 PM 3880 (0xF28)
The MP name retrieved is 'CM16.doctor.com' with version '8498' and capabiliti... LocationServices 6/29/2017 3:23:44 PM 1972 (0x7B4)
MP 'CM16.doctor.com' is compatible LocationServices 6/29/2017 3:23:44 PM 1972 (0x7B4)
Persisted AAD on-boarding info. LocationServices 6/29/2017 3:23:44 PM 1972 (0x7B4)
Refreshed security settings over AD LocationServices 6/29/2017 3:23:44 PM 1972 (0x7B4)
No security settings update detected. LocationServices 6/29/2017 3:23:44 PM 1972 (0x7B4)
Date/Time: 6/29/2017 3:23:44 PM Component: LocationServices
Thread: 1972 (0x7B4) Source: lsadcache.cpp:339
MP 'CM16.doctor.com' is compatible
Elapsed time is 0h 3m 13s 663ms (193.663 seconds)

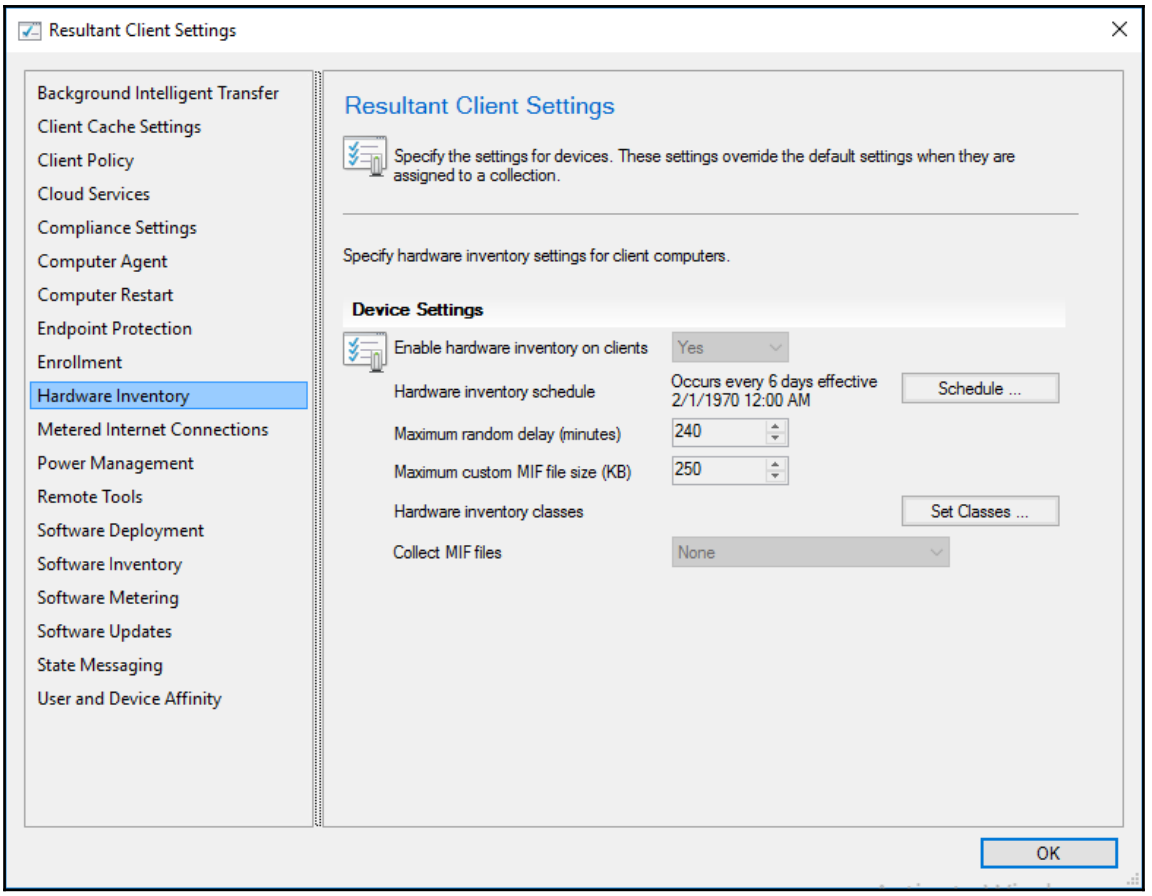

System Center Configuration Manager - Resource Explorer
PACKT001
Hardware
AutoStart Software
CDROM Drive
Client Events
Computer System
Configuration Manager Client SSL Configurations
Configuration Manager Client State
Desktop Monitor
Disk Drives
Disk Partitions
Firmware
Folder Redirection Health
Installed Applications
Installed Applications (64)
Filter...
Display Name
Product ID
Microsoft Visual C++ 2013 x86 Minimum Runtime - 12.0.21005
Microsoft Visual C++ 2013 Redistributable (x64) - 12.0.21005
Microsoft Silverlight
Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.21005
Microsoft Visual C++ 2013 x86 Additional Runtime - 12.0.21005

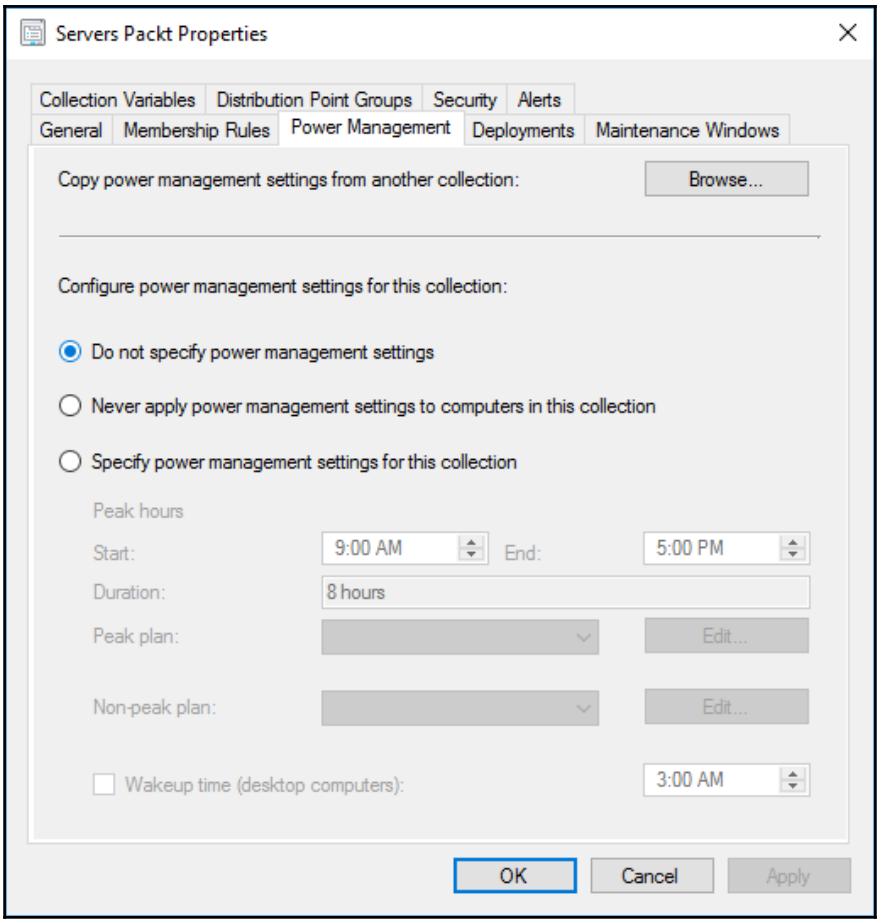

System Center Configuration Manager - Resource Explorer
PACKT001
Hardware
Hardware History
Software
Collected Files
File Details
Last Software Scan
Product Details
Microsoft Corporation
Microsoft ReportViewer 2010 SP1 Redistributable Lar
Microsoft ReportViewer 2010 SP1 Redistributable Lar
Microsoft ReportViewer 2010 SP1 Redistributable (KE
Microsoft ReportViewer 2010 SP1 Redistributable Lar
Microsoft ReportViewer 2010 SP1 Redistributable Lar
Microsoft Windows Operating System:10.0.15063.0:1
Internet Explorer:11.00.15063.0:1033
Microsoft(R) Policy Platform:68.1.1010.0:0
Microsoft Windows Operating System:4.11.15063.0:1
Filter...
File Name
File Description
reportviewerlp_2052.exe
reportviewerlp_2052.exe
reportviewerlp_1028.exe
reportviewerlp_1028.exe
reportviewer.exe
reportviewerlp_1031.exe
reportviewerlp_3082.exe
FlickLearningWizard.exe
InputPersonalization.exe
mip.exe
ShapeCollector.exe
TabTip.exe
msinfo32.exe
ExtExport.exe
Microsoft ReportViewer 20
Microsoft ReportViewer 20
Microsoft ReportViewer 20
Microsoft ReportViewer 20
Microsoft ReportViewer 20
Microsoft ReportViewer 20
Microsoft ReportViewer 20
Flicks Training
Input Personalization Serve
Math Input Panel Accessor
Personalize Handwriting Re
Touch Keyboard and Hand
System Information
Internet Explorer ImpExp FF

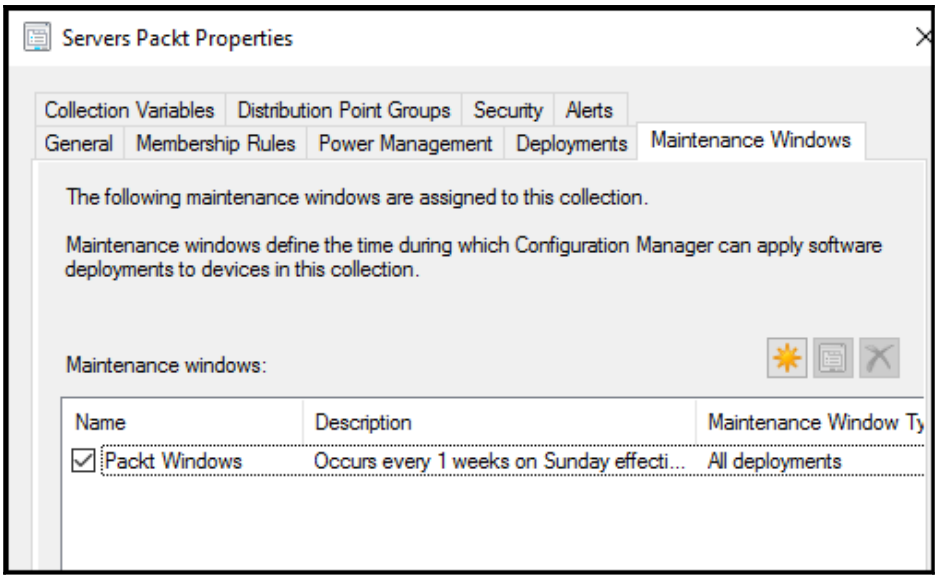
# Chapter 5: Creating Client Settings for Servers and Workstations

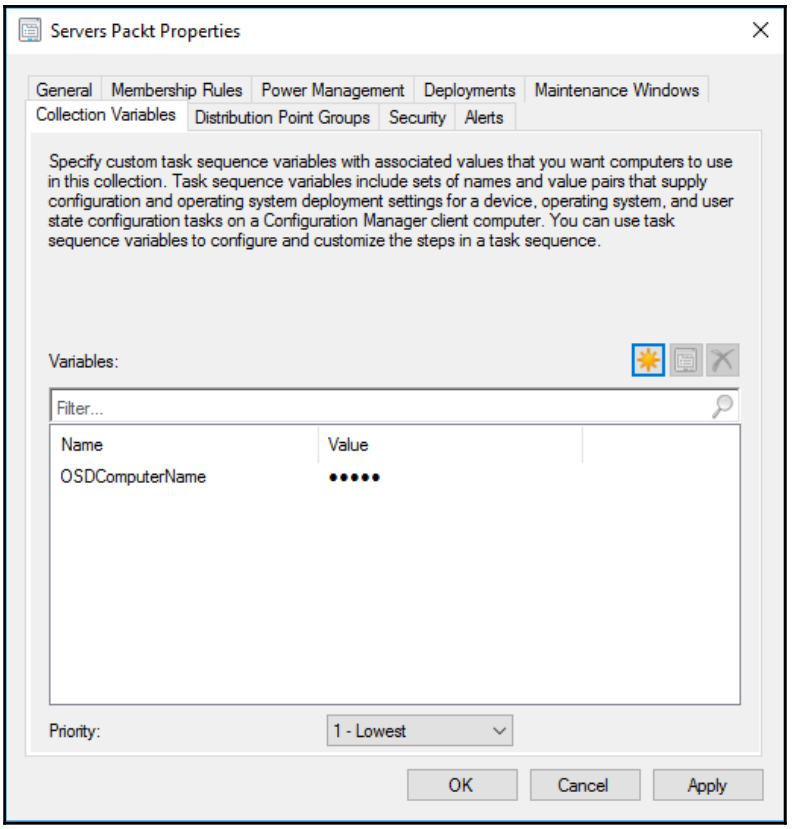


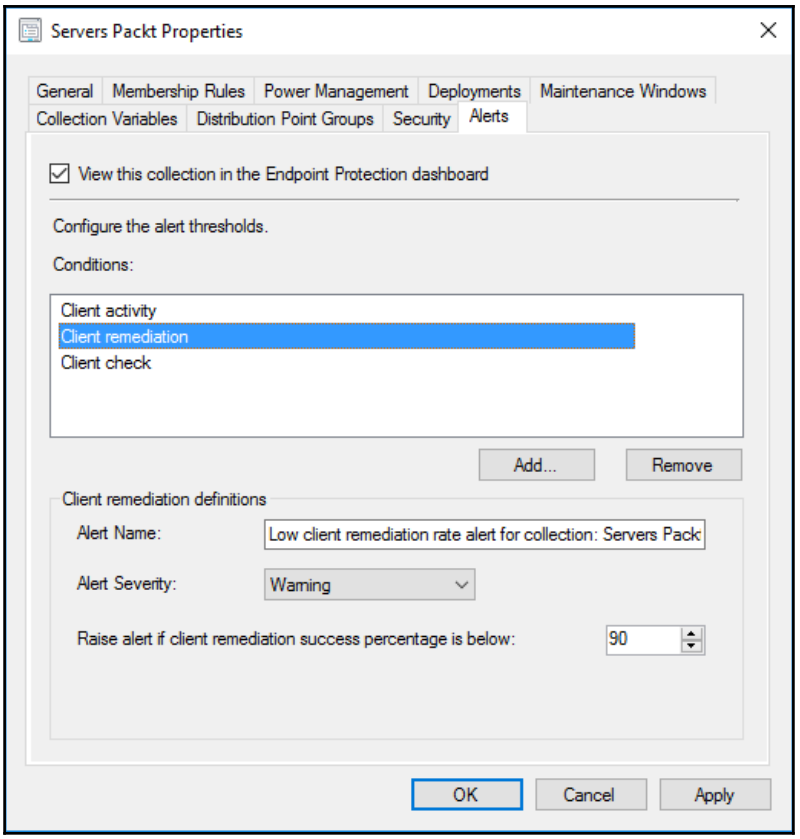




Resultant Client Settings
Background Intelligent Transfer
Client Cache Settings
Client Policy
Cloud Services
Compliance Settings
Computer Agent
Computer Restart
Endpoint Protection
Enrollment
Hardware Inventory
Metered Internet Connections
Power Management
Remote Tools
Software Deployment
Software Inventory
Software Metering
Software Updates
State Messaging
User and Device Affinity
Resultant Client Settings
Specify the settings for devices. These settings override the default settings when they are assigned to a collection.
Specify hardware inventory settings for client computers.
Device Settings
Enable hardware inventory on clients
Yes
Hardware inventory schedule
Occurs every 6 days effective 2/1/1970 12:00 AM
Schedule ...
Maximum random delay (minutes)
240
Maximum custom MIF file size (KB)
250
Hardware inventory classes
Set Classes ...
Collect MIF files
None
OK

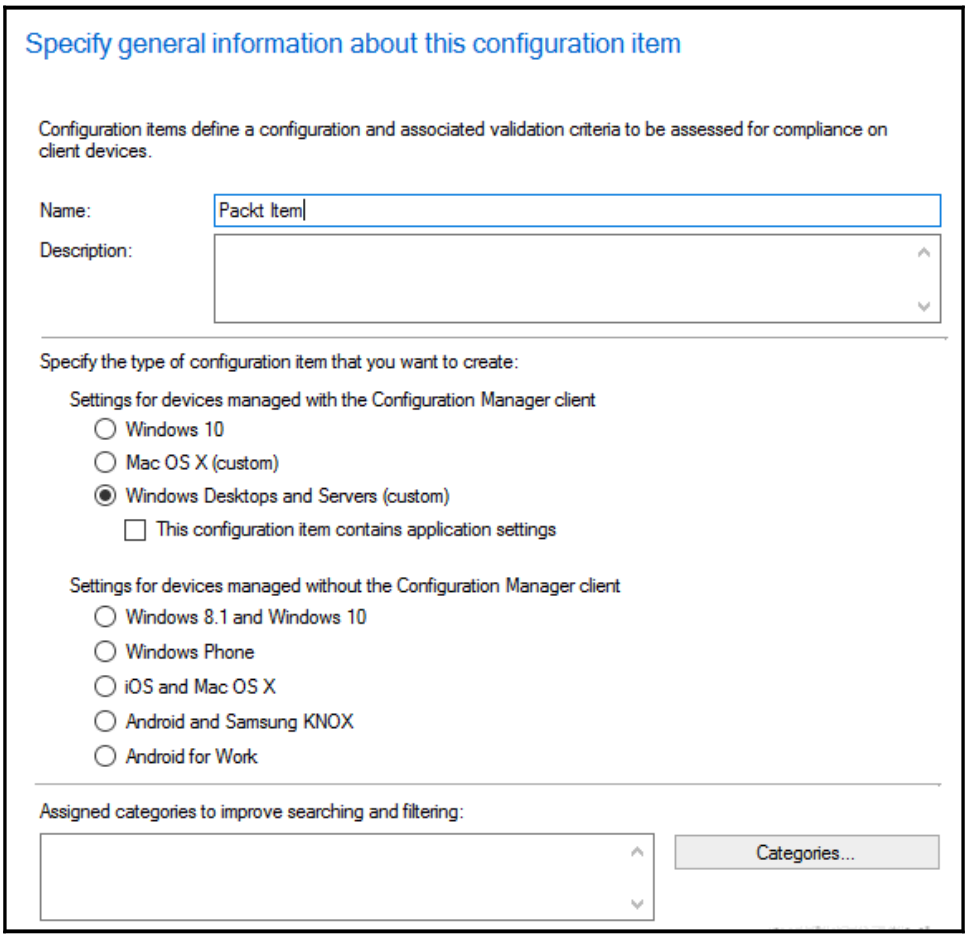

Servers Packt Properties
Collection Variables
Distribution Point Groups
Security
Alerts
General
Membership Rules
Power Management
Deployments
Maintenance Windows
Copy power management settings from another collection:
Browse...
Configure power management settings for this collection:
Do not specify power management settings
Never apply power management settings to computers in this collection
Specify power management settings for this collection
Peak hours
Start:
9:00 AM
End:
5:00 PM
Duration:
8 hours
Peak plan:
Edit...
Non-peak plan:
Edit...
Wakeup time (desktop computers):
3:00 AM
OK
Cancel
Apply

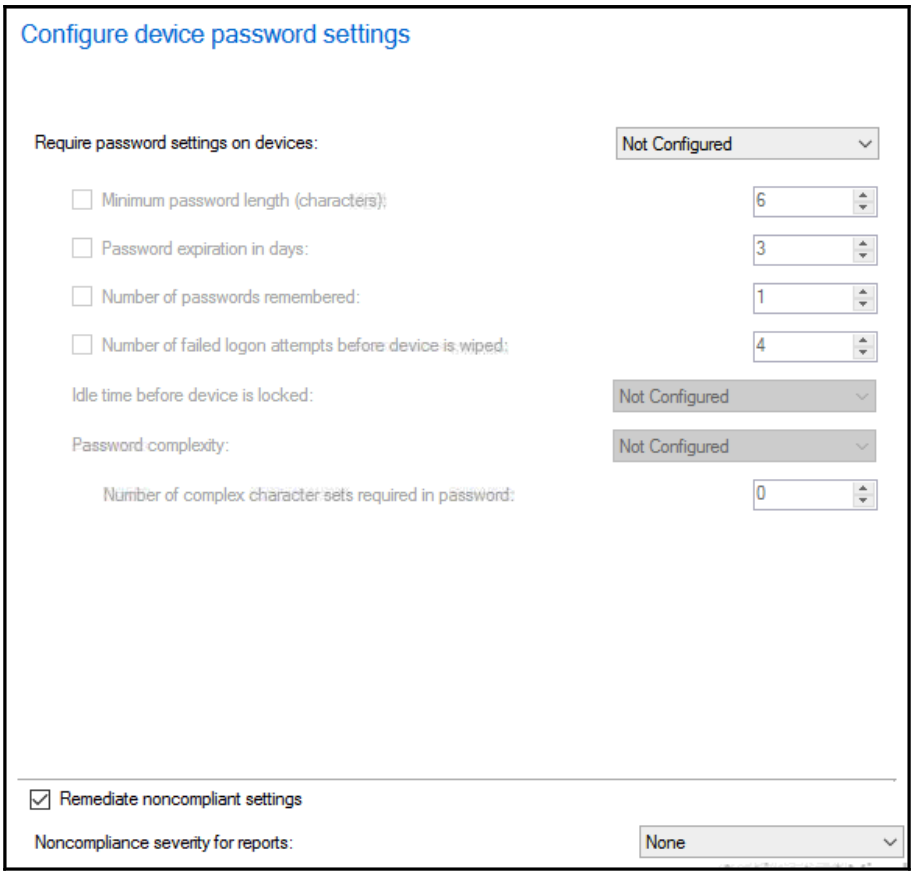

Servers Packt Properties
Collection Variables
Distribution Point Groups
Security
Alerts
General
Membership Rules
Power Management
Deployments
Maintenance Windows
The following maintenance windows are assigned to this collection.
Maintenance windows define the time during which Configuration Manager can apply software deployments to devices in this collection.
Maintenance windows:
Name
Description
Maintenance Window Ty
Packt Windows
Occurs every 1 weeks on Sunday effecti...
All deployments

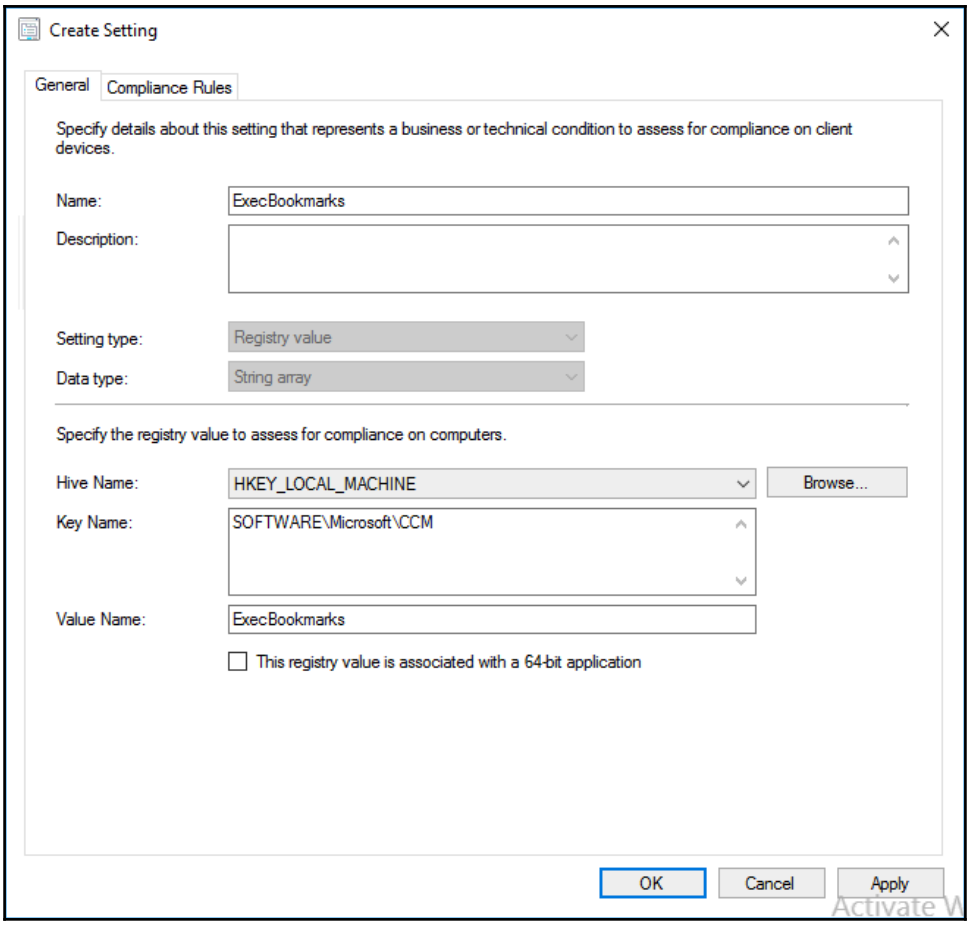

Servers Packt Properties
General
Membership Rules
Power Management
Deployments
Maintenance Windows
Collection Variables
Distribution Point Groups
Security
Alerts
Specify custom task sequence variables with associated values that you want computers to use in this collection. Task sequence variables include sets of names and value pairs that supply configuration and operating system deployment settings for a device, operating system, and user state configuration tasks on a Configuration Manager client computer. You can use task sequence variables to configure and customize the steps in a task sequence.
Variables:
Filter...
Name
Value
OSDComputerName
●●●●●
Priority:
1 - Lowest
OK
Cancel
Apply

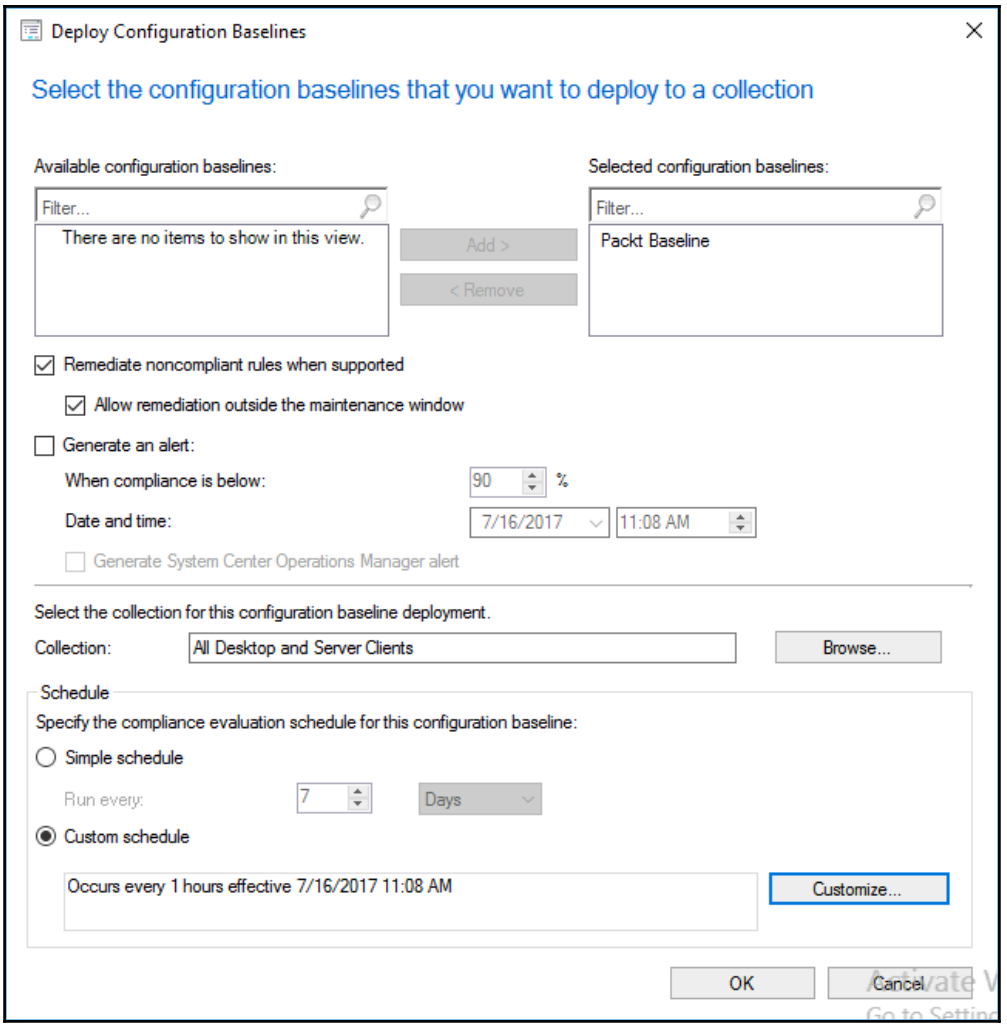

Servers Packt Properties
General
Membership Rules
Power Management
Deployments
Maintenance Windows
Collection Variables
Distribution Point Groups
Security
Alerts
View this collection in the Endpoint Protection dashboard
Configure the alert thresholds.
Conditions:
Client activity
Client remediation
Client check
Add...
Remove
Client remediation definitions
Alert Name:
Low client remediation rate alert for collection: Servers Pack
Alert Severity:
Warning
Raise alert if client remediation success percentage is below:
90
OK
Cancel
Apply

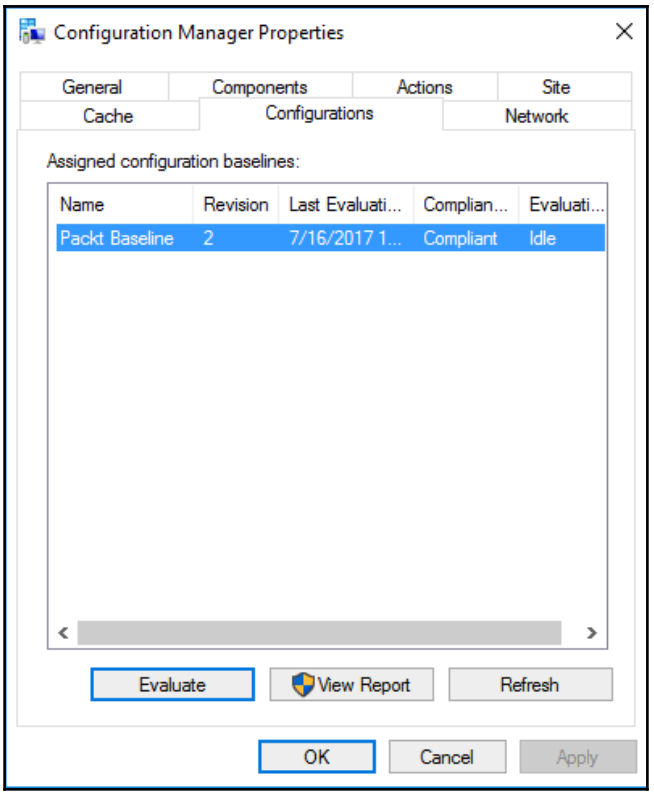
# Chapter 6: Compliance Settings

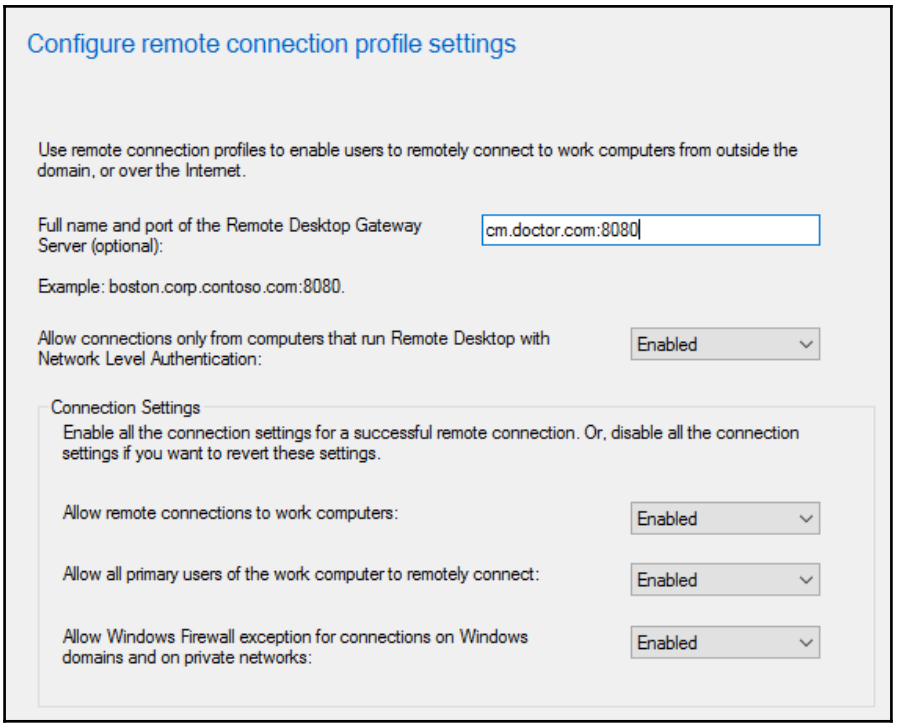


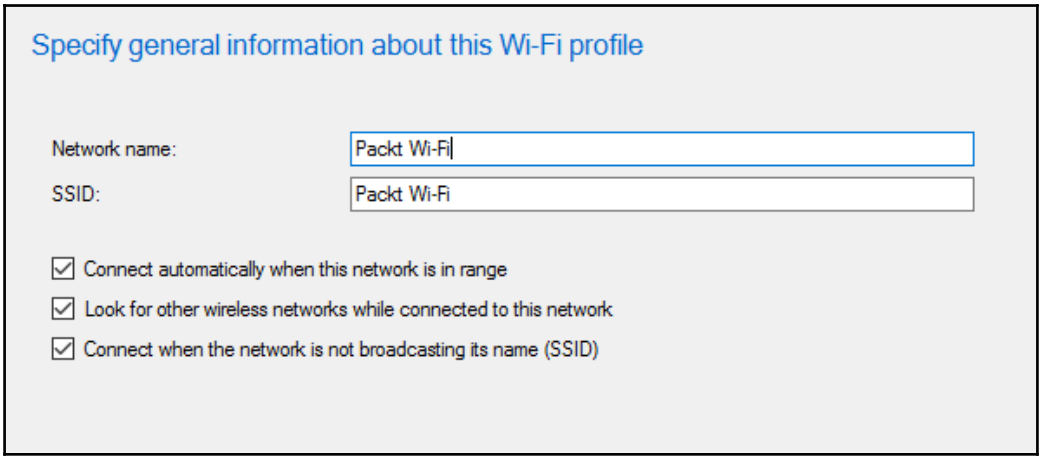

Configure device password settings
Require password settings on devices:
Not Configured
Minimum password length (characters):
6
Password expiration in days:
3
Number of passwords remembered:
1
Number of failed logon attempts before device is wiped:
4
Idle time before device is locked:
Not Configured
Password complexity:
Not Configured
Number of complex character sets required in password:
0
Remediate noncompliant settings
Noncompliance severity for reports:
None

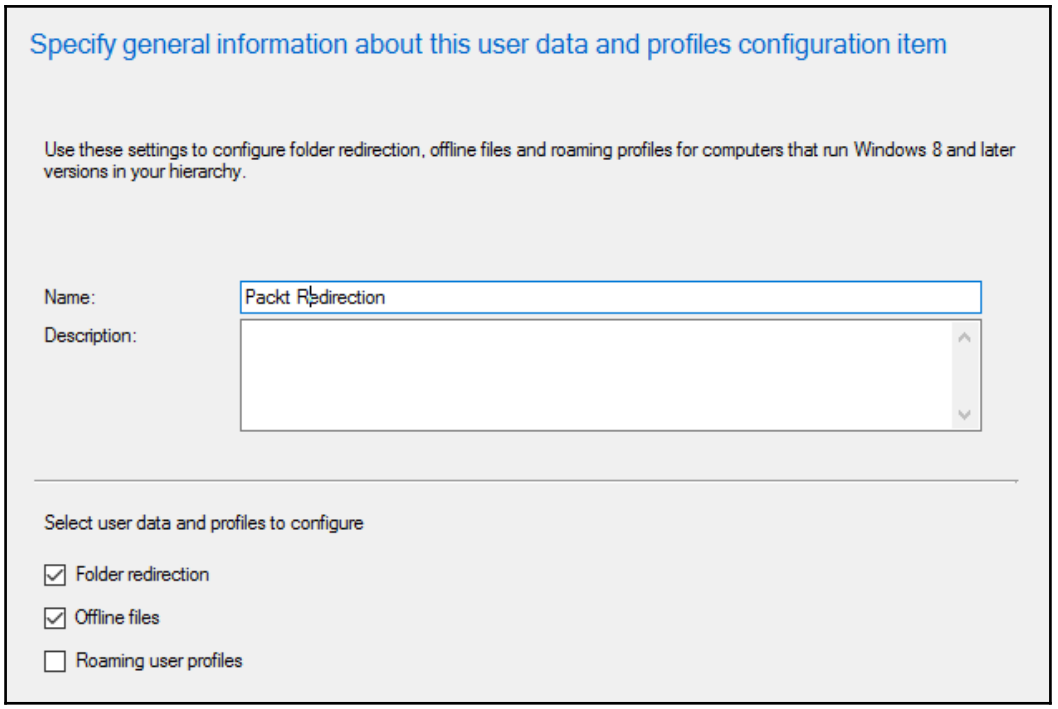

Create Setting
General
Compliance Rules
Specify details about this setting that represents a business or technical condition to assess for compliance on client devices.
Name:
ExecBookmarks
Description:
Setting type:
Registry value
Data type:
String array
Specify the registry value to assess for compliance on computers.
Hive Name:
HKEY_LOCAL_MACHINE
Browse...
Key Name:
SOFTWARE\Microsoft\CCM
Value Name:
ExecBookmarks
This registry value is associated with a 64-bit application
OK
Cancel
Apply


Deploy Configuration Baselines
Select the configuration baselines that you want to deploy to a collection
Available configuration baselines:
Filter...
There are no items to show in this view.
Add >
< Remove
Selected configuration baselines:
Filter...
Packt Baseline
Remediate noncompliant rules when supported
Allow remediation outside the maintenance window
Generate an alert:
When compliance is below:
90
%
Date and time:
7/16/2017
11:08 AM
Generate System Center Operations Manager alert
Select the collection for this configuration baseline deployment.
Collection:
All Desktop and Server Clients
Browse...
Schedule
Specify the compliance evaluation schedule for this configuration baseline:
Simple schedule
Run every:
7
Days
Custom schedule
Occurs every 1 hours effective 7/16/2017 11:08 AM
Customize...
OK
Cancel

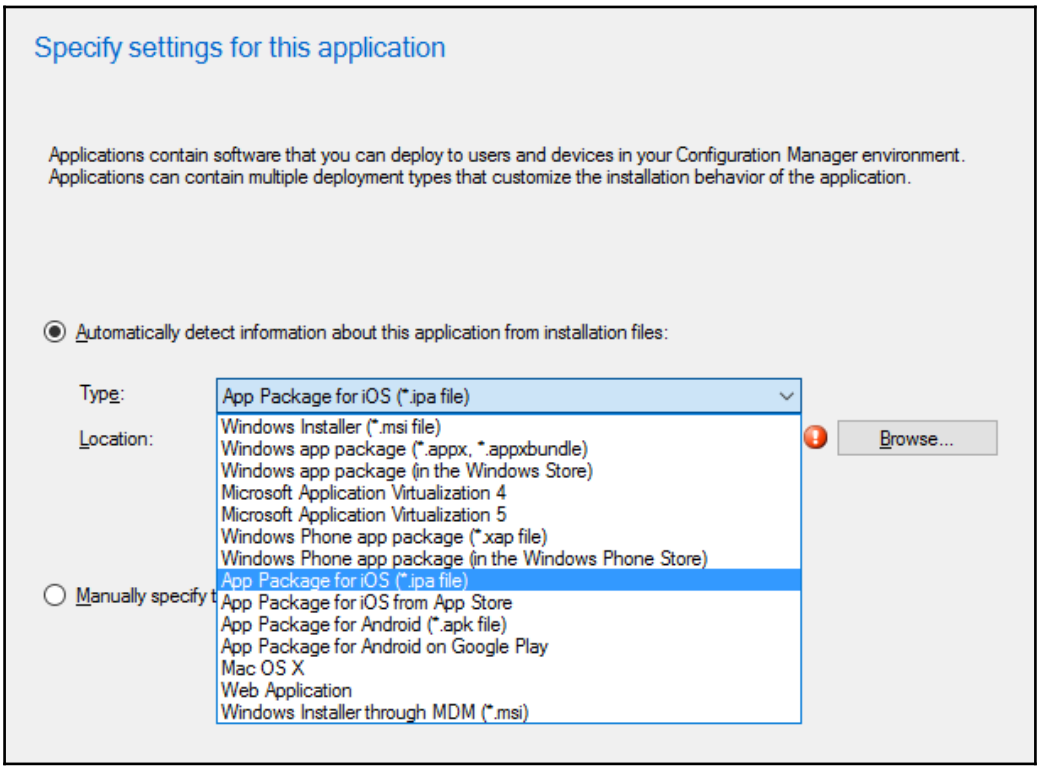

Configuration Manager Properties
General
Components
Actions
Site
Cache
Configurations
Network
Assigned configuration baselines:
Name
Revision
Last Evaluati...
Complian...
Evaluati...
Packt Baseline
2
7/16/2017 1...
Compliant
Idle
Evaluate
View Report
Refresh
OK
Cancel
Apply

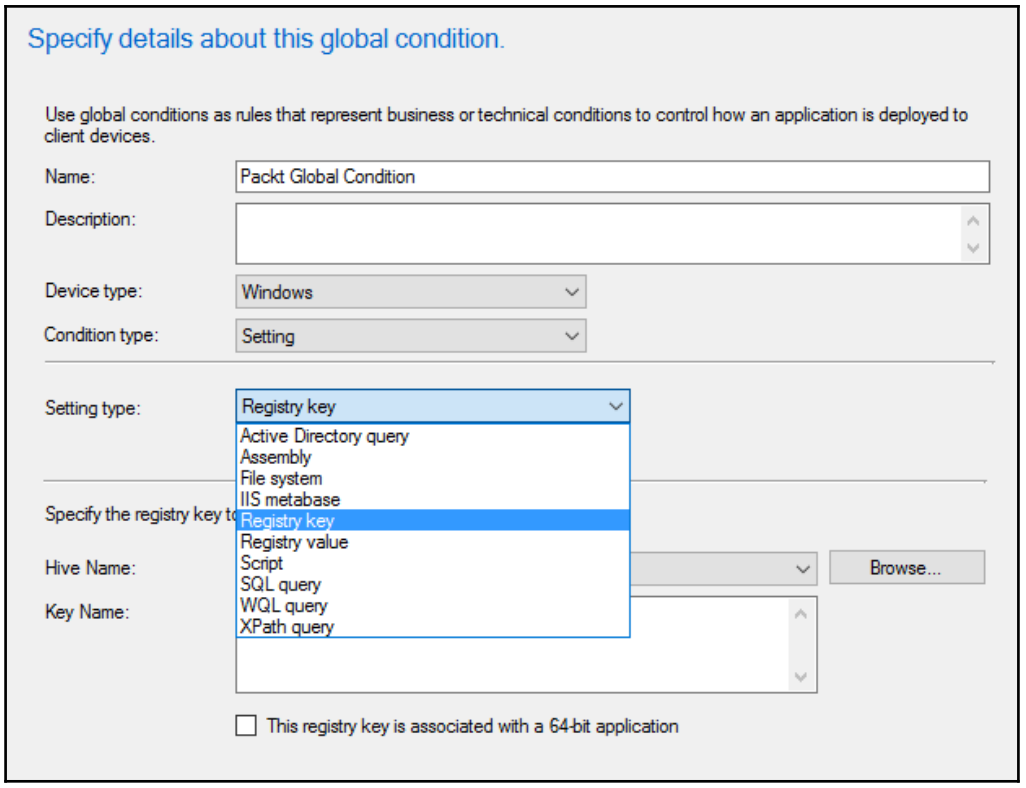

Configure remote connection profile settings
Use remote connection profiles to enable users to remotely connect to work computers from outside the domain, or over the Internet.
Full name and port of the Remote Desktop Gateway Server (optional):
cm.doctor.com:8080
Example: boston.corp.contoso.com:8080.
Allow connections only from computers that run Remote Desktop with Network Level Authentication:
Enabled
Connection Settings
Enable all the connection settings for a successful remote connection. Or, disable all the connection settings if you want to revert these settings.
Allow remote connections to work computers:
Enabled
Allow all primary users of the work computer to remotely connect:
Enabled
Allow Windows Firewall exception for connections on Windows domains and on private networks:
Enabled

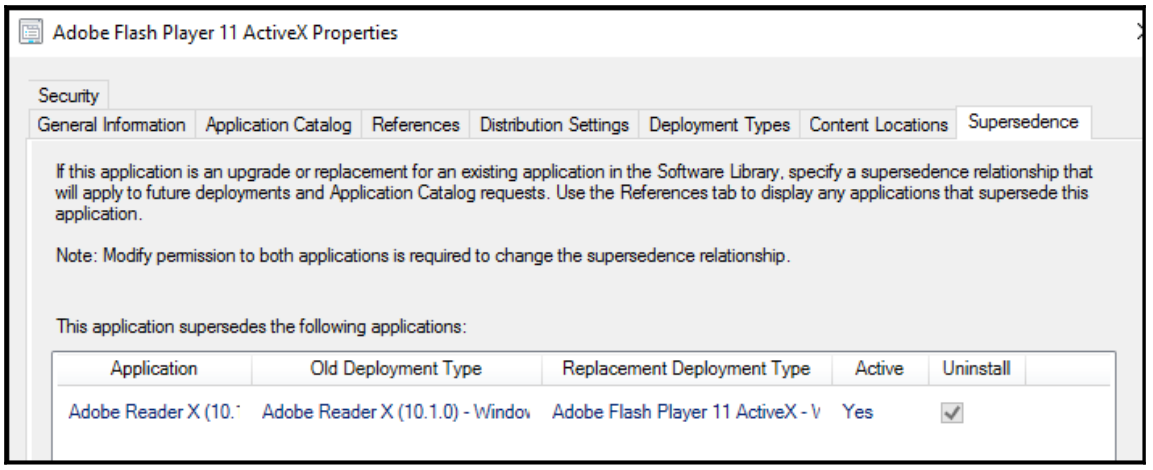

Specify general information about this Wi-Fi profile
Network name:
Packt Wi-Fi
SSID:
Packt Wi-Fi
Connect automatically when this network is in range
Look for other wireless networks while connected to this network
Connect when the network is not broadcasting its name (SSID)

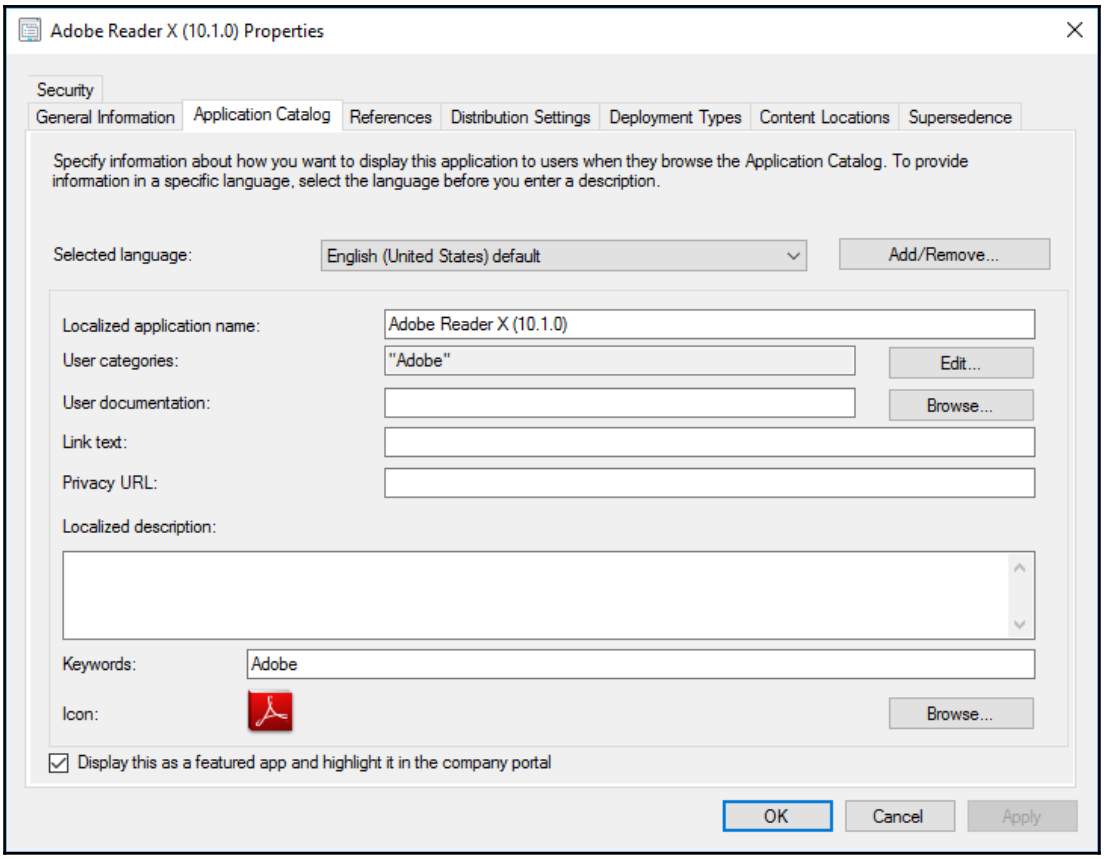

Specify general information about this user data and profiles configuration item
Use these settings to configure folder redirection, offline files and roaming profiles for computers that run Windows 8 and later versions in your hierarchy.
Name:
Packt Redirection
Description:
Select user data and profiles to configure
Folder redirection
Offline files
Roaming user profiles

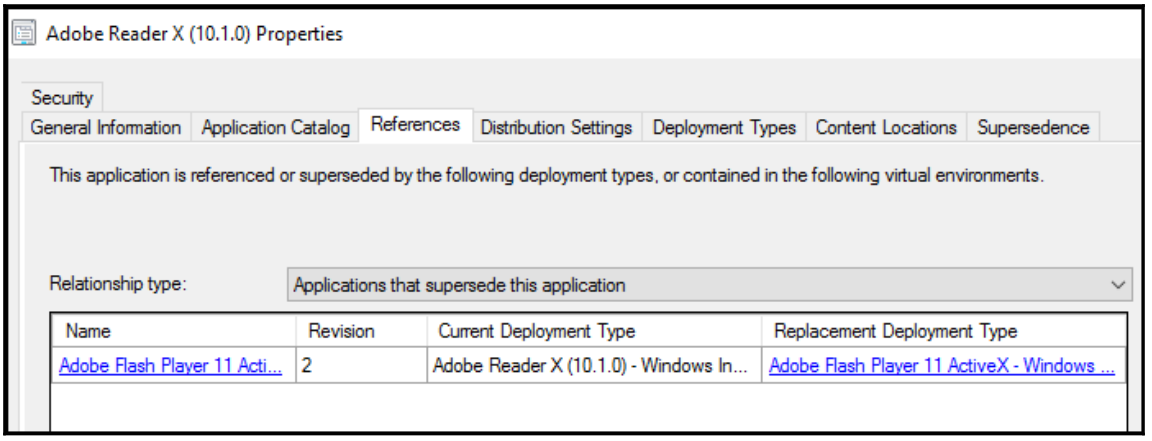
# Chapter 7: Software Distributions

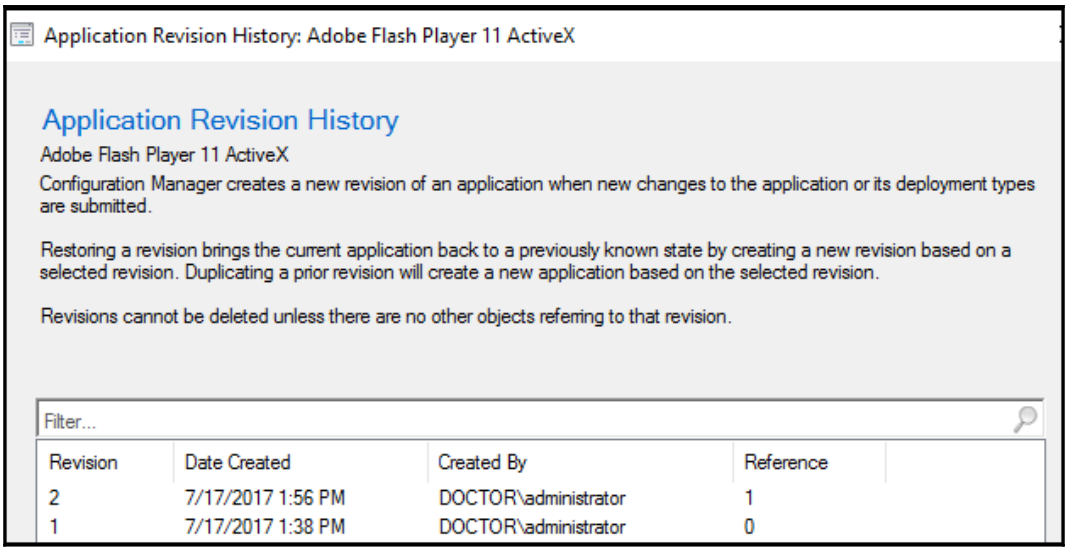


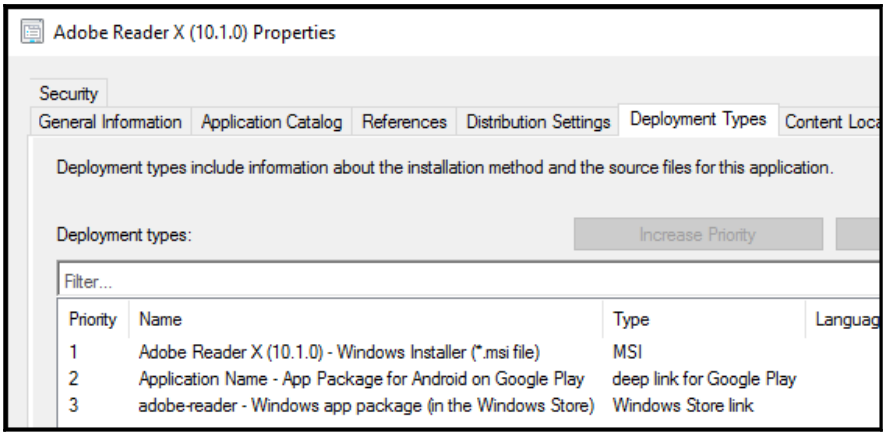

Specify details about this global condition.
Use global conditions as rules that represent business or technical conditions to control how an application is deployed to client devices.
Name:
Packt Global Condition
Description:
Device type:
Windows
Condition type:
Setting
Setting type:
Registry key
Active Directory query
Assembly
File system
IIS metabase
Registry key
Registry value
Script
SQL query
WQL query
XPath query
Specify the registry key to
Hive Name:
Browse...
Key Name:
This registry key is associated with a 64-bit application

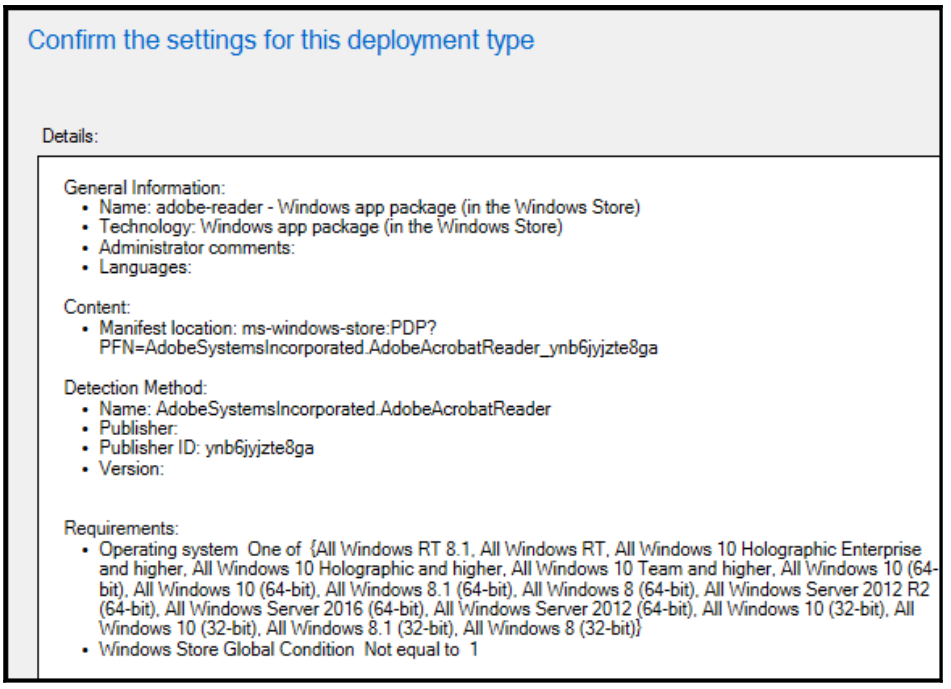

Adobe Flash Player 11 ActiveX Properties
Security
General Information
Application Catalog
References
Distribution Settings
Deployment Types
Content Locations
Supersedence
If this application is an upgrade or replacement for an existing application in the Software Library, specify a supersedence relationship that will apply to future deployments and Application Catalog requests. Use the References tab to display any applications that supersede this application.
Note: Modify permission to both applications is required to change the supersedence relationship.
This application supersedes the following applications:
Application
Old Deployment Type
Replacement Deployment Type
Active
Uninstall
Adobe Reader X (10.
Adobe Reader X (10.1.0) - Windov
Adobe Flash Player 11 ActiveX - V
Yes

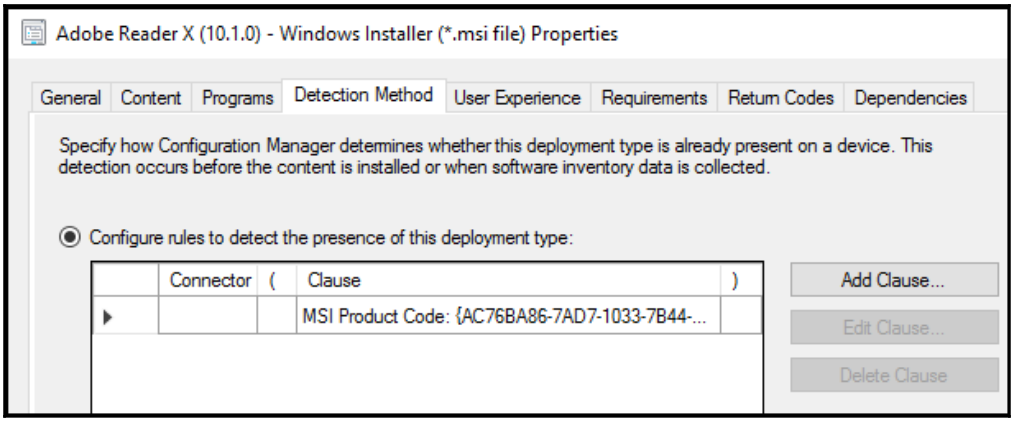

Adobe Reader X (10.1.0) Properties
Security
General Information
Application Catalog
References
Distribution Settings
Deployment Types
Content Locations
Supersedence
Specify information about how you want to display this application to users when they browse the Application Catalog. To provide information in a specific language, select the language before you enter a description.
Selected language:
English (United States) default
Add/Remove...
Localized application name:
Adobe Reader X (10.1.0)
User categories:
"Adobe"
Edit...
User documentation:
Browse...
Link text:
Privacy URL:
Localized description:
Keywords:
Adobe
Icon:
Browse...
Display this as a featured app and highlight it in the company portal
OK
Cancel
Apply

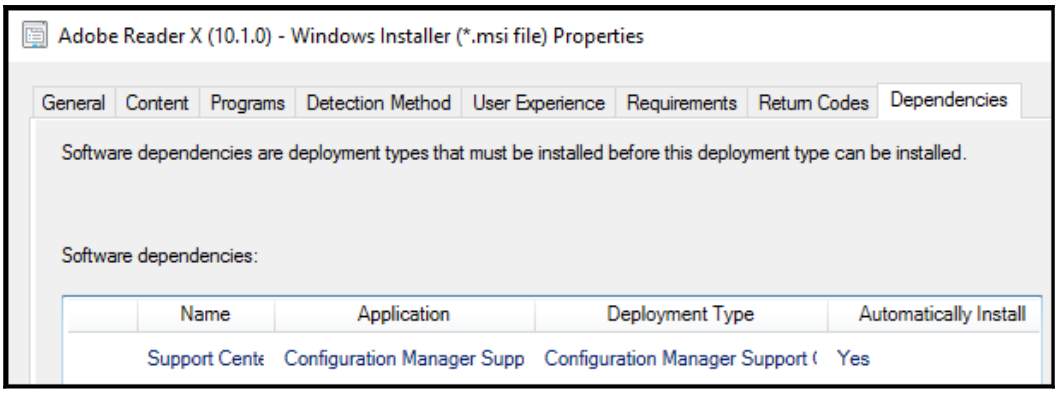

Adobe Reader X (10.1.0) Properties
Security
General Information
Application Catalog
References
Distribution Settings
Deployment Types
Content Locations
Supersedence
This application is referenced or superseded by the following deployment types, or contained in the following virtual environments.
Relationship type:
Applications that supersede this application
Name
Revision
Current Deployment Type
Replacement Deployment Type
Adobe Flash Player 11 Acti...
2
Adobe Reader X (10.1.0) - Windows In...
Adobe Flash Player 11 ActiveX - Windows ...

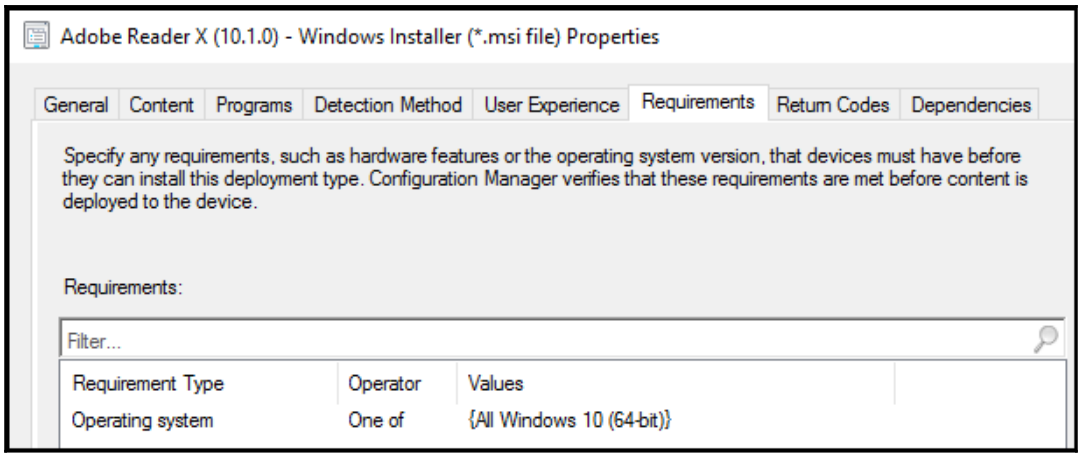

Application Revision History: Adobe Flash Player 11 ActiveX
Application Revision History
Adobe Flash Player 11 ActiveX
Configuration Manager creates a new revision of an application when new changes to the application or its deployment types are submitted.
Restoring a revision brings the current application back to a previously known state by creating a new revision based on a selected revision. Duplicating a prior revision will create a new application based on the selected revision.
Revisions cannot be deleted unless there are no other objects referring to that revision.
Filter...
Revision
Date Created
Created By
Reference
2
7/17/2017 1:56 PM
DOCTOR\administrator
1
1
7/17/2017 1:38 PM
DOCTOR\administrator
0

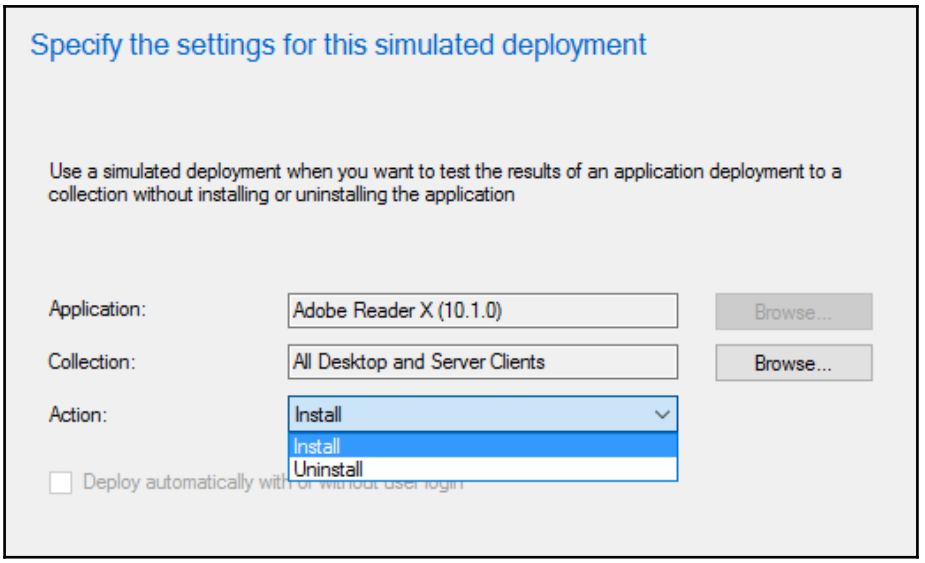

Adobe Reader X (10.1.0) Properties
Security
General Information
Application Catalog
References
Distribution Settings
Deployment Types
Content Loca
Deployment types include information about the installation method and the source files for this application.
Deployment types:
Increase Priority
Filter...
Priority
Name
Type
Languag
1
Adobe Reader X (10.1.0) - Windows Installer (*.msi file)
MSI
2
Application Name - App Package for Android on Google Play
deep link for Google Play
3
adobe-reader - Windows app package (in the Windows Store)
Windows Store link

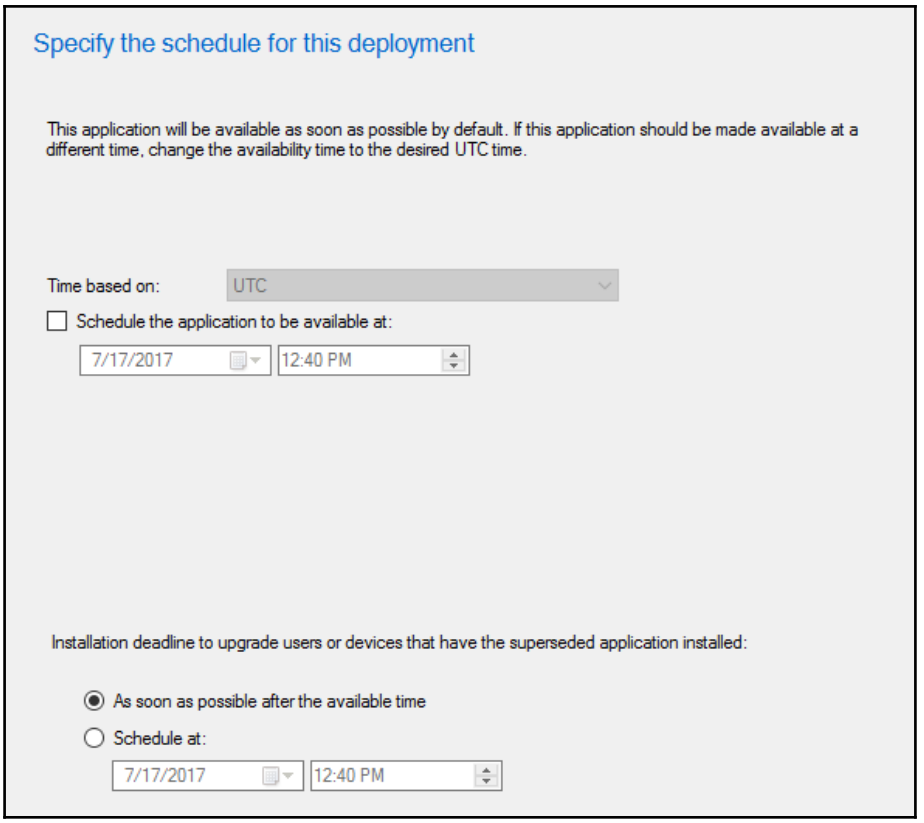

Confirm the settings for this deployment type
Details:
General Information:
• Name: adobe-reader - Windows app package (in the Windows Store)
• Technology: Windows app package (in the Windows Store)
• Administrator comments:
• Languages:
Content:
• Manifest location: ms-windows-store:PDP?
PFN=AdobeSystemsIncorporated.AdobeAcrobatReader_ynb6jyjzte8ga
Detection Method:
• Name: AdobeSystemsIncorporated.AdobeAcrobatReader
• Publisher:
• Publisher ID: ynb6jyjzte8ga
• Version:
Requirements:
• Operating system One of {All Windows RT 8.1, All Windows RT, All Windows 10 Holographic Enterprise and higher, All Windows 10 Holographic and higher, All Windows 10 Team and higher, All Windows 10 (64-bit), All Windows 10 (64-bit), All Windows 8.1 (64-bit), All Windows 8 (64-bit), All Windows Server 2012 R2 (64-bit), All Windows Server 2016 (64-bit), All Windows Server 2012 (64-bit), All Windows 10 (32-bit), All Windows 10 (32-bit), All Windows 8.1 (32-bit), All Windows 8 (32-bit)}
• Windows Store Global Condition Not equal to 1

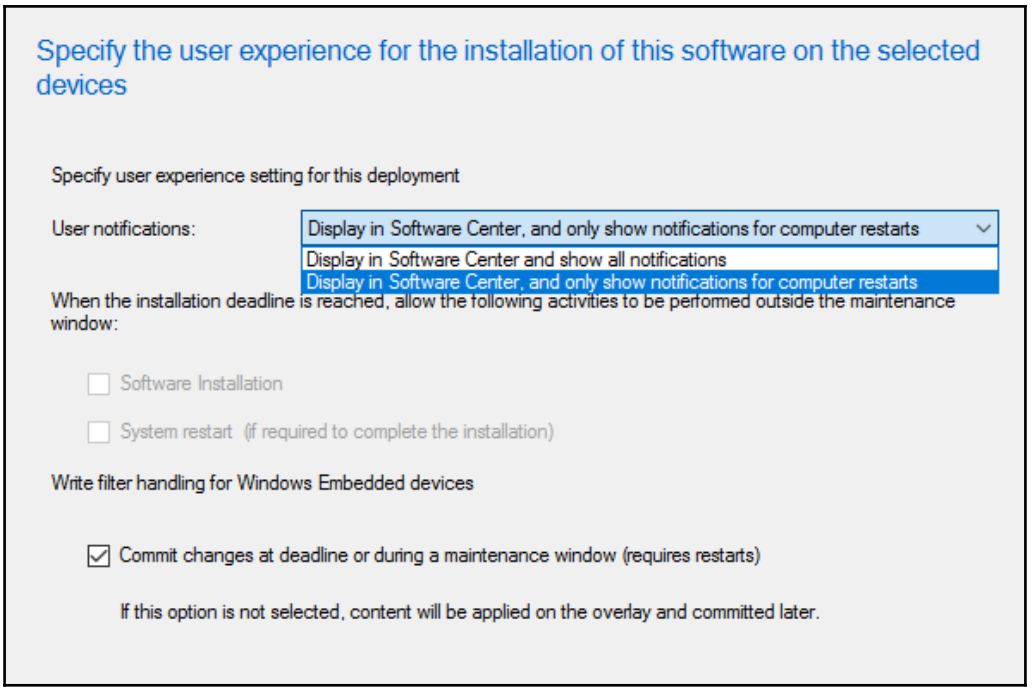

Adobe Reader X (10.1.0) - Windows Installer (*.msi file) Properties
General
Content
Programs
Detection Method
User Experience
Requirements
Return Codes
Dependencies
Specify how Configuration Manager determines whether this deployment type is already present on a device. This detection occurs before the content is installed or when software inventory data is collected.
Configure rules to detect the presence of this deployment type:
Connector
(
Clause
)
MSI Product Code: {AC76BA86-7AD7-1033-7B44-...
Add Clause...
Edit Clause...
Delete Clause

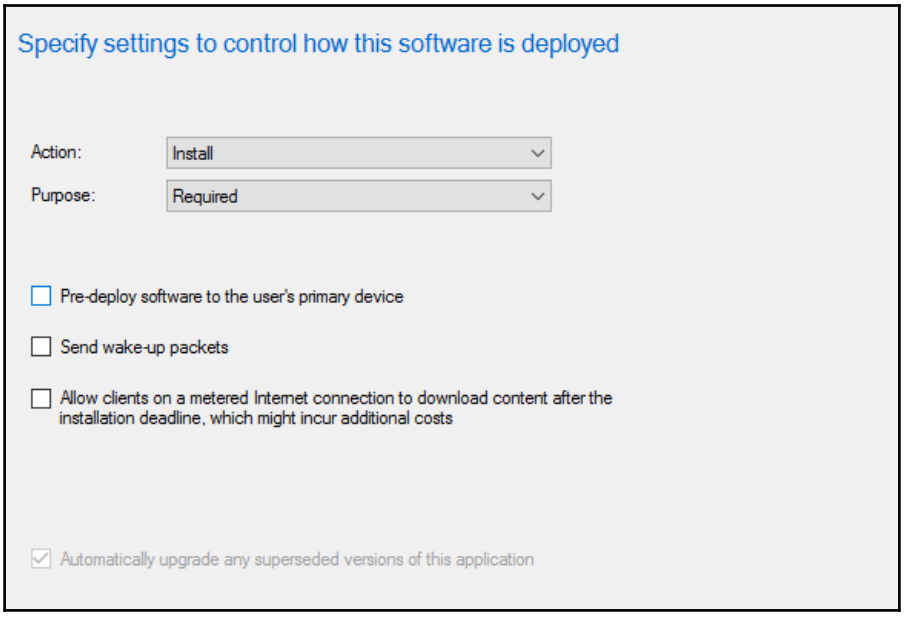

Adobe Reader X (10.1.0) - Windows Installer (*.msi file) Properties
General
Content
Programs
Detection Method
User Experience
Requirements
Return Codes
Dependencies
Software dependencies are deployment types that must be installed before this deployment type can be installed.
Software dependencies:
Name
Application
Deployment Type
Automatically Install
Support Cente
Configuration Manager Supp
Configuration Manager Support (
Yes

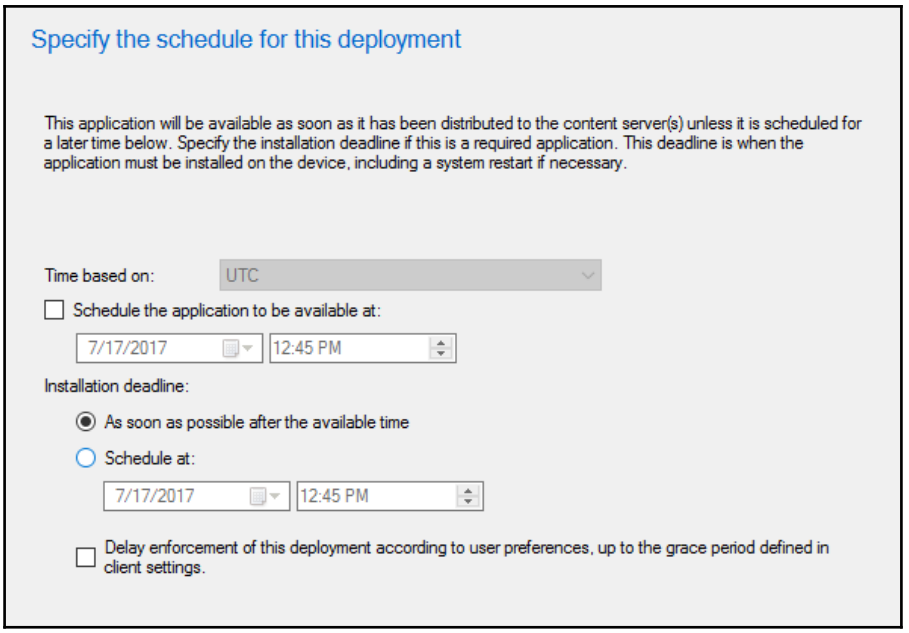

Adobe Reader X (10.1.0) - Windows Installer (*.msi file) Properties
General
Content
Programs
Detection Method
User Experience
Requirements
Return Codes
Dependencies
Specify any requirements, such as hardware features or the operating system version, that devices must have before they can install this deployment type. Configuration Manager verifies that these requirements are met before content is deployed to the device.
Requirements:
Filter...
Requirement Type
Operator
Values
Operating system
One of
{All Windows 10 (64-bit)}

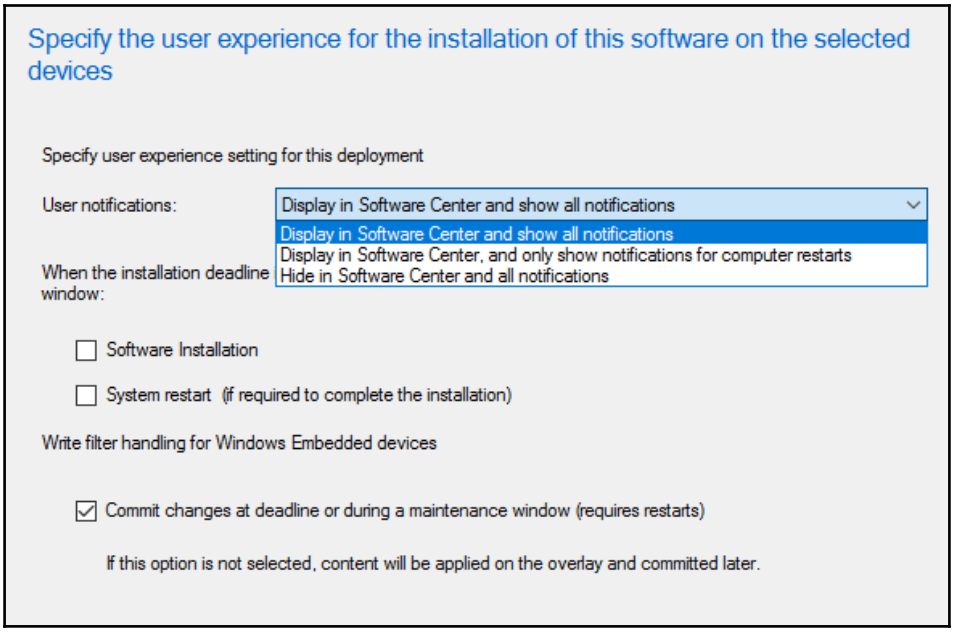

Specify the settings for this simulated deployment
Use a simulated deployment when you want to test the results of an application deployment to a collection without installing or uninstalling the application
Application:
Adobe Reader X (10.1.0)
Browse...
Collection:
All Desktop and Server Clients
Browse...
Action:
Install
Install
Uninstall
Deploy automatically with or without user login

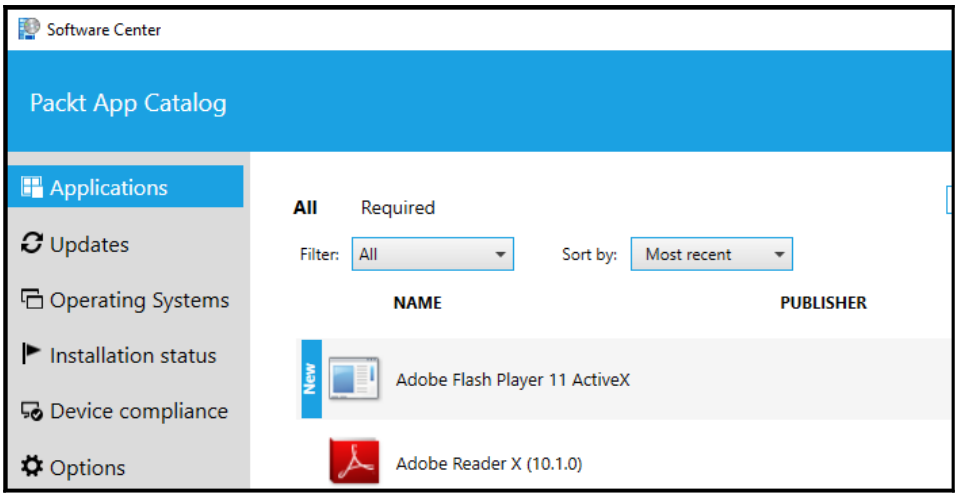

Specify the schedule for this deployment
This application will be available as soon as possible by default. If this application should be made available at a different time, change the availability time to the desired UTC time.
Time based on:
UTC
Schedule the application to be available at:
7/17/2017
12:40 PM
Installation deadline to upgrade users or devices that have the superseded application installed:
As soon as possible after the available time
Schedule at:
7/17/2017
12:40 PM

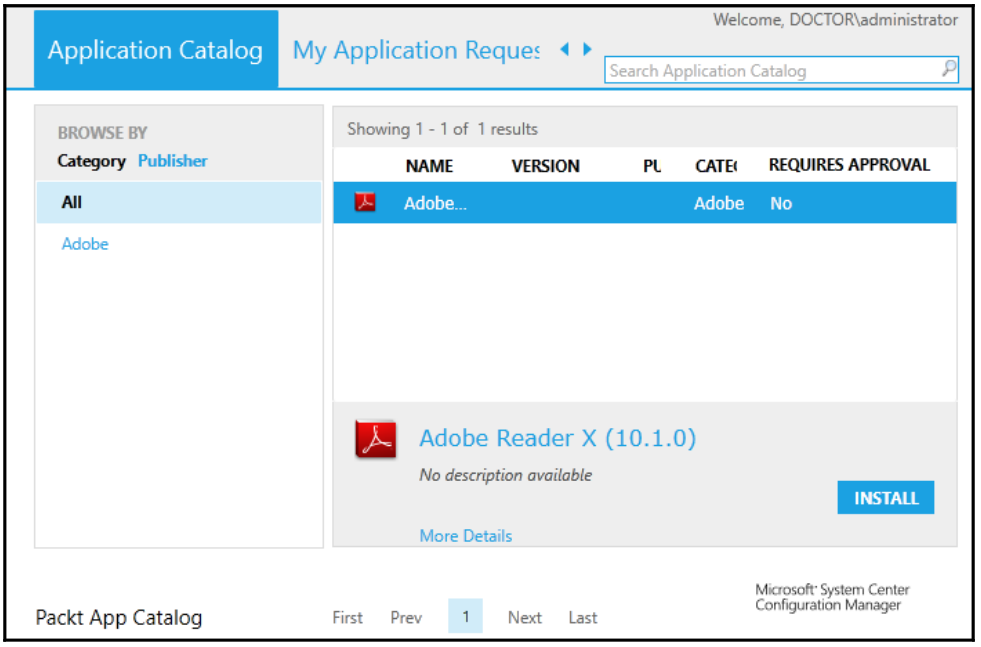

Specify the user experience for the installation of this software on the selected devices
Specify user experience setting for this deployment
User notifications:
Display in Software Center, and only show notifications for computer restarts
Display in Software Center and show all notifications
Display in Software Center, and only show notifications for computer restarts
When the installation deadline is reached, allow the following activities to be performed outside the maintenance window:
Software Installation
System restart (if required to complete the installation)
Write filter handling for Windows Embedded devices
Commit changes at deadline or during a maintenance window (requires restarts)
If this option is not selected, content will be applied on the overlay and committed later.

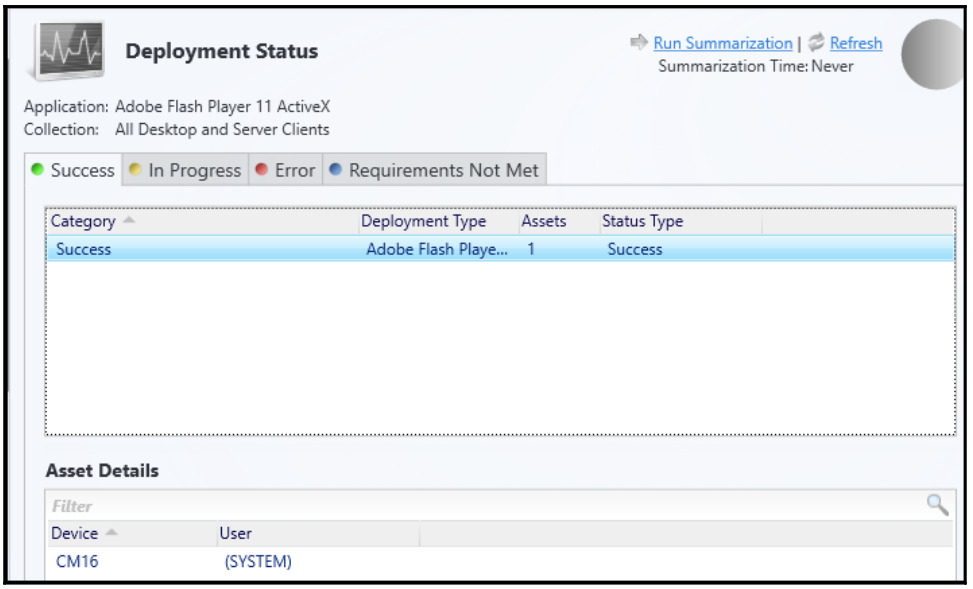

Specify settings to control how this software is deployed
Action:
Install
Purpose:
Required
Pre-deploy software to the user's primary device
Send wake-up packets
Allow clients on a metered Internet connection to download content after the installation deadline, which might incur additional costs
Automatically upgrade any superseded versions of this application


Specify the schedule for this deployment
This application will be available as soon as it has been distributed to the content server(s) unless it is scheduled for a later time below. Specify the installation deadline if this is a required application. This deadline is when the application must be installed on the device, including a system restart if necessary.
Time based on:
UTC
Schedule the application to be available at:
7/17/2017
12:45 PM
Installation deadline:
As soon as possible after the available time
Schedule at:
7/17/2017
12:45 PM
Delay enforcement of this deployment according to user preferences, up to the grace period defined in client settings.

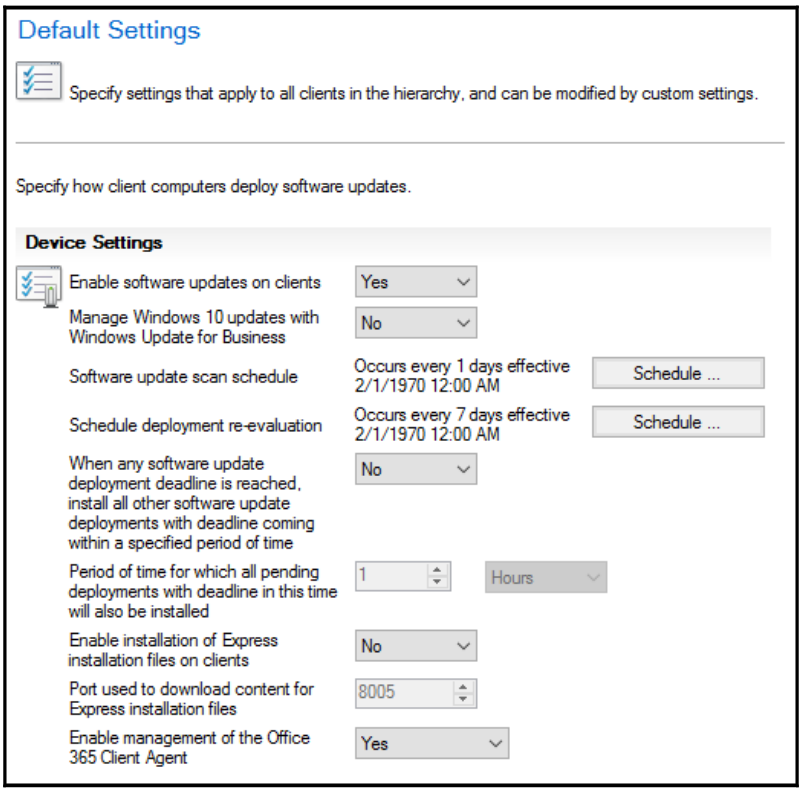

Specify the user experience for the installation of this software on the selected devices
Specify user experience setting for this deployment
User notifications:
Display in Software Center and show all notifications
Display in Software Center and show all notifications
Display in Software Center, and only show notifications for computer restarts
Hide in Software Center and all notifications
When the installation deadline window:
Software Installation
System restart (if required to complete the installation)
Write filter handling for Windows Embedded devices
Commit changes at deadline or during a maintenance window (requires restarts)
If this option is not selected, content will be applied on the overlay and committed later.

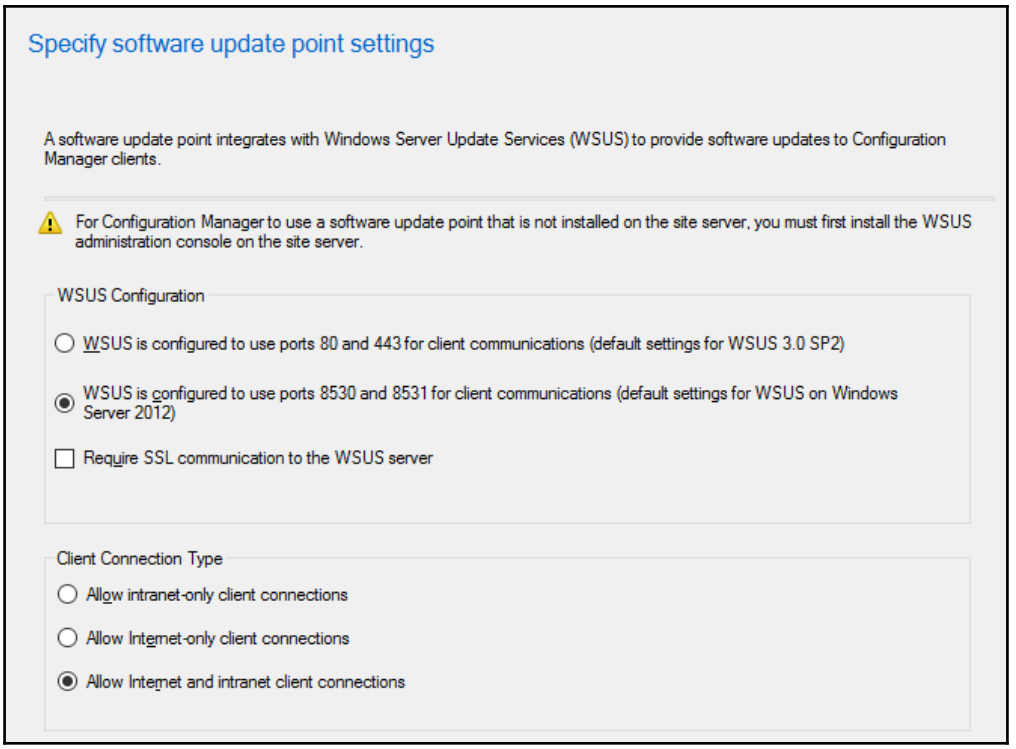

Software Center
Packt App Catalog
Applications
Updates
Operating Systems
Installation status
Device compliance
Options
All
Required
Filter:
All
Sort by:
Most recent
NAME
PUBLISHER
New
Adobe Flash Player 11 ActiveX
Adobe Reader X (10.1.0)

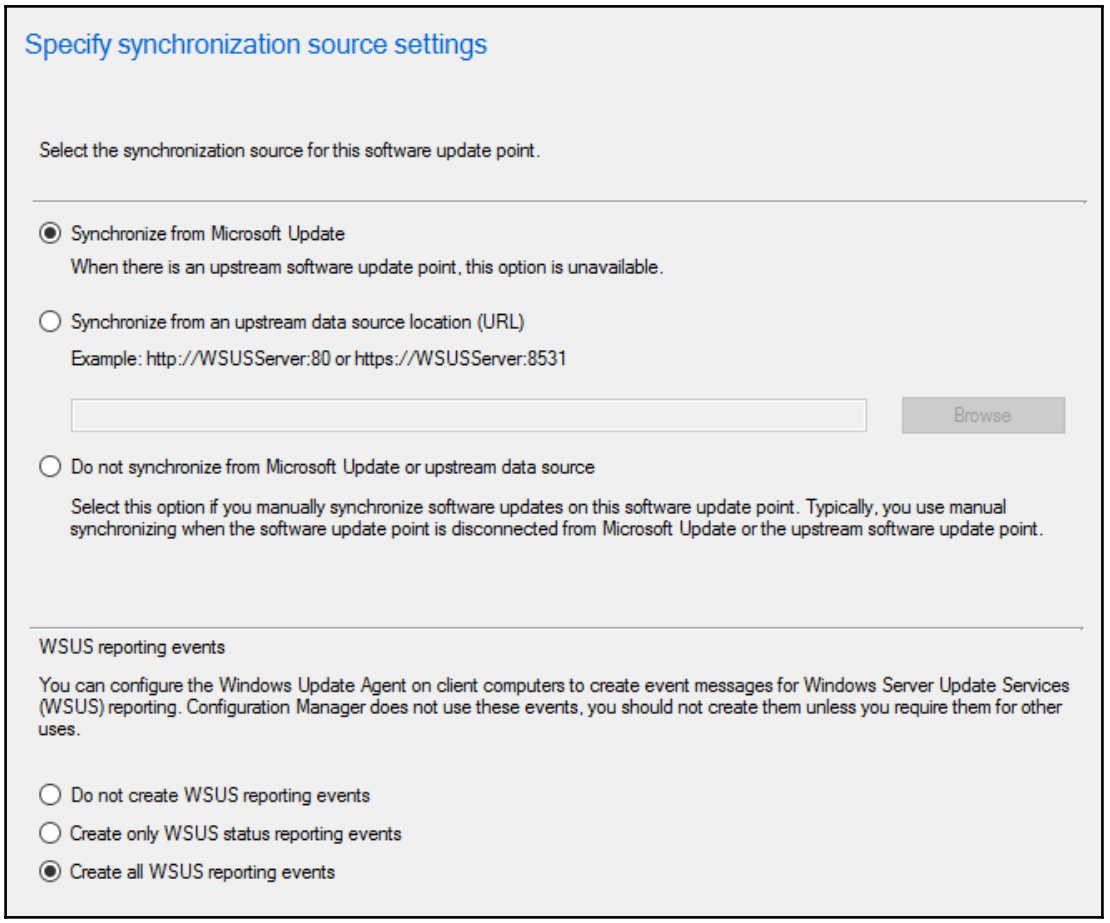

Application Catalog
My Application Reques
Welcome, DOCTOR\administrator
Search Application Catalog
BROWSE BY
Category
Publisher
All
Adobe
Showing 1 - 1 of 1 results
NAME
VERSION
PU
CATE(
REQUIRES APPROVAL
Adobe...
Adobe
No
Adobe Reader X (10.1.0)
No description available
INSTALL
More Details
Packt App Catalog
First
Prev
1
Next
Last
Microsoft System Center
Configuration Manager

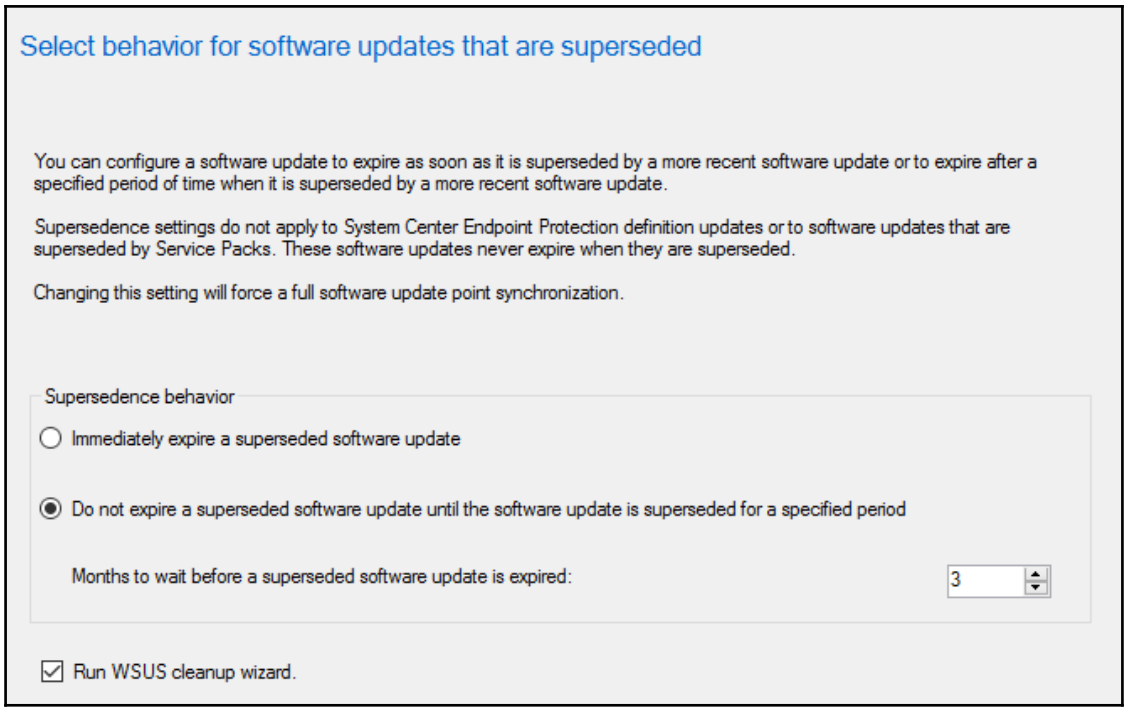

Deployment Status
Run Summarization | Refresh
Summarization Time: Never
Application: Adobe Flash Player 11 ActiveX
Collection: All Desktop and Server Clients
Success
In Progress
Error
Requirements Not Met
Category
Deployment Type
Assets
Status Type
Success
Adobe Flash Playe...
1
Success
Asset Details
Filter
Device
User
CM16
(SYSTEM)

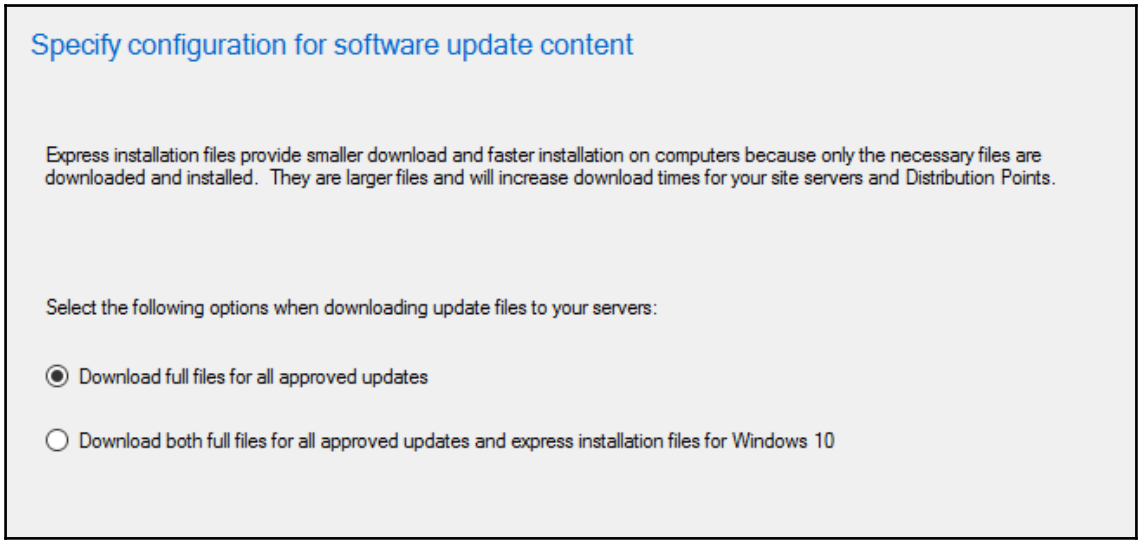
# Chapter 8: Software Update Management

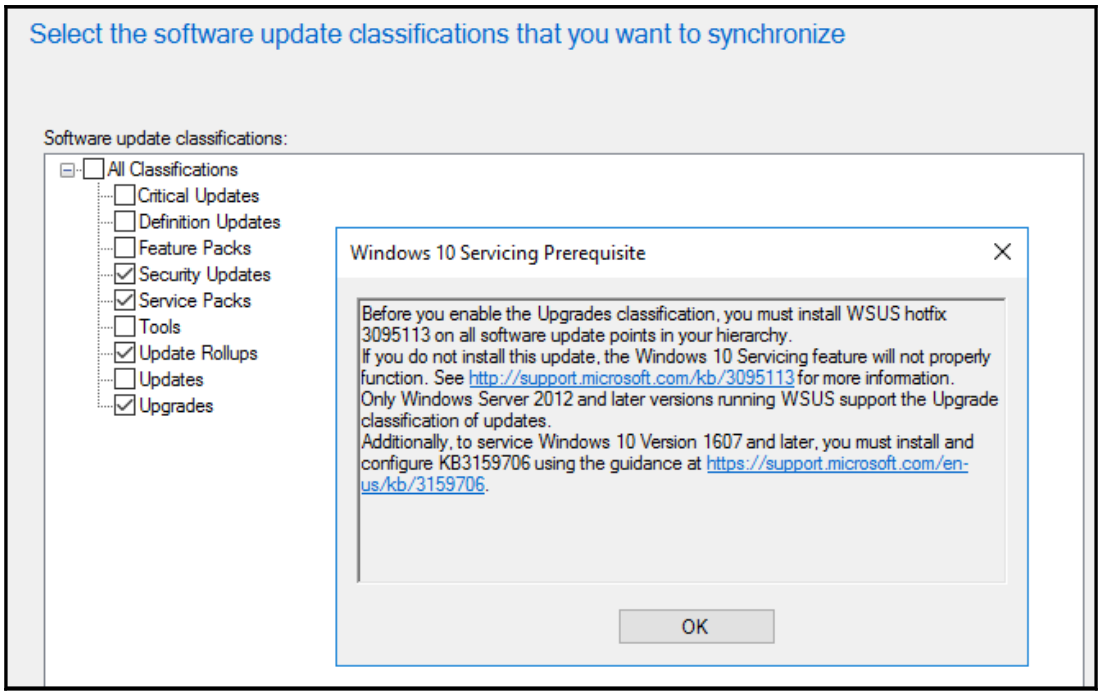


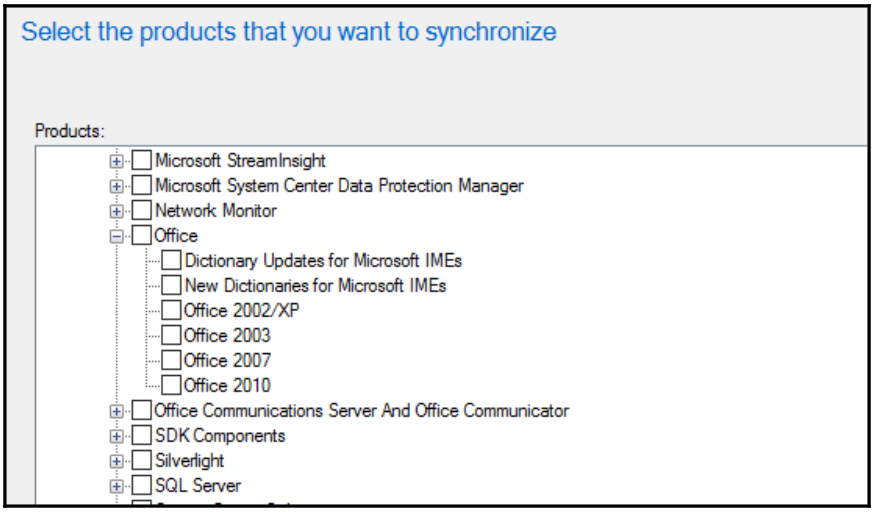

Specify software update point settings
A software update point integrates with Windows Server Update Services (WSUS) to provide software updates to Configuration Manager clients.
For Configuration Manager to use a software update point that is not installed on the site server, you must first install the WSUS administration console on the site server.
WSUS Configuration
WSUS is configured to use ports 80 and 443 for client communications (default settings for WSUS 3.0 SP2)
WSUS is configured to use ports 8530 and 8531 for client communications (default settings for WSUS on Windows Server 2012)
Require SSL communication to the WSUS server
Client Connection Type
Allow intranet-only client connections
Allow Internet-only client connections
Allow Internet and intranet client connections

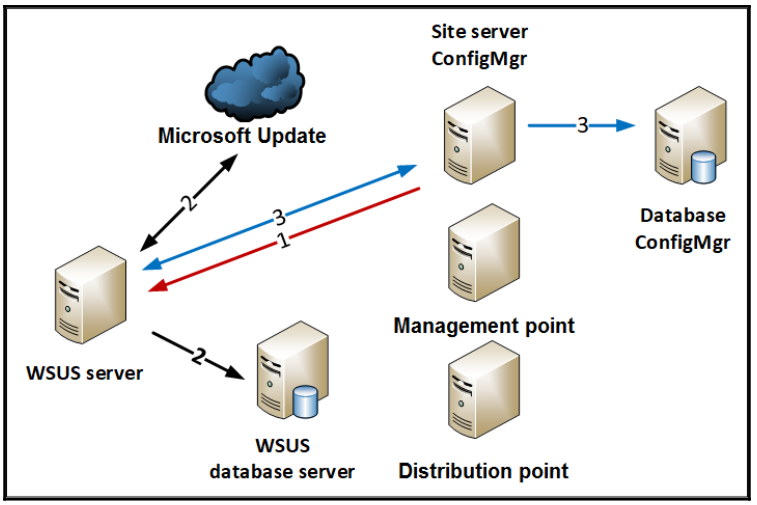

Specify synchronization source settings
Select the synchronization source for this software update point.
Synchronize from Microsoft Update
When there is an upstream software update point, this option is unavailable.
Synchronize from an upstream data source location (URL)
Example: http://WSUSServer:80 or https://WSUSServer:8531
Browse
Do not synchronize from Microsoft Update or upstream data source
Select this option if you manually synchronize software updates on this software update point. Typically, you use manual synchronizing when the software update point is disconnected from Microsoft Update or the upstream software update point.
WSUS reporting events
You can configure the Windows Update Agent on client computers to create event messages for Windows Server Update Services (WSUS) reporting. Configuration Manager does not use these events, you should not create them unless you require them for other uses.
Do not create WSUS reporting events
Create only WSUS status reporting events
Create all WSUS reporting events

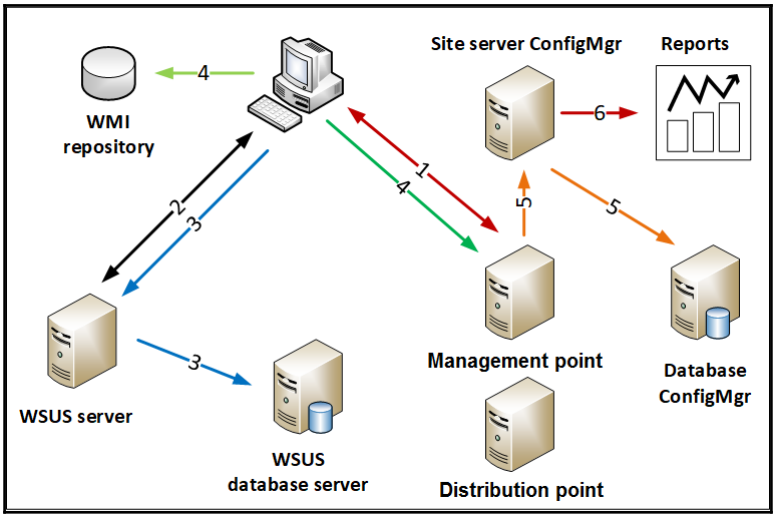

Select behavior for software updates that are superseded
You can configure a software update to expire as soon as it is superseded by a more recent software update or to expire after a specified period of time when it is superseded by a more recent software update.
Supersedence settings do not apply to System Center Endpoint Protection definition updates or to software updates that are superseded by Service Packs. These software updates never expire when they are superseded.
Changing this setting will force a full software update point synchronization.
Supersedence behavior
Immediately expire a superseded software update
Do not expire a superseded software update until the software update is superseded for a specified period
Months to wait before a superseded software update is expired:
3
Run WSUS cleanup wizard.

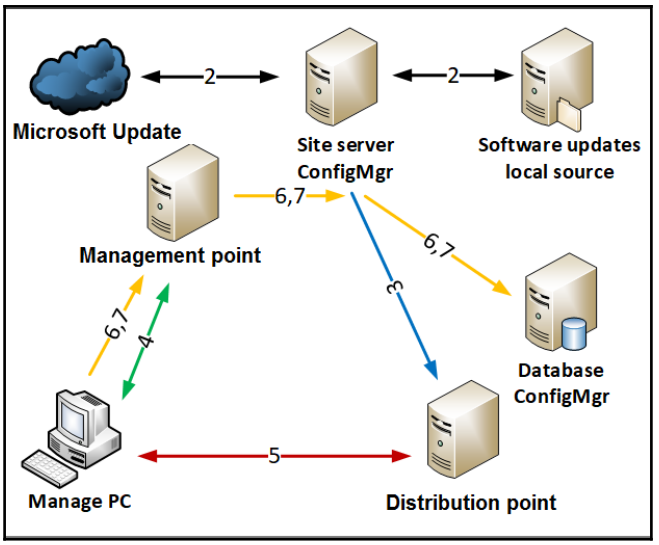

Specify configuration for software update content
Express installation files provide smaller download and faster installation on computers because only the necessary files are downloaded and installed. They are larger files and will increase download times for your site servers and Distribution Points.
Select the following options when downloading update files to your servers:
Download full files for all approved updates
Download both full files for all approved updates and express installation files for Windows 10


Select the software update classifications that you want to synchronize
Software update classifications:
All Classifications
Critical Updates
Definition Updates
Feature Packs
Security Updates
Service Packs
Tools
Update Rollups
Updates
Upgrades
Windows 10 Servicing Prerequisite
Before you enable the Upgrades classification, you must install WSUS hotfix 3095113 on all software update points in your hierarchy.
If you do not install this update, the Windows 10 Servicing feature will not properly function. See http://support.microsoft.com/kb/3095113 for more information.
Only Windows Server 2012 and later versions running WSUS support the Upgrade classification of updates.
Additionally, to service Windows 10 Version 1607 and later, you must install and configure KB3159706 using the guidance at https://support.microsoft.com/en-us/kb/3159706.
OK


Select the products that you want to synchronize
Products:
Microsoft StreamInsight
Microsoft System Center Data Protection Manager
Network Monitor
Office
Dictionary Updates for Microsoft IMEs
New Dictionaries for Microsoft IMEs
Office 2002/XP
Office 2003
Office 2007
Office 2010
Office Communications Server And Office Communicator
SDK Components
Silverlight
SQL Server


Site server
ConfigMgr
Microsoft Update
3
2
3
1
Database
ConfigMgr
Management point
WSUS server
2
WSUS
database server
Distribution point


Site server ConfigMgr
Reports
4
6
WMI
repository
1
4
5
5
2
3
3
Management point
Database
ConfigMgr
WSUS server
WSUS
database server
Distribution point




All Software Updates Search Results - 1 items shown

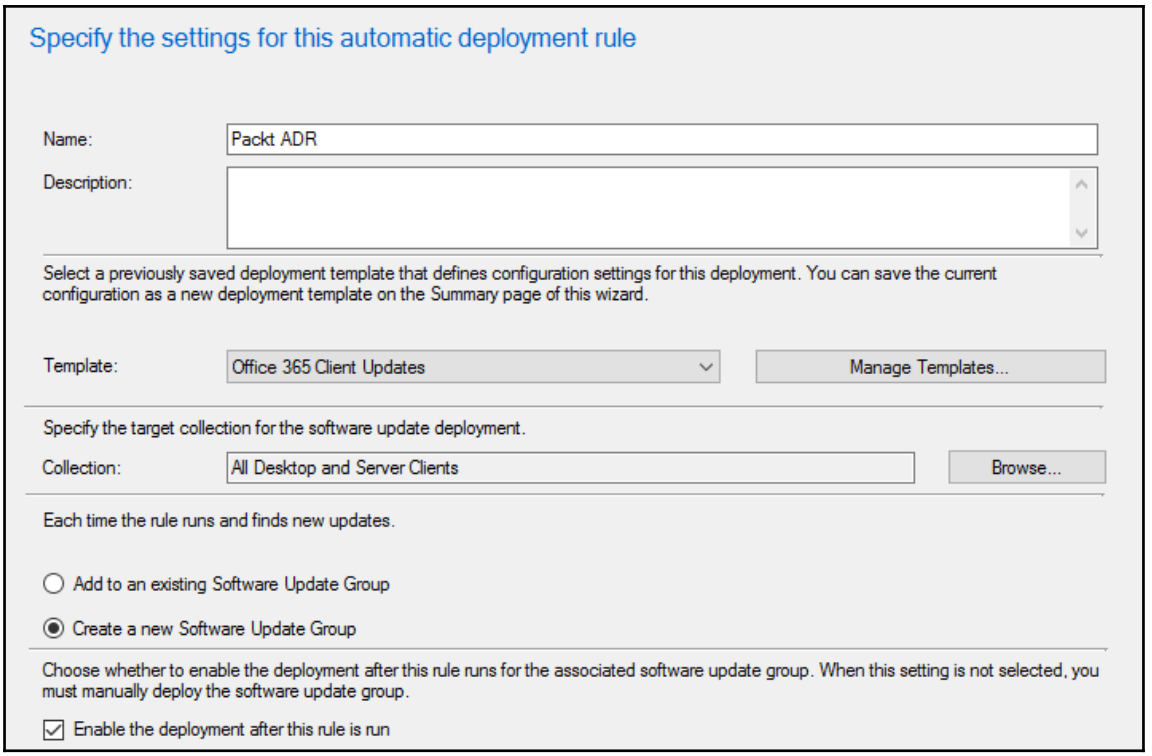
Search | Search | Add Criteria

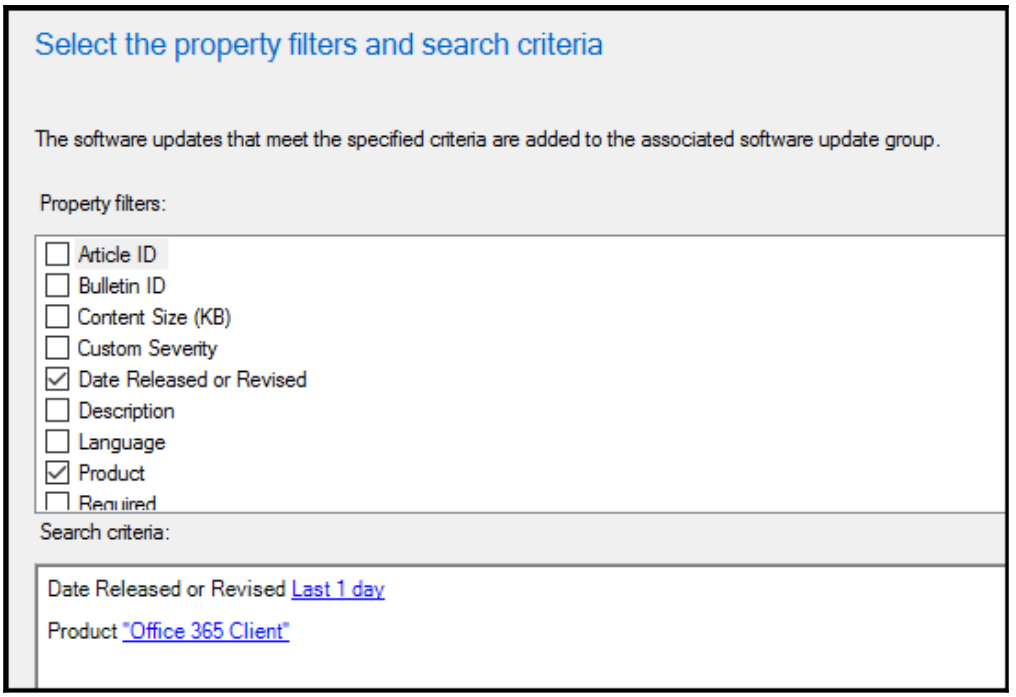
AND Installed is less than or equal to Enter valid characters

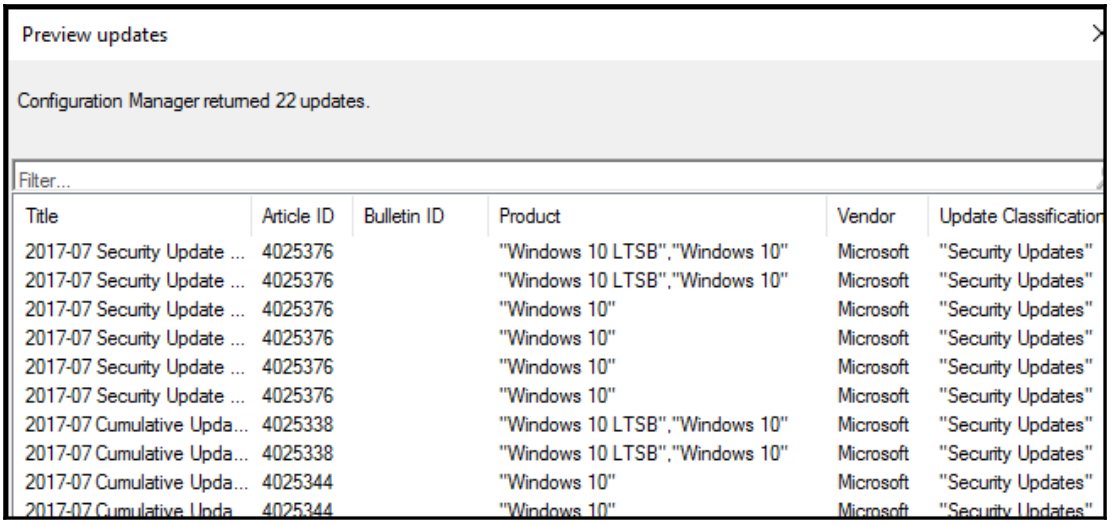
AND Product Windows Server 2016

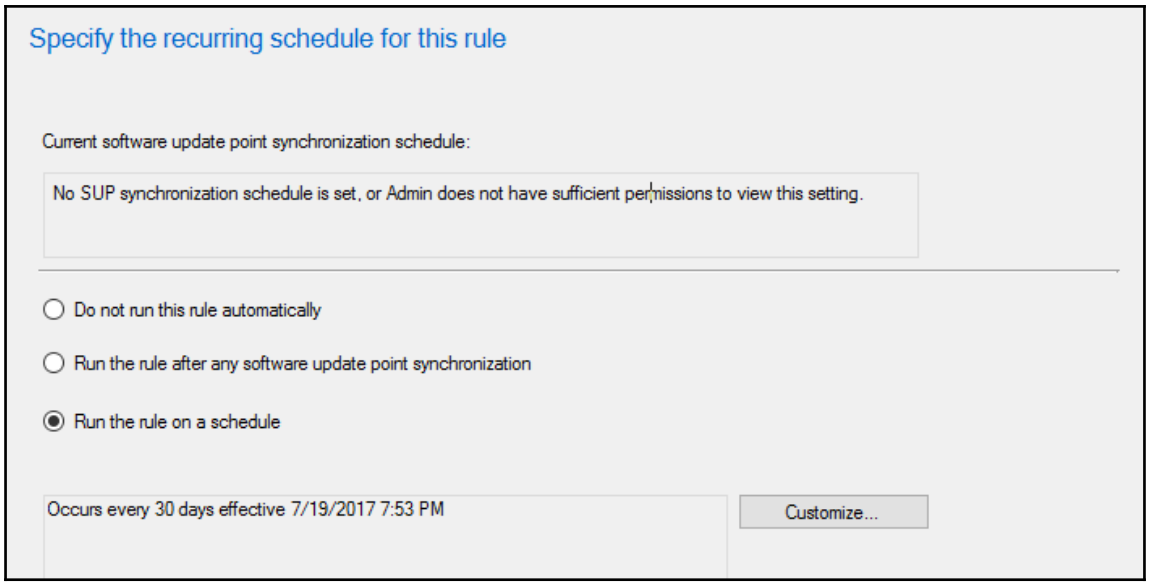
AND Update Classification Critical Updates

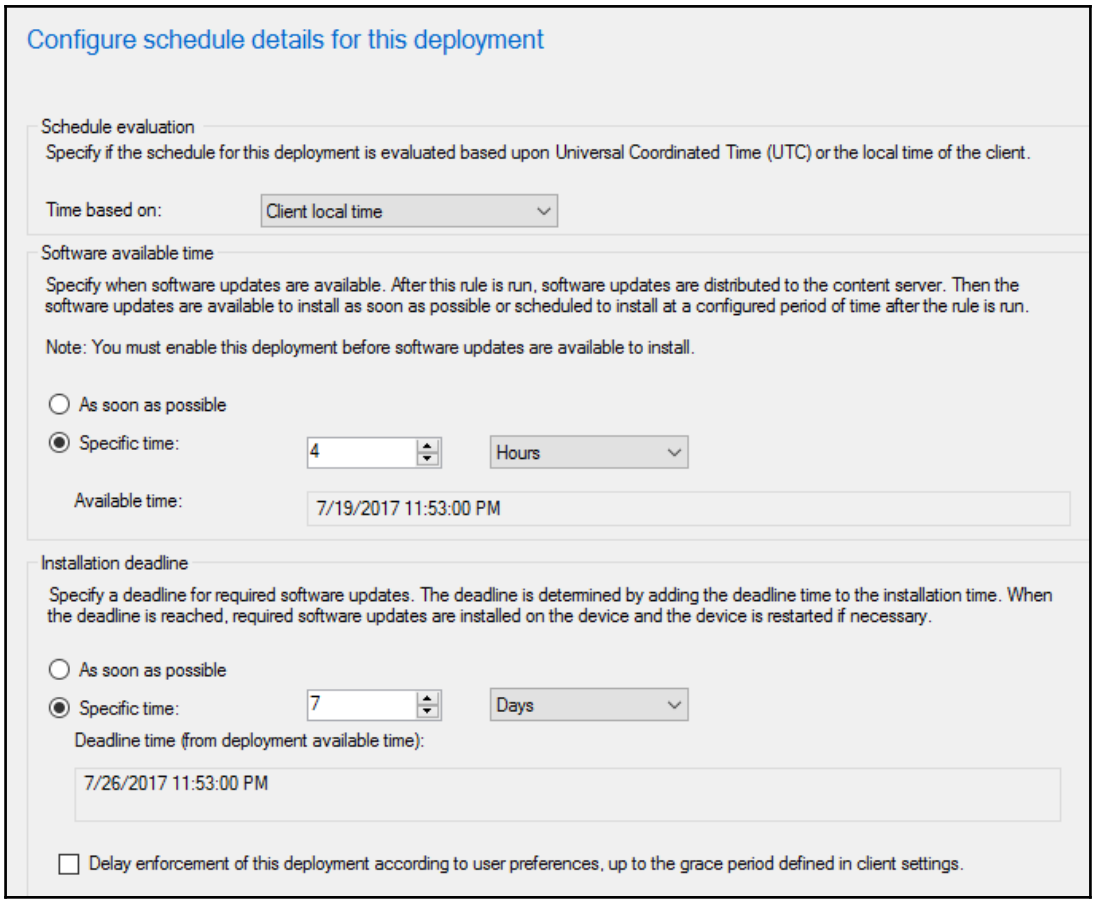
| Icon | Title | Bulletin ID | Unknown | Required | Installed | Percent Compliant |
|---|---|---|---|---|---|---|
| | Update for Windows Server 2016 for x64-ba... | | 0 | 0 | 0 | 100 |

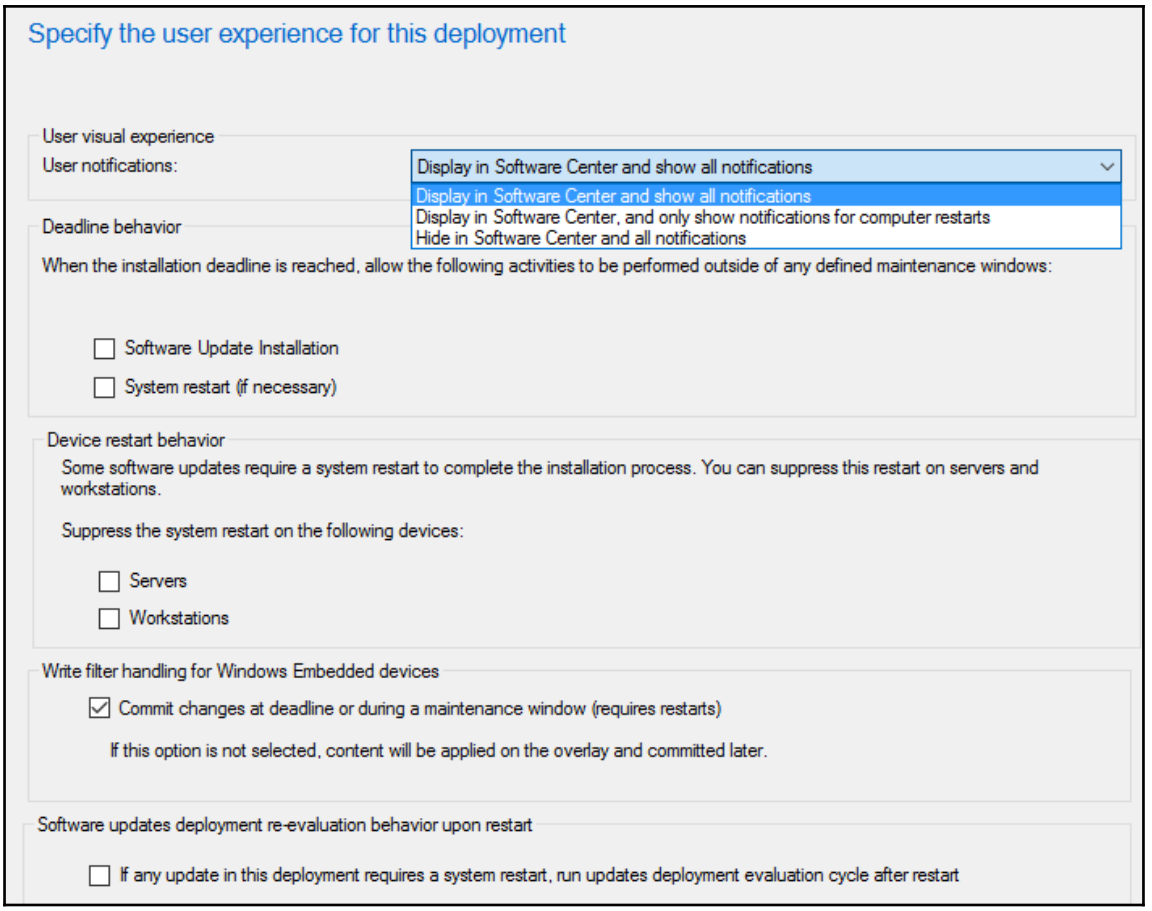

Specify the settings for this automatic deployment rule
Name:
Packt ADR
Description:
Select a previously saved deployment template that defines configuration settings for this deployment. You can save the current configuration as a new deployment template on the Summary page of this wizard.
Template:
Office 365 Client Updates
Manage Templates...
Specify the target collection for the software update deployment.
Collection:
All Desktop and Server Clients
Browse...
Each time the rule runs and finds new updates.
Add to an existing Software Update Group
Create a new Software Update Group
Choose whether to enable the deployment after this rule runs for the associated software update group. When this setting is not selected, you must manually deploy the software update group.
Enable the deployment after this rule is run

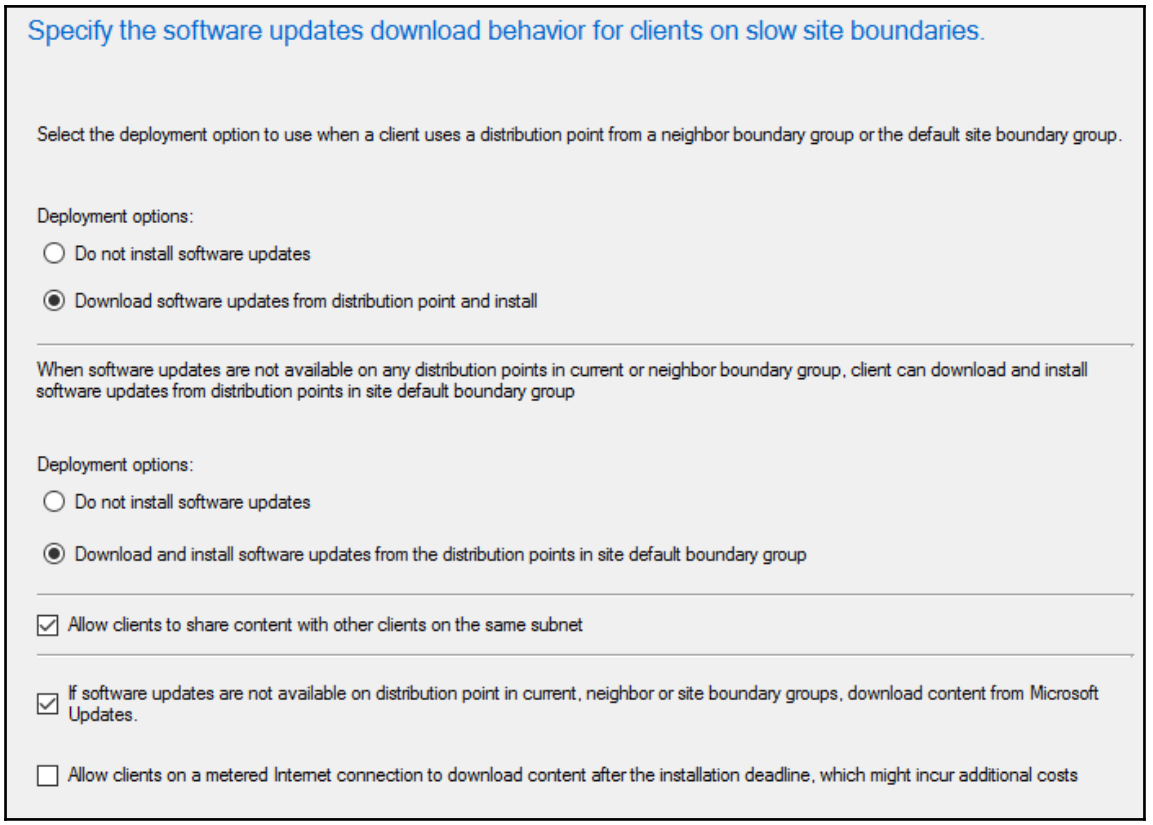

Select the property filters and search criteria
The software updates that meet the specified criteria are added to the associated software update group.
Property filters:
Article ID
Bulletin ID
Content Size (KB)
Custom Severity
Date Released or Revised
Description
Language
Product
Required
Search criteria:
Date Released or Revised Last 1 day
Product "Office 365 Client"

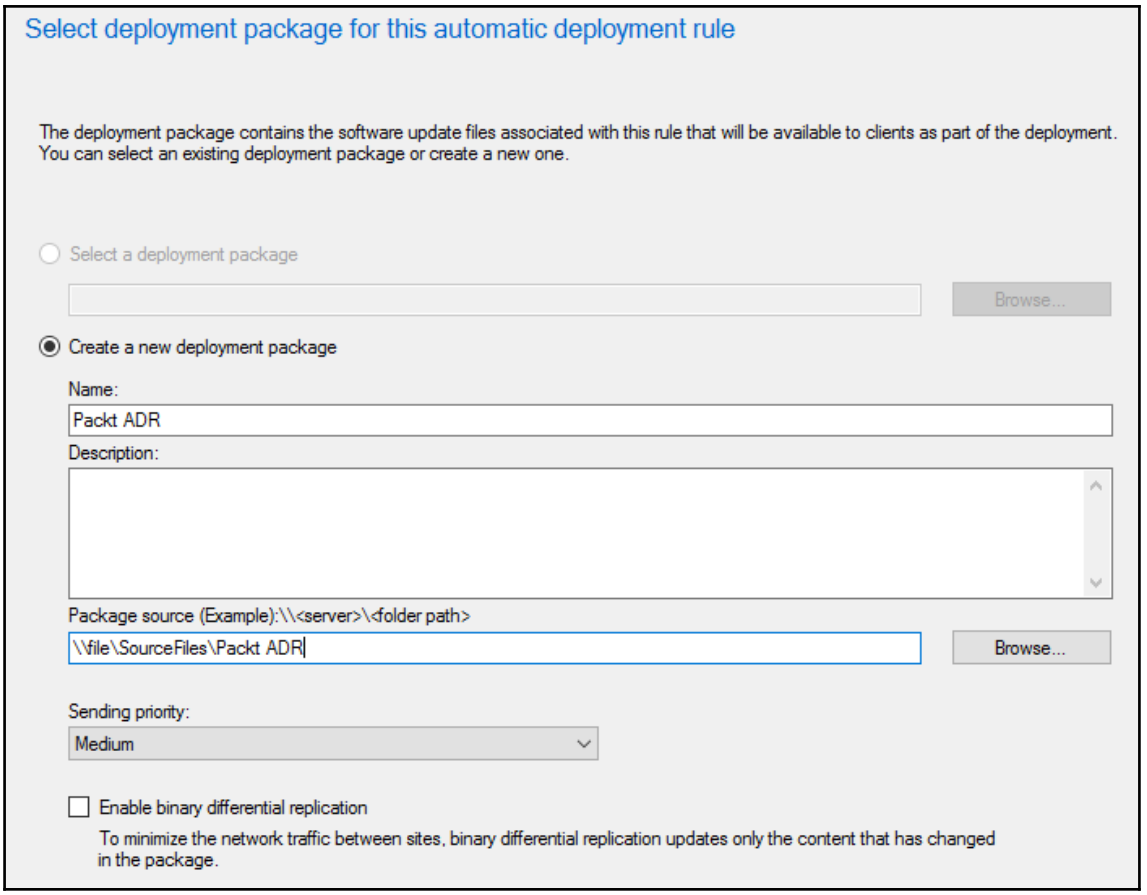

Preview updates
Configuration Manager returned 22 updates.
Filter...
Title
Article ID
Bulletin ID
Product
Vendor
Update Classification
2017-07 Security Update ... 4025376 "Windows 10 LTSB","Windows 10" Microsoft "Security Updates"
2017-07 Security Update ... 4025376 "Windows 10 LTSB","Windows 10" Microsoft "Security Updates"
2017-07 Security Update ... 4025376 "Windows 10" Microsoft "Security Updates"
2017-07 Security Update ... 4025376 "Windows 10" Microsoft "Security Updates"
2017-07 Security Update ... 4025376 "Windows 10" Microsoft "Security Updates"
2017-07 Security Update ... 4025376 "Windows 10" Microsoft "Security Updates"
2017-07 Cumulative Upda... 4025338 "Windows 10 LTSB","Windows 10" Microsoft "Security Updates"
2017-07 Cumulative Upda... 4025338 "Windows 10 LTSB","Windows 10" Microsoft "Security Updates"
2017-07 Cumulative Upda... 4025344 "Windows 10" Microsoft "Security Updates"
2017-07 Cumulative Upda... 4025344 "Windows 10" Microsoft "Security Updates"

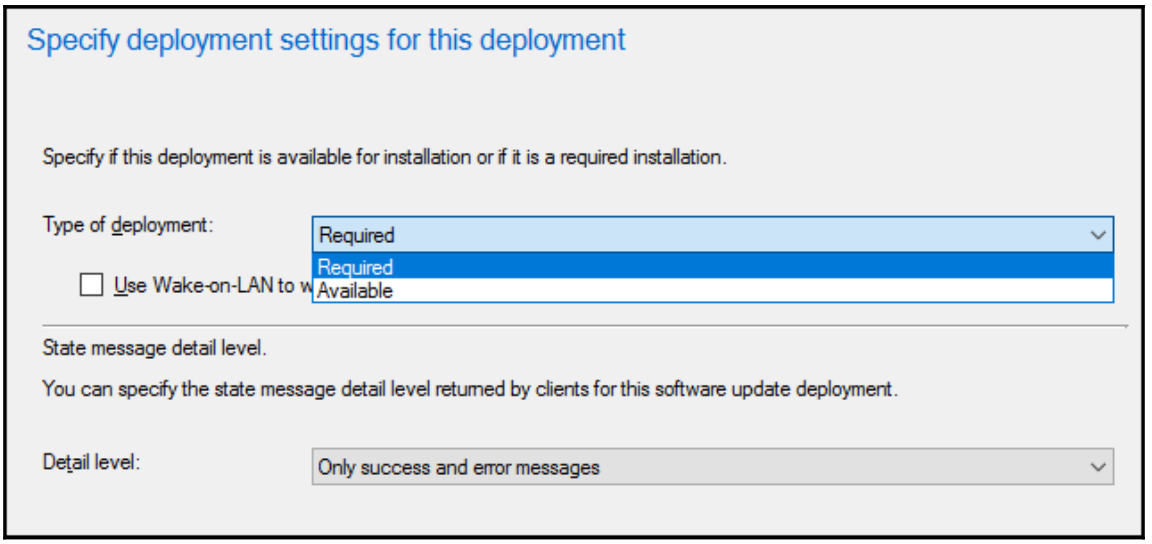

Specify the recurring schedule for this rule
Current software update point synchronization schedule:
No SUP synchronization schedule is set, or Admin does not have sufficient permissions to view this setting.
Do not run this rule automatically
Run the rule after any software update point synchronization
Run the rule on a schedule
Occurs every 30 days effective 7/19/2017 7:53 PM
Customize...

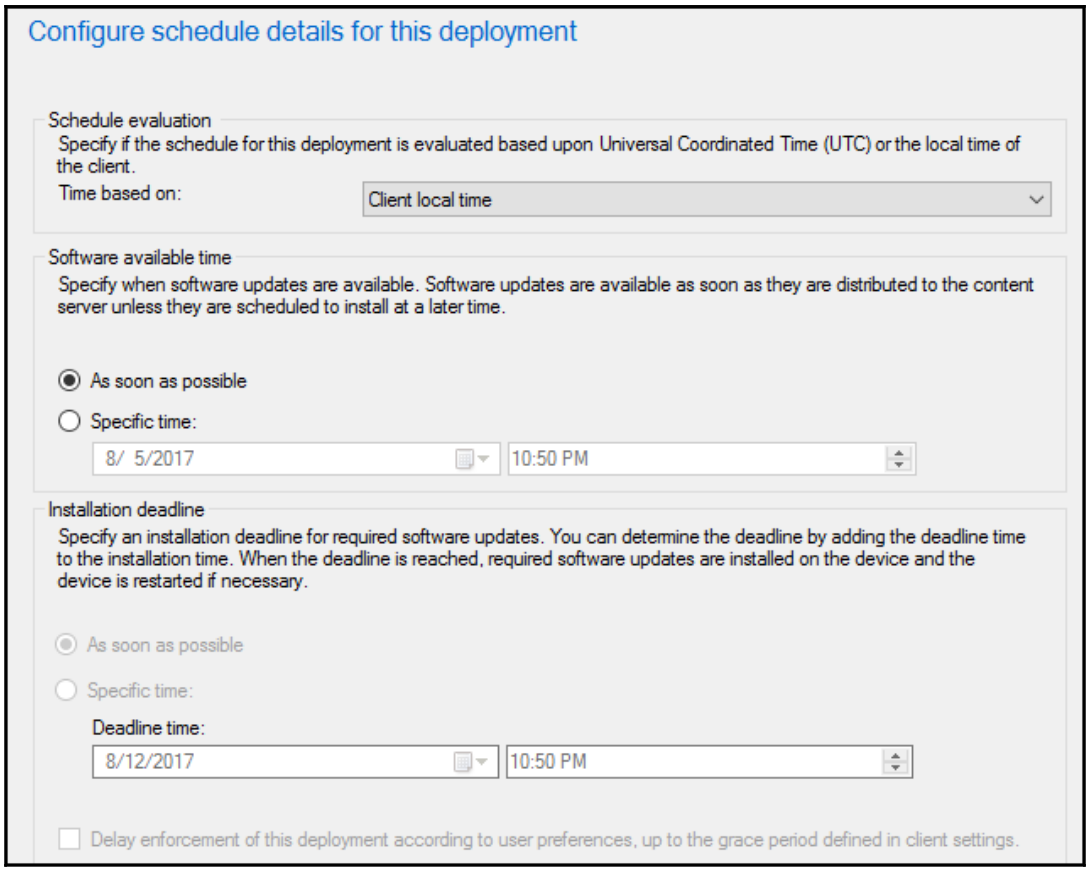

Configure schedule details for this deployment
Schedule evaluation
Specify if the schedule for this deployment is evaluated based upon Universal Coordinated Time (UTC) or the local time of the client.
Time based on:
Client local time
Software available time
Specify when software updates are available. After this rule is run, software updates are distributed to the content server. Then the software updates are available to install as soon as possible or scheduled to install at a configured period of time after the rule is run.
Note: You must enable this deployment before software updates are available to install.
As soon as possible
Specific time:
4
Hours
Available time:
7/19/2017 11:53:00 PM
Installation deadline
Specify a deadline for required software updates. The deadline is determined by adding the deadline time to the installation time. When the deadline is reached, required software updates are installed on the device and the device is restarted if necessary.
As soon as possible
Specific time:
7
Days
Deadline time (from deployment available time):
7/26/2017 11:53:00 PM
Delay enforcement of this deployment according to user preferences, up to the grace period defined in client settings.

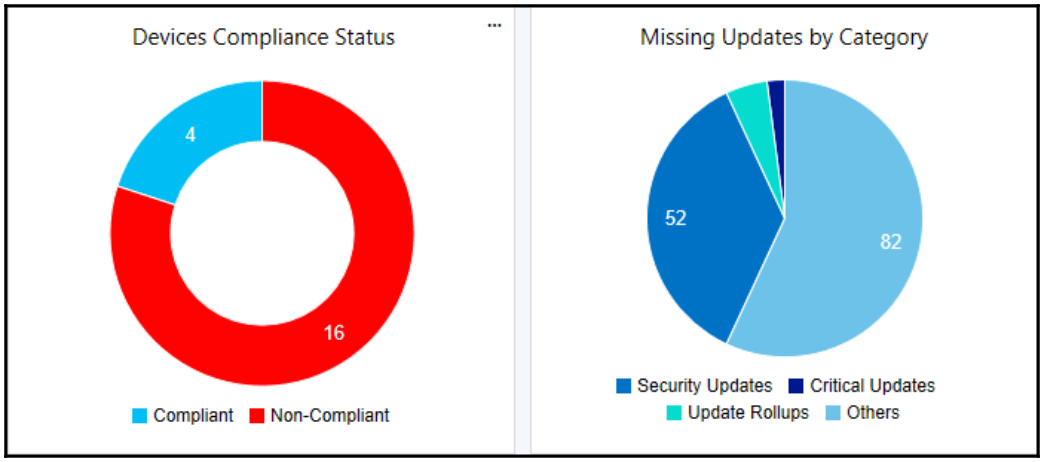

Specify the user experience for this deployment
User visual experience
User notifications:
Display in Software Center and show all notifications
Display in Software Center and show all notifications
Display in Software Center, and only show notifications for computer restarts
Hide in Software Center and all notifications
Deadline behavior
When the installation deadline is reached, allow the following activities to be performed outside of any defined maintenance windows:
Software Update Installation
System restart (if necessary)
Device restart behavior
Some software updates require a system restart to complete the installation process. You can suppress this restart on servers and workstations.
Suppress the system restart on the following devices:
Servers
Workstations
Write filter handling for Windows Embedded devices
Commit changes at deadline or during a maintenance window (requires restarts)
If this option is not selected, content will be applied on the overlay and committed later.
Software updates deployment re-evaluation behavior upon restart
If any update in this deployment requires a system restart, run updates deployment evaluation cycle after restart

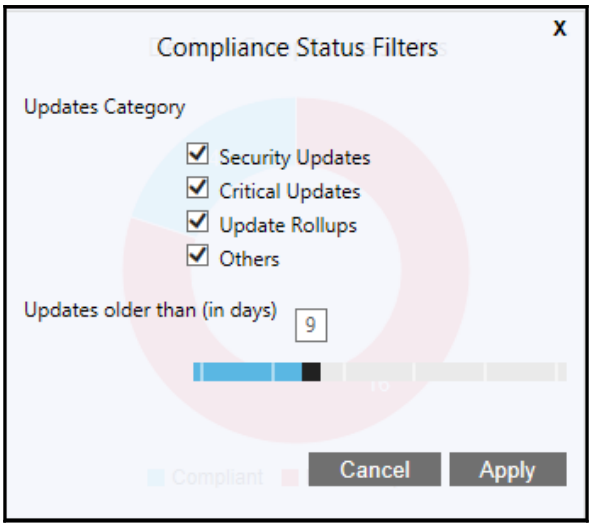

Specify the software updates download behavior for clients on slow site boundaries.
Select the deployment option to use when a client uses a distribution point from a neighbor boundary group or the default site boundary group.
Deployment options:
Do not install software updates
Download software updates from distribution point and install
When software updates are not available on any distribution points in current or neighbor boundary group, client can download and install software updates from distribution points in site default boundary group
Deployment options:
Do not install software updates
Download and install software updates from the distribution points in site default boundary group
Allow clients to share content with other clients on the same subnet
If software updates are not available on distribution point in current, neighbor or site boundary groups, download content from Microsoft Updates.
Allow clients on a metered Internet connection to download content after the installation deadline, which might incur additional costs

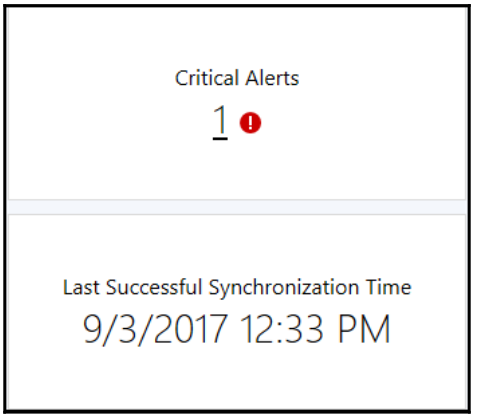

Select deployment package for this automatic deployment rule
The deployment package contains the software update files associated with this rule that will be available to clients as part of the deployment. You can select an existing deployment package or create a new one.
Select a deployment package
Browse...
Create a new deployment package
Name:
Packt ADR
Description:
Package source (Example):\\<server>\<folder path>
\\file\SourceFiles\Packt ADR
Browse...
Sending priority:
Medium
Enable binary differential replication
To minimize the network traffic between sites, binary differential replication updates only the content that has changed in the package.

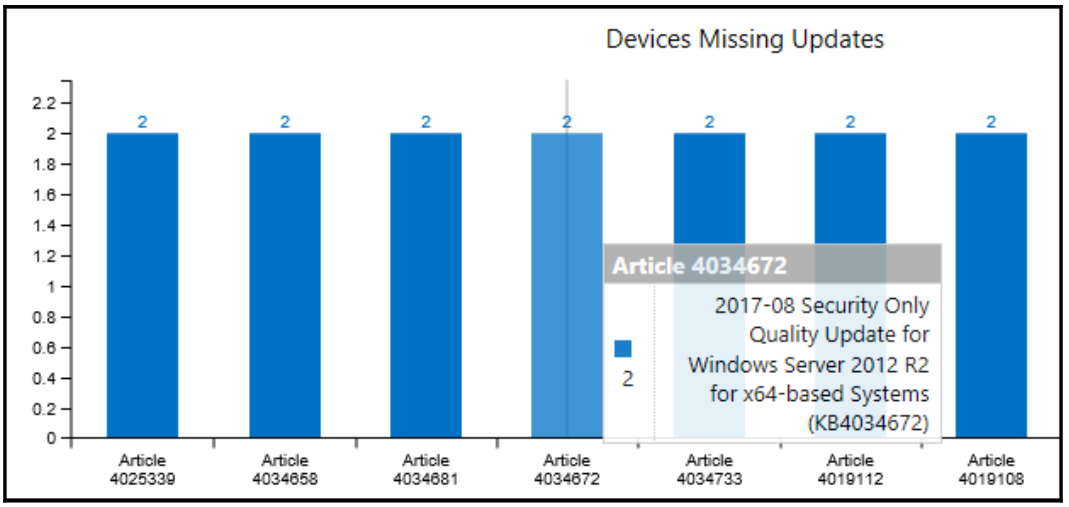

Specify deployment settings for this deployment
Specify if this deployment is available for installation or if it is a required installation.
Type of deployment:
Required
Required
Available
Use Wake-on-LAN to w
State message detail level.
You can specify the state message detail level returned by clients for this software update deployment.
Detail level:
Only success and error messages

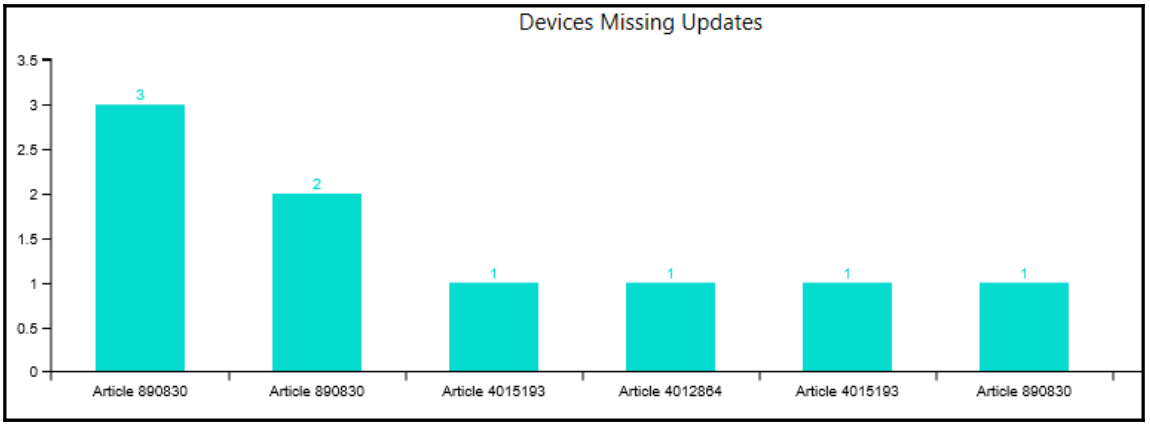

Configure schedule details for this deployment
Schedule evaluation
Specify if the schedule for this deployment is evaluated based upon Universal Coordinated Time (UTC) or the local time of the client.
Time based on:
Client local time
Software available time
Specify when software updates are available. Software updates are available as soon as they are distributed to the content server unless they are scheduled to install at a later time.
As soon as possible
Specific time:
8/ 5/2017
10:50 PM
Installation deadline
Specify an installation deadline for required software updates. You can determine the deadline by adding the deadline time to the installation time. When the deadline is reached, required software updates are installed on the device and the device is restarted if necessary.
As soon as possible
Specific time:
Deadline time:
8/12/2017
10:50 PM
Delay enforcement of this deployment according to user preferences, up to the grace period defined in client settings.


Devices Compliance Status
4
16
Compliant
Non-Compliant
Missing Updates by Category
52
82
Security Updates
Critical Updates
Update Rollups
Others

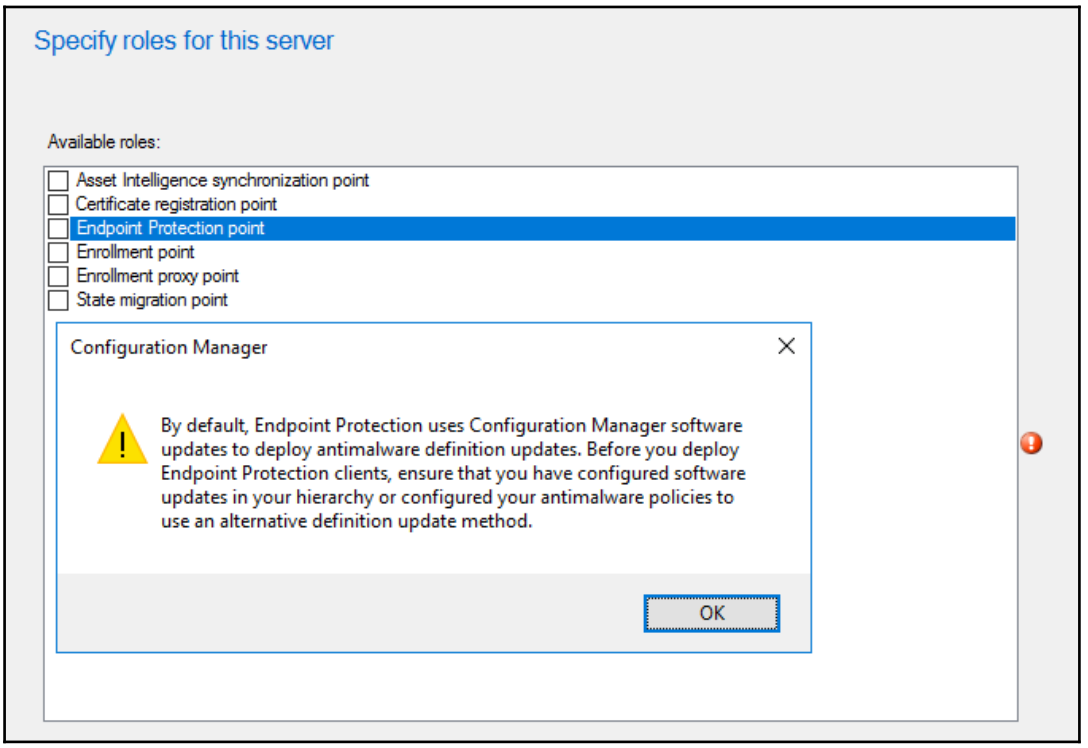

Compliance Status Filters
X
Updates Category
Security Updates
Critical Updates
Update Rollups
Others
Updates older than (in days)
9
Cancel
Apply

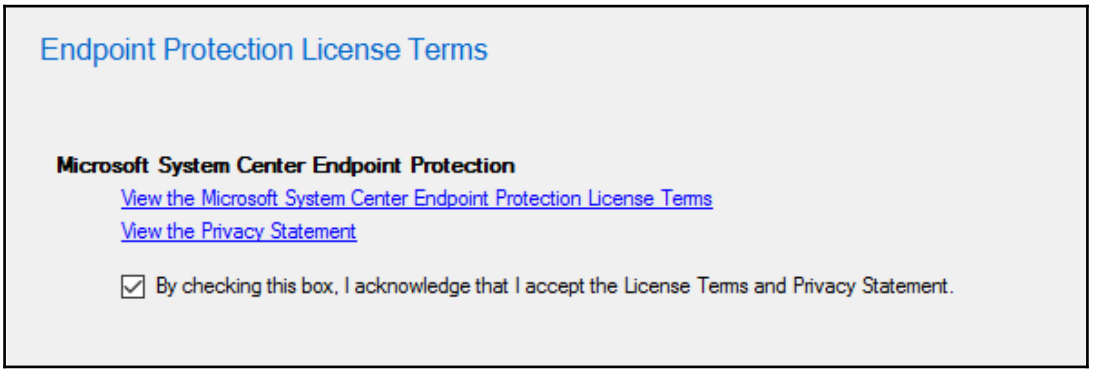

Critical Alerts
1
Last Successful Synchronization Time
9/3/2017 12:33 PM

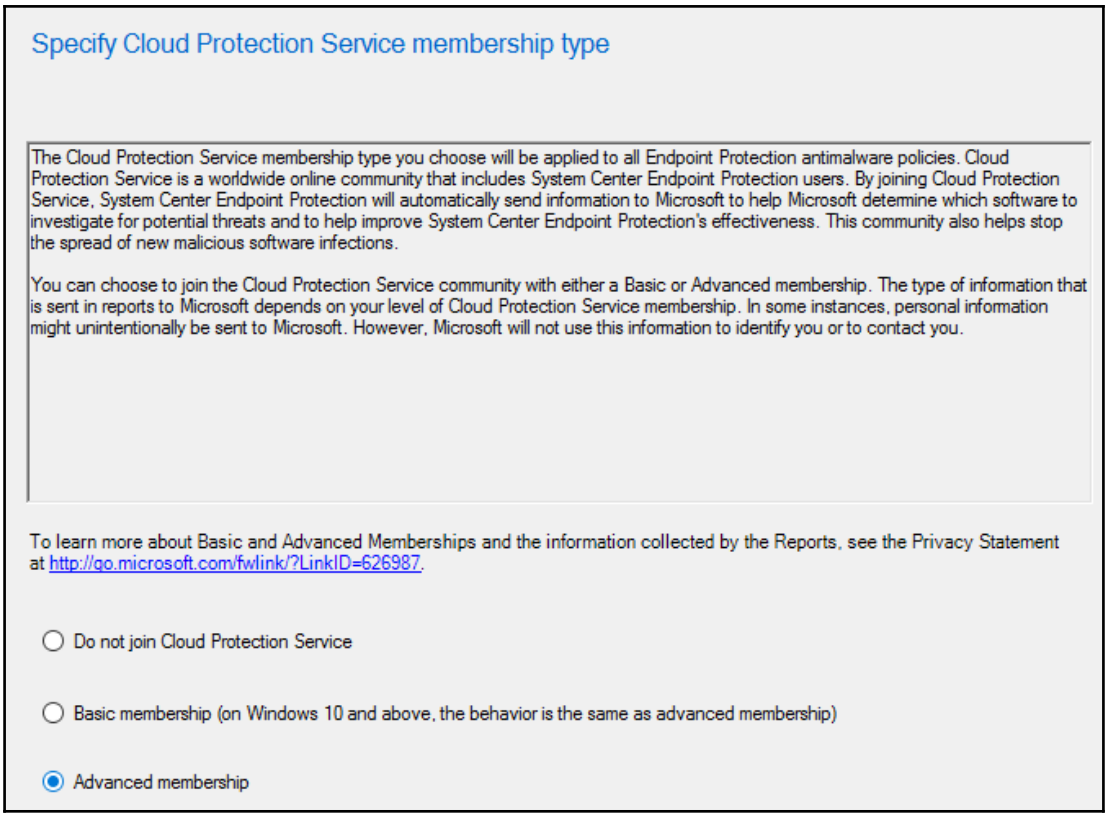

Devices Missing Updates
2.2
2
1.8
1.6
1.4
1.2
1
0.8
0.6
0.4
0.2
0
2
2
2
2
2
2
2
Article 4034672
2
2017-08 Security Only Quality Update for Windows Server 2012 R2 for x64-based Systems (KB4034672)
Article 4025339
Article 4034658
Article 4034681
Article 4034672
Article 4034733
Article 4019112
Article 4019108

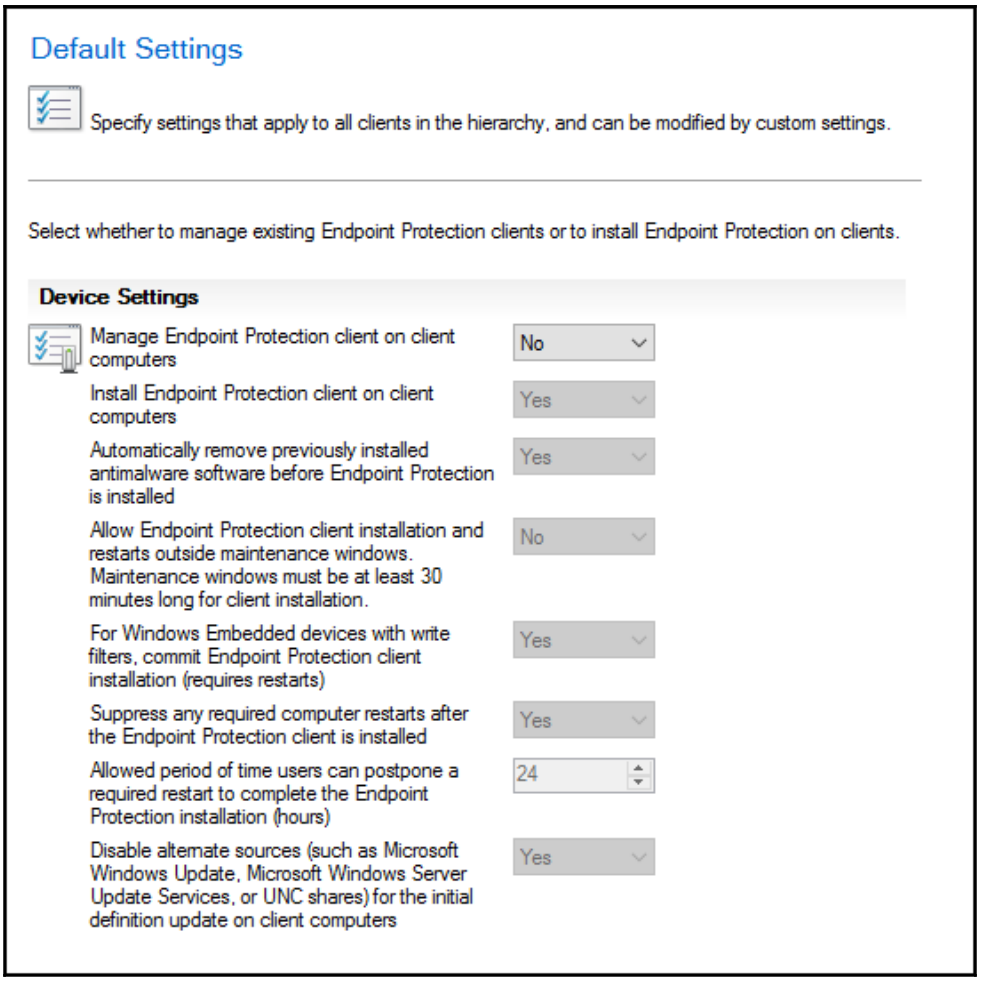

Devices Missing Updates
3.5
3
2.5
2
1.5
1
0.5
0
3
2
1
1
1
1
Article 890830
Article 890830
Article 4015193
Article 4012864
Article 4015193
Article 890830

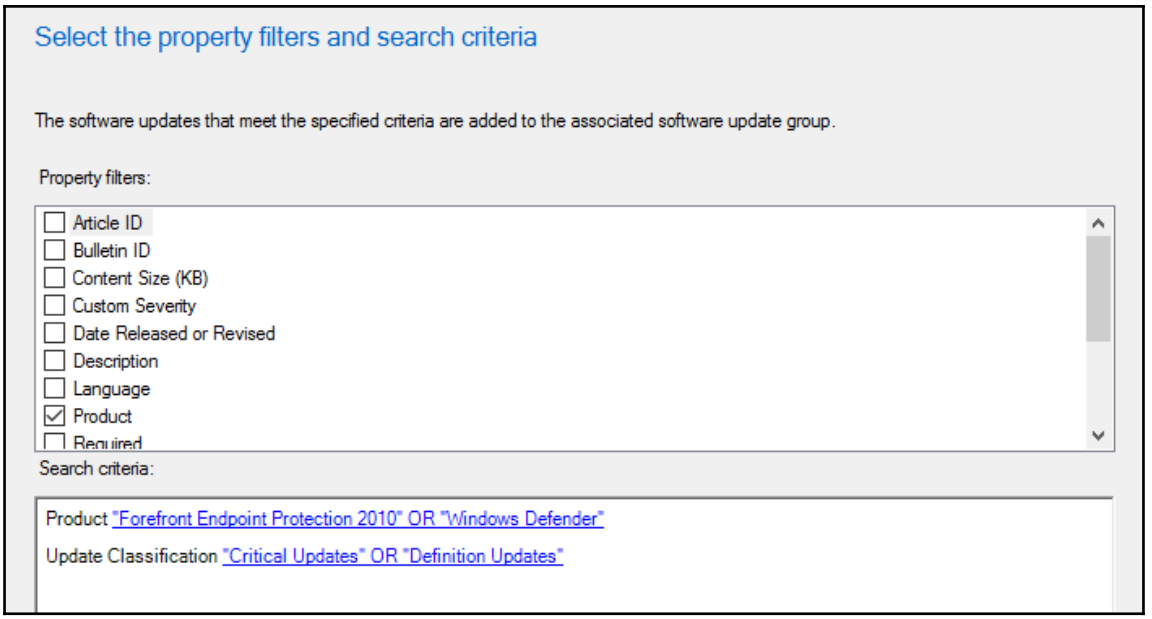
# Chapter 9: Endpoint Protection

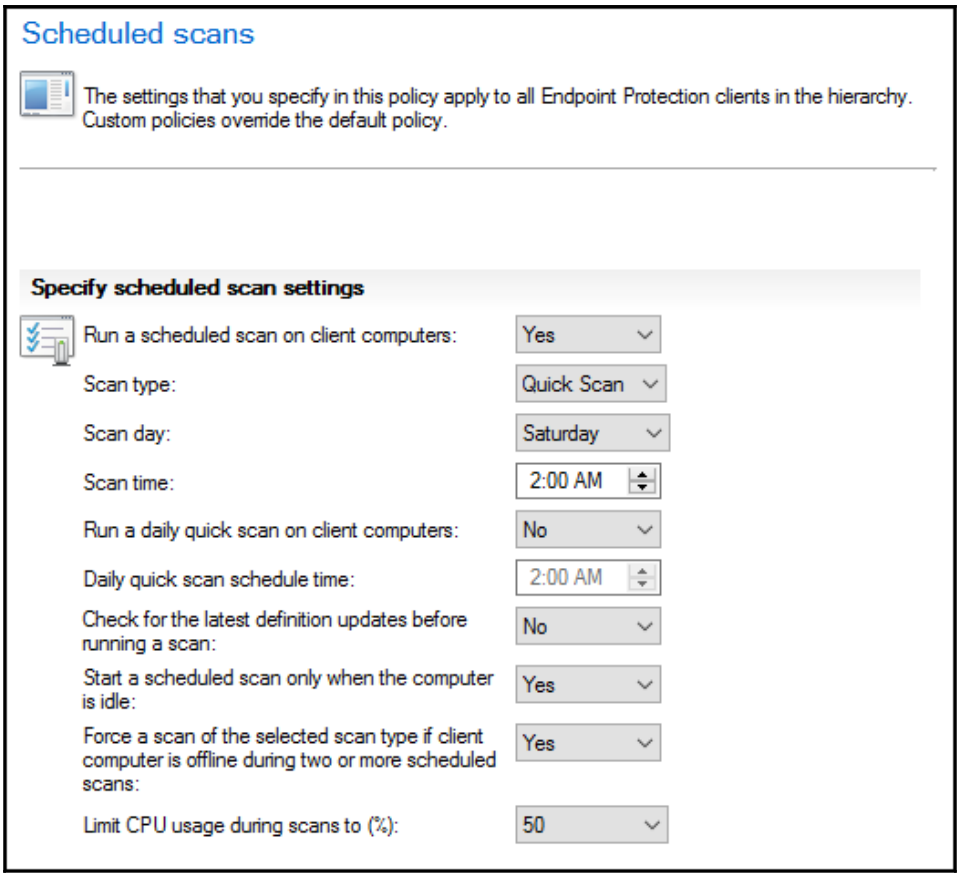


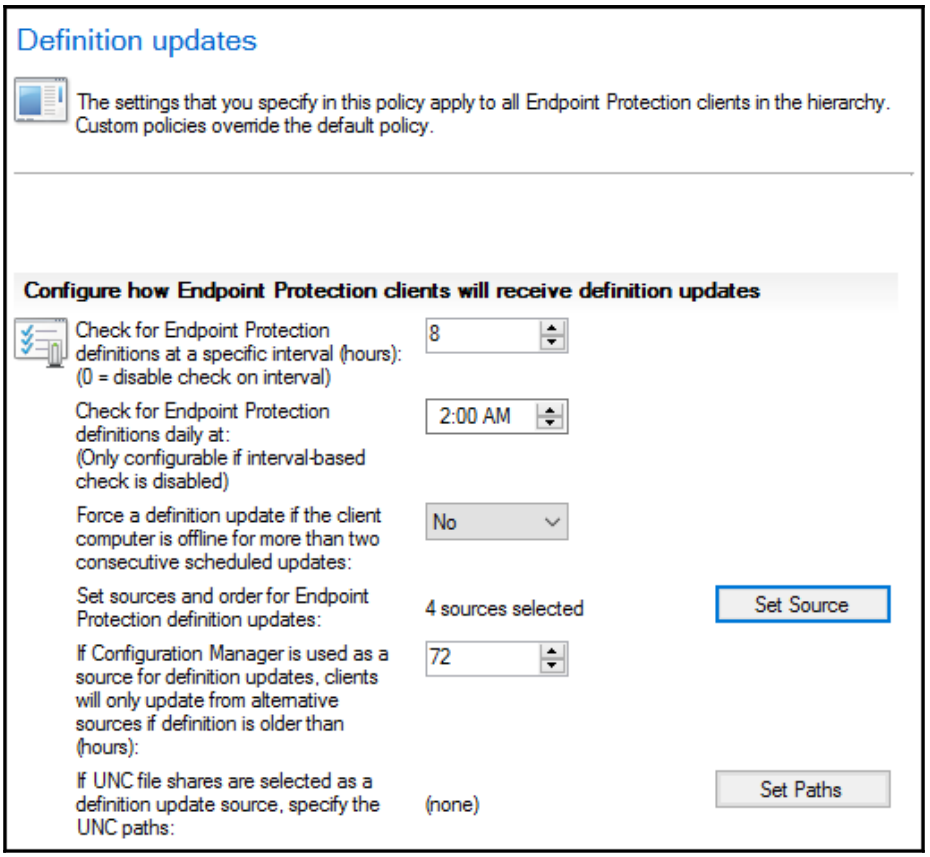



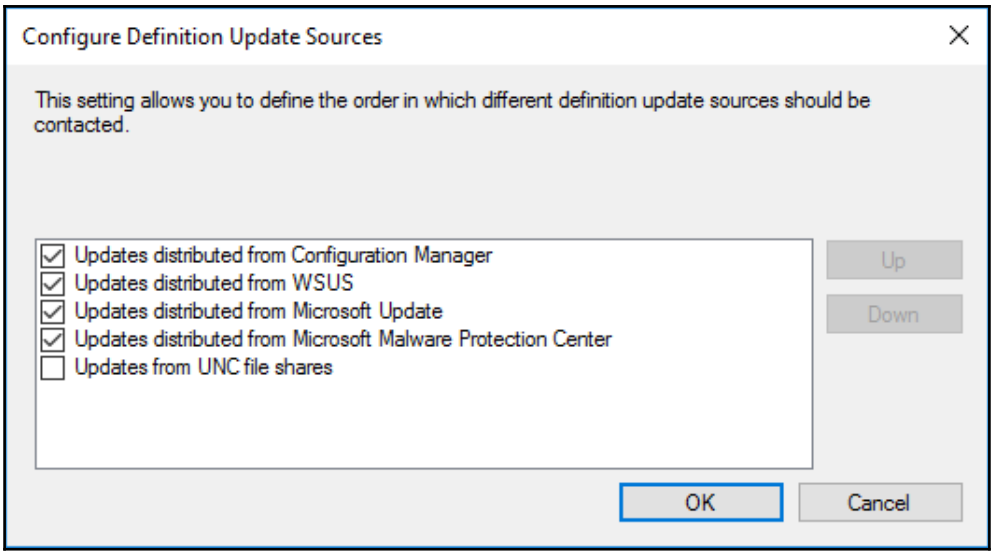

Specify Cloud Protection Service membership type
The Cloud Protection Service membership type you choose will be applied to all Endpoint Protection antimalware policies. Cloud Protection Service is a worldwide online community that includes System Center Endpoint Protection users. By joining Cloud Protection Service, System Center Endpoint Protection will automatically send information to Microsoft to help Microsoft determine which software to investigate for potential threats and to help improve System Center Endpoint Protection's effectiveness. This community also helps stop the spread of new malicious software infections.
You can choose to join the Cloud Protection Service community with either a Basic or Advanced membership. The type of information that is sent in reports to Microsoft depends on your level of Cloud Protection Service membership. In some instances, personal information might unintentionally be sent to Microsoft. However, Microsoft will not use this information to identify you or to contact you.
To learn more about Basic and Advanced Memberships and the information collected by the Reports, see the Privacy Statement at http://go.microsoft.com/fwlink/?LinkID=626987.
Do not join Cloud Protection Service
Basic membership (on Windows 10 and above, the behavior is the same as advanced membership)
Advanced membership

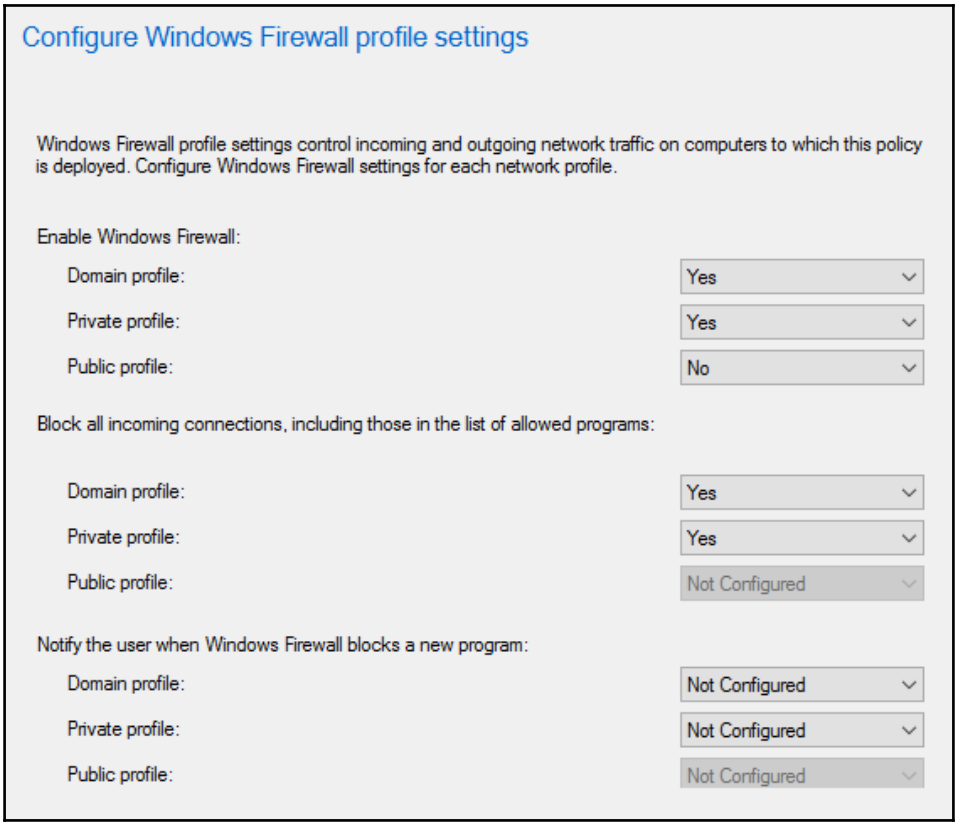

Default Settings
Specify settings that apply to all clients in the hierarchy, and can be modified by custom settings.
Select whether to manage existing Endpoint Protection clients or to install Endpoint Protection on clients.
Device Settings
Manage Endpoint Protection client on client computers
No
Install Endpoint Protection client on client computers
Yes
Automatically remove previously installed antimalware software before Endpoint Protection is installed
Yes
Allow Endpoint Protection client installation and restarts outside maintenance windows. Maintenance windows must be at least 30 minutes long for client installation.
No
For Windows Embedded devices with write filters, commit Endpoint Protection client installation (requires restarts)
Yes
Suppress any required computer restarts after the Endpoint Protection client is installed
Yes
Allowed period of time users can postpone a required restart to complete the Endpoint Protection installation (hours)
24
Disable alternate sources (such as Microsoft Windows Update, Microsoft Windows Server Update Services, or UNC shares) for the initial definition update on client computers
Yes

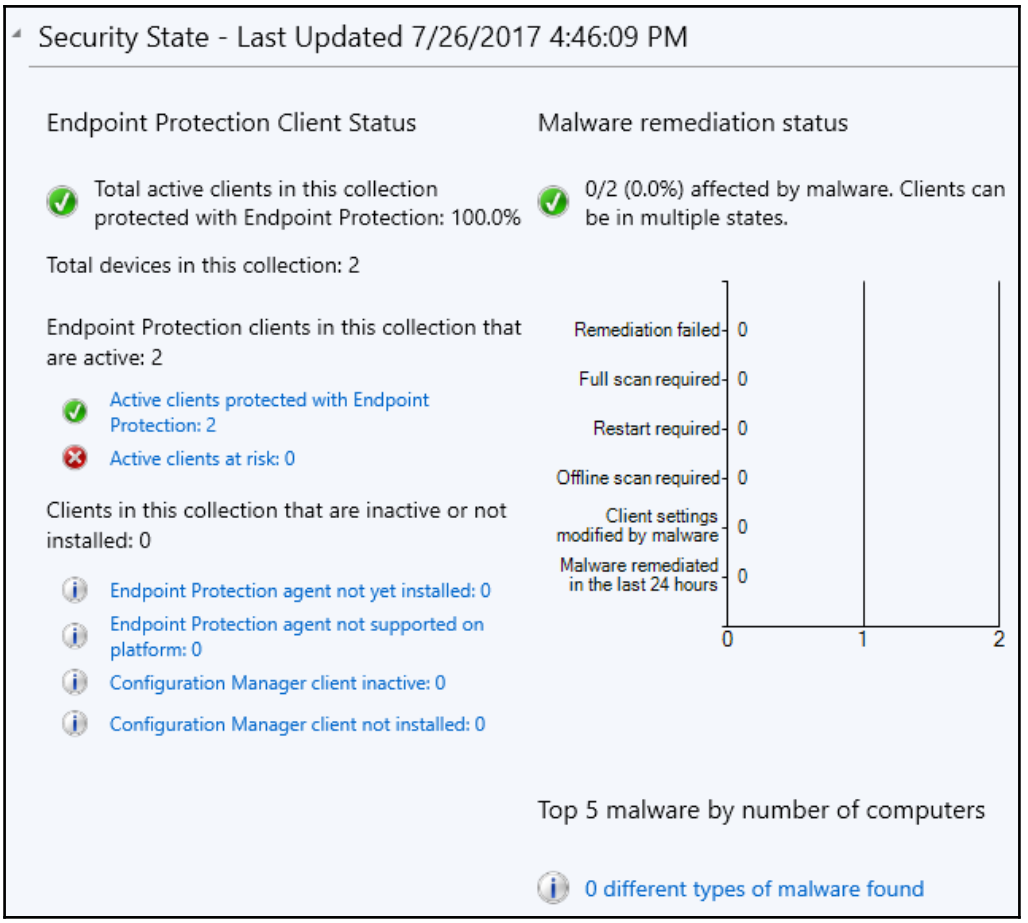

Select the property filters and search criteria
The software updates that meet the specified criteria are added to the associated software update group.
Property filters:
Article ID
Bulletin ID
Content Size (KB)
Custom Severity
Date Released or Revised
Description
Language
Product
Required
Search criteria:
Product "Forefront Endpoint Protection 2010" OR "Windows Defender"
Update Classification "Critical Updates" OR "Definition Updates"

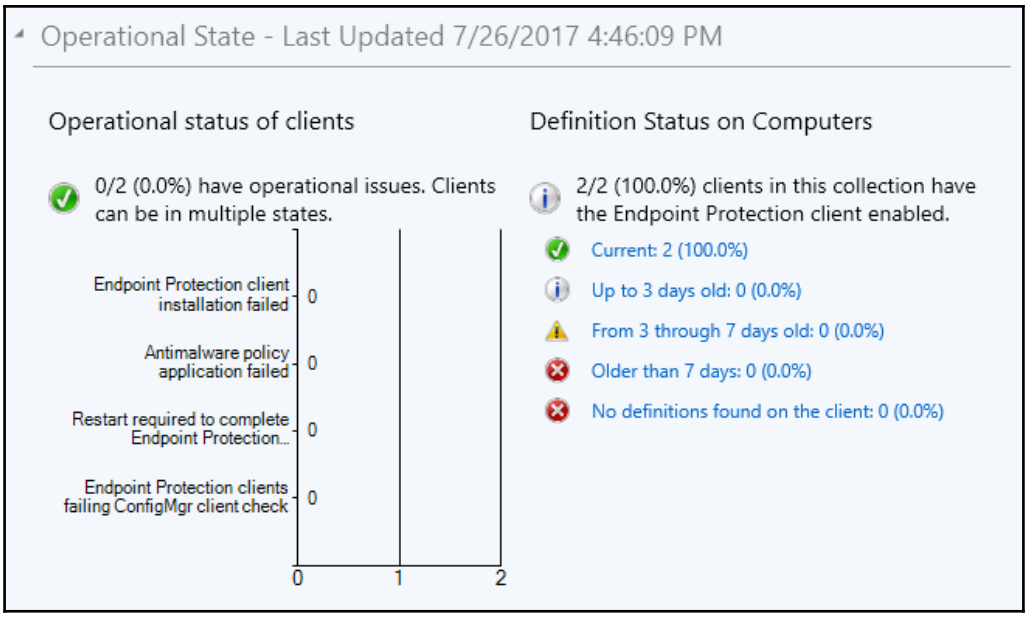

Scheduled scans
The settings that you specify in this policy apply to all Endpoint Protection clients in the hierarchy. Custom policies override the default policy.
Specify scheduled scan settings
Run a scheduled scan on client computers:
Yes
Scan type:
Quick Scan
Scan day:
Saturday
Scan time:
2:00 AM
Run a daily quick scan on client computers:
No
Daily quick scan schedule time:
2:00 AM
Check for the latest definition updates before running a scan:
No
Start a scheduled scan only when the computer is idle:
Yes
Force a scan of the selected scan type if client computer is offline during two or more scheduled scans:
Yes
Limit CPU usage during scans to (%):
50

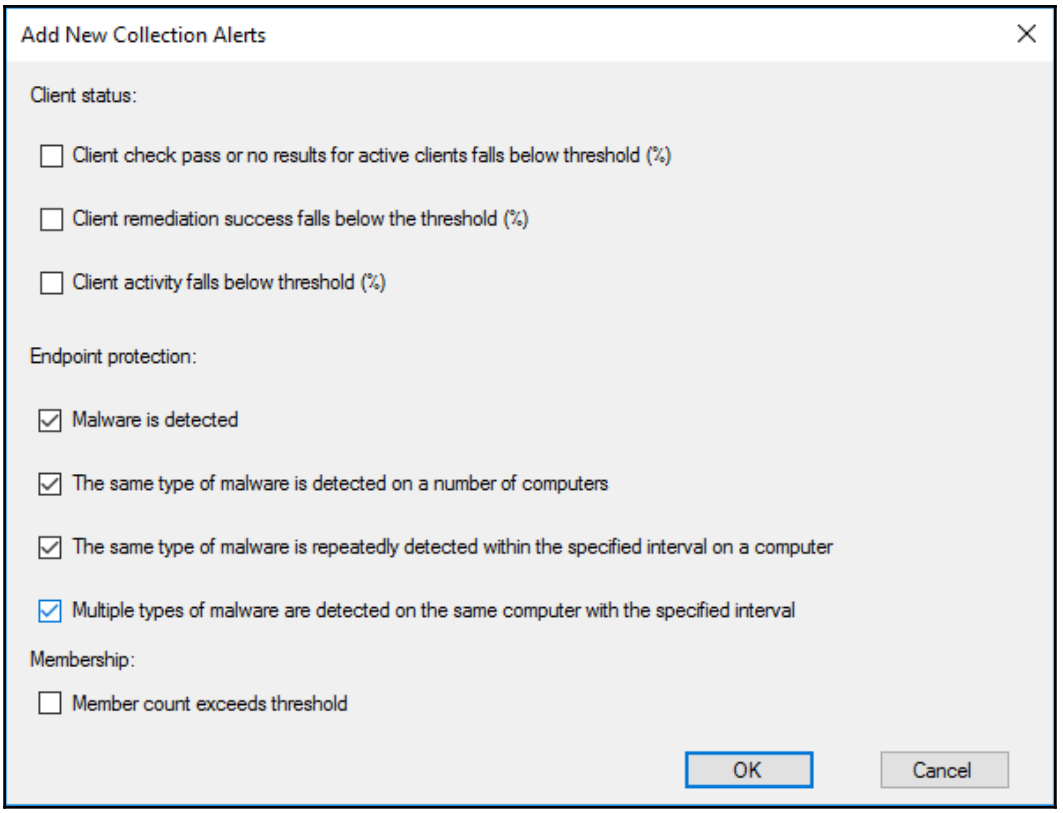

Definition updates
The settings that you specify in this policy apply to all Endpoint Protection clients in the hierarchy. Custom policies override the default policy.
Configure how Endpoint Protection clients will receive definition updates
Check for Endpoint Protection definitions at a specific interval (hours): (0 = disable check on interval)
8
Check for Endpoint Protection definitions daily at: (Only configurable if interval-based check is disabled)
2:00 AM
Force a definition update if the client computer is offline for more than two consecutive scheduled updates:
No
Set sources and order for Endpoint Protection definition updates:
4 sources selected
Set Source
If Configuration Manager is used as a source for definition updates, clients will only update from alternative sources if definition is older than (hours):
72
If UNC file shares are selected as a definition update source, specify the UNC paths:
(none)
Set Paths

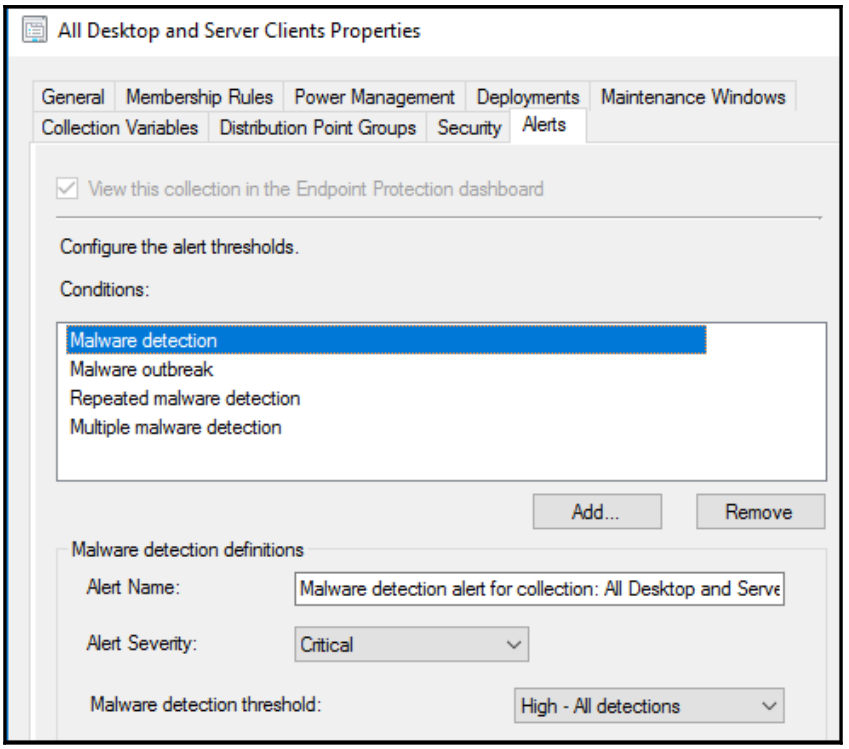

Configure Definition Update Sources
This setting allows you to define the order in which different definition update sources should be contacted.
Updates distributed from Configuration Manager
Updates distributed from WSUS
Updates distributed from Microsoft Update
Updates distributed from Microsoft Malware Protection Center
Updates from UNC file shares
Up
Down
OK
Cancel


Configure Windows Firewall profile settings
Windows Firewall profile settings control incoming and outgoing network traffic on computers to which this policy is deployed. Configure Windows Firewall settings for each network profile.
Enable Windows Firewall:
Domain profile: Yes
Private profile: Yes
Public profile: No
Block all incoming connections, including those in the list of allowed programs:
Domain profile: Yes
Private profile: Yes
Public profile: Not Configured
Notify the user when Windows Firewall blocks a new program:
Domain profile: Not Configured
Private profile: Not Configured
Public profile: Not Configured

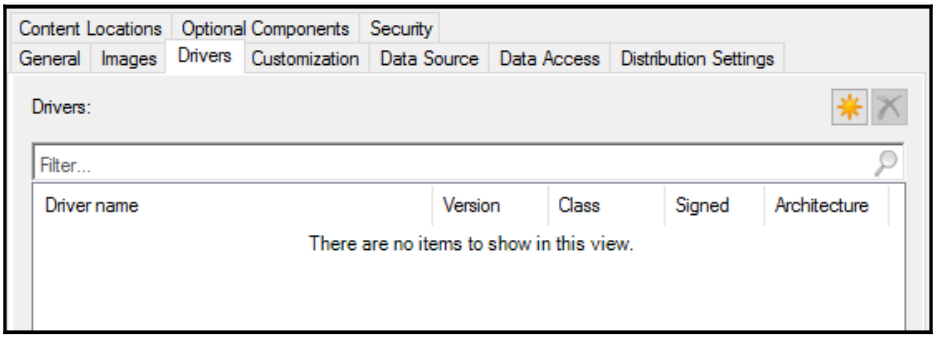

Security State - Last Updated 7/26/2017 4:46:09 PM
Endpoint Protection Client Status
Total active clients in this collection protected with Endpoint Protection: 100.0%
Total devices in this collection: 2
Endpoint Protection clients in this collection that are active: 2
Active clients protected with Endpoint Protection: 2
Active clients at risk: 0
Clients in this collection that are inactive or not installed: 0
Endpoint Protection agent not yet installed: 0
Endpoint Protection agent not supported on platform: 0
Configuration Manager client inactive: 0
Configuration Manager client not installed: 0
Malware remediation status
0/2 (0.0%) affected by malware. Clients can be in multiple states.
Remediation failed 0
Full scan required 0
Restart required 0
Offline scan required 0
Client settings modified by malware 0
Malware remediated in the last 24 hours 0
0
1
2
Top 5 malware by number of computers
0 different types of malware found

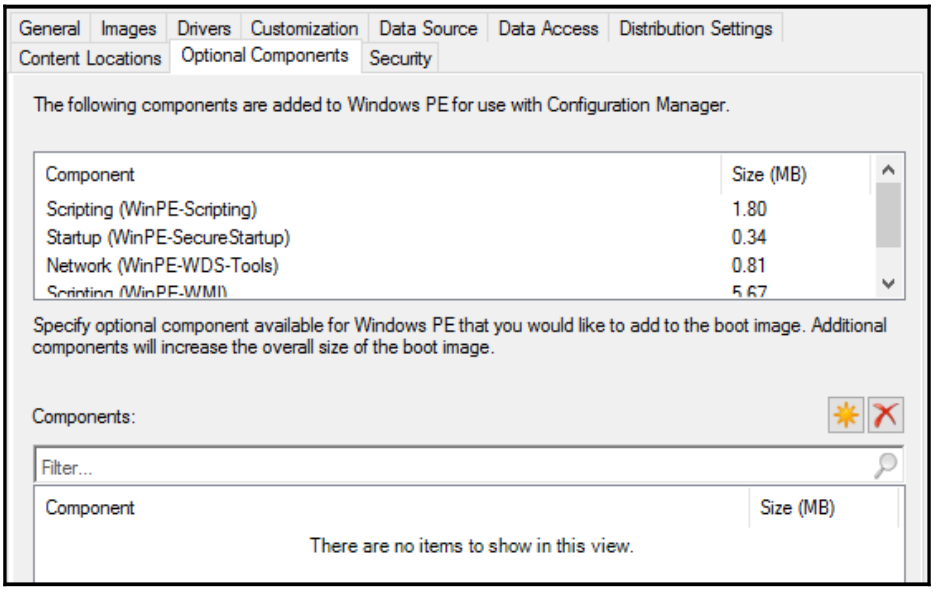

Operational State - Last Updated 7/26/2017 4:46:09 PM
Operational status of clients
0/2 (0.0%) have operational issues. Clients can be in multiple states.
Endpoint Protection client installation failed
0
Antimalware policy application failed
0
Restart required to complete Endpoint Protection...
0
Endpoint Protection clients failing ConfigMgr client check
0
0
1
2
Definition Status on Computers
2/2 (100.0%) clients in this collection have the Endpoint Protection client enabled.
Current: 2 (100.0%)
Up to 3 days old: 0 (0.0%)
From 3 through 7 days old: 0 (0.0%)
Older than 7 days: 0 (0.0%)
No definitions found on the client: 0 (0.0%)

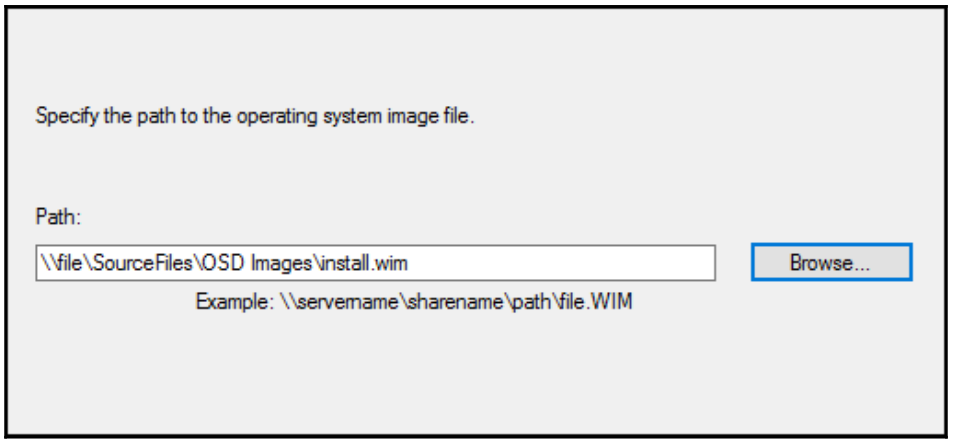

Add New Collection Alerts
Client status:
Client check pass or no results for active clients falls below threshold (%)
Client remediation success falls below the threshold (%)
Client activity falls below threshold (%)
Endpoint protection:
Malware is detected
The same type of malware is detected on a number of computers
The same type of malware is repeatedly detected within the specified interval on a computer
Multiple types of malware are detected on the same computer with the specified interval
Membership:
Member count exceeds threshold
OK
Cancel

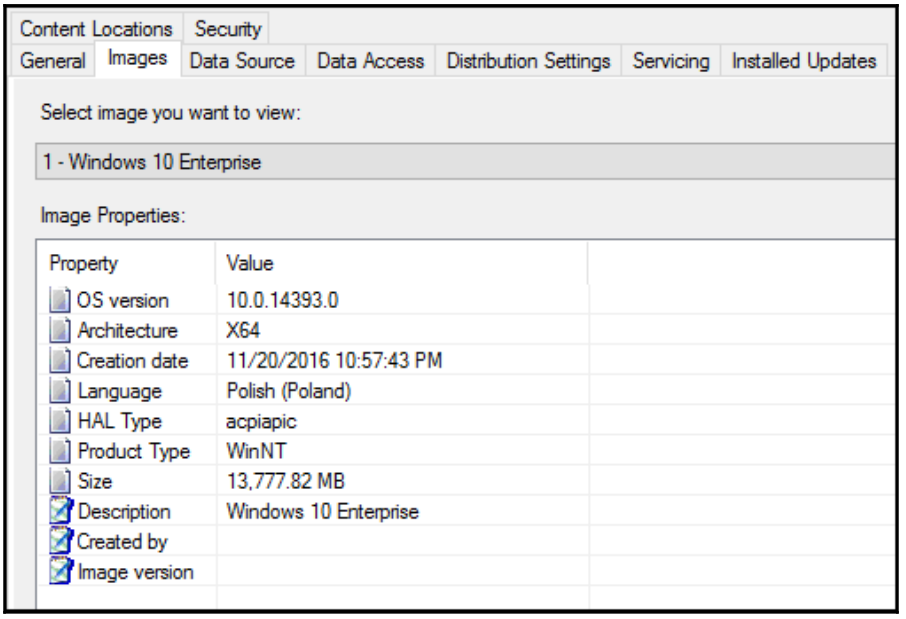

All Desktop and Server Clients Properties
General
Membership Rules
Power Management
Deployments
Maintenance Windows
Collection Variables
Distribution Point Groups
Security
Alerts
View this collection in the Endpoint Protection dashboard
Configure the alert thresholds.
Conditions:
Malware detection
Malware outbreak
Repeated malware detection
Multiple malware detection
Add...
Remove
Malware detection definitions
Alert Name:
Malware detection alert for collection: All Desktop and Serve
Alert Severity:
Critical
Malware detection threshold:
High - All detections

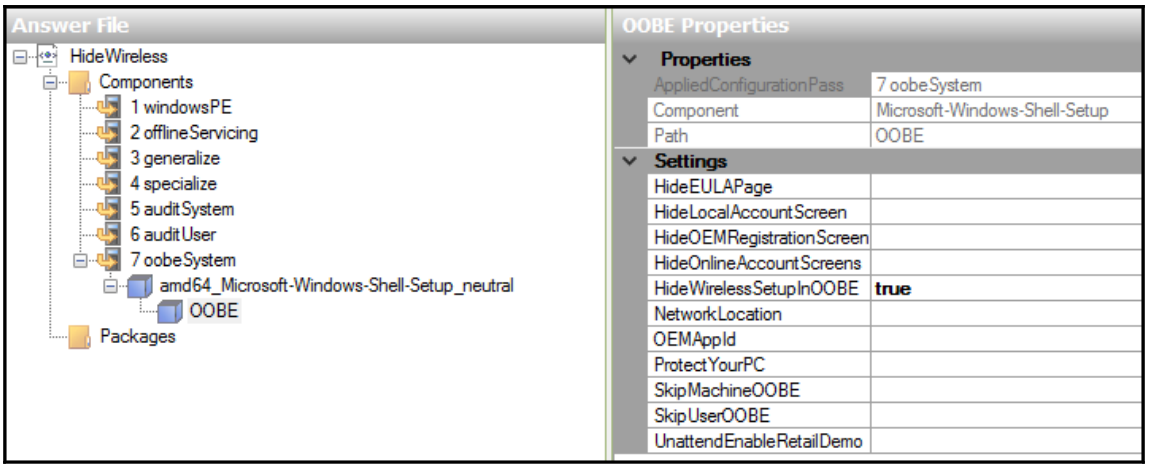
# Chapter 10: Operating System Deployment

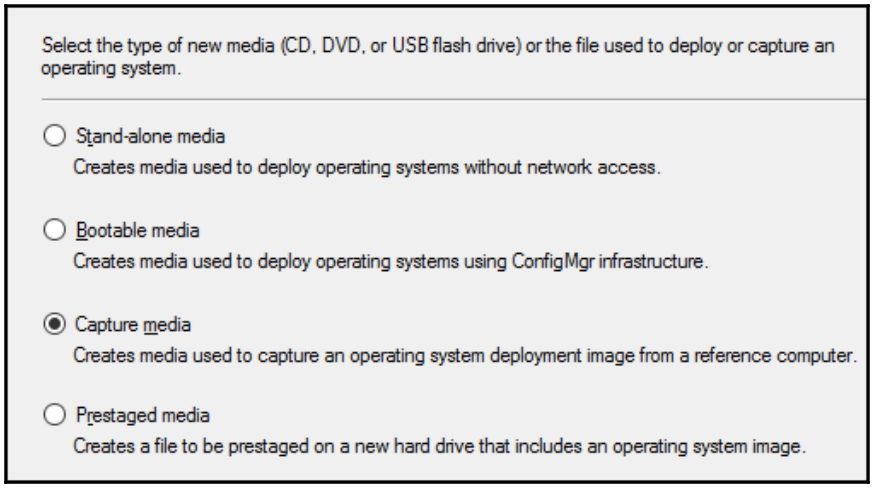


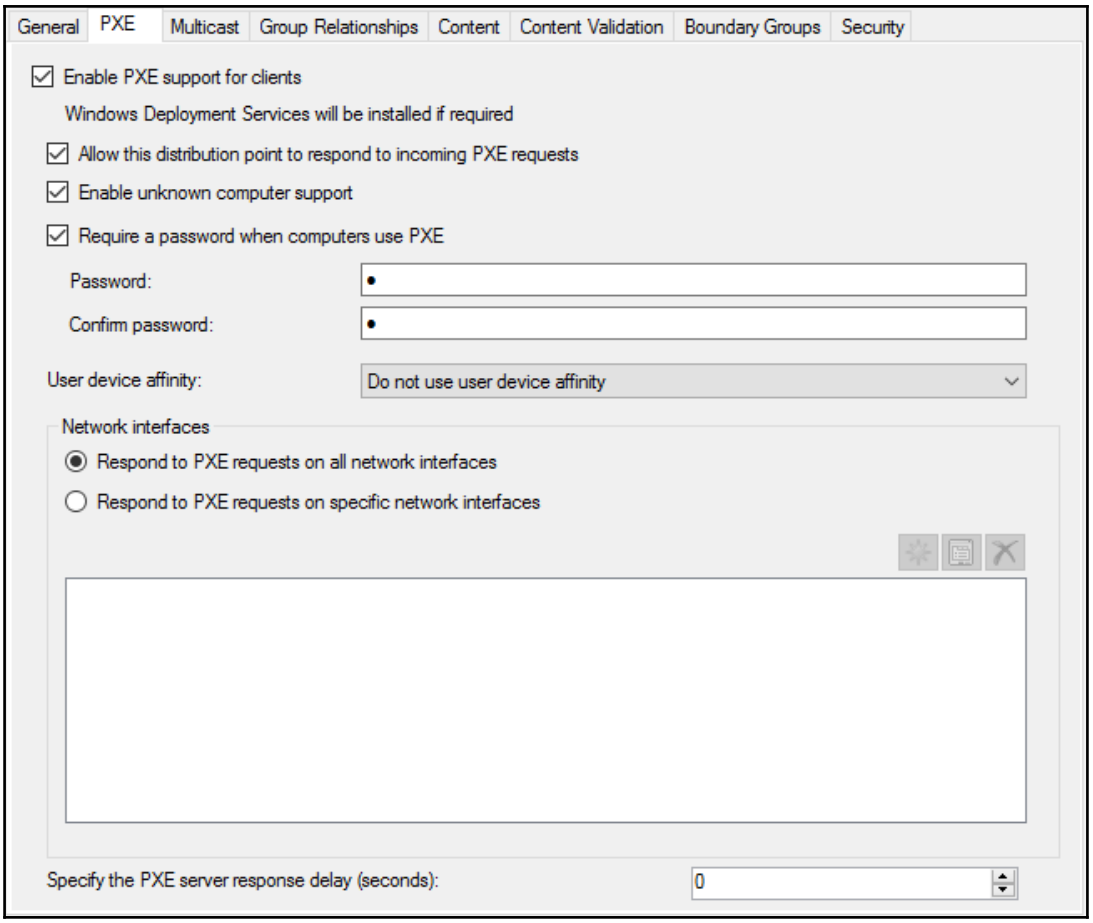



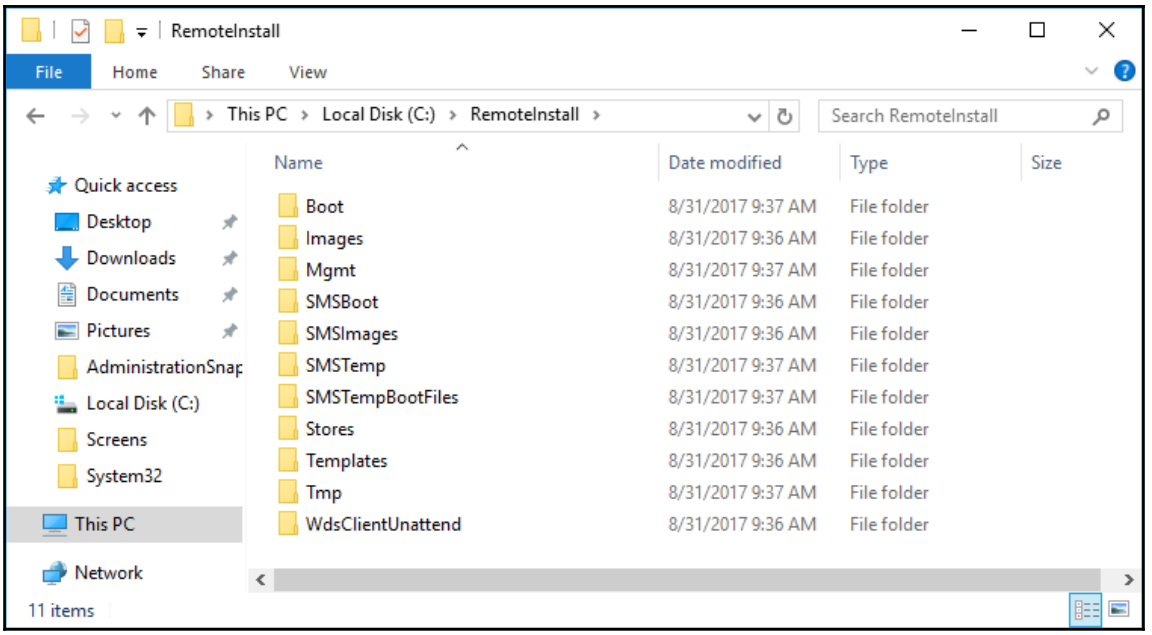

Specify the path to the operating system image file.
Path:
\\file\SourceFiles\OSD Images\install.wim
Browse...
Example: \\servername\sharename\path\file.WIM

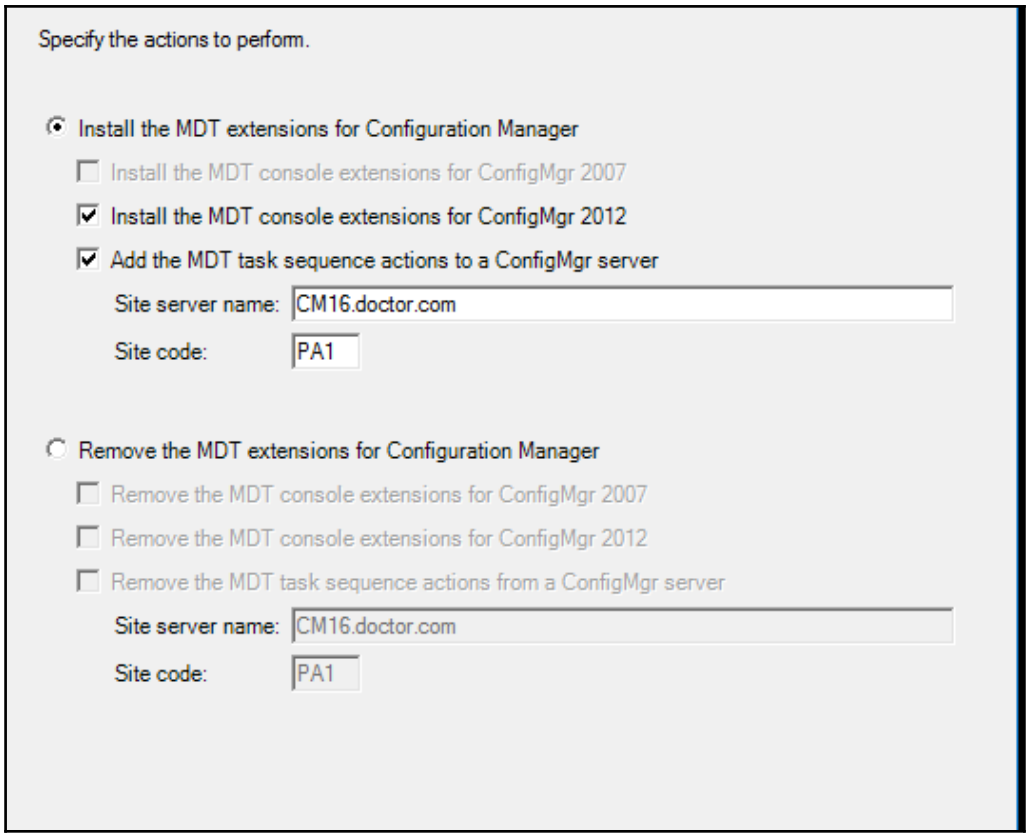

Content Locations
Security
General
Images
Data Source
Data Access
Distribution Settings
Servicing
Installed Updates
Select image you want to view:
1 - Windows 10 Enterprise
Image Properties:
Property
Value
OS version
10.0.14393.0
Architecture
X64
Creation date
11/20/2016 10:57:43 PM
Language
Polish (Poland)
HAL Type
acpiapic
Product Type
WinNT
Size
13,777.82 MB
Description
Windows 10 Enterprise
Created by
Image version

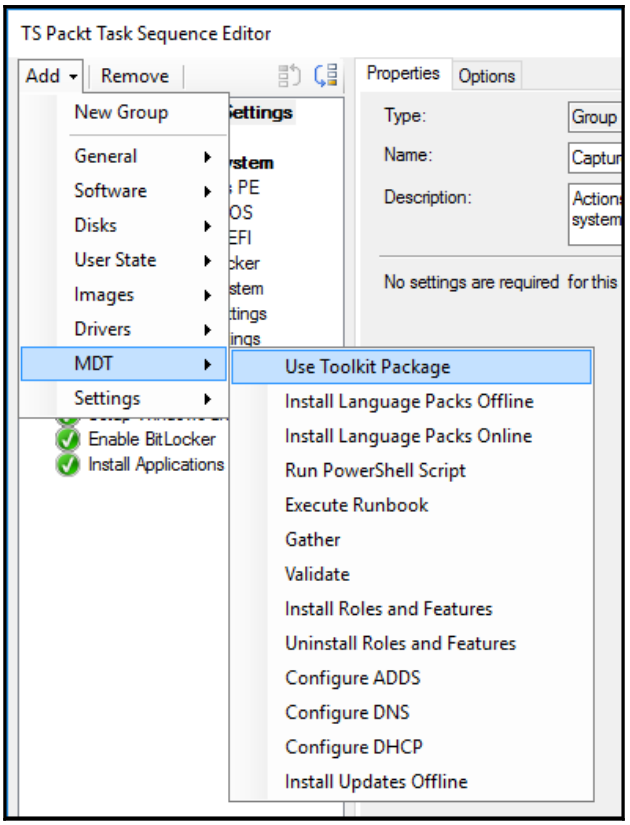

Answer File
HideWireless
Components
1 windowsPE
2 offlineServicing
3 generalize
4 specialize
5 auditSystem
6 auditUser
7 oobeSystem
amd64_Microsoft-Windows-Shell-Setup_neutral
OOBE
Packages
OOBE Properties
Properties
AppliedConfigurationPass
7 oobeSystem
Component
Microsoft-Windows-Shell-Setup
Path
OOBE
Settings
HideEULAPage
HideLocalAccountScreen
HideOEMRegistrationScreen
HideOnlineAccountScreens
HideWirelessSetupInOOBE
true
NetworkLocation
OEMAppId
ProtectYourPC
SkipMachineOOBE
SkipUserOOBE
UnattendEnableRetailDemo

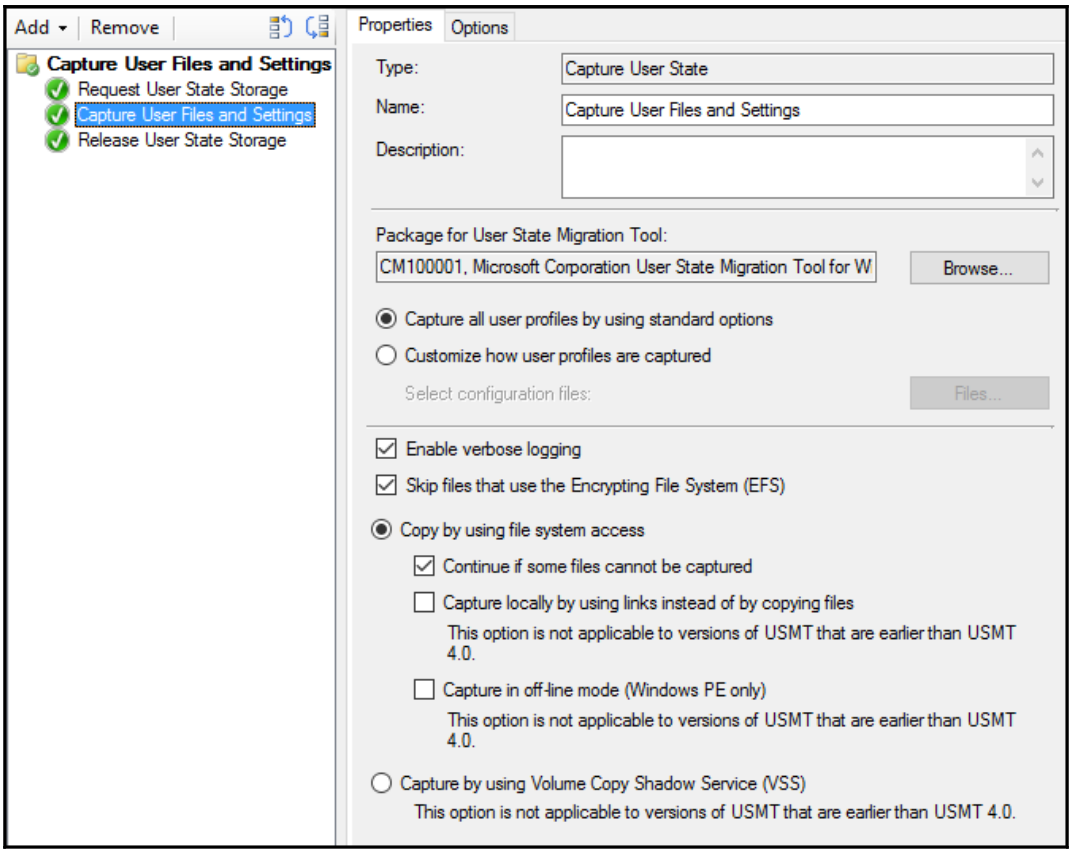

Select the type of new media (CD, DVD, or USB flash drive) or the file used to deploy or capture an operating system.
Stand-alone media
Creates media used to deploy operating systems without network access.
Bootable media
Creates media used to deploy operating systems using ConfigMgr infrastructure.
Capture media
Creates media used to capture an operating system deployment image from a reference computer.
Prestaged media
Creates a file to be prestaged on a new hard drive that includes an operating system image.

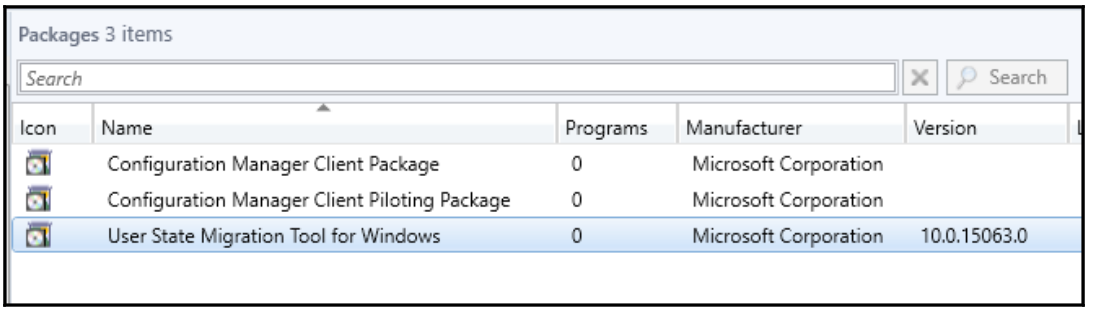

General
PXE
Multicast
Group Relationships
Content
Content Validation
Boundary Groups
Security
Enable PXE support for clients
Windows Deployment Services will be installed if required
Allow this distribution point to respond to incoming PXE requests
Enable unknown computer support
Require a password when computers use PXE
Password:
Confirm password:
User device affinity:
Do not use user device affinity
Network interfaces
Respond to PXE requests on all network interfaces
Respond to PXE requests on specific network interfaces
Specify the PXE server response delay (seconds):
0

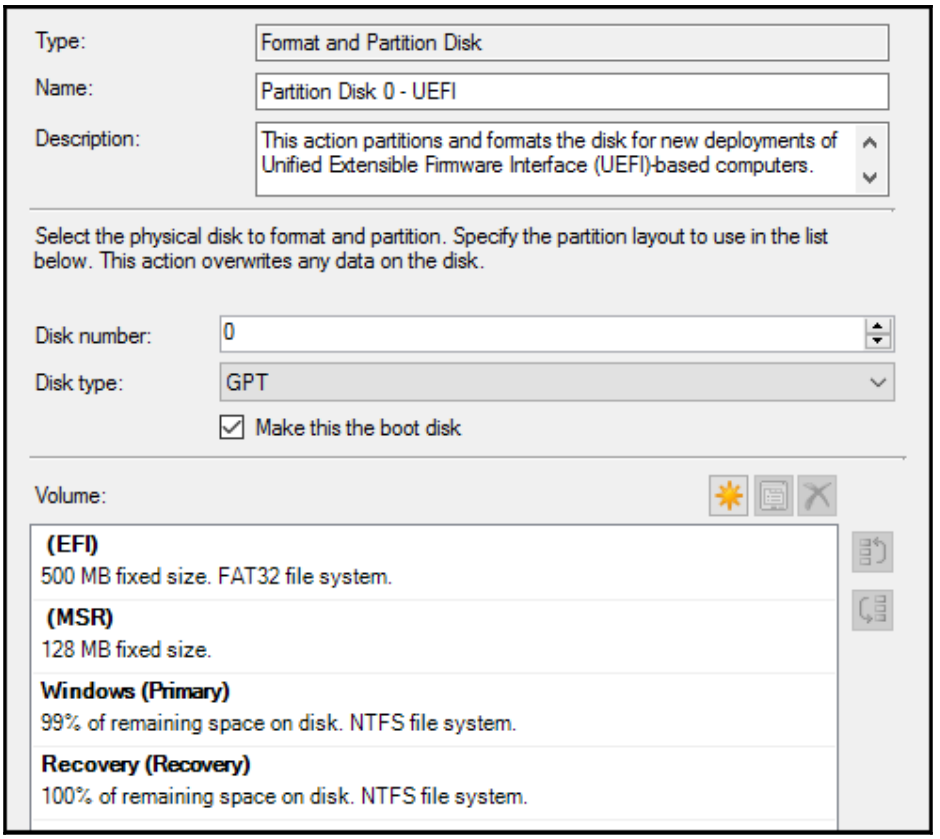

RemoteInstall
File
Home
Share
View
This PC
Local Disk (C:)
RemoteInstall
Search RemoteInstall
Quick access
Desktop
Downloads
Documents
Pictures
AdministrationSnap
Local Disk (C:)
Screens
System32
This PC
Network
Name
Date modified
Type
Size
Boot 8/31/2017 9:37 AM File folder
Images 8/31/2017 9:36 AM File folder
Mgmt 8/31/2017 9:37 AM File folder
SMSBoot 8/31/2017 9:36 AM File folder
SMSImages 8/31/2017 9:36 AM File folder
SMSTemp 8/31/2017 9:37 AM File folder
SMSTempBootFiles 8/31/2017 9:37 AM File folder
Stores 8/31/2017 9:36 AM File folder
Templates 8/31/2017 9:36 AM File folder
Tmp 8/31/2017 9:37 AM File folder
WdsClientUnattend 8/31/2017 9:36 AM File folder
11 items

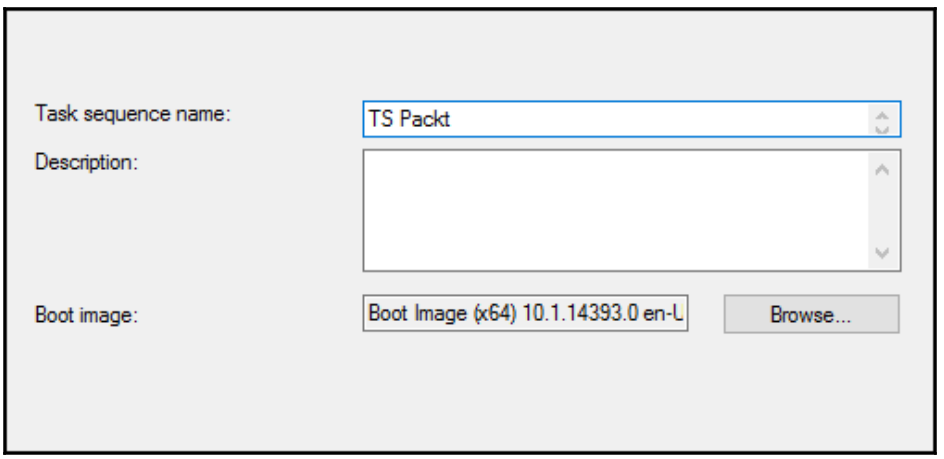

Specify the actions to perform.
Install the MDT extensions for Configuration Manager
Install the MDT console extensions for ConfigMgr 2007
Install the MDT console extensions for ConfigMgr 2012
Add the MDT task sequence actions to a ConfigMgr server
Site server name:
CM16.doctor.com
Site code:
PA1
Remove the MDT extensions for Configuration Manager
Remove the MDT console extensions for ConfigMgr 2007
Remove the MDT console extensions for ConfigMgr 2012
Remove the MDT task sequence actions from a ConfigMgr server
Site server name:
CM16.doctor.com
Site code:
PA1

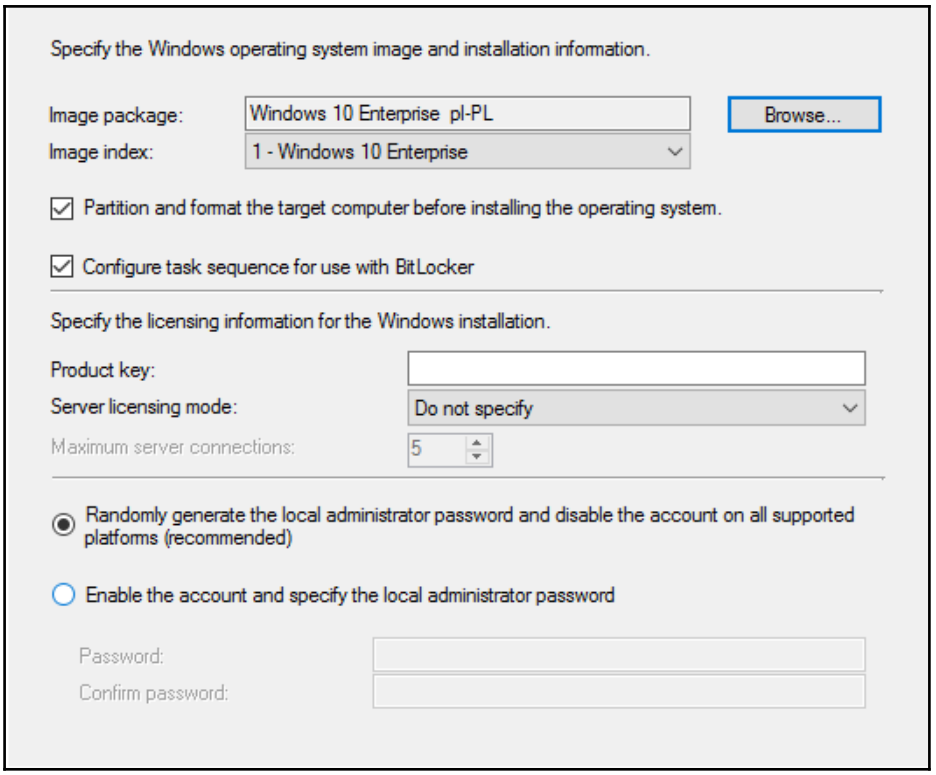

TS Packt Task Sequence Editor
Add
Remove
Properties
Options
New Group
General
Software
Disks
User State
Images
Drivers
MDT
Settings
Type:
Group
Name:
Description:
No settings are required for this
Enable BitLocker
Install Applications
Use Toolkit Package
Install Language Packs Offline
Install Language Packs Online
Run PowerShell Script
Execute Runbook
Gather
Validate
Install Roles and Features
Uninstall Roles and Features
Configure ADDS
Configure DNS
Configure DHCP
Install Updates Offline

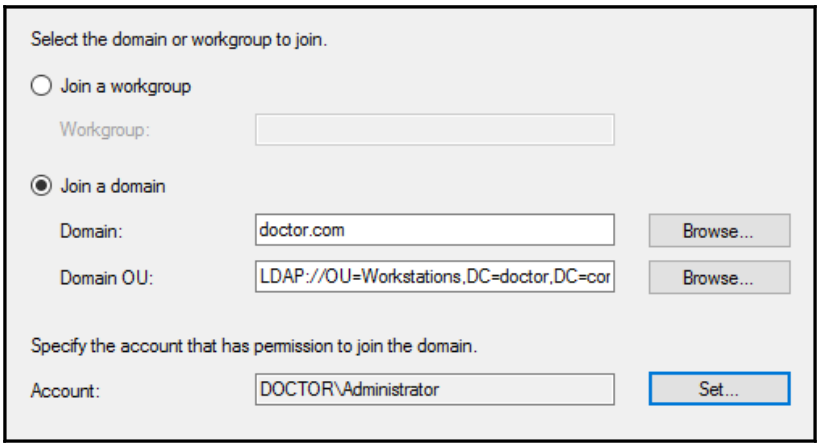

Add
Remove
Capture User Files and Settings
Request User State Storage
Capture User Files and Settings
Release User State Storage
Properties
Options
Type:
Capture User State
Name:
Capture User Files and Settings
Description:
Package for User State Migration Tool:
CM100001, Microsoft Corporation User State Migration Tool for W
Browse...
Capture all user profiles by using standard options
Customize how user profiles are captured
Select configuration files:
Files...
Enable verbose logging
Skip files that use the Encrypting File System (EFS)
Copy by using file system access
Continue if some files cannot be captured
Capture locally by using links instead of by copying files
This option is not applicable to versions of USMT that are earlier than USMT 4.0.
Capture in off-line mode (Windows PE only)
This option is not applicable to versions of USMT that are earlier than USMT 4.0.
Capture by using Volume Copy Shadow Service (VSS)
This option is not applicable to versions of USMT that are earlier than USMT 4.0.

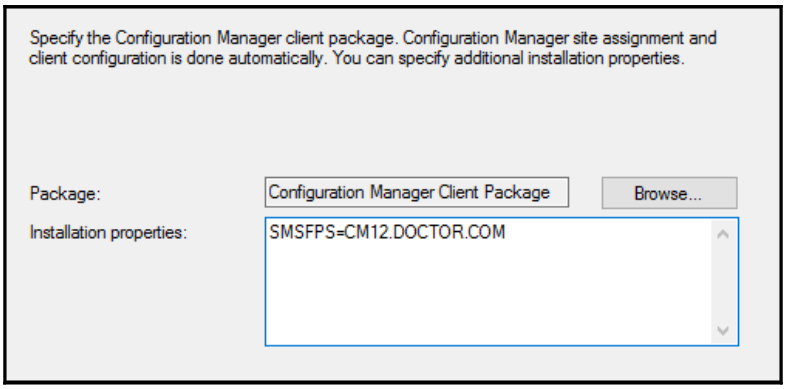

Packages 3 items
Search
Search
Icon
Name
Programs
Manufacturer
Version
Configuration Manager Client Package
0
Microsoft Corporation
Configuration Manager Client Piloting Package
0
Microsoft Corporation
User State Migration Tool for Windows
0
Microsoft Corporation
10.0.15063.0

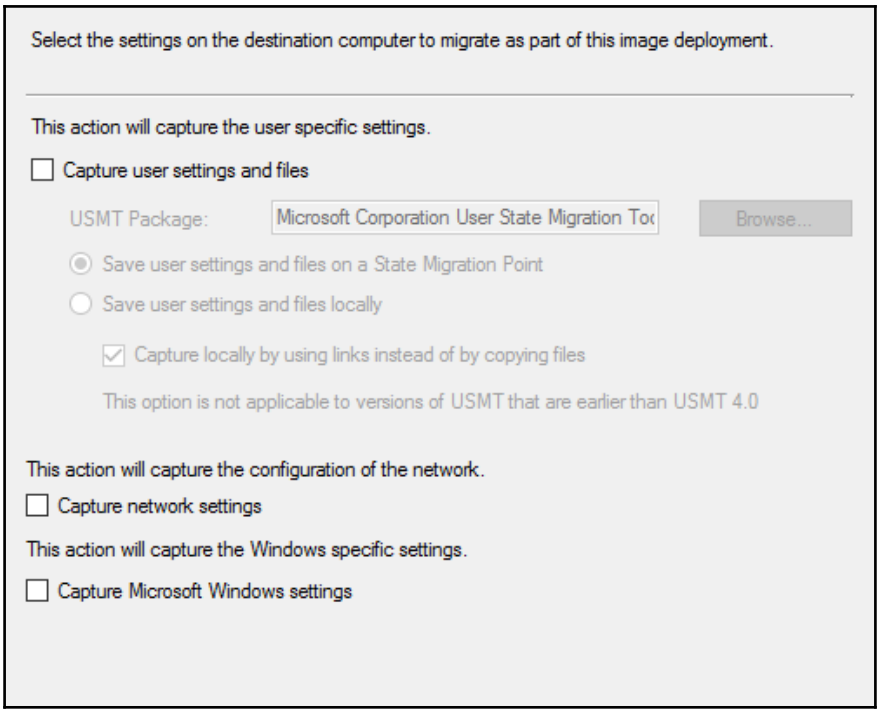

Type:
Format and Partition Disk
Name:
Partition Disk 0 - UEFI
Description:
This action partitions and formats the disk for new deployments of Unified Extensible Firmware Interface (UEFI)-based computers.
Select the physical disk to format and partition. Specify the partition layout to use in the list below. This action overwrites any data on the disk.
Disk number:
0
Disk type:
GPT
Make this the boot disk
Volume:
(EFI)
500 MB fixed size. FAT32 file system.
(MSR)
128 MB fixed size.
Windows (Primary)
99% of remaining space on disk. NTFS file system.
Recovery (Recovery)
100% of remaining space on disk. NTFS file system.

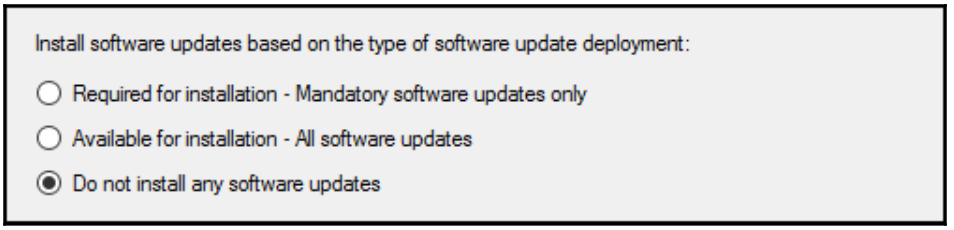

Task sequence name:
TS Packt
Description:
Boot image:
Boot Image (x64) 10.1.14393.0 en-L
Browse...

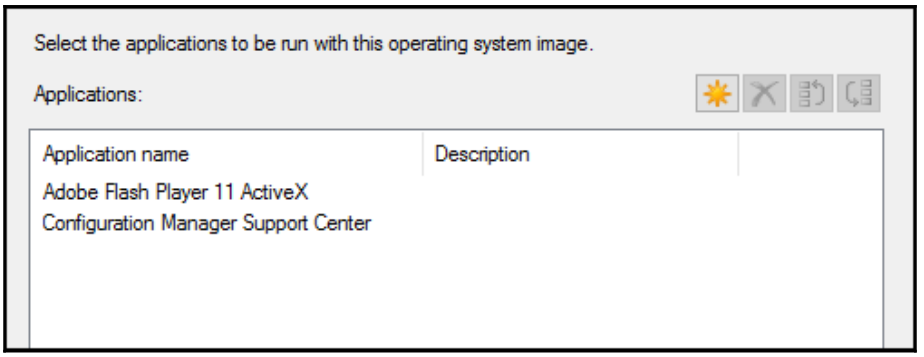

Specify the Windows operating system image and installation information.
Image package:
Windows 10 Enterprise pl-PL
Browse...
Image index:
1 - Windows 10 Enterprise
Partition and format the target computer before installing the operating system.
Configure task sequence for use with BitLocker
Specify the licensing information for the Windows installation.
Product key:
Server licensing mode:
Do not specify
Maximum server connections:
5
Randomly generate the local administrator password and disable the account on all supported platforms (recommended)
Enable the account and specify the local administrator password
Password:
Confirm password:

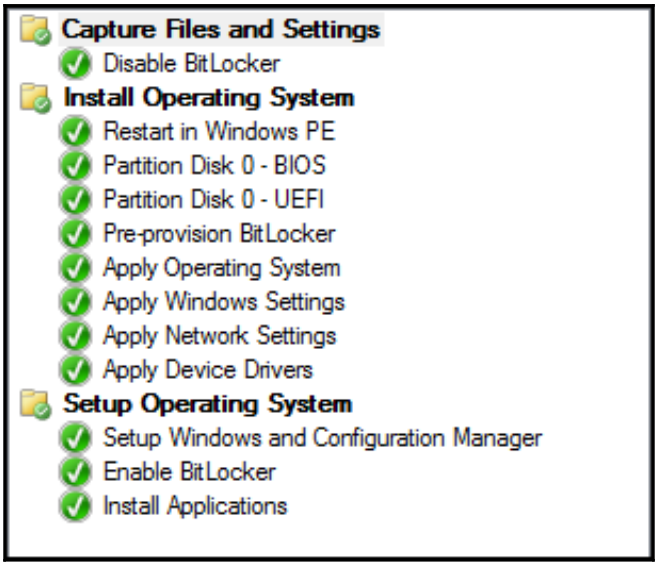

Select the domain or workgroup to join.
Join a workgroup
Workgroup:
Join a domain
Domain:
doctor.com
Browse...
Domain OU:
LDAP://OU=Workstations,DC=doctor,DC=cor
Browse...
Specify the account that has permission to join the domain.
Account:
DOCTOR\Administrator
Set...

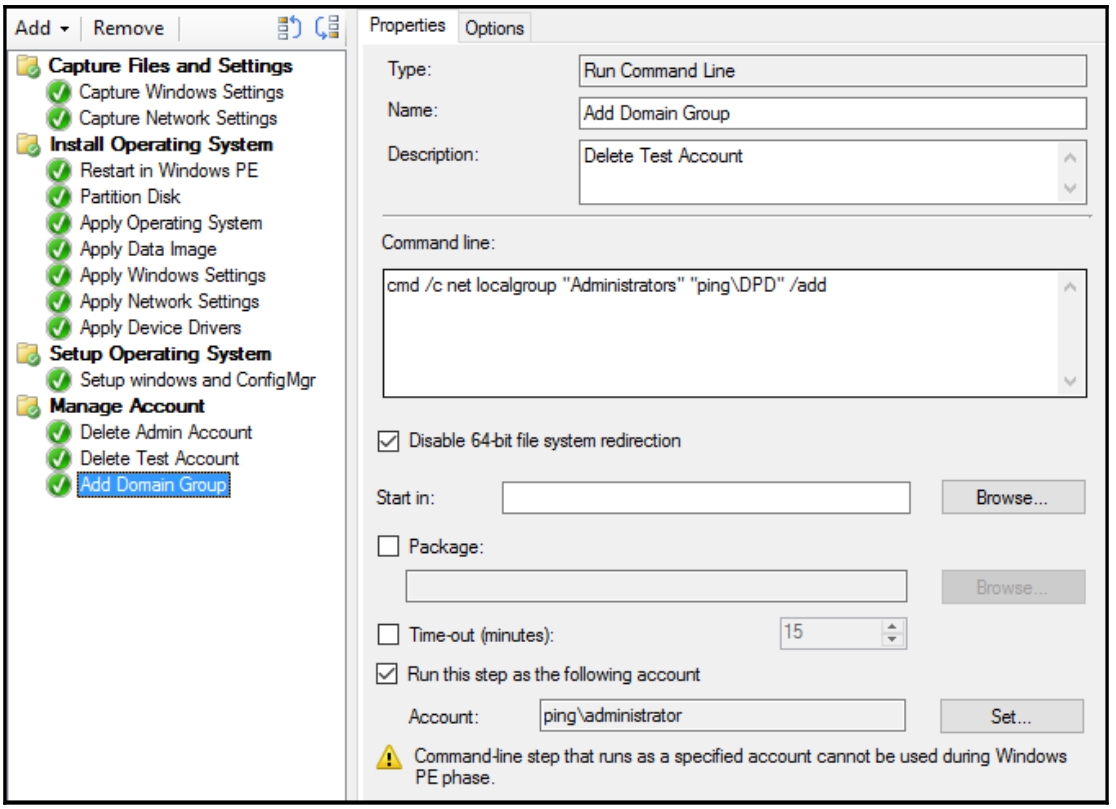

Specify the Configuration Manager client package. Configuration Manager site assignment and client configuration is done automatically. You can specify additional installation properties.
Package:
Configuration Manager Client Package
Browse...
Installation properties:
SMSFPS=CM12.DOCTOR.COM

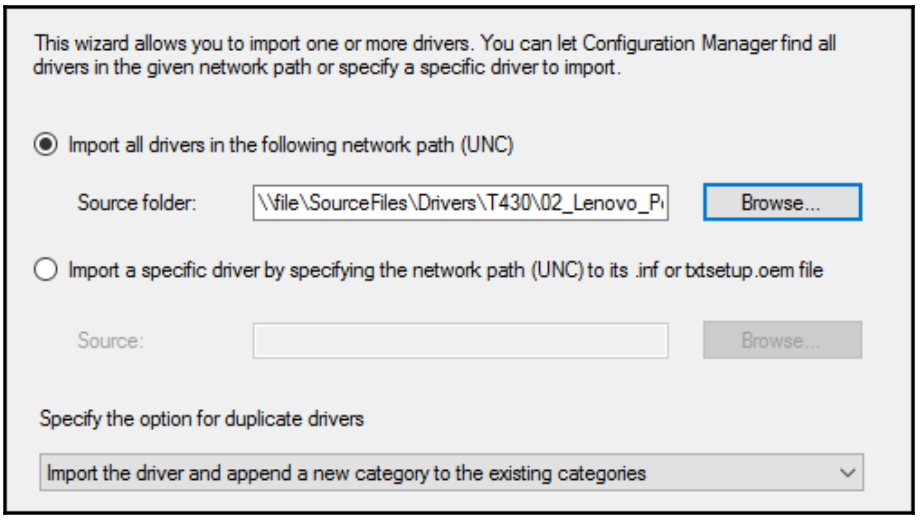

Select the settings on the destination computer to migrate as part of this image deployment.
This action will capture the user specific settings.
Capture user settings and files
USMT Package:
Microsoft Corporation User State Migration Too
Browse...
Save user settings and files on a State Migration Point
Save user settings and files locally
Capture locally by using links instead of by copying files
This option is not applicable to versions of USMT that are earlier than USMT 4.0
This action will capture the configuration of the network.
Capture network settings
This action will capture the Windows specific settings.
Capture Microsoft Windows settings

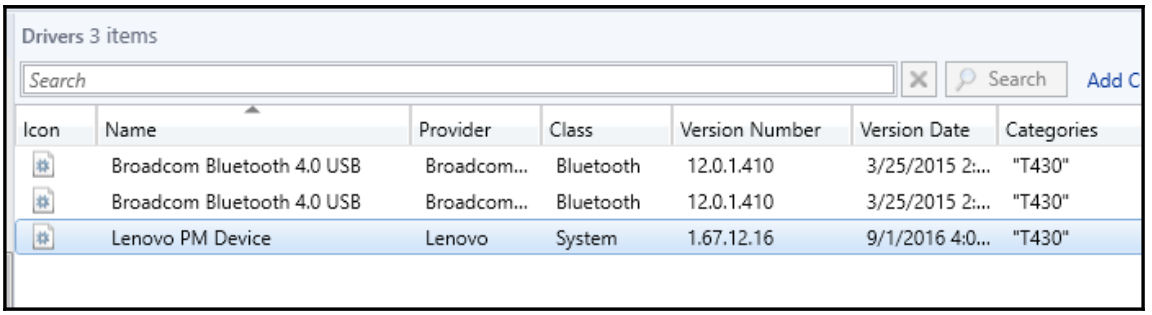

Install software updates based on the type of software update deployment:
Required for installation - Mandatory software updates only
Available for installation - All software updates
Do not install any software updates

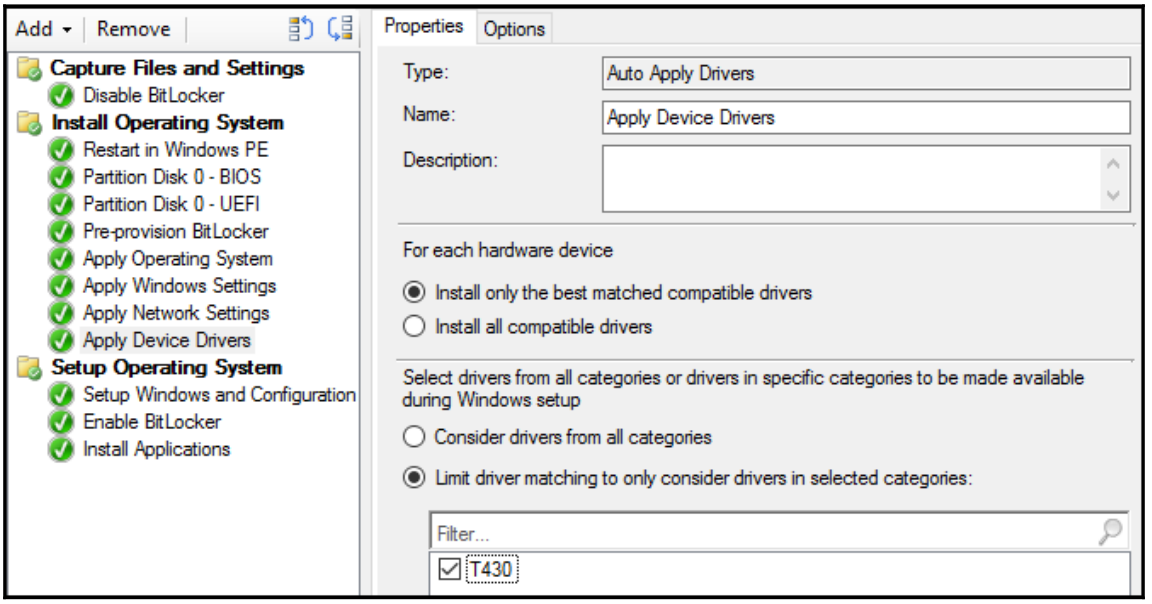

Select the applications to be run with this operating system image.
Applications:
Application name
Description
Adobe Flash Player 11 ActiveX
Configuration Manager Support Center

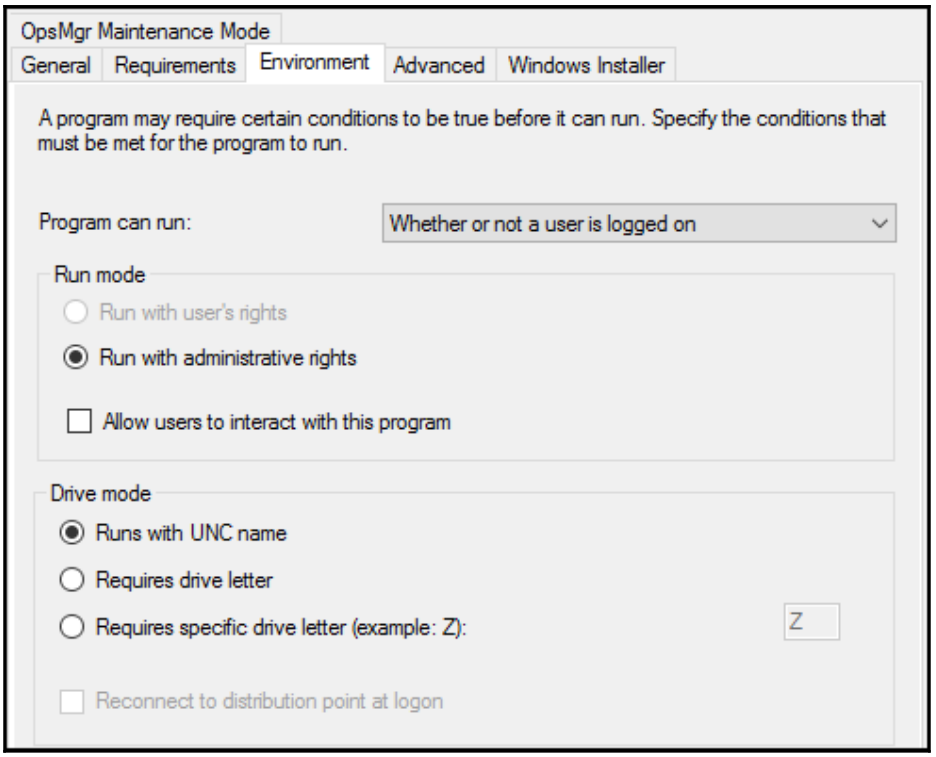

Capture Files and Settings
Disable BitLocker
Install Operating System
Restart in Windows PE
Partition Disk 0 - BIOS
Partition Disk 0 - UEFI
Pre-provision BitLocker
Apply Operating System
Apply Windows Settings
Apply Network Settings
Apply Device Drivers
Setup Operating System
Setup Windows and Configuration Manager
Enable BitLocker
Install Applications

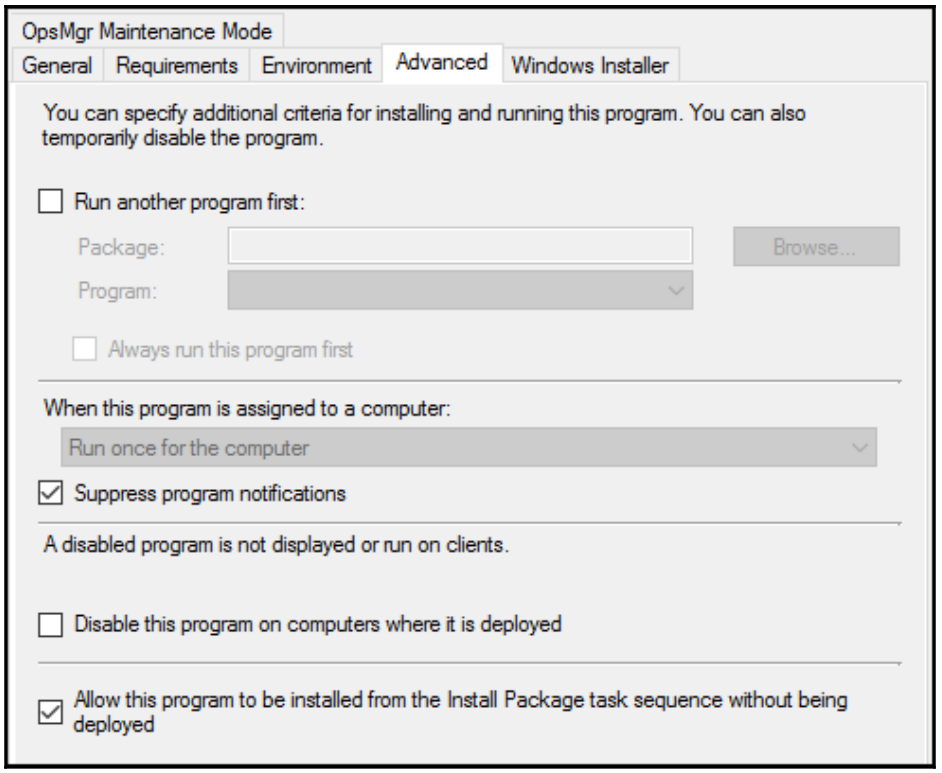

Add
Remove
Capture Files and Settings
Capture Windows Settings
Capture Network Settings
Install Operating System
Restart in Windows PE
Partition Disk
Apply Operating System
Apply Data Image
Apply Windows Settings
Apply Network Settings
Apply Device Drivers
Setup Operating System
Setup windows and ConfigMgr
Manage Account
Delete Admin Account
Delete Test Account
Add Domain Group
Properties
Options
Type:
Run Command Line
Name:
Add Domain Group
Description:
Delete Test Account
Command line:
cmd /c net localgroup "Administrators" "ping\DPD" /add
Disable 64-bit file system redirection
Start in:
Browse...
Package:
Browse...
Time-out (minutes):
15
Run this step as the following account
Account:
ping\administrator
Set...
Command-line step that runs as a specified account cannot be used during Windows PE phase.

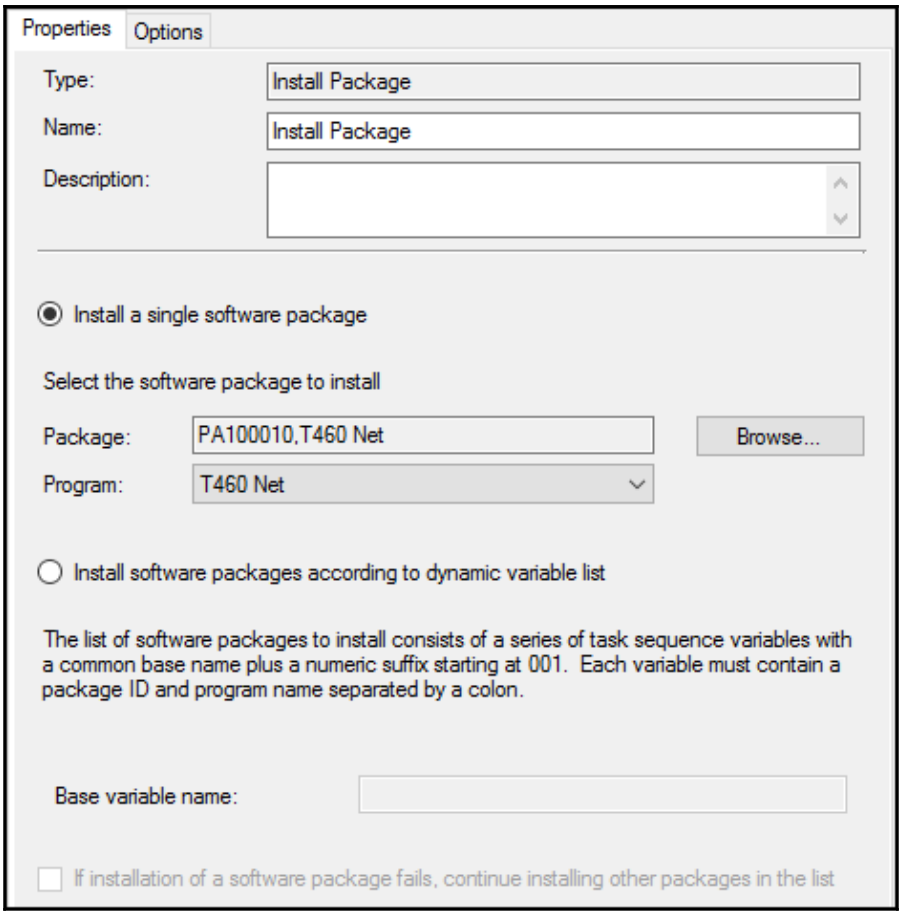

This wizard allows you to import one or more drivers. You can let Configuration Manager find all drivers in the given network path or specify a specific driver to import.
Import all drivers in the following network path (UNC)
Source folder:
\\file\SourceFiles\Drivers\T430\02_Lenovo_P
Browse...
Import a specific driver by specifying the network path (UNC) to its .inf or txtsetup.oem file
Source:
Browse...
Specify the option for duplicate drivers
Import the driver and append a new category to the existing categories

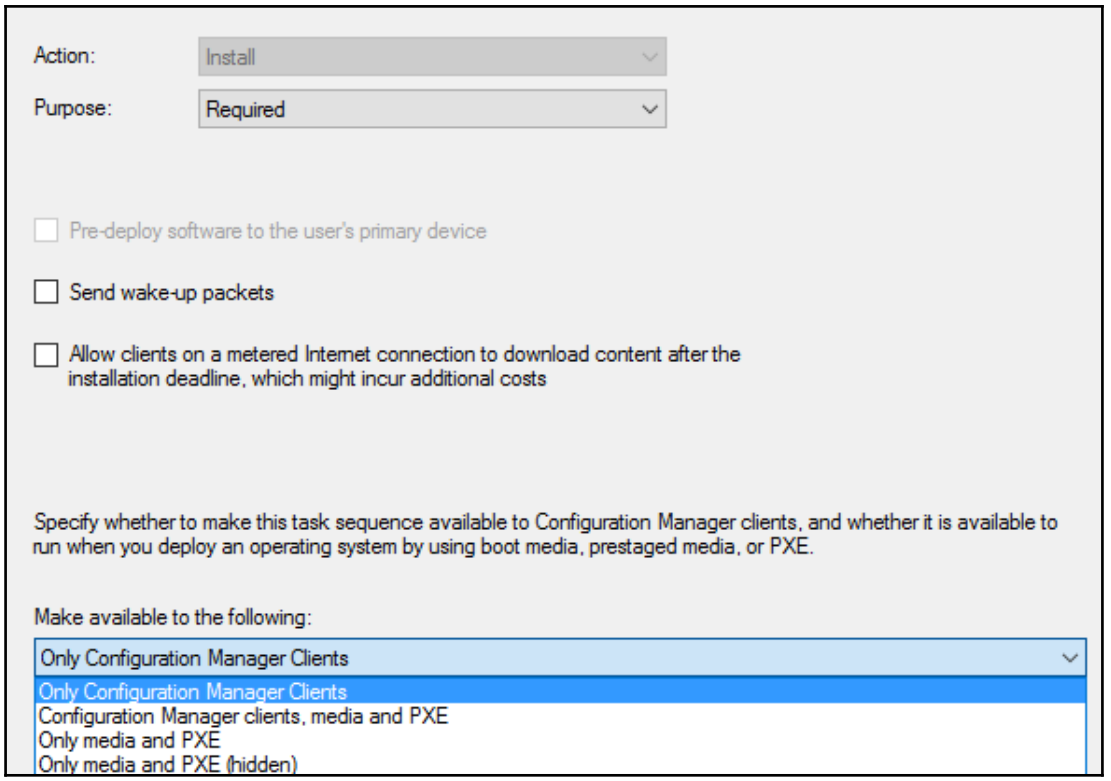

Drivers 3 items
Search
Search
Add C
Icon
Name
Provider
Class
Version Number
Version Date
Categories
Broadcom Bluetooth 4.0 USB
Broadcom...
Bluetooth
12.0.1.410
3/25/2015 2:...
"T430"
Broadcom Bluetooth 4.0 USB
Broadcom...
Bluetooth
12.0.1.410
3/25/2015 2:...
"T430"
Lenovo PM Device
Lenovo
System
1.67.12.16
9/1/2016 4:0...
"T430"

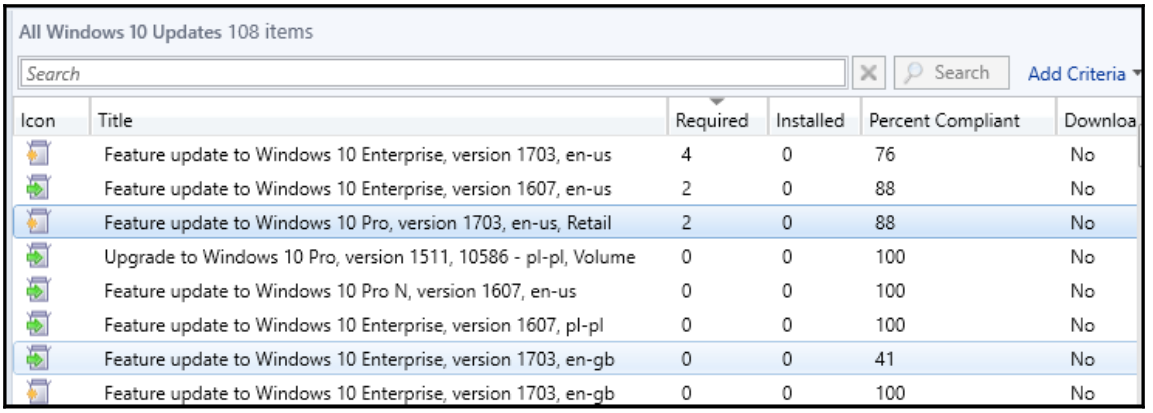

Add
Remove
Capture Files and Settings
Disable BitLocker
Install Operating System
Restart in Windows PE
Partition Disk 0 - BIOS
Partition Disk 0 - UEFI
Pre-provision BitLocker
Apply Operating System
Apply Windows Settings
Apply Network Settings
Apply Device Drivers
Setup Operating System
Setup Windows and Configuration
Enable BitLocker
Install Applications
Properties
Options
Type:
Auto Apply Drivers
Name:
Apply Device Drivers
Description:
For each hardware device
Install only the best matched compatible drivers
Install all compatible drivers
Select drivers from all categories or drivers in specific categories to be made available during Windows setup
Consider drivers from all categories
Limit driver matching to only consider drivers in selected categories:
Filter...
T430

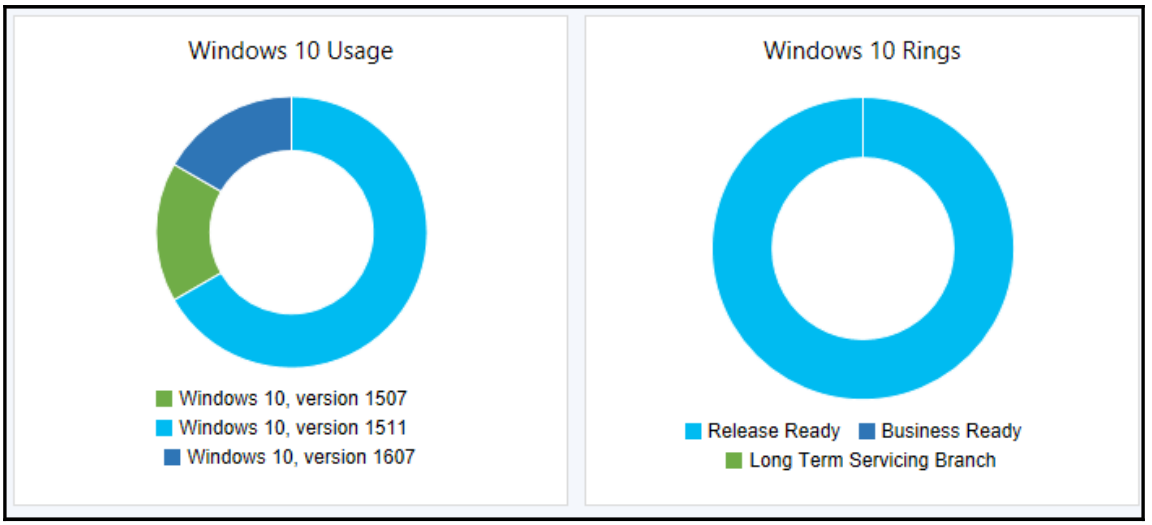

OpsMgr Maintenance Mode
General
Requirements
Environment
Advanced
Windows Installer
A program may require certain conditions to be true before it can run. Specify the conditions that must be met for the program to run.
Program can run:
Whether or not a user is logged on
Run mode
Run with user's rights
Run with administrative rights
Allow users to interact with this program
Drive mode
Runs with UNC name
Requires drive letter
Requires specific drive letter (example: Z):
Z
Reconnect to distribution point at logon

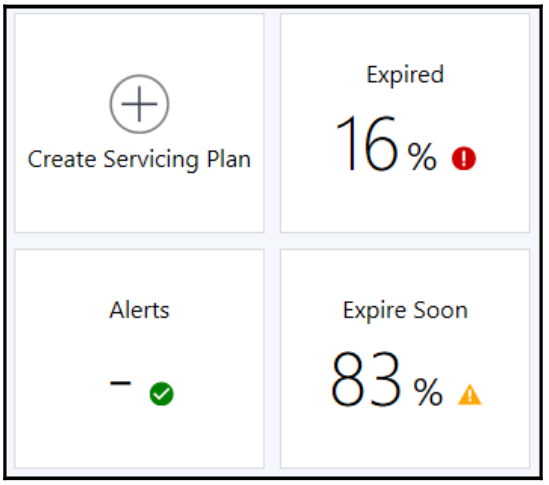

OpsMgr Maintenance Mode
General
Requirements
Environment
Advanced
Windows Installer
You can specify additional criteria for installing and running this program. You can also temporarily disable the program.
Run another program first:
Package:
Browse...
Program:
Always run this program first
When this program is assigned to a computer:
Run once for the computer
Suppress program notifications
A disabled program is not displayed or run on clients.
Disable this program on computers where it is deployed
Allow this program to be installed from the Install Package task sequence without being deployed

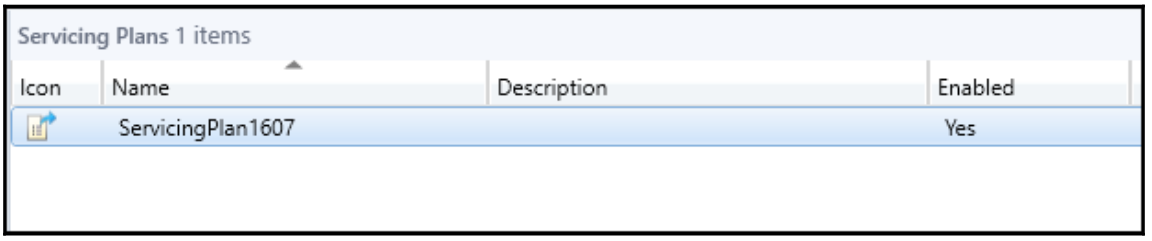

Properties
Options
Type:
Install Package
Name:
Install Package
Description:
Install a single software package
Select the software package to install
Package:
PA100010,T460 Net
Browse...
Program:
T460 Net
Install software packages according to dynamic variable list
The list of software packages to install consists of a series of task sequence variables with a common base name plus a numeric suffix starting at 001. Each variable must contain a package ID and program name separated by a colon.
Base variable name:
If installation of a software package fails, continue installing other packages in the list

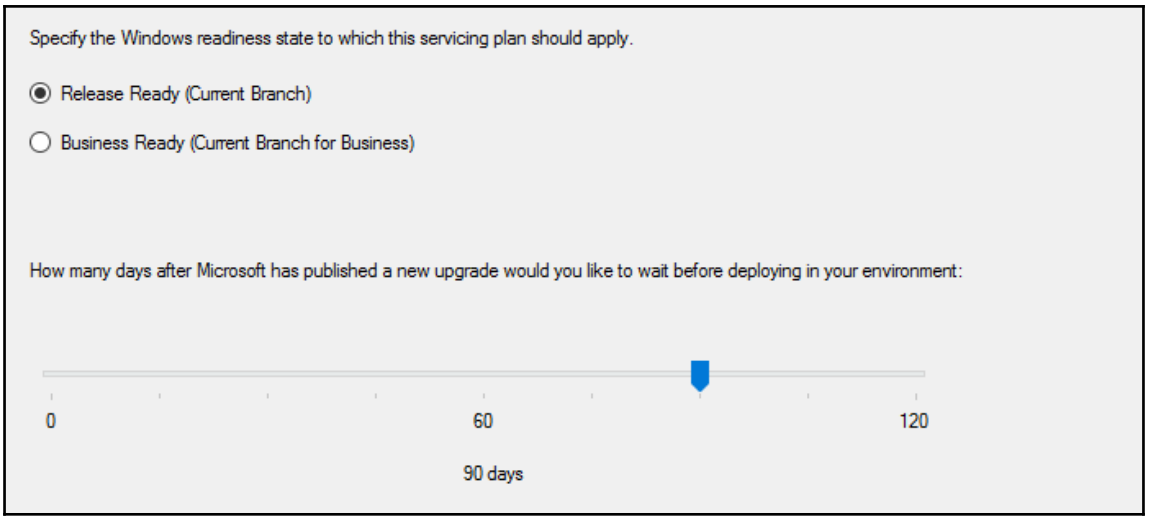

Action:
Install
Purpose:
Required
Pre-deploy software to the user's primary device
Send wake-up packets
Allow clients on a metered Internet connection to download content after the installation deadline, which might incur additional costs
Specify whether to make this task sequence available to Configuration Manager clients, and whether it is available to run when you deploy an operating system by using boot media, prestaged media, or PXE.
Make available to the following:
Only Configuration Manager Clients
Only Configuration Manager Clients
Configuration Manager clients, media and PXE
Only media and PXE
Only media and PXE (hidden)

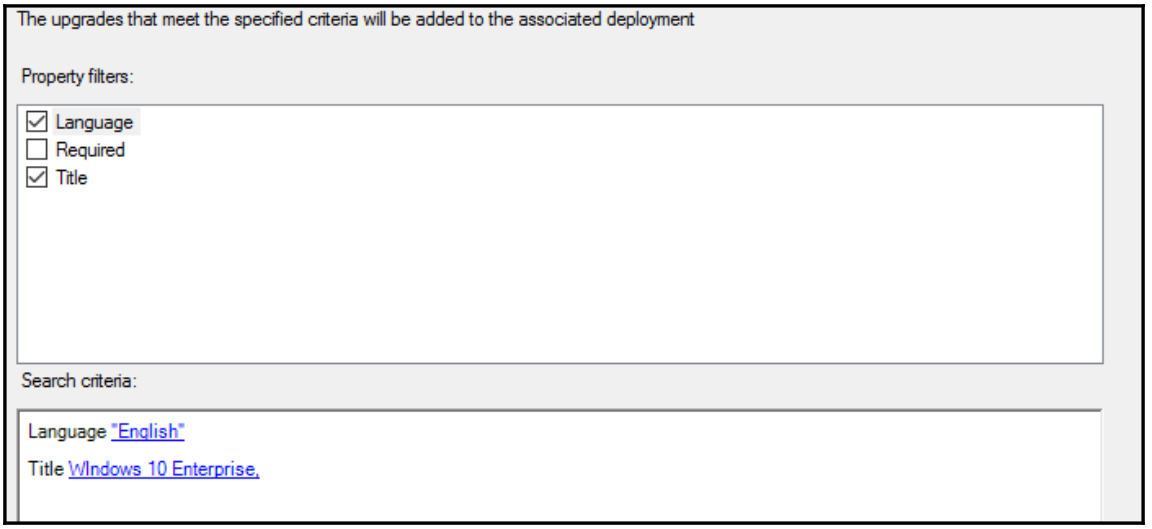

All Windows 10 Updates 108 items
Search
Search
Add Criteria
Icon
Title
Required
Installed
Percent Compliant
Downloa
Feature update to Windows 10 Enterprise, version 1703, en-us 4 0 76 No
Feature update to Windows 10 Enterprise, version 1607, en-us 2 0 88 No
Feature update to Windows 10 Pro, version 1703, en-us, Retail 2 0 88 No
Upgrade to Windows 10 Pro, version 1511, 10586 - pl-pl, Volume 0 0 100 No
Feature update to Windows 10 Pro N, version 1607, en-us 0 0 100 No
Feature update to Windows 10 Enterprise, version 1607, pl-pl 0 0 100 No
Feature update to Windows 10 Enterprise, version 1703, en-gb 0 0 41 No
Feature update to Windows 10 Enterprise, version 1703, en-gb 0 0 100 No

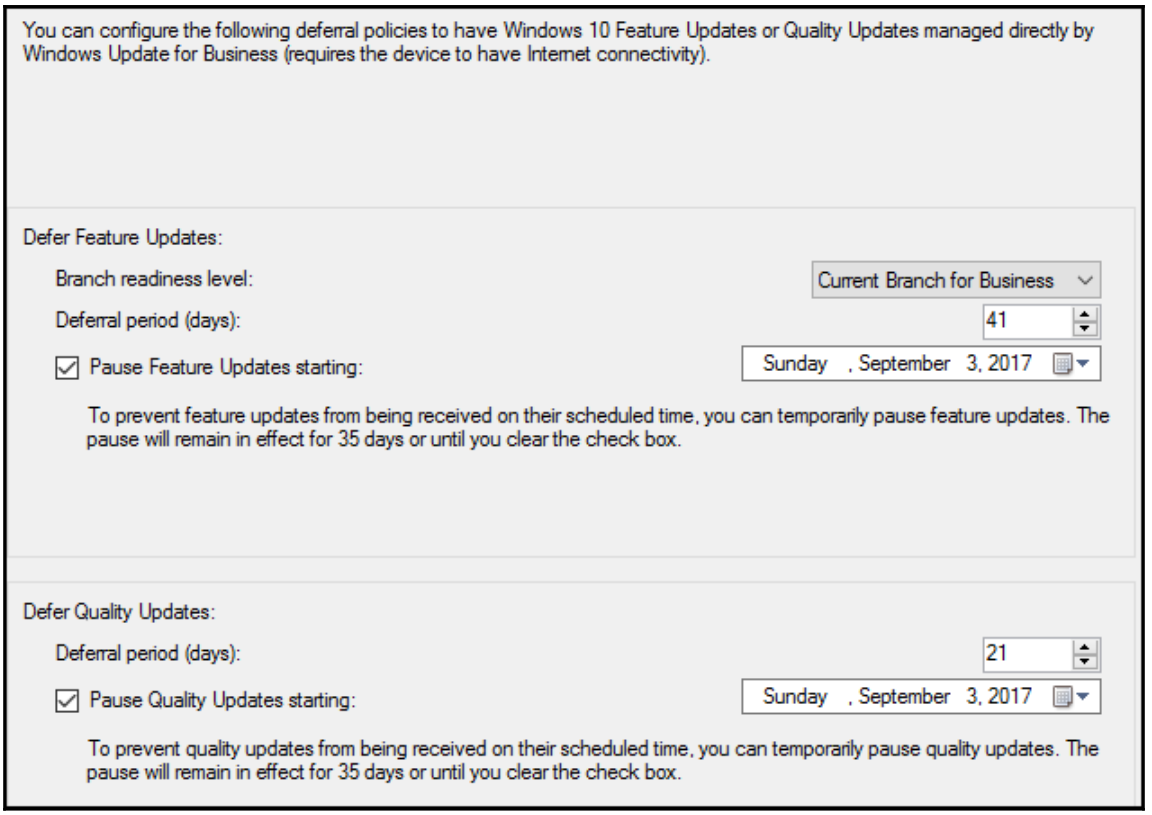

Windows 10 Usage
Windows 10, version 1507
Windows 10, version 1511
Windows 10, version 1607
Windows 10 Rings
Release Ready
Business Ready
Long Term Servicing Branch

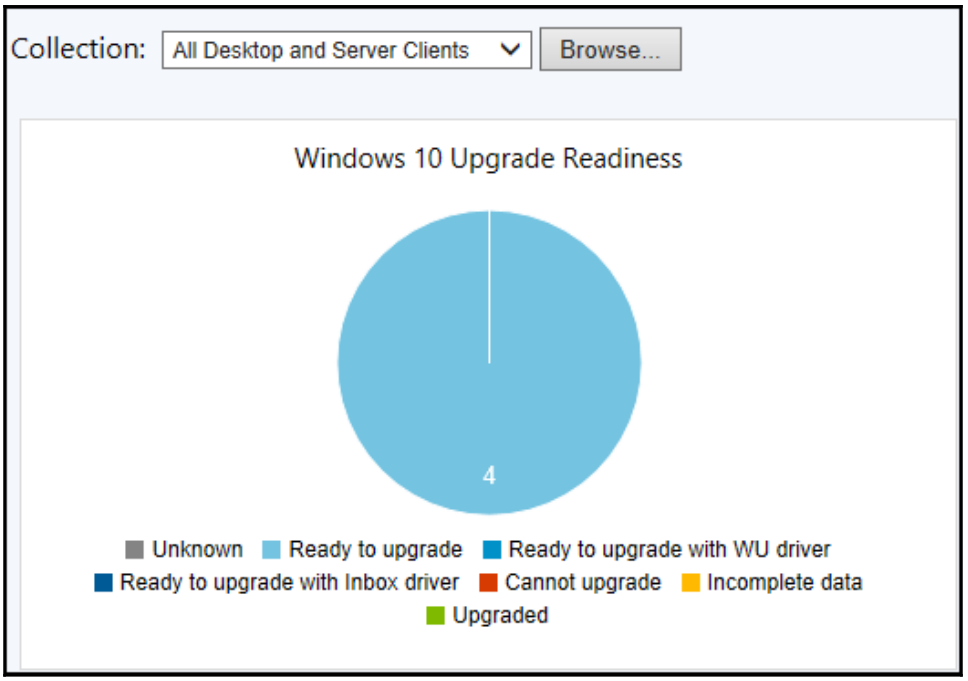

Create Servicing Plan
Expired
16 %
Alerts
-
Expire Soon
83 %


Servicing Plans 1 items
Icon
Name
Description
Enabled
ServicingPlan1607
Yes

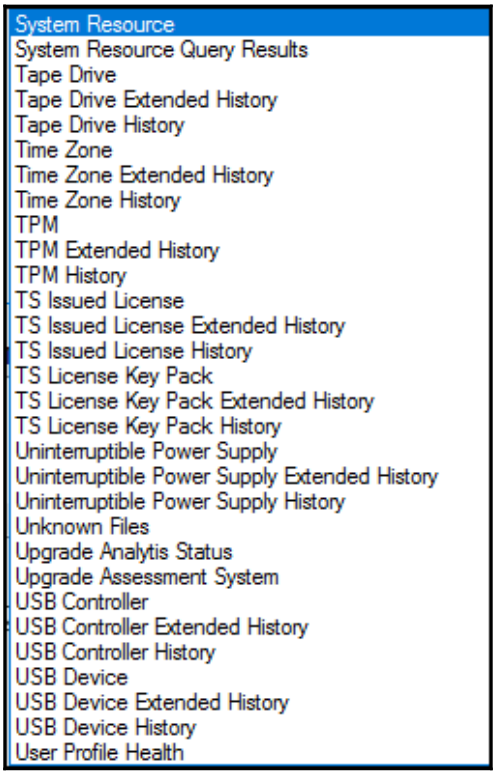

Specify the Windows readiness state to which this servicing plan should apply.
Release Ready (Current Branch)
Business Ready (Current Branch for Business)
How many days after Microsoft has published a new upgrade would you like to wait before deploying in your environment:
0
60
120
90 days

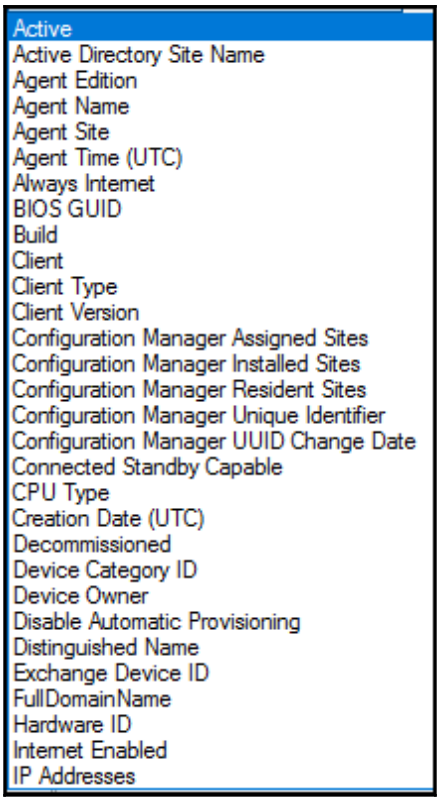

The upgrades that meet the specified criteria will be added to the associated deployment
Property filters:
Language
Required
Title
Search criteria:
Language "English"
Title Windows 10 Enterprise,

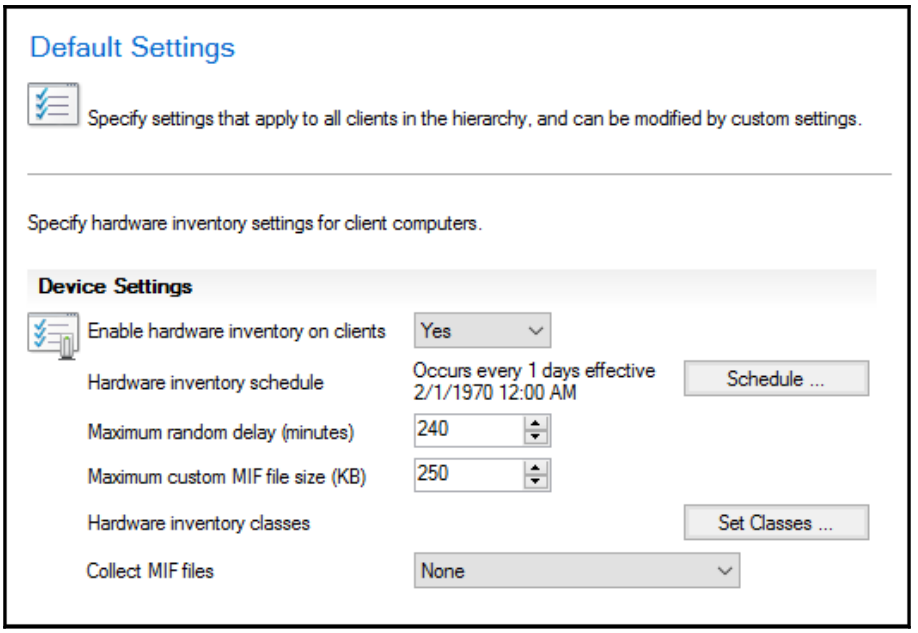

You can configure the following deferral policies to have Windows 10 Feature Updates or Quality Updates managed directly by Windows Update for Business (requires the device to have Internet connectivity).
Defer Feature Updates:
Branch readiness level:
Current Branch for Business
Deferral period (days):
41
Pause Feature Updates starting:
Sunday , September 3, 2017
To prevent feature updates from being received on their scheduled time, you can temporarily pause feature updates. The pause will remain in effect for 35 days or until you clear the check box.
Defer Quality Updates:
Deferral period (days):
21
Pause Quality Updates starting:
Sunday , September 3, 2017
To prevent quality updates from being received on their scheduled time, you can temporarily pause quality updates. The pause will remain in effect for 35 days or until you clear the check box.

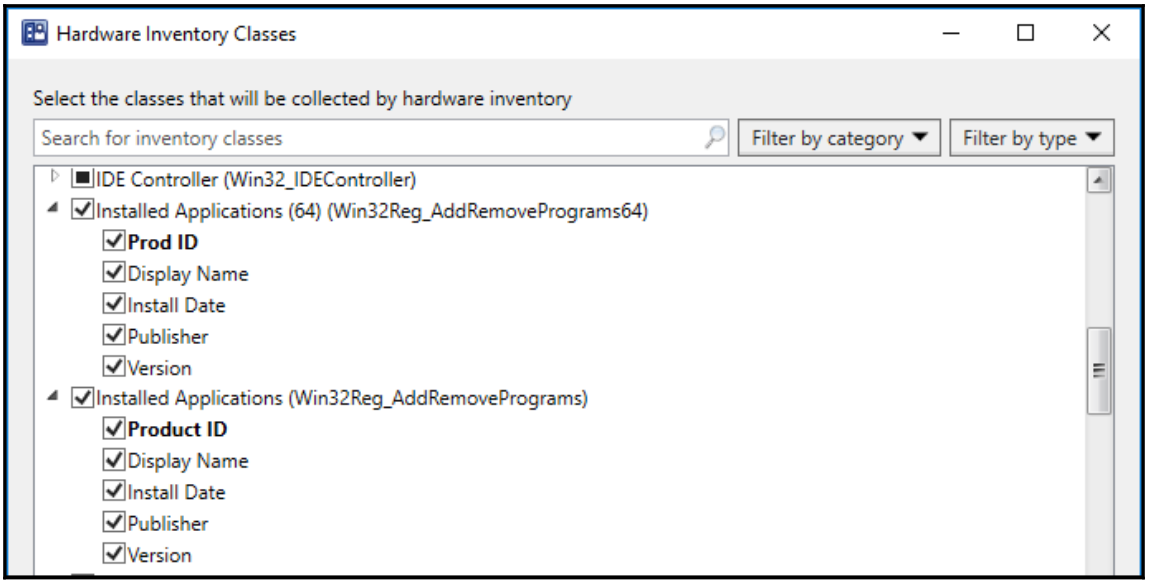

Collection:
All Desktop and Server Clients
Browse...
Windows 10 Upgrade Readiness
4
Unknown
Ready to upgrade
Ready to upgrade with WU driver
Ready to upgrade with Inbox driver
Cannot upgrade
Incomplete data
Upgraded

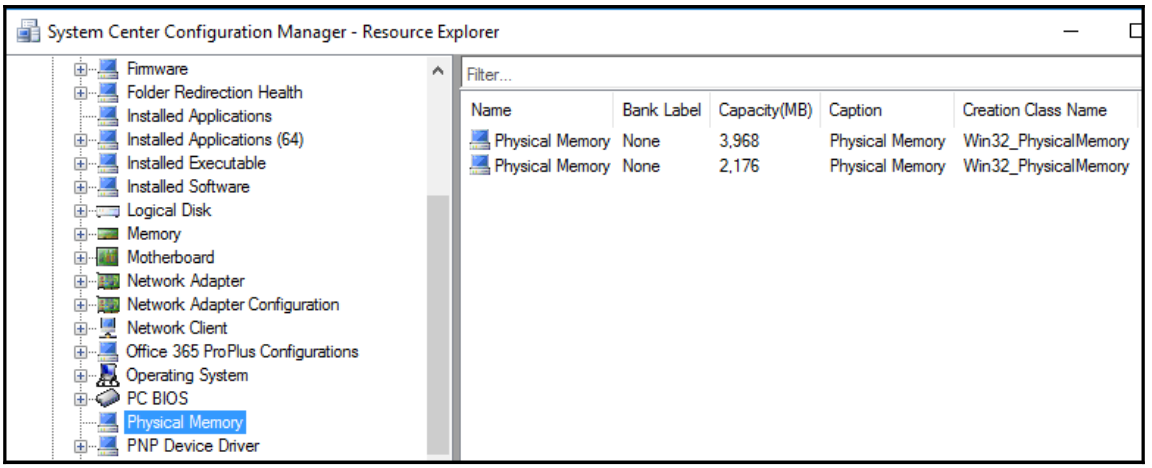
# Chapter 11: Configuration Manager Assets

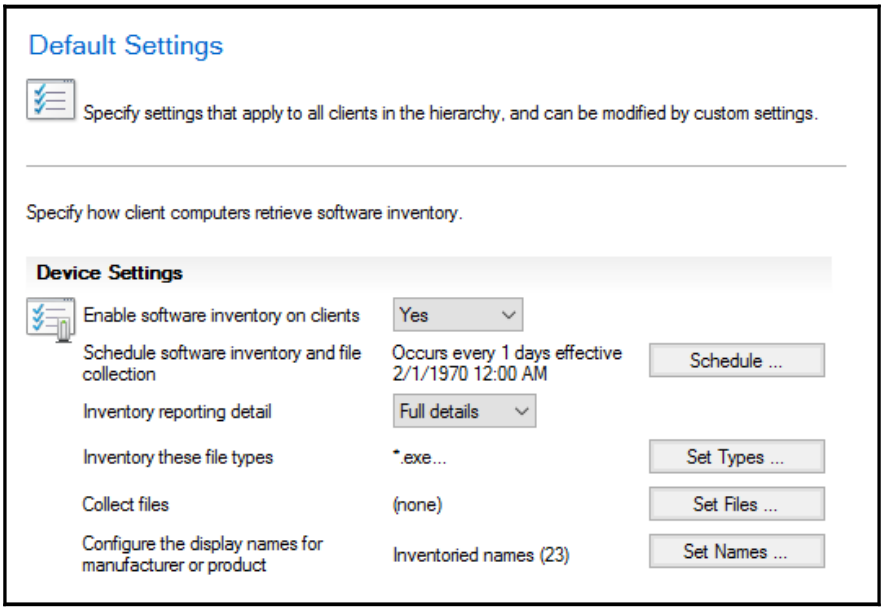


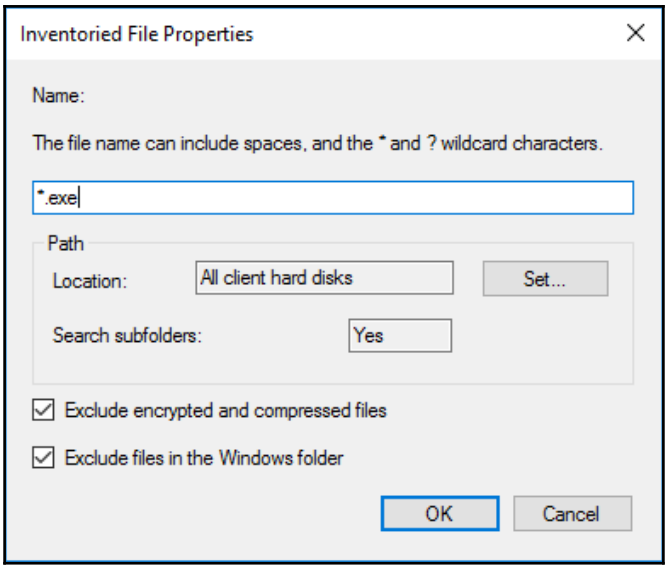

Active
Active Directory Site Name
Agent Edition
Agent Name
Agent Site
Agent Time (UTC)
Always Internet
BIOS GUID
Build
Client
Client Type
Client Version
Configuration Manager Assigned Sites
Configuration Manager Installed Sites
Configuration Manager Resident Sites
Configuration Manager Unique Identifier
Configuration Manager UUID Change Date
Connected Standby Capable
CPU Type
Creation Date (UTC)
Decommissioned
Device Category ID
Device Owner
Disable Automatic Provisioning
Distinguished Name
Exchange Device ID
FullDomainName
Hardware ID
Internet Enabled
IP Addresses

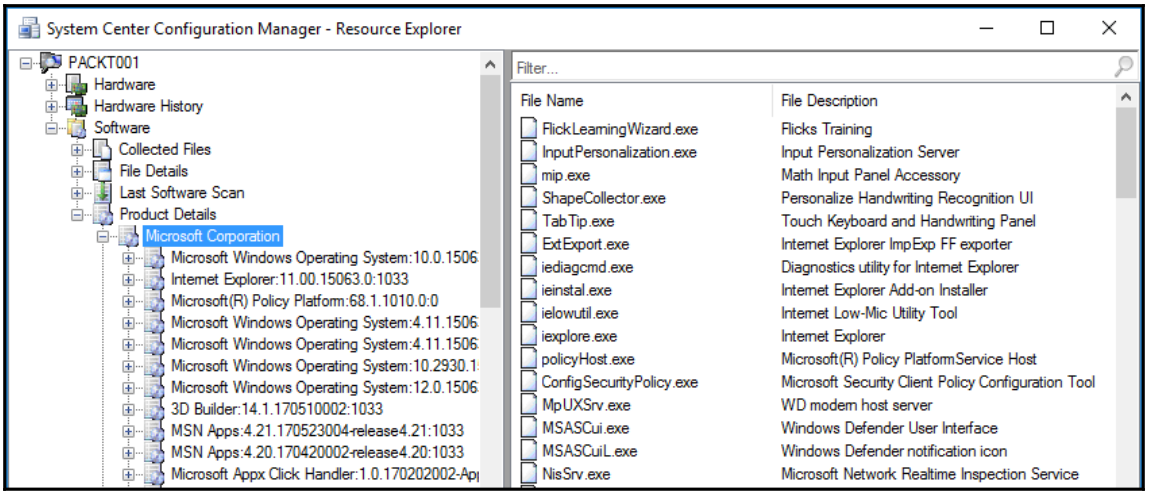

Default Settings
Specify settings that apply to all clients in the hierarchy, and can be modified by custom settings.
Specify hardware inventory settings for client computers.
Device Settings
Enable hardware inventory on clients
Yes
Hardware inventory schedule
Occurs every 1 days effective 2/1/1970 12:00 AM
Schedule ...
Maximum random delay (minutes)
240
Maximum custom MIF file size (KB)
250
Hardware inventory classes
Set Classes ...
Collect MIF files
None

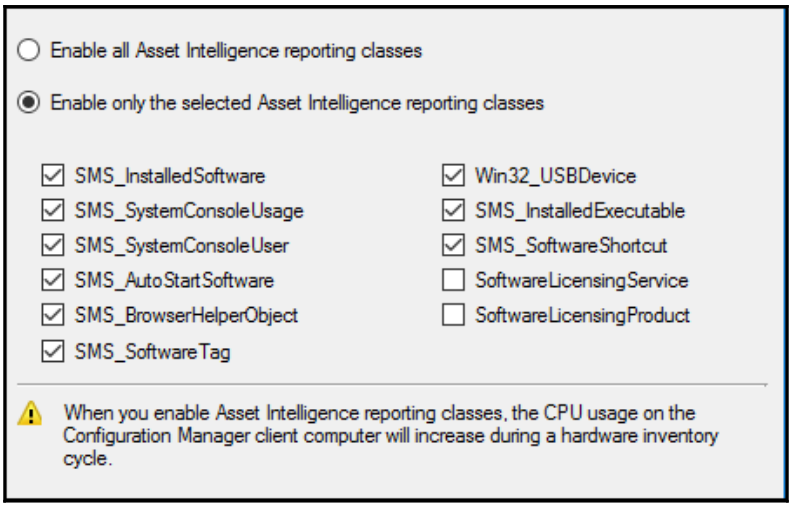

Hardware Inventory Classes
Select the classes that will be collected by hardware inventory
Search for inventory classes
Filter by category
Filter by type
IDE Controller (Win32_IDEController)
Installed Applications (64) (Win32Reg_AddRemovePrograms64)
Prod ID
Display Name
Install Date
Publisher
Version
Installed Applications (Win32Reg_AddRemovePrograms)
Product ID
Display Name
Install Date
Publisher
Version

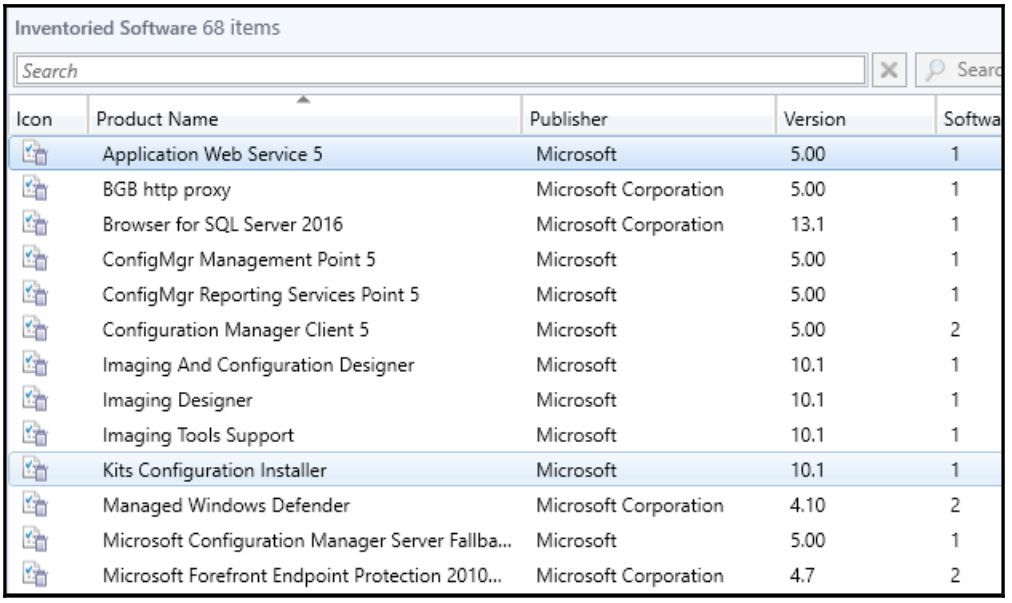

System Center Configuration Manager - Resource Explorer
Firmware
Folder Redirection Health
Installed Applications
Installed Applications (64)
Installed Executable
Installed Software
Logical Disk
Memory
Motherboard
Network Adapter
Network Adapter Configuration
Network Client
Office 365 ProPlus Configurations
Operating System
PC BIOS
Physical Memory
PNP Device Driver
Filter...
Name
Bank Label
Capacity(MB)
Caption
Creation Class Name
Physical Memory None 3,968 Physical Memory Win32_PhysicalMemory
Physical Memory None 2,176 Physical Memory Win32_PhysicalMemory

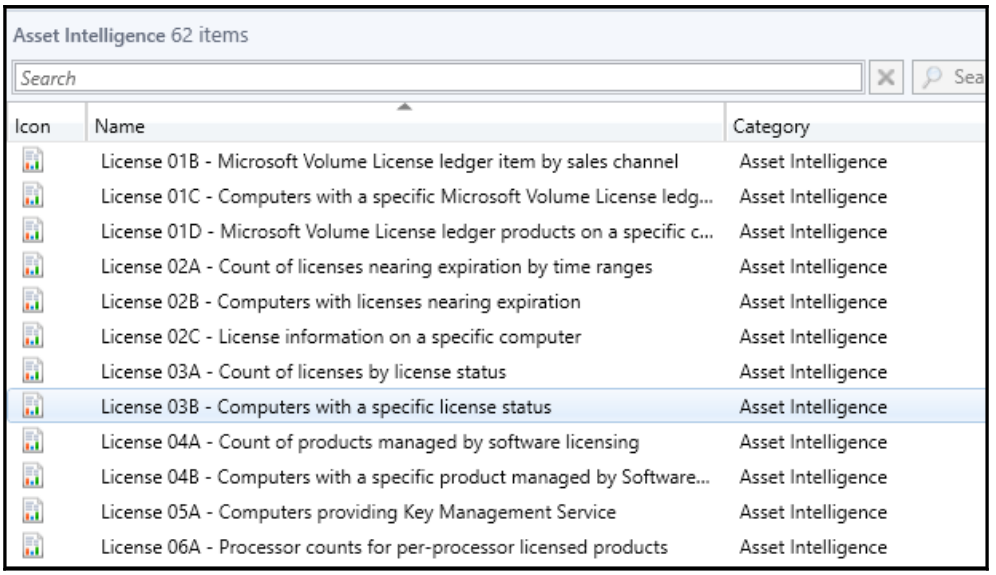

Default Settings
Specify settings that apply to all clients in the hierarchy, and can be modified by custom settings.
Specify how client computers retrieve software inventory.
Device Settings
Enable software inventory on clients
Yes
Schedule software inventory and file collection
Occurs every 1 days effective 2/1/1970 12:00 AM
Schedule ...
Inventory reporting detail
Full details
Inventory these file types
*.exe...
Set Types ...
Collect files
(none)
Set Files ...
Configure the display names for manufacturer or product
Inventoried names (23)
Set Names ...


Inventoried File Properties
Name:
The file name can include spaces, and the * and ? wildcard characters.
*.exe
Path
Location:
All client hard disks
Set...
Search subfolders:
Yes
Exclude encrypted and compressed files
Exclude files in the Windows folder
OK
Cancel


System Center Configuration Manager - Resource Explorer
PACKT001
Hardware
Hardware History
Software
Collected Files
File Details
Last Software Scan
Product Details
Microsoft Corporation
Microsoft Windows Operating System:10.0.1506
Internet Explorer:11.00.15063.0:1033
Microsoft(R) Policy Platform:68.1.1010.0:0
Microsoft Windows Operating System:4.11.1506
Microsoft Windows Operating System:4.11.1506
Microsoft Windows Operating System:10.2930.1
Microsoft Windows Operating System:12.0.1506
3D Builder:14.1.170510002:1033
MSN Apps:4.21.170523004-release4.21:1033
MSN Apps:4.20.170420002-release4.20:1033
Microsoft Appx Click Handler:1.0.170202002-Ap
Filter...
File Name
File Description
FlickLearningWizard.exe
Flicks Training
InputPersonalization.exe
Input Personalization Server
mip.exe
Math Input Panel Accessory
ShapeCollector.exe
Personalize Handwriting Recognition UI
TabTip.exe
Touch Keyboard and Handwriting Panel
ExtExport.exe
Internet Explorer ImpExp FF exporter
iediagcmd.exe
Diagnostics utility for Internet Explorer
ieinstal.exe
Internet Explorer Add-on Installer
ielowutil.exe
Internet Low-Mic Utility Tool
iexplore.exe
Internet Explorer
policyHost.exe
Microsoft(R) Policy PlatformService Host
ConfigSecurityPolicy.exe
Microsoft Security Client Policy Configuration Tool
MpUXSrv.exe
WD modem host server
MSASCui.exe
Windows Defender User Interface
MSASCuiL.exe
Windows Defender notification icon
NisSrv.exe
Microsoft Network Realtime Inspection Service


Enable all Asset Intelligence reporting classes
Enable only the selected Asset Intelligence reporting classes
SMS_InstalledSoftware
SMS_SystemConsoleUsage
SMS_SystemConsoleUser
SMS_AutoStartSoftware
SMS_BrowserHelperObject
SMS_SoftwareTag
Win32_USBDevice
SMS_InstalledExecutable
SMS_SoftwareShortcut
SoftwareLicensingService
SoftwareLicensingProduct
When you enable Asset Intelligence reporting classes, the CPU usage on the Configuration Manager client computer will increase during a hardware inventory cycle.


Inventoried Software 68 items
Search
Icon
Product Name
Publisher
Version
Softwa
Application Web Service 5
Microsoft
5.00
1
BGB http proxy
Microsoft Corporation
5.00
1
Browser for SQL Server 2016
Microsoft Corporation
13.1
1
ConfigMgr Management Point 5
Microsoft
5.00
1
ConfigMgr Reporting Services Point 5
Microsoft
5.00
1
Configuration Manager Client 5
Microsoft
5.00
2
Imaging And Configuration Designer
Microsoft
10.1
1
Imaging Designer
Microsoft
10.1
1
Imaging Tools Support
Microsoft
10.1
1
Kits Configuration Installer
Microsoft
10.1
1
Managed Windows Defender
Microsoft Corporation
4.10
2
Microsoft Configuration Manager Server Fallba...
Microsoft
5.00
1
Microsoft Forefront Endpoint Protection 2010...
Microsoft Corporation
4.7
2

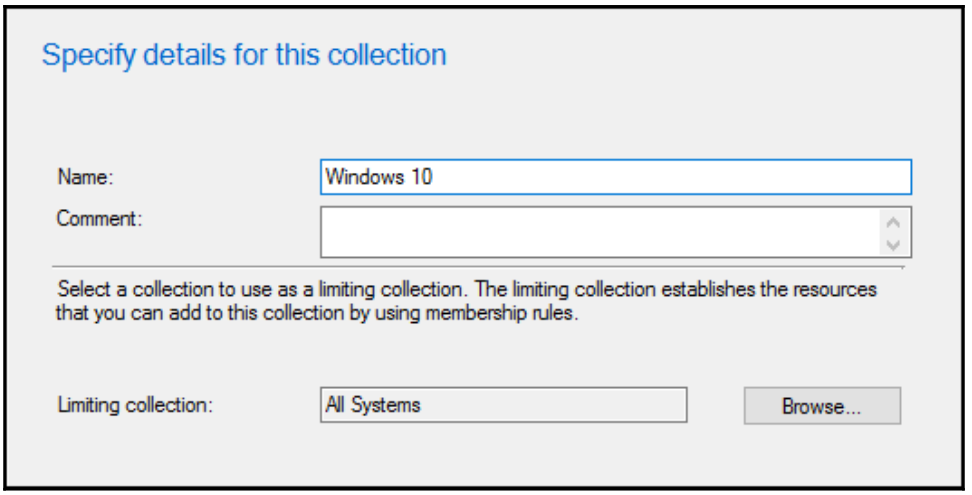


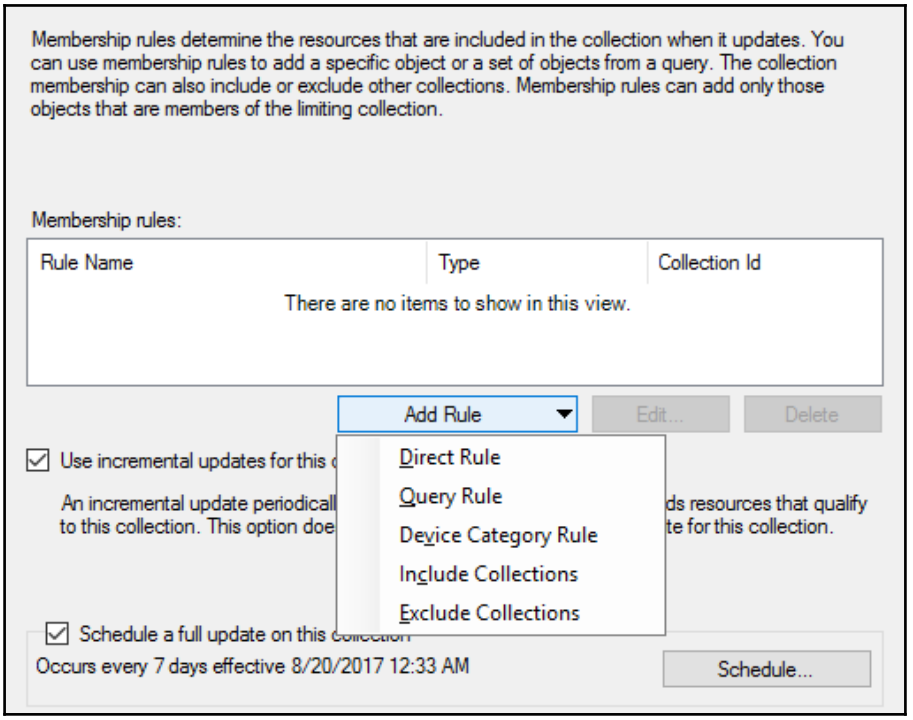

Microsoft System Center Configuration Manager

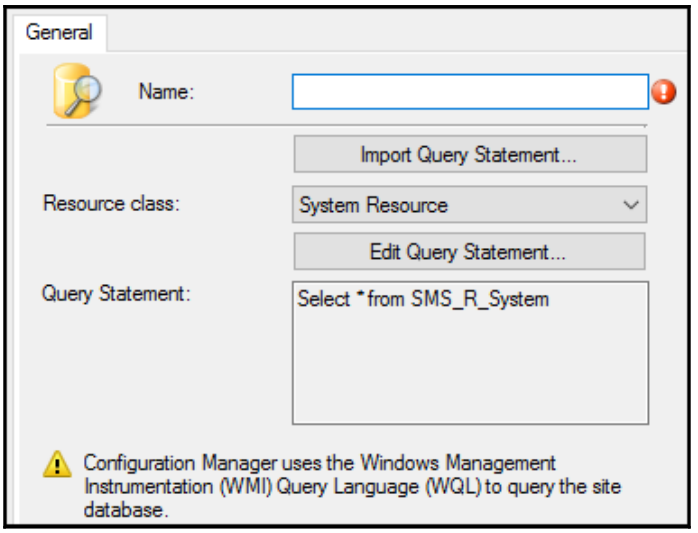
## License 15A - General license reconciliation report

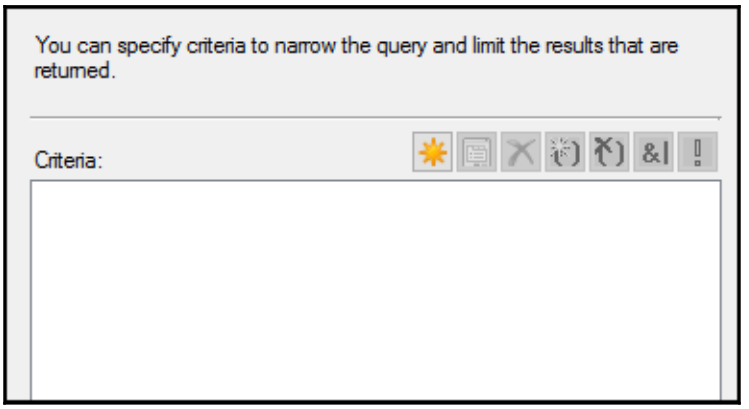
Description

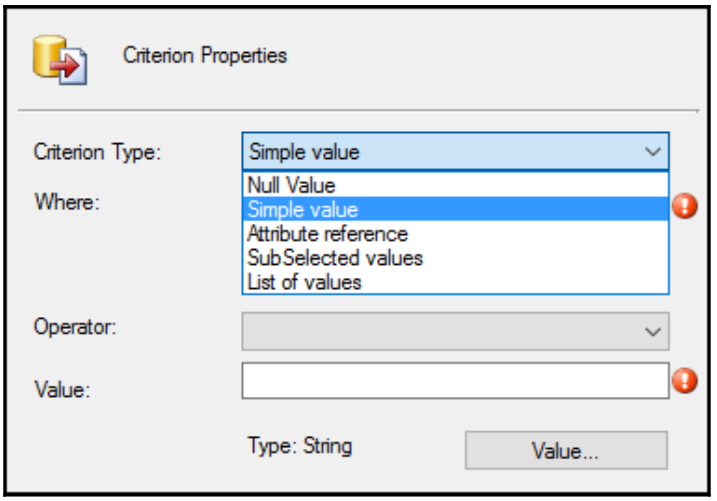
| Product Name | Version | Licensed Quantity | Inventory Count | Difference |
|---|---|---|---|---|
| 1E AppClarity | 3 | 5 | 0 | 5 |
| Ala | 2 | 1 | 0 | 1 |
| Camtasia Studio 6 | 6 | 5 | 1 | 4 |
| Cisco Systems VPN Client 5.0 | 5 | 2 | 0 | 2 |
| Configuration Manager Client | 5 | 15 | 15 | 0 |
| NetObjects Fusion 2013 | 13 | 1 | 0 | 1 |
| Snagit 11 | 11 | 5 | 0 | 5 |
| Snagit 12 | 12 | 5 | 2 | 3 |

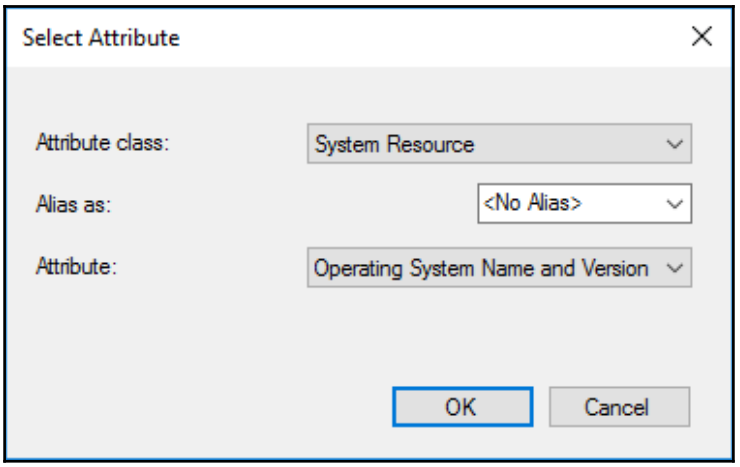

Specify details for this collection
Name:
Windows 10
Comment:
Select a collection to use as a limiting collection. The limiting collection establishes the resources that you can add to this collection by using membership rules.
Limiting collection:
All Systems
Browse...

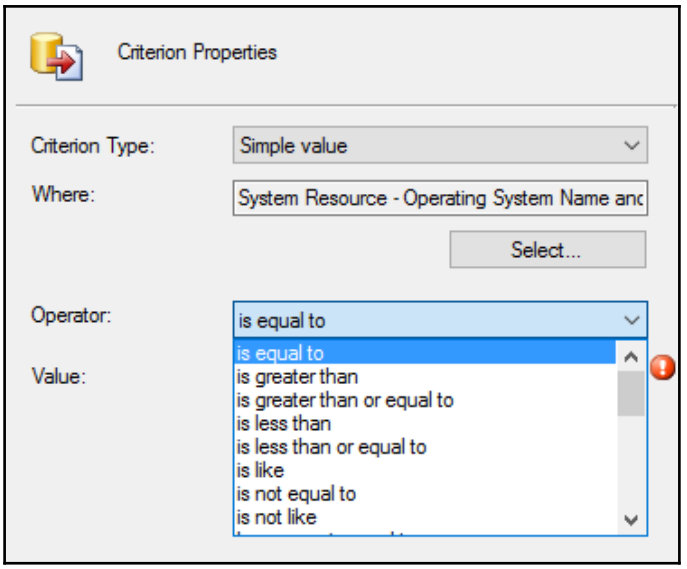

Membership rules determine the resources that are included in the collection when it updates. You can use membership rules to add a specific object or a set of objects from a query. The collection membership can also include or exclude other collections. Membership rules can add only those objects that are members of the limiting collection.
Membership rules:
Rule Name
Type
Collection Id
There are no items to show in this view.
Add Rule
Edit...
Delete
Direct Rule
Query Rule
Device Category Rule
Include Collections
Exclude Collections
Use incremental updates for this
An incremental update periodicall
ds resources that qualify
to this collection. This option doe
te for this collection.
Schedule a full update on this
Occurs every 7 days effective 8/20/2017 12:33 AM
Schedule...

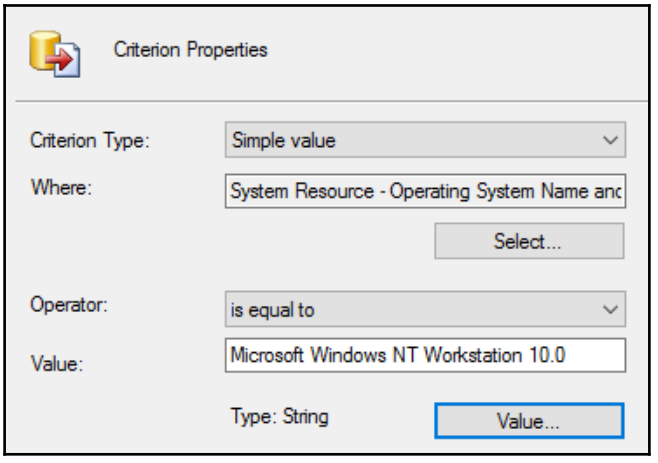

General
Name:
Import Query Statement...
Resource class:
System Resource
Edit Query Statement...
Query Statement:
Select * from SMS_R_System
Configuration Manager uses the Windows Management Instrumentation (WMI) Query Language (WQL) to query the site database.

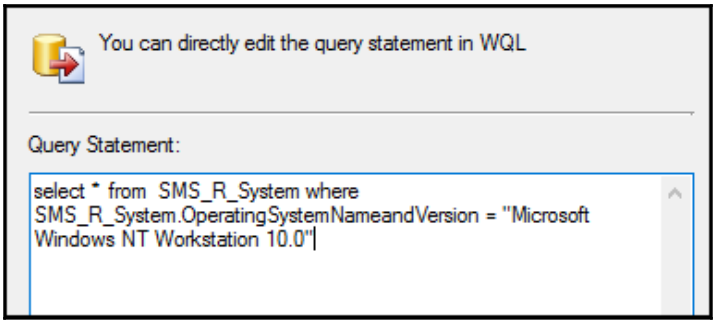

You can specify criteria to narrow the query and limit the results that are returned.
Criteria:

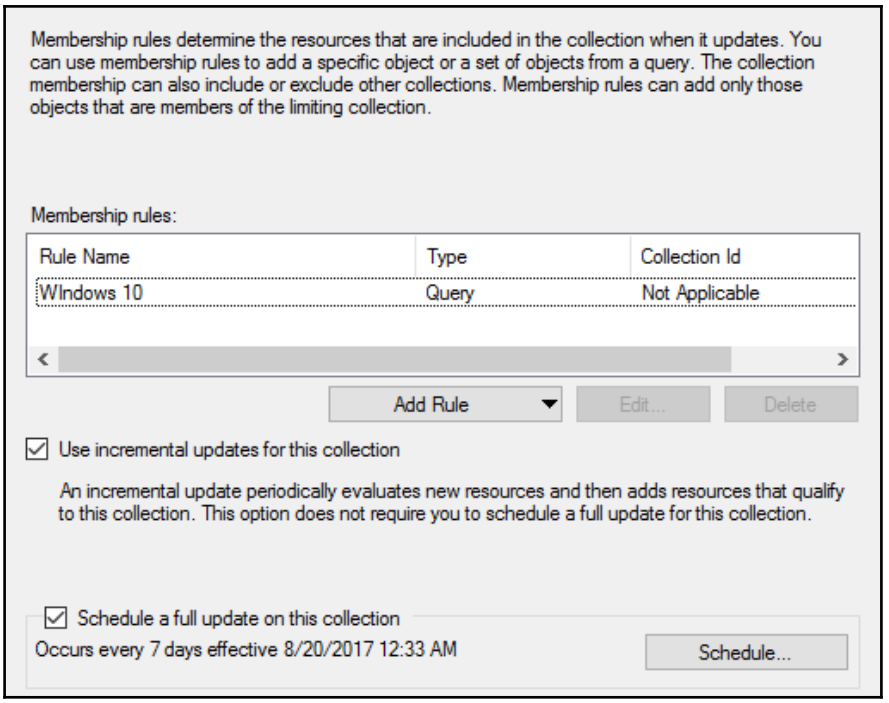

Criterion Properties
Criterion Type:
Simple value
Null Value
Simple value
Attribute reference
SubSelected values
List of values
Where:
Operator:
Value:
Type: String
Value...

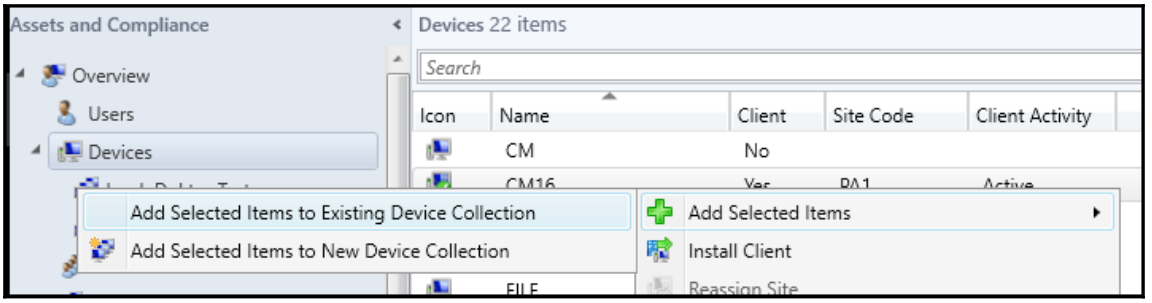

Select Attribute
Attribute class:
System Resource
Alias as:
<No Alias>
Attribute:
Operating System Name and Version
OK
Cancel

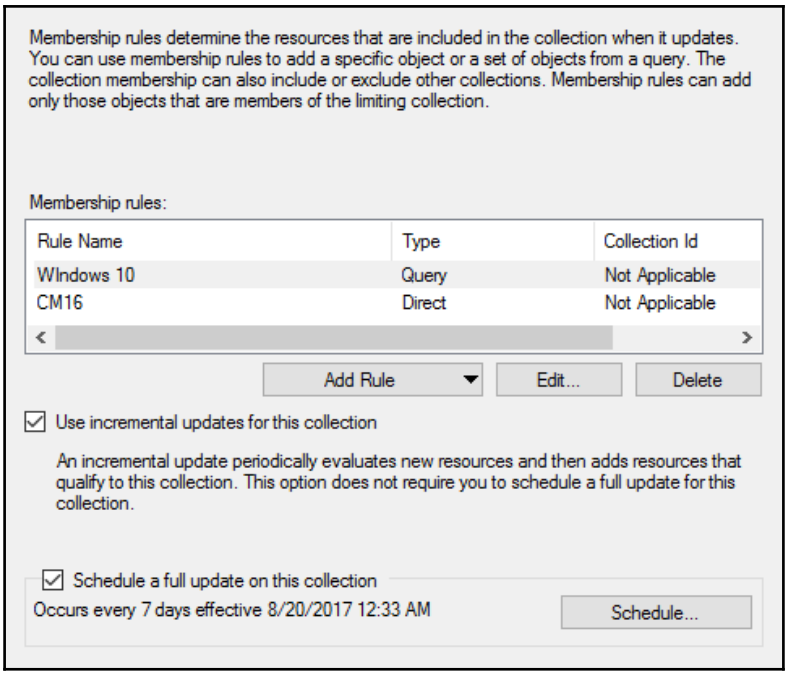

Criterion Properties
Criterion Type:
Simple value
Where:
System Resource - Operating System Name and
Select...
Operator:
is equal to
Value:
is equal to
is greater than
is greater than or equal to
is less than
is less than or equal to
is like
is not equal to
is not like

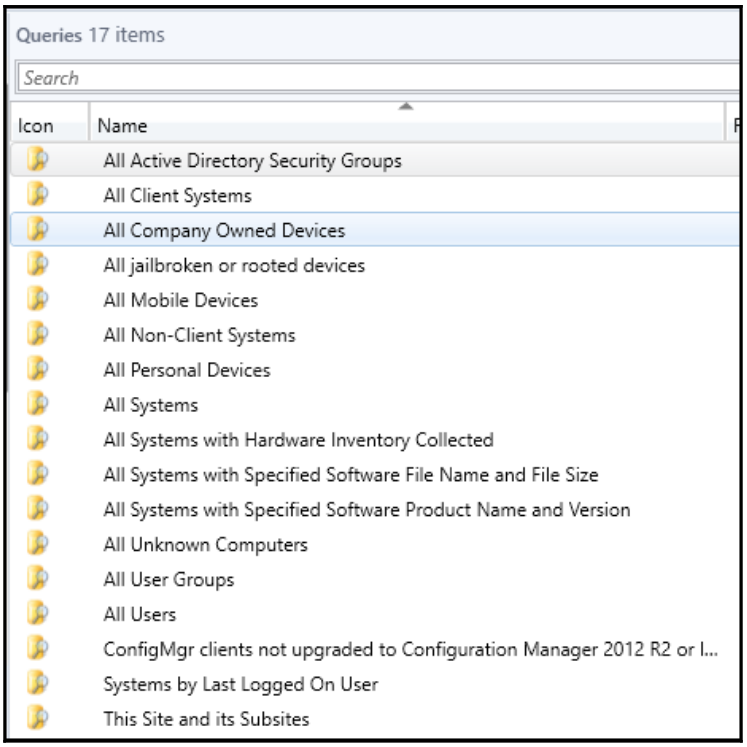

Criterion Properties
Criterion Type:
Simple value
Where:
System Resource - Operating System Name and
Select...
Operator:
is equal to
Value:
Microsoft Windows NT Workstation 10.0
Type: String
Value...

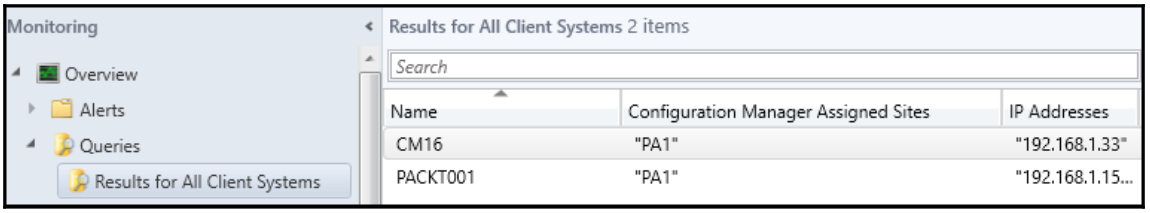

You can directly edit the query statement in WQL
Query Statement:
select * from SMS_R_System where
SMS_R_System.OperatingSystemNameandVersion = "Microsoft
Windows NT Workstation 10.0"

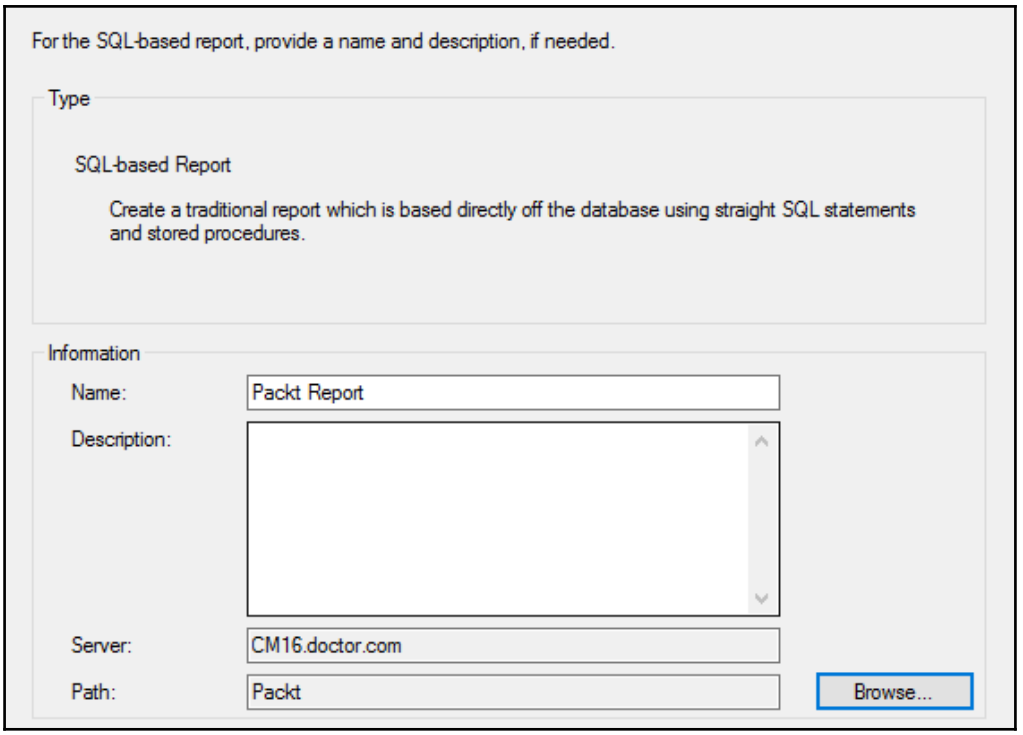

Membership rules determine the resources that are included in the collection when it updates. You can use membership rules to add a specific object or a set of objects from a query. The collection membership can also include or exclude other collections. Membership rules can add only those objects that are members of the limiting collection.
Membership rules:
Rule Name
Type
Collection Id
WIndows 10
Query
Not Applicable
Add Rule
Edit...
Delete
Use incremental updates for this collection
An incremental update periodically evaluates new resources and then adds resources that qualify to this collection. This option does not require you to schedule a full update for this collection.
Schedule a full update on this collection
Occurs every 7 days effective 8/20/2017 12:33 AM
Schedule...

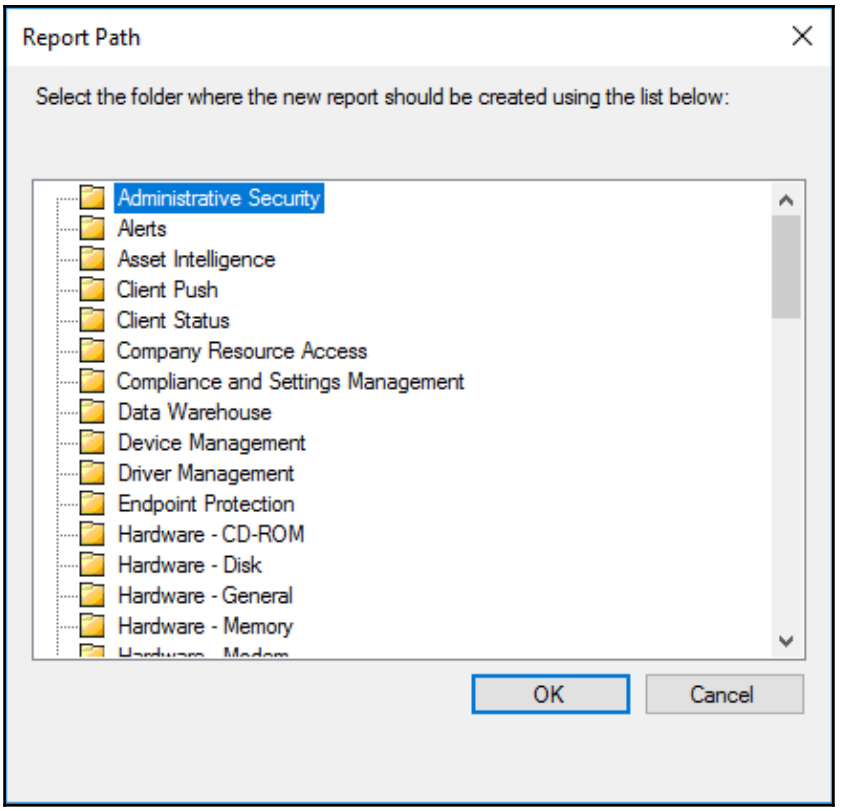

Assets and Compliance
Overview
Users
Devices
Devices 22 items
Search
Icon
Name
Client
Site Code
Client Activity
CM
No
Add Selected Items to Existing Device Collection
Add Selected Items to New Device Collection
Add Selected Items
Install Client

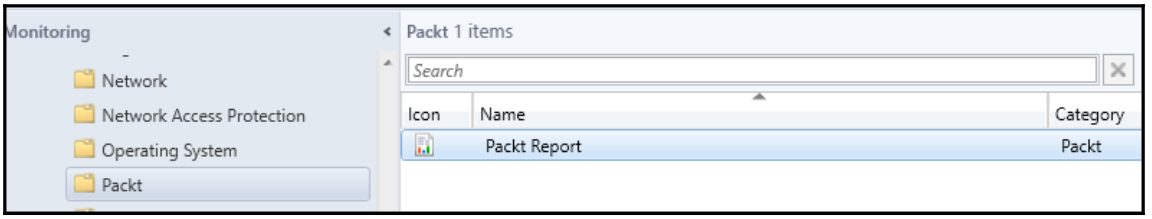

Membership rules determine the resources that are included in the collection when it updates. You can use membership rules to add a specific object or a set of objects from a query. The collection membership can also include or exclude other collections. Membership rules can add only those objects that are members of the limiting collection.
Membership rules:
Rule Name
Type
Collection Id
WIndows 10
Query
Not Applicable
CM16
Direct
Not Applicable
Add Rule
Edit...
Delete
Use incremental updates for this collection
An incremental update periodically evaluates new resources and then adds resources that qualify to this collection. This option does not require you to schedule a full update for this collection.
Schedule a full update on this collection
Occurs every 7 days effective 8/20/2017 12:33 AM
Schedule...

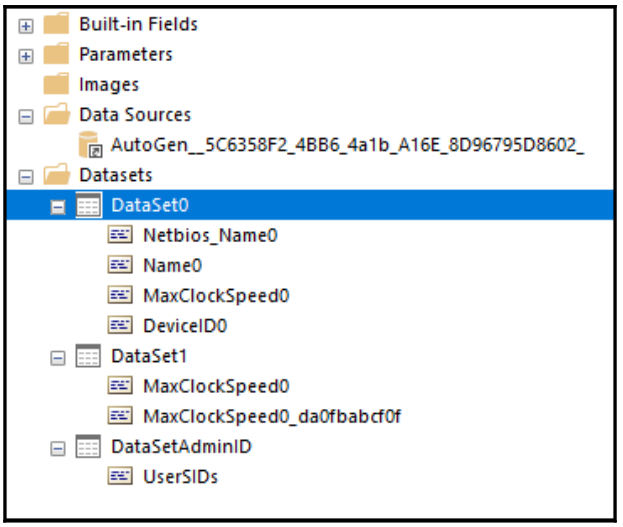

Queries 17 items
Search
Icon
Name
All Active Directory Security Groups
All Client Systems
All Company Owned Devices
All jailbroken or rooted devices
All Mobile Devices
All Non-Client Systems
All Personal Devices
All Systems
All Systems with Hardware Inventory Collected
All Systems with Specified Software File Name and File Size
All Systems with Specified Software Product Name and Version
All Unknown Computers
All User Groups
All Users
ConfigMgr clients not upgraded to Configuration Manager 2012 R2 or l...
Systems by Last Logged On User
This Site and its Subsites

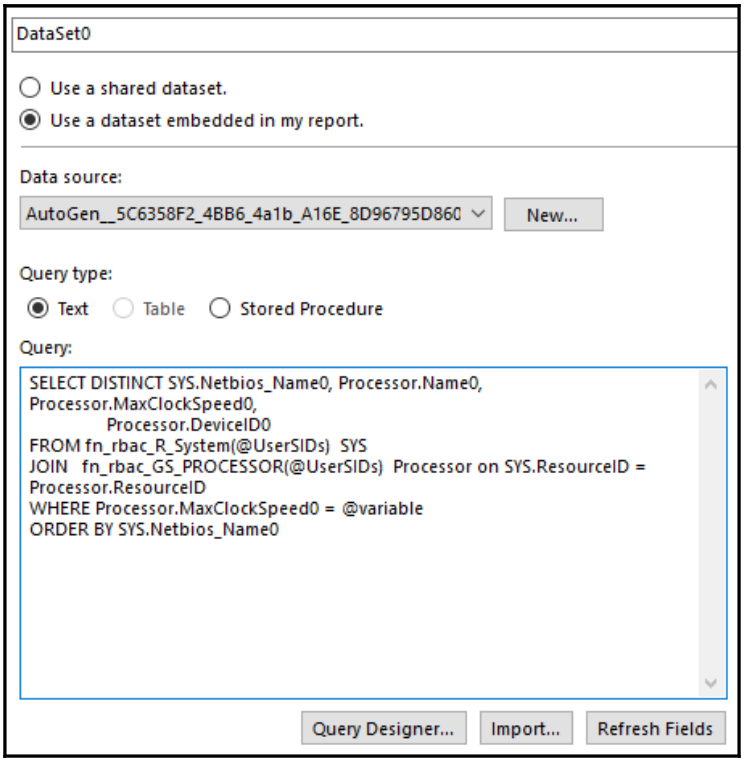

Monitoring
Overview
Alerts
Queries
Results for All Client Systems
Results for All Client Systems 2 items
Search
Name
Configuration Manager Assigned Sites
IP Addresses
CM16
"PA1"
"192.168.1.33"
PACKT001
"PA1"
"192.168.1.15...


For the SQL-based report, provide a name and description, if needed.
Type
SQL-based Report
Create a traditional report which is based directly off the database using straight SQL statements and stored procedures.
Information
Name:
Packt Report
Description:
Server:
CM16.doctor.com
Path:
Packt
Browse...


Report Path
Select the folder where the new report should be created using the list below:
Administrative Security
Alerts
Asset Intelligence
Client Push
Client Status
Company Resource Access
Compliance and Settings Management
Data Warehouse
Device Management
Driver Management
Endpoint Protection
Hardware - CD-ROM
Hardware - Disk
Hardware - General
Hardware - Memory
OK
Cancel


Monitoring
Network
Network Access Protection
Operating System
Packt
Packt 1 items
Search
Icon
Name
Category
Packt Report
Packt


Built-in Fields
Parameters
Images
Data Sources
AutoGen__5C6358F2_4BB6_4a1b_A16E_8D96795D8602_
Datasets
DataSet0
Netbios_Name0
Name0
MaxClockSpeed0
DeviceID0
DataSet1
MaxClockSpeed0
MaxClockSpeed0_da0fbabcf0f
DataSetAdminID
UserSIDs

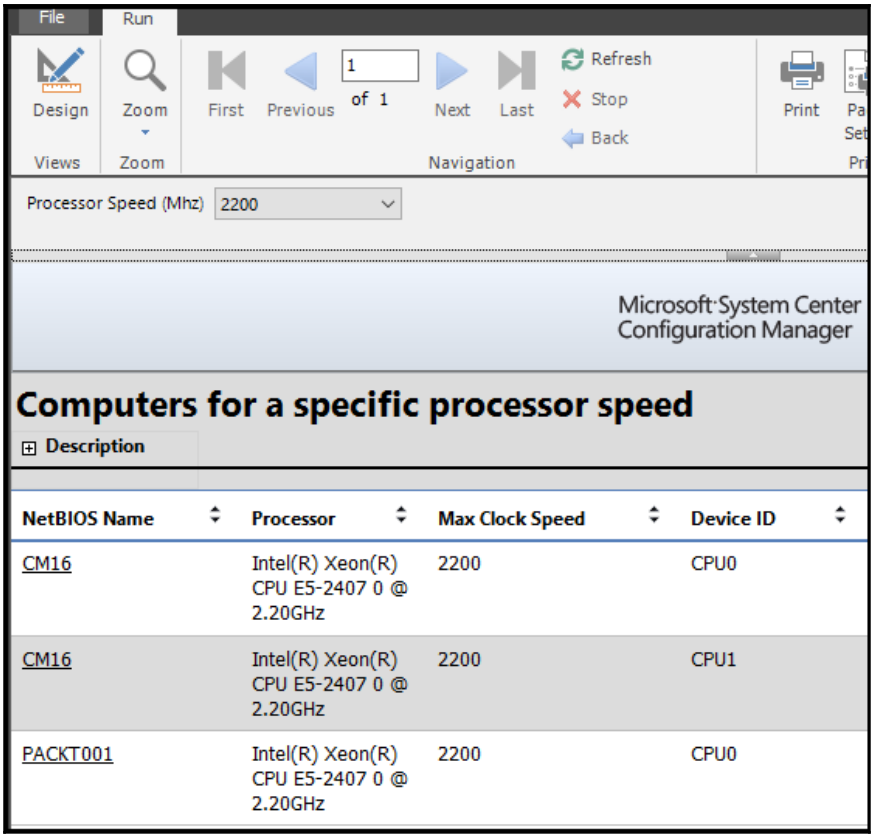

DataSet0
Use a shared dataset.
Use a dataset embedded in my report.
Data source:
AutoGen__5C6358F2_4BB6_4a1b_A16E_8D96795D860
New...
Query type:
Text
Table
Stored Procedure
Query:
SELECT DISTINCT SYS.Netbios_Name0, Processor.Name0,
Processor.MaxClockSpeed0,
Processor.DeviceID0
FROM fn_rbac_R_System(@UserSIDs) SYS
JOIN fn_rbac_GS_PROCESSOR(@UserSIDs) Processor on SYS.ResourceID =
Processor.ResourceID
WHERE Processor.MaxClockSpeed0 = @variable
ORDER BY SYS.Netbios_Name0
Query Designer...
Import...
Refresh Fields

Microsoft System Center Configuration Manager

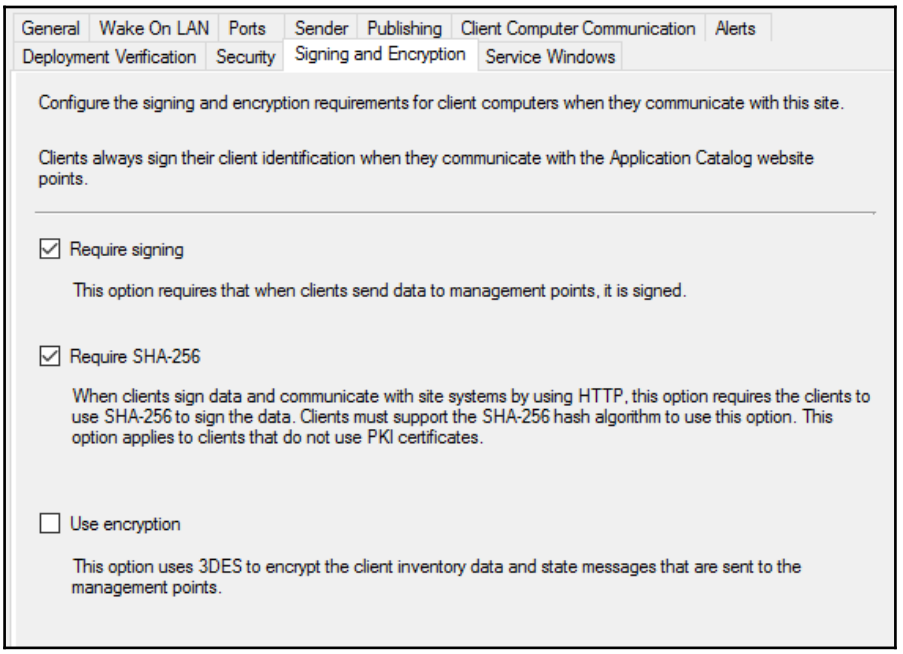
«Expr»

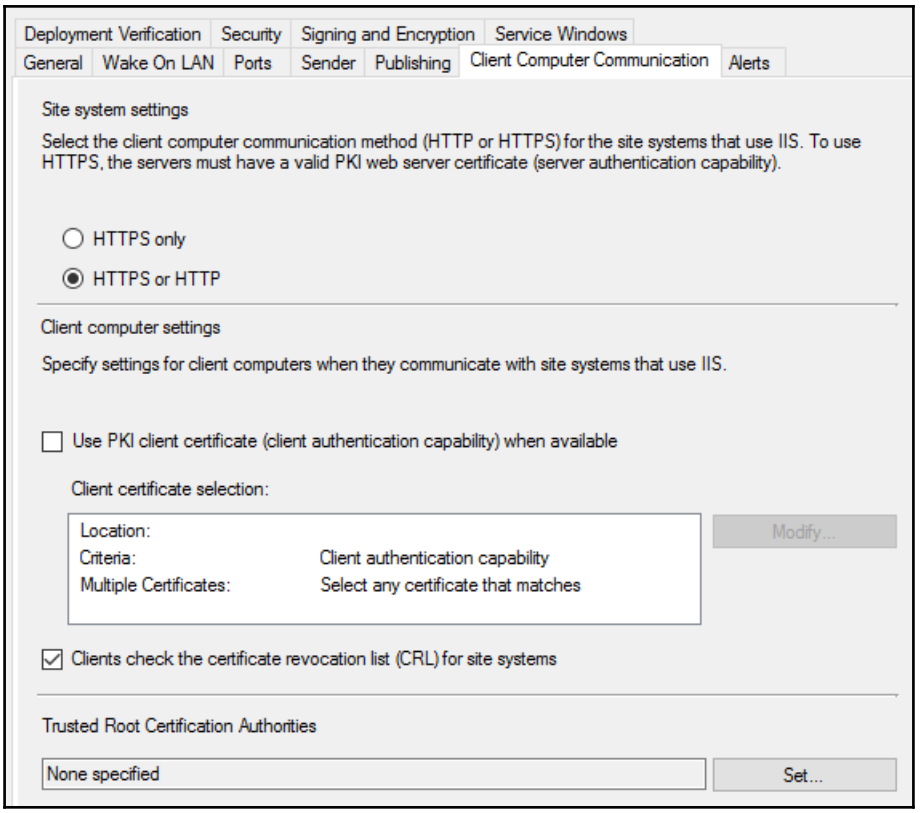
«Expr» «Expr»

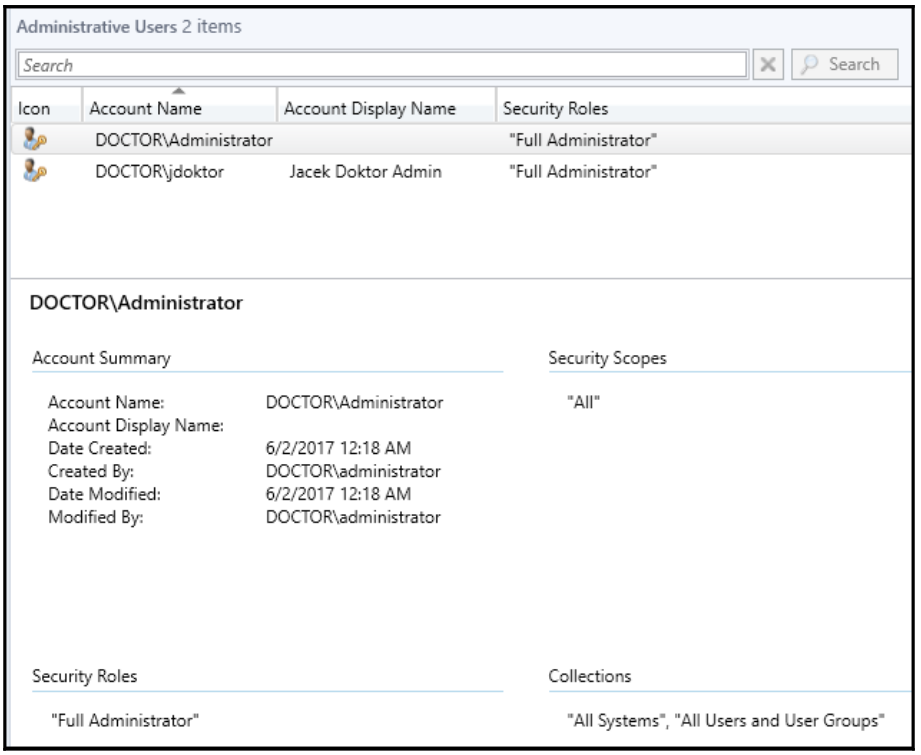
| «Expr» | «Expr» | «Expr» | «Expr» |
|---|---|---|---|
| [Netbios_Name0] | [Name0] | [MaxClockSpeed0] | [DeviceID0] |

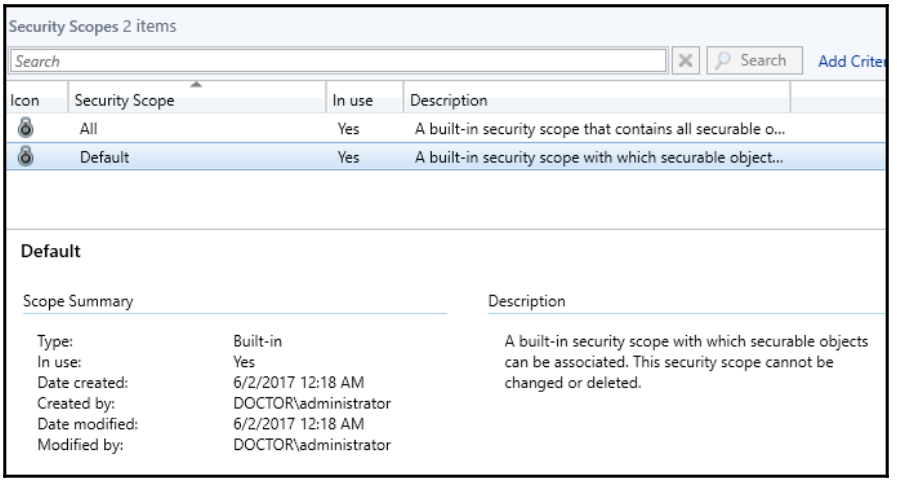


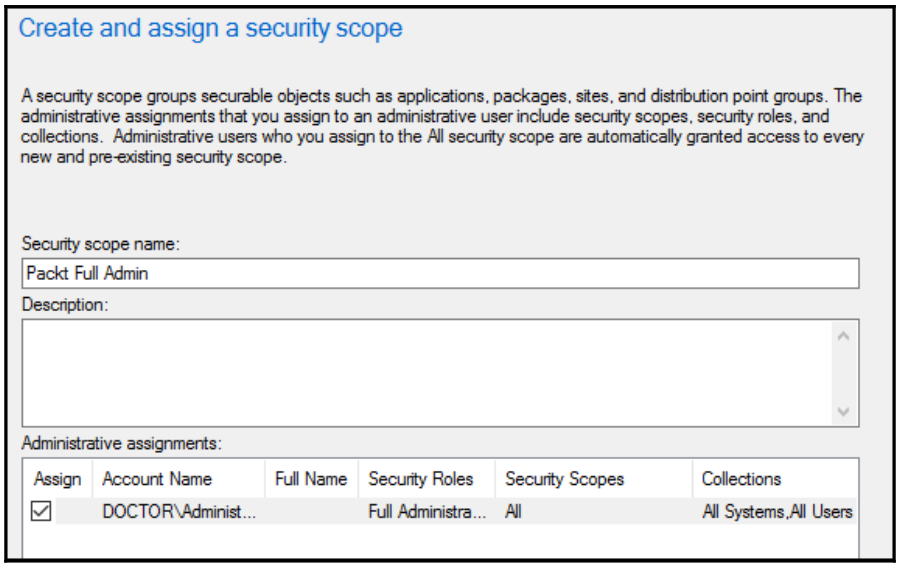
# Chapter 12: Role-Based Administration and Security



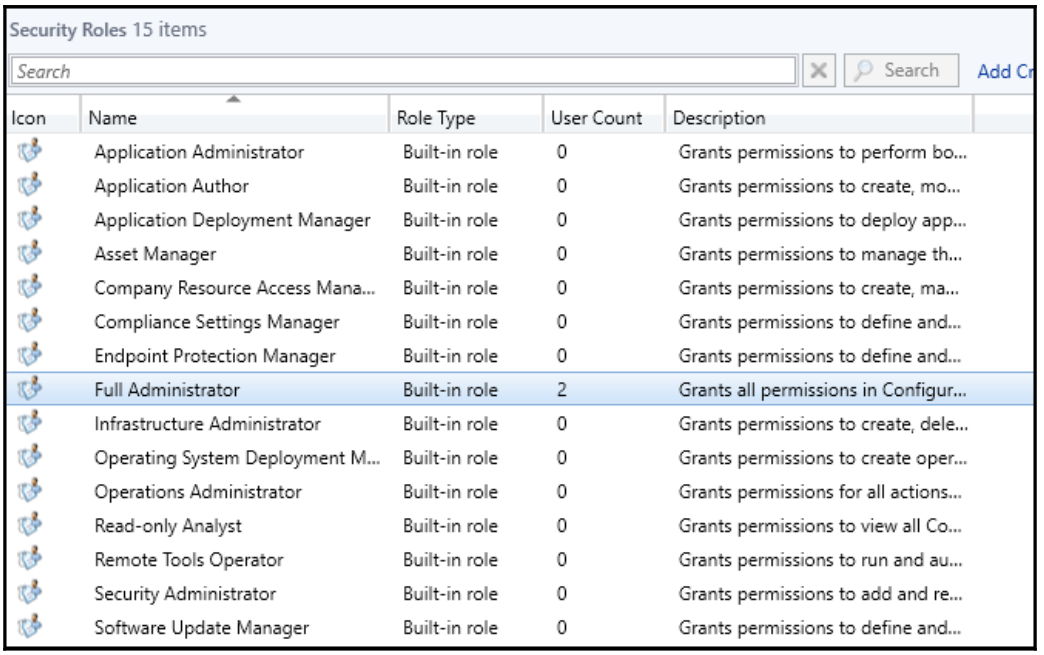

Deployment Verification
Security
Signing and Encryption
Service Windows
General
Wake On LAN
Ports
Sender
Publishing
Client Computer Communication
Alerts
Site system settings
Select the client computer communication method (HTTP or HTTPS) for the site systems that use IIS. To use HTTPS, the servers must have a valid PKI web server certificate (server authentication capability).
HTTPS only
HTTPS or HTTP
Client computer settings
Specify settings for client computers when they communicate with site systems that use IIS.
Use PKI client certificate (client authentication capability) when available
Client certificate selection:
Location:
Criteria:
Client authentication capability
Multiple Certificates:
Select any certificate that matches
Modify...
Clients check the certificate revocation list (CRL) for site systems
Trusted Root Certification Authorities
None specified
Set...

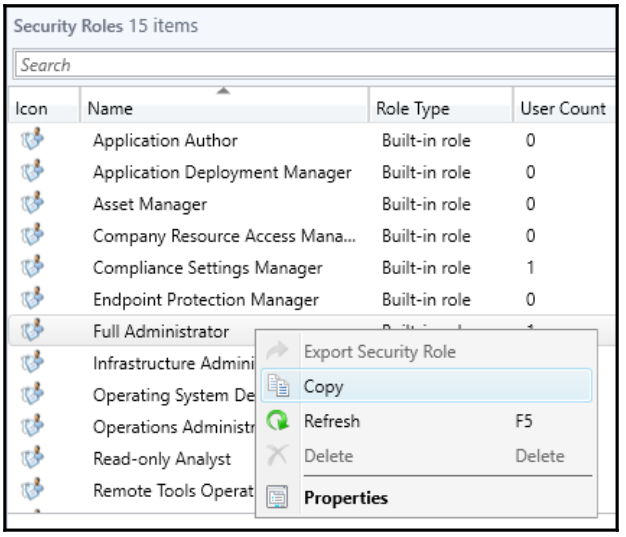

Administrative Users 2 items
Search
Search
Icon
Account Name
Account Display Name
Security Roles
DOCTOR\Administrator
"Full Administrator"
DOCTOR\jdoktor
Jacek Doktor Admin
"Full Administrator"
DOCTOR\Administrator
Account Summary
Account Name: DOCTOR\Administrator
Account Display Name:
Date Created: 6/2/2017 12:18 AM
Created By: DOCTOR\administrator
Date Modified: 6/2/2017 12:18 AM
Modified By: DOCTOR\administrator
Security Scopes
"All"
Security Roles
"Full Administrator"
Collections
"All Systems", "All Users and User Groups"

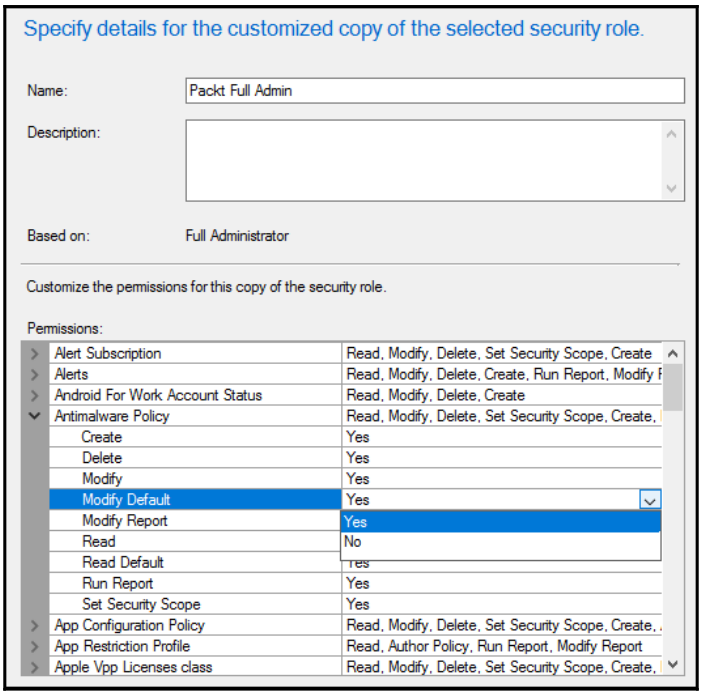

Security Scopes 2 items
Search
Search
Add Crite
Icon
Security Scope
In use
Description
All
Yes
A built-in security scope that contains all securable o...
Default
Yes
A built-in security scope with which securable object...
Default
Scope Summary
Type: Built-in
In use: Yes
Date created: 6/2/2017 12:18 AM
Created by: DOCTOR\administrator
Date modified: 6/2/2017 12:18 AM
Modified by: DOCTOR\administrator
Description
A built-in security scope with which securable objects can be associated. This security scope cannot be changed or deleted.

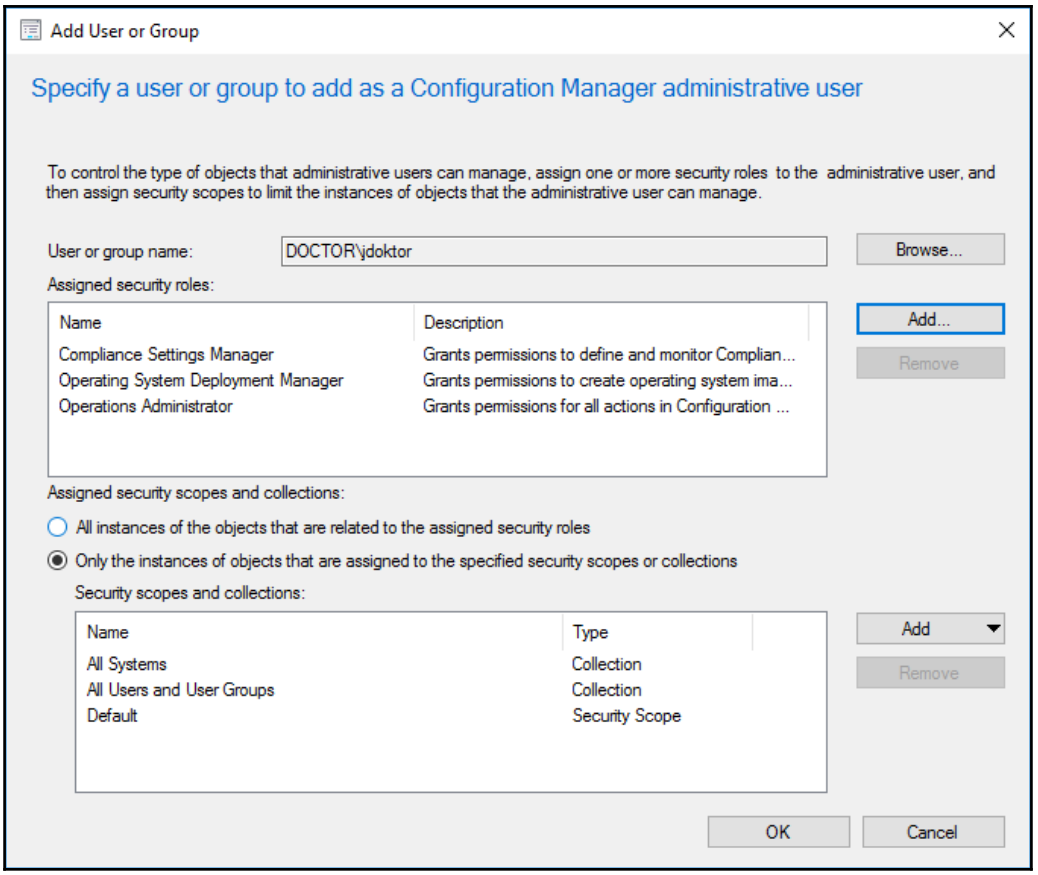

Create and assign a security scope
A security scope groups securable objects such as applications, packages, sites, and distribution point groups. The administrative assignments that you assign to an administrative user include security scopes, security roles, and collections. Administrative users who you assign to the All security scope are automatically granted access to every new and pre-existing security scope.
Security scope name:
Packt Full Admin
Description:
Administrative assignments:
Assign
Account Name
Full Name
Security Roles
Security Scopes
Collections
DOCTOR\Administ...
Full Administra...
All
All Systems,All Users

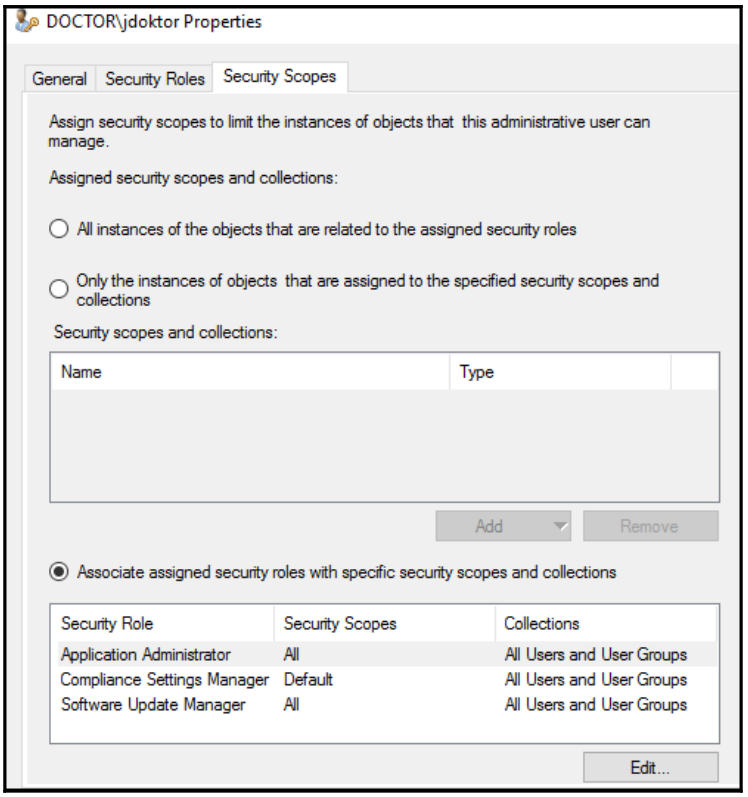

Set Security Scopes for Adobe Flash Player 10 ActiveX
Set the security scopes for the selected securable objects.
All objects must be associated with at least one security scope.
Available security scopes:
Default
Packt Full Admin

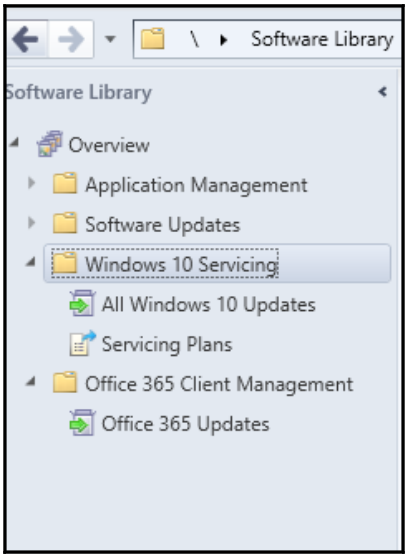

Security Roles 15 items
Search
Search
Add Cr
Icon
Name
Role Type
User Count
Description
Application Administrator
Built-in role
0
Grants permissions to perform bo...
Application Author
Built-in role
0
Grants permissions to create, mo...
Application Deployment Manager
Built-in role
0
Grants permissions to deploy app...
Asset Manager
Built-in role
0
Grants permissions to manage th...
Company Resource Access Mana...
Built-in role
0
Grants permissions to create, ma...
Compliance Settings Manager
Built-in role
0
Grants permissions to define and...
Endpoint Protection Manager
Built-in role
0
Grants permissions to define and...
Full Administrator
Built-in role
2
Grants all permissions in Configur...
Infrastructure Administrator
Built-in role
0
Grants permissions to create, dele...
Operating System Deployment M...
Built-in role
0
Grants permissions to create oper...
Operations Administrator
Built-in role
0
Grants permissions for all actions...
Read-only Analyst
Built-in role
0
Grants permissions to view all Co...
Remote Tools Operator
Built-in role
0
Grants permissions to run and au...
Security Administrator
Built-in role
0
Grants permissions to add and re...
Software Update Manager
Built-in role
0
Grants permissions to define and...

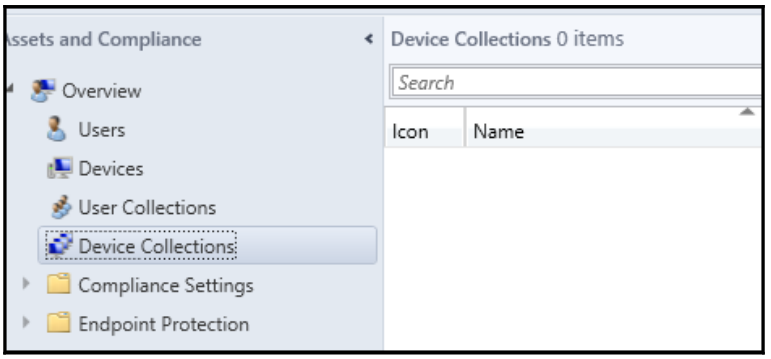

Security Roles 15 items
Search
Icon
Name
Role Type
User Count
Application Author
Built-in role
0
Application Deployment Manager
Built-in role
0
Asset Manager
Built-in role
0
Company Resource Access Mana...
Built-in role
0
Compliance Settings Manager
Built-in role
1
Endpoint Protection Manager
Built-in role
0
Full Administrator
Infrastructure Admini
Operating System De
Operations Administr
Read-only Analyst
Remote Tools Operat
Export Security Role
Copy
Refresh
F5
Delete
Delete
Properties

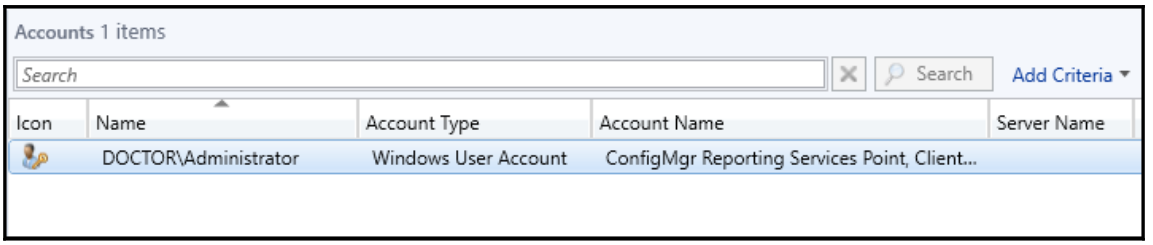

Specify details for the customized copy of the selected security role.
Name:
Packt Full Admin
Description:
Based on:
Full Administrator
Customize the permissions for this copy of the security role.
Permissions:
Alert Subscription
Read, Modify, Delete, Set Security Scope, Create
Alerts
Read, Modify, Delete, Create, Run Report, Modify
Android For Work Account Status
Read, Modify, Delete, Create
Antimalware Policy
Read, Modify, Delete, Set Security Scope, Create,
Create
Yes
Delete
Yes
Modify
Yes
Modify Default
Yes
Modify Report
Yes
No
Read
Read Default
Run Report
Yes
Set Security Scope
Yes
App Configuration Policy
Read, Modify, Delete, Set Security Scope, Create,
App Restriction Profile
Read, Author Policy, Run Report, Modify Report
Apple Vpp Licenses class
Read, Modify, Delete, Set Security Scope, Create,

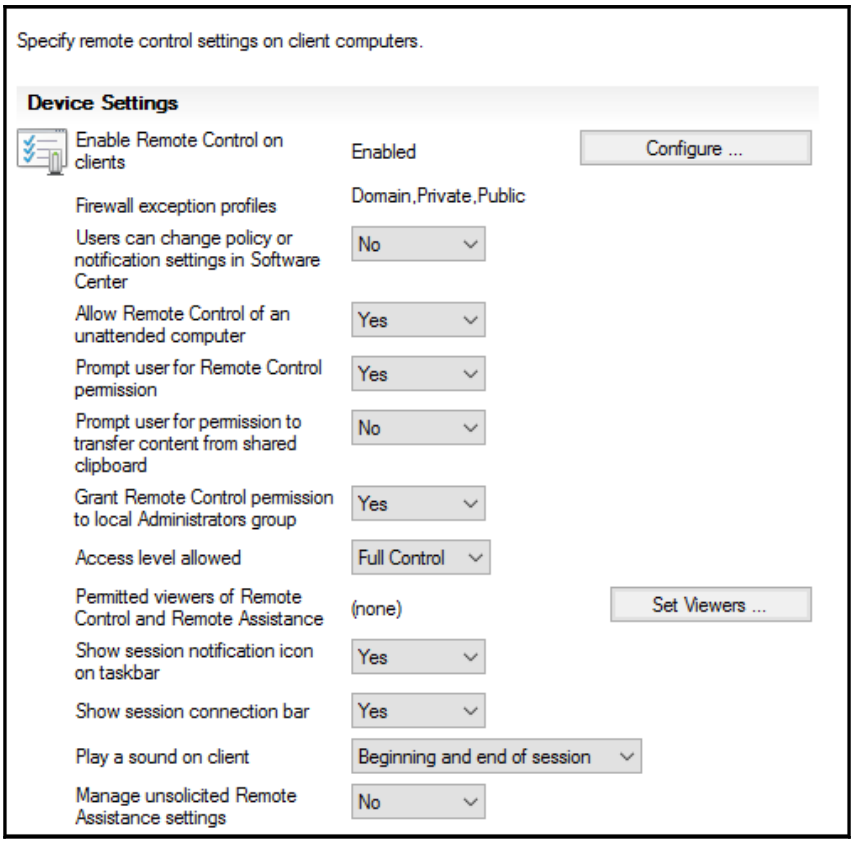

Add User or Group
Specify a user or group to add as a Configuration Manager administrative user
To control the type of objects that administrative users can manage, assign one or more security roles to the administrative user, and then assign security scopes to limit the instances of objects that the administrative user can manage.
User or group name:
DOCTOR\jdoktor
Browse...
Assigned security roles:
Name
Description
Compliance Settings Manager
Grants permissions to define and monitor Complian...
Operating System Deployment Manager
Grants permissions to create operating system ima...
Operations Administrator
Grants permissions for all actions in Configuration ...
Add...
Remove
Assigned security scopes and collections:
All instances of the objects that are related to the assigned security roles
Only the instances of objects that are assigned to the specified security scopes or collections
Security scopes and collections:
Name
Type
All Systems
Collection
All Users and User Groups
Collection
Default
Security Scope
Add
Remove
OK
Cancel

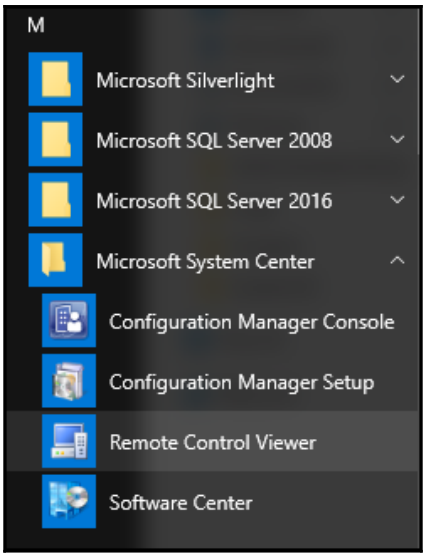

DOCTOR\jdoktor Properties
General
Security Roles
Security Scopes
Assign security scopes to limit the instances of objects that this administrative user can manage.
Assigned security scopes and collections:
All instances of the objects that are related to the assigned security roles
Only the instances of objects that are assigned to the specified security scopes and collections
Security scopes and collections:
Name
Type
Add
Remove
Associate assigned security roles with specific security scopes and collections
Security Role
Security Scopes
Collections
Application Administrator
All
All Users and User Groups
Compliance Settings Manager
Default
All Users and User Groups
Software Update Manager
All
All Users and User Groups
Edit...


Software Library
Software Library
Overview
Application Management
Software Updates
Windows 10 Servicing
All Windows 10 Updates
Servicing Plans
Office 365 Client Management
Office 365 Updates

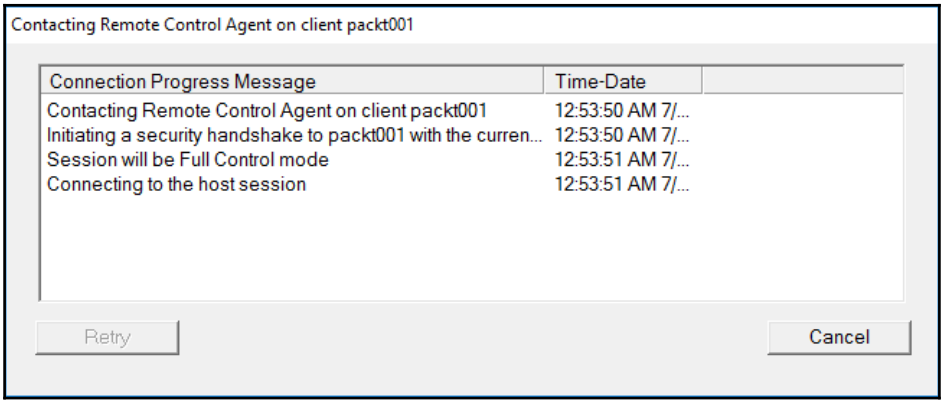

ssets and Compliance
Overview
Users
Devices
User Collections
Device Collections
Compliance Settings
Endpoint Protection
Device Collections 0 items
Search
Icon
Name

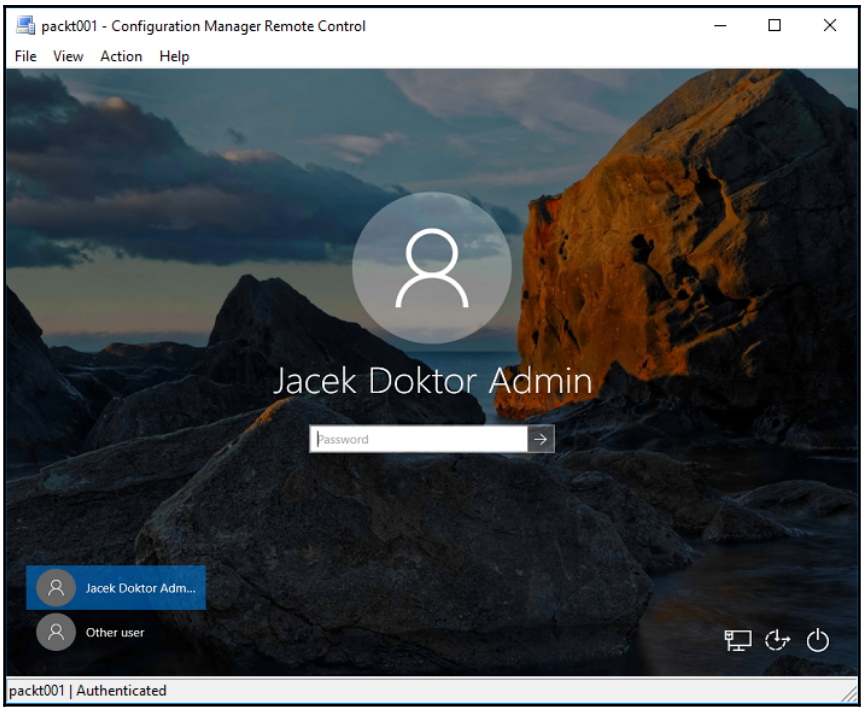

Accounts 1 items
Search
Search
Add Criteria
Icon
Name
Account Type
Account Name
Server Name
DOCTOR\Administrator
Windows User Account
ConfigMgr Reporting Services Point, Client...


Specify remote control settings on client computers.
Device Settings
Enable Remote Control on clients
Enabled
Configure ...
Firewall exception profiles
Domain,Private,Public
Users can change policy or notification settings in Software Center
No
Allow Remote Control of an unattended computer
Yes
Prompt user for Remote Control permission
Yes
Prompt user for permission to transfer content from shared clipboard
No
Grant Remote Control permission to local Administrators group
Yes
Access level allowed
Full Control
Permitted viewers of Remote Control and Remote Assistance
(none)
Set Viewers ...
Show session notification icon on taskbar
Yes
Show session connection bar
Yes
Play a sound on client
Beginning and end of session
Manage unsolicited Remote Assistance settings
No

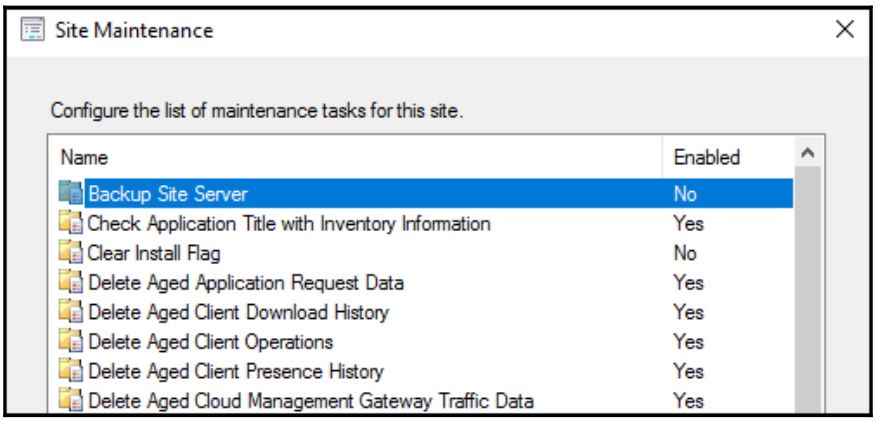

M
Microsoft Silverlight
Microsoft SQL Server 2008
Microsoft SQL Server 2016
Microsoft System Center
Configuration Manager Console
Configuration Manager Setup
Remote Control Viewer
Software Center

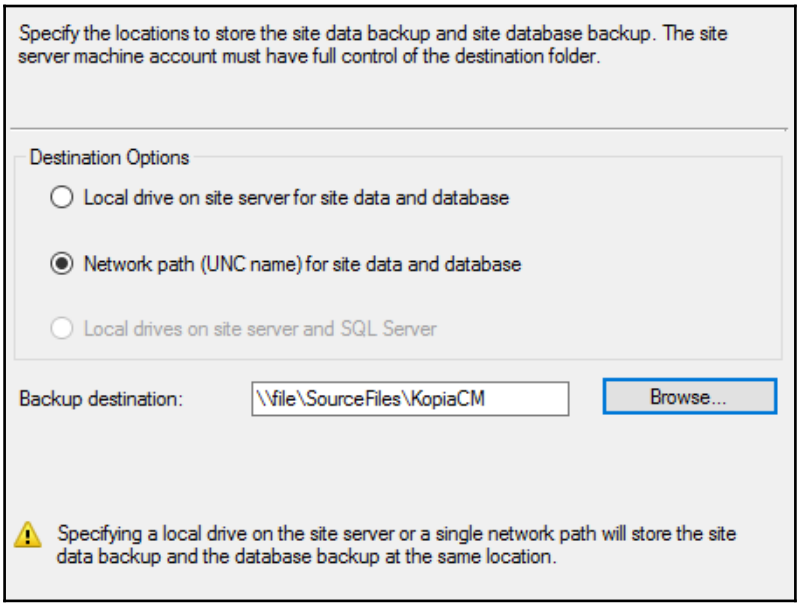

Configuration Manager Remote Control
File View Action Help

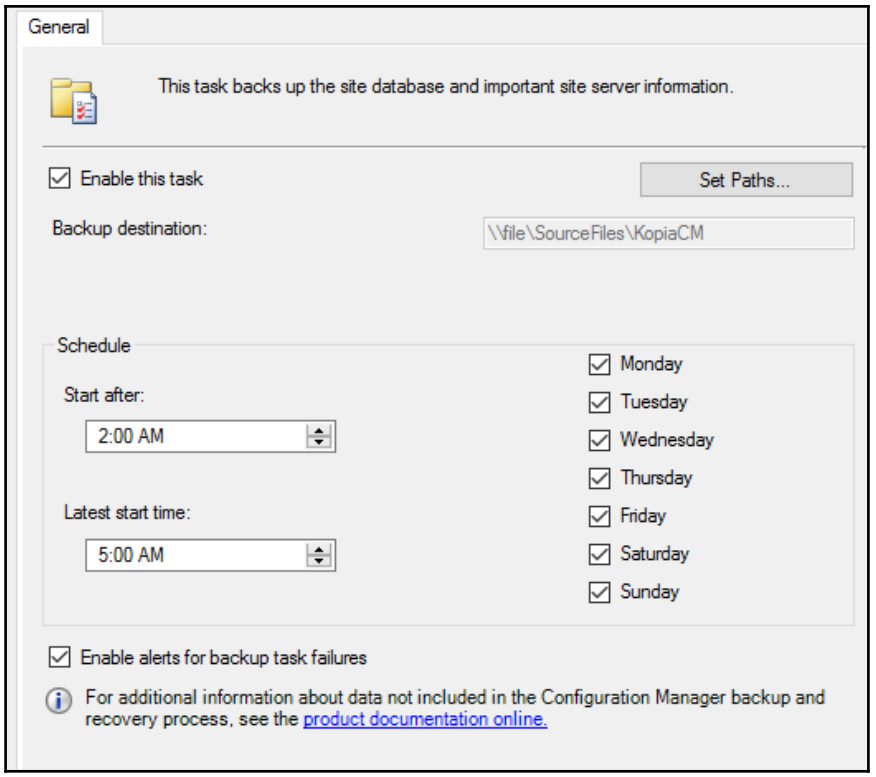

Contacting Remote Control Agent on client packt001
Connection Progress Message
Time-Date
Contacting Remote Control Agent on client packt001
12:53:50 AM 7/...
Initiating a security handshake to packt001 with the curren...
12:53:50 AM 7/...
Session will be Full Control mode
12:53:51 AM 7/...
Connecting to the host session
12:53:51 AM 7/...
Retry
Cancel

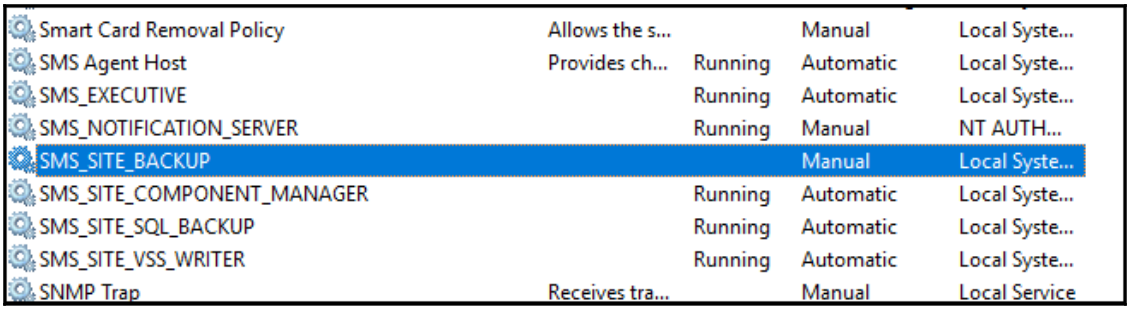

packkt001 - Configuration Manager Remote Control
File View Action Help
Jacek Doktor Admin
Password
Jacek Doktor Adm...
Other user
packkt001 | Authenticated

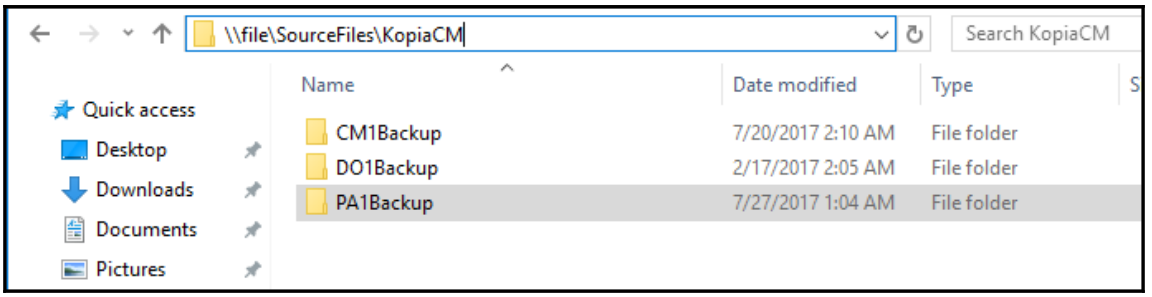
# Chapter 13: Site Server Maintenance Tasks

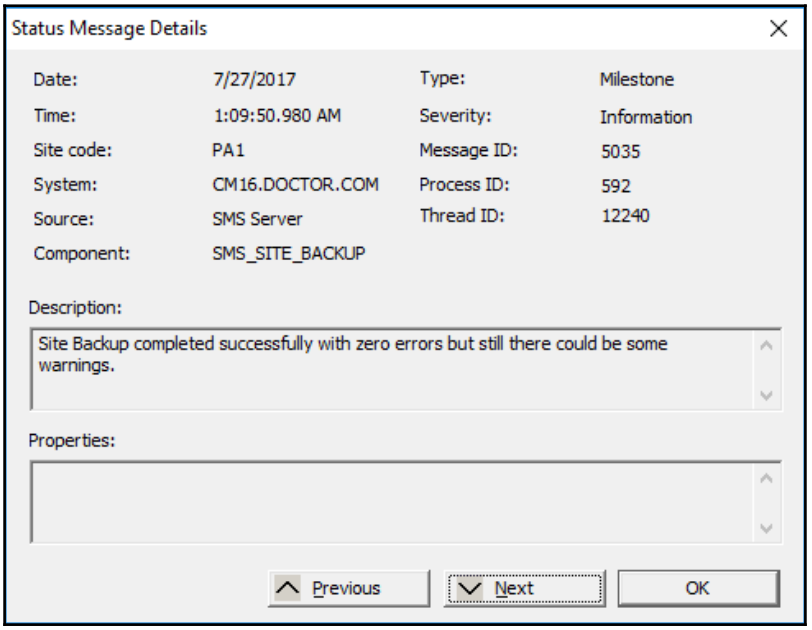


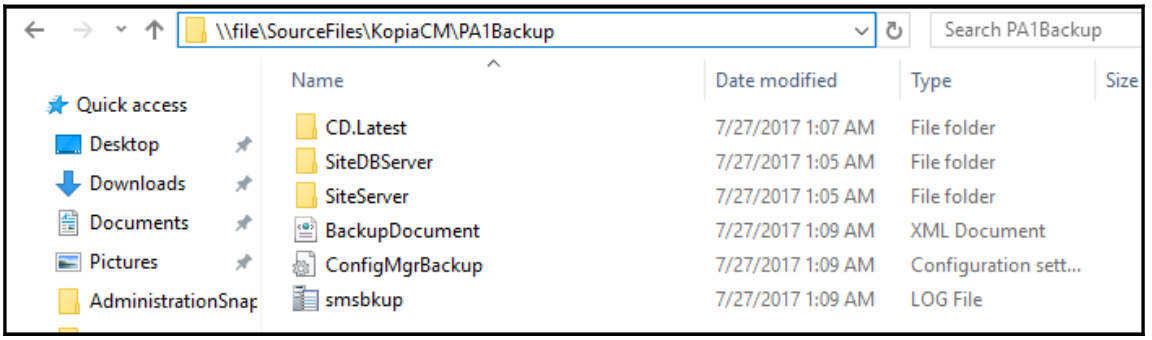



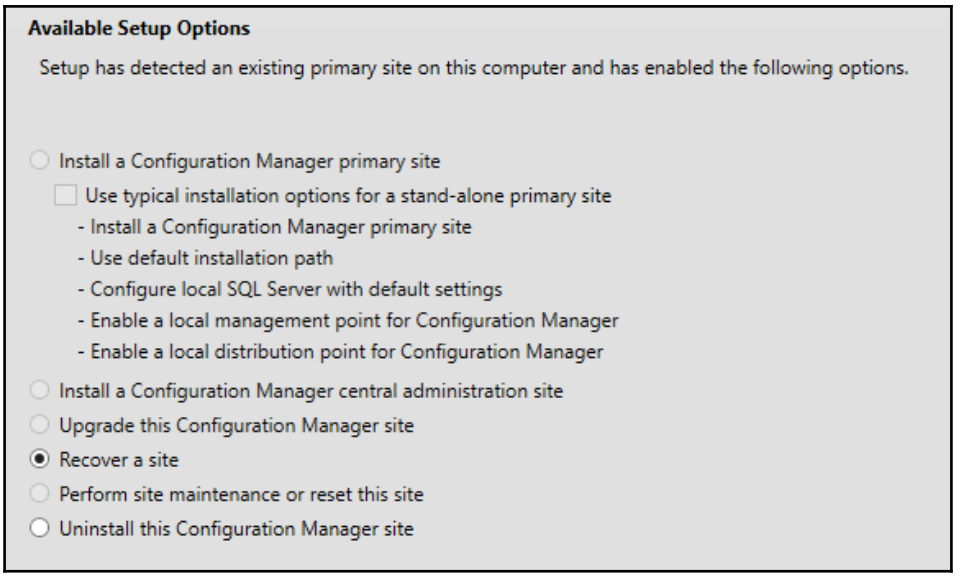

General
This task backs up the site database and important site server information.
Enable this task
Set Paths...
Backup destination:
\\file\SourceFiles\KopiaCM
Schedule
Start after:
2:00 AM
Latest start time:
5:00 AM
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
Sunday
Enable alerts for backup task failures
For additional information about data not included in the Configuration Manager backup and recovery process, see the product documentation online.

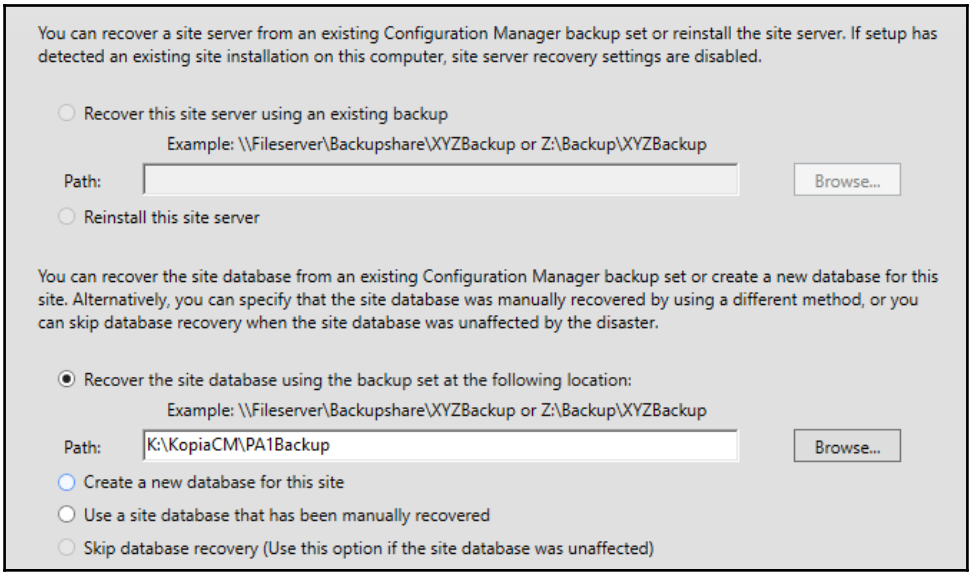

Smart Card Removal Policy Allows the s... Manual Local Syste...
SMS Agent Host Provides ch... Running Automatic Local Syste...
SMS_EXECUTIVE Running Automatic Local Syste...
SMS_NOTIFICATION_SERVER Running Manual NT AUTH...
SMS_SITE_BACKUP Manual Local Syste...
SMS_SITE_COMPONENT_MANAGER Running Automatic Local Syste...
SMS_SITE_SQL_BACKUP Running Automatic Local Syste...
SMS_SITE_VSS_WRITER Running Automatic Local Syste...
SNMP Trap Receives tra... Manual Local Service

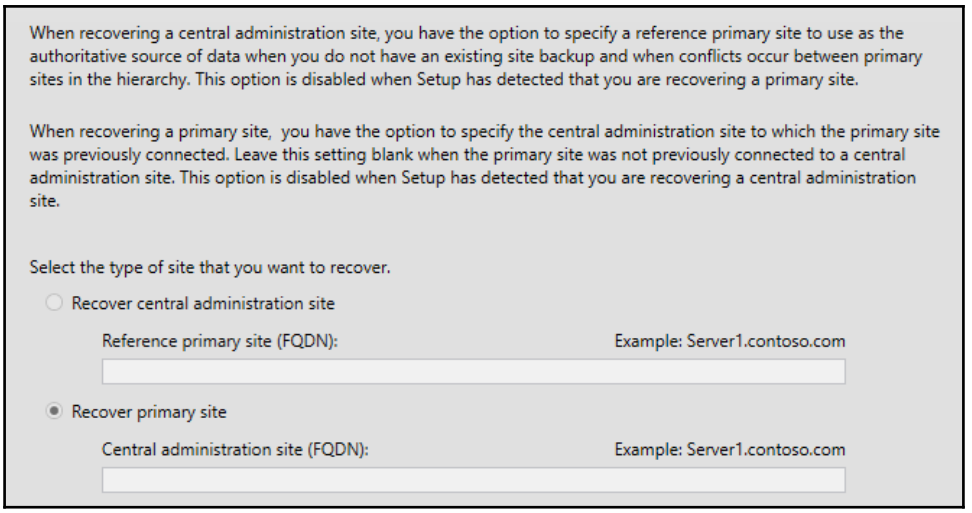

\\file\SourceFiles\KopiaCM
Search KopiaCM
Quick access
Desktop
Downloads
Documents
Pictures
Name
Date modified
Type
CM1Backup
7/20/2017 2:10 AM
File folder
DO1Backup
2/17/2017 2:05 AM
File folder
PA1Backup
7/27/2017 1:04 AM
File folder

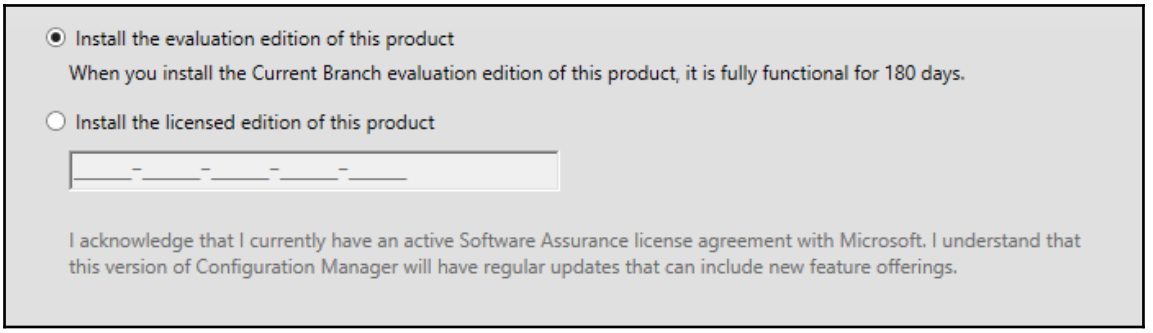

Status Message Details
Date:
7/27/2017
Type:
Milestone
Time:
1:09:50.980 AM
Severity:
Information
Site code:
PA1
Message ID:
5035
System:
CM16.DOCTOR.COM
Process ID:
592
Source:
SMS Server
Thread ID:
12240
Component:
SMS_SITE_BACKUP
Description:
Site Backup completed successfully with zero errors but still there could be some warnings.
Properties:
Previous
Next
OK

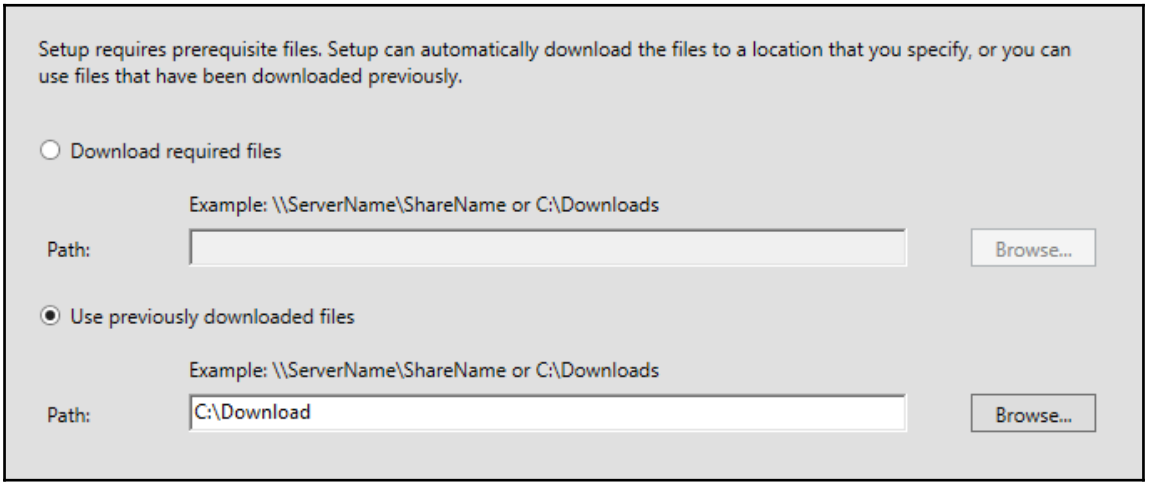

\\file\SourceFiles\KopiaCM\PA1Backup
Search PA1Backup
Quick access
Desktop
Downloads
Documents
Pictures
AdministrationSnap
Name
Date modified
Type
Size
CD.Latest
7/27/2017 1:07 AM
File folder
SiteDBServer
7/27/2017 1:05 AM
File folder
SiteServer
7/27/2017 1:05 AM
File folder
BackupDocument
7/27/2017 1:09 AM
XML Document
ConfigMgrBackup
7/27/2017 1:09 AM
Configuration sett...
smsbkup
7/27/2017 1:09 AM
LOG File

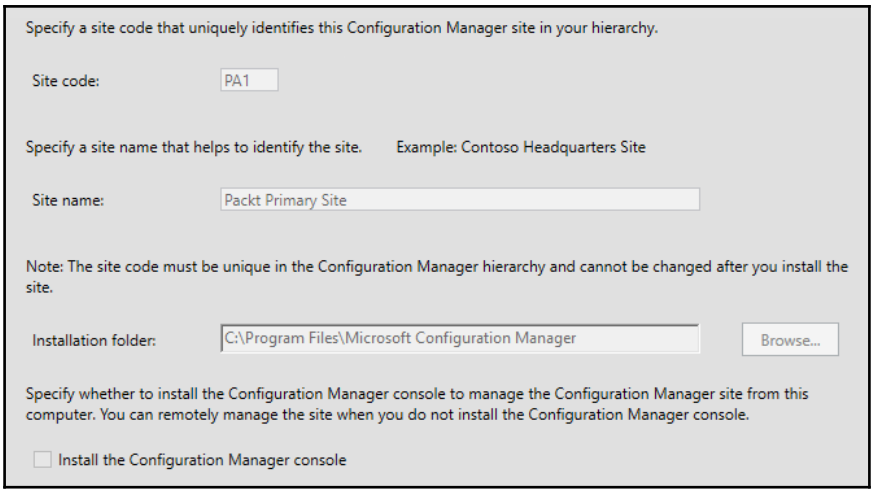

Available Setup Options
Setup has detected an existing primary site on this computer and has enabled the following options.
Install a Configuration Manager primary site
Use typical installation options for a stand-alone primary site
- Install a Configuration Manager primary site
- Use default installation path
- Configure local SQL Server with default settings
- Enable a local management point for Configuration Manager
- Enable a local distribution point for Configuration Manager
Install a Configuration Manager central administration site
Upgrade this Configuration Manager site
Recover a site
Perform site maintenance or reset this site
Uninstall this Configuration Manager site

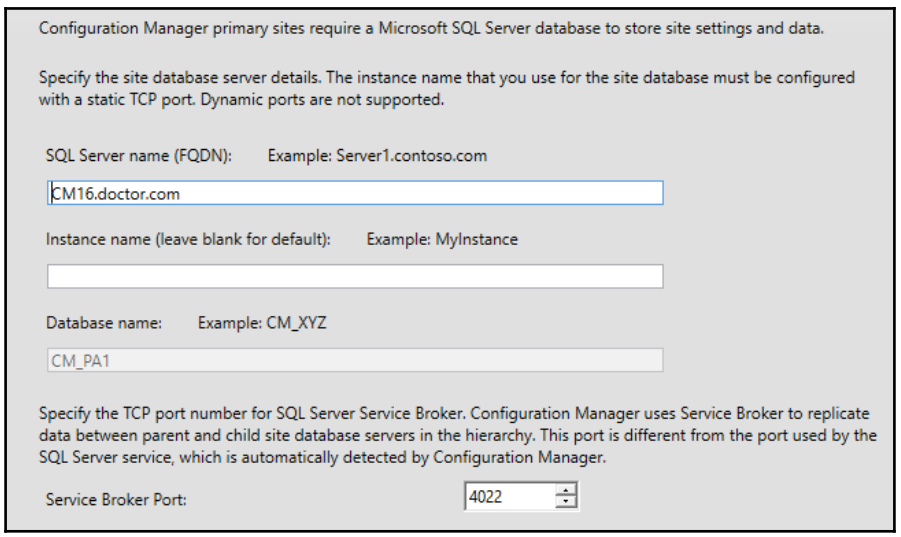

You can recover a site server from an existing Configuration Manager backup set or reinstall the site server. If setup has detected an existing site installation on this computer, site server recovery settings are disabled.
Recover this site server using an existing backup
Example: \\Fileserver\Backupshare\XYZBackup or Z:\Backup\XYZBackup
Path:
Browse...
Reinstall this site server
You can recover the site database from an existing Configuration Manager backup set or create a new database for this site. Alternatively, you can specify that the site database was manually recovered by using a different method, or you can skip database recovery when the site database was unaffected by the disaster.
Recover the site database using the backup set at the following location:
Example: \\Fileserver\Backupshare\XYZBackup or Z:\Backup\XYZBackup
Path:
K:\KopiaCM\PA1Backup
Browse...
Create a new database for this site
Use a site database that has been manually recovered
Skip database recovery (Use this option if the site database was unaffected)

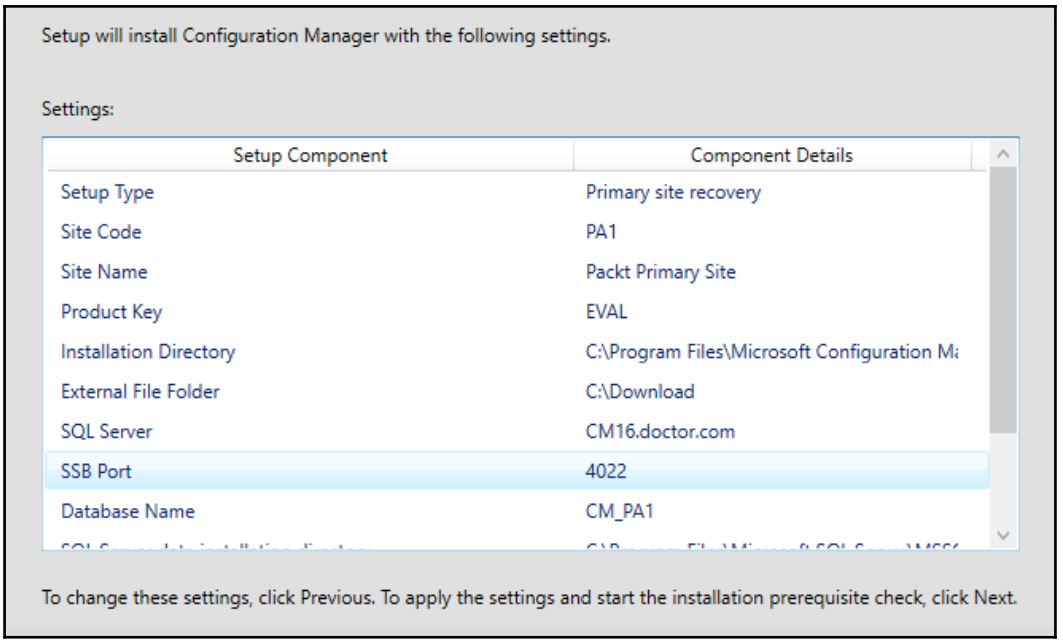

When recovering a central administration site, you have the option to specify a reference primary site to use as the authoritative source of data when you do not have an existing site backup and when conflicts occur between primary sites in the hierarchy. This option is disabled when Setup has detected that you are recovering a primary site.
When recovering a primary site, you have the option to specify the central administration site to which the primary site was previously connected. Leave this setting blank when the primary site was not previously connected to a central administration site. This option is disabled when Setup has detected that you are recovering a central administration site.
Select the type of site that you want to recover.
Recover central administration site
Reference primary site (FQDN):
Example: Server1.contoso.com
Recover primary site
Central administration site (FQDN):
Example: Server1.contoso.com

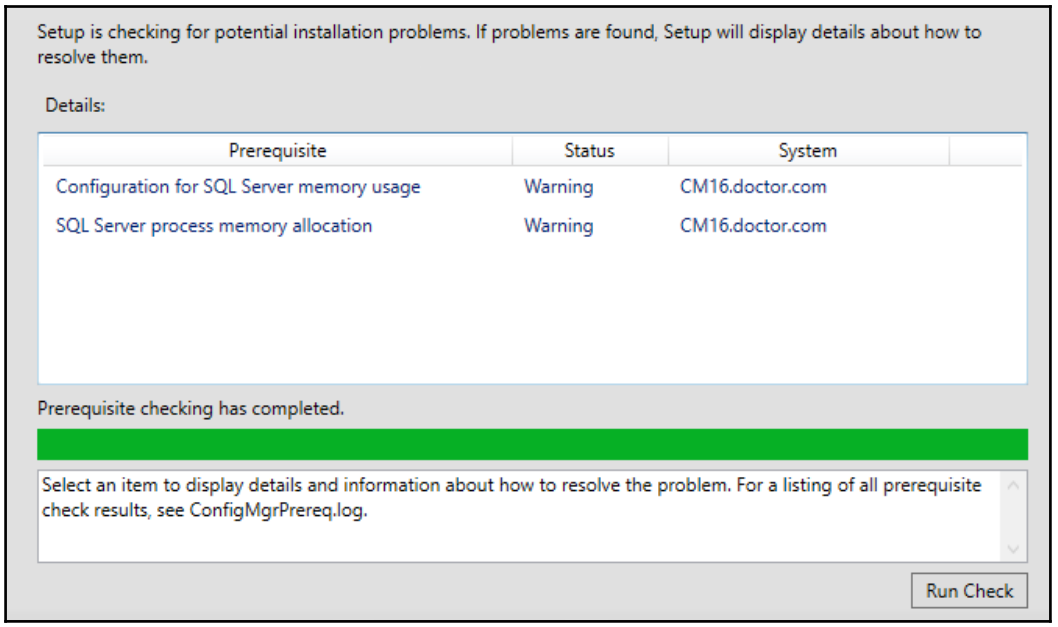

Install the evaluation edition of this product
When you install the Current Branch evaluation edition of this product, it is fully functional for 180 days.
Install the licensed edition of this product
I acknowledge that I currently have an active Software Assurance license agreement with Microsoft. I understand that this version of Configuration Manager will have regular updates that can include new feature offerings.


Setup requires prerequisite files. Setup can automatically download the files to a location that you specify, or you can use files that have been downloaded previously.
Download required files
Example: \\ServerName\ShareName or C:\Downloads
Path:
Browse...
Use previously downloaded files
Example: \\ServerName\ShareName or C:\Downloads
Path:
C:\Download
Browse...

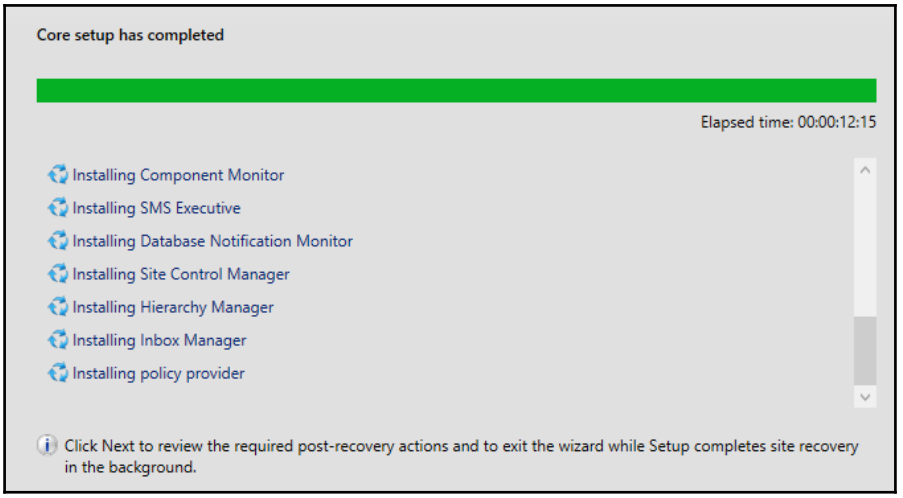

Specify a site code that uniquely identifies this Configuration Manager site in your hierarchy.
Site code:
PA1
Specify a site name that helps to identify the site.
Example: Contoso Headquarters Site
Site name:
Packt Primary Site
Note: The site code must be unique in the Configuration Manager hierarchy and cannot be changed after you install the site.
Installation folder:
C:\Program Files\Microsoft Configuration Manager
Browse...
Specify whether to install the Configuration Manager console to manage the Configuration Manager site from this computer. You can remotely manage the site when you do not install the Configuration Manager console.
Install the Configuration Manager console

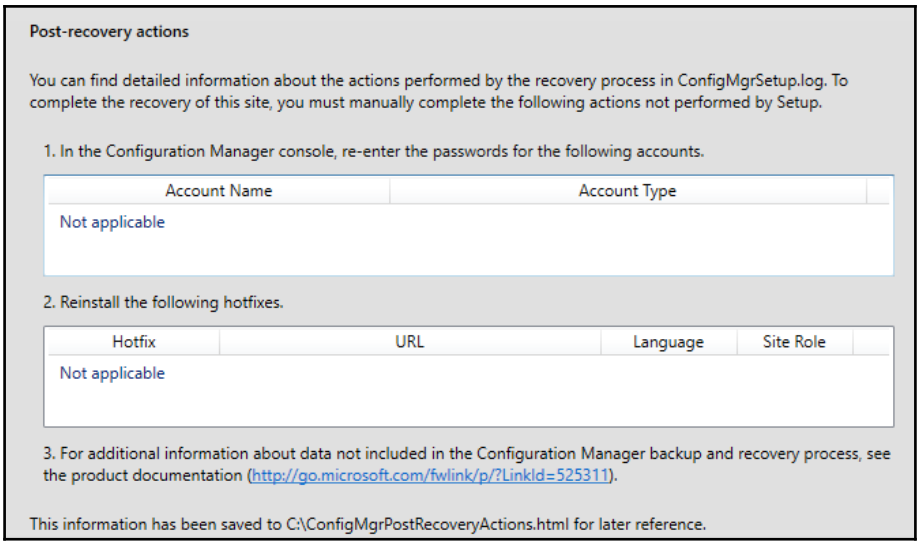

Configuration Manager primary sites require a Microsoft SQL Server database to store site settings and data.
Specify the site database server details. The instance name that you use for the site database must be configured with a static TCP port. Dynamic ports are not supported.
SQL Server name (FQDN):
Example: Server1.contoso.com
CM16.doctor.com
Instance name (leave blank for default):
Example: MyInstance
Database name:
Example: CM_XYZ
CM_PA1
Specify the TCP port number for SQL Server Service Broker. Configuration Manager uses Service Broker to replicate data between parent and child site database servers in the hierarchy. This port is different from the port used by the SQL Server service, which is automatically detected by Configuration Manager.
Service Broker Port:
4022

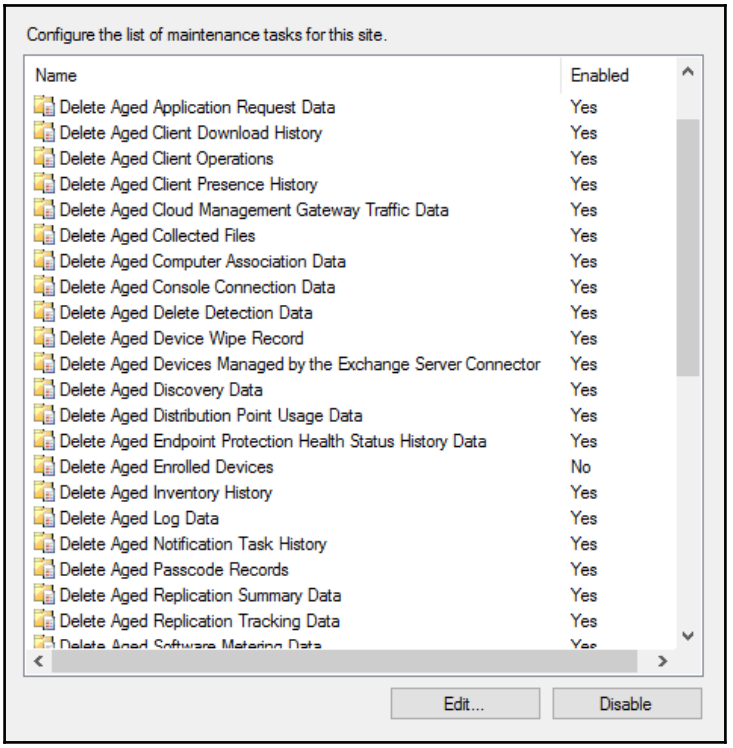

Setup will install Configuration Manager with the following settings.
Settings:
Setup Component
Component Details
Setup Type
Primary site recovery
Site Code
PA1
Site Name
Packt Primary Site
Product Key
EVAL
Installation Directory
C:\Program Files\Microsoft Configuration M
External File Folder
C:\Download
SQL Server
CM16.doctor.com
SSB Port
4022
Database Name
CM_PA1
To change these settings, click Previous. To apply the settings and start the installation prerequisite check, click Next.

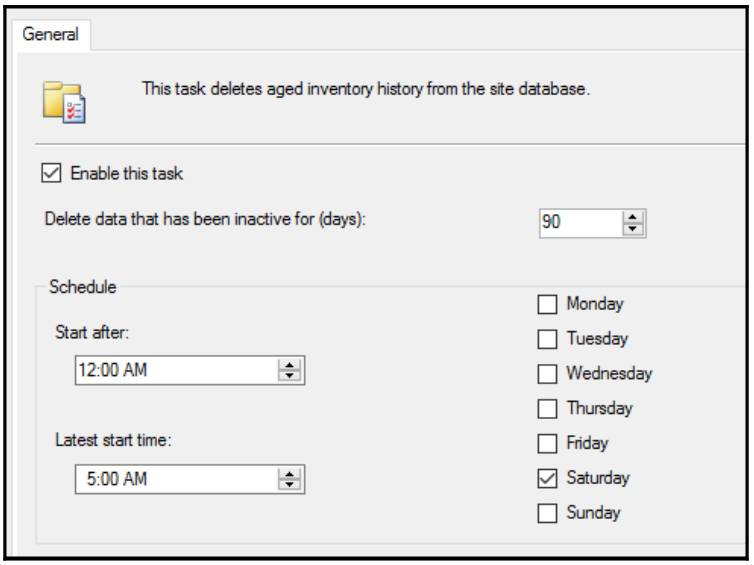

Setup is checking for potential installation problems. If problems are found, Setup will display details about how to resolve them.
Details:
Prerequisite
Status
System
Configuration for SQL Server memory usage
Warning
CM16.doctor.com
SQL Server process memory allocation
Warning
CM16.doctor.com
Prerequisite checking has completed.
Select an item to display details and information about how to resolve the problem. For a listing of all prerequisite check results, see ConfigMgrPrereq.log.
Run Check

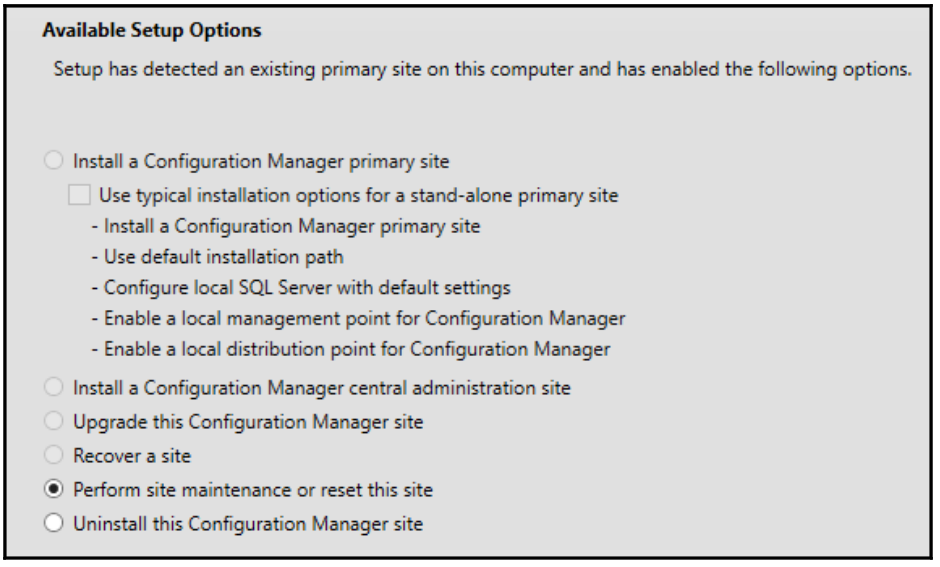

Overall progress
Elapsed time: 00:00:04:43
Evaluating setup environment
Stopping Configuration Manager services
Generating public key and SQL Server certificate
Setting up the SQL Server database

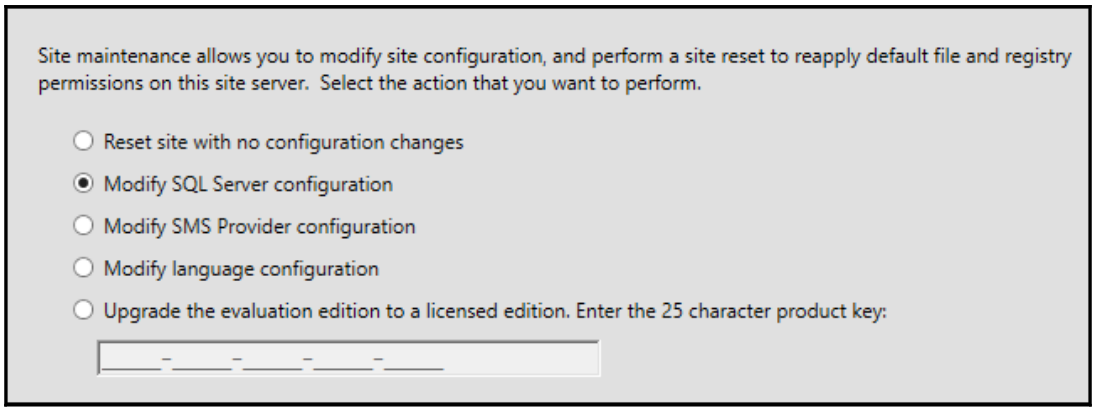

Core setup has completed
Elapsed time: 00:00:12:15
Installing Component Monitor
Installing SMS Executive
Installing Database Notification Monitor
Installing Site Control Manager
Installing Hierarchy Manager
Installing Inbox Manager
Installing policy provider
Click Next to review the required post-recovery actions and to exit the wizard while Setup completes site recovery in the background.

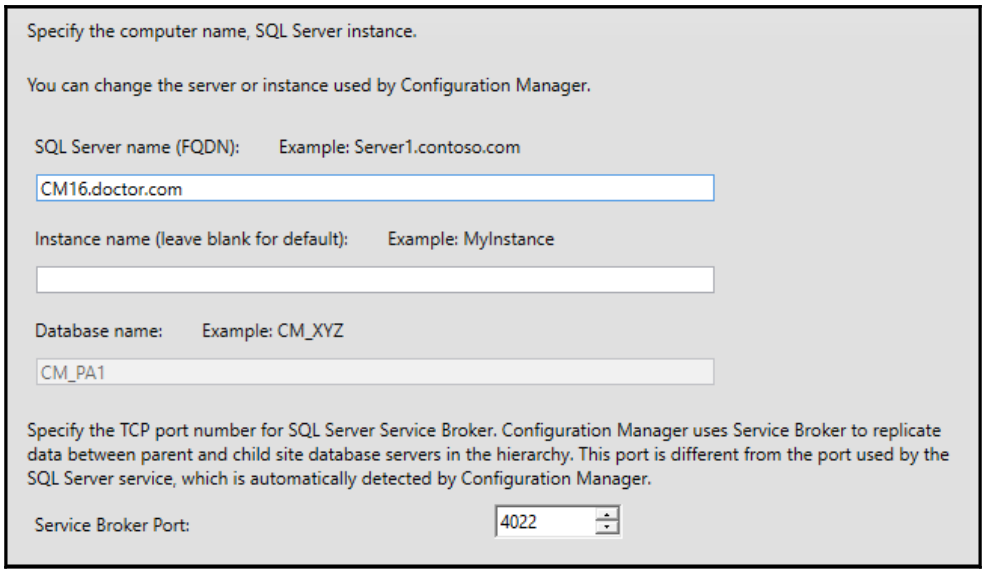

Post-recovery actions
You can find detailed information about the actions performed by the recovery process in ConfigMgrSetup.log. To complete the recovery of this site, you must manually complete the following actions not performed by Setup.
1. In the Configuration Manager console, re-enter the passwords for the following accounts.
Account Name
Account Type
Not applicable
2. Reinstall the following hotfixes.
Hotfix
URL
Language
Site Role
Not applicable
3. For additional information about data not included in the Configuration Manager backup and recovery process, see the product documentation (http://go.microsoft.com/fwlink/p/?LinkId=525311).
This information has been saved to C:\ConfigMgrPostRecoveryActions.html for later reference.

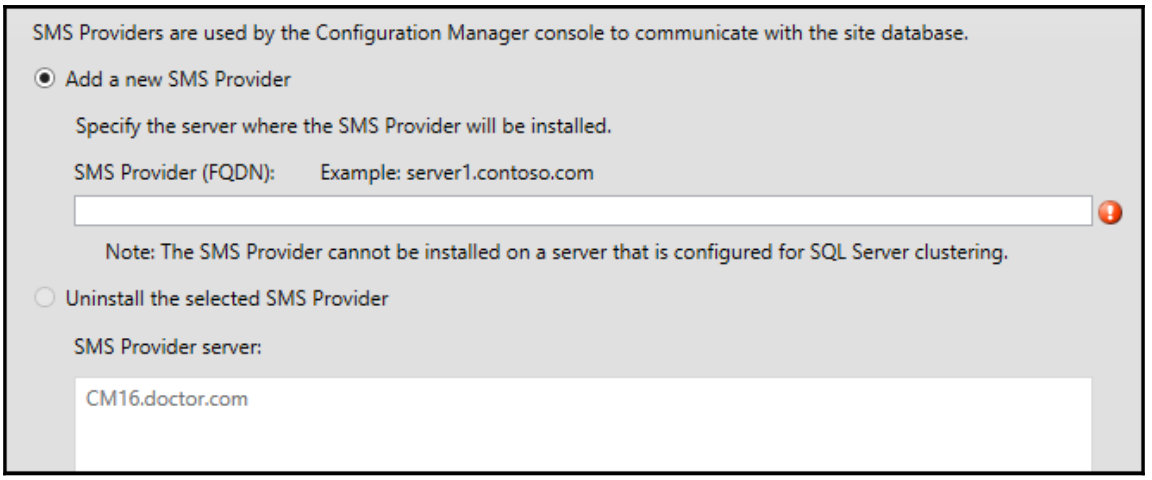

Configure the list of maintenance tasks for this site.
Name
Enabled
Delete Aged Application Request Data Yes
Delete Aged Client Download History Yes
Delete Aged Client Operations Yes
Delete Aged Client Presence History Yes
Delete Aged Cloud Management Gateway Traffic Data Yes
Delete Aged Collected Files Yes
Delete Aged Computer Association Data Yes
Delete Aged Console Connection Data Yes
Delete Aged Delete Detection Data Yes
Delete Aged Device Wipe Record Yes
Delete Aged Devices Managed by the Exchange Server Connector Yes
Delete Aged Discovery Data Yes
Delete Aged Distribution Point Usage Data Yes
Delete Aged Endpoint Protection Health Status History Data Yes
Delete Aged Enrolled Devices No
Delete Aged Inventory History Yes
Delete Aged Log Data Yes
Delete Aged Notification Task History Yes
Delete Aged Passcode Records Yes
Delete Aged Replication Summary Data Yes
Delete Aged Replication Tracking Data Yes
Edit...
Disable

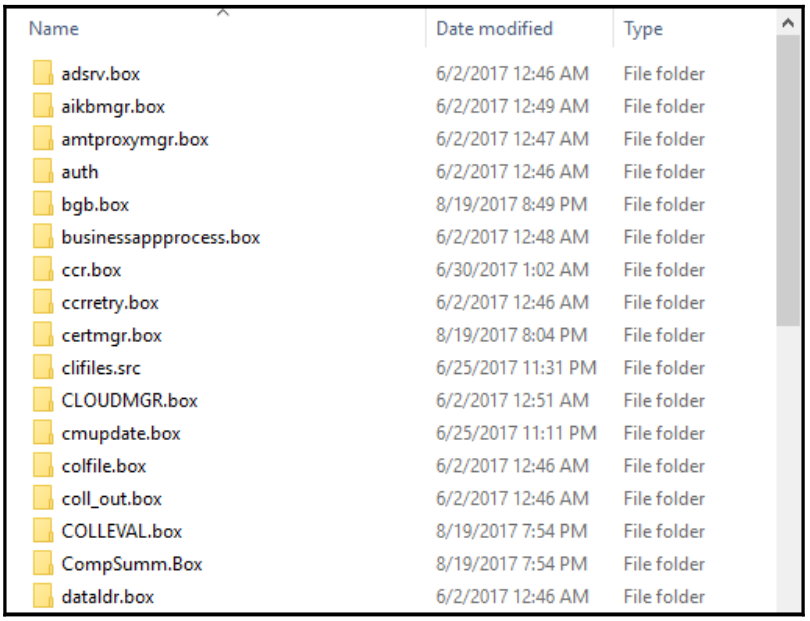

General
This task deletes aged inventory history from the site database.
Enable this task
Delete data that has been inactive for (days):
90
Schedule
Start after:
12:00 AM
Latest start time:
5:00 AM
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
Sunday

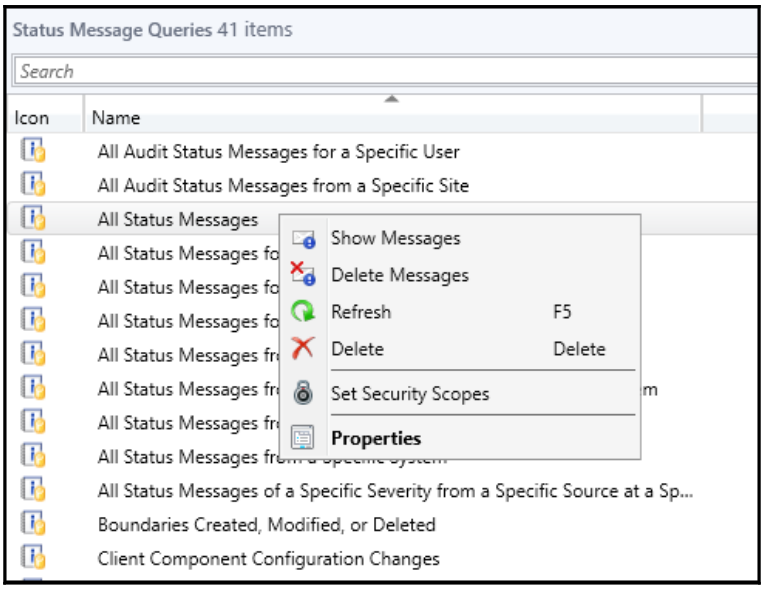

Available Setup Options
Setup has detected an existing primary site on this computer and has enabled the following options.
Install a Configuration Manager primary site
Use typical installation options for a stand-alone primary site
- Install a Configuration Manager primary site
- Use default installation path
- Configure local SQL Server with default settings
- Enable a local management point for Configuration Manager
- Enable a local distribution point for Configuration Manager
Install a Configuration Manager central administration site
Upgrade this Configuration Manager site
Recover a site
Perform site maintenance or reset this site
Uninstall this Configuration Manager site

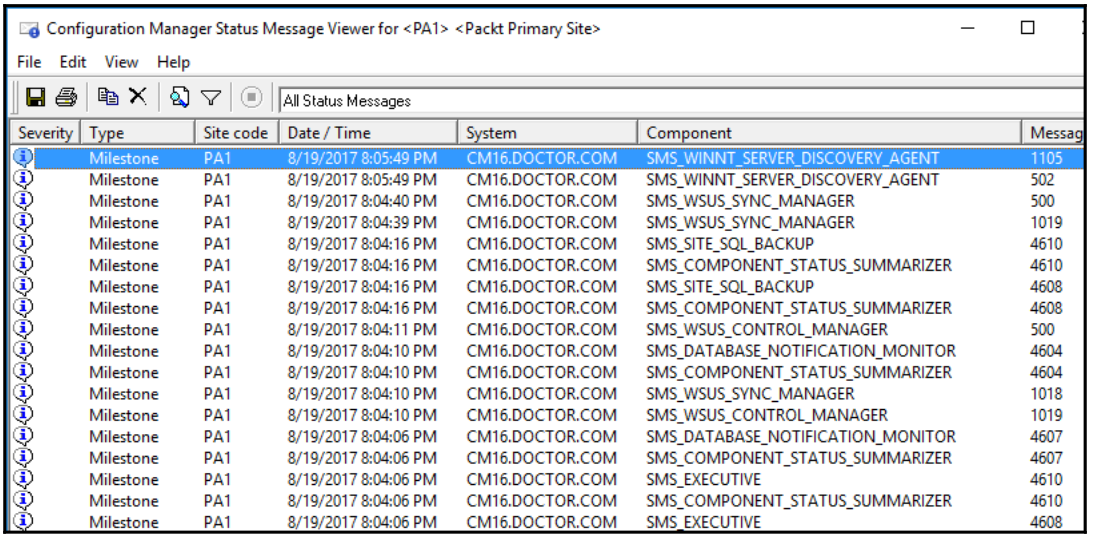

Site maintenance allows you to modify site configuration, and perform a site reset to reapply default file and registry permissions on this site server. Select the action that you want to perform.
Reset site with no configuration changes
Modify SQL Server configuration
Modify SMS Provider configuration
Modify language configuration
Upgrade the evaluation edition to a licensed edition. Enter the 25 character product key:


Specify the computer name, SQL Server instance.
You can change the server or instance used by Configuration Manager.
SQL Server name (FQDN): Example: Server1.contoso.com
CM16.doctor.com
Instance name (leave blank for default): Example: MyInstance
Database name: Example: CM_XYZ
CM_PA1
Specify the TCP port number for SQL Server Service Broker. Configuration Manager uses Service Broker to replicate data between parent and child site database servers in the hierarchy. This port is different from the port used by the SQL Server service, which is automatically detected by Configuration Manager.
Service Broker Port:
4022

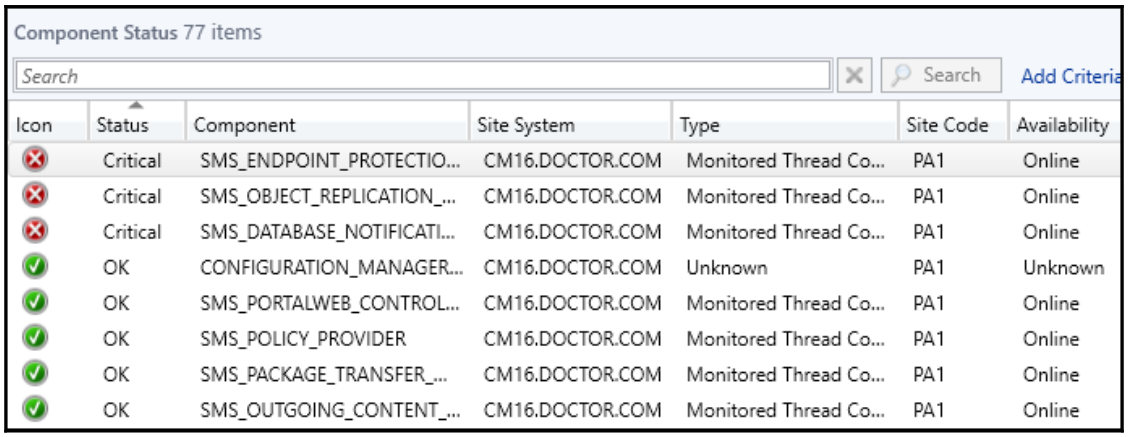

SMS Providers are used by the Configuration Manager console to communicate with the site database.
Add a new SMS Provider
Specify the server where the SMS Provider will be installed.
SMS Provider (FQDN):
Example: server1.contoso.com
Note: The SMS Provider cannot be installed on a server that is configured for SQL Server clustering.
Uninstall the selected SMS Provider
SMS Provider server:
CM16.doctor.com

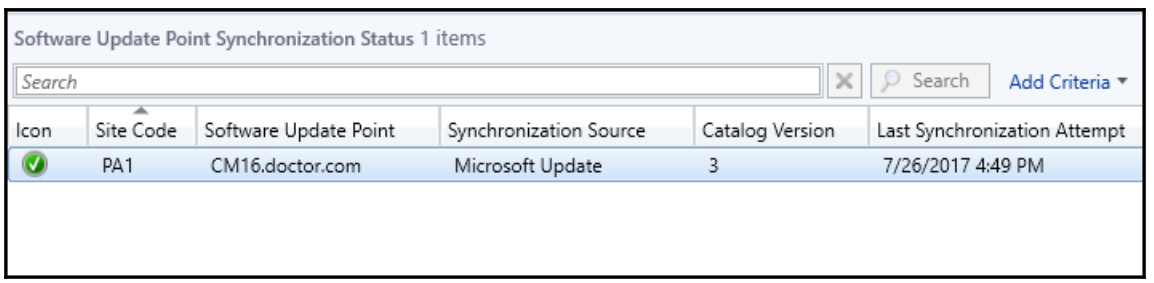

Name
Date modified
Type
adsrv.box 6/2/2017 12:46 AM File folder
aikbmgr.box 6/2/2017 12:49 AM File folder
amtproxymgr.box 6/2/2017 12:47 AM File folder
auth 6/2/2017 12:46 AM File folder
bgb.box 8/19/2017 8:49 PM File folder
businessappprocess.box 6/2/2017 12:48 AM File folder
ccr.box 6/30/2017 1:02 AM File folder
ccrretry.box 6/2/2017 12:46 AM File folder
certmgr.box 8/19/2017 8:04 PM File folder
clifiles.src 6/25/2017 11:31 PM File folder
CLOUDMGR.box 6/2/2017 12:51 AM File folder
cmupdate.box 6/25/2017 11:11 PM File folder
colfile.box 6/2/2017 12:46 AM File folder
coll_out.box 6/2/2017 12:46 AM File folder
COLLEVAL.box 8/19/2017 7:54 PM File folder
CompSumm.Box 8/19/2017 7:54 PM File folder
dataldr.box 6/2/2017 12:46 AM File folder

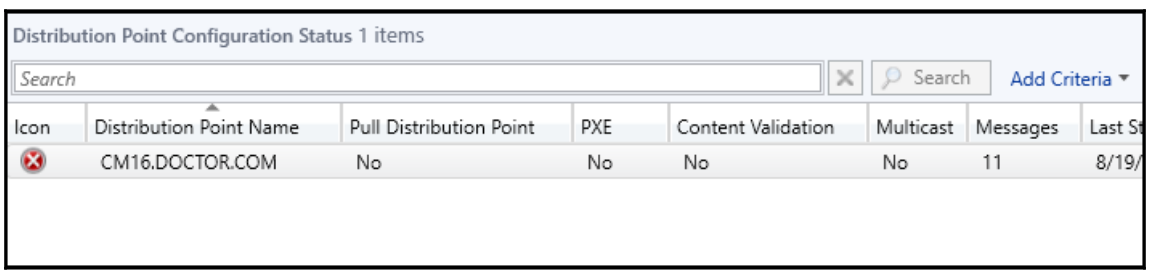


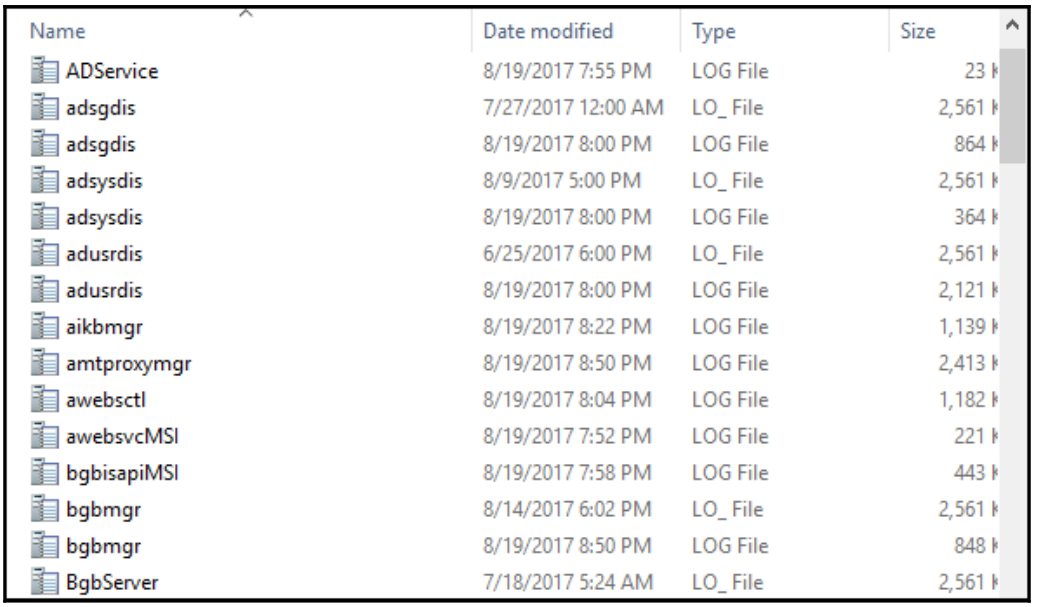




| Severity | Type | Site code | Date / Time | System | Component | Messag |
|---|---|---|---|---|---|---|
| | Milestone | PA1 | 8/19/2017 8:05:49 PM | CM16.DOCTOR.COM | SMS_WINNT_SERVER_DISCOVERY_AGENT | 1105 |
| | Milestone | PA1 | 8/19/2017 8:05:49 PM | CM16.DOCTOR.COM | SMS_WINNT_SERVER_DISCOVERY_AGENT | 502 |
| | Milestone | PA1 | 8/19/2017 8:04:40 PM | CM16.DOCTOR.COM | SMS_WSUS_SYNC_MANAGER | 500 |
| | Milestone | PA1 | 8/19/2017 8:04:39 PM | CM16.DOCTOR.COM | SMS_WSUS_SYNC_MANAGER | 1019 |
| | Milestone | PA1 | 8/19/2017 8:04:16 PM | CM16.DOCTOR.COM | SMS_SITE_SQL_BACKUP | 4610 |
| | Milestone | PA1 | 8/19/2017 8:04:16 PM | CM16.DOCTOR.COM | SMS_COMPONENT_STATUS_SUMMARIZER | 4610 |
| | Milestone | PA1 | 8/19/2017 8:04:16 PM | CM16.DOCTOR.COM | SMS_SITE_SQL_BACKUP | 4608 |
| | Milestone | PA1 | 8/19/2017 8:04:16 PM | CM16.DOCTOR.COM | SMS_COMPONENT_STATUS_SUMMARIZER | 4608 |
| | Milestone | PA1 | 8/19/2017 8:04:11 PM | CM16.DOCTOR.COM | SMS_WSUS_CONTROL_MANAGER | 500 |
| | Milestone | PA1 | 8/19/2017 8:04:10 PM | CM16.DOCTOR.COM | SMS_DATABASE_NOTIFICATION_MONITOR | 4604 |
| | Milestone | PA1 | 8/19/2017 8:04:10 PM | CM16.DOCTOR.COM | SMS_COMPONENT_STATUS_SUMMARIZER | 4604 |
| | Milestone | PA1 | 8/19/2017 8:04:10 PM | CM16.DOCTOR.COM | SMS_WSUS_SYNC_MANAGER | 1018 |
| | Milestone | PA1 | 8/19/2017 8:04:10 PM | CM16.DOCTOR.COM | SMS_WSUS_CONTROL_MANAGER | 1019 |
| | Milestone | PA1 | 8/19/2017 8:04:06 PM | CM16.DOCTOR.COM | SMS_DATABASE_NOTIFICATION_MONITOR | 4607 |
| | Milestone | PA1 | 8/19/2017 8:04:06 PM | CM16.DOCTOR.COM | SMS_COMPONENT_STATUS_SUMMARIZER | 4607 |
| | Milestone | PA1 | 8/19/2017 8:04:06 PM | CM16.DOCTOR.COM | SMS_EXECUTIVE | 4610 |
| | Milestone | PA1 | 8/19/2017 8:04:06 PM | CM16.DOCTOR.COM | SMS_COMPONENT_STATUS_SUMMARIZER | 4610 |
| | Milestone | PA1 | 8/19/2017 8:04:06 PM | CM16.DOCTOR.COM | SMS_EXECUTIVE | 4608 |


Component Status 77 items
Search
Search
Add Criteria
Icon
Status
Component
Site System
Type
Site Code
Availability
Critical
SMS_ENDPOINT_PROTECTIO...
CM16.DOCTOR.COM
Monitored Thread Co...
PA1
Online
Critical
SMS_OBJECT_REPLICATION_...
CM16.DOCTOR.COM
Monitored Thread Co...
PA1
Online
Critical
SMS_DATABASE_NOTIFICATI...
CM16.DOCTOR.COM
Monitored Thread Co...
PA1
Online
OK
CONFIGURATION_MANAGER...
CM16.DOCTOR.COM
Unknown
PA1
Unknown
OK
SMS_PORTALWEB_CONTROL...
CM16.DOCTOR.COM
Monitored Thread Co...
PA1
Online
OK
SMS_POLICY_PROVIDER
CM16.DOCTOR.COM
Monitored Thread Co...
PA1
Online
OK
SMS_PACKAGE_TRANSFER_...
CM16.DOCTOR.COM
Monitored Thread Co...
PA1
Online
OK
SMS_OUTGOING_CONTENT_...
CM16.DOCTOR.COM
Monitored Thread Co...
PA1
Online


Software Update Point Synchronization Status 1 items
Search
Search
Add Criteria
Icon
Site Code
Software Update Point
Synchronization Source
Catalog Version
Last Synchronization Attempt
PA1
CM16.doctor.com
Microsoft Update
3
7/26/2017 4:49 PM


Distribution Point Configuration Status 1 items
Search
Search
Add Criteria
Icon
Distribution Point Name
Pull Distribution Point
PXE
Content Validation
Multicast
Messages
Last St
CM16.DOCTOR.COM
No
No
No
No
11
8/19/



| Name | Date modified | Type | Size |
|---|---|---|---|
| ADService | 8/19/2017 7:55 PM | LOG File | 23 K |
| adsgdis | 7/27/2017 12:00 AM | LO_ File | 2,561 K |
| adsgdis | 8/19/2017 8:00 PM | LOG File | 864 K |
| adsysdis | 8/9/2017 5:00 PM | LO_ File | 2,561 K |
| adsysdis | 8/19/2017 8:00 PM | LOG File | 364 K |
| adusrdis | 6/25/2017 6:00 PM | LO_ File | 2,561 K |
| adusrdis | 8/19/2017 8:00 PM | LOG File | 2,121 K |
| aikbmgr | 8/19/2017 8:22 PM | LOG File | 1,139 K |
| amtproxymgr | 8/19/2017 8:50 PM | LOG File | 2,413 K |
| awebsctl | 8/19/2017 8:04 PM | LOG File | 1,182 K |
| awebsvcMSI | 8/19/2017 7:52 PM | LOG File | 221 K |
| bgbisapiMSI | 8/19/2017 7:58 PM | LOG File | 443 K |
| bgbmgr | 8/14/2017 6:02 PM | LO_ File | 2,561 K |
| bgbmgr | 8/19/2017 8:50 PM | LOG File | 848 K |
| BgbServer | 7/18/2017 5:24 AM | LO_ File | 2,561 K |