SCCM Quick Lab Guide

Version 22.05

Ahmed Abdelwahed
ahmed@abdelwahed.me
LinkedIn

Contents

Getting Started with SCCM

SCCM (System Center Configuration Manager) is a Microsoft software management suite used by administrators to oversee extensive distributions of Windows operating systems and apps. Here are some steps to help you get started with SCCM:

1. **Prepare for SCCM rollout:** It's crucial to map out your deployment strategy for a seamless integration of SCCM. Consider the following steps:

    - Determining your SCCM structure: This step entails assessing the required number of sites and their geographical distribution.
    - Setting up security parameters: With SCCM, you have the ability to set up role-based access control (RBAC), enabling you to define user permissions within SCCM according to their specific roles.
    - Setting up client installation options: Determine your preferred deployment settings for clients on computers, including where to install from and what properties to set.

2. **Deploy SCCM**: After finalizing your deployment strategy, proceed with the SCCM installation. The installation procedure comprises the subsequent steps:

    - Prepare the required prerequisites: Before setting up SCCM, you need to install specific prerequisites which comprise SQL Server, .NET Framework, and the Windows ADK (Assessment and Deployment Kit).
    - Setting up SCCM: Run the installation wizard to install SCCM, and follow its instructions throughout the setup. Be prepared for the installation to take a few hours.

3. **Set up SCCM:** Once SCCM is installed, it's necessary to set it up properly to ensure it operates correctly. The setup should include these actions:

    - Set up boundaries and boundary groups: In SCCM, boundaries and boundary groups are utilized to ascertain the assignment of clients to specific sites.
    - Adjust site configurations: This includes setting up parameters for client interactions, maintaining the site, and managing reports.
    - Set up SCCM discovery methods: SCCM employs these methods to find manageable resources. Choose and set up the ones you wish to use.

4. **Client Deployment:** To administer your Windows systems and applications via SCCM, it's necessary to install SCCM clients on your client machines. This can be achieved through various methods, such as:

    - Manual Deployment: The SCCM client can be installed on individual computers by hand.
    - Group Policy enables the distribution of the SCCM client to domain-joined computers.
    - Software deployment: Utilize SCCM for rolling out the SCCM client onto computers.

5. **Develop and distribute software bundles:** SCCM enables you to construct packages containing updates, patches, and new applications, and roll them out to client systems. Here are the steps for this process:

- To build a package, select the files for inclusion, define the installation command, and note any extra requirements.
- Deploying the package: Before deployment to client systems can occur, SCCM necessitates the distribution of the package to various distribution points.
- Install the package: Utilize SCCM to distribute the package to clients. You have the option to roll out the package right away or schedule it for a specific time.

6. **Keep track and solve problems:** After deploying software packages, monitor their status and handle any problems. SCCM offers numerous monitoring tools such as reports and logs to oversee your deployments. Use these resources to identify and fix issues if they occur.

What is the necessity for it?

1. **Centralized management:**
   - Offers a unified platform for overseeing Windows deployments and applications throughout the company.
   - Diminishes the resources and time necessary to individually manage every computer.
   - Enhances the aggregate effectiveness of IT processes.
2. **Automated deployment:**
   - Provides automation for deploying applications and Windows OS.
   - Reduces the time and effort required for updates, patches, and software installations.
   - Allows for the creation and deployment of custom Windows OS images, making the setup of new PCs more efficient.
3. **Improved security:**
   - Maintains the currency of all computers with respect to critical security patches and updates.
   - Aids enterprises in the implementation and enforcement of security protocols and regulatory compliance.
   - Minimizes vulnerability to security infringements and upholds adherence to established security guidelines.
4. **Asset management:**
   - Offers resources for overseeing both hardware and software assets throughout the company.
   - Assists enterprises in tracing their IT assets, supervising software licenses, and pinpointing potential cost reduction opportunities.
   - Aids enterprises in managing inventory, monitoring alterations in hardware and software, and strategizing for upcoming IT infrastructure requirements.
5. **Reporting and analytics:**
   - Offers tools for reporting and analysis, enabling organizations to keep an eye on their IT infrastructure and spot potential improvement areas.
   - Delivers in-depth reports on software usage, compliance levels, and hardware inventory.

- Assists organizations in making informed choices and enhancing their IT management.

6. **Integration with other Microsoft tools:**
   - Works in conjunction with Microsoft solutions like Active Directory, Group Policy, and Microsoft Endpoint Protection.
   - Assists enterprises in more efficient and effective IT infrastructure management.
   - Delivers a continuous and cohesive experience for IT infrastructure administration utilizing Microsoft technologies.

Hierarchy topology

SCCM (System Center Configuration Manager) employs a layered structure for overseeing Windows installations and software in sizable, multifaceted enterprises. This managerial architecture encompasses one or more SCCM sites, with the capability to administer as many as 400,000 clients per site. Below is a synopsis of the SCCM hierarchical design:

1. **Central administration site:** Serving as the apex of the SCCM hierarchy, the central administration site oversees various primary sites, offering a unified platform for governing the full SCCM structure. It further handles cross-primary site functionalities, covering reporting and adherence to policies.
2. A **primary site** refers to an autonomous SCCM site tasked with the oversight of Windows deployments and applications within a designated geographic or organizational area. Capable of overseeing up to 400,000 clients, primary sites have the option to link up with a central administration site or operate independently.
3. A **secondary site** functions as a regional or network-segment-specific management point for Windows deployments and applications. It's linked to a primary site and serves the purpose of reducing WAN traffic and enhancing the remote client experience.
4. **SCCM clients:** These are installed on Windows machines under SCCM management. They interact with the SCCM site server and its system roles for configuration, software deployment, and status reporting.
5. SCCM **site system roles** consist of roles installed on servers within the SCCM hierarchy to carry out distinct functions. Roles like management point, distribution point, and software update point are deployed across various servers to enhance scalability and ensure redundancy.

Configuration Manager site system roles

Site system roles in SCCM (System Center Configuration Manager) are integral components established on servers within the SCCM structure. Every role is designated to fulfill distinct functions, overseeing particular responsibilities pertinent to the deployment of Windows and management of applications. The following provides a summary of the various roles within SCCM's site system:

1. **Management Role:** Serving as the primary conduit for client requests, the management point processes these inquiries and disseminates configuration details and policy directives to clients. This pivotal element of the SCCM framework is indispensable for regulating client interactions.

2. **Distribution point:** This is where software packages, OS images, and other content are stored and sent out to clients. It helps cut down on WAN traffic by holding the content in a local cache and sharing it with nearby clients.

3. **Software update point:** This component is tasked with the management and deployment of software updates to clients. It has the ability to sync with either Microsoft Update or an on-premises Windows Server Update Services (WSUS) server to procure updates and distribute them to client systems.
4. **State migration point:** Utilized for transferring user state data from one machine to another, this point works alongside the User State Migration Tool (USMT) to facilitate the migration of users' files, configurations, and preferences to new machines.
5. **Endpoint protection point:** The role of this point involves the deployment and administration of Microsoft Endpoint Protection policies to client devices. It oversees definition updates distribution, tracks client adherence to policies, and provides status reports on endpoint protection.
6. **PXE-enabled distribution point**: This distribution point leverages PXE boot to deploy operating system images to client devices. It can simplify and automate the task of installing Windows operating systems on new devices.
7. **Site system:** Operating as a broad category, the site system role encompasses various components not specifically assigned to other roles. This includes elements such as the fallback status point, management reporter, and application catalog web service.

Overview of the Configuration Manager architecture

The architecture of SCCM (System Center Configuration Manager) is designed to provide a scalable and flexible management solution for Windows deployments and applications. Here's an overview of the SCCM architecture:

1. SCCM Site Server: This component is the core of the SCCM architecture, maintaining and controlling the site database that holds all configuration and client information for SCCM. It manages client requests and oversees the operations of other SCCM elements.
2. **SCCM Site System Roles:** These are distinct components deployed on servers within the SCCM structure. They execute particular tasks such as:
    - Management point: Processes client requests and delivers configuration data and policies.
    - Distribution point: Stores and distributes software, OS images, and content.
    - Software update point: Oversees software updates and distribution to clients.
    - State migration point: Facilitates user state data transfer between computers.
    - Endpoint protection point: Deploys and manages Endpoint Protection policies.

---

3. **SCCM Clients:** Installed on Windows devices under SCCM management, these clients communicate with the site server for configurations, software deployment, and status reporting, and can be set up through methods like manual installs or Group Policy.
4. **SCCM Console:** This user interface allows SCCM administrators to handle deployments and applications. It requires access to the site server to pull data and manage configuration.
5. **SCCM Database:** A SQL Server database that conserves SCCM's configuration and client information, instrumental for tracking deployments and updates. Regular SQL Server techniques ensure its backup and recovery process.
6. **SCCM Boundaries:** Designators for network locations overseen by SCCM using criteria such as IP subnets or Active Directory sites, helping assign clients to correct site system roles for streamlined management.

Size and scale numbers for Configuration Manager

SCCM (System Center Configuration Manager) is equipped to manage extensive and intricate Windows deployments and applications. Below are some important statistics regarding its size and capacity:

1. Number of supported clients: SCCM can manage up to 400,000 clients per primary site. This means that organizations can deploy SCCM to manage many Windows computers, even in distributed environments.
2. Number of primary sites: A single SCCM hierarchy can have up to 25 primary sites. This allows organizations to manage Windows deployments and applications across multiple geographic or organizational boundaries.
3. Number of distribution points: SCCM can support up to 250 distribution points per primary site. Distribution points are used to store and distribute software packages, operating system images, and other content to clients.
4. Number of management points: SCCM can support up to 250 management points per primary site. Management points are used to process client requests and send configuration data and policy information to clients.
5. Number of software update points: SCCM can support up to 50 software update points per primary site. Software update points are used to manage software updates and deploy them to clients.
6. Scalability for large organizations: SCCM is designed to scale up and out to support large organizations with thousands of clients and complex network topologies. SCCM can be deployed using a hierarchical topology with central administration sites, primary sites, and secondary sites to manage large and complex environments.

Configuration Manager Installation Guide

1. Prepare for installation:
   - Go through the SCCM documentation and installation prerequisites.
   - Set up required software and OS prerequisites like Microsoft .NET Framework and Windows ADK.
   - Set up the SQL Server database and configure SQL Server Reporting Services.
   - Make sure the SCCM installation account has the right permissions.
2. Install the SCCM site server:
   - Launch the SCCM setup wizard and choose "Install a Configuration Manager primary site". Input required details like site code, name, and database server. Set up the site database with options for replication and backup. Pick components for installation, including management point, distribution point, and software update point.
3. Install site system roles:
   - Deploy site system roles on the SCCM hierarchy servers to enhance capabilities including management point, distribution point, software update point, among others.
   - Tailor the site system role configurations to suit your particular needs, for instance, by choosing the location for the content library on distribution points.
4. Configure site settings:
   - Set up site preferences, including perimeter definitions, exploration techniques, and settings for clients.
   - Arrange the required components of the site, including tasks related to site upkeep and scheduling periods for site maintenance.
5. Deploy SCCM clients:
   - Install SCCM clients on the Windows machines you wish to manage.
   - Choose from several client deployment methods, like manual setup, Group Policy, or software distribution tools, depending on what suits your situation best.
   - Ensure that the clients have been correctly implemented and are communicating with SCCM.
6. Configure software deployments:
   - Set up software deployments by assembling software packages, defining groups of clients for the deployment targets, and establishing rules for software deployment.
   - Track the progress of software deployments and client interactions to confirm the successful installation of software on client systems.
7. Monitor and maintain SCCM:
   - Track client activities and conditions to confirm the proper operation of SCCM.
   - Set up reports and oversee the status of SCCM to pinpoint potential problems.
   - Carry out routine maintenance duties, including backing up databases and updating SCCM software.

Steps to Install SCCM 1802

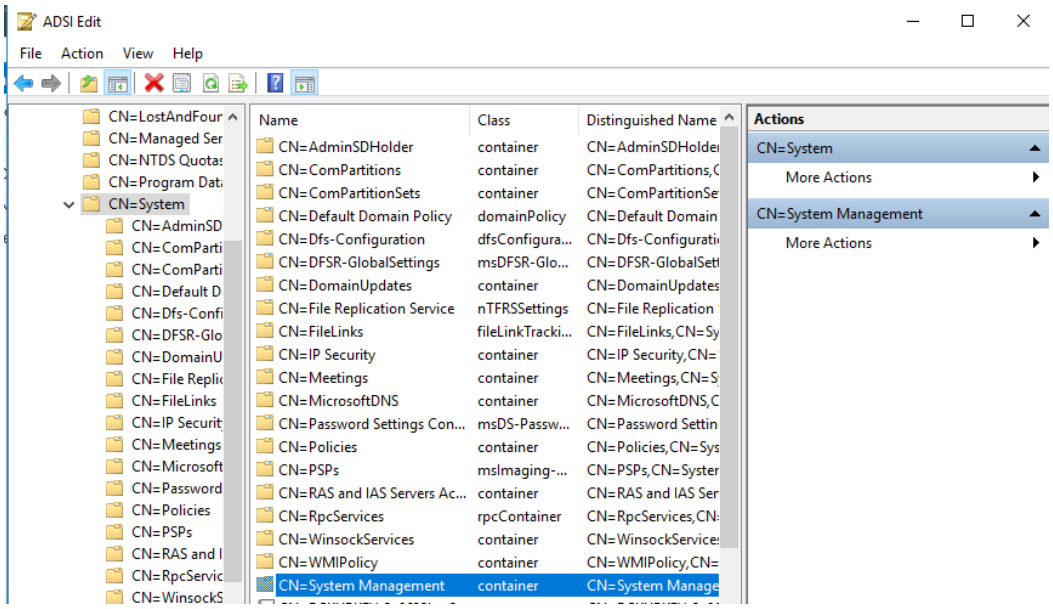
Prerequisites for Active Directory involve the installation of SQL Server 2016 Standard with Service Pack

1. Enable necessary components such as IIS along with Active Directory prerequisites.
2. Proceed to extend the AD Schema.
3. The Windows ADK is essential for deploying operating systems with Configuration Manager; this includes running adksetup and adkwinpesetup.
4. Again, ensure SQL Server 2016 Standard with Service Pack 2 is set up appropriately.
5. Configure the WSUS Role and connect the WSUS Database to SQL.
6. Lastly, implement System Center Configuration Manager and Endpoint Protection (current branch – version 1802).

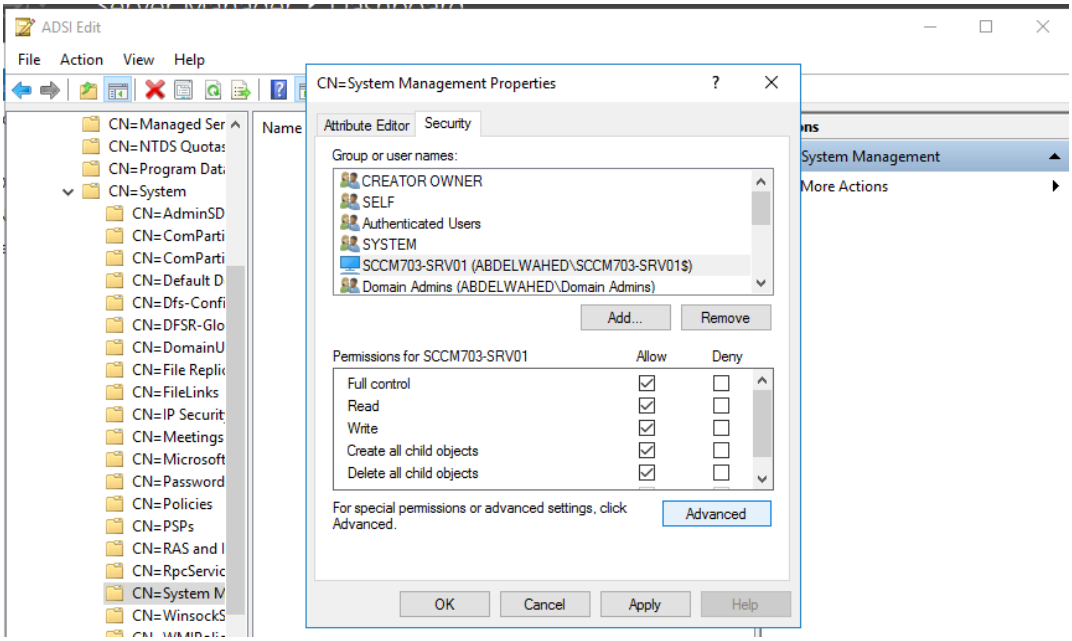
Active Directory prerequisites

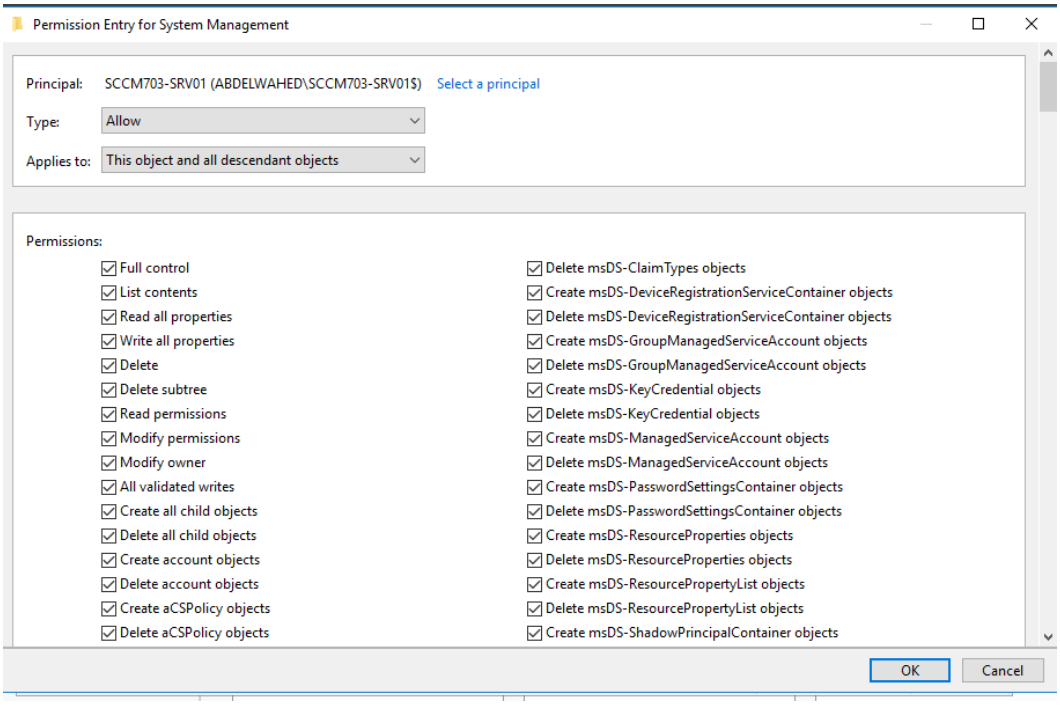
Through Active Directory, utilize ADSI Edit to establish the System Management Container and assign permissions to the SCCM Computer for the system management container.

1. Access the domain controller. Open Server Manager, navigate to Tools, and select ADSI Edit.
2. Right-click on ADSI Edit and choose Connect to.
3. In the Connection Settings dialog, ensure that Default naming context is selected. Confirm by clicking OK.
4. Expand the Default Naming Context node. Right-click CN=System, select New, and then create an Object.
5. Choose container as the class type and proceed by clicking Next.
6. Assign the name System Management.
7. Proceed with Next again and complete the process by clicking Finish to exit the wizard.



To grant complete permissions to the SCCM server, follow these steps:





install/enable some features (IIS)

Please install these features:

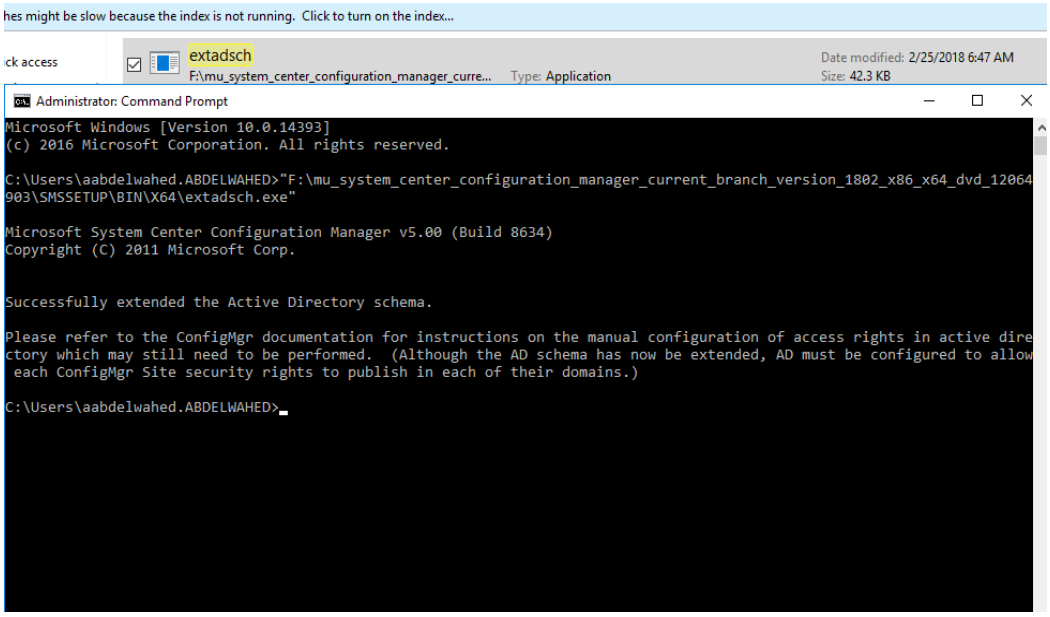
- .Net Framework 3.5 Features [Install all sub features]
- .Net Framework 4.5 Features [Install all sub features]
- BITS
- Remote Differential Compression

Enable the following Roles Services:

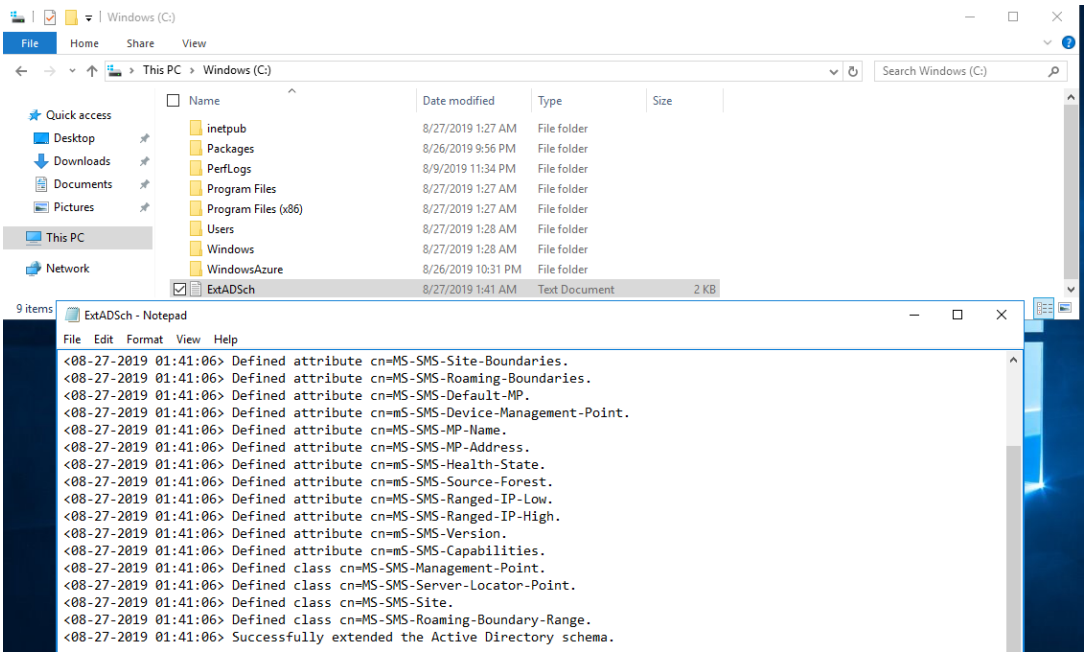
- Typical HTTP Options – Default Page, Static Files.
- App Creation – .NET Extension 3.5, ASP.NET 3.5, ISAPI Extensions, ASP.NET 4.5, and .NET Extension 4.5.
- Protection – Windows Authentication Protocol.
- Legacy IIS 6 Support – IIS Management Interface, Compatibility with IIS 6 Metabase and WMI, Scripts and Management Tools for IIS.

Extend AD Schema

Navigate to the extadsch utility in the SCCM source (SMSSETUP\BIN\X64), press and hold the shift key, right-click on extadsch, select "Copy as Path," then paste it into the command prompt.

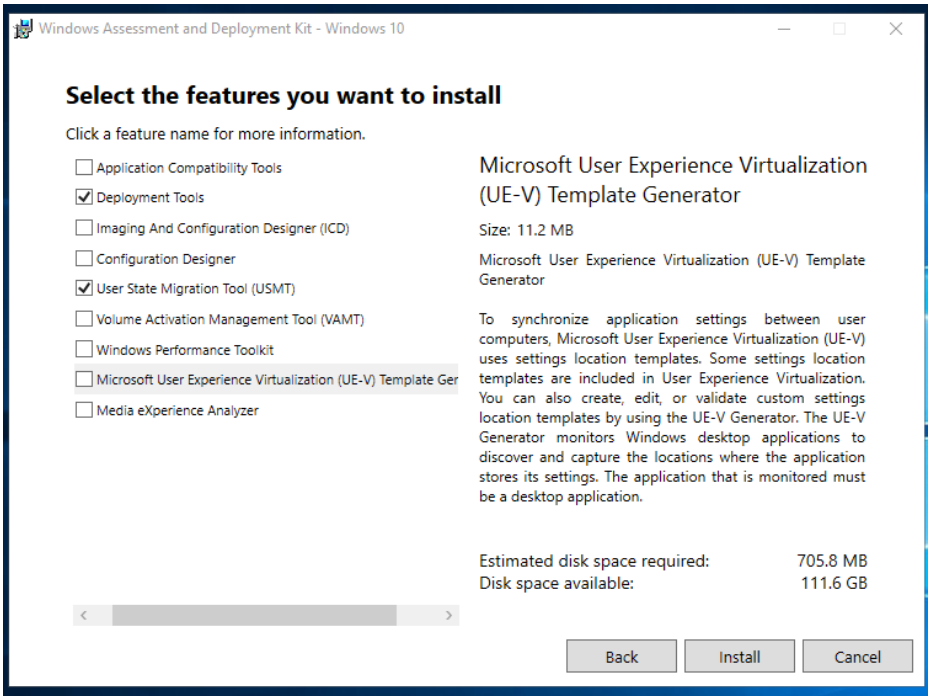


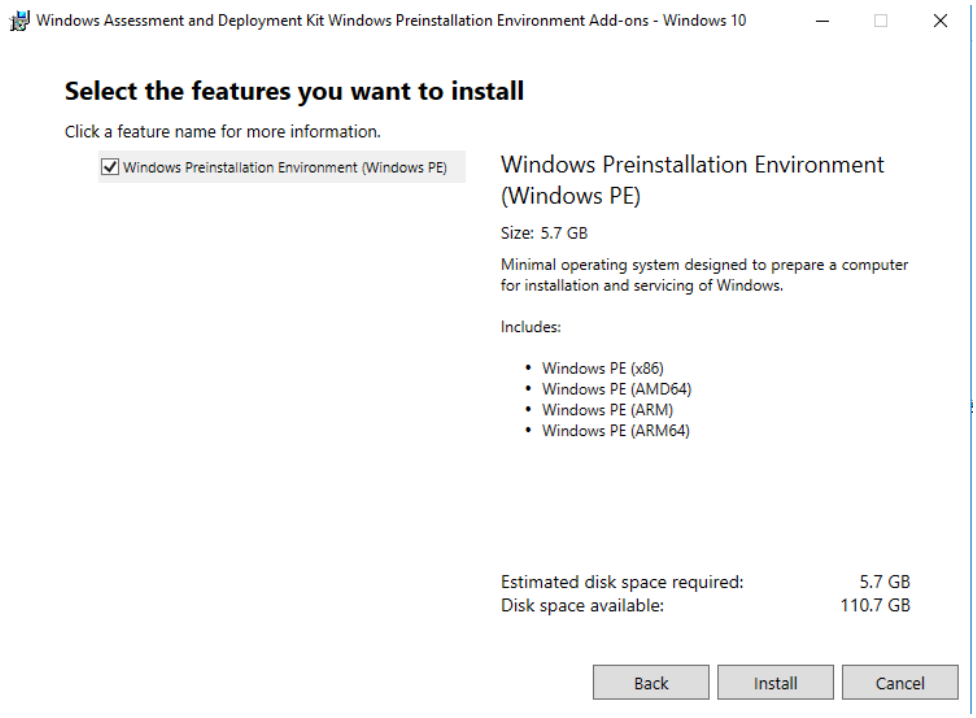
you can view the schema extension report at the provided path



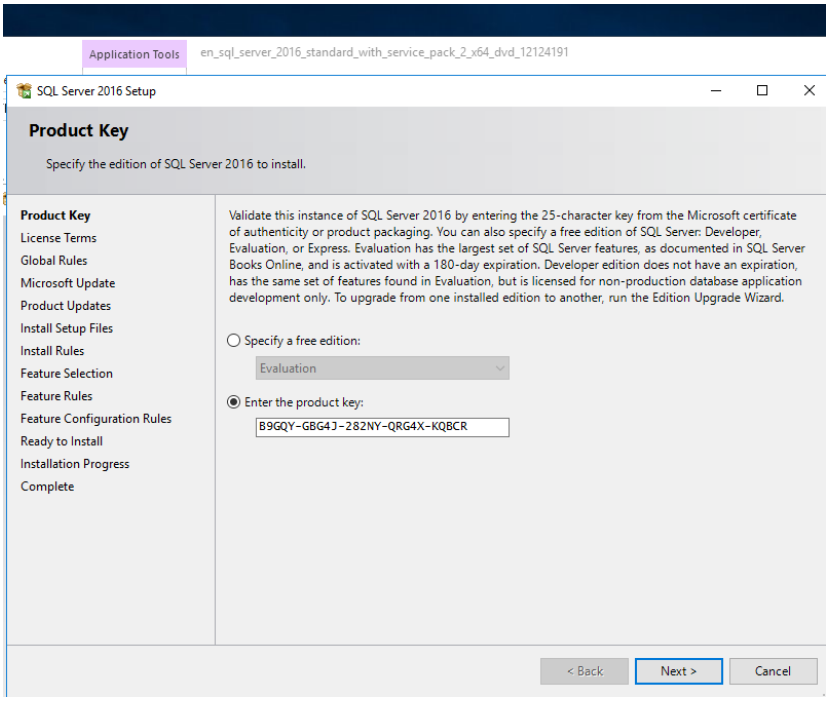
Windows ADK (required to deploy operating systems with Configuration Manager)

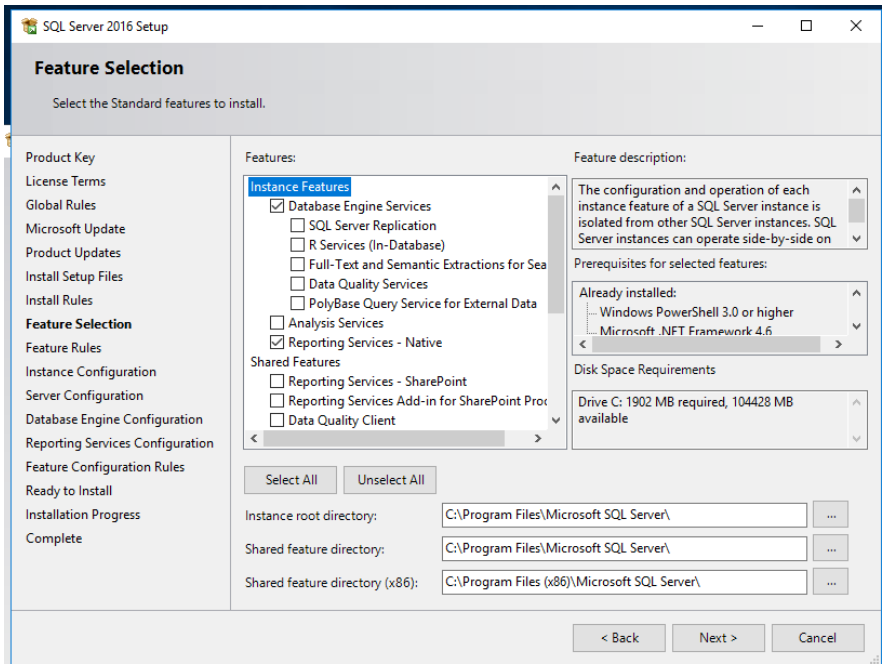
Note: ADK and Windows PE Addon (it separated after windows 10 version 1809) so we must install two tools adksetup and adkwinpesetup

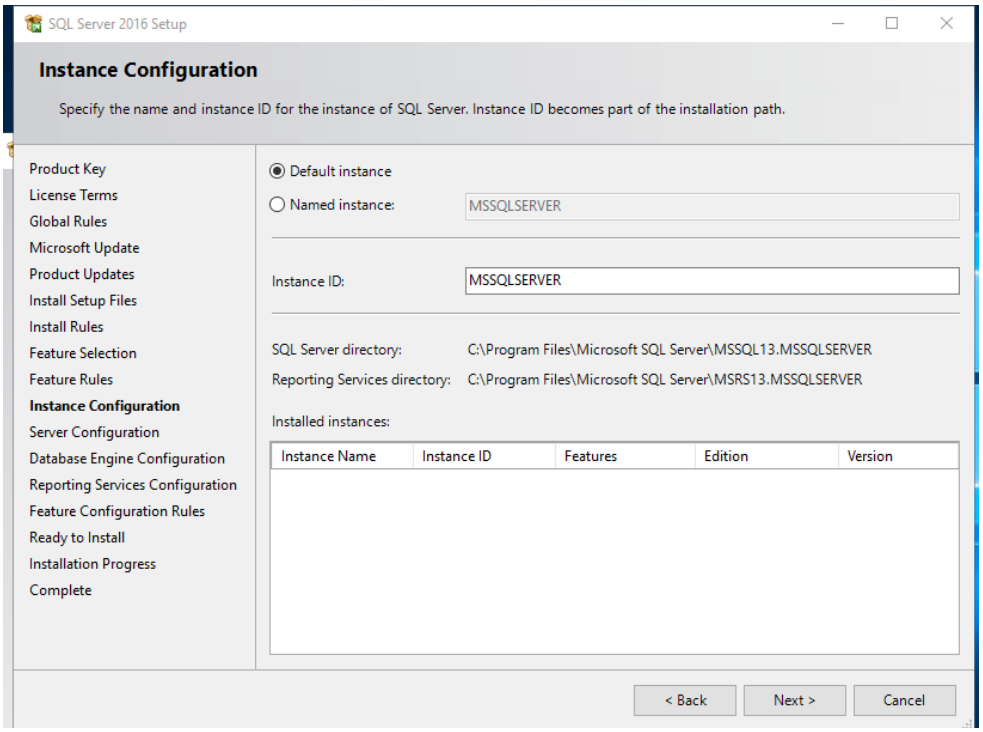




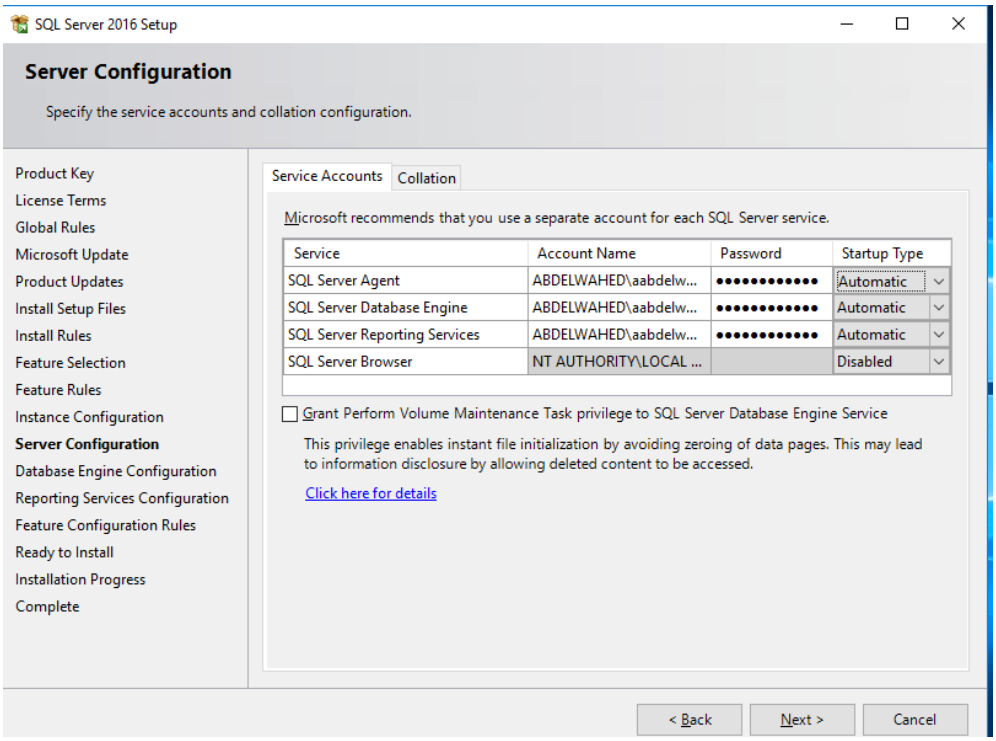
Install SQL (in our lab we use SQL 2016 Standard service pack 2)

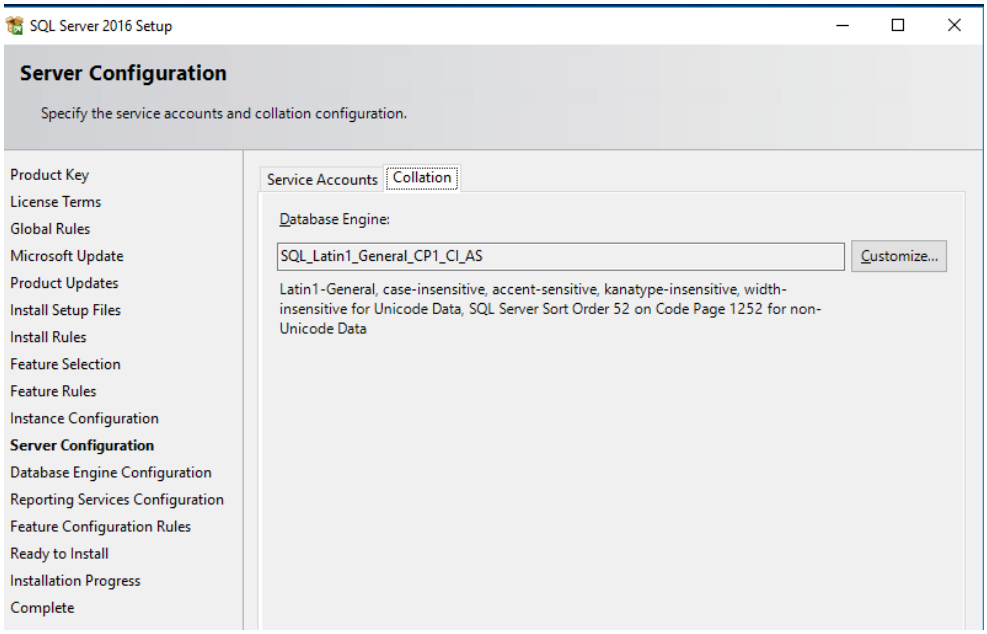


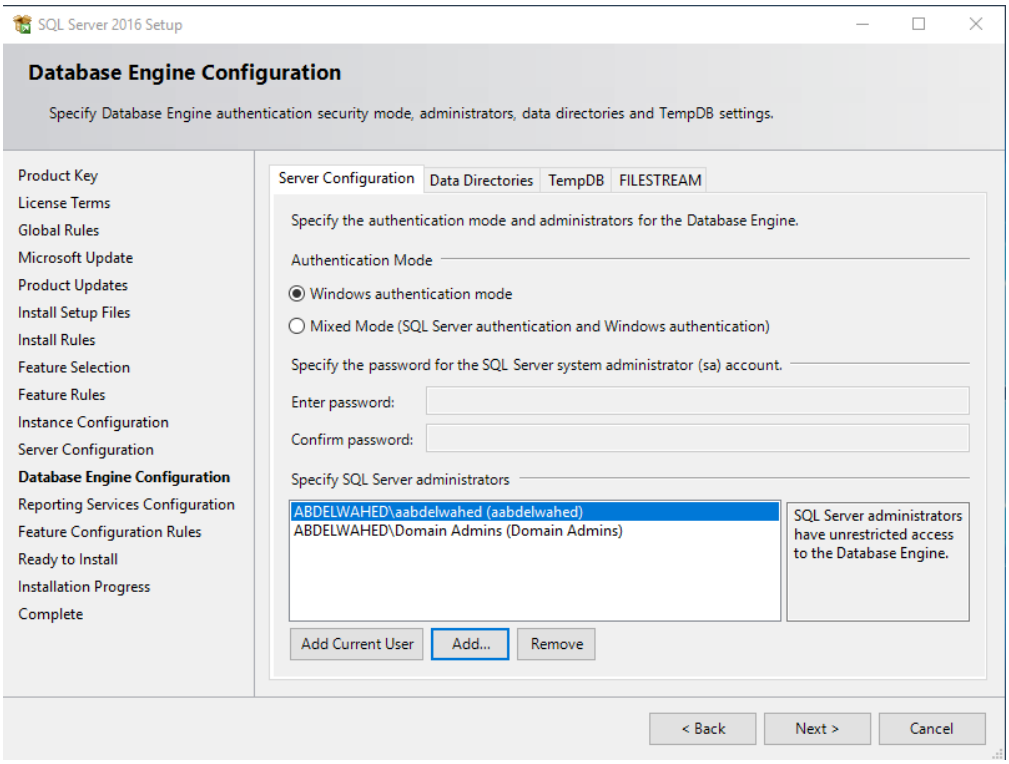

SQL Server 2016 Setup
Feature Selection
Select the Standard features to install.
Product Key
License Terms
Global Rules
Microsoft Update
Product Updates
Install Setup Files
Install Rules
Feature Selection
Feature Rules
Instance Configuration
Server Configuration
Database Engine Configuration
Reporting 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:
The configuration and operation of each instance feature of a SQL Server instance is isolated from other SQL Server instances. SQL Server instances can operate side-by-side on
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, 104428 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

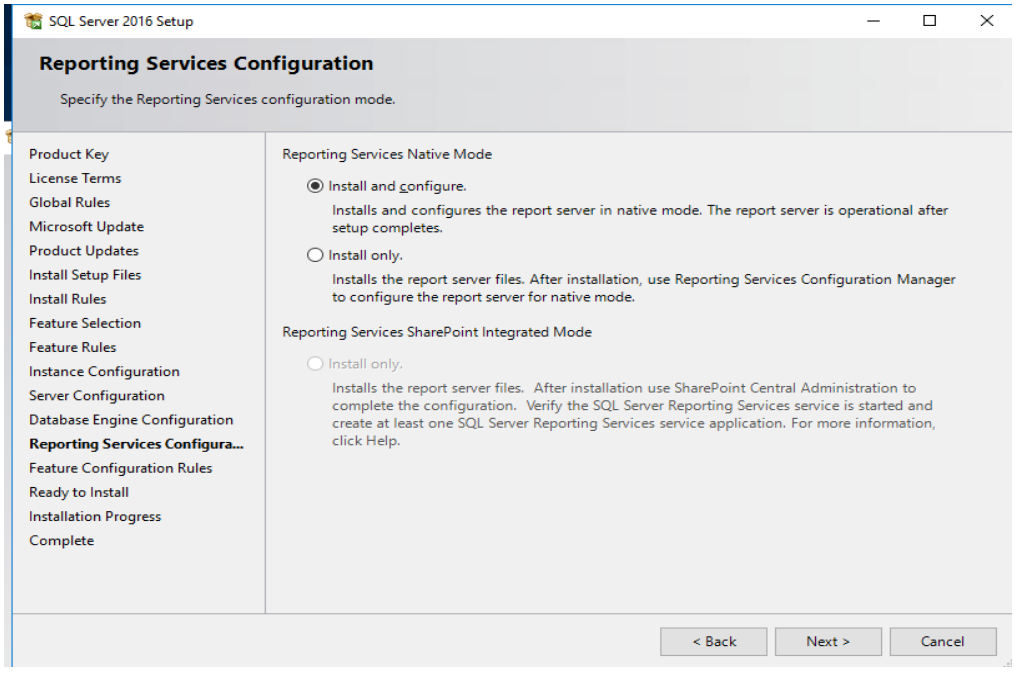

SQL Server 2016 Setup
Instance Configuration
Specify the name and instance ID for the instance of SQL Server. Instance ID becomes part of the installation path.
Product Key
License Terms
Global Rules
Microsoft Update
Product Updates
Install Setup Files
Install Rules
Feature Selection
Feature Rules
Instance 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

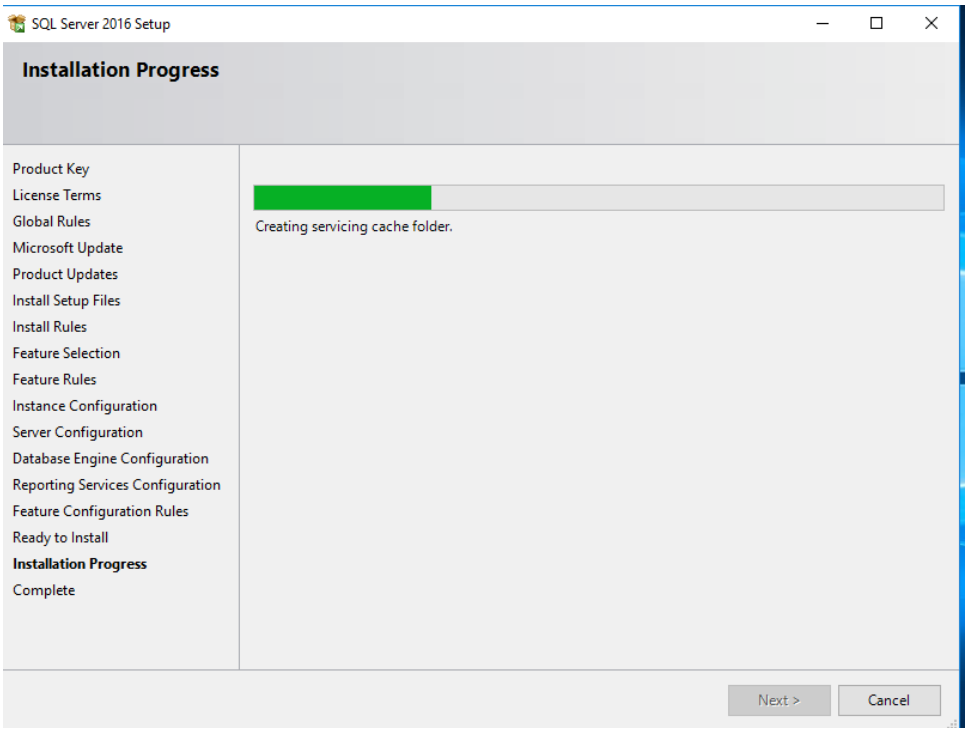
Only for testing purposes, we install with administrator privileges (this is not advised).

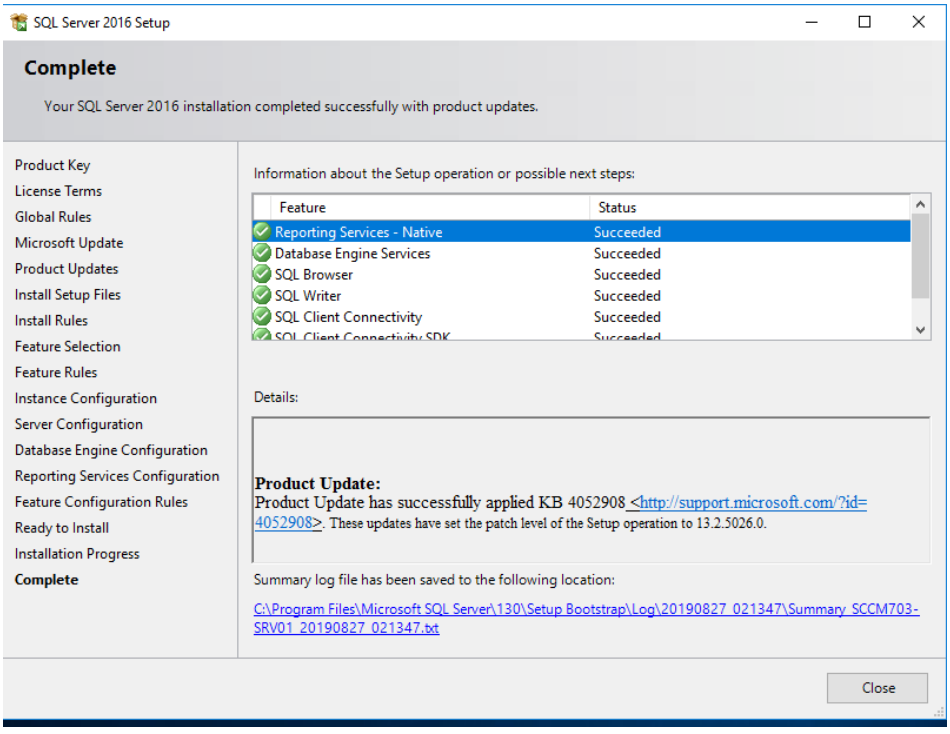




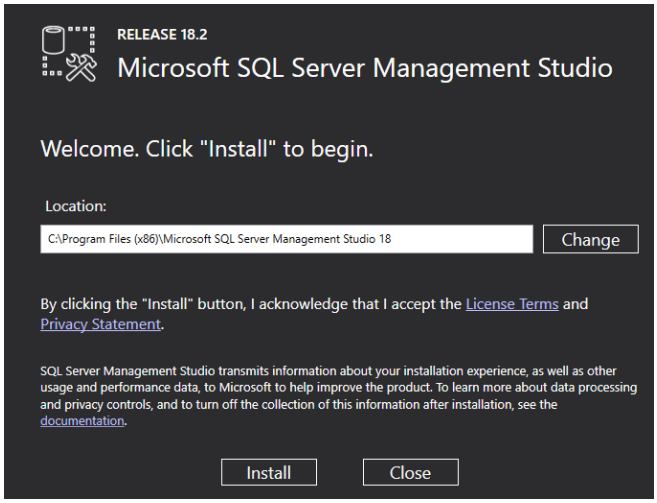

SQL Server 2016 Setup
Database Engine Configuration
Specify Database Engine authentication security mode, administrators, data directories and TempDB settings.
Product Key
License Terms
Global Rules
Microsoft Update
Product Updates
Install Setup Files
Install Rules
Feature Selection
Feature Rules
Instance 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
ABDELWAHED\aabdelwahed (aabdelwahed)
ABDELWAHED\Domain Admins (Domain Admins)
SQL Server administrators have unrestricted access to the Database Engine.
Add Current User
Add...
Remove
< Back
Next >
Cancel


SQL Server 2016 Setup
Reporting Services Configuration
Specify the Reporting Services configuration mode.
Product Key
License Terms
Global Rules
Microsoft Update
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

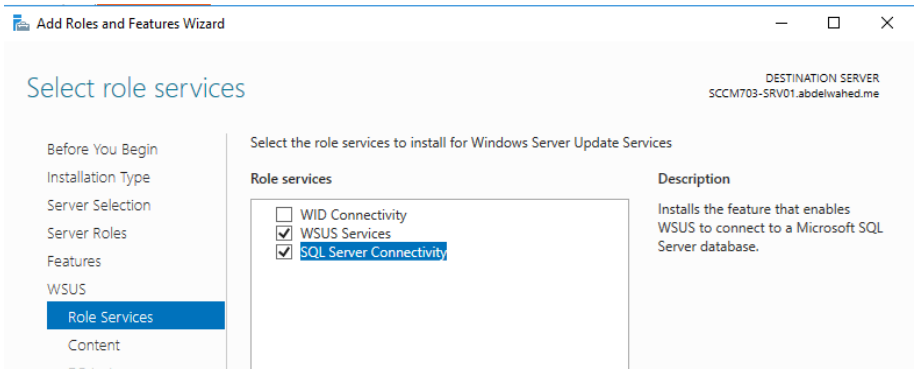

SQL Server 2016 Setup
Installation Progress
Product Key
License Terms
Global Rules
Microsoft Update
Product Updates
Install Setup Files
Install Rules
Feature Selection
Feature Rules
Instance Configuration
Server Configuration
Database Engine Configuration
Reporting Services Configuration
Feature Configuration Rules
Ready to Install
Installation Progress
Complete
Creating servicing cache folder.
Next >
Cancel

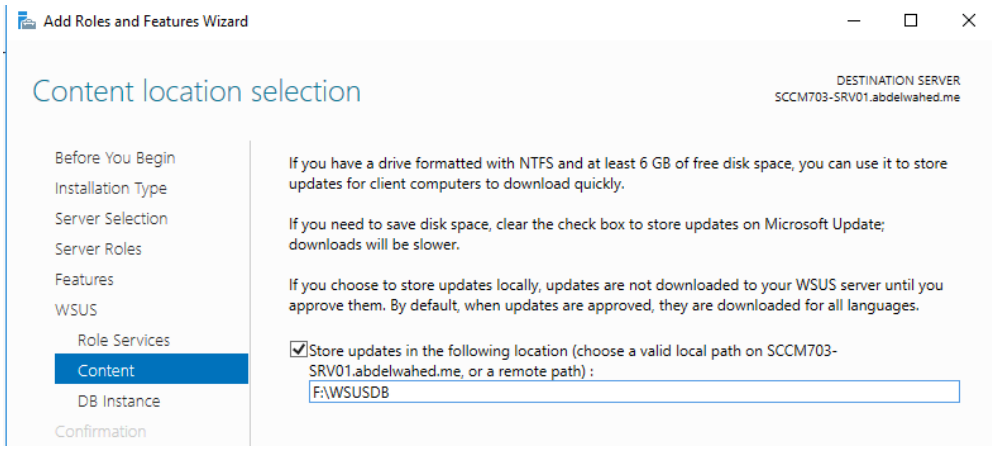

SQL Server 2016 Setup
Complete
Your SQL Server 2016 installation completed successfully with product updates.
Product Key
License Terms
Global Rules
Microsoft Update
Product Updates
Install Setup Files
Install Rules
Feature Selection
Feature Rules
Instance Configuration
Server Configuration
Database Engine Configuration
Reporting Services Configuration
Feature Configuration Rules
Ready to Install
Installation Progress
Complete
Information about the Setup operation or possible next steps:
Feature
Status
Reporting Services - Native
Succeeded
Database Engine Services
Succeeded
SQL Browser
Succeeded
SQL Writer
Succeeded
SQL Client Connectivity
Succeeded
Details:
Product Update:
Product Update has successfully applied KB 4052908 <http://support.microsoft.com/?id=4052908>. These updates have set the patch level of the Setup operation to 13.2.5026.0.
Summary log file has been saved to the following location:
C:\Program Files\Microsoft SQL Server\130\Setup Bootstrap\Log\20190827_021347\Summary_SCCM703-SRV01_20190827_021347.txt
Close

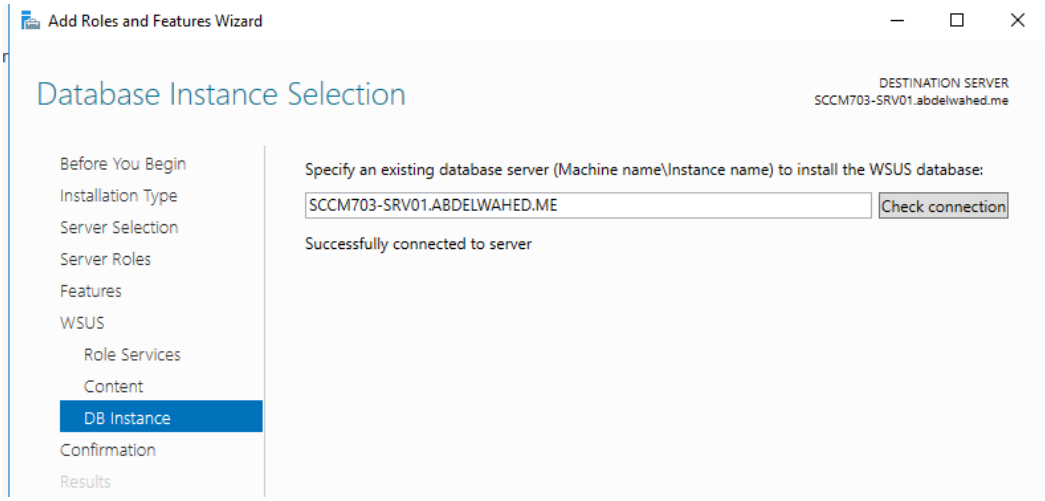
Install SSMS separately if it's not included by default as in SQL 2017 for SQL connectivity.

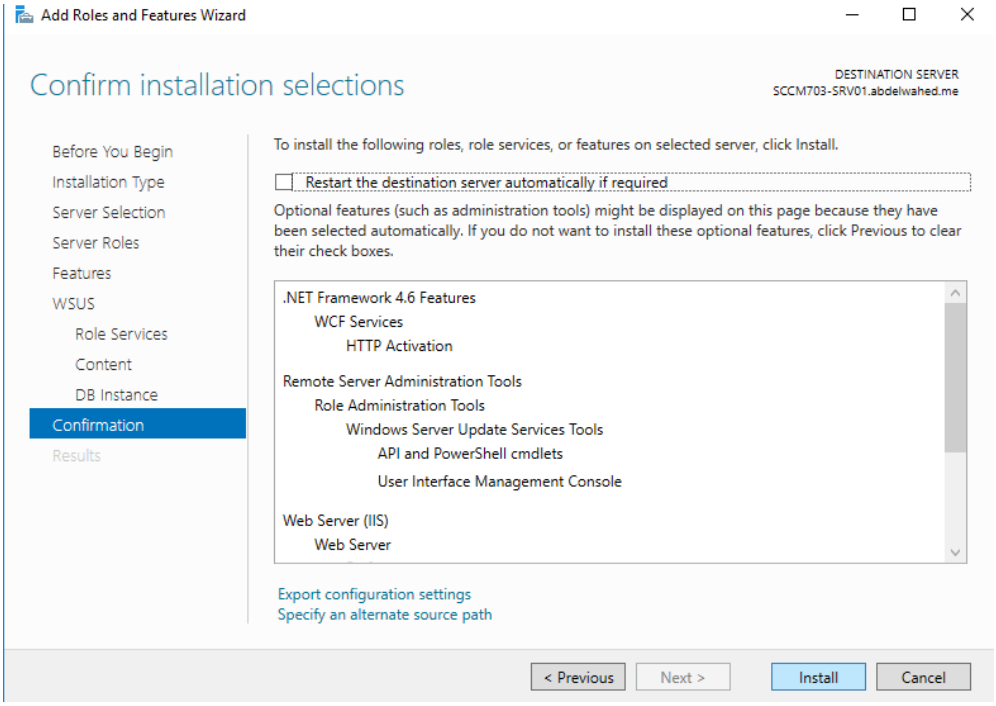


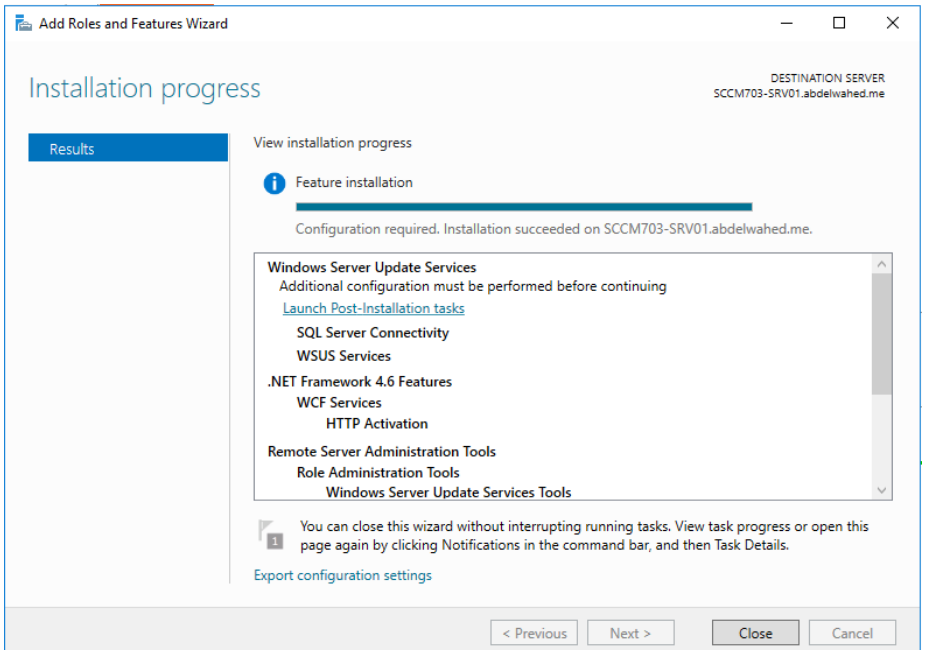
Install WSUS Role and link WSUS Database to SQL



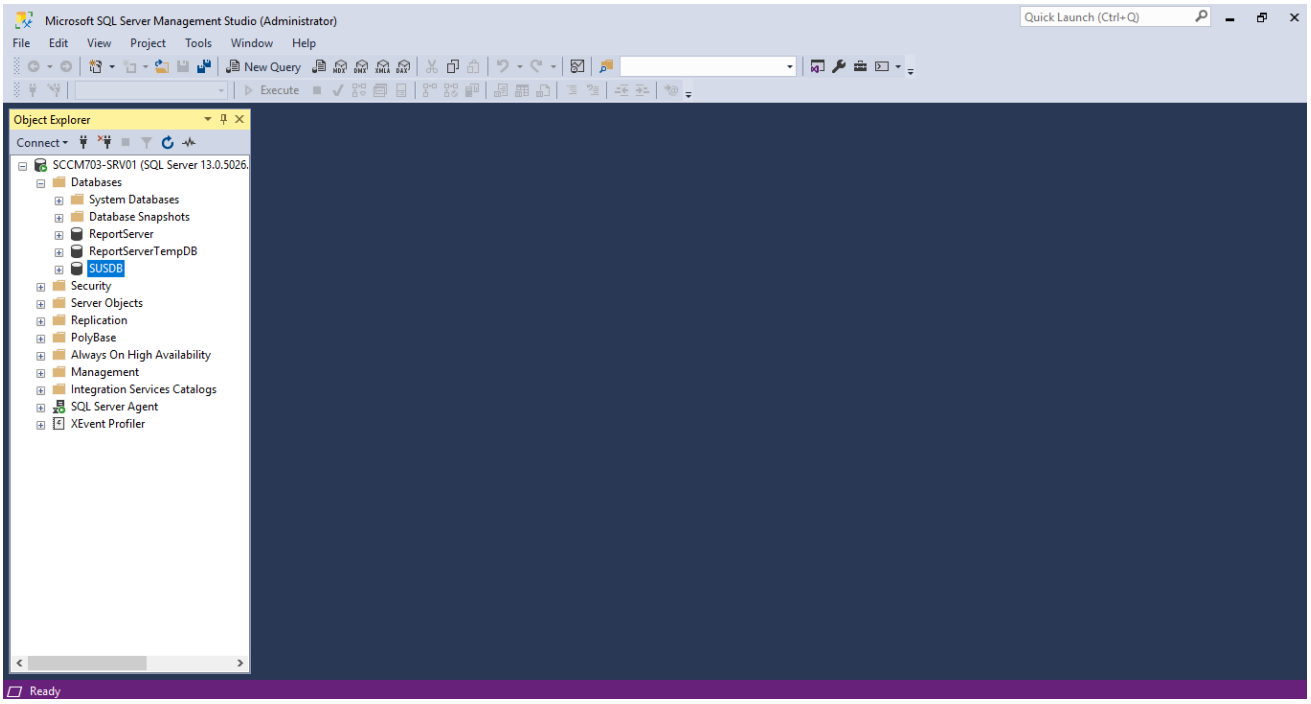



Add Roles and Features Wizard
Database Instance Selection
DESTINATION SERVER
SCCM703-SRV01.abdelwahed.me
Before You Begin
Installation Type
Server Selection
Server Roles
Features
WSUS
Role Services
Content
DB Instance
Confirmation
Results
Specify an existing database server (Machine name\Instance name) to install the WSUS database:
SCCM703-SRV01.ABDELWAHED.ME
Check connection
Successfully connected to server

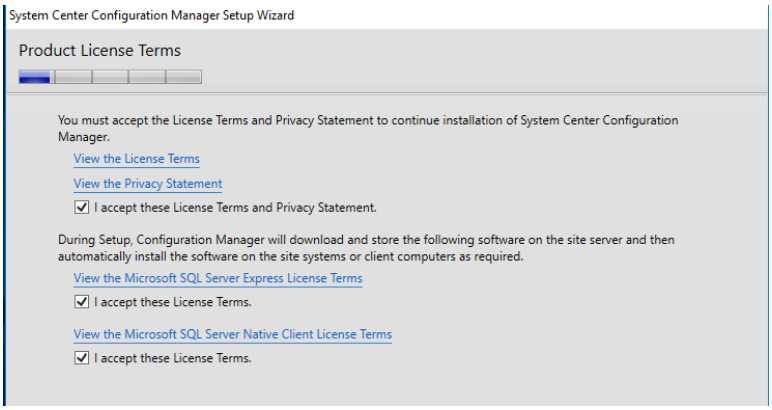

Add Roles and Features Wizard
Confirm installation selections
DESTINATION SERVER
SCCM703-SRV01.abdelwahed.me
Before You Begin
Installation Type
Server Selection
Server Roles
Features
WSUS
Role Services
Content
DB Instance
Confirmation
Results
To install the following roles, role services, or features on selected server, click Install.
Restart the destination server automatically if required
Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.
.NET Framework 4.6 Features
WCF Services
HTTP Activation
Remote Server Administration Tools
Role Administration Tools
Windows Server Update Services Tools
API and PowerShell cmdlets
User Interface Management Console
Web Server (IIS)
Web Server
Export configuration settings
Specify an alternate source path
< Previous
Next >
Install
Cancel

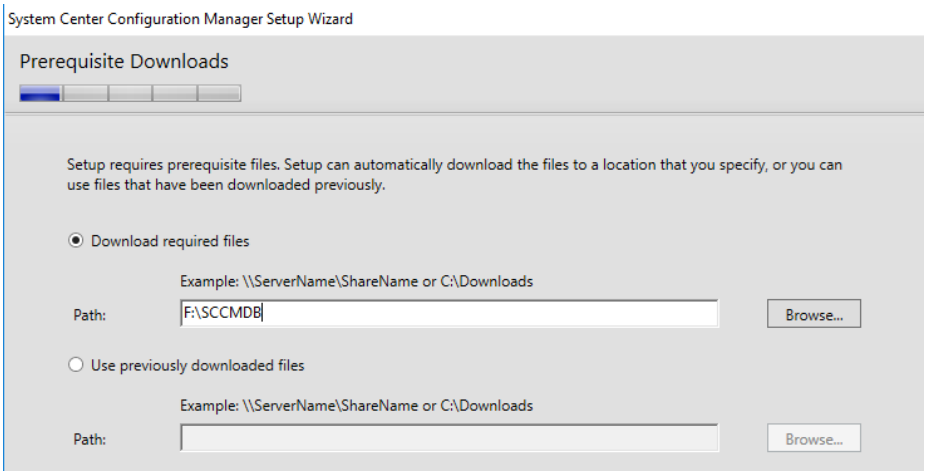


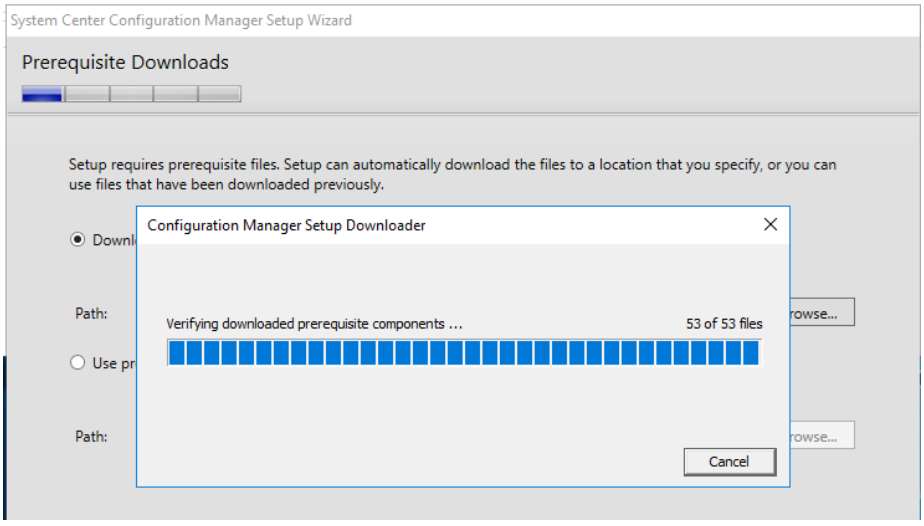
Open SSMS and select the Database to locate SUSDB.

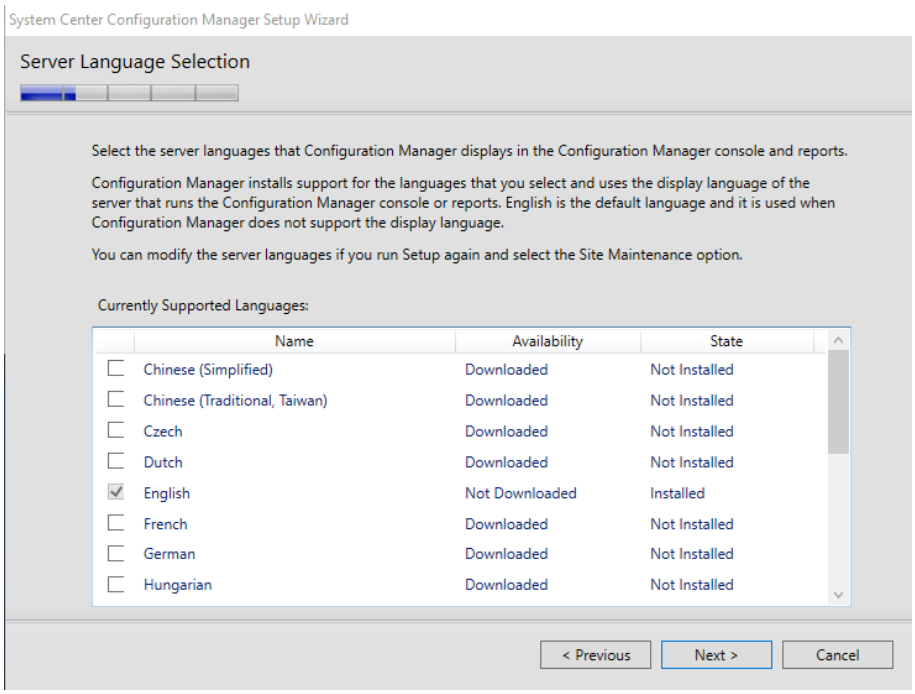


System Center Configuration Manager and Endpoint Protection (current branch – version 1802)

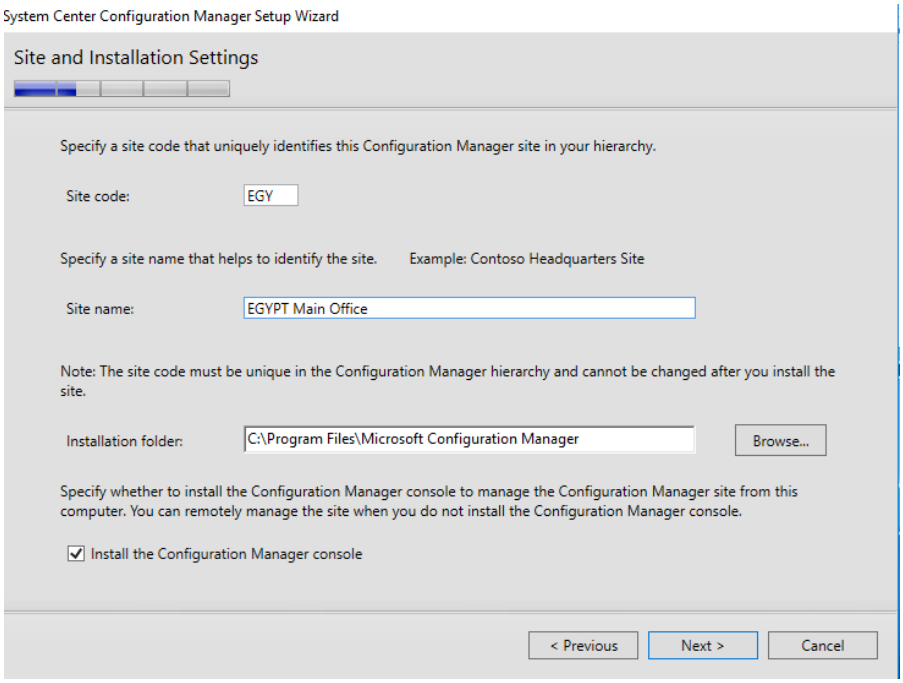


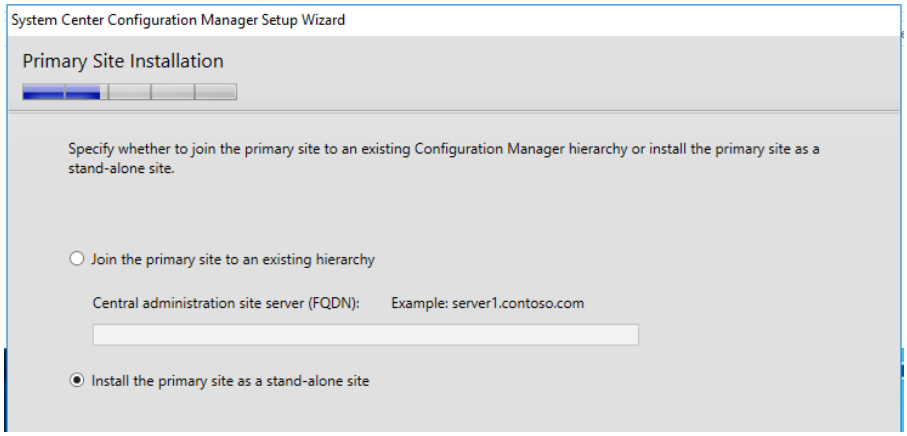


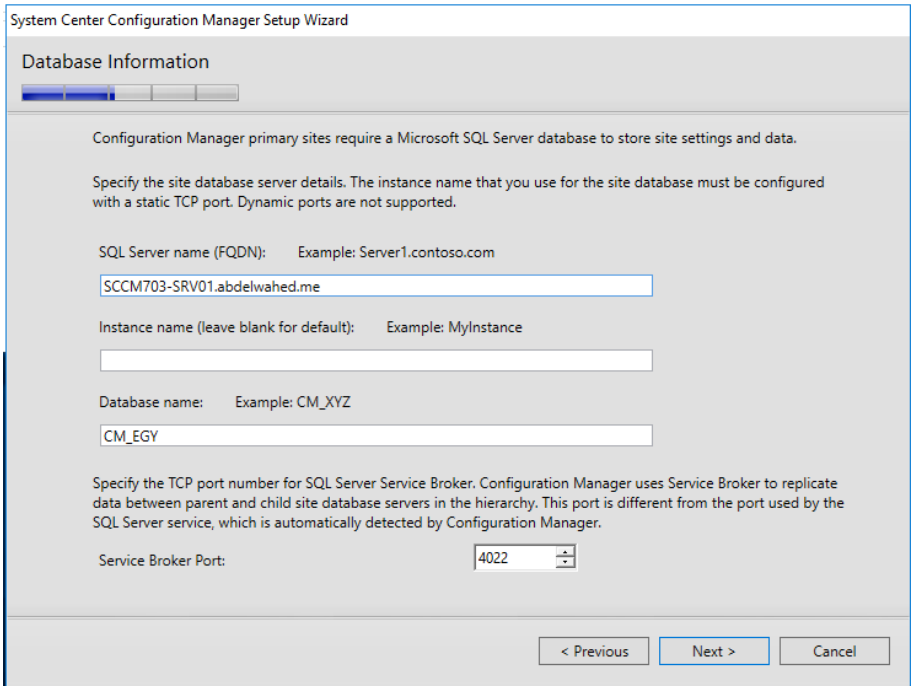


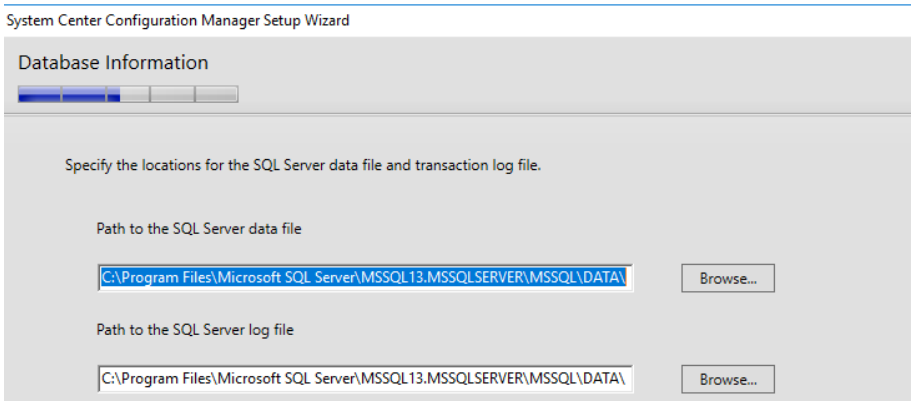


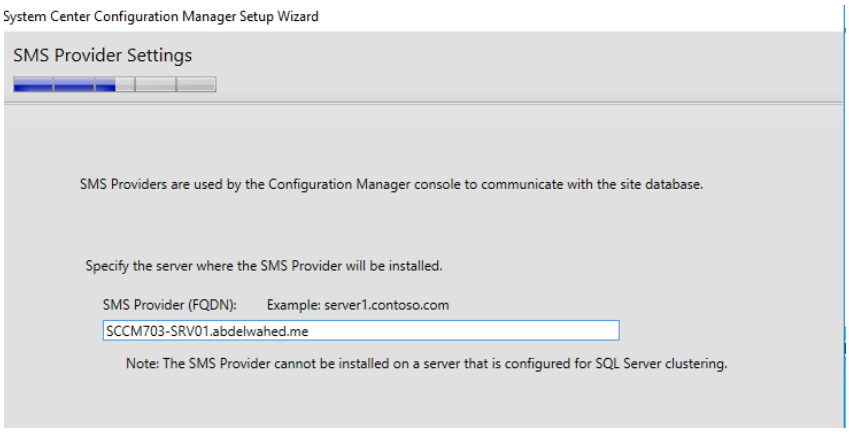
Site codes serve as identifiers for locations within a Configuration Manager, which is a central element in SCCM.

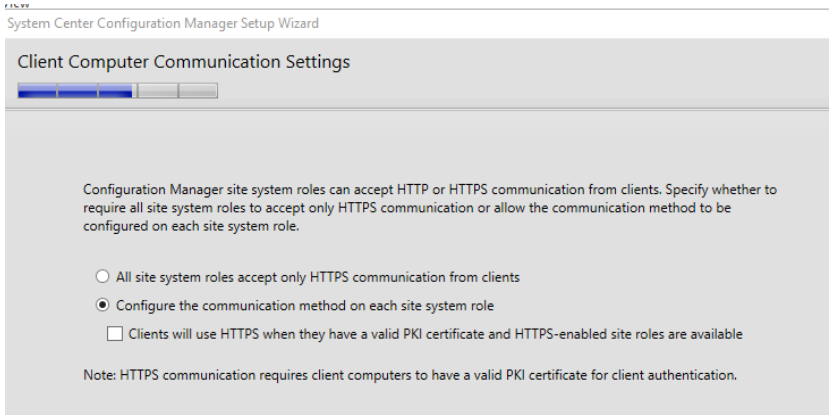


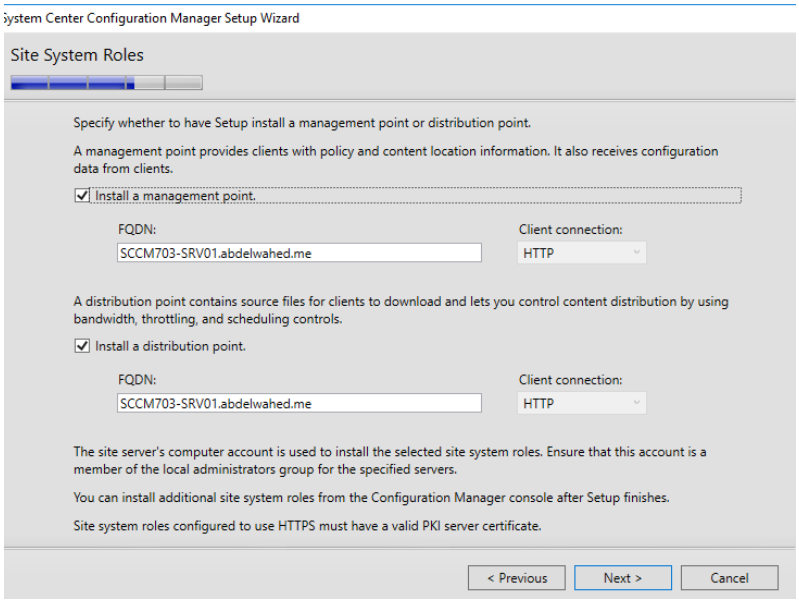

System Center Configuration Manager Setup Wizard
Primary Site Installation
Specify whether to join the primary site to an existing Configuration Manager hierarchy or install the primary site as a stand-alone site.
Join the primary site to an existing hierarchy
Central administration site server (FQDN):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

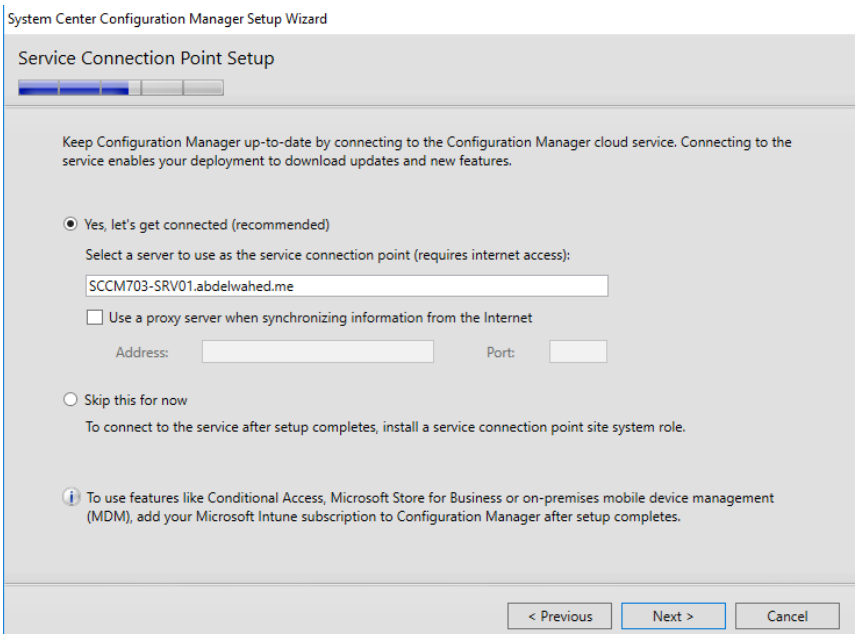

System Center Configuration Manager Setup Wizard
Database Information
Configuration Manager primary sites require a Microsoft SQL Server database to store site settings and data.
Specify the site database server details. The instance name that you use for the site database must be configured with a static TCP port. Dynamic ports are not supported.
SQL Server name (FQDN):
Example: Server1.contoso.com
SCCM703-SRV01.abdelwahed.me
Instance name (leave blank for default):
Example: MyInstance
Database name:
Example: CM_XYZ
CM_EGY
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

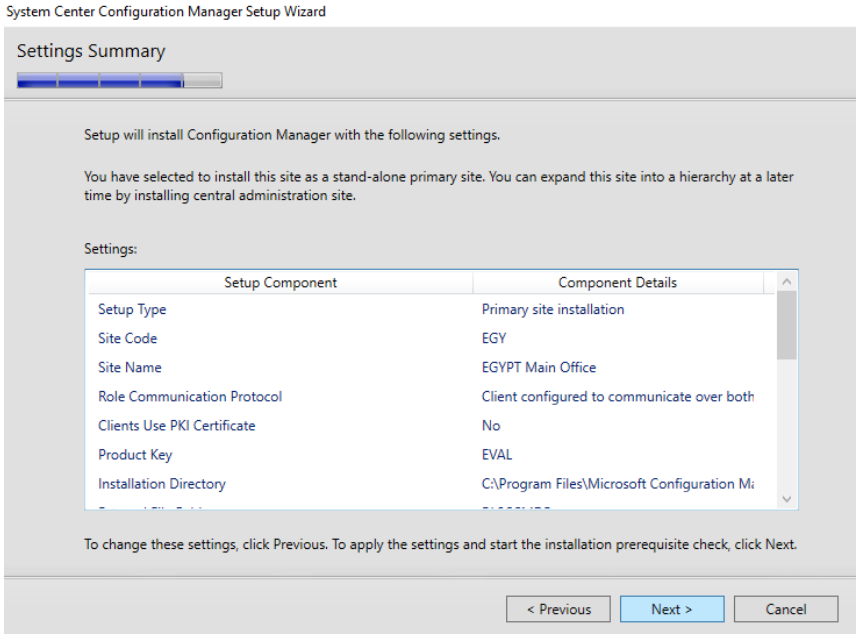

System Center Configuration Manager Setup Wizard
Database Information
Specify the locations for the SQL Server data file and transaction log file.
Path to the SQL Server data file
C:\Program Files\Microsoft SQL Server\MSSQL13.MSSQLSERVER\MSSQL\DATA\
Browse...
Path to the SQL Server log file
C:\Program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

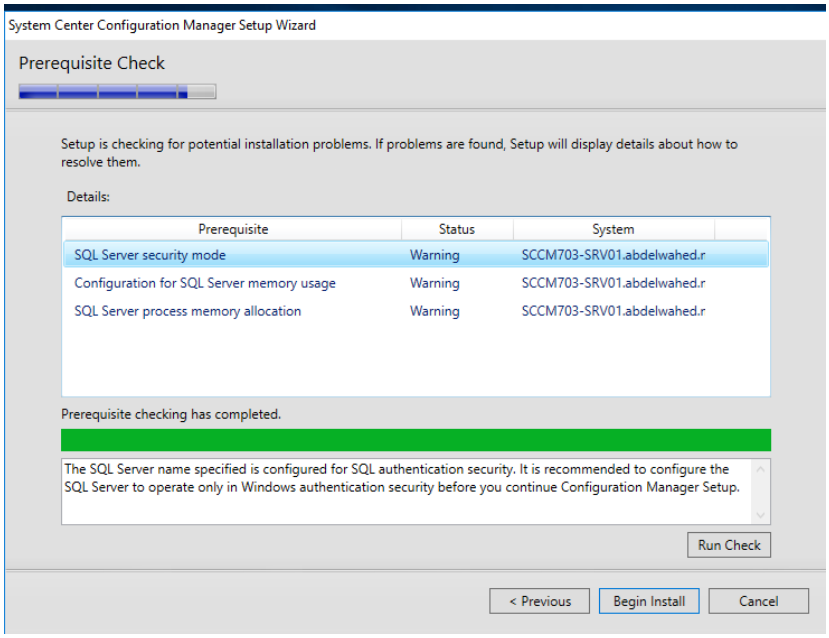

System Center Configuration Manager Setup Wizard
SMS Provider Settings
SMS Providers are used by the Configuration Manager console to communicate with the site database.
Specify the server where the SMS Provider will be installed.
SMS Provider (FQDN):
Example: server1.contoso.com
SCCM703-SRV01.abdelwahed.me
Note: The SMS Provider cannot be installed on a server that is configured for SQL Server clustering.

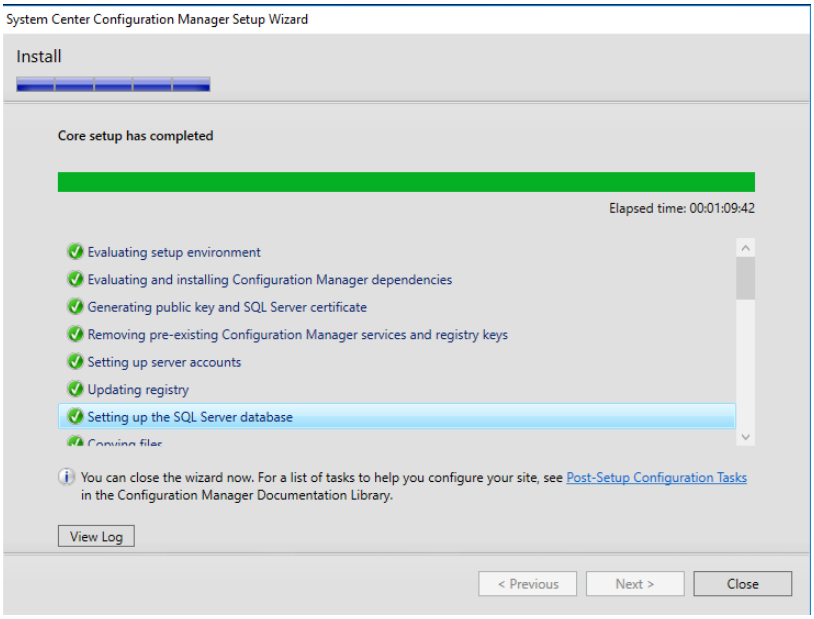

System Center Configuration Manager Setup Wizard
Client Computer Communication Settings
Configuration Manager site system roles can accept HTTP or HTTPS communication from clients. Specify whether to require all site system roles to accept only HTTPS communication or allow the communication method to 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.

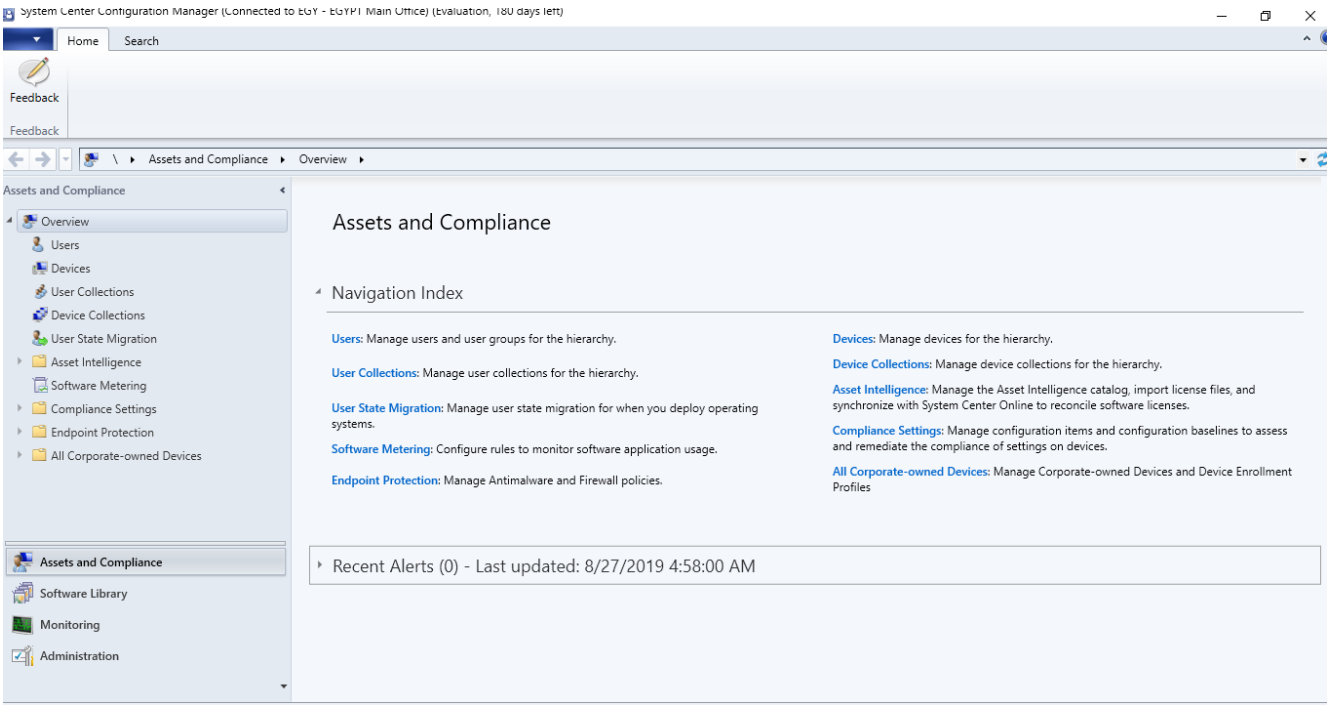

System Center Configuration Manager Setup Wizard
Site System Roles
Specify whether to have Setup install a management point or distribution point.
A management point provides clients with policy and content location information. It also receives configuration data from clients.
Install a management point.
FQDN:
SCCM703-SRV01.abdelwahed.me
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:
SCCM703-SRV01.abdelwahed.me
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):
SCCM703-SRV01.abdelwahed.me
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, Microsoft 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
EGY
Site Name
EGYPT Main Office
Role Communication Protocol
Client configured to communicate over both
Clients Use PKI Certificate
No
Product Key
EVAL
Installation Directory
C:\Program Files\Microsoft Configuration Ma
To change these settings, click Previous. To apply the settings and start the installation prerequisite check, click Next.
< Previous
Next >
Cancel

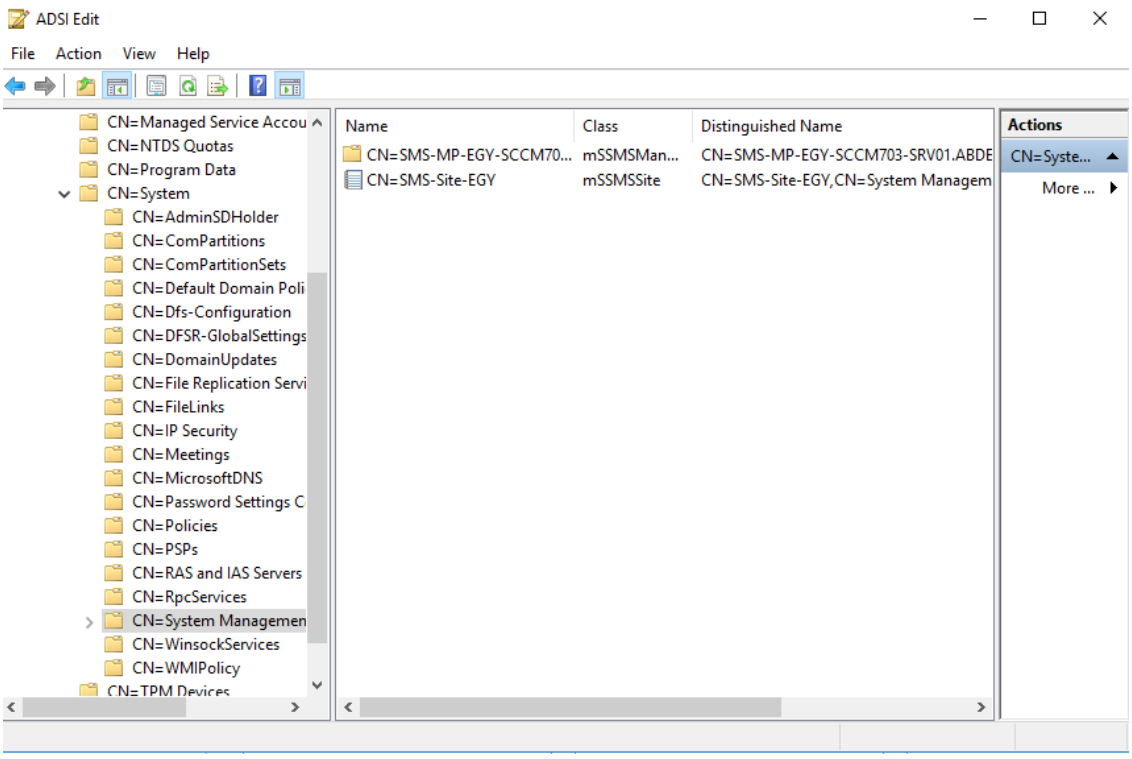

System Center Configuration Manager Setup Wizard
Prerequisite Check
Setup is checking for potential installation problems. If problems are found, Setup will display details about how to resolve them.
Details:
Prerequisite
Status
System
SQL Server security mode
Warning
SCCM703-SRV01.abdelwahed.r
Configuration for SQL Server memory usage
Warning
SCCM703-SRV01.abdelwahed.r
SQL Server process memory allocation
Warning
SCCM703-SRV01.abdelwahed.r
Prerequisite checking has completed.
The SQL Server name specified is configured for SQL authentication security. It is recommended to configure the SQL Server to operate only in Windows authentication security before you continue Configuration Manager Setup.
Run Check
< Previous
Begin Install
Cancel


System Center Configuration Manager Setup Wizard
Install
Core setup has completed
Elapsed time: 00:01:09:42
Evaluating setup environment
Evaluating and installing Configuration Manager dependencies
Generating public key and SQL Server certificate
Removing pre-existing Configuration Manager services and registry keys
Setting up server accounts
Updating registry
Setting up the SQL Server database
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



Verify the container that was set up in Active Directory during preparation to see if the SCCM server has added any attributes.

a



SCCM Post-Installation Configuration Tasks

Once you've set up SCCM (System Center Configuration Manager), there are a number of important steps to take post-installation to make sure everything is running smoothly. The following are some essential tasks you should carry out after installing SCCM:

1. Configure site maintenance tasks

- For optimal performance of SCCM, routine maintenance such as backing up the database and purging log files is crucial. These tasks should be set to execute periodically without manual intervention.
- To set up these maintenance tasks, launch the SCCM console and go to Administration > Site Configuration > Sites. Right-click on the site you wish to configure and choose Site Maintenance. There, you can adjust the settings for each task according to your preferences and establish a regular schedule for them to run.

2. Configure client settings

- Client settings in SCCM dictate client actions and site server interactions. Set these to control features like software updates, hardware inventory, and software metering.
- To adjust client settings, access the SCCM console, go to Administration > Client Settings, then either establish a new policy or alter an existing one. Customize the settings and roll out the policy to the appropriate client groups.

3. Configure discovery methods

- SCCM employs discovery methods to locate and incorporate new clients into its site database. Set up these methods to identify new clients in your network.
- Access the SCCM console, proceed to Administration > Hierarchy Configuration > Discovery Methods, and adjust settings for each method, including Active Directory System Discovery, Active Directory User Discovery, or Network Discovery as needed.

4. Configure boundaries

- Boundaries in SCCM delineate the network locations under SCCM management. Setting up boundaries is crucial to ensure clients are associated with the appropriate SCCM site.
- For boundary configuration, access the SCCM console and proceed to Administration > Hierarchy Configuration > Boundaries. Either establish a new boundary or adjust an existing one. Incorporate necessary IP addresses, IP ranges, or subnets. Link the boundary with the intended site.

5. Configure security

- Securing SCCM is crucial for safeguarding your company's information and assets. Set up SCCM security to allow only approved users entry to SCCM data and features.
- To set up security, access the SCCM console and go to Administration > Security. Establish security roles, then allocate permissions to users and groups accordingly. Use security scopes to restrict access to certain SCCM items.

6. Configure reporting

- SCCM offers numerous reports to oversee and control your SCCM setup. Set up reporting for convenient access to crucial management data in SCCM.
- To set it up, launch the SCCM console and go to Monitoring > Reporting. Link the reporting services point with the SQL Server Reporting Services. Organize report folders and give suitable permissions to users and groups according to your preference.

7. Monitor SCCM status

- Keep an eye on SCCM's performance by regularly checking its operational status. Utilize the Configuration Manager console and review log files for any potential problems. To oversee SCCM’s condition, access the console, move to the Monitoring section, and employ different monitoring tools to observe client activity, software rollouts, and important metrics. Analyze the log files to diagnose problems and spot opportunities for enhancements.

Device Collection and Queries

Building device collections and queries in System Center Configuration Manager (SCCM) is essential for efficiently managing and deploying software, updates, and configurations across an organization's devices. Here are some key aspects to consider when working with device collections and queries in SCCM:

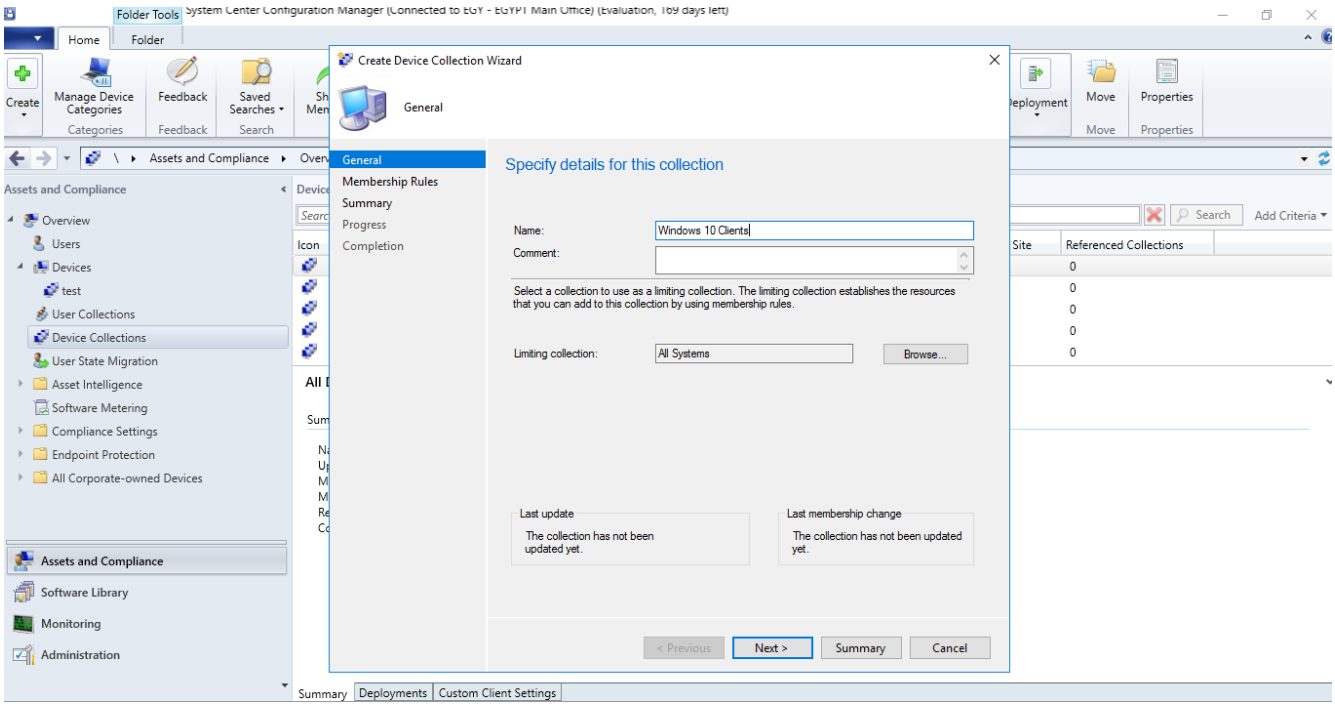
Device Collections

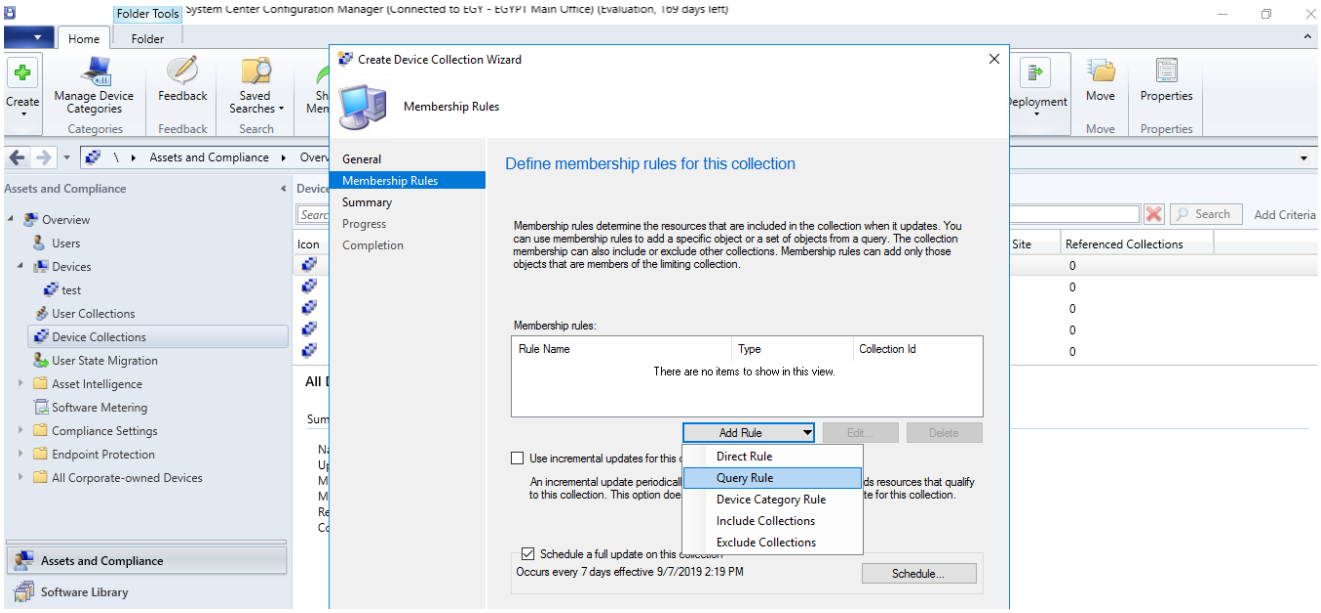
1. **Purpose**: Device collections are used to group devices based on specific criteria. These collections can then be targeted for software deployment, updates, compliance settings, and other management tasks.
2. **Types**:
    - **Static Collections**: Manually defined and do not change unless manually updated.
    - **Dynamic Collections**: Automatically updated based on a query that defines the membership criteria.
3. **Creating Device Collections**:
    - **Navigate to**: SCCM Console -> Assets and Compliance -> Device Collections.
    - **Steps**:
        - Right-click on "Device Collections" and select "Create Device Collection."
        - Provide a name and a limiting collection (the collection within which this collection will operate).
        - Define the membership rules (either direct or query-based).

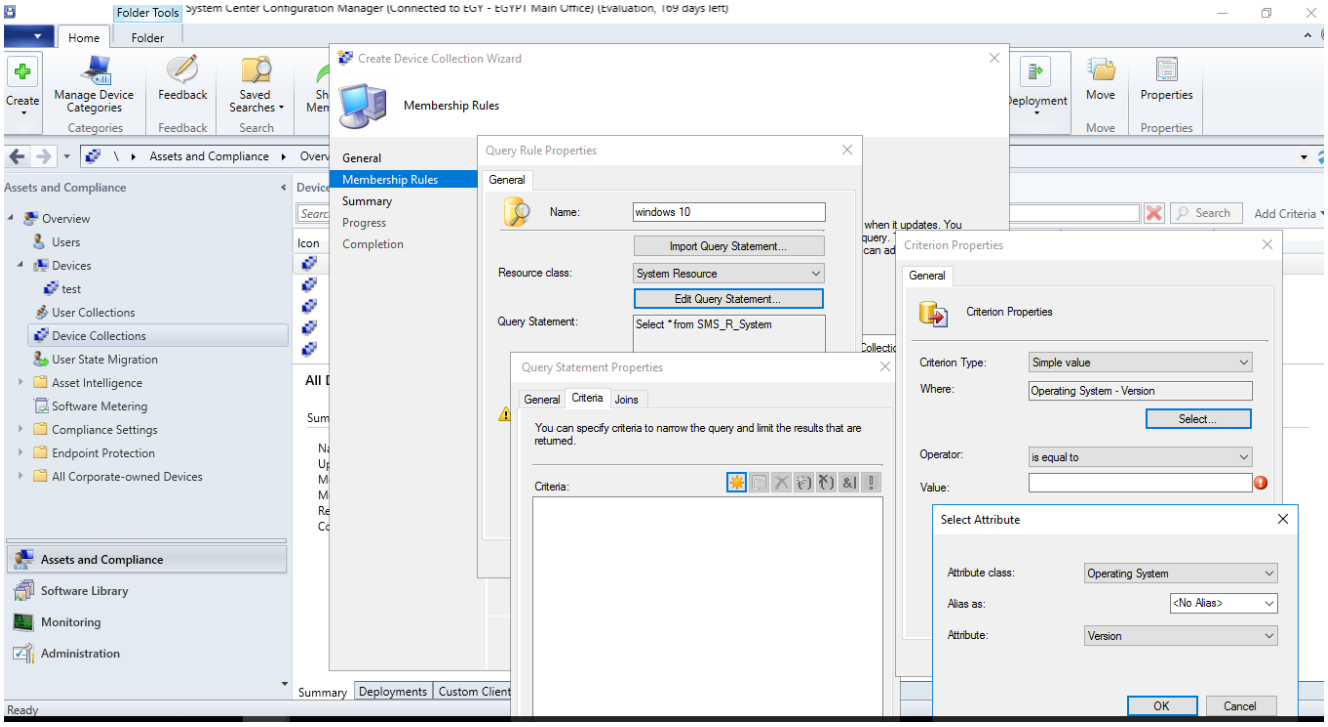
Queries

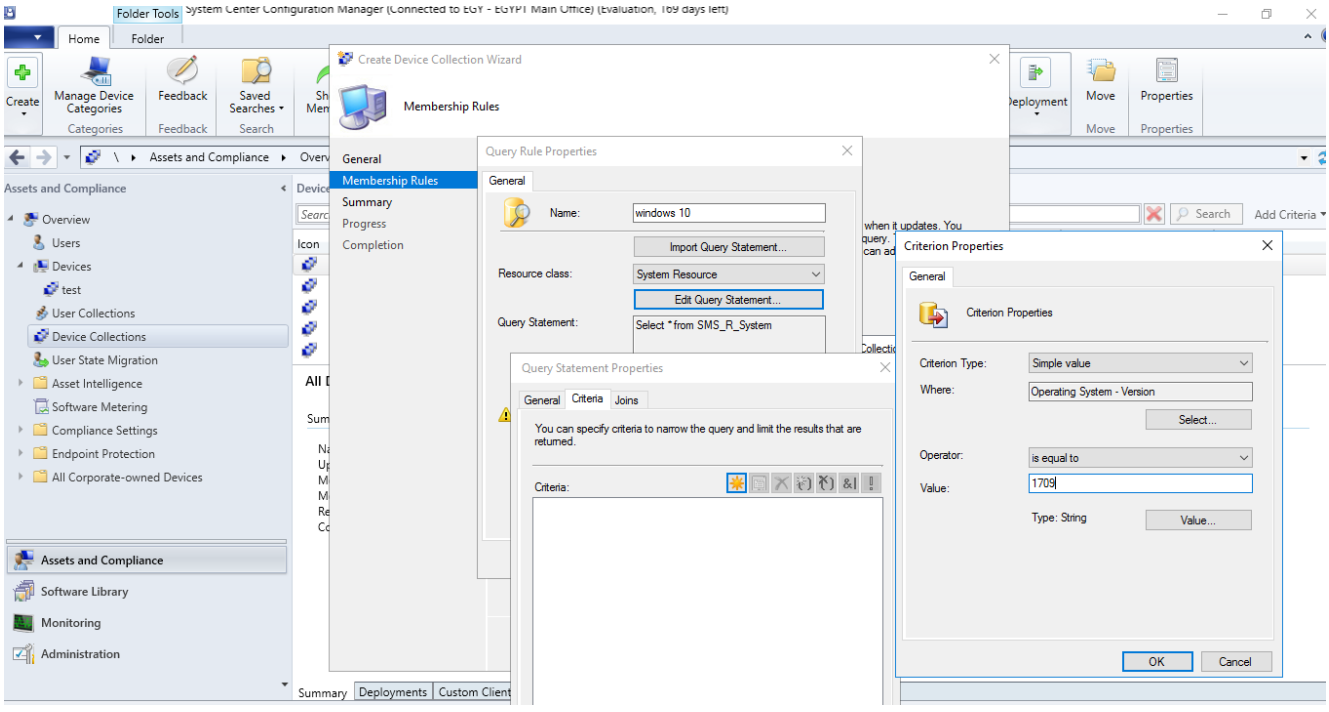
1. **Purpose**: Queries are used to define the criteria for dynamic collections and to retrieve specific information about devices or users.
2. **Creating Queries**:
    - **Navigate to**: SCCM Console -> Monitoring -> Queries.
    - **Steps**:
        - Right-click on "Queries" and select "Create Query."
        - Provide a name and a target collection.
        - Define the criteria by selecting attributes from the SCCM database.
3. **Common Query Criteria**:
    - Operating System Version.
    - Installed Applications.
    - Hardware Specifications (e.g., memory, CPU).
    - Active Directory Organizational Unit (OU).
    - Last Logon User.

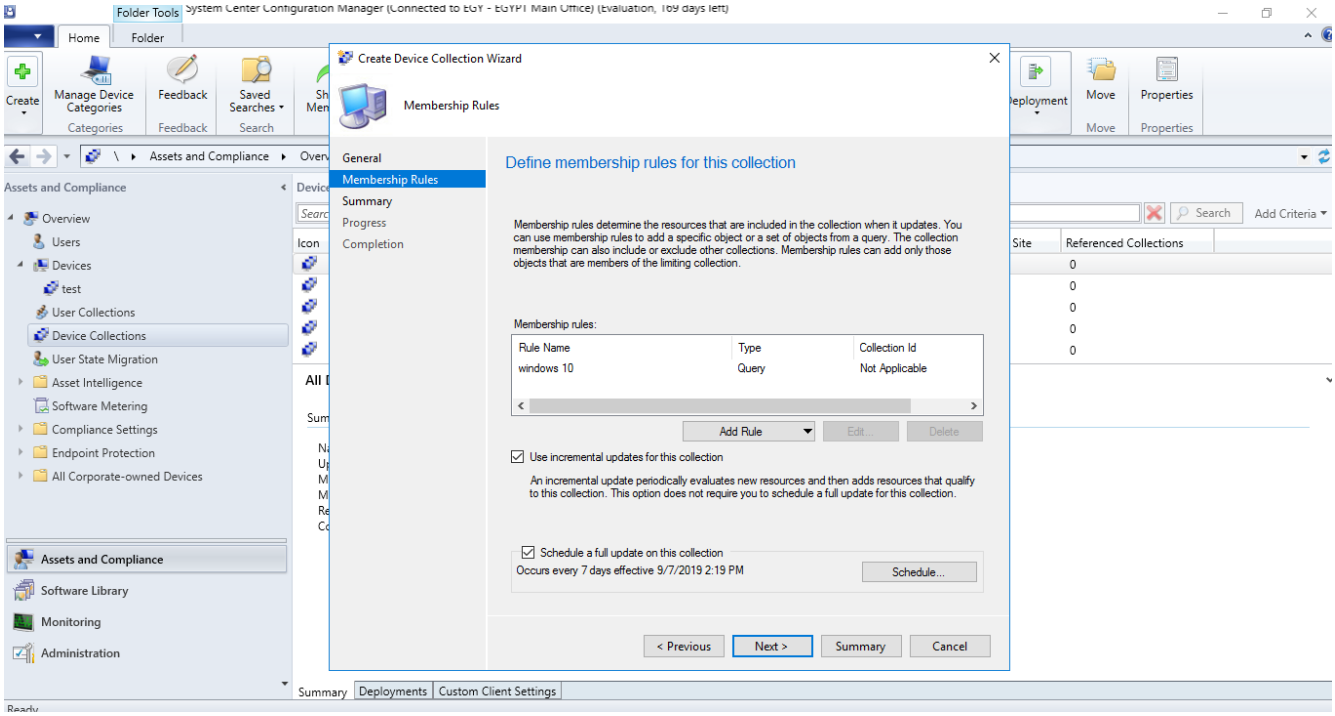
Windows 10 Collection using Version and build number

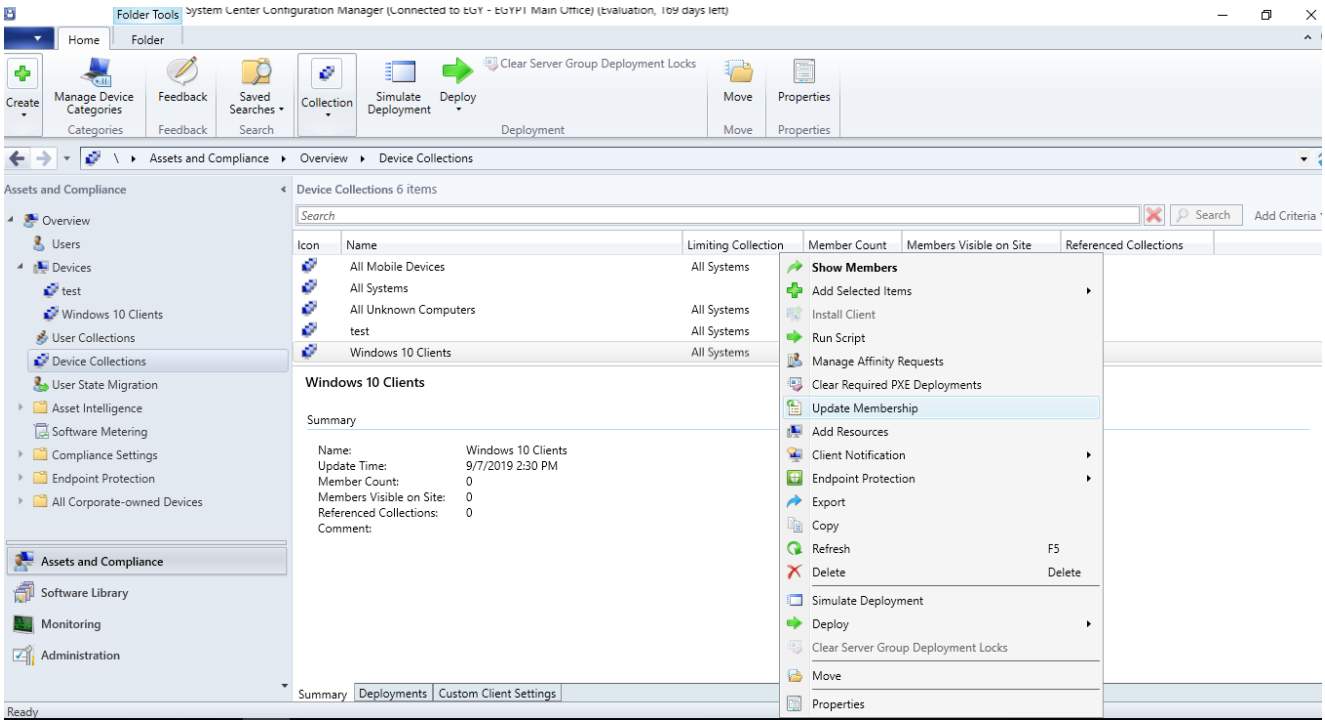


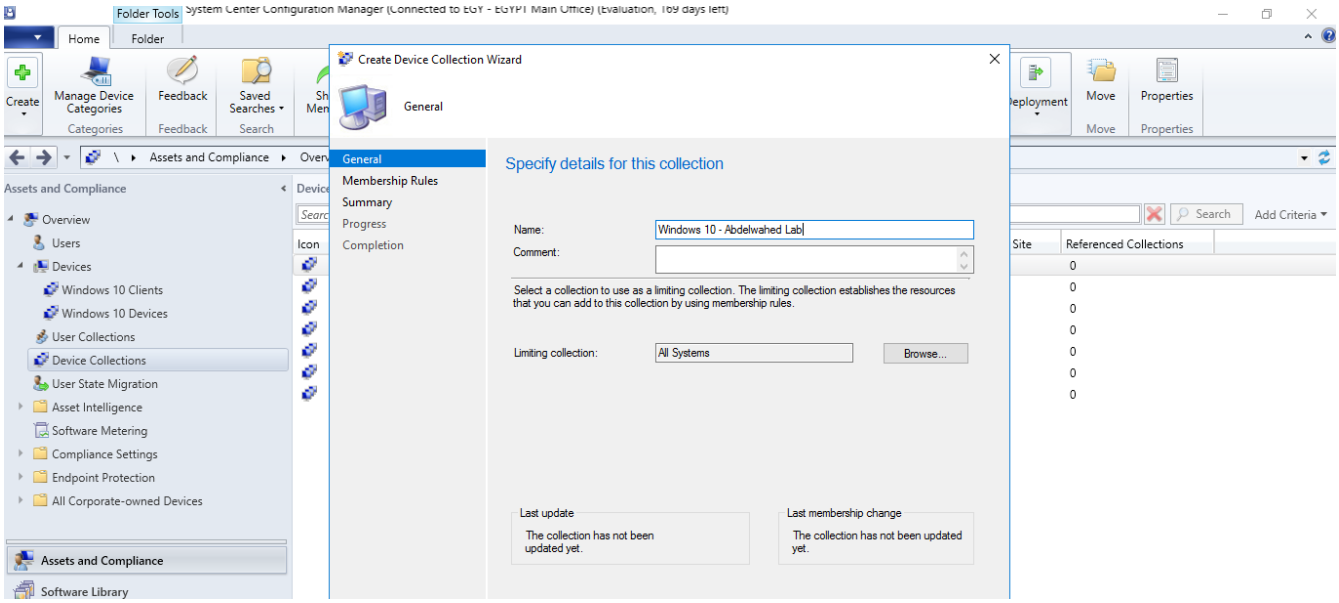


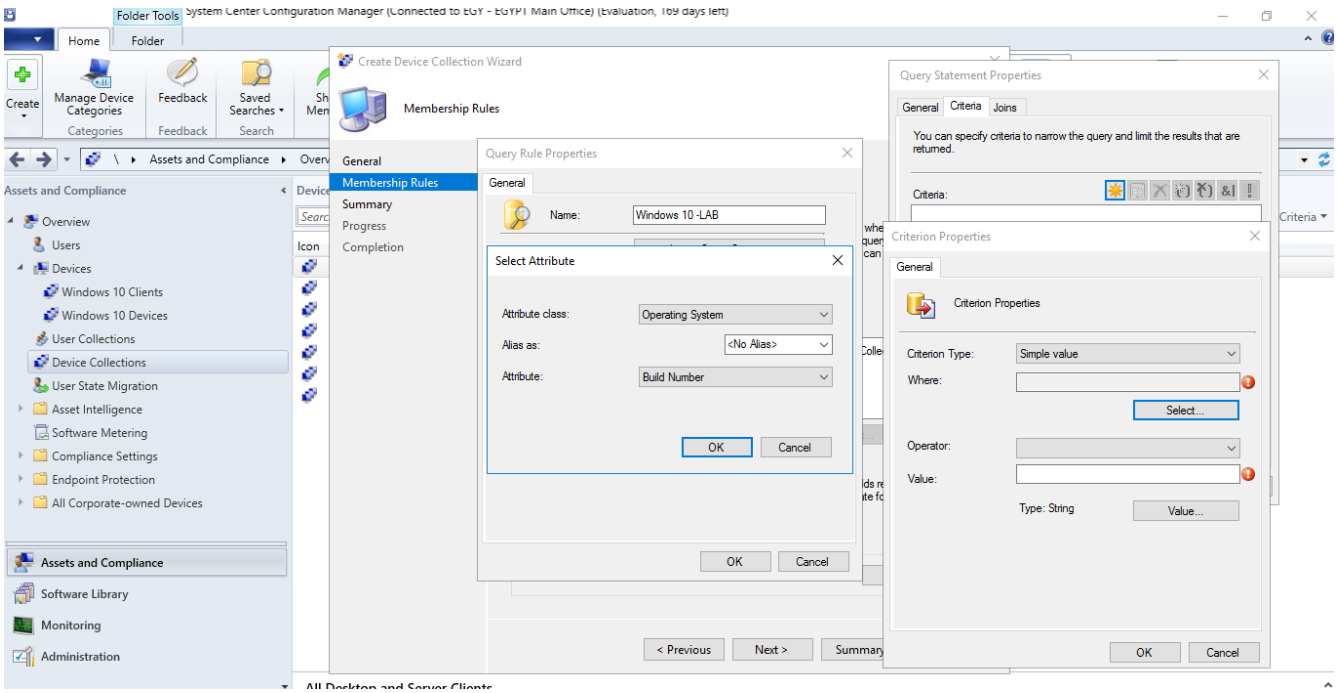

Create Device Collection Wizard
Membership Rules
General
Membership Rules
Summary
Progress
Completion
Query Rule Properties
Name: windows 10
Import Query Statement...
Resource class: System Resource
Edit Query Statement...
Query Statement: Select * from SMS_R_System
Query Statement Properties
General Criteria Joins
You can specify criteria to narrow the query and limit the results that are returned.
Criteria:
Criterion Properties
Criterion Type: Simple value
Where: Operating System - Version
Select...
Operator: is equal to
Value:
Select Attribute
Attribute class: Operating System
Alias as: <No Alias>
Attribute: Version
OK
Cancel

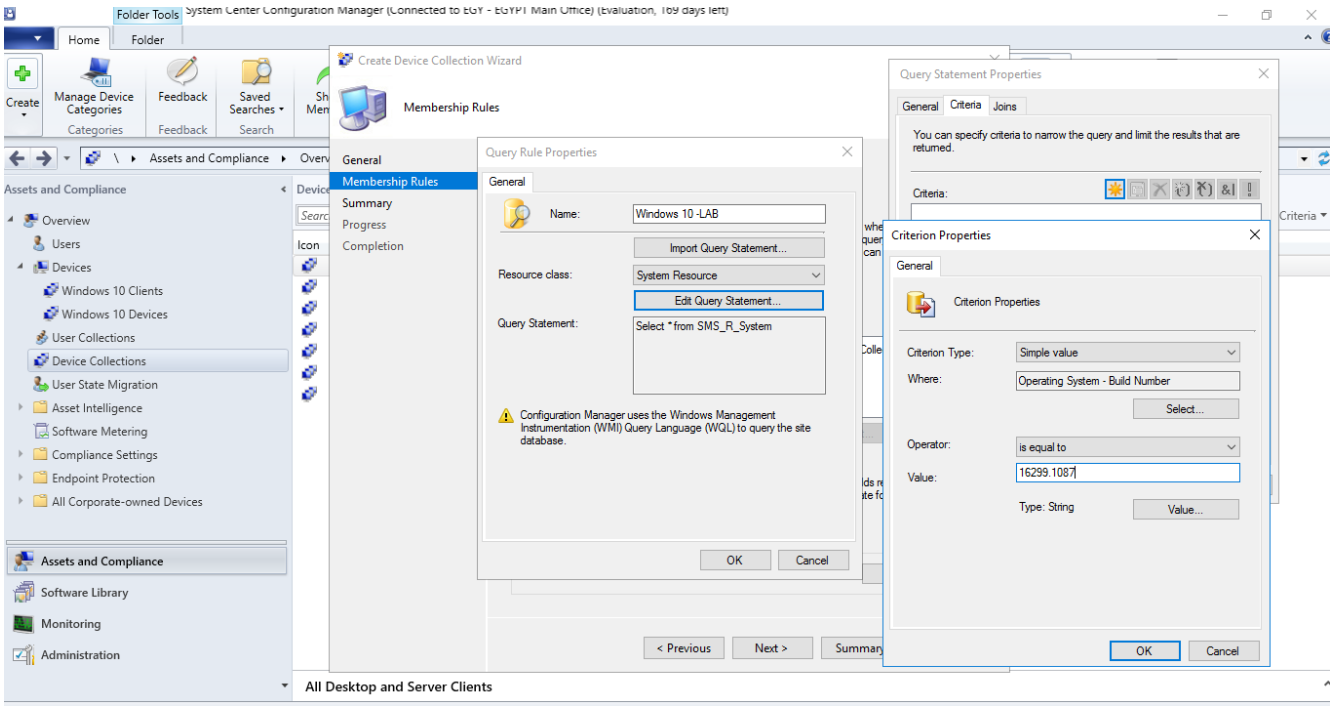

Create Device Collection Wizard
Membership Rules
General
Membership Rules
Summary
Progress
Completion
Query Rule Properties
Name: windows 10
Import Query Statement...
Resource class: System Resource
Edit Query Statement...
Query Statement: Select * from SMS_R_System
Query Statement Properties
General Criteria Joins
You can specify criteria to narrow the query and limit the results that are returned.
Criteria:
Criterion Properties
Criterion Type: Simple value
Where: Operating System - Version
Select...
Operator: is equal to
Value: 1709
Type: String
Value...
OK
Cancel

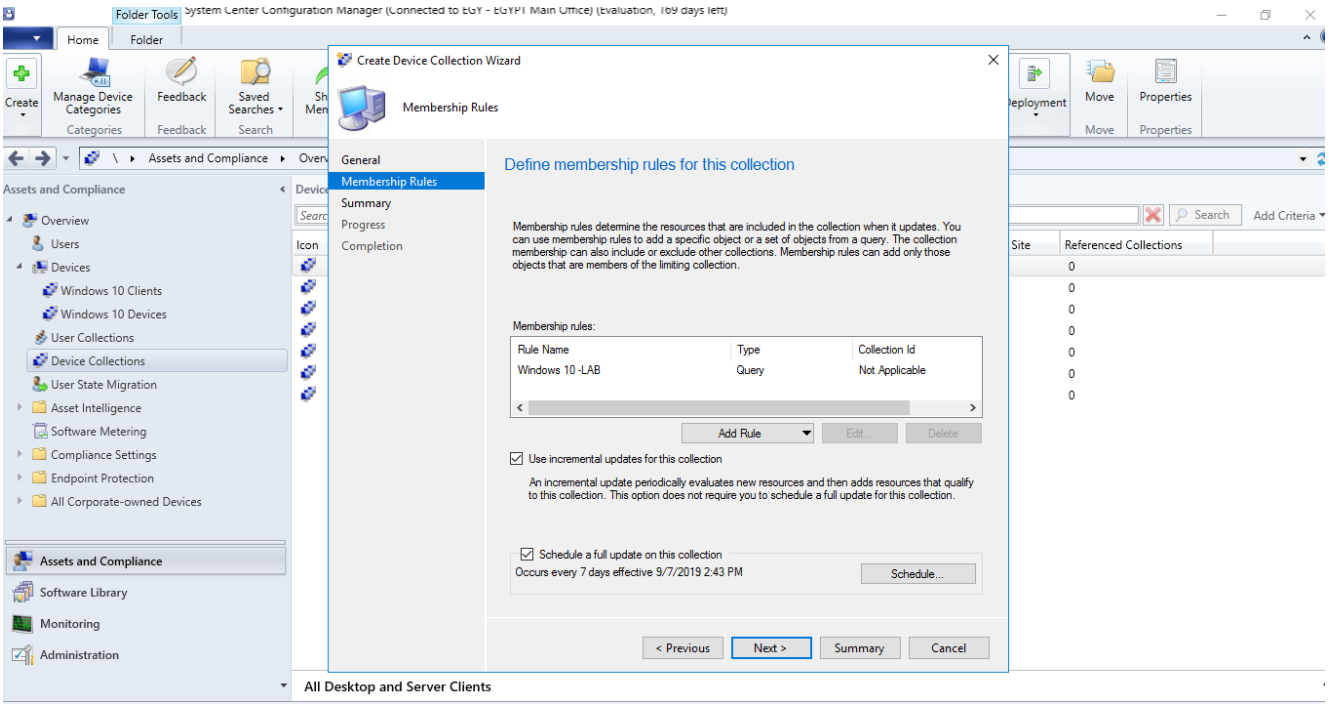

Create Device Collection Wizard
Membership Rules
General
Membership Rules
Summary
Progress
Completion
Define membership rules for this collection
Membership rules determine the resources that are included in the collection when it updates. You can use membership rules to add a specific object or a set 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 9/7/2019 2:19 PM
Schedule...
< Previous
Next >
Summary
Cancel


Windows 10 Clients
Summary
Name: Windows 10 Clients
Update Time: 9/7/2019 2:30 PM
Member Count: 0
Members Visible on Site: 0
Referenced Collections: 0
Comment:
Show Members
Add Selected Items
Install Client
Run Script
Manage Affinity Requests
Clear Required PXE Deployments
Update Membership
Add Resources
Client Notification
Endpoint Protection
Export
Copy
Refresh F5
Delete Delete
Simulate Deployment
Deploy
Clear Server Group Deployment Locks
Move
Properties


Create Device Collection Wizard
General
Specify details for this collection
Name: Windows 10 - Abdelwahed Lab
Comment:
Limiting collection: All Systems
Browse...
Last update
The collection has not been updated yet.
Last membership change
The collection has not been updated yet.


Create Device Collection Wizard
Membership Rules
Query Rule Properties
Name: Windows 10 -LAB
Select Attribute
Attribute class: Operating System
Alias as: <No Alias>
Attribute: Build Number
Query Statement Properties
Criterion Properties
Criterion Type: Simple value
Where:
Select...
Operator:
Value:
Type: String
Value...


Create Device Collection Wizard
Membership Rules
General
Membership Rules
Summary
Progress
Completion
Query Rule Properties
Name: Windows 10 -LAB
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.
OK
Cancel
Query Statement Properties
General
Criteria
Joins
You can specify criteria to narrow the query and limit the results that are returned.
Criteria:
Criterion Properties
General
Criterion Properties
Criterion Type: Simple value
Where: Operating System - Build Number
Select...
Operator: is equal to
Value: 16299.1087
Type: String
Value...
OK
Cancel
< Previous
Next >
Summary
All Desktop and Server Clients


Create Device Collection Wizard
Membership Rules
General
Membership Rules
Summary
Progress
Completion
Define membership rules for this collection
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 -LAB
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 9/7/2019 2:43 PM
Schedule...
< Previous
Next >
Summary
Cancel
All Desktop and Server Clients

SCCM Collections using queries

SCCM (System Center Configuration Manager) collections are used to group together devices or users in your environment based on specific criteria. SCCM collections are a powerful tool that can be used for software deployment, configuration management, compliance, and reporting. Here are some common SCCM collection queries that can be used to create collections based on specific criteria:

All SCCM client computers with less than 10GB free disk space on C drive

```
select SMS_R_SYSTEM.ResourceID,SMS_R_SYSTEM.ResourceType,SMS_R_SYSTEM.Name,
SMS_R_SYSTEM.SMSUniqueIdentifier,SMS_R_SYSTEM.ResourceDomainORWorkgroup,
SMS_R_SYSTEM.Client from SMS_R_System inner join SMS_G_System_LOGICAL_DISK on
SMS_G_System_LOGICAL_DISK.ResourceID = SMS_R_System.ResourceId
where SMS_G_System_LOGICAL_DISK.DeviceID = "C:" and
SMS_G_System_LOGICAL_DISK.FreeSpace <= 10000
```

Collection based on OU

```
select SMS_R_System.NetbiosName,
SMS_R_System.SystemOUName from
SMS_R_System where
SMS_R_System.SystemOUName = "PCs"
```

Collection based on domain membership

```
select * from  SMS_R_System where SMS_R_System.ResourceDomainORWorkgroup =
"andelwahed.me"
```

all Windows 10 clients

```
select SMS_R_System.NetbiosName,
SMS_R_System.OperatingSystemNameandVersion from
SMS_R_System where
SMS_R_System.OperatingSystemNameandVersion like "%Workstation 10%"
```

All Windows 10 Update 20H2 Collection

```
select
SMS_R_SYSTEM.ResourceID,SMS_R_SYSTEM.ResourceType,SMS_R_SYSTEM.Name,SMS_R_SYSTEM.SM
SUniqueIdentifier,SMS_R_SYSTEM.ResourceDomainORWorkgroup,SMS_R_SYSTEM.Client from
SMS_R_System inner join SMS_G_System_OPERATING_SYSTEM on
SMS_G_System_OPERATING_SYSTEM.ResourceID = SMS_R_System.ResourceId where
SMS_G_System_OPERATING_SYSTEM.BuildNumber = "19042"
```

Collections based on vendor (DELL)

```
select *  from  SMS_R_System inner join SMS_G_System_COMPUTER_SYSTEM on
SMS_G_System_COMPUTER_SYSTEM.ResourceID = SMS_R_System.ResourceId
where SMS_G_System_COMPUTER_SYSTEM.Manufacturer like "Dell%"
```

Computers with a specific software installed Collection

```
select SMS_R_System.NetbiosName,
SMS_G_System_ADD_REMOVE_PROGRAMS.DisplayName from
SMS_R_System inner join SMS_G_System_ADD_REMOVE_PROGRAMS on
SMS_G_System_ADD_REMOVE_PROGRAMS.ResourceId =
SMS_R_System.ResourceId where
SMS_G_System_ADD_REMOVE_PROGRAMS.DisplayName like "Microsoft%office%"
```

SCCM Quick Lab Guide

All Windows Servers Collection

```
select SMS_R_SYSTEM.ResourceID, SMS_R_SYSTEM.ResourceType, SMS_R_SYSTEM.Name,
SMS_R_SYSTEM.SMSUniqueIdentifier,SMS_R_System.OperatingSystemNameandVersion,
SMS_R_SYSTEM.ResourceDomainORWorkgroup, SMS_R_SYSTEM.Client
from SMS_R_System where SMS_R_System.OperatingSystemNameandVersion like "Microsoft
Windows NT Server%"
OR SMS_R_System.OperatingSystemNameandVersion like "Microsoft Windows NT Advanced
Server%"
```

Windows 2019 Servers Collection

```
select
SMS_R_SYSTEM.ResourceID,SMS_R_SYSTEM.ResourceType,SMS_R_SYSTEM.Name,SMS_R_SYSTEM.SM
SUniqueIdentifier,SMS_R_SYSTEM.ResourceDomainORWorkgroup,SMS_R_SYSTEM.Client from
SMS_R_System inner join SMS_G_System_OPERATING_SYSTEM on
SMS_G_System_OPERATING_SYSTEM.ResourceID = SMS_R_System.ResourceId where
SMS_G_System_OPERATING_SYSTEM.Name like "Microsoft Windows Server 2019 %"
```

All Windows 2016 Servers Collection

```
select SMS_R_SYSTEM.ResourceID, SMS_R_SYSTEM.ResourceType, SMS_R_SYSTEM.Name,
SMS_R_SYSTEM.SMSUniqueIdentifier,SMS_R_System.OperatingSystemNameandVersion,
SMS_R_SYSTEM.ResourceDomainORWorkgroup, SMS_R_SYSTEM.Client
from SMS_R_System where SMS_R_System.OperatingSystemNameandVersion like "Microsoft
Windows NT Server 10.0%"
OR SMS_R_System.OperatingSystemNameandVersion like "Microsoft Windows NT Advanced
Server 10.0%"
```

SQL Servers Collection

```
select *  from  SMS_R_System inner join SMS_G_System_COMPUTER_SYSTEM on
SMS_G_System_COMPUTER_SYSTEM.ResourceID = SMS_R_System.ResourceId
where SMS_G_System_COMPUTER_SYSTEM.Roles like "%SQLServer%"
```

All SQL Server Management Studio installed Collection

```
select
SMS_R_SYSTEM.ResourceID,SMS_R_SYSTEM.ResourceType,SMS_R_SYSTEM.Name,SMS_R_SYSTEM.SM
SUniqueIdentifier,SMS_R_SYSTEM.ResourceDomainORWorkgroup,SMS_R_SYSTEM.Client from
SMS_R_System inner join SMS_G_System_INSTALLED_SOFTWARE on
SMS_G_System_INSTALLED_SOFTWARE.ResourceID = SMS_R_System.ResourceId where
SMS_G_System_INSTALLED_SOFTWARE.ProductName like "Microsoft SQL Server Management
Studio %"
```

All Domain Controllers Collection

```
select *  from  SMS_R_System inner join SMS_G_System_COMPUTER_SYSTEM on
SMS_G_System_COMPUTER_SYSTEM.ResourceId = SMS_R_System.ResourceId
where SMS_G_System_COMPUTER_SYSTEM.Roles like "%Domain_Controller%"
```

All VMs Collection

```
select SMS_R_System.ResourceId, SMS_R_System.ResourceType, SMS_R_System.Name,
SMS_R_System.SMSUniqueIdentifier, SMS_R_System.OperatingSystemNameandVersion,
SMS_R_System.ResourceDomainORWorkgroup, SMS_R_System.Client from  SMS_R_System
where SMS_R_System.IsVirtualMachine like "True"
```

IP range Collection

```
select *
from SMS_R_System
where SMS_R_System.IPAddresses like "192.168.0.1[1-9]"
```

Computers with a specific software installed (Visio) Collection

```
select SMS_R_System.NetbiosName,
SMS_G_System_ADD_REMOVE_PROGRAMS.DisplayName from
SMS_R_System inner join SMS_G_System_ADD_REMOVE_PROGRAMS on
SMS_G_System_ADD_REMOVE_PROGRAMS.ResourceId =
SMS_R_System.ResourceId where
SMS_G_System_ADD_REMOVE_PROGRAMS.DisplayName like "Microsoft%Visio%"
```

Last Logon Time: You can create a collection based on the last logon time of a device. The following query can be used to create a collection of devices that have not logged in for the last 30 days:

```
SELECT * FROM SMS_R_System WHERE DATEDIFF(day, SMS_R_System.LastLogonTimeStamp,
GETDATE()) >= 30
```

Processor: You can create a collection based on the processor type or speed.
The following query can be used to create a collection of devices with a processor speed of 2.5 GHz or higher:

```
SELECT * FROM SMS_R_System INNER JOIN SMS_G_System_PROCESSOR ON
SMS_G_System_PROCESSOR.ResourceID = SMS_R_System.ResourceId WHERE
SMS_G_System_PROCESSOR.MaxClockSpeed >= 2500
```

SCCM CMPivot

SCCM CMPivot is an on-the-fly exploration and problem-solving tool integrated into Microsoft System Center Configuration Manager (SCCM). It enables SCCM administrators to query and access current information from client systems of SCCM instantly, bypassing the requirement for deep SQL or SCCM database architecture expertise.

Administrators can utilize SCCM CMPivot to execute real-time queries on client machines for insights on installed applications, active processes, configuration details, and more. This utility supports data filtration, ordering, and grouping to expedite problem detection and resolution.

For large-scale troubleshooting, such as determining which machines have certain programs or assessing the standing of a particular SCCM client, SCCM CMPivot proves extremely beneficial. Furthermore, it serves as a means to promptly reveal security flaws or compliance issues across numerous devices.

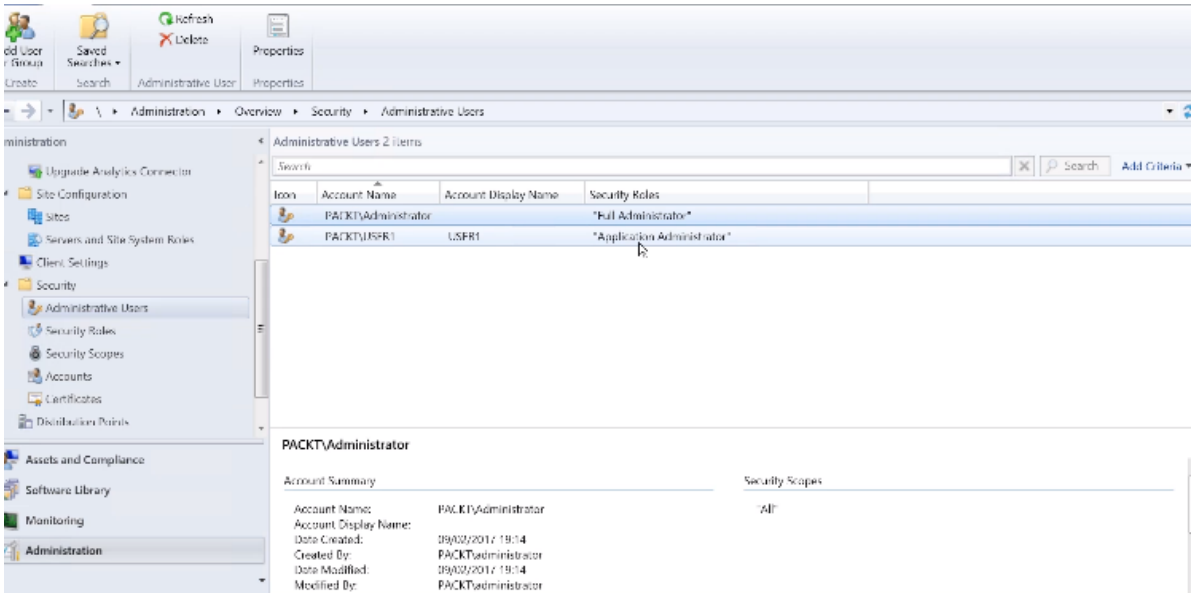
Here are some examples of how SCCM CMPivot can be used:

5. Locating devices with a certain application via CMPivot: Administrators can initiate a real-time query in CMPivot to identify all devices within the SCCM framework that have a specific application. The related query could be formatted as follows: Application | where DisplayName == "Application Name" | distinct Device.
6. Verifying a particular SCCM client's status: To review the condition of an individual SCCM client, admins can execute a query revealing comprehensive details about the client, encompassing its current setup, installed programs, active processes, etc. This query might resemble: Device | where Device == "Client Device Name" | summarize by Device, LastCheckInTime, OSVersion, IPAddress.
7. Spotting devices missing recent updates: Admins can use CMPivot to detect any devices that haven't received the latest software patch in the SCCM environment. They can run a query structured like: Update | where Title == "Update Title" | where TimeLastDeployed < ago(7d) | distinct Device.
8. Monitoring a specific service across devices: To assess the operation of a particular service over the entirety of SCCM-enrolled devices, administrators have the option to perform a live query for data on service conditions. A typical query might be: Service | where DisplayName == "Service Name" | summarize by Device, DisplayName, StartMode, State.
9. Identifying devices with insufficient disk space: Administrators tasked with pinpointing devices running low on storage space can turn to CMPivot to enact a query collating details on the storage availability across all devices. Such a query may look like: LogicalDisk | where FreeSpace < 1073741824 | summarize by Device, DriveLetter, Size, FreeSpace.
10. Checking a specific process's status on devices: In situations where an admin needs to verify a specific process's activity throughout the SCCM ecosystem, they can deploy a prompt query to obtain stats about the process engagement. The desired query formulation might be: Process | where Name == "Process Name" | summarize by Device, Name, Path, CommandLine, ProcessId.
11. Detecting devices with non-current antivirus definitions: Ensuring modern antivirus protection, administrators can leverage CMPivot to unearth devices with old antivirus definitions, running a query that gleans information about the antivirus status on every device configured. This could equate to a query like: AntiMalwareStatus | where AMProductStatus == "UpToDate" | where AMLastFullScanAge > 7 | summarize by Device, AMProductName, AMEngineVersion, AMLastFullScanAge.
12. Pinpointing devices with a designated registry key: Admins can utilize CMPivot for the identification of devices carrying a specific registry key by performing a query that fetches data regarding the pertinent registry keys across all devices. A suggested query format is: Registry | where Hive == "HKEY_LOCAL_MACHINE" | where KeyPath == "SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run" | where ValueName == "StartupItem" | distinct Device.

Role-Based Administration (RBA)

Role-Based Access Control (RBAC) is a method of regulating access to System Center Configuration Manager (SCCM) resources by assigning permissions to specific roles. RBAC in SCCM offers an adaptable and detailed approach for overseeing user privileges, allowing for precise management of resource and feature access within SCCM. This ensures that users possess only the necessary access required to fulfill their duties.

- **Roles in SCCM RBAC: SCCM RBAC operates on defined roles, which delineate the access permissions for users. Standard roles such as Security Administrator, Read-Only Analyst, and Application Administrator are readily available in SCCM. Additionally, you can tailor custom roles to satisfy particular needs.**
- **Scopes in SCCM RBAC: In SCCM RBAC, scopes specify the range of resources accessible by a user. These scopes can encompass collections, sites, and organizational units (OUs), enabling you to regulate what resources a user can view or control based on their assigned scope.**
- **Security Roles Feature: The SCCM RBAC system includes various security roles that specify user permissions. Roles like Full Administrator and Application Administrator, among others, come with predefined permissions outlining the permissible user actions within the system.**
- **Defining Collection Scopes: With SCCM RBAC, defining collection scopes restricts users' access to designated collections, ensuring they manage only the necessary devices or user groups.**
- **Implementing Site Scopes: By utilizing site scopes within SCCM RBAC, user access is limited to specific SCCM sites, allowing for precise management of the sites necessary for their role.**
- **Organizational Unit (OU) Scopes Functionality: SCCM RBAC allows the configuration of OU scopes, restricting users to interact only with devices or users within their assigned OUs, thereby streamlining the scope of their management responsibilities.**



Reports

SCCM (System Center Configuration Manager) offers robust reporting features that leverage SQL Server Reporting Services (SSRS) to create, manage, and deliver a variety of reports. These reports cover different aspects of the IT environment, such as software deployment, compliance, and asset inventory. Here's a detailed overview of SCCM reporting capabilities:

1. Integration with SSRS

- **Server-Based Reporting**: SCCM uses SSRS, a server-based reporting platform, to deliver a wide range of reports.
- **Pre-Built Reports**: SCCM includes numerous pre-built reports that can be customized to meet specific needs.

2. Comprehensive Reporting Scope

- **Software Deployment**: Generate reports on software deployment statuses, success rates, and issues.
- **Compliance**: Monitor compliance with security policies, configurations, and software updates.
- **Asset Inventory**: Track hardware and software inventory across the organization.

3. Scheduling and Automation

- **Automated Reports**: Reports can be scheduled to run automatically at specified intervals.
- **Email Delivery**: Scheduled reports can be emailed to specific users or groups, ensuring timely access to critical information.

4. Report Templates

- **Wide Range of Templates**: Access a variety of report templates that serve as a starting point for custom reports.
- **Customization**: Templates can be modified to meet specific requirements or used as-is for common report types.

5. Custom Report Creation

- **SSRS and Other Tools**: Custom reports can be created using SSRS or other reporting tools.
- **Database Access**: Utilize the SCCM database to pull extensive data about the IT environment for custom reports.

6. Data Visualization

- **Visualization Options**: Include charts, tables, and graphs to represent data visually.
- **Customization**: Visualizations can be tailored to meet specific reporting requirements, making data easier to interpret.

7. Drill-Down Capability

- **In-Depth Analysis**: Drill down into specific data points for additional context and insight.
- **Trend and Pattern Identification**: Identify trends, patterns, and issues that may not be apparent from a high-level overview.

8. Data Filtering and Sorting

- **Focus on Specific Data**: Filter and sort data to concentrate on particular aspects of the IT environment.
- **Informed Decision Making**: Easier identification of issues and trends leads to better decision-making.

Example Use Case

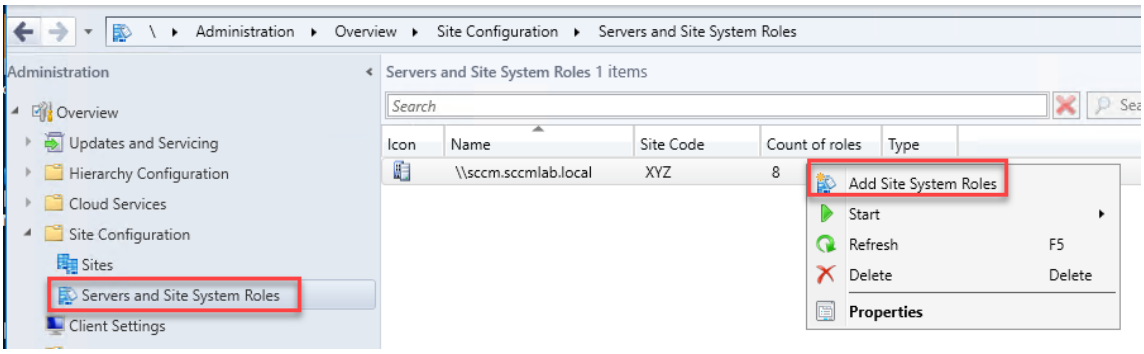
Generating a Software Compliance Report

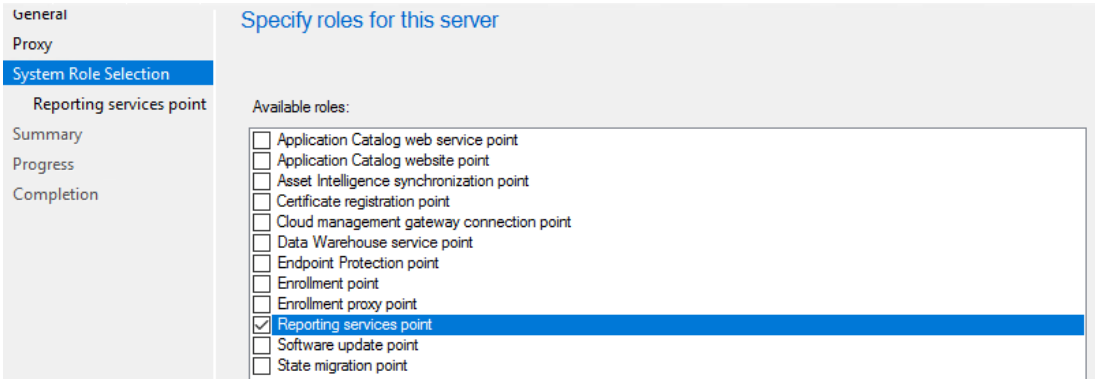
1. **Navigate to Reporting**:
    - SCCM Console -> Monitoring -> Reporting -> Reports.

2. **Select a Report**:
    - Choose a pre-built compliance report, such as "Compliance 1 - Overall Compliance."
3. **Customize the Report**:
    - Modify the report template if needed to include specific compliance rules or device collections.
4. **Schedule the Report**:
    - Set up a schedule for the report to run automatically, such as weekly or monthly.
    - Configure email delivery to send the report to the compliance team.
5. **Analyze Results**:
    - Review the report to identify non-compliant devices.
    - Drill down into specific non-compliance issues to determine root causes and take corrective actions.

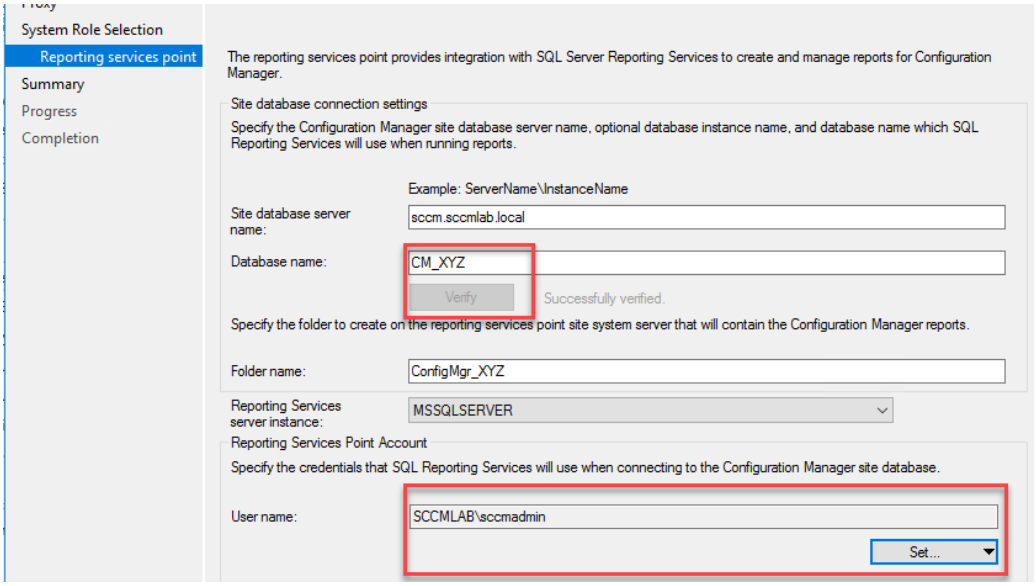
By leveraging SCCM's reporting features, IT administrators can gain valuable insights into their IT environment, ensure compliance, and make data-driven decisions to enhance overall management and operations.

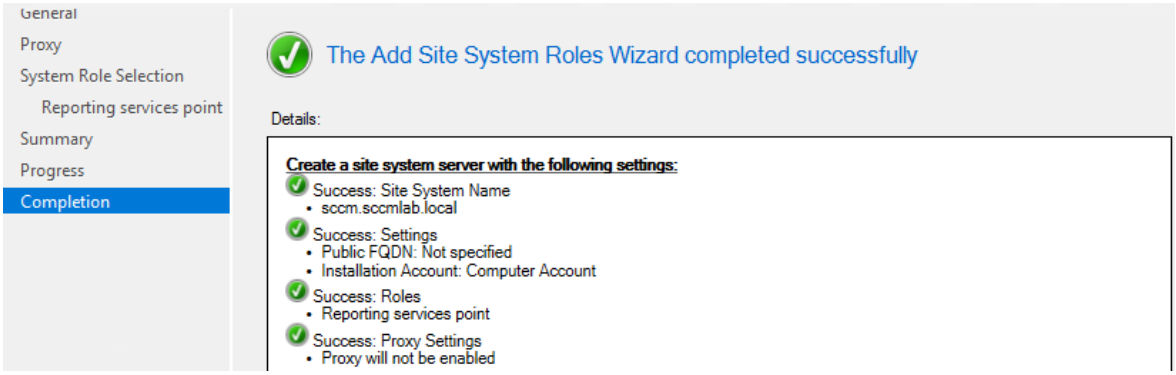
To complete this task, set up a reporting service point and an asset intelligence point. Additionally, an internet connection is required for the initial retrieval of online reports by SCCM.

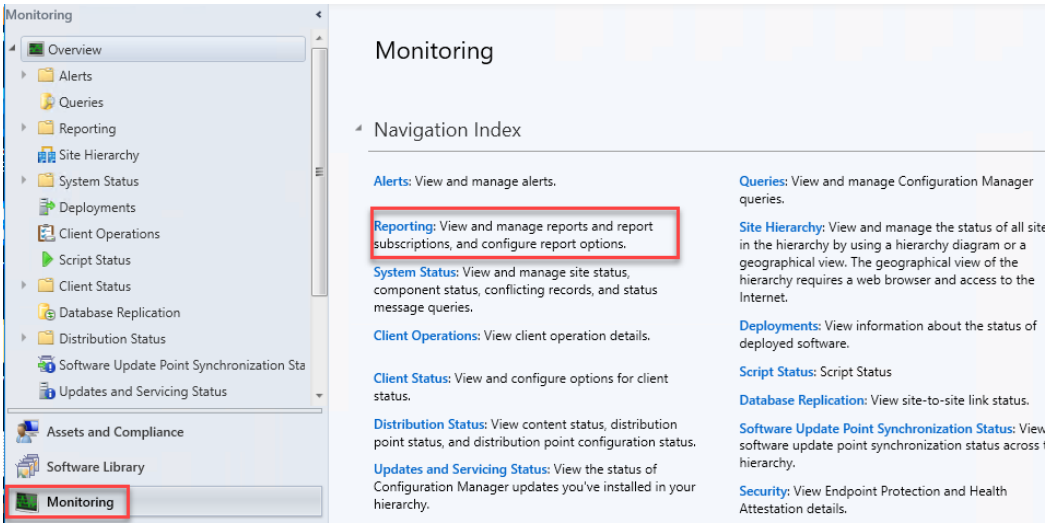




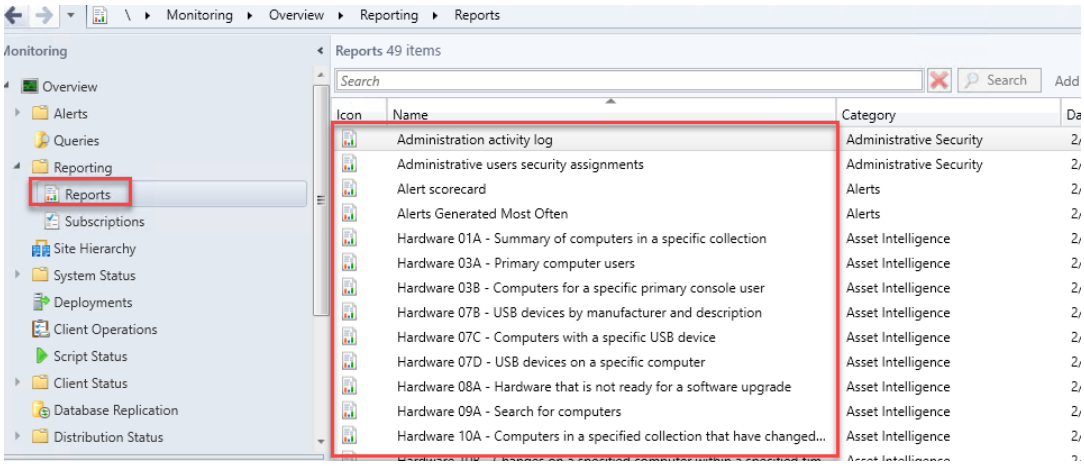
In the subsequent step, you will need to add a user who has the SQL permissions that were utilized during the SCCM installation.





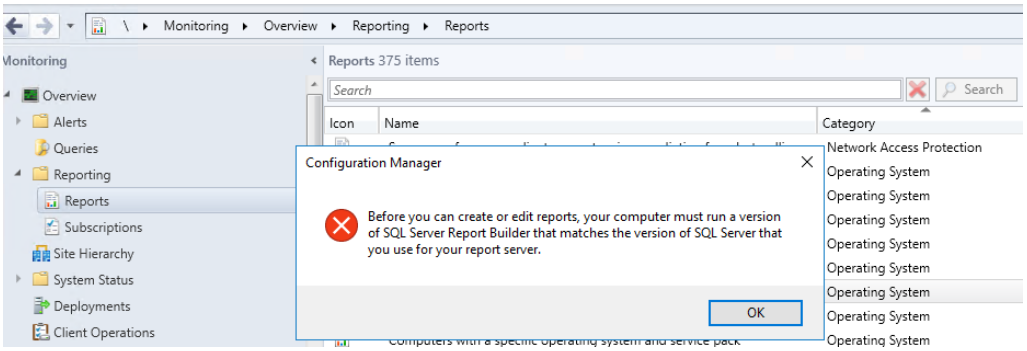


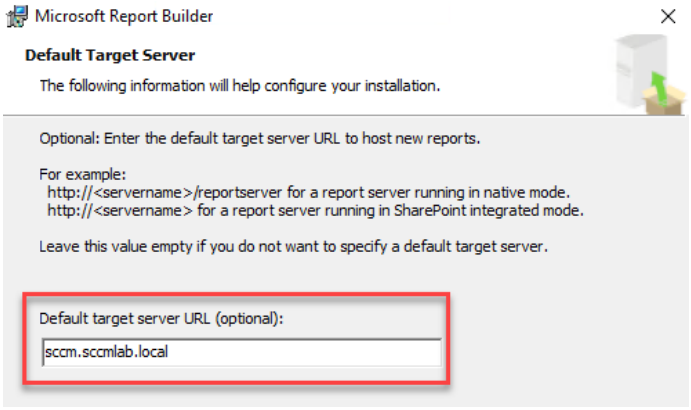
Upon accessing the "Reports" area found within the "Monitoring" section of the SCCM console, there might be a slight delay as the server collects all the report templates. This occurs as SCCM compiles all templates from the SQL Reporting Services (SSRS) server to display them within the console interface.



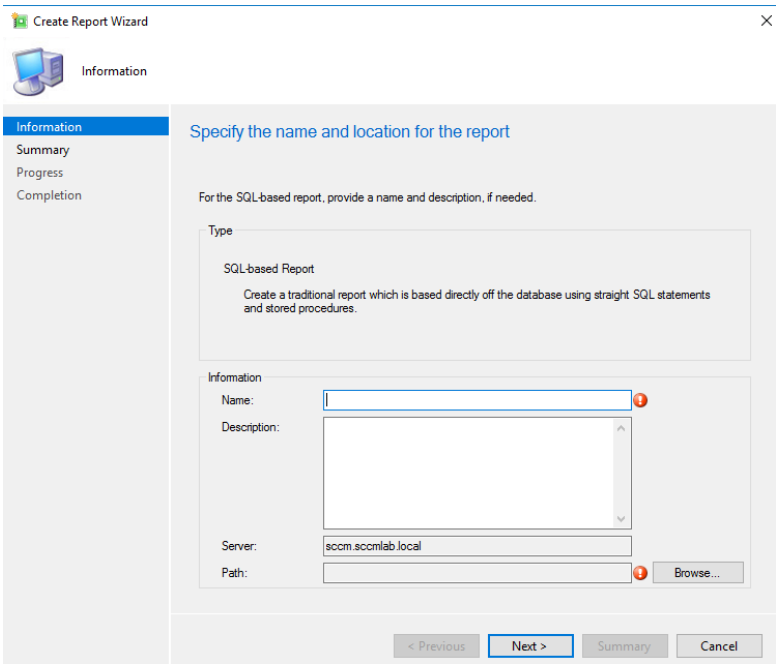
Create custom report

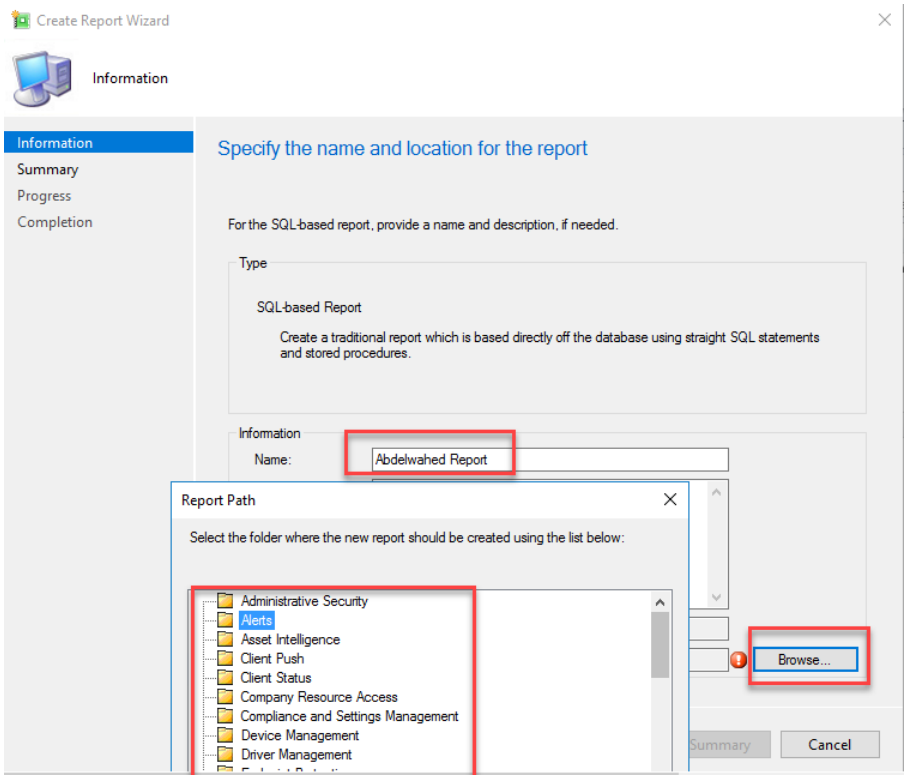
download and install SQL report builder

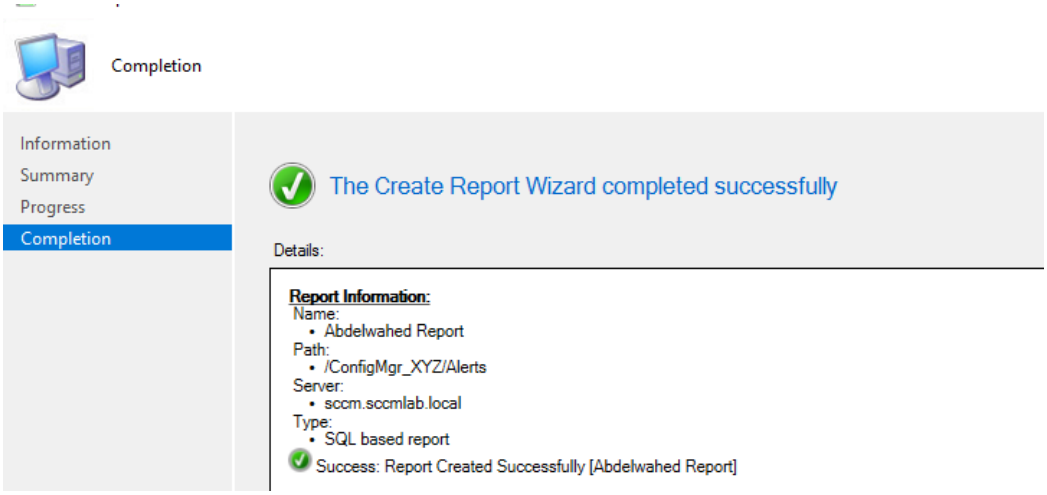


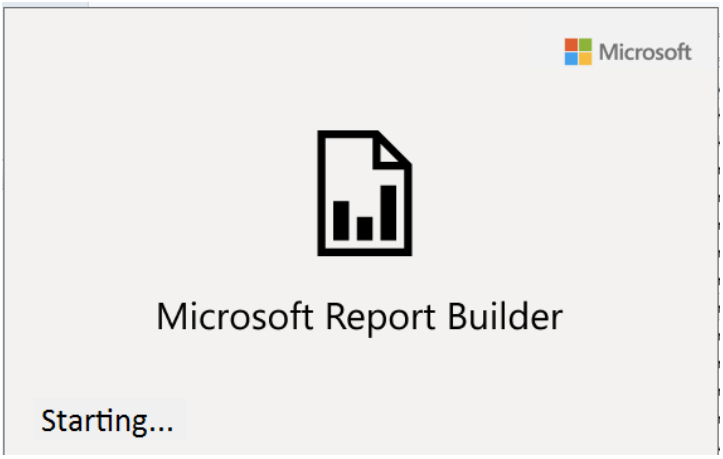


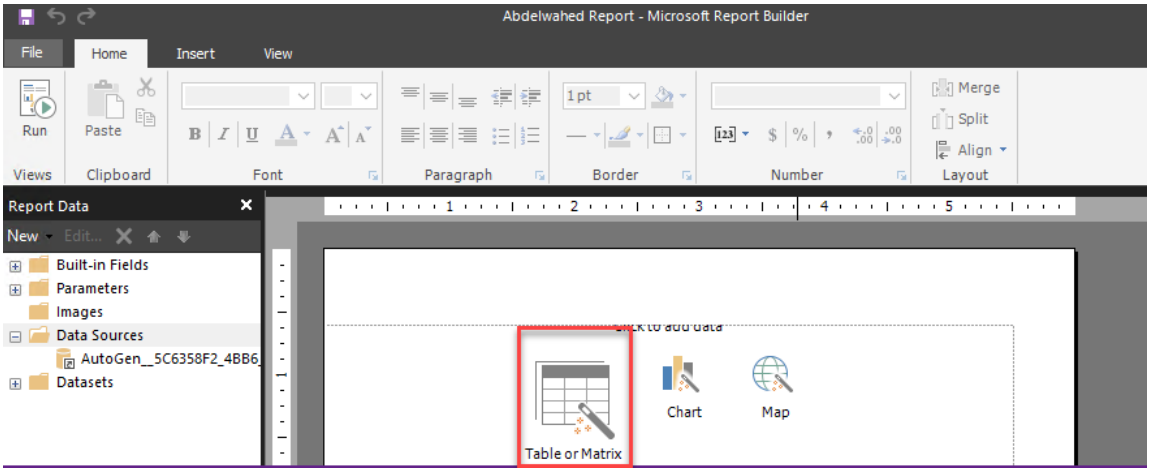
create custom report

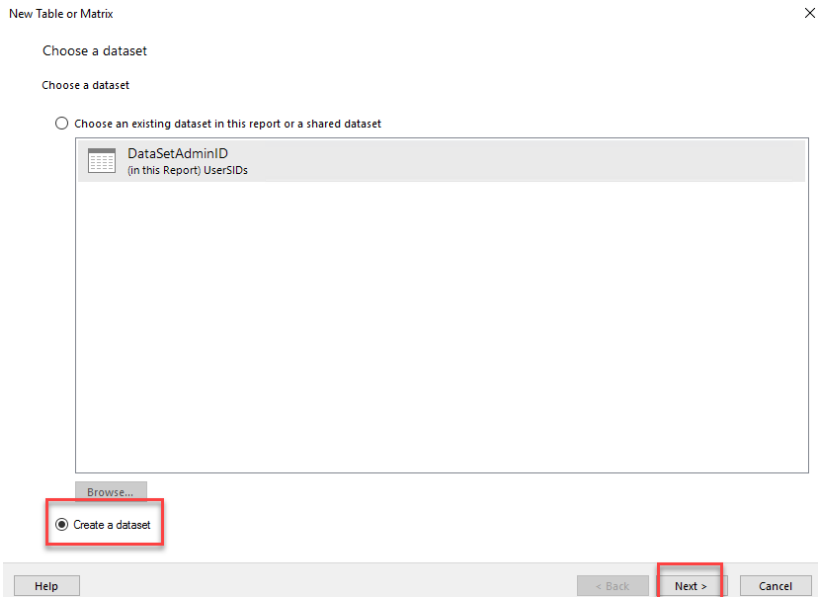


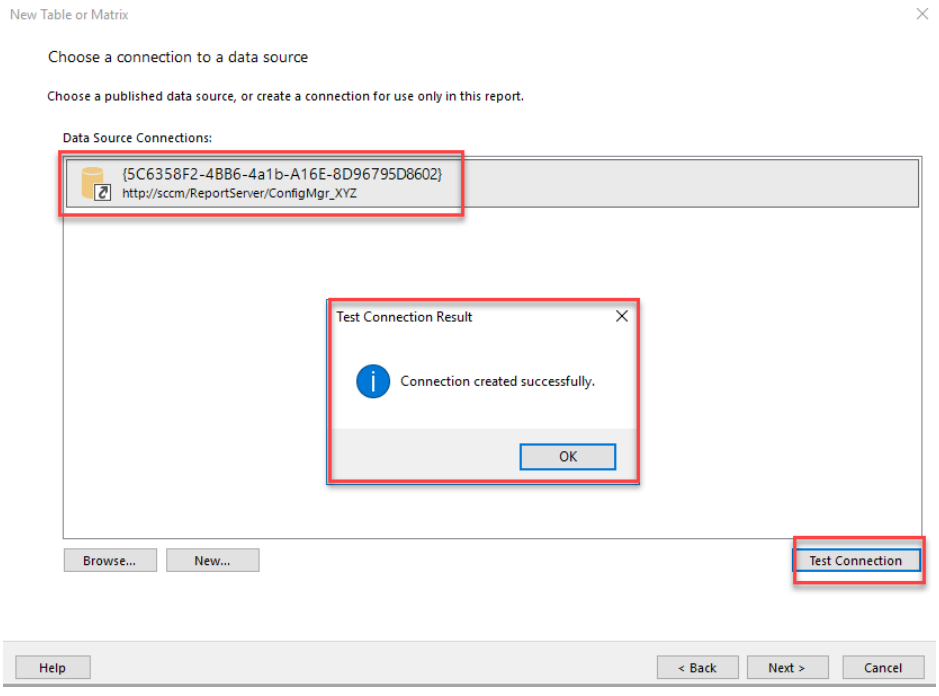


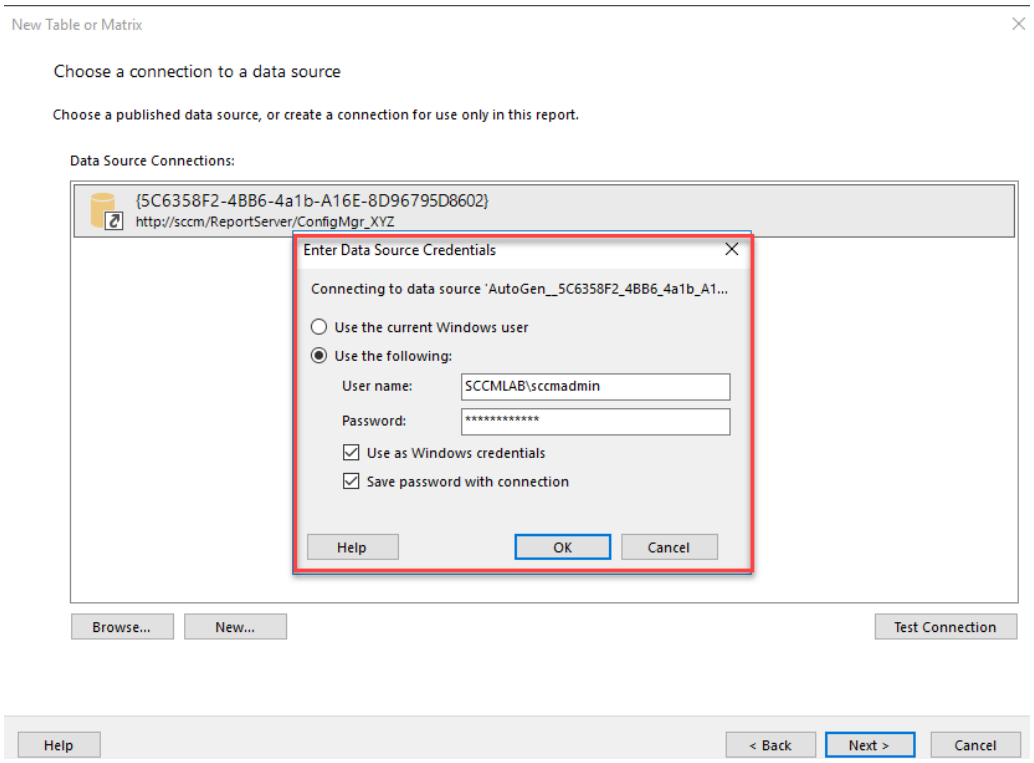

Completion
Information
Summary
Progress
Completion
The Create Report Wizard completed successfully
Details:
Report Information:
Name:
• Abdelwahed Report
Path:
• /ConfigMgr_XYZ/Alerts
Server:
• sccm.sccmlab.local
Type:
• SQL based report
Success: Report Created Successfully [Abdelwahed Report]

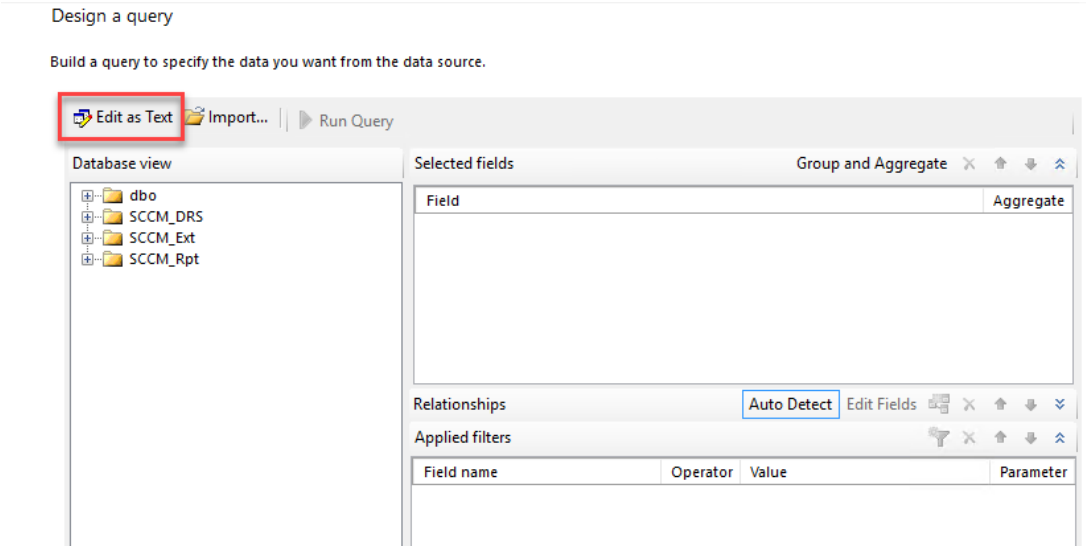

Microsoft
Microsoft Report Builder
Starting...


Abdelwahed Report - Microsoft Report Builder
File
Home
Insert
View
Run
Paste
Views
Clipboard
Font
Paragraph
Border
Number
Merge
Split
Align
Layout
Report Data
New
Edit...
Built-in Fields
Parameters
Images
Data Sources
AutoGen__5C6358F2_4BB6
Datasets
Table or Matrix
Chart
Map

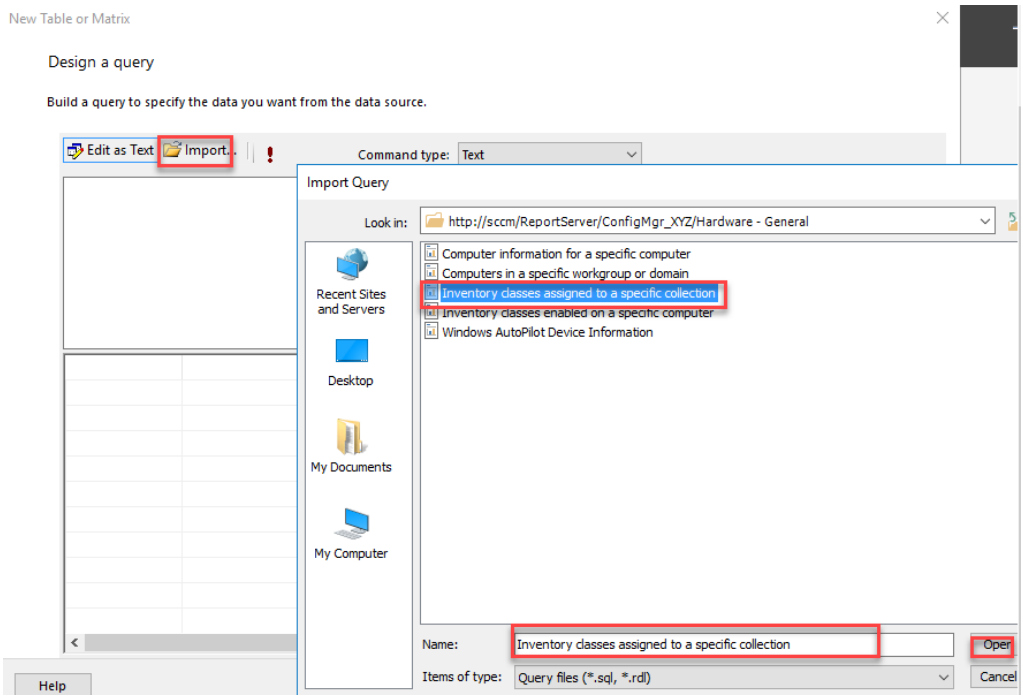

New Table or Matrix
Choose a dataset
Choose a dataset
Choose an existing dataset in this report or a shared dataset
DataSetAdminID
(in this Report) UserSIDs
Browse...
Create a dataset
Help
< Back
Next >
Cancel

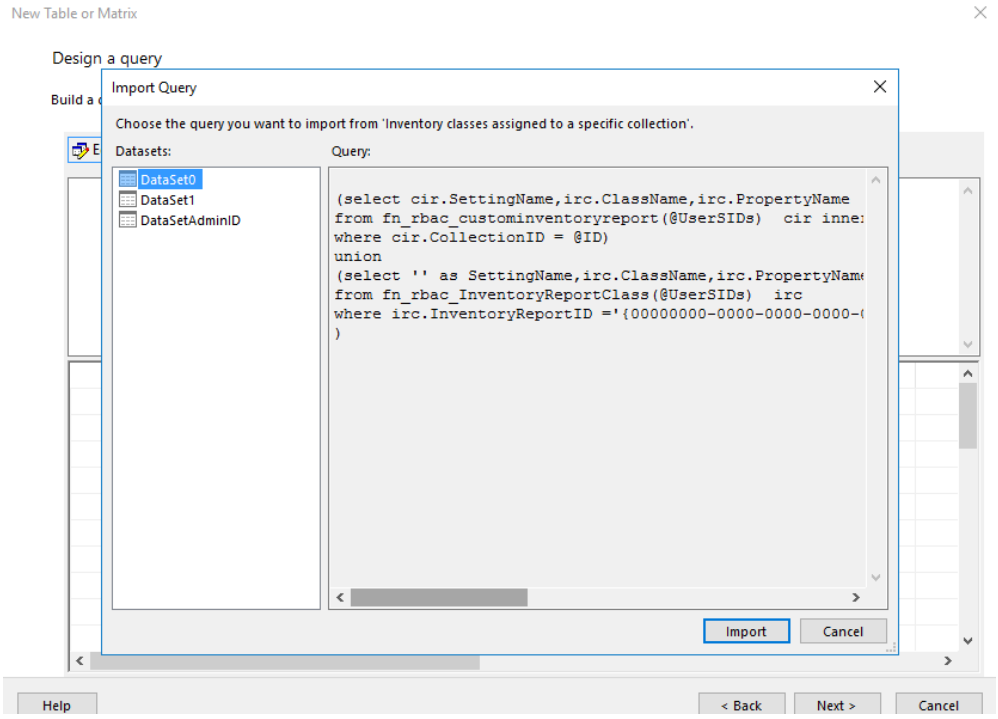

New Table or Matrix
Choose a connection to a data source
Choose a published data source, or create a connection for use only in this report.
Data Source Connections:
{5C6358F2-4BB6-4a1b-A16E-8D96795D8602}
http://sccm/ReportServer/ConfigMgr_XYZ
Test Connection Result
Connection created successfully.
OK
Browse...
New...
Test Connection
Help
< Back
Next >
Cancel

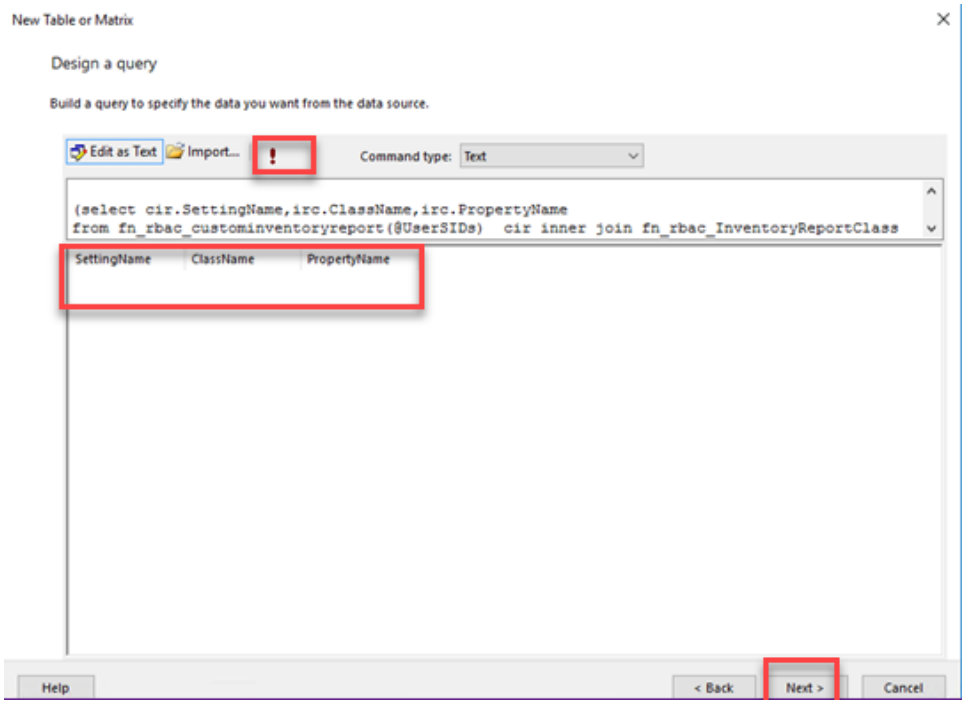

New Table or Matrix
Choose a connection to a data source
Choose a published data source, or create a connection for use only in this report.
Data Source Connections:
{5C6358F2-4BB6-4a1b-A16E-8D96795D8602}
http://sccm/ReportServer/ConfigMgr_XYZ
Enter Data Source Credentials
Connecting to data source 'AutoGen__5C6358F2_4BB6_4a1b_A1...
Use the current Windows user
Use the following:
User name:
SCCMLAB\sccmadmin
Password:
Use as Windows credentials
Save password with connection
Help
OK
Cancel
Browse...
New...
Test Connection
Help
< Back
Next >
Cancel

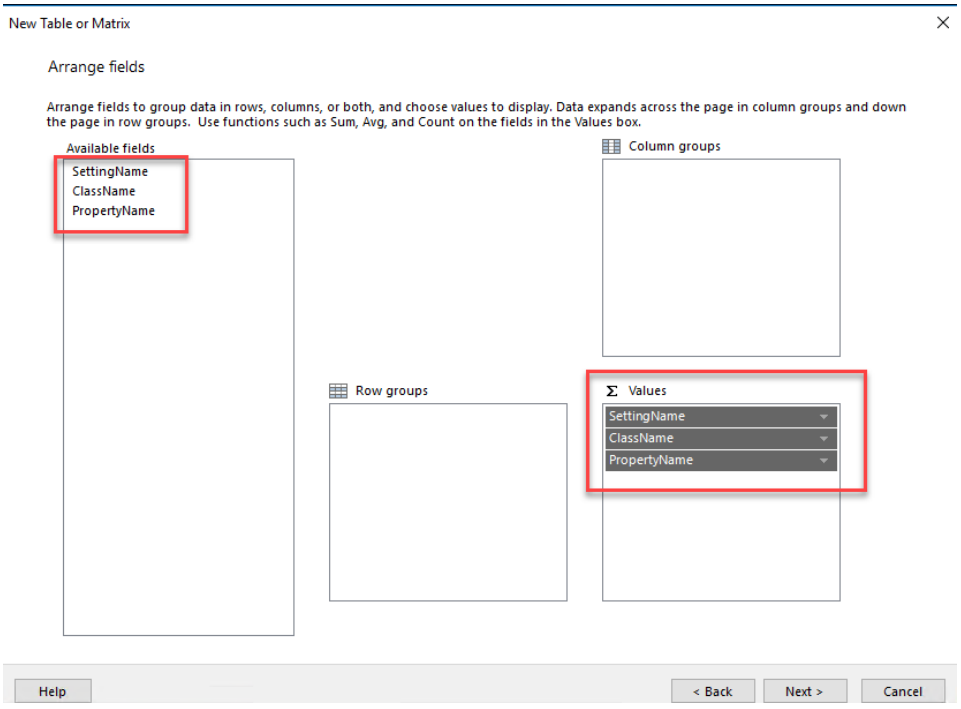

Design a query
Build a query to specify the data you want from the data source.
Edit as Text
Import...
Run Query
Database view
dbo
SCCM_DRS
SCCM_Ext
SCCM_Rpt
Selected fields
Group and Aggregate
Field
Aggregate
Relationships
Auto Detect
Edit Fields
Applied filters
Field name
Operator
Value
Parameter

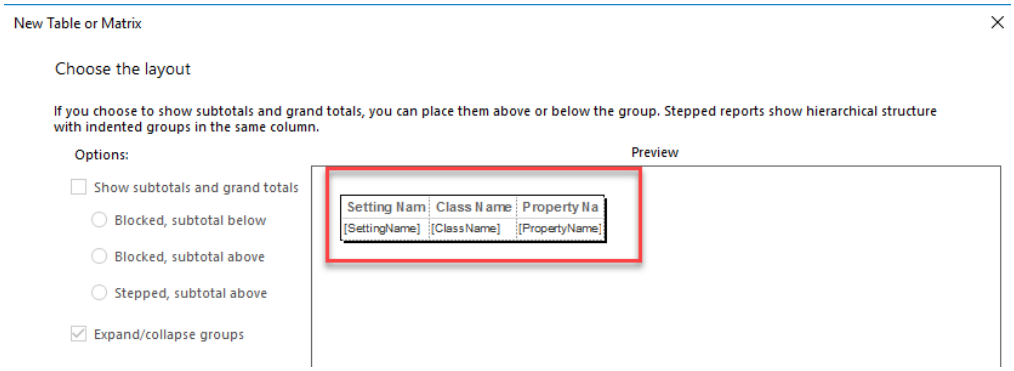
Source code can be imported if you lack one.

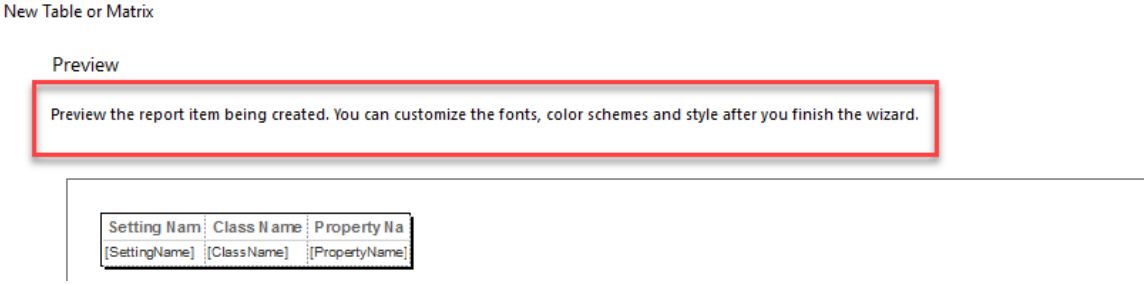




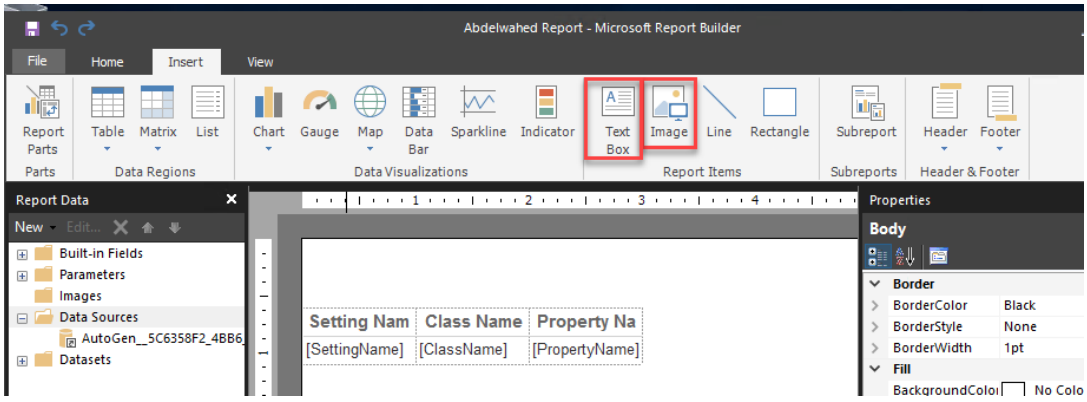

New Table or Matrix
Design a query
Build a query to specify the data you want from the data source.
Edit as Text
Import...
Command type:
Text
(select cir.SettingName,irc.ClassName,irc.PropertyName
from fn_rbac_custominventoryreport(@UserSIDs) cir inner join fn_rbac_InventoryReportClass
SettingName
ClassName
PropertyName
Help
< Back
Next >
Cancel

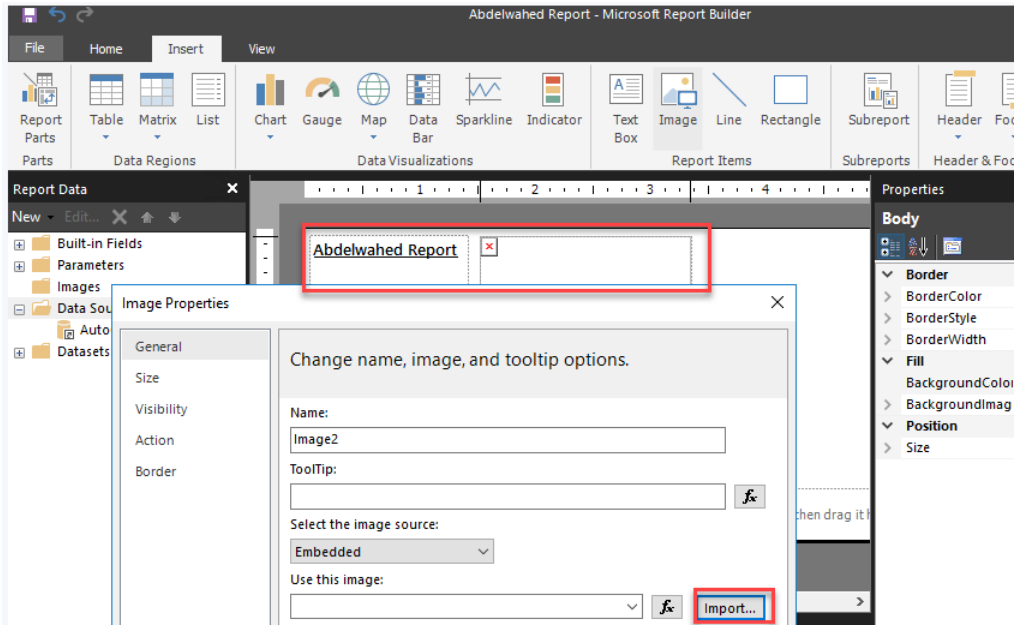

New Table or Matrix
Arrange fields
Arrange fields to group data in rows, columns, or both, and choose values to display. Data expands across the page in column groups and down the page in row groups. Use functions such as Sum, Avg, and Count on the fields in the Values box.
Available fields
SettingName
ClassName
PropertyName
Column groups
Row groups
Values
SettingName
ClassName
PropertyName
Help
< Back
Next >
Cancel

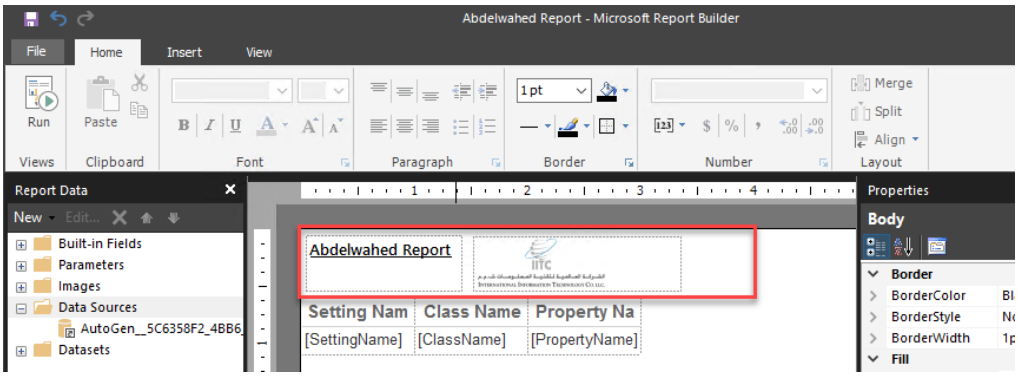


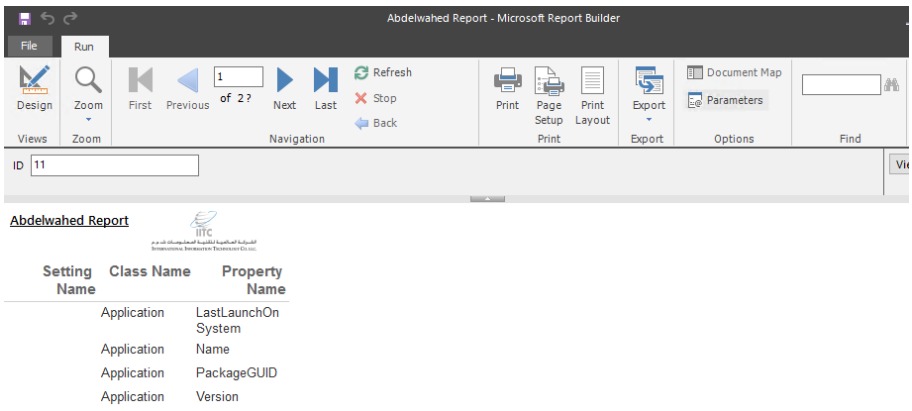


Add photo and text

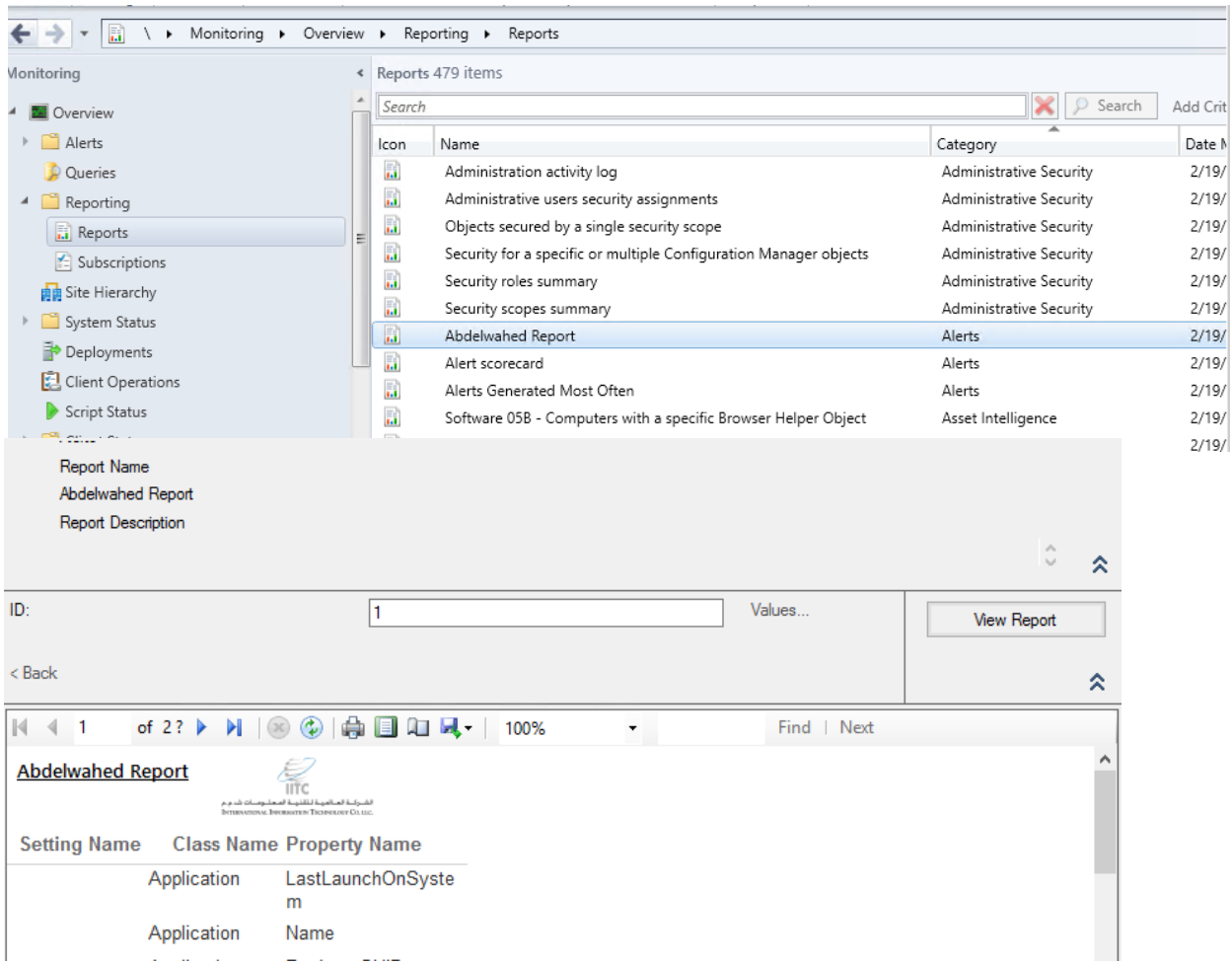



Abdelwahed Report - Microsoft Report Builder
File
Home
Insert
View
Report Parts
Table
Matrix
List
Chart
Gauge
Map
Data Bar
Sparkline
Indicator
Text Box
Image
Line
Rectangle
Subreport
Header
Parts
Data Regions
Data Visualizations
Report Items
Subreports
Header & Foo
Report Data
New
Edit...
Built-in Fields
Parameters
Images
Data Sou
Auto
Datasets
Abdelwahed Report
Image Properties
General
Size
Visibility
Action
Border
Change name, image, and tooltip options.
Name:
Image2
ToolTip:
Select the image source:
Embedded
Use this image:
Import...
Properties
Body
Border
BorderColor
BorderStyle
BorderWidth
Fill
BackgroundColor
BackgroundImag
Position
Size


Abdelwahed Report - Microsoft Report Builder
File
Home
Insert
View
Run
Paste
Views
Clipboard
Font
Paragraph
Border
Number
Merge
Split
Align
Layout
Report Data
New
Edit...
Built-in Fields
Parameters
Images
Data Sources
AutoGen__5C6358F2_4BB6
Datasets
Abdelwahed Report
Setting Nam
Class Name
Property Na
[SettingName]
[ClassName]
[PropertyName]
Properties
Body
Border
BorderColor
BorderStyle
BorderWidth
Fill


Abdelwahed Report - Microsoft Report Builder
File
Run
Design
Zoom
First
Previous
1
of 2?
Next
Last
Refresh
Stop
Back
Print
Page Setup
Print Layout
Export
Document Map
Parameters
Views
Zoom
Navigation
Print
Export
Options
Find
ID
11
Abdelwahed Report
Setting Name
Class Name
Property Name
Application
LastLaunchOn System
Application
Name
Application
PackageGUID
Application
Version

Please navigate to the reports section and locate the Abdelwahed report that was recently created.



Software metering

Software metering is a feature in System Center Configuration Manager (SCCM) that tracks and reports on software usage within an organization. This provides insights into which software is being used, by whom, and how often.

Enabling Software Metering

To enable software metering in SCCM, follow these steps:

1. **Open the SCCM Console**:
   - Launch the SCCM console from your system.
2. **Navigate to Client Settings**:
   - Go to Administration -> Client Settings.
3. **Select or Create Client Settings**:
   - Select the default client settings or create a new set of client settings.
4. **Enable Software Metering**:
   - Click on the Software Metering tab.
   - Select the checkbox to enable software metering.
5. **Configure Software Metering Settings**:
   - Adjust the settings as needed to meet your organizational requirements.
6. **Deploy Client Settings**:
   - Deploy the configured client settings to the required devices.

Generating Software Metering Reports

After enabling software metering and allowing it to run for a while, you can generate reports to view the usage data. However, sometimes the report may show blank data. Here are steps to troubleshoot this issue:

1. **Verify Software Metering Client Installation**:
   - Ensure that the software metering client is installed and running on the devices in question.
   - Check the SCCM client logs (located in C:\Windows\CCM\Logs) to confirm that software metering is functioning correctly.
2. **Check Software Metering Rules Configuration**:
   - Verify that software metering rules are configured correctly.
   - Ensure that the rules are set to track the correct software and are applied to the appropriate devices.
3. **Ensure Data Collection and Storage**:
   - Confirm that software metering data is being collected and stored in the SCCM database.
   - Check the relevant SCCM log files (mtrmgr.log and swmproc.log) for any errors related to data collection or storage.
4. **Verify Reporting Services Configuration**:
   - Ensure that SCCM reporting services are running and configured correctly.
   - Check that reporting services have the necessary permissions to access the SCCM database.
5. **Re-run the Report**:
   - Wait a few days and then run the report again to see if any data has been collected since the last report.

Example Scenario: Troubleshooting Blank Software Metering Reports

Scenario: You've enabled software metering, but the generated report shows no data.

Steps to Resolve:

1. **Check Software Metering Client**:
   - Open the mtrmgr.log on the client device.
   - Ensure there are no errors and that the client is reporting usage data.
2. **Review Software Metering Rules**:
   - Go to Monitoring -> Software Metering -> Rules.
   - Verify that rules are correctly set up to track the desired software.
3. **Check Data Collection**:
   - On the SCCM server, open the swmproc.log file.
   - Ensure there are no errors indicating issues with processing metering data.
4. **Verify Reporting Services**:
   - Go to Monitoring -> Reporting -> Reports.
   - Ensure that the SSRS instance is running and configured properly.
5. **Wait and Re-run the Report**:
   - Give it some time for the data to be collected.
   - Run the report again after a few days to check for collected data.

Using RunMetersumm to Summarize Software Metering Data in SCCM

The RunMetersumm tool in SCCM (System Center Configuration Manager) is used to aggregate and summarize software metering data, creating summary reports that provide insights into software usage patterns and trends. Below are the detailed steps on how to use RunMetersumm:

Steps to Run Meter Summarization Tool

1. **Open Command Prompt**:
   - Open the Command Prompt on the server where SCCM is installed.
2. **Navigate to the SCCM bin Directory**:
   - Navigate to the bin folder in the SCCM installation directory. The default location is:

```
cd C:\Program Files (x86)\Microsoft Configuration Manager\bin
```

3. **Run the RunMetersumm Command**:
   - Use the following command to summarize the software metering data:

```
RunMetersumm.exe /d:yyyy-mm-dd [/m:hh] [/s] [/f:filename]
```

Command Parameters

- `/d` : Specifies the date for which you want to summarize the data. Enter the date in the "yyyy-mm-dd" format.
- `/m` : (Optional) Specifies the time of day for which you want to summarize the data. Enter the time in the "hh" format.
- `/s`: (Optional) Specifies that you want to summarize the data for all metered software, not just the top 100.
- `/f` : (Optional) Specifies the filename for the output report. If not specified, the report will be saved to the "Metersumm.rpt" file in the SCCM installation directory.

Example Command

To summarize software metering data for January 1, 2024, including all metered software and save the report as January2024Summary.rpt, you would run:

```
RunMetersumm.exe /d:2024-01-01 /s /f:January2024Summary.rpt
```

Wait for Summarization to Complete

- Wait for the tool to finish summarizing the software metering data. This may take several minutes, depending on the size of your SCCM environment and the amount of software metering data.

View the Output Report

- Once the tool has finished summarizing the data, you can open the output report to view the software usage patterns and trends. The report will be located in the specified directory or default location if no filename was provided.

Example Scenario

Scenario: You want to summarize software metering data for all software used on April 30, 2024, and save the report as April2024Summary.rpt.

Steps:

1. Open Command Prompt as an administrator on the SCCM server.
2. Navigate to the bin directory:

bash

Copy code

cd C:\Program Files (x86)\Microsoft Configuration Manager\bin

3. Run the summarization command:

```
RunMetersumm.exe /d:2024-04-30 /s /f:April2024Summary.rpt
```

4. Wait for the summarization process to complete.
5. Open April2024Summary.rpt from the SCCM installation directory to review the summarized software usage data.

Distributing and Managing Content in SCCM

Distributing and managing content for deployments in System Center Configuration Manager (SCCM) involves several steps, ensuring that the necessary files and programs reach the client computers effectively. Here's an overview of the key steps and content types involved:

Common Content Types in SCCM

1. **Packages**:
   - Collection of files and programs for distribution (software, scripts, etc.).
2. **Applications**:
   - Advanced deployment options with user device affinity, dependencies, and detection methods.
3. **Operating System Images**:
   - Files and settings to deploy an OS, often used in task sequences for automation.
4. **Driver Packages**:
   - Drivers necessary for client computers to function properly.
5. **Software Update Packages**:
   - Collections of software updates for maintaining up-to-date security patches and updates.

Steps for Distributing and Managing Content

1. Create Content

- **Packages and Programs**:
  - Use the Create Package and Program Wizard in SCCM.
  - Navigate to Software Library -> Overview -> Application Management -> Packages.
  - Specify settings like the source folder, distribution points, and requirements.
- **Task Sequences**:
  - Use the Create Task Sequence Wizard.
  - Navigate to Software Library -> Overview -> Operating Systems -> Task Sequences.

2. Create Distribution Points

- **Steps**:
  - Navigate to Administration -> Overview -> Site Configuration -> Servers and Site System Roles.
  - Select the server, right-click, and choose Add Site System Roles.
  - Follow the wizard to select the distribution point role and configure settings.

3. Distribute Content

- **Steps**:
  - Navigate to Software Library -> Overview -> Application Management -> Packages.
  - Select the desired package, right-click, and choose Distribute Content.
  - Follow the wizard to select the distribution points.

4. Monitor Content Distribution

- **Steps**:

- Navigate to Monitoring -> Overview -> Distribution Status -> Content Status.
- Review the distribution status and address any issues.

5. Manage Content

- **Steps**:
  - Navigate to Software Library -> Overview -> Application Management -> Packages.
  - Select the package, right-click, and choose Manage Distribution Points.
  - Update or remove distribution points as needed.

6. Configure Content Replication

- **Steps**:
  - Navigate to Administration -> Overview -> Site Configuration -> Sites.
  - Right-click on the site and choose Configure Site Components -> Software Distribution.
  - Configure replication settings, such as transfer rates and schedules.

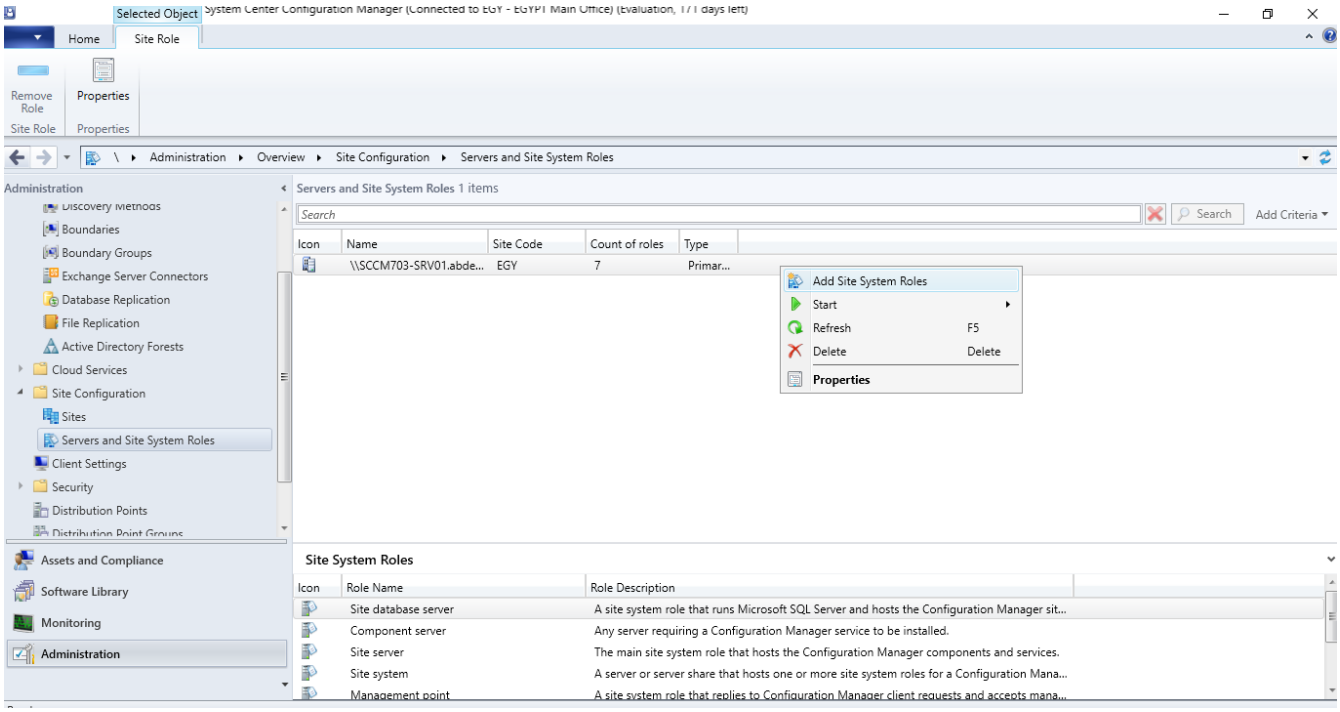
7. Manage Bandwidth

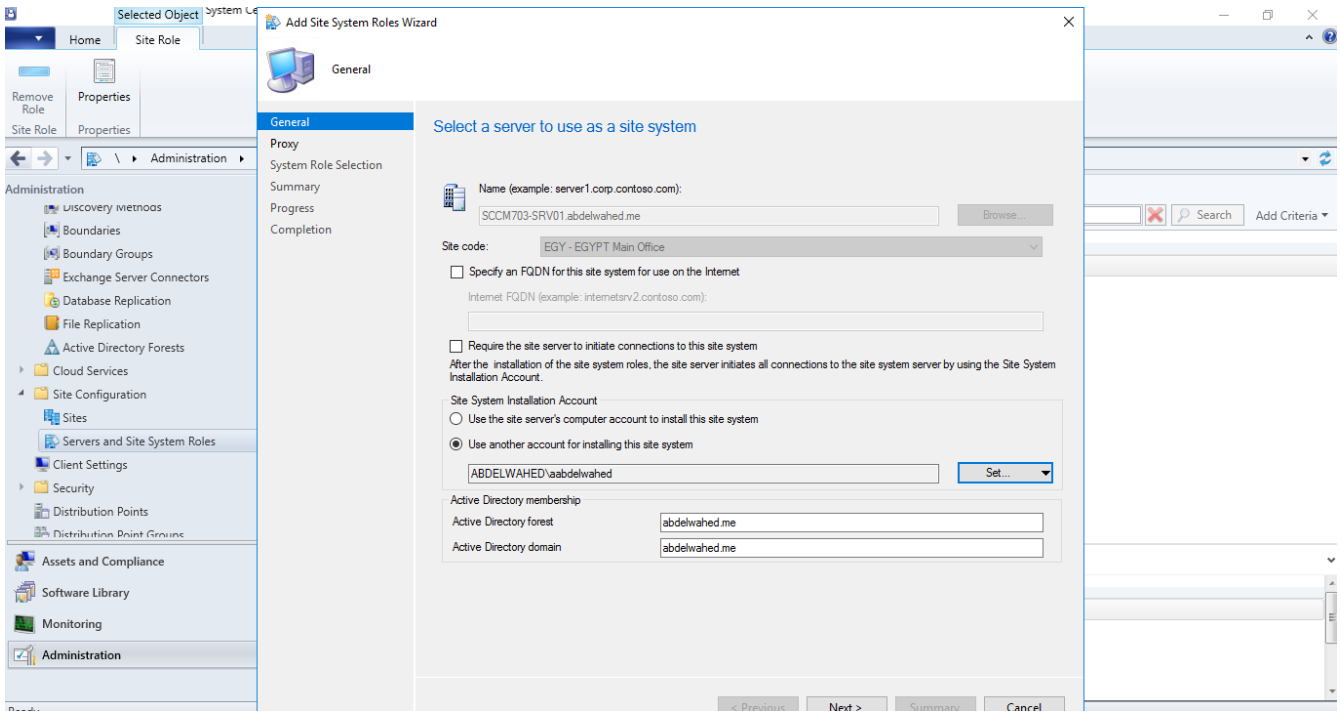
- **Steps**:
  - Navigate to Administration -> Overview -> Site Configuration -> Sites.
  - Right-click on the site and choose Configure Site Components -> Software Distribution.
  - Enable BITS throttling or configure distribution points to manage bandwidth effectively.

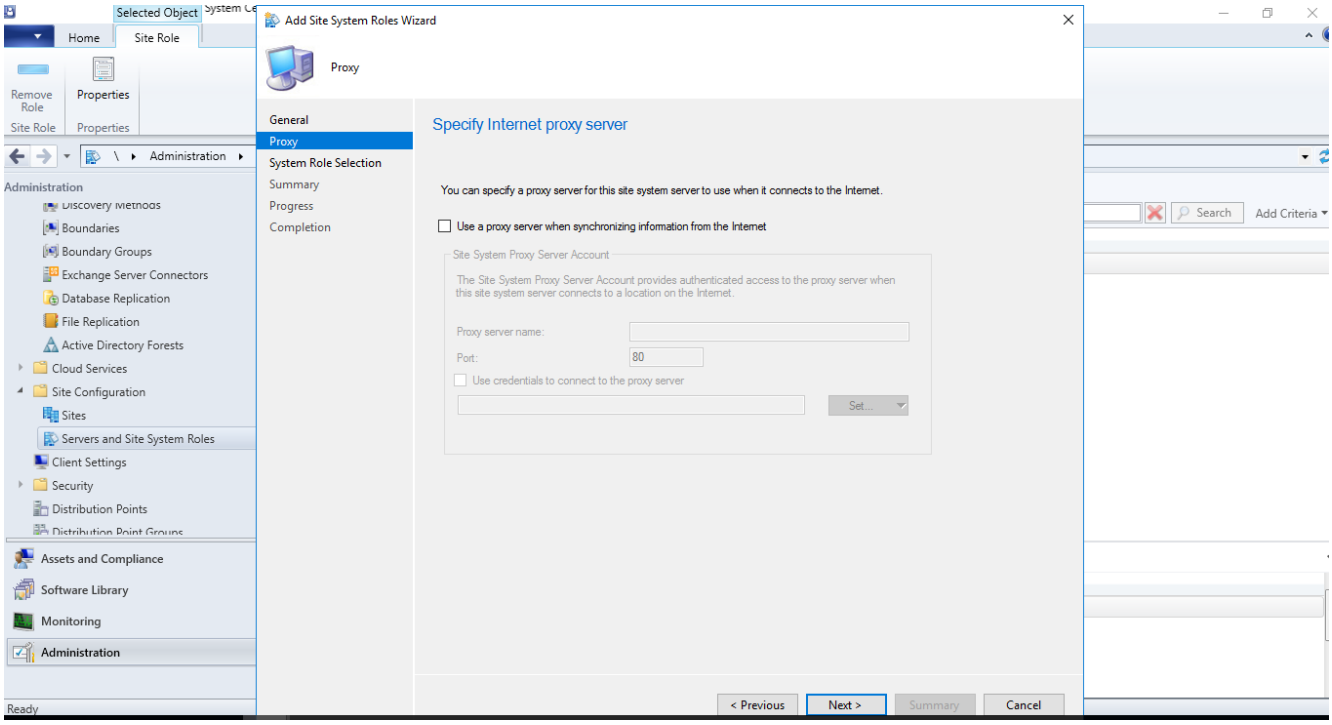
Example Scenario: Distributing an Application

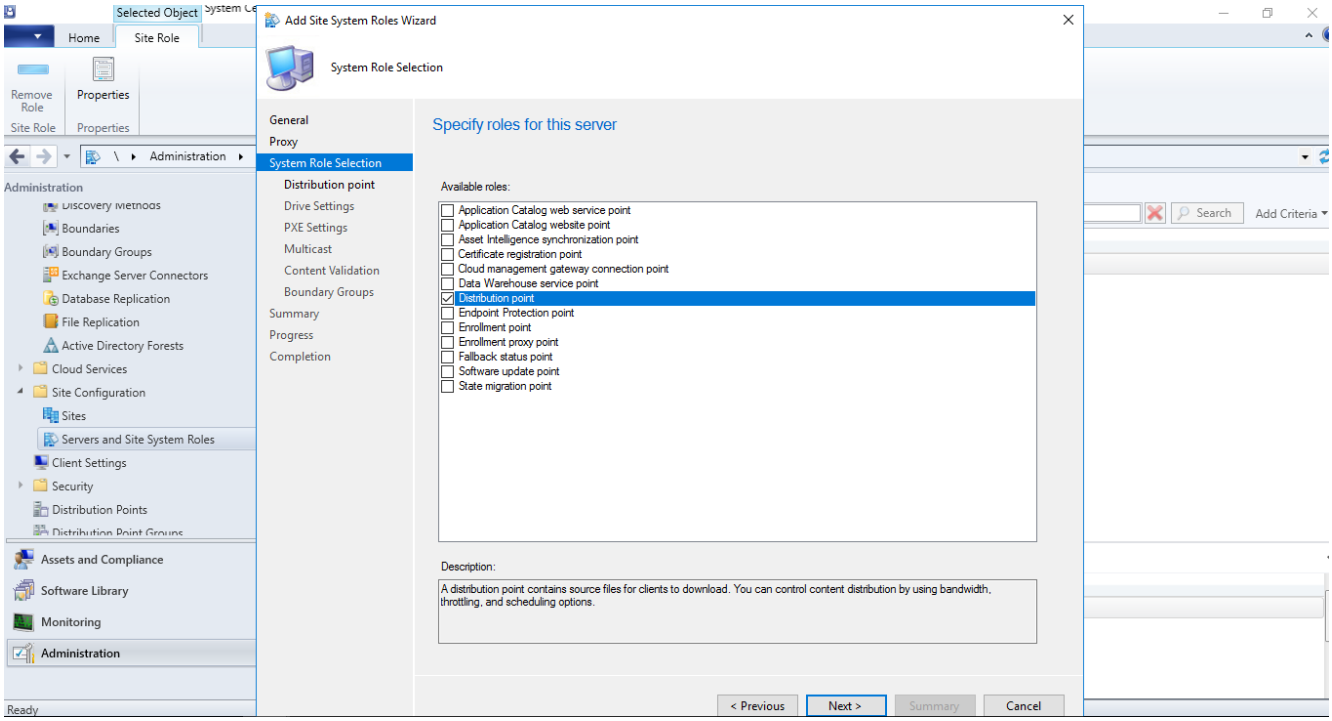
1. **Create an Application**:
   - Navigate to Software Library -> Overview -> Application Management -> Applications.
   - Use the Create Application Wizard to specify the application's source files, detection methods, and deployment types.
2. **Distribute the Application**:
   - Select the application, right-click, and choose Distribute Content.
   - Follow the wizard to choose the appropriate distribution points.
3. **Monitor the Distribution**:
   - Navigate to Monitoring -> Overview -> Distribution Status -> Content Status.
   - Check the status of the application distribution and resolve any issues.
4. **Manage Distribution Points**:
   - If needed, update or remove distribution points by selecting the application and choosing Manage Distribution Points.

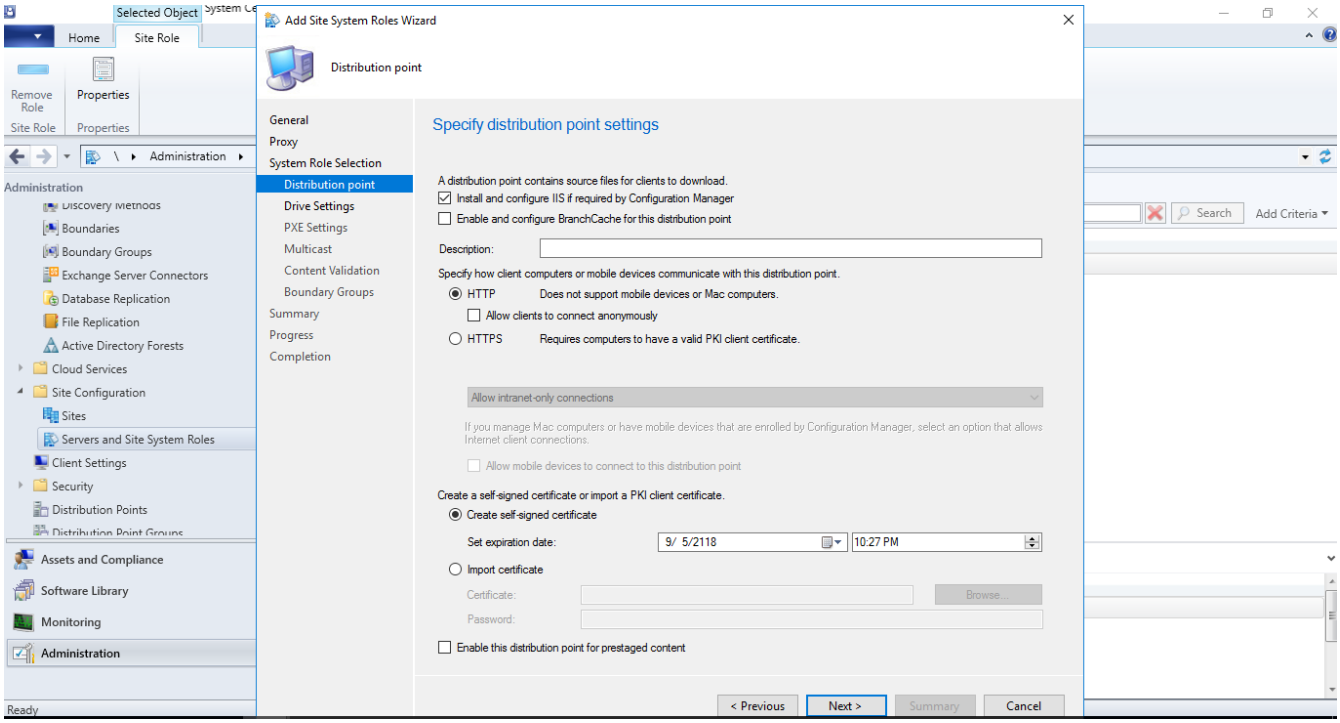
Add DP Site Role

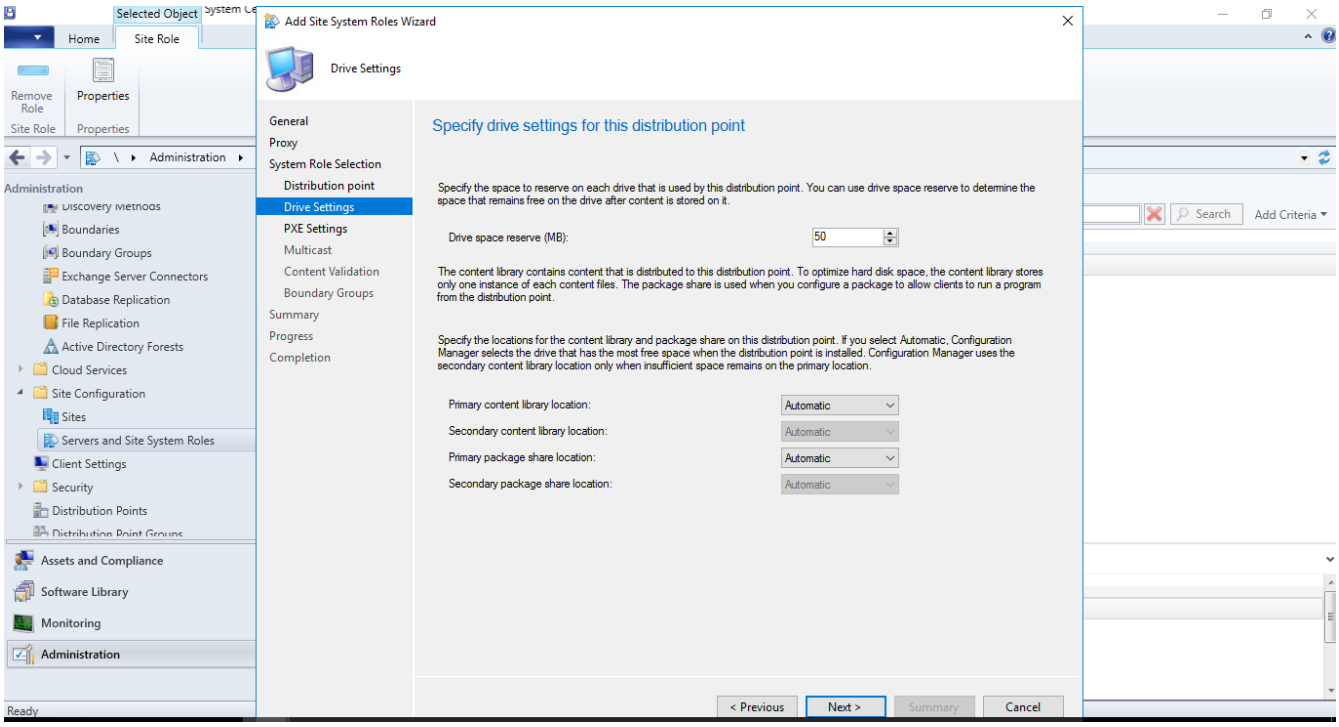





Add Site System Roles Wizard
Proxy
General
Proxy
System Role Selection
Summary
Progress
Completion
Specify Internet proxy server
You can specify a proxy server for this site system server to use when it connects to the Internet.
Use a proxy server when synchronizing information from the Internet
Site System Proxy Server Account
The Site System Proxy Server Account provides authenticated access to the proxy server when this site system server connects to a location on the Internet.
Proxy server name:
Port:
80
Use credentials to connect to the proxy server
Set...
< Previous
Next >
Summary
Cancel
Selected Object
Home
Site Role
Remove Role
Properties
Site Role
Properties
Administration
Boundaries
Boundary Groups
Exchange Server Connectors
Database Replication
File Replication
Active Directory Forests
Cloud Services
Site Configuration
Sites
Servers and Site System Roles
Client Settings
Security
Distribution Points
Assets and Compliance
Software Library
Monitoring
Administration
Search
Add Criteria
Ready


Add Site System Roles Wizard
System Role Selection
General
Proxy
System Role Selection
Distribution point
Drive Settings
PXE Settings
Multicast
Content Validation
Boundary Groups
Summary
Progress
Completion
Specify roles for this server
Available roles:
Application Catalog web service point
Application Catalog website point
Asset Intelligence synchronization point
Certificate registration point
Cloud management gateway connection point
Data Warehouse service point
Distribution point
Endpoint Protection point
Enrollment point
Enrollment proxy point
Fallback status point
Software update point
State migration point
Description:
A distribution point contains source files for clients to download. You can control content distribution by using bandwidth, throttling, and scheduling options.
< Previous
Next >
Summary
Cancel
Selected Object
Home
Site Role
Remove Role
Properties
Site Role
Properties
Administration
Boundaries
Boundary Groups
Exchange Server Connectors
Database Replication
File Replication
Active Directory Forests
Cloud Services
Site Configuration
Sites
Servers and Site System Roles
Client Settings
Security
Distribution Points
Assets and Compliance
Software Library
Monitoring
Administration
Search
Add Criteria
Ready

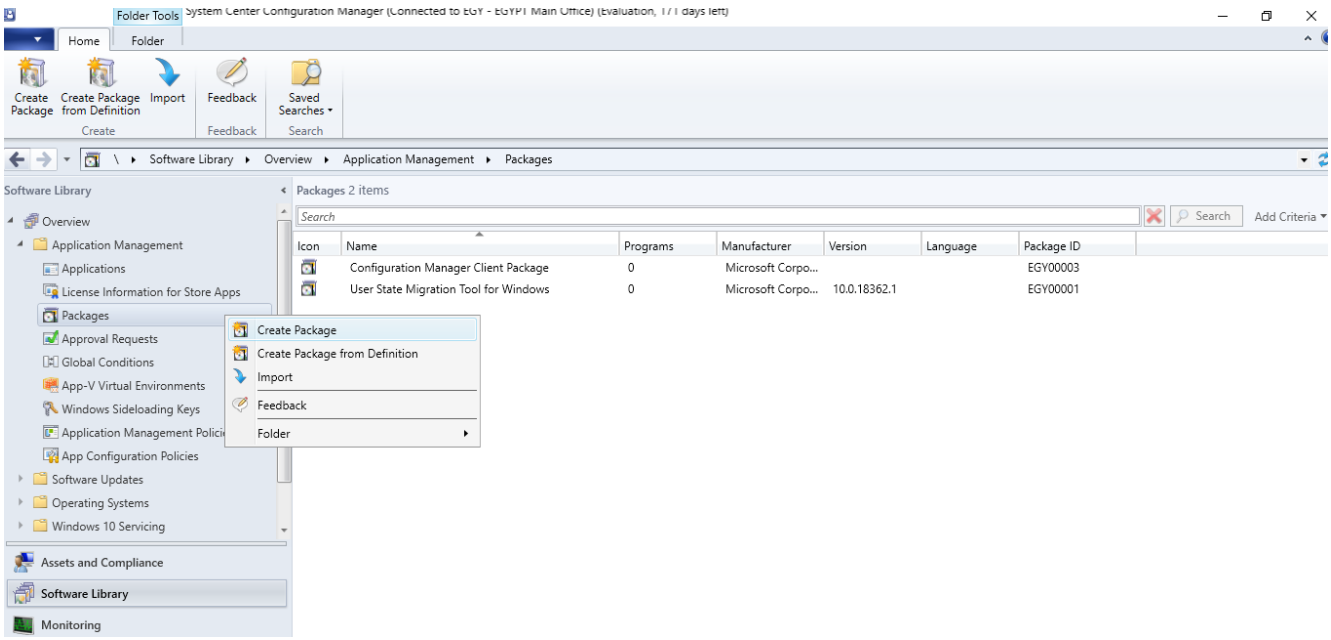

Add Site System Roles Wizard
Distribution point
General
Proxy
System Role Selection
Distribution point
Drive Settings
PXE Settings
Multicast
Content Validation
Boundary Groups
Summary
Progress
Completion
Specify distribution point settings
A distribution point contains source files for clients to download.
Install and configure IIS if required by Configuration Manager
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:
9/ 5/2118
10:27 PM
Import certificate
Certificate:
Browse...
Password:
Enable this distribution point for prestaged content
< Previous
Next >
Summary
Cancel


Add Site System Roles Wizard
Drive Settings
General
Proxy
System Role Selection
Distribution point
Drive Settings
PXE Settings
Multicast
Content Validation
Boundary Groups
Summary
Progress
Completion
Specify drive settings for this distribution point
Specify the space to reserve on each drive that is used by this distribution point. You can use drive space reserve to determine the space that remains free on the drive after content is stored on it.
Drive space reserve (MB):
50
The content library contains content that is distributed to this distribution point. To optimize hard disk space, the content library stores only one instance of each content files. The package share is used when you configure a package to allow clients to run a program from the distribution point.
Specify the locations for the content library and package share on this distribution point. If you select Automatic, Configuration Manager selects the drive that has the most free space when the distribution point is installed. Configuration Manager uses the secondary content library location only when insufficient space remains on the primary location.
Primary content library location:
Automatic
Secondary content library location:
Automatic
Primary package share location:
Automatic
Secondary package share location:
Automatic
< Previous
Next >
Summary
Cancel

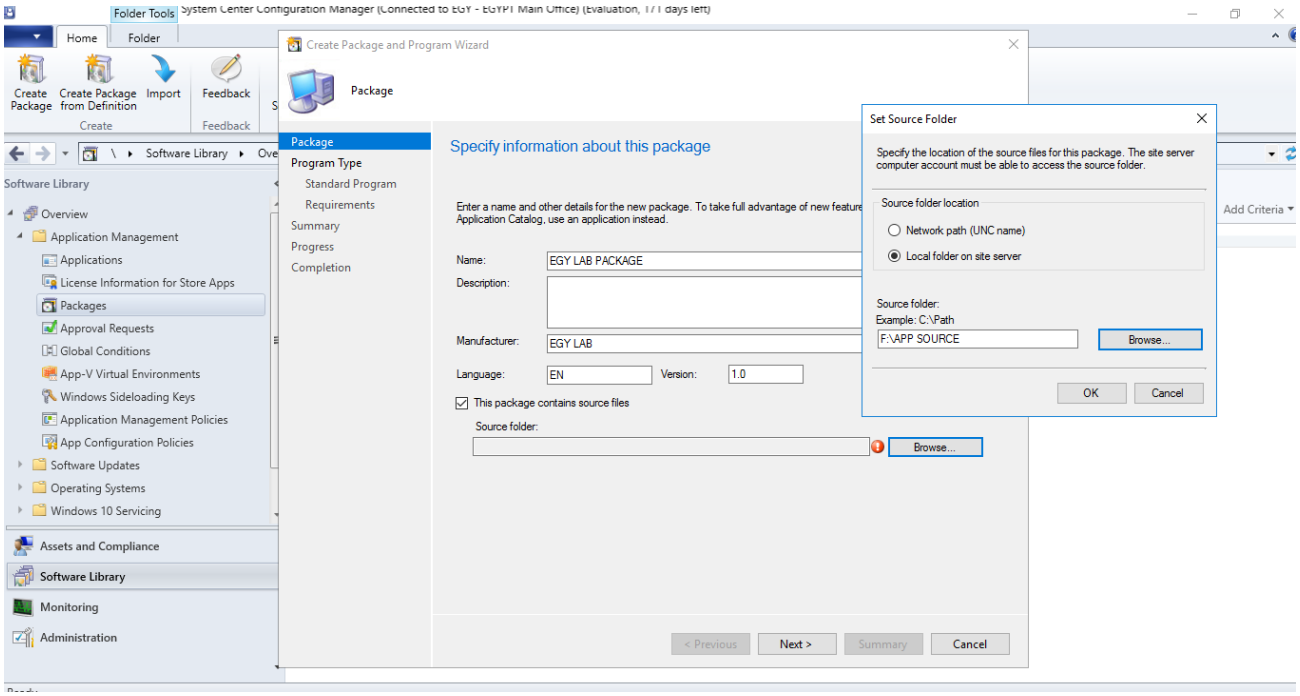
Install Software through CM

Create New Packages

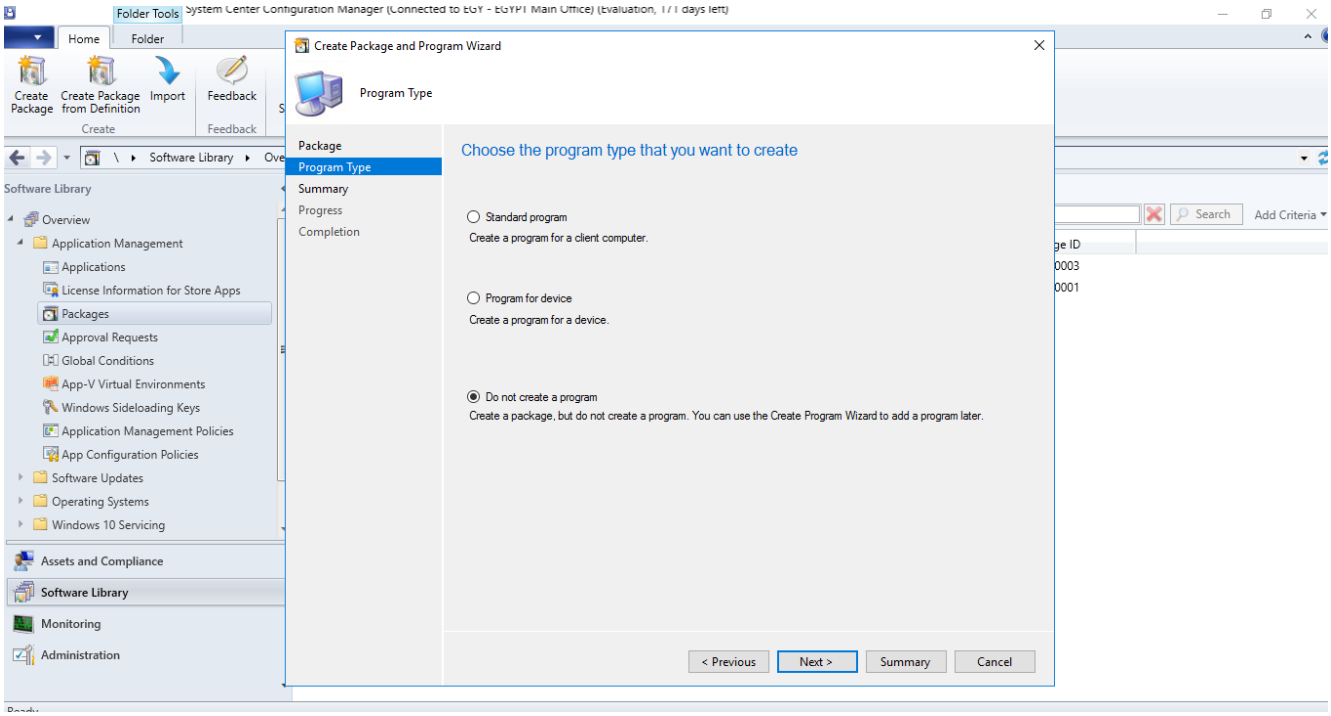
1- Add package and programs

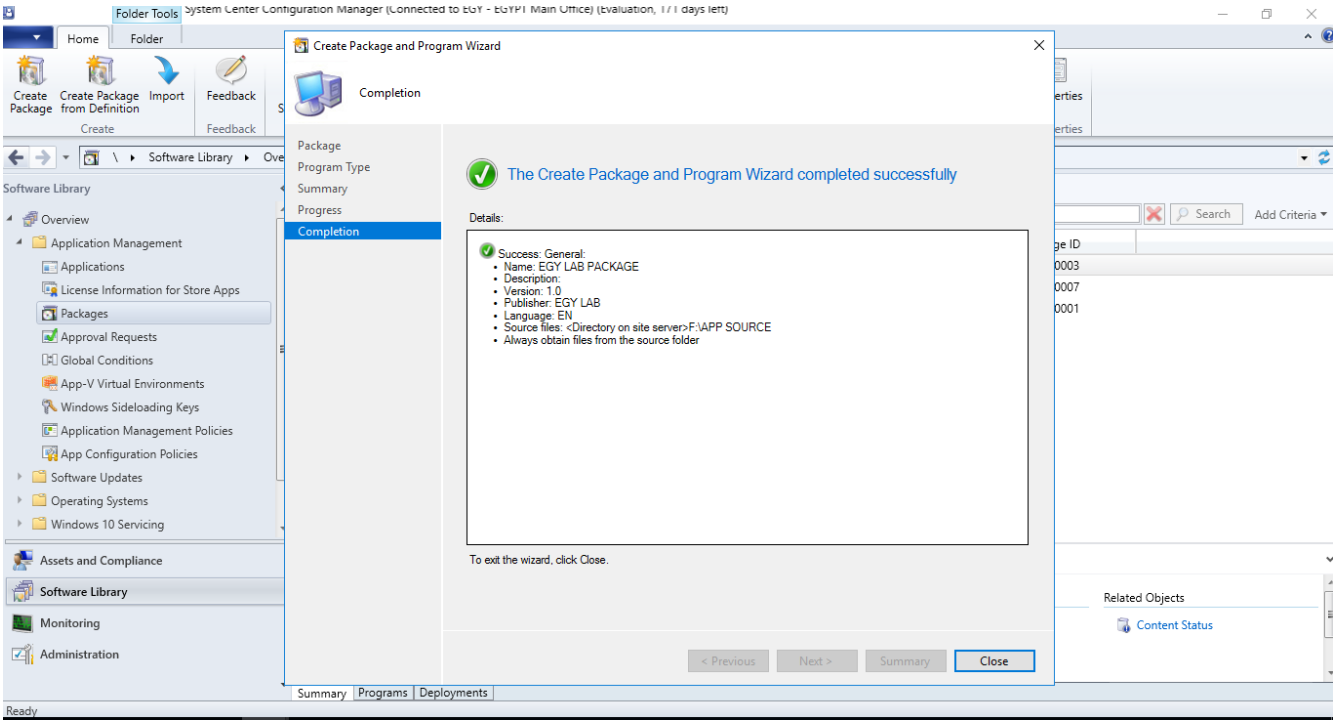


Include a source directory for packages, allowing the Configuration Manager to reference it when installing applications you intend to deploy.



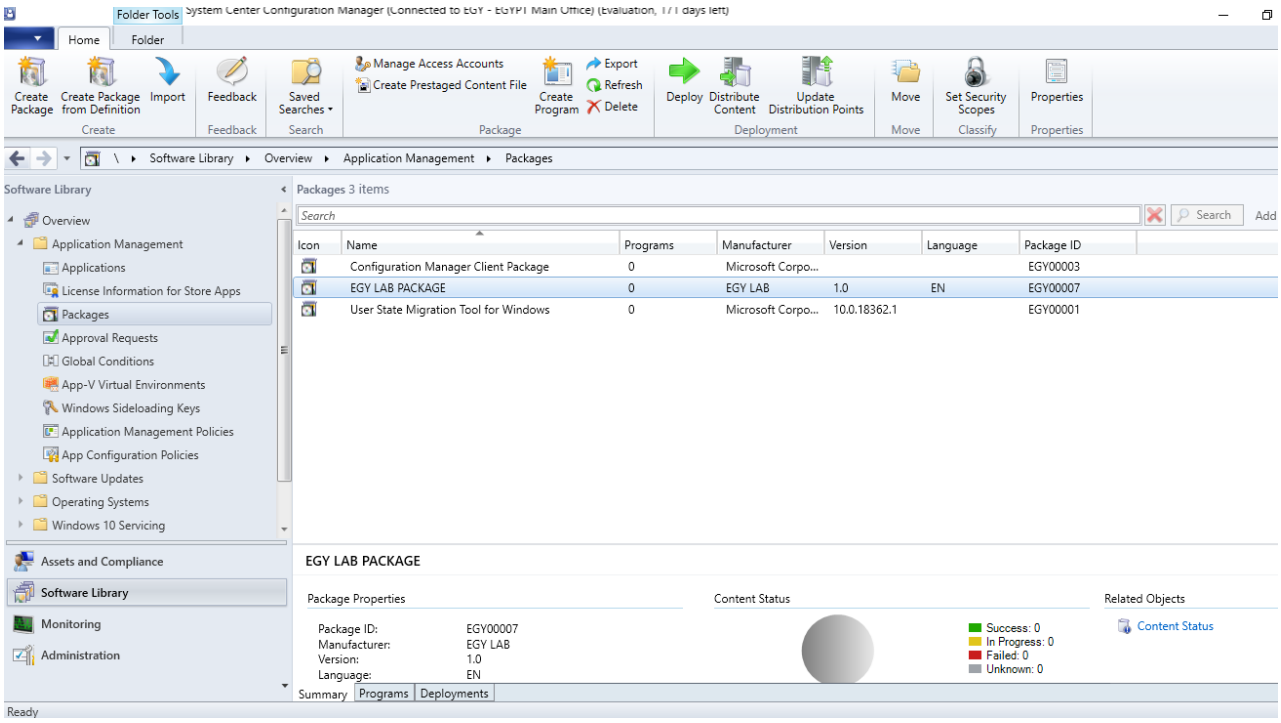
apps will be included in the future



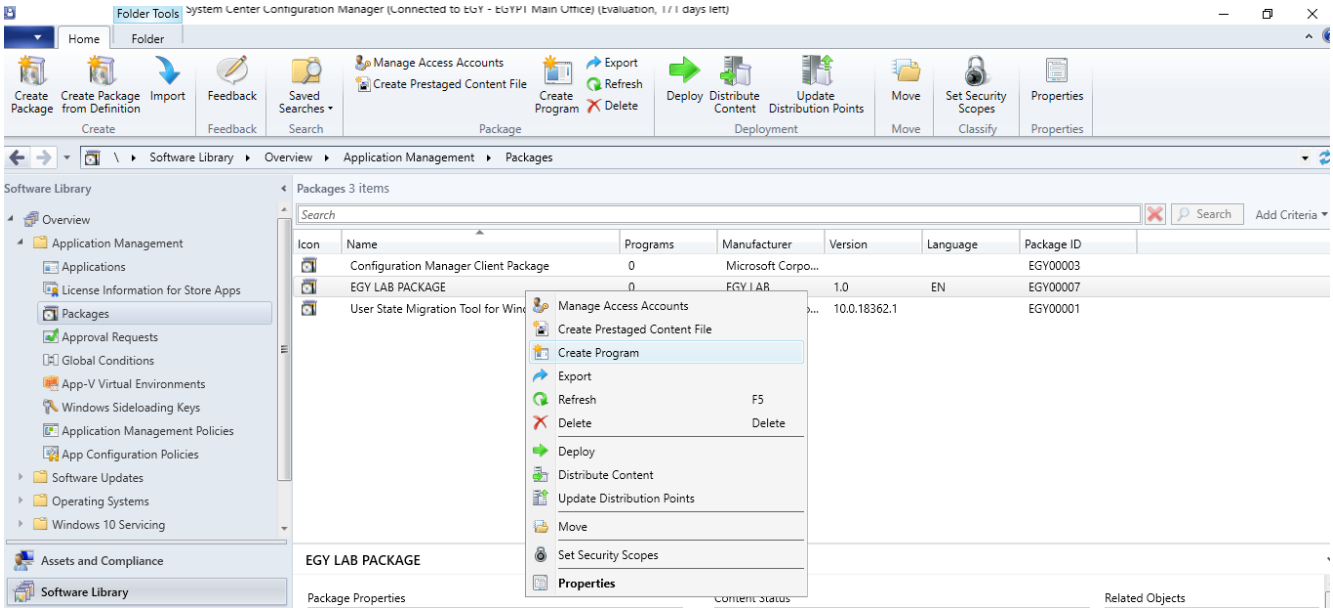


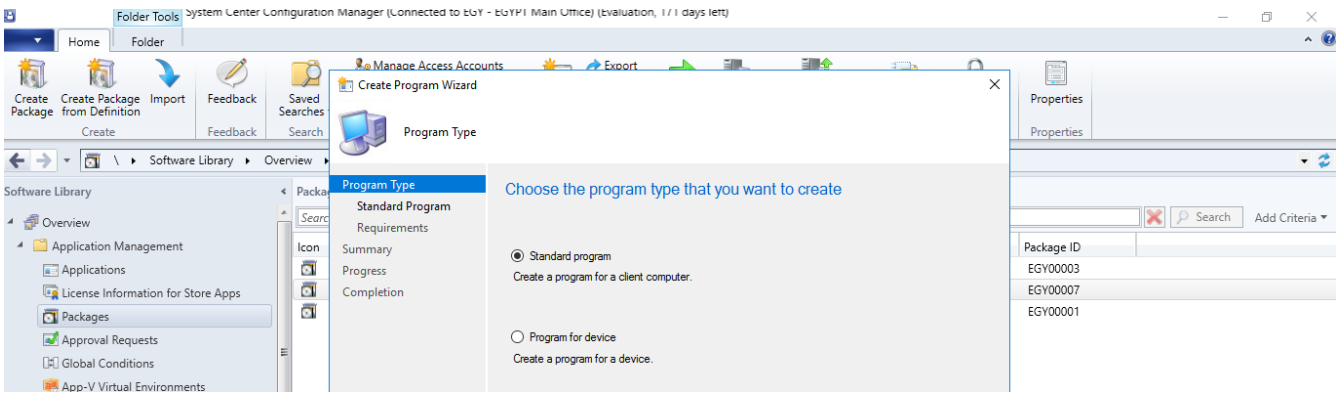
SCCM Quick Lab Guide

Within SCCM (System Center Configuration Manager), there appears to be a package that has no programs linked to it.

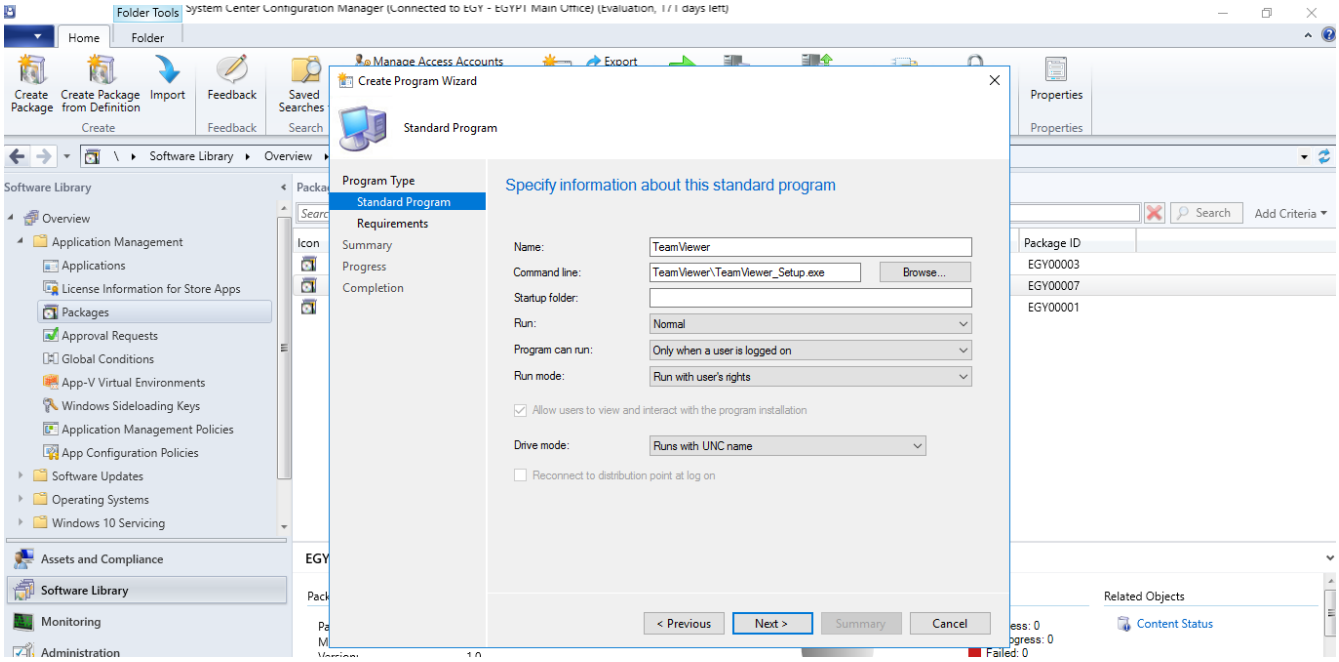


now add programs inside the package

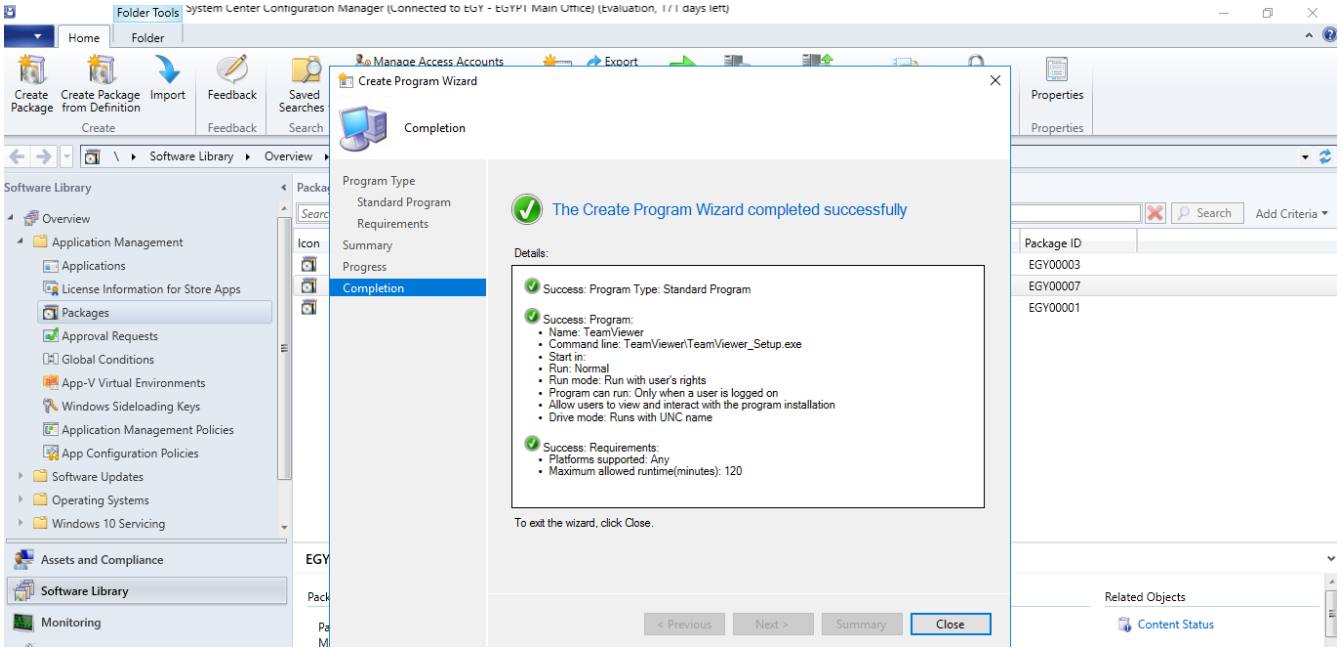


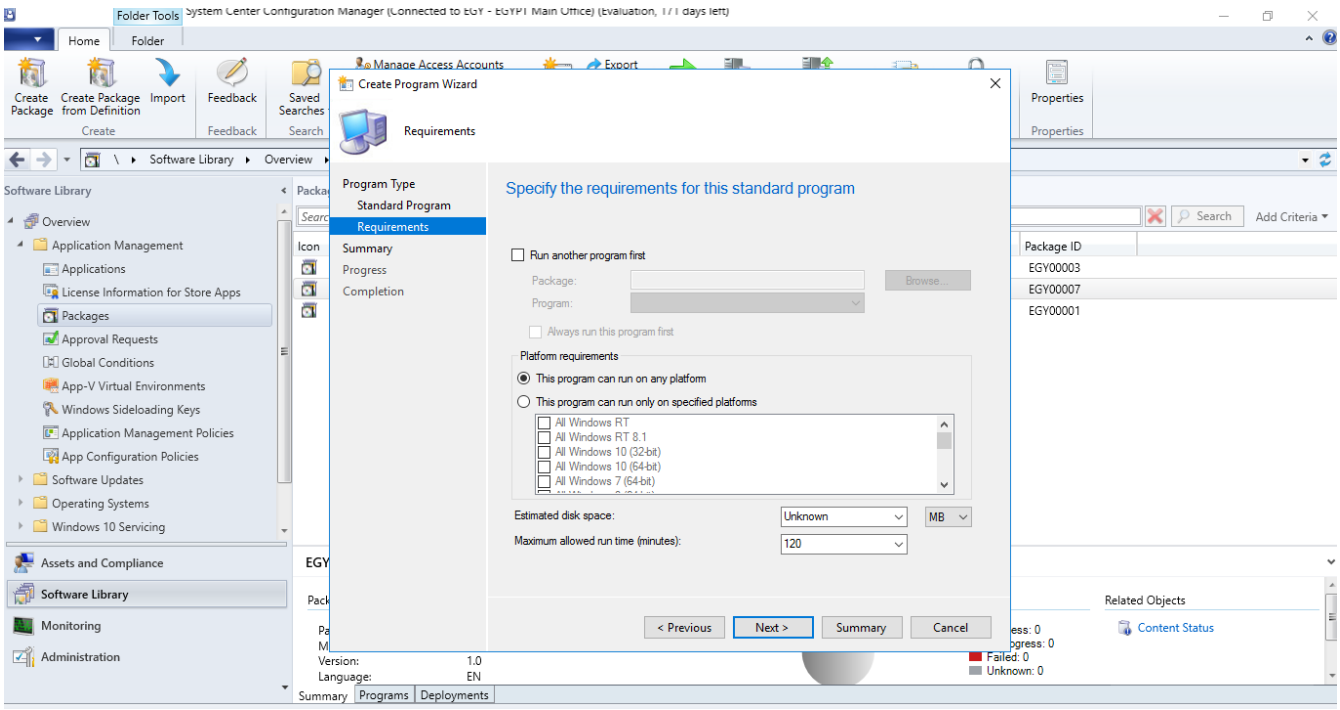


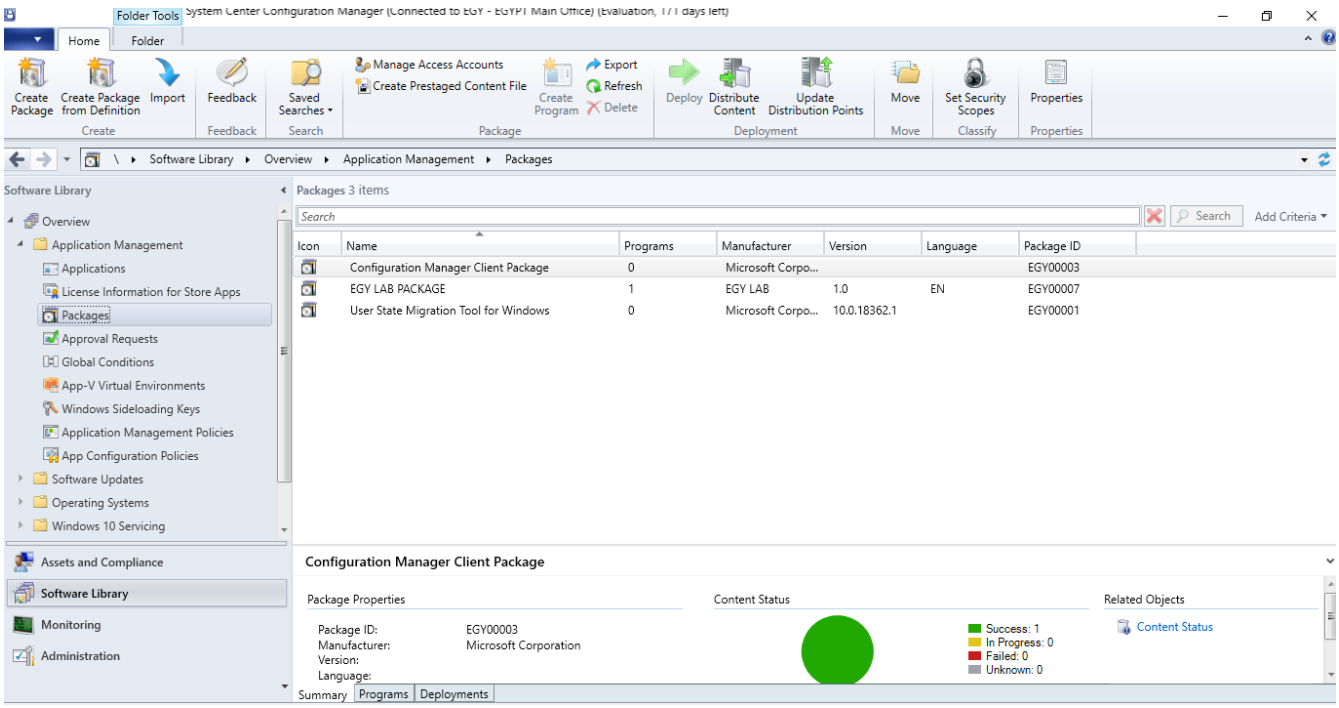
To install a software application on a particular device, like a smartphone, navigate through the package source in SCCM and copy the application's source files. Then set up the package so that standard users have the ability to install the applications by choosing the option "Run with user rights."



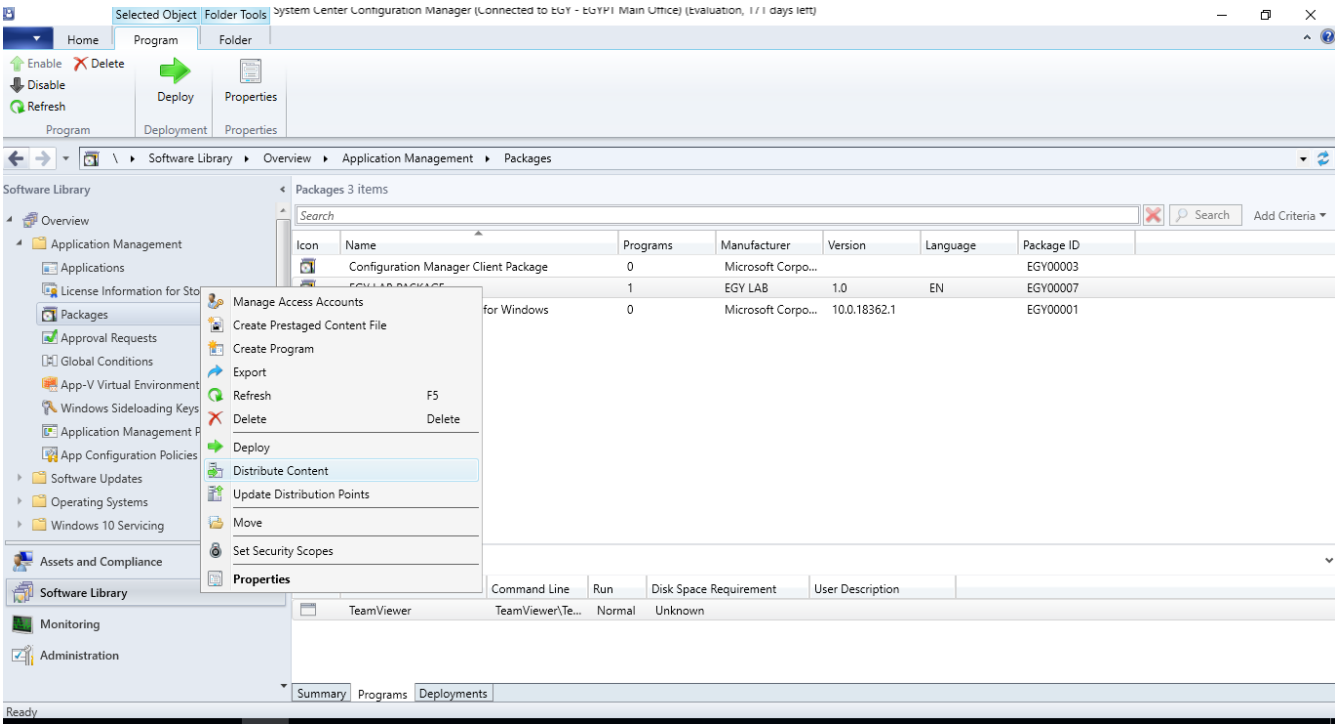
When your app requires other components installed prior to its own installation, you can choose these prerequisites in SCCM while setting up the program.

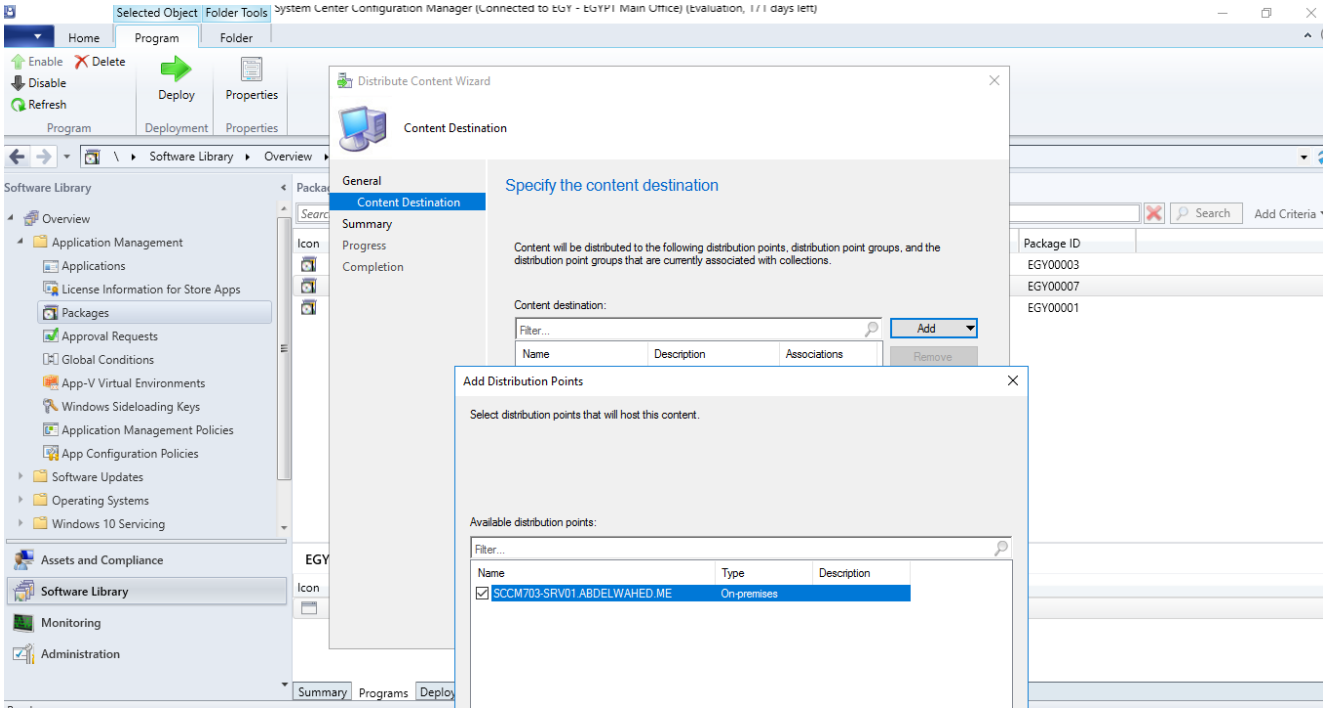

Create Program Wizard
Completion
Program Type
Standard Program
Requirements
Summary
Progress
Completion
The Create Program Wizard completed successfully
Details:
Success: Program Type: Standard Program
Success: Program:
Name: TeamViewer
Command line: TeamViewer\TeamViewer_Setup.exe
Start in:
Run: Normal
Run mode: Run with user's rights
Program can run: Only when a user is logged on
Allow users to view and interact with the program installation
Drive mode: Runs with UNC name
Success: Requirements:
Platforms supported: Any
Maximum allowed runtime(minutes): 120
To exit the wizard, click Close.
< Previous
Next >
Summary
Close

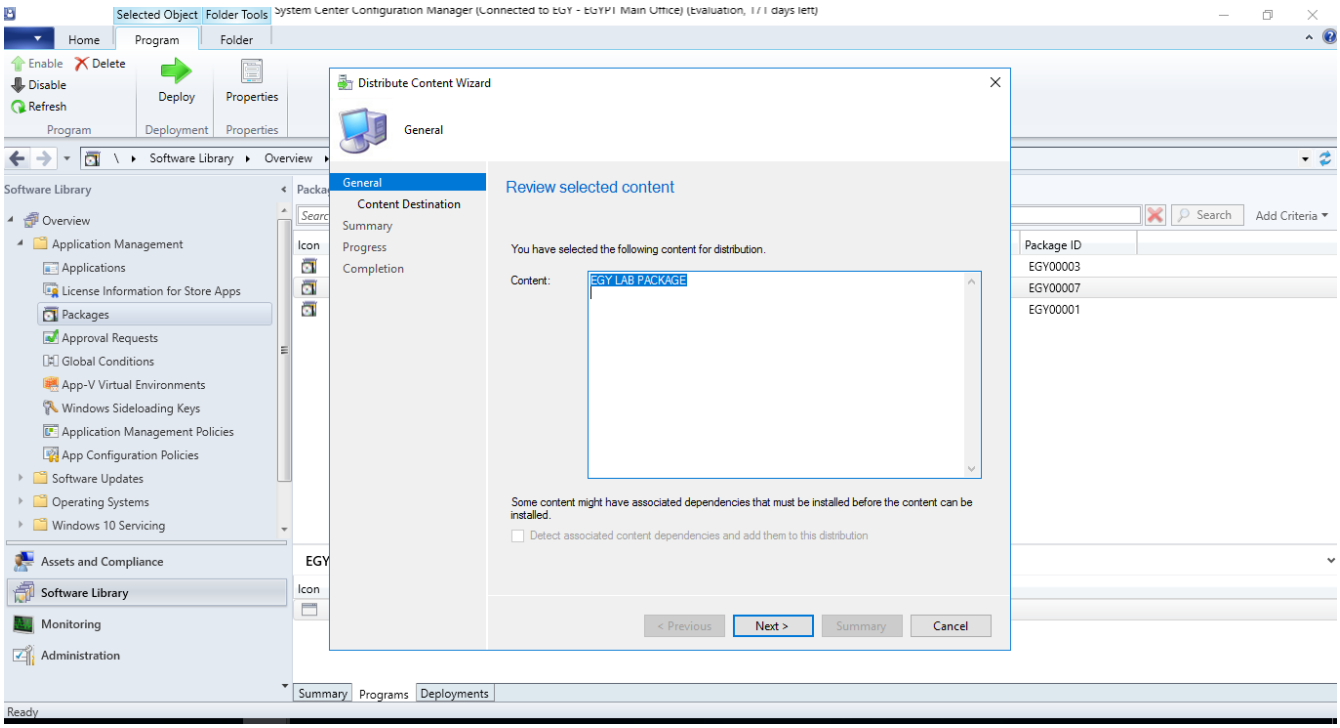

Create Program Wizard
Requirements
Program Type
Standard Program
Requirements
Summary
Progress
Completion
Specify the requirements for this standard program
Run another program first
Package:
Program:
Browse...
Always run this program first
Platform requirements
This program can run on any platform
This program can run only on specified platforms
All Windows RT
All Windows RT 8.1
All Windows 10 (32-bit)
All Windows 10 (64-bit)
All Windows 7 (64-bit)
Estimated disk space:
Unknown
MB
Maximum allowed run time (minutes):
120
< Previous
Next >
Summary
Cancel



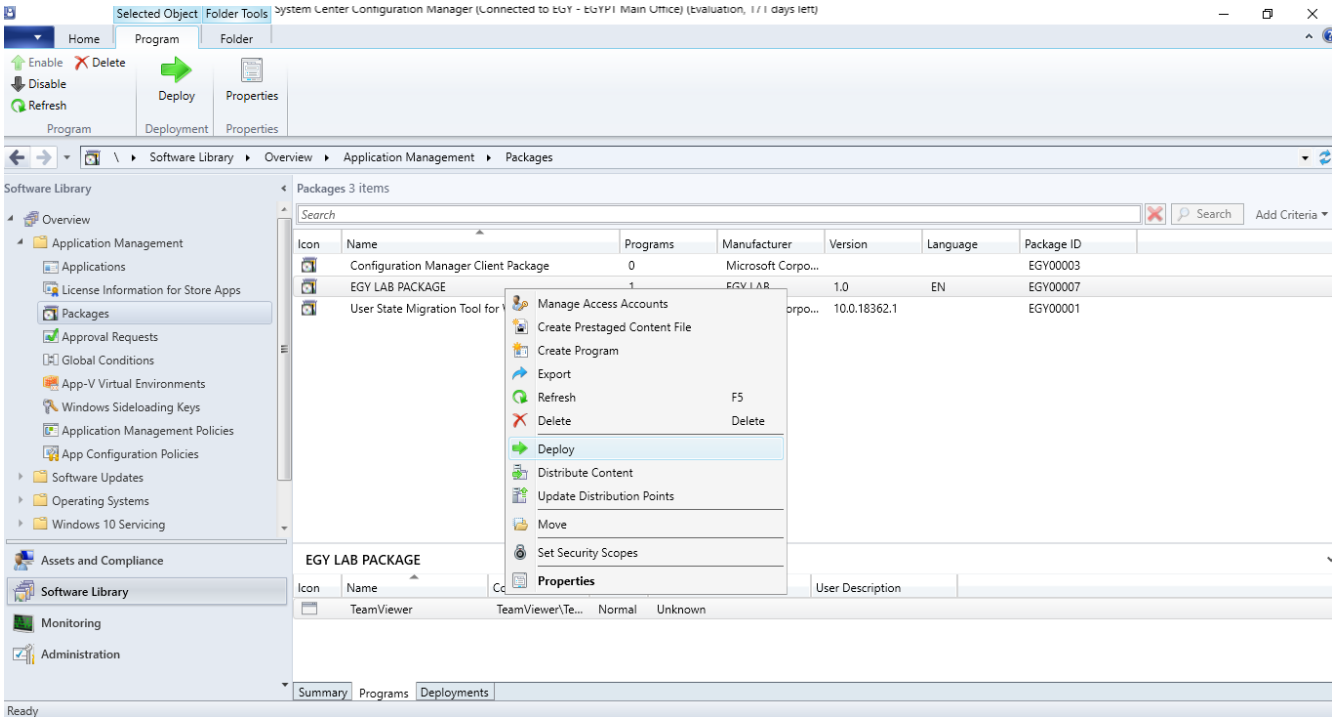
2- Distribute packages content in distribution point

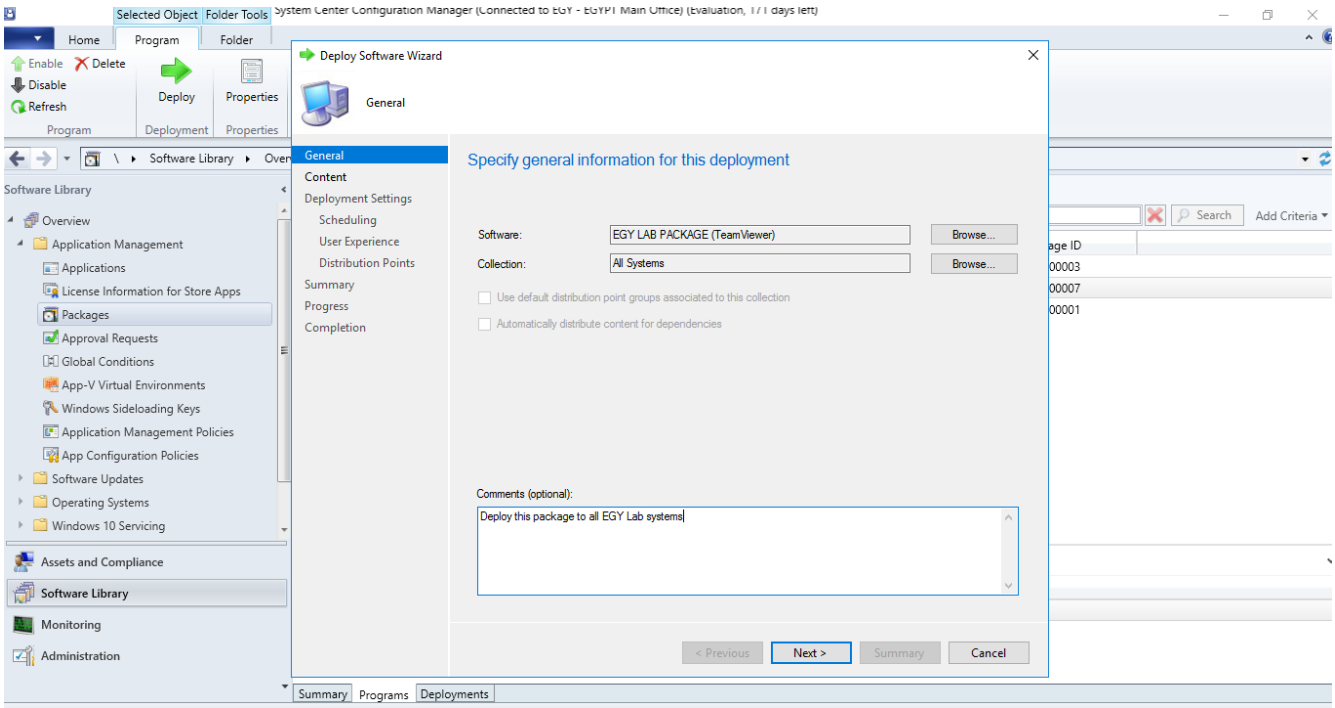



Distribute Content Wizard
Content Destination
Specify the content destination
Content will be distributed to the following distribution points, distribution point groups, and the distribution point groups that are currently associated with collections.
Content destination:
Add Distribution Points
Select distribution points that will host this content.
Available distribution points:
SCCM703-SRV01.ABDELWAHED.ME
On-premises

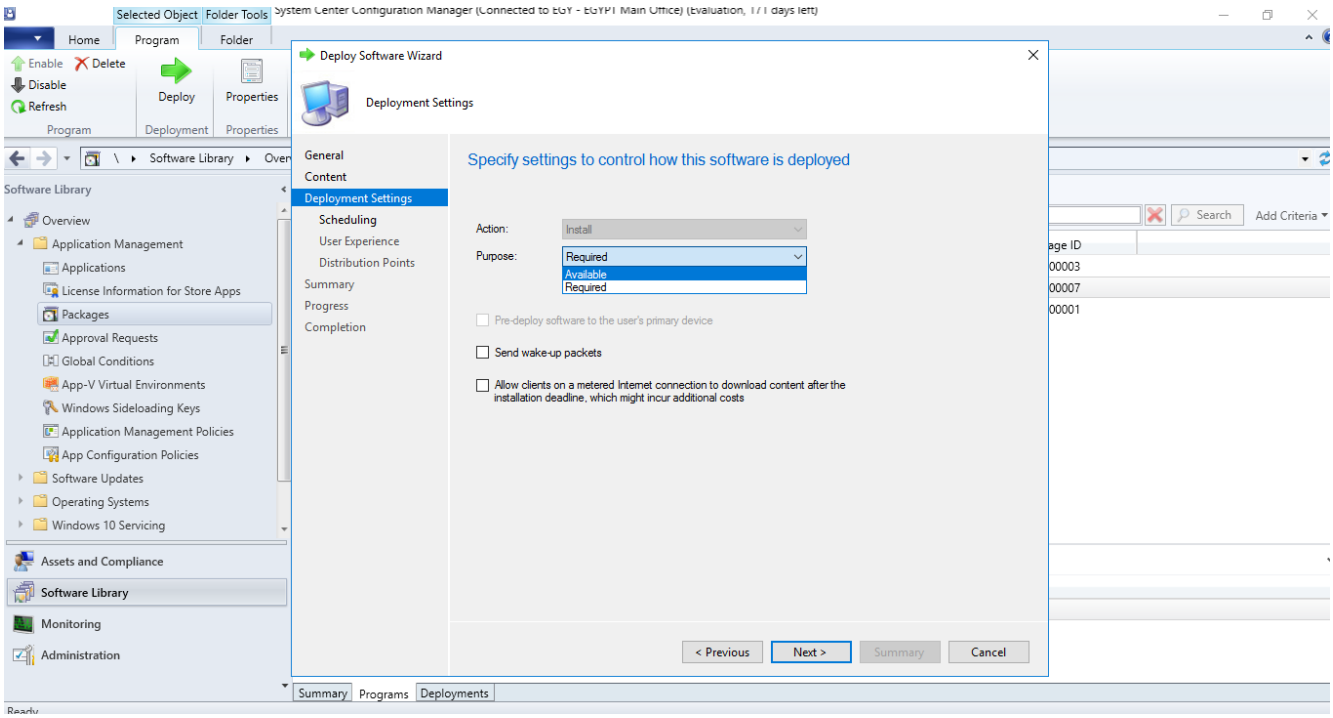

Distribute Content Wizard
General
Review selected content
You have selected the following content for distribution.
Content:
EGY LAB PACKAGE
Some content might have associated dependencies that must be installed before the content can be installed.
Detect associated content dependencies and add them to this distribution
Next >
Cancel

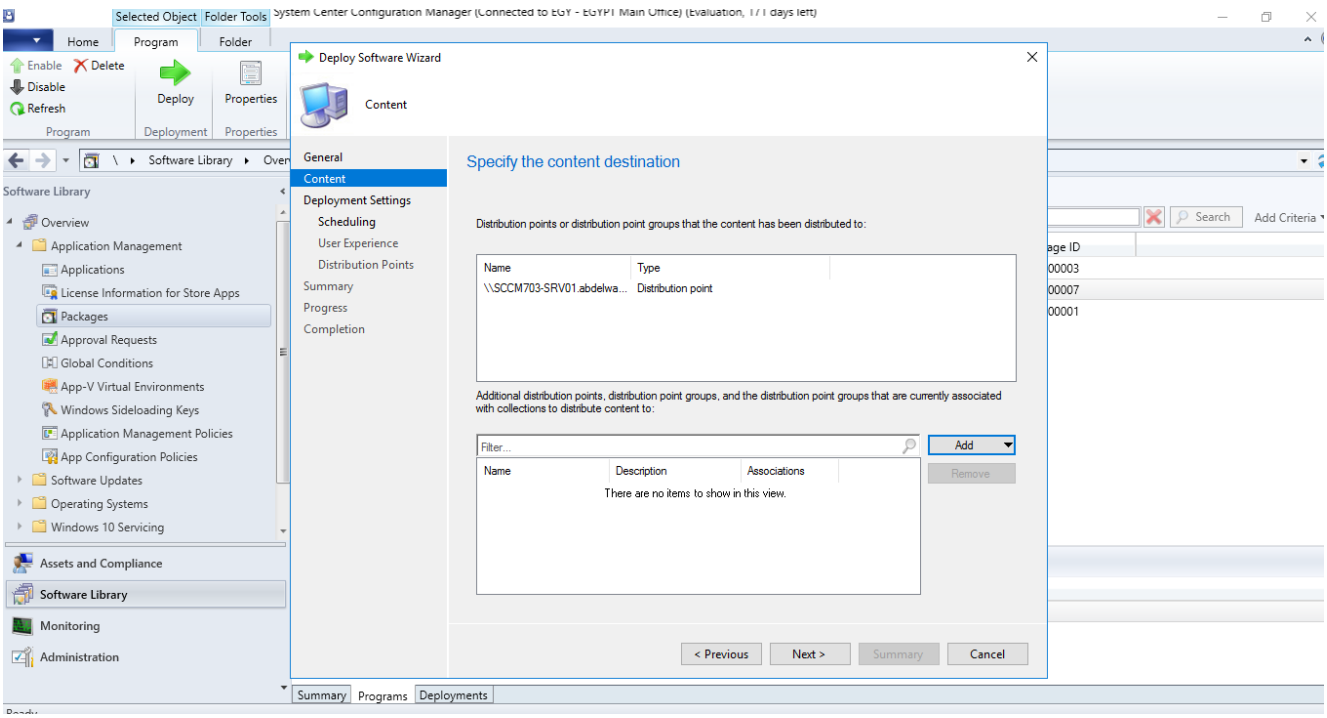
3- Deploy Package to collections



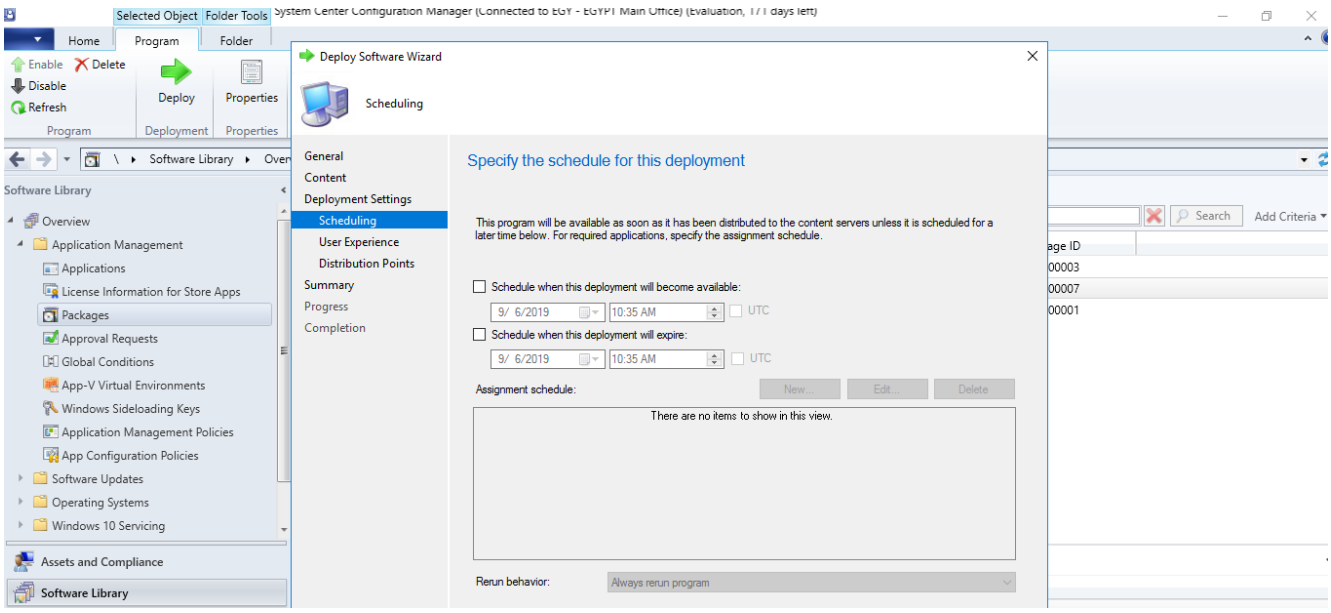


To give users control over the installation, set the SCCM program deployment to the "Available" option. This lets users decide the installation timing and interact with the setup process.

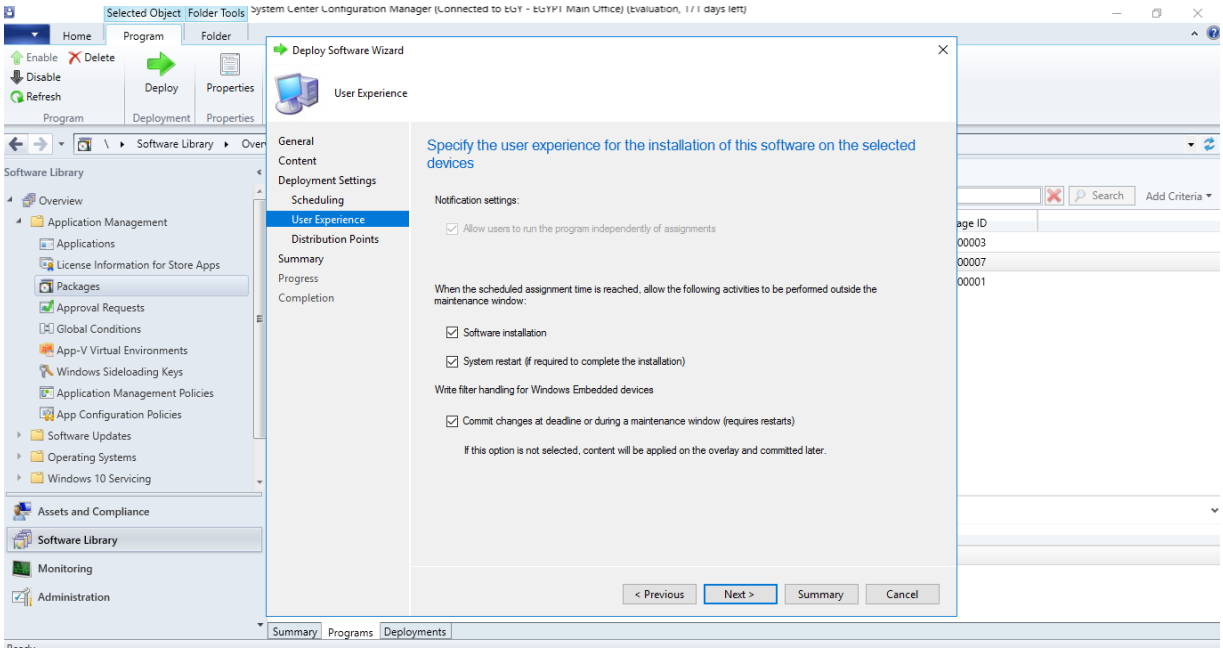




You can set up a schedule for when the application will be visible to users in the software center, or you can update the policy on the user's side through the control panel.



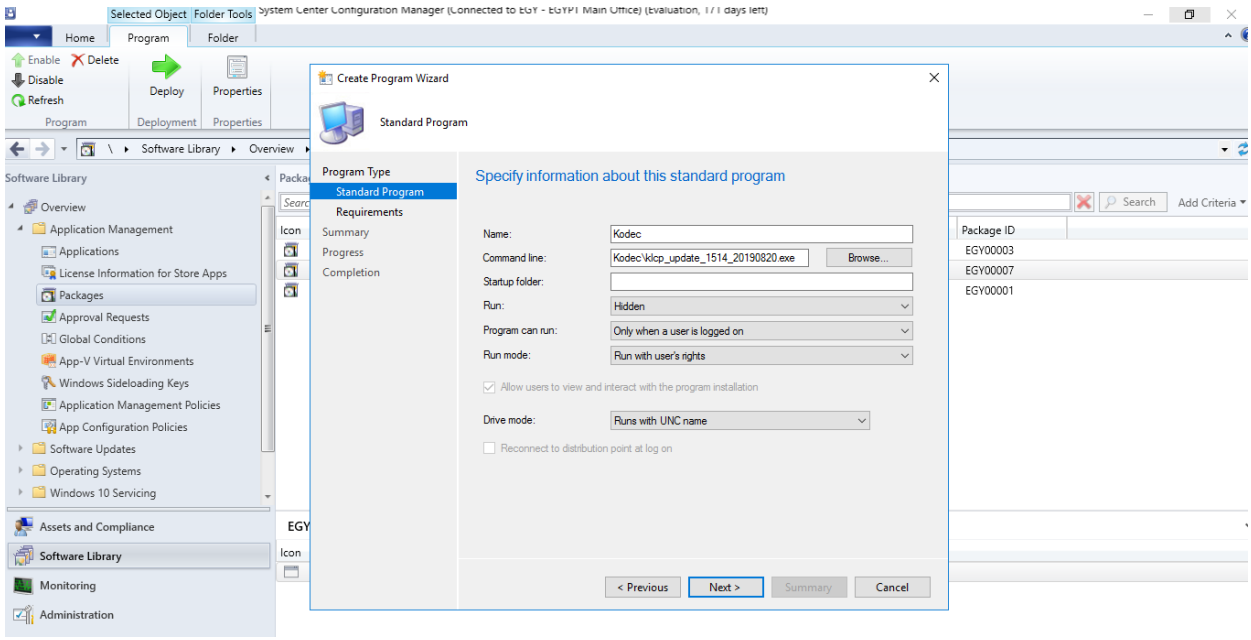
To notify users about new software updates or when a system restart is necessary, you can adjust the notification settings for users within SCCM. These preferences dictate the manner and timing of how users get alerts regarding software availability and required system reboots.

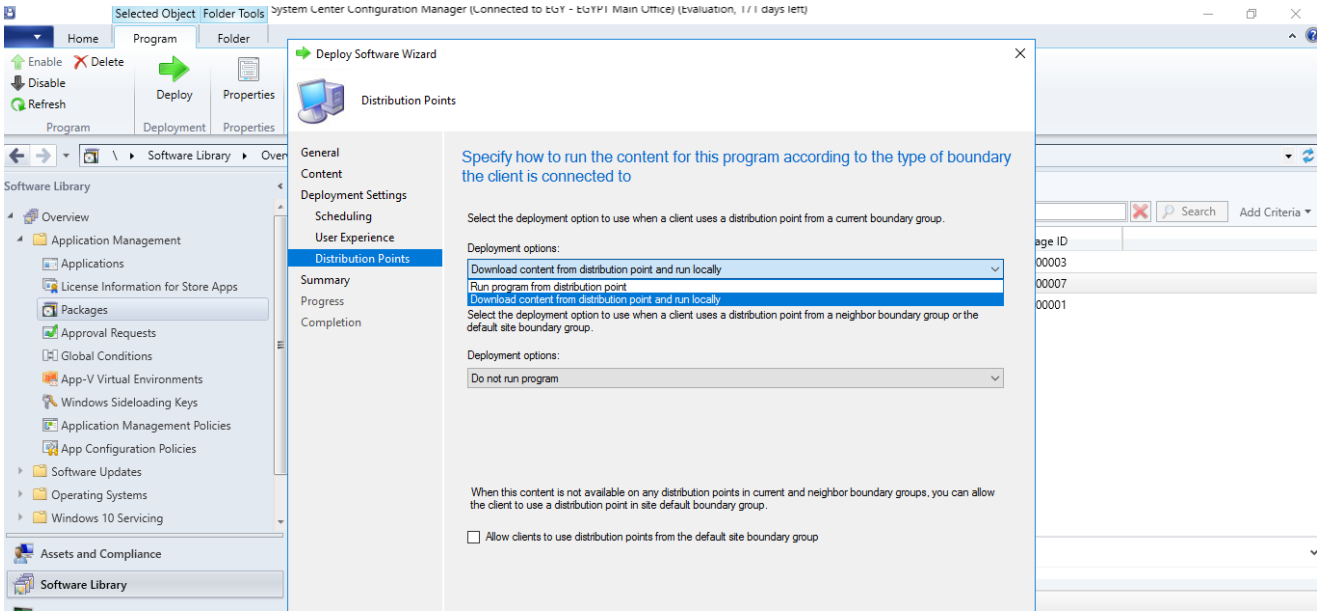


Set up SCCM to pre-

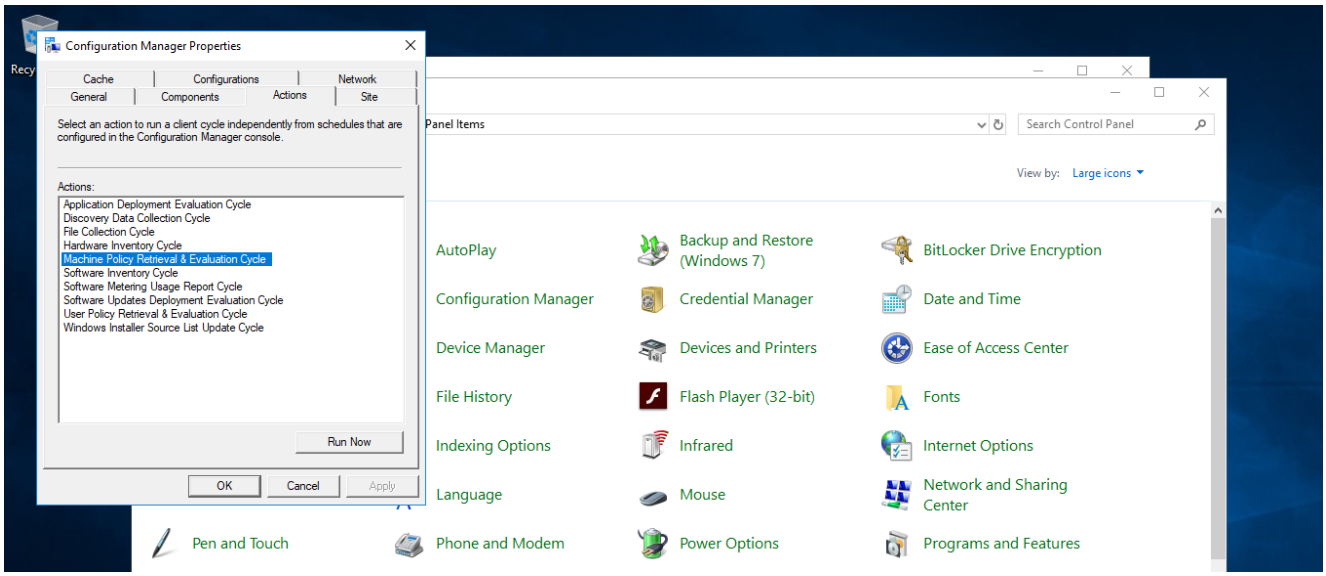
download the software to the client machine before installing it by selecting "Download content locally when needed by running task sequence" in the deployment settings. Normally, this will save the program to the C:\Windows\ccmcache folder on the client computer prior to installation, enhancing installation speed by decreasing network load and shortening installation time.

Create another program to the same package

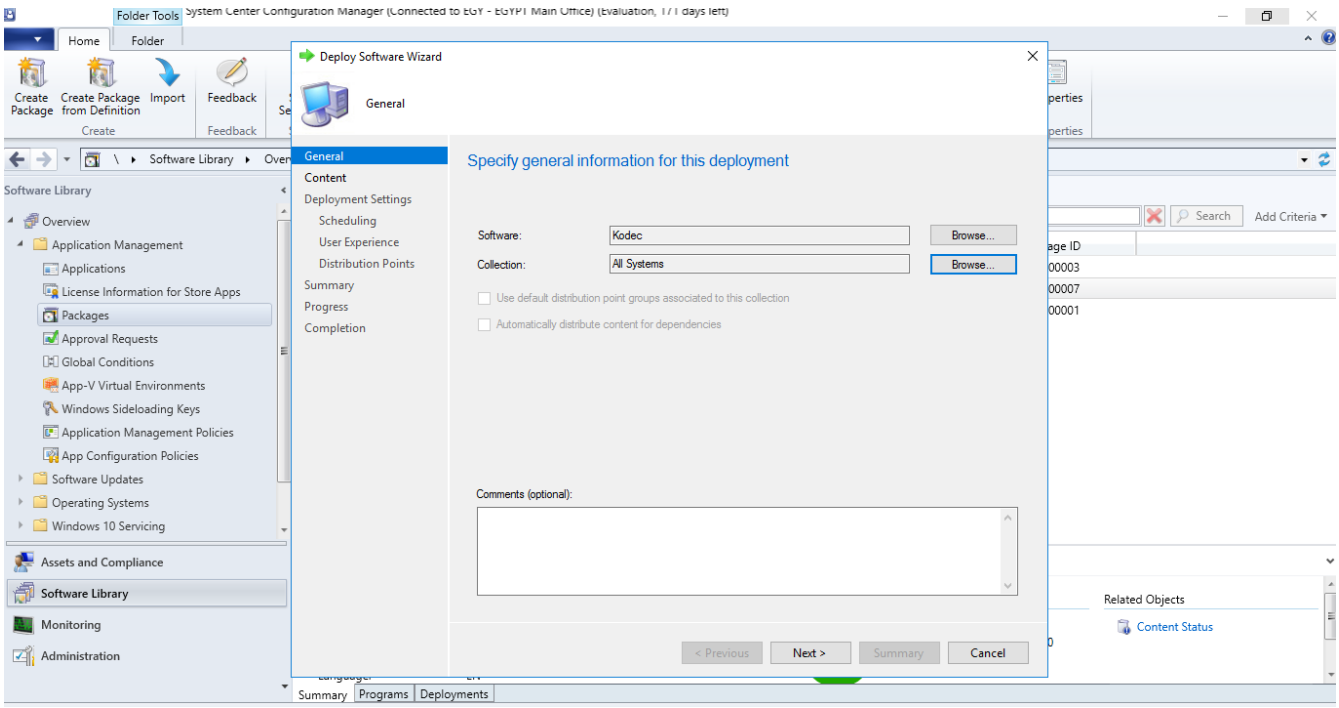




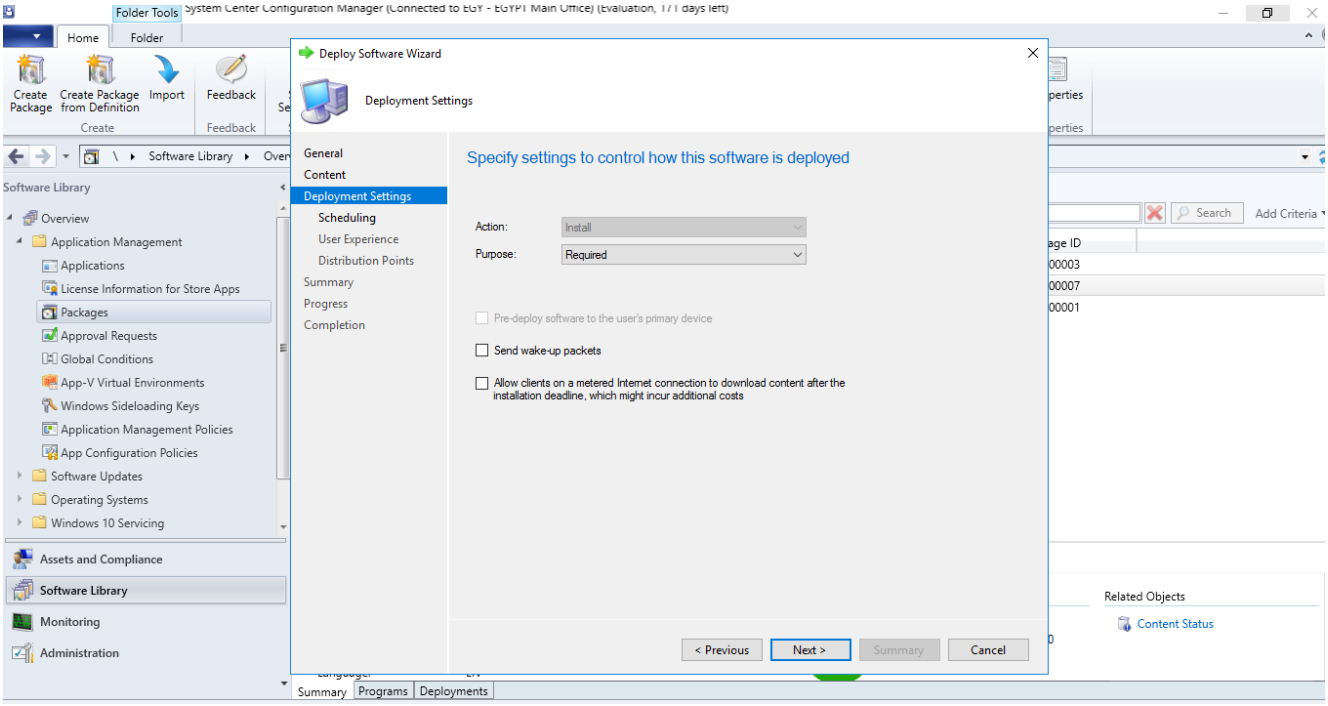
To ensure updates appear in the client's software center, execute the following steps on the client side.

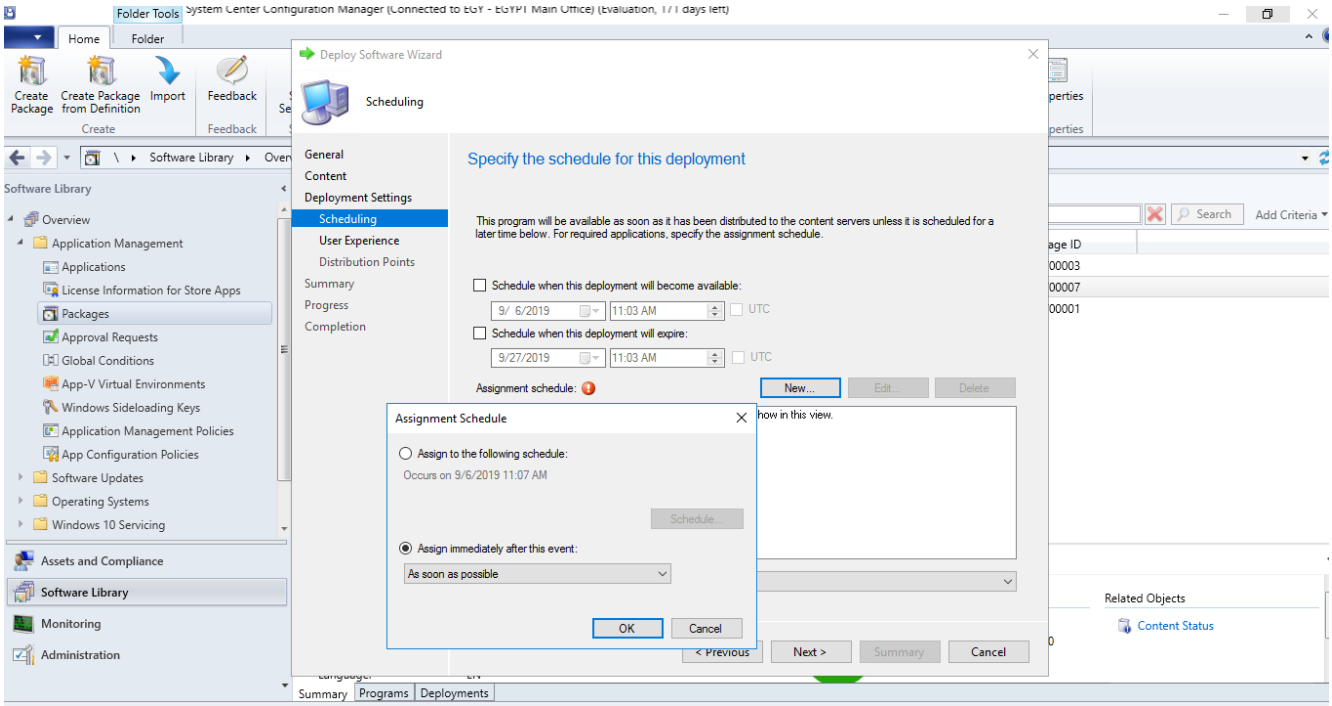


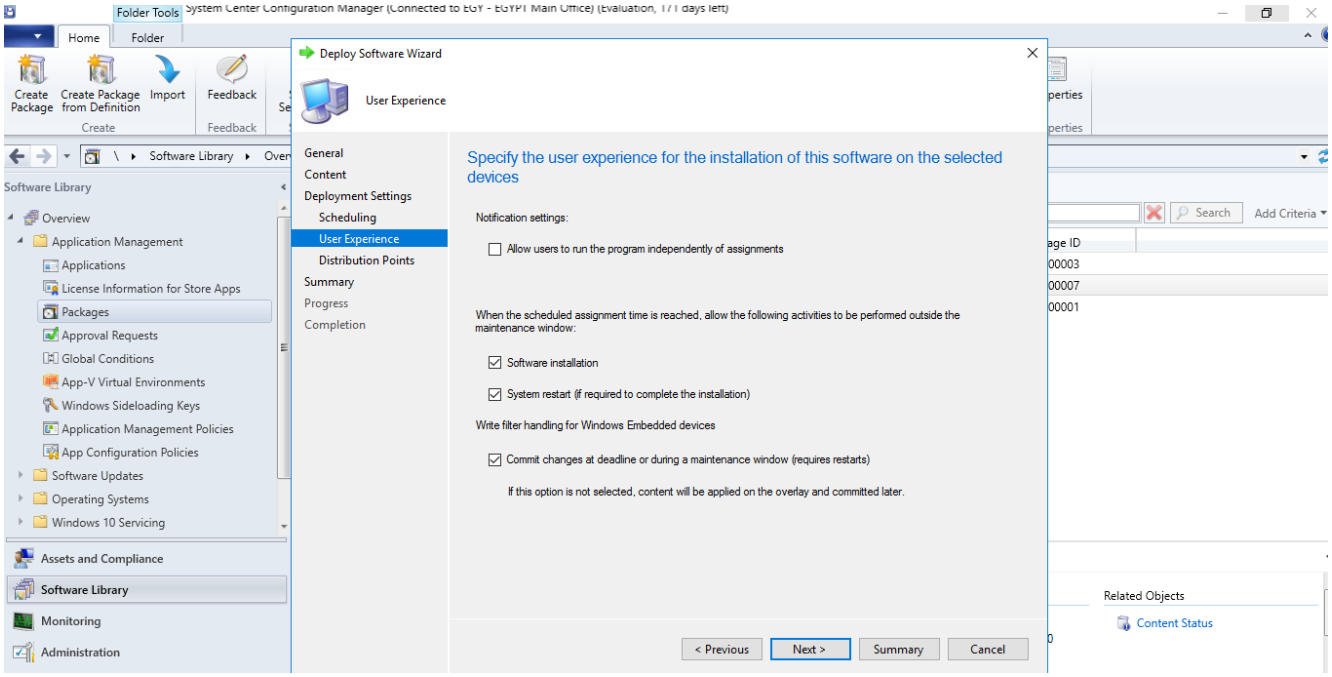
To install a new application on a group of devices in SCCM and make it visible in the Software Center.

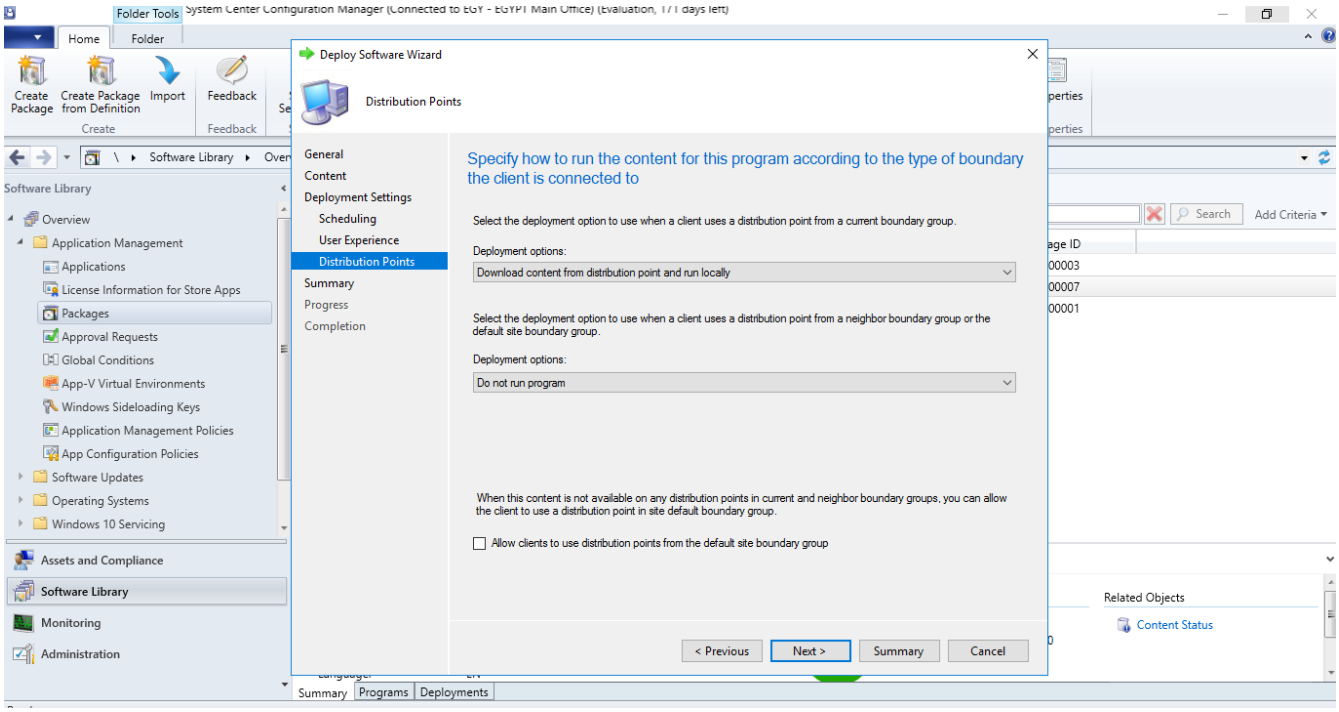


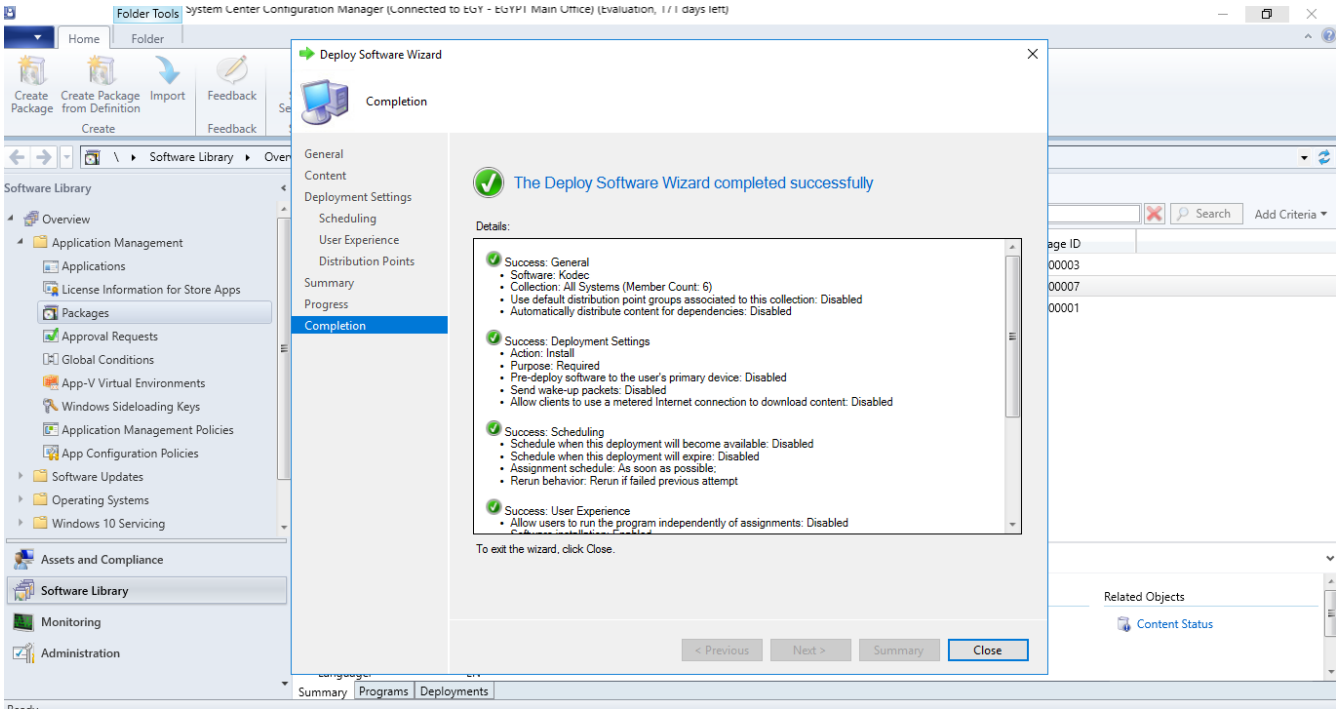
,


Deploy Software Wizard
Deployment Settings
General
Content
Deployment Settings
Scheduling
User Experience
Distribution Points
Summary
Progress
Completion
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
< Previous
Next >
Summary
Cancel

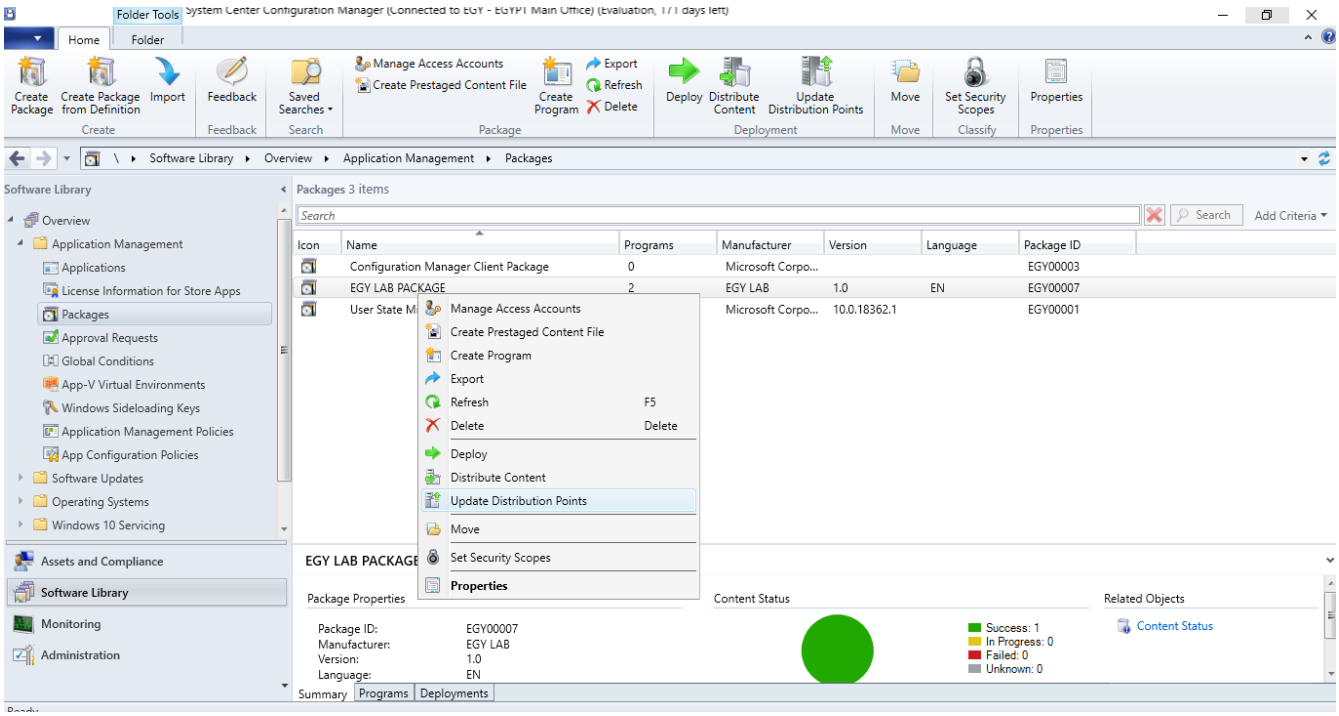

Deploy Software Wizard
Scheduling
General
Content
Deployment Settings
Scheduling
User Experience
Distribution Points
Summary
Progress
Completion
Specify the schedule for this deployment
This program will be available as soon as it has been distributed to the content servers unless it is scheduled for a later time below. For required applications, specify the assignment schedule.
Schedule when this deployment will become available:
Schedule when this deployment will expire:
Assignment schedule:
New...
Edit...
Delete
Assignment Schedule
Assign to the following schedule:
Occurs on 9/6/2019 11:07 AM
Schedule...
Assign immediately after this event:
As soon as possible
OK
Cancel
< Previous
Next >
Summary
Cancel


Deploy Software Wizard
User Experience
General
Content
Deployment Settings
Scheduling
User Experience
Distribution Points
Summary
Progress
Completion
Specify the user experience for the installation of this software on the selected devices
Notification settings:
Allow users to run the program independently of assignments
When the scheduled assignment time 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.
< Previous
Next >
Summary
Cancel

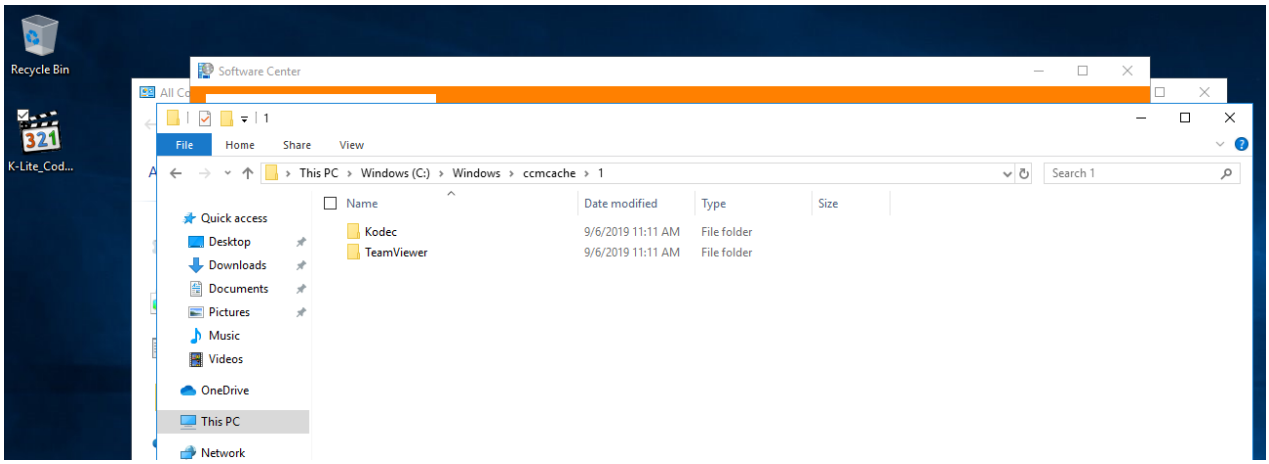

Deploy Software Wizard
Distribution Points
General
Content
Deployment Settings
Scheduling
User Experience
Distribution Points
Summary
Progress
Completion
Specify how to run the content for this program according to the type of boundary the client is connected to
Select the deployment option to use when a client uses a distribution point from a current boundary group.
Deployment options:
Download content from distribution point and run locally
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 run program
When this content is not available on any distribution points in current and neighbor boundary groups, you can allow the client to use a distribution point in site default boundary group.
Allow clients to use distribution points from the default site boundary group
< Previous
Next >
Summary
Cancel

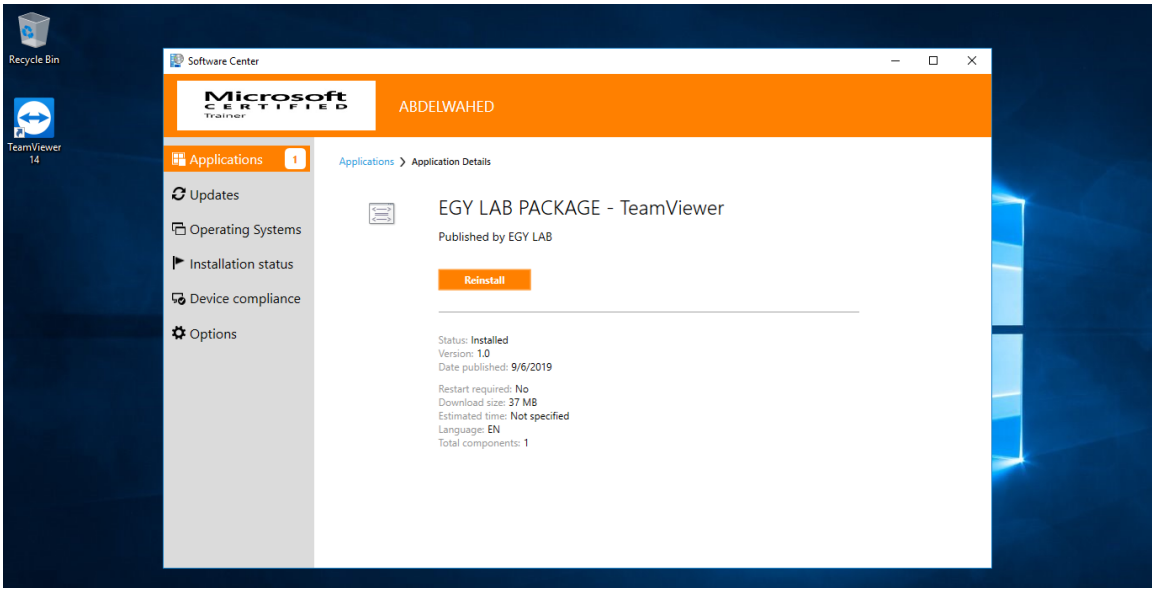


Please proceed to refresh the distribution point.

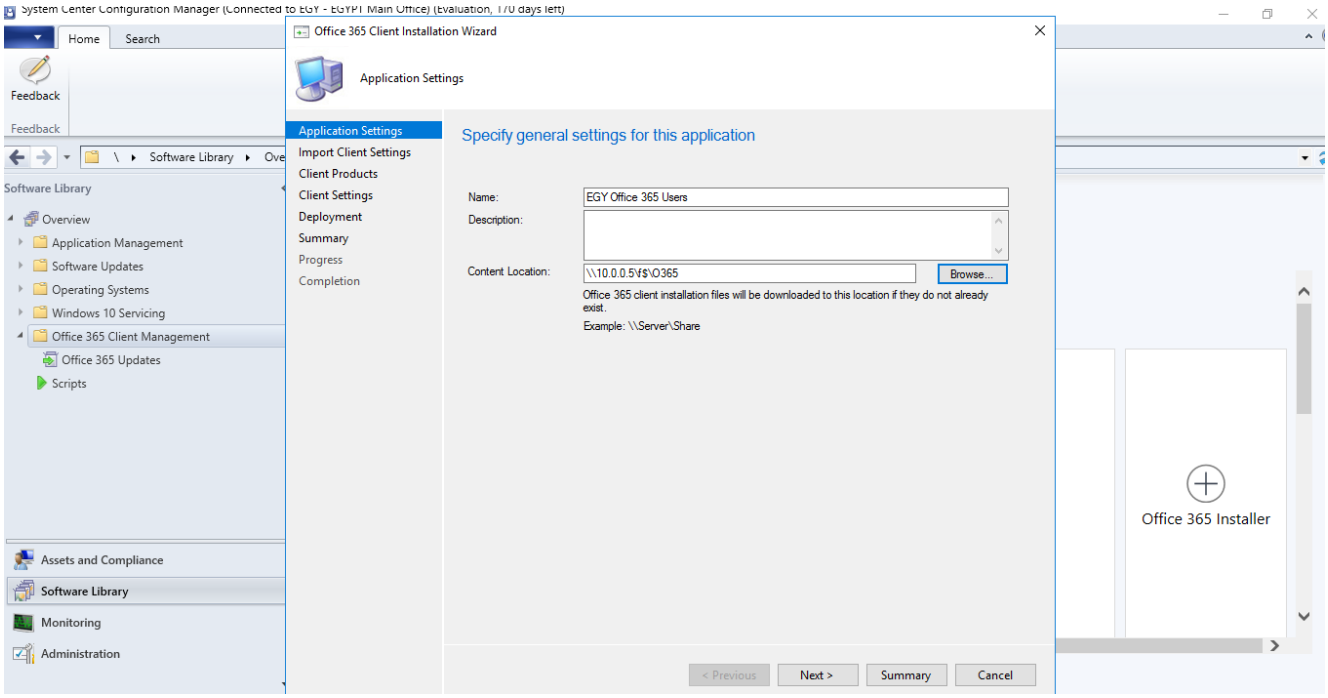


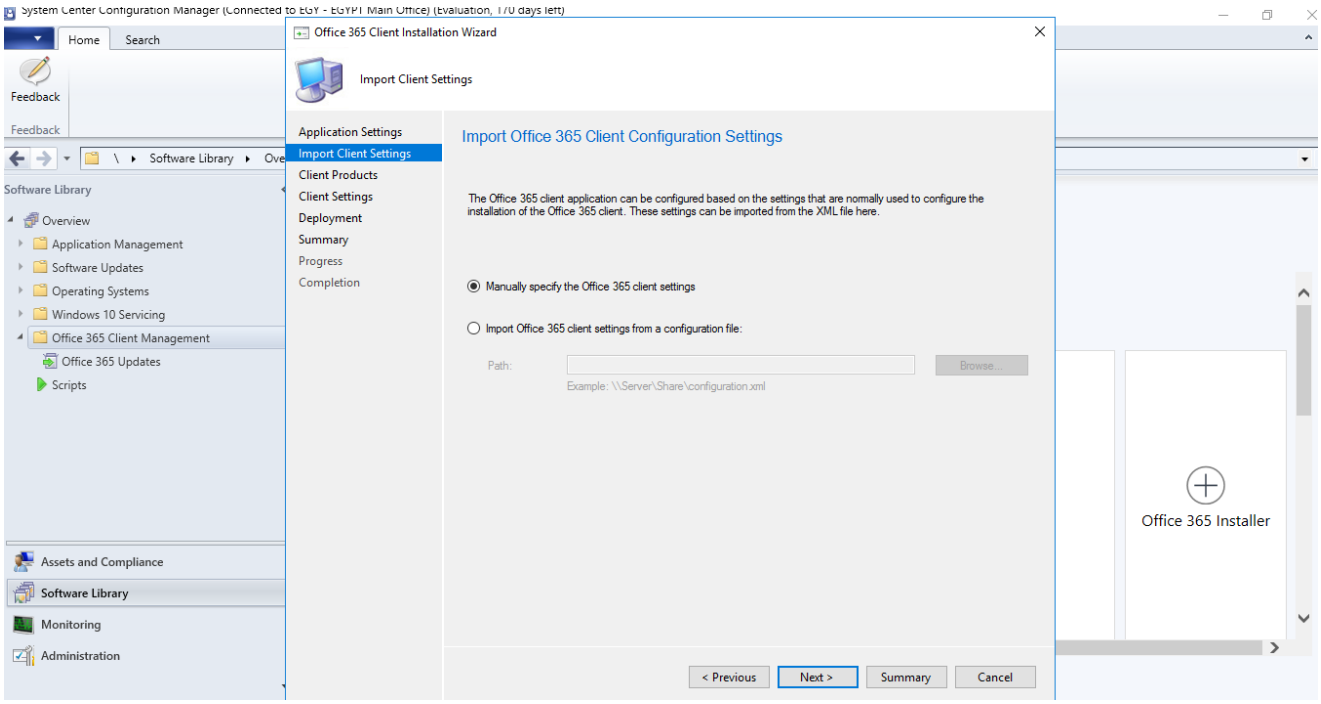
Verify if client packages have been successfully copied to local cache.

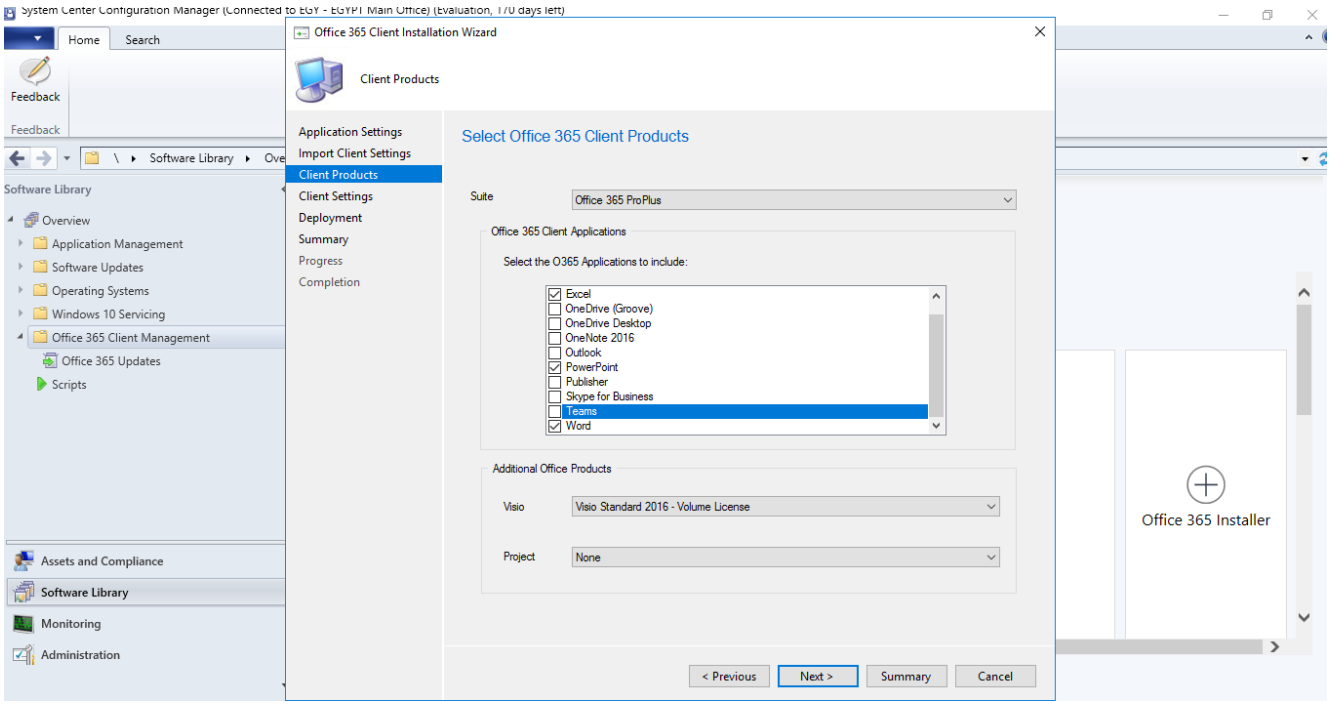


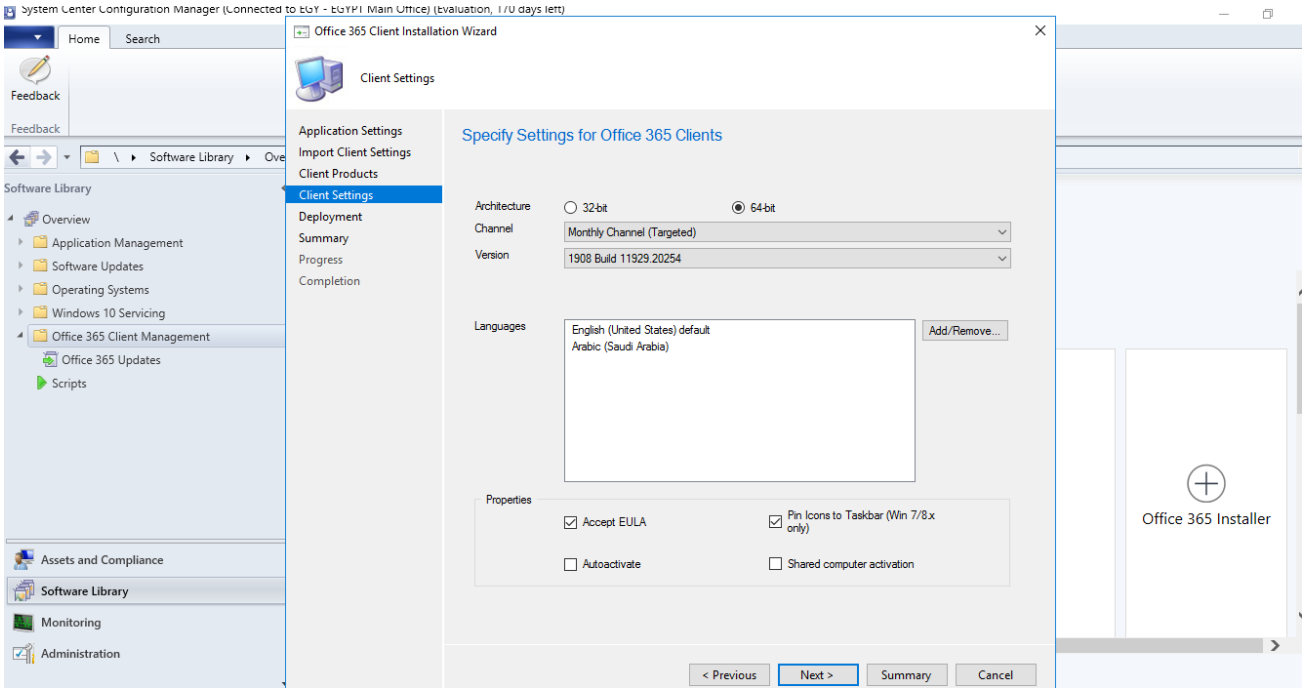


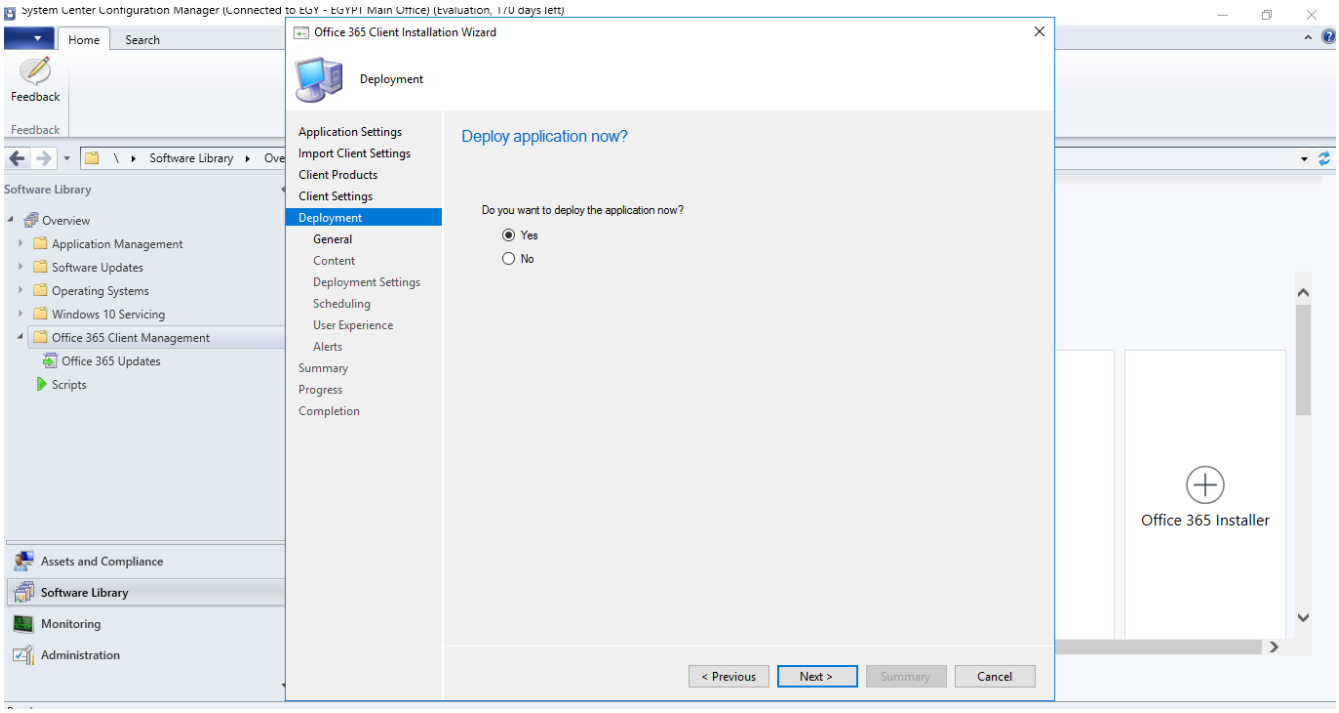
Install Office 365 using SCCM

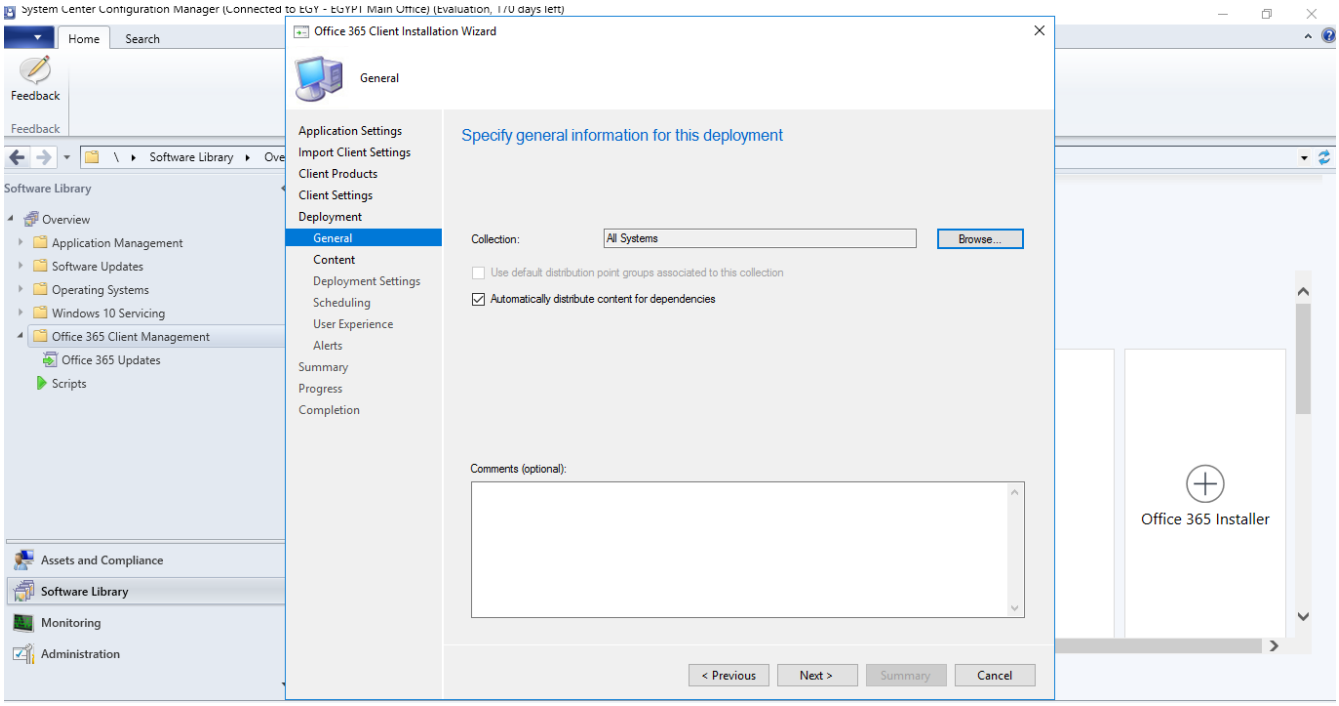


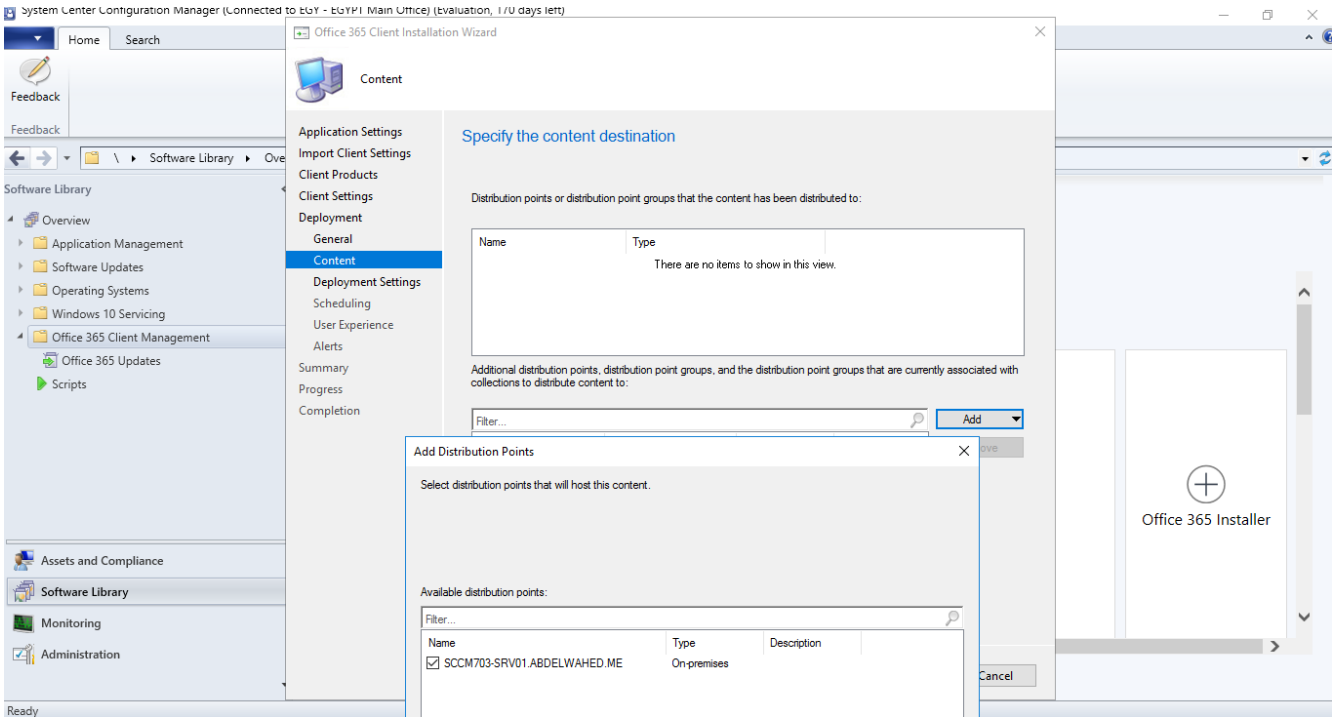


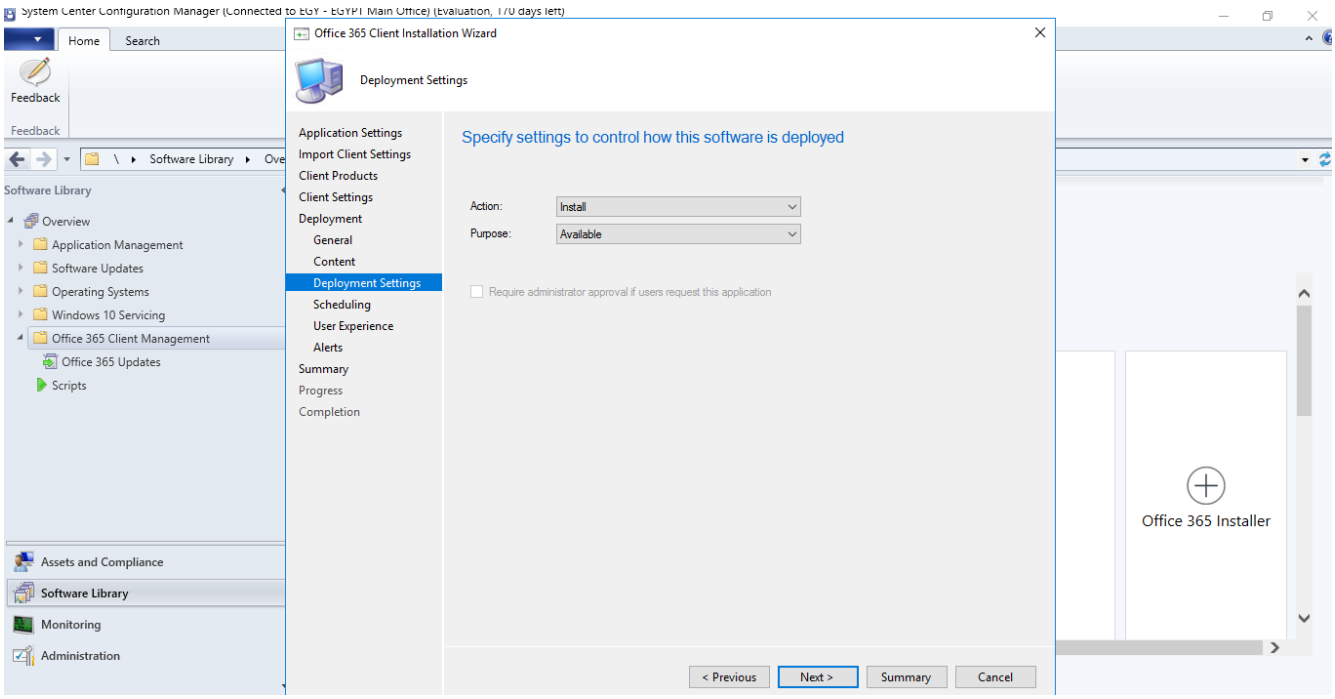

Office 365 Client Installation Wizard
Client Products
Application Settings
Import Client Settings
Client Products
Client Settings
Deployment
Summary
Progress
Completion
Select Office 365 Client Products
Suite
Office 365 ProPlus
Office 365 Client Applications
Select the O365 Applications to include:
Excel
OneDrive (Groove)
OneDrive Desktop
OneNote 2016
Outlook
PowerPoint
Publisher
Skype for Business
Teams
Word
Additional Office Products
Visio
Visio Standard 2016 - Volume License
Project
None
< Previous
Next >
Summary
Cancel
Office 365 Installer
Assets and Compliance
Software Library
Monitoring
Administration

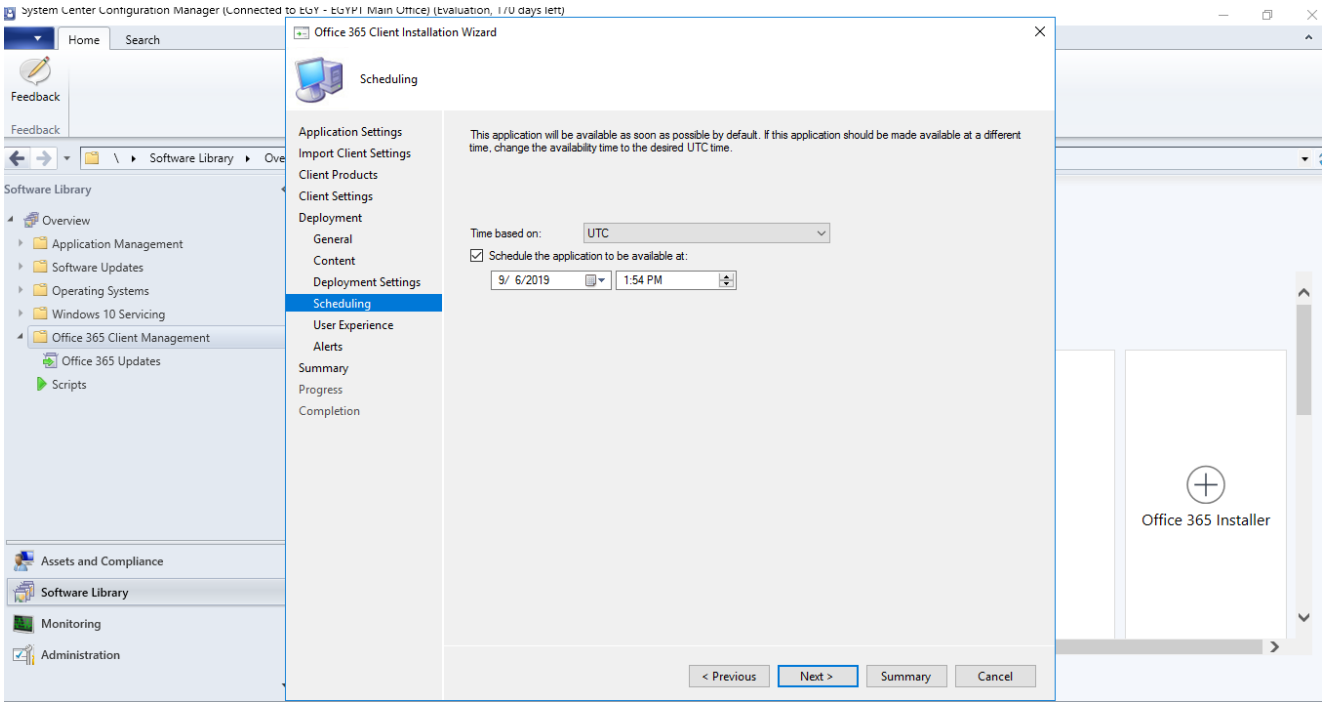

Office 365 Client Installation Wizard
Client Settings
Application Settings
Import Client Settings
Client Products
Client Settings
Deployment
Summary
Progress
Completion
Specify Settings for Office 365 Clients
Architecture
32-bit
64-bit
Channel
Monthly Channel (Targeted)
Version
1908 Build 11929.20254
Languages
English (United States) default
Arabic (Saudi Arabia)
Add/Remove...
Properties
Accept EULA
Pin Icons to Taskbar (Win 7/8.x only)
Autoactivate
Shared computer activation
< Previous
Next >
Summary
Cancel
Office 365 Installer
Assets and Compliance
Software Library
Monitoring
Administration

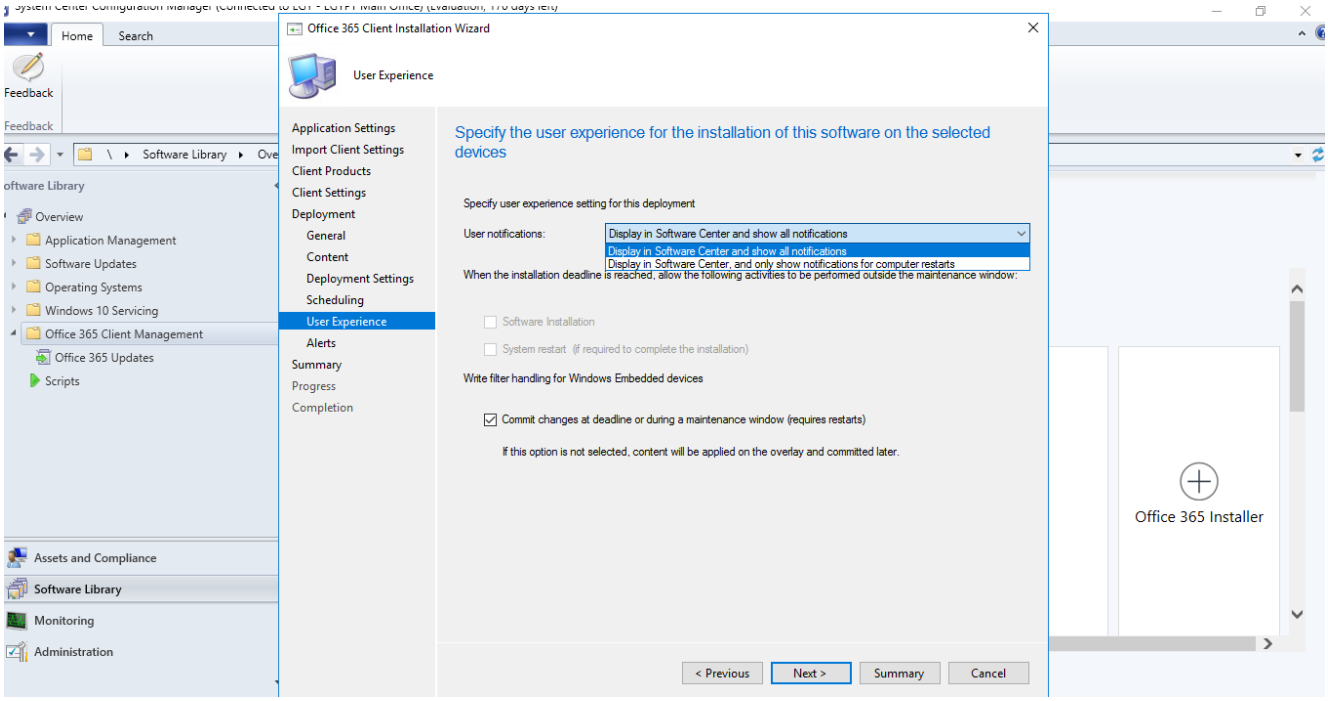

Office 365 Client Installation Wizard
Deployment
Application Settings
Import Client Settings
Client Products
Client Settings
Deployment
General
Content
Deployment Settings
Scheduling
User Experience
Alerts
Summary
Progress
Completion
Deploy application now?
Do you want to deploy the application now?
Yes
No
< Previous
Next >
Summary
Cancel
Office 365 Installer

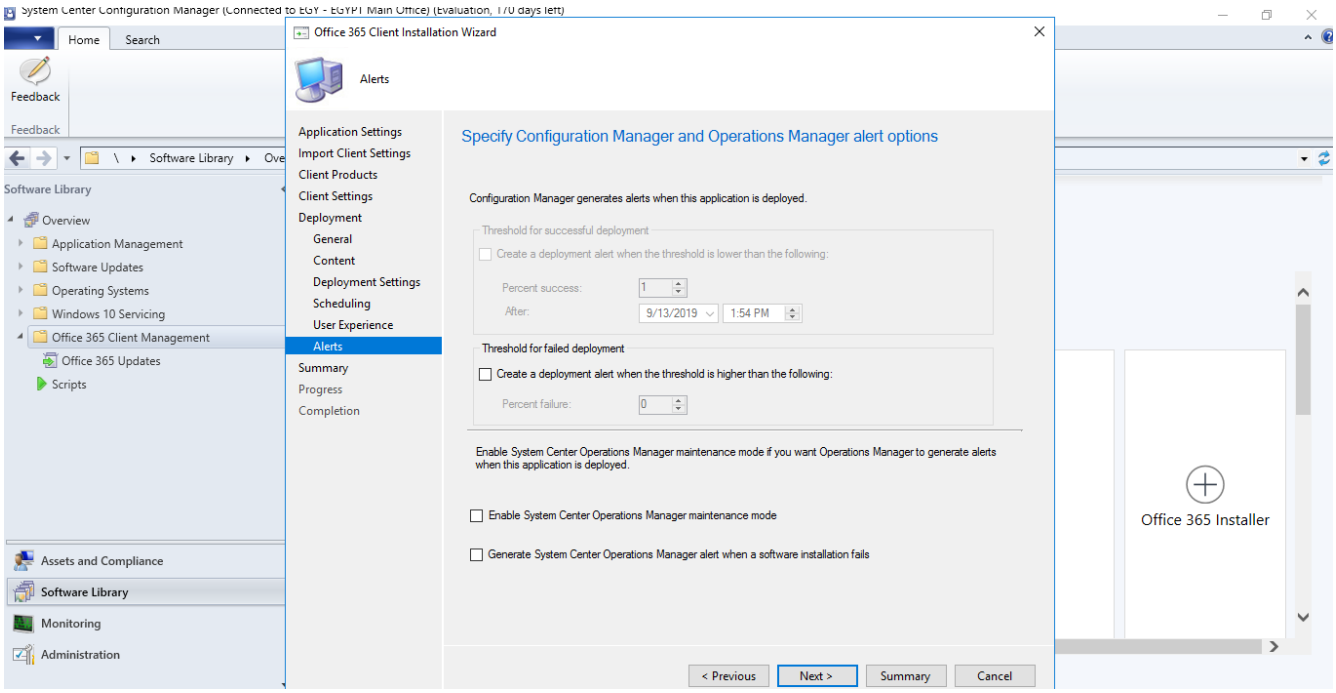

Office 365 Client Installation Wizard
General
Application Settings
Import Client Settings
Client Products
Client Settings
Deployment
General
Content
Deployment Settings
Scheduling
User Experience
Alerts
Summary
Progress
Completion
Specify general information for this deployment
Collection:
All Systems
Browse...
Use default distribution point groups associated to this collection
Automatically distribute content for dependencies
Comments (optional):
< Previous
Next >
Summary
Cancel
Office 365 Installer

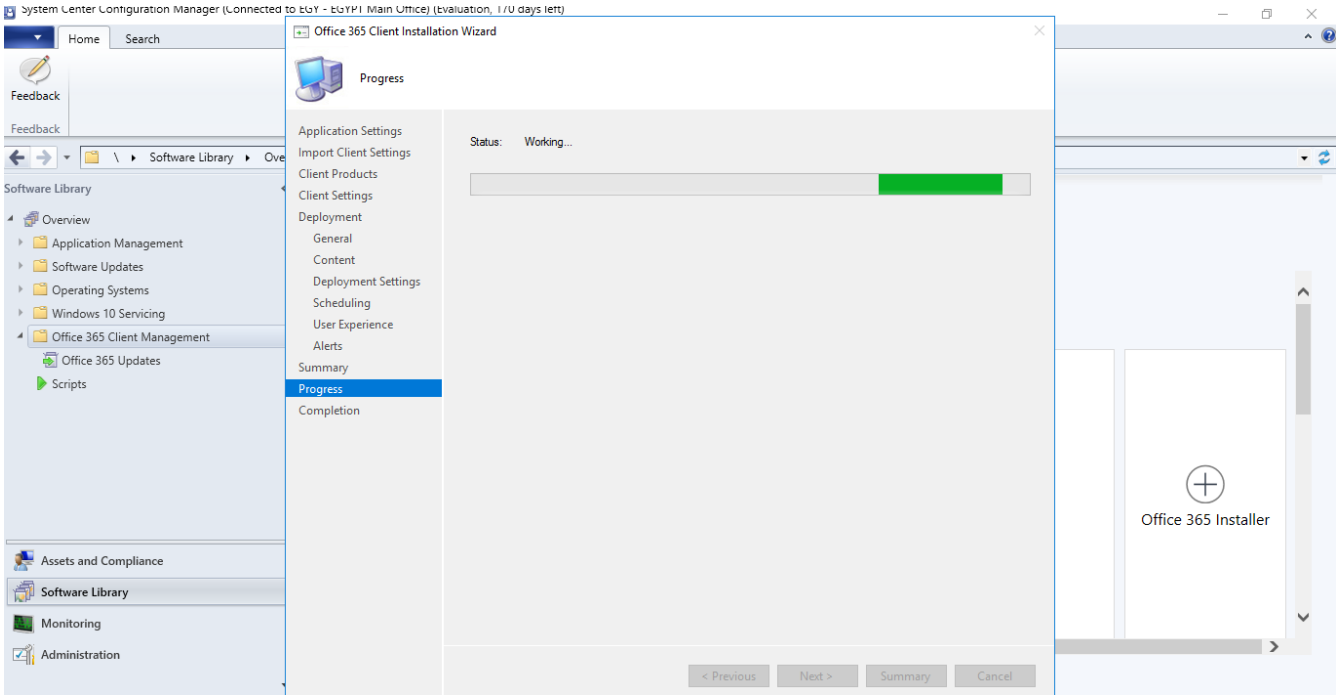

Office 365 Client Installation Wizard
Content
Application Settings
Import Client Settings
Client Products
Client Settings
Deployment
General
Content
Deployment Settings
Scheduling
User Experience
Alerts
Summary
Progress
Completion
Specify the content destination
Distribution points or distribution point groups that the content has been distributed to:
Name
Type
There are no items to show in this view.
Additional distribution points, distribution point groups, and the distribution point groups that are currently associated with collections to distribute content to:
Filter...
Add
Add Distribution Points
Select distribution points that will host this content.
Available distribution points:
Filter...
Name
Type
Description
SCCM703-SRV01.ABDELWAHED.ME
On-premises
Cancel
Office 365 Installer
Software Library
Overview
Application Management
Software Updates
Operating Systems
Windows 10 Servicing
Office 365 Client Management
Office 365 Updates
Scripts
Assets and Compliance
Monitoring
Administration
Ready

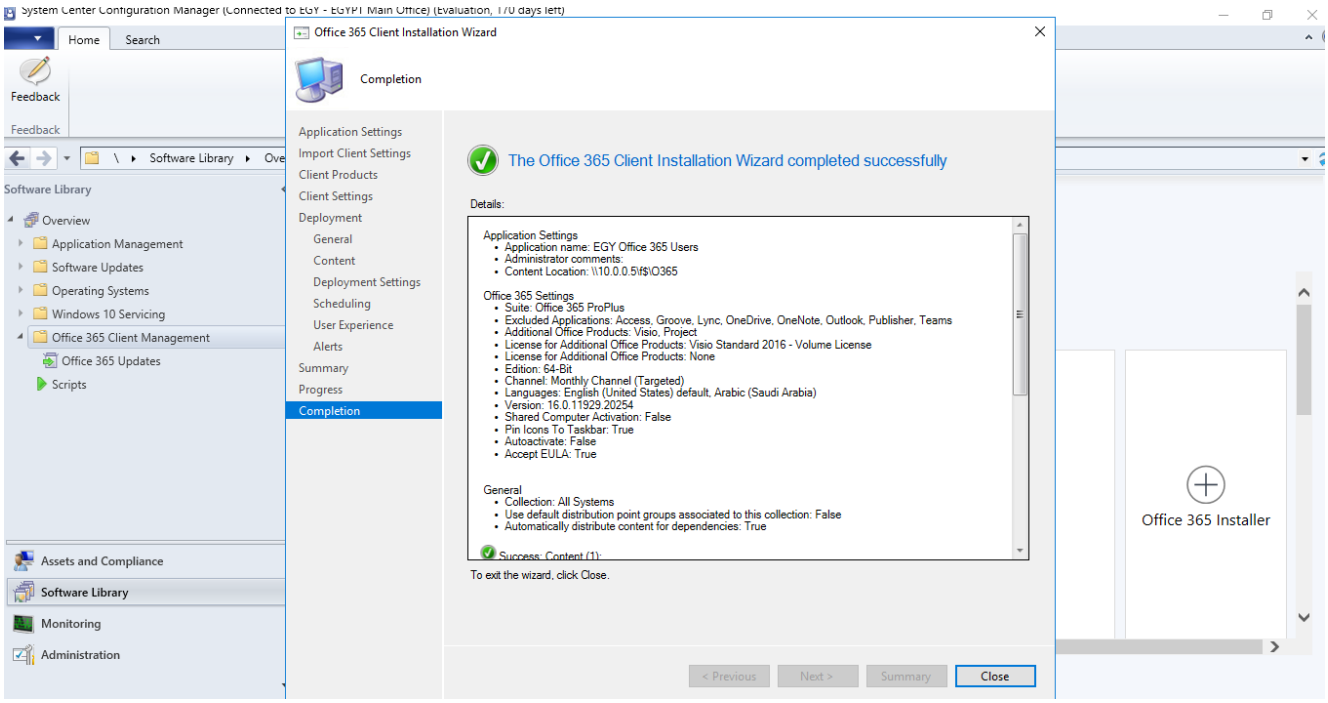

Office 365 Client Installation Wizard
Deployment Settings
Application Settings
Import Client Settings
Client Products
Client Settings
Deployment
General
Content
Deployment Settings
Scheduling
User Experience
Alerts
Summary
Progress
Completion
Specify settings to control how this software is deployed
Action:
Install
Purpose:
Available
Require administrator approval if users request this application
< Previous
Next >
Summary
Cancel
Office 365 Installer
Software Library
Overview
Application Management
Software Updates
Operating Systems
Windows 10 Servicing
Office 365 Client Management
Office 365 Updates
Scripts
Assets and Compliance
Monitoring
Administration

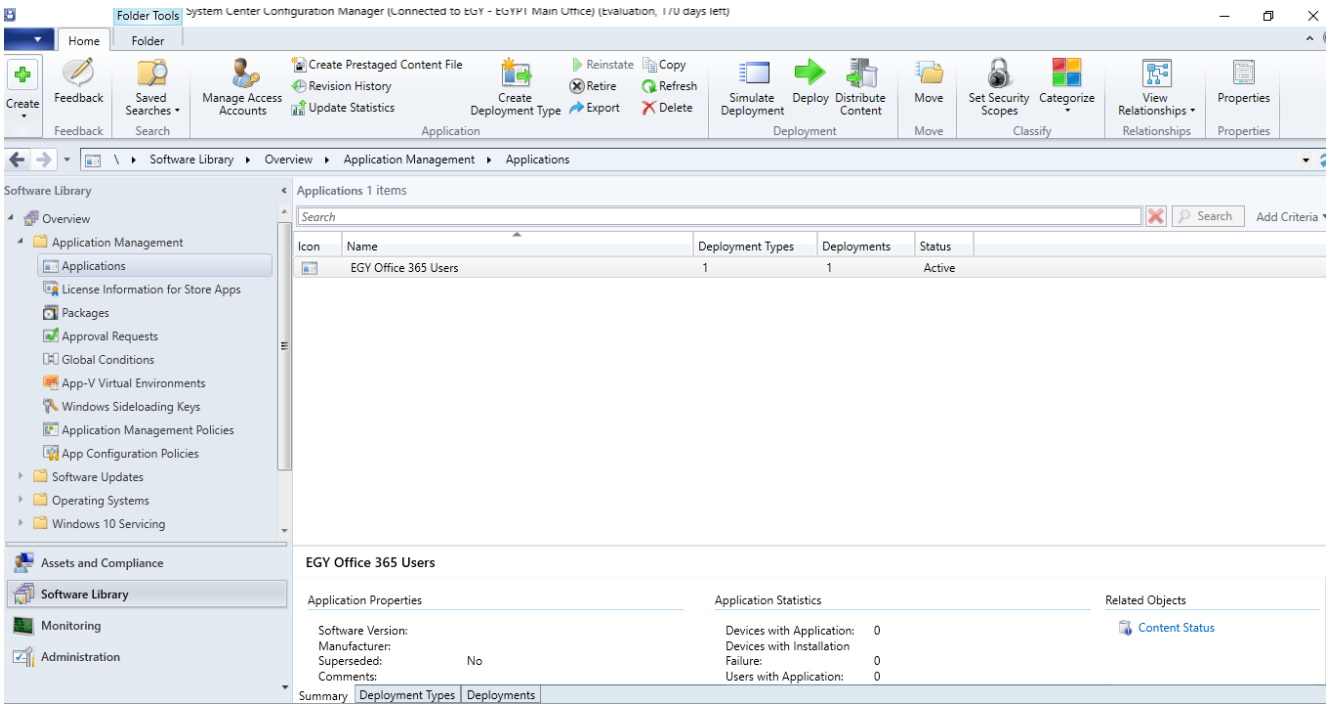

Office 365 Client Installation Wizard
Scheduling
Application Settings
Import Client Settings
Client Products
Client Settings
Deployment
General
Content
Deployment Settings
Scheduling
User Experience
Alerts
Summary
Progress
Completion
This application will be available as soon as possible by default. 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:
9/ 6/2019
1:54 PM
< Previous
Next >
Summary
Cancel
Office 365 Installer

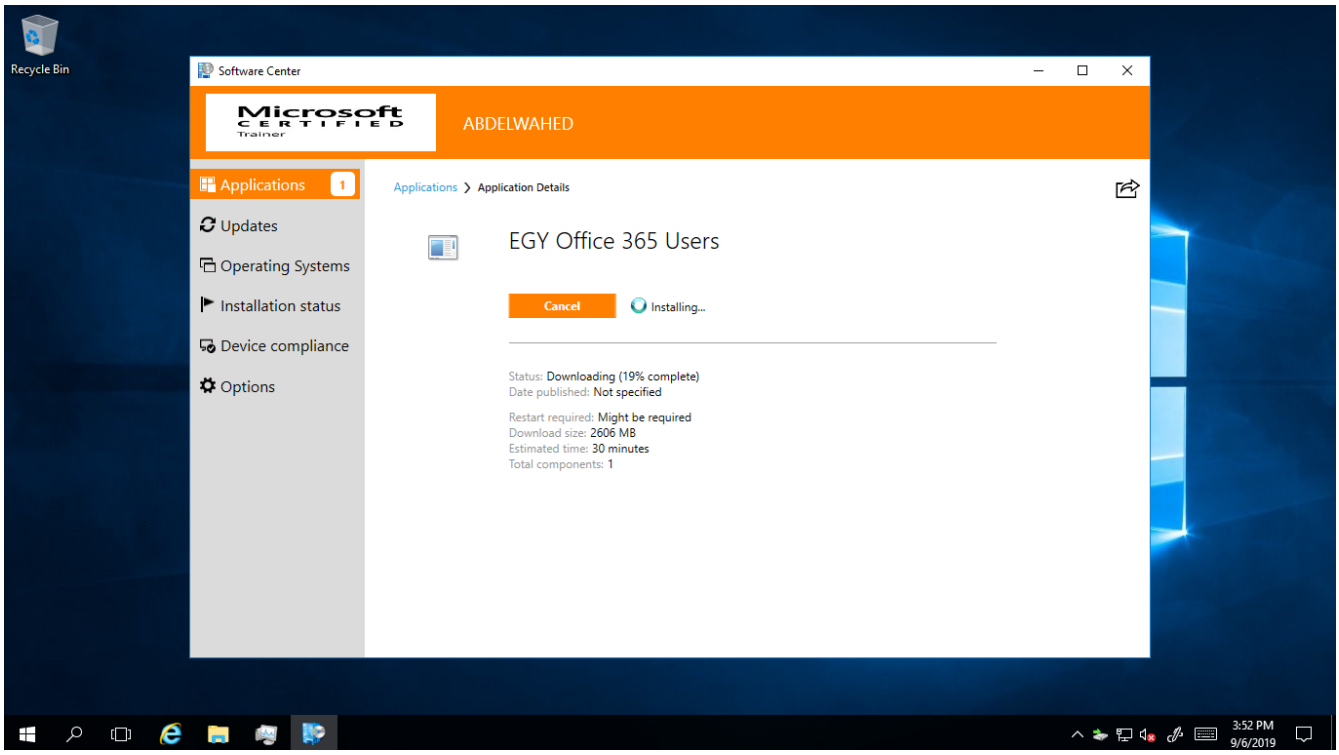

Office 365 Client Installation Wizard
User Experience
Application Settings
Import Client Settings
Client Products
Client Settings
Deployment
General
Content
Deployment Settings
Scheduling
User Experience
Alerts
Summary
Progress
Completion
Specify the user experience for the installation of this software 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
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.
< Previous
Next >
Summary
Cancel
Office 365 Installer

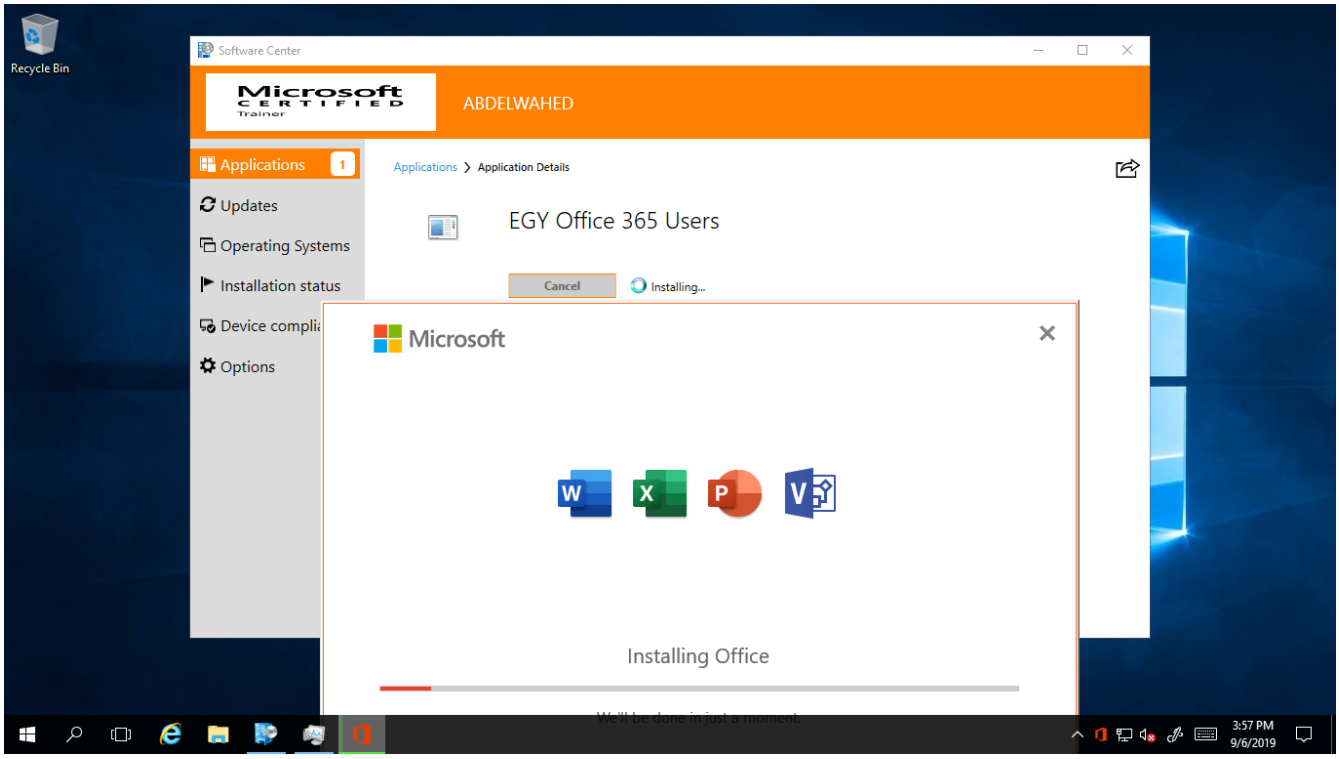

Office 365 Client Installation Wizard
Alerts
Application Settings
Import Client Settings
Client Products
Client Settings
Deployment
General
Content
Deployment Settings
Scheduling
User Experience
Alerts
Summary
Progress
Completion
Specify Configuration Manager and Operations Manager alert options
Configuration Manager generates alerts when this application is deployed.
Threshold for successful deployment
Create a deployment alert when the threshold is lower than the following:
Percent success:
After:
9/13/2019
1:54 PM
Threshold for failed deployment
Create a deployment alert when the threshold is higher than the following:
Percent failure:
Enable System Center Operations Manager maintenance mode if you want Operations Manager to generate alerts when this application is deployed.
Enable System Center Operations Manager maintenance mode
Generate System Center Operations Manager alert when a software installation fails
< Previous
Next >
Summary
Cancel
Office 365 Installer

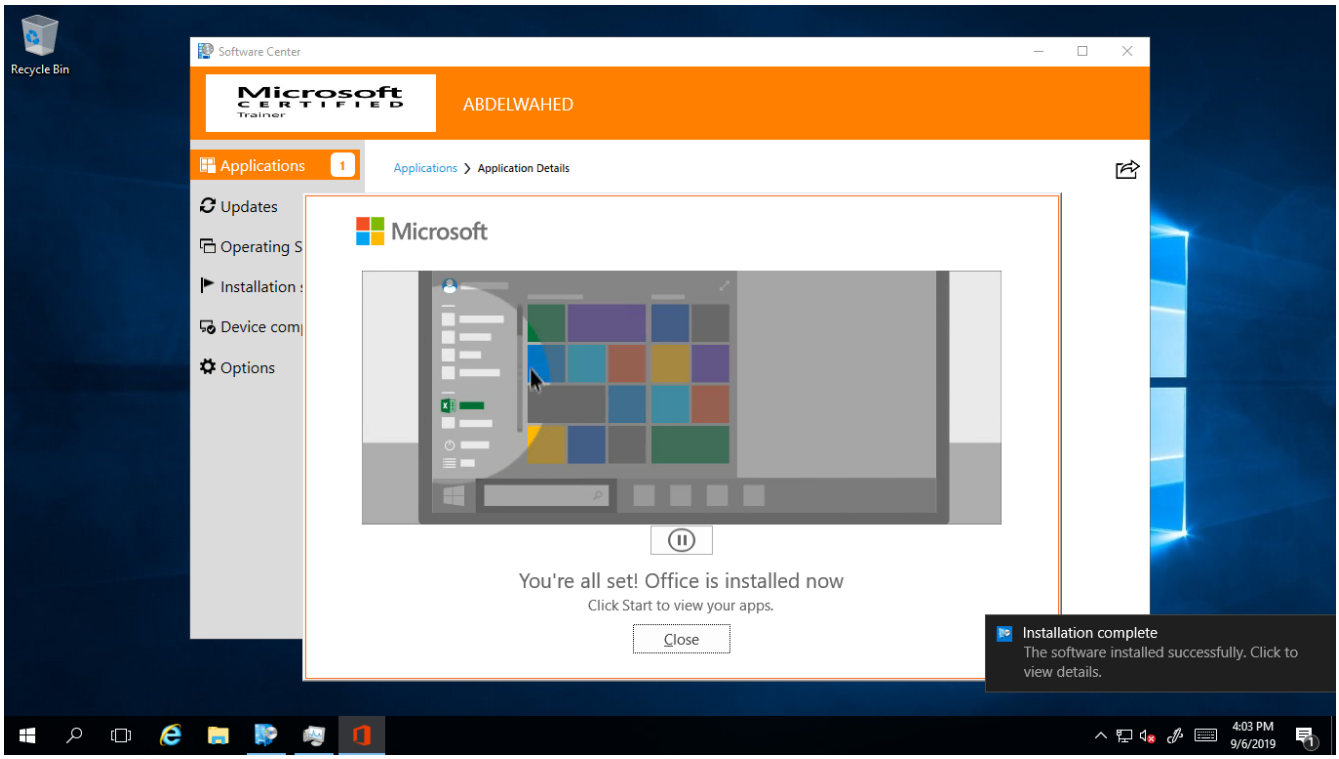

Office 365 Client Installation Wizard
Progress
Application Settings
Import Client Settings
Client Products
Client Settings
Deployment
General
Content
Deployment Settings
Scheduling
User Experience
Alerts
Summary
Progress
Completion
Status: Working...
< Previous
Next >
Summary
Cancel
Office 365 Installer

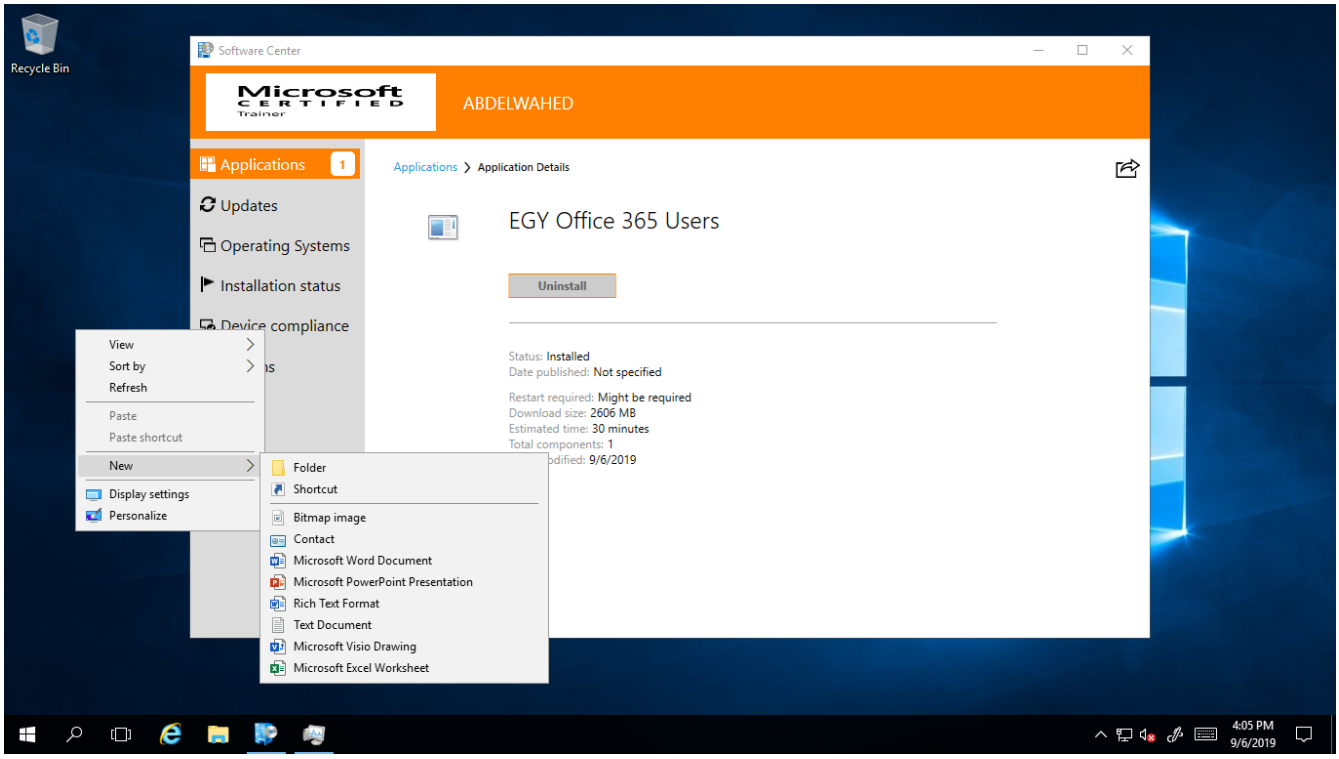

Office 365 Client Installation Wizard
Completion
Application Settings
Import Client Settings
Client Products
Client Settings
Deployment
General
Content
Deployment Settings
Scheduling
User Experience
Alerts
Summary
Progress
Completion
The Office 365 Client Installation Wizard completed successfully
Details:
Application Settings
• Application name: EGY Office 365 Users
• Administrator comments:
• Content Location: \\10.0.0.5\f$\O365
Office 365 Settings
• Suite: Office 365 ProPlus
• Excluded Applications: Access, Groove, Lync, OneDrive, OneNote, Outlook, Publisher, Teams
• Additional Office Products: Visio, Project
• License for Additional Office Products: Visio Standard 2016 - Volume License
• License for Additional Office Products: None
• Edition: 64-Bit
• Channel: Monthly Channel (Targeted)
• Languages: English (United States) default, Arabic (Saudi Arabia)
• Version: 16.0.11929.20254
• Shared Computer Activation: False
• Pin Icons To Taskbar: True
• Autoactivate: False
• Accept EULA: True
General
• Collection: All Systems
• Use default distribution point groups associated to this collection: False
• Automatically distribute content for dependencies: True
Success: Content (1):
To exit the wizard, click Close.
< Previous
Next >
Summary
Close
Office 365 Installer
Software Library
Overview
Application Management
Software Updates
Operating Systems
Windows 10 Servicing
Office 365 Client Management
Office 365 Updates
Scripts
Assets and Compliance
Software Library
Monitoring
Administration


Folder Tools
Home
Folder
Create
Feedback
Saved Searches
Manage Access Accounts
Create Prestaged Content File
Revision History
Update Statistics
Create Deployment Type
Reinstate
Retire
Export
Copy
Refresh
Delete
Simulate Deployment
Deploy
Distribute Content
Move
Set Security Scopes
Categorize
View Relationships
Properties
Feedback
Search
Application
Deployment
Move
Classify
Relationships
Properties
Software Library > Overview > Application Management > Applications
Applications 1 items
Search
Add Criteria
Icon
Name
Deployment Types
Deployments
Status
EGY Office 365 Users
1
1
Active
Overview
Application Management
Applications
License Information for Store Apps
Packages
Approval Requests
Global Conditions
App-V Virtual Environments
Windows Sideloading Keys
Application Management Policies
App Configuration Policies
Software Updates
Operating Systems
Windows 10 Servicing
Assets and Compliance
Software Library
Monitoring
Administration
EGY Office 365 Users
Application Properties
Software Version:
Manufacturer:
Superseded: No
Comments:
Application Statistics
Devices with Application: 0
Devices with Installation Failure: 0
Users with Application: 0
Related Objects
Content Status
Summary
Deployment Types
Deployments


Recycle Bin
Software Center
Microsoft CERTIFIED Trainer
ABDELWAHED
Applications 1
Updates
Operating Systems
Installation status
Device compliance
Options
Applications > Application Details
EGY Office 365 Users
Cancel
Installing...
Status: Downloading (19% complete)
Date published: Not specified
Restart required: Might be required
Download size: 2606 MB
Estimated time: 30 minutes
Total components: 1
3:52 PM
9/6/2019


Recycle Bin
Software Center
Microsoft CERTIFIED Trainer
ABDELWAHED
Applications 1
Updates
Operating Systems
Installation status
Options
Applications > Application Details
EGY Office 365 Users
Cancel
Installing...
Microsoft
Installing Office
3:57 PM
9/6/2019


Recycle Bin
Software Center
Microsoft Certified Trainer
ABDELWAHED
Applications 1
Updates
Operating S
Installation
Device com
Options
Applications > Application Details
Microsoft
You're all set! Office is installed now
Click Start to view your apps.
Close
Installation complete
The software installed successfully. Click to view details.
4:03 PM
9/6/2019


Recycle Bin
Software Center
Microsoft Certified Trainer
ABDELWAHED
Applications 1
Updates
Operating Systems
Installation status
Device compliance
Applications > Application Details
EGY Office 365 Users
Uninstall
Status: Installed
Date published: Not specified
Restart required: Might be required
Download size: 2606 MB
Estimated time: 30 minutes
Total components: 1
View
Sort by
Refresh
Paste
Paste shortcut
New
Display settings
Personalize
Folder
Shortcut
Bitmap image
Contact
Microsoft Word Document
Microsoft PowerPoint Presentation
Rich Text Format
Text Document
Microsoft Visio Drawing
Microsoft Excel Worksheet
4:05 PM
9/6/2019

Removing an Application Using SCCM

Removing an application using System Center Configuration Manager (SCCM) involves several steps to ensure that the application is properly uninstalled from client computers and the associated content is managed appropriately. Here's a detailed guide on how to remove an application using SCCM:

Steps to Remove an Application Using SCCM

1. Create an Uninstall Deployment

1. **Navigate to the SCCM Console**:
   - Open the SCCM console and navigate to Software Library -> Overview -> Application Management -> Applications.
2. **Select the Application**:
   - Locate and select the application you want to remove.
3. **Create an Uninstall Deployment**:
   - Right-click on the application and select Deploy.
   - In the Deploy Software Wizard, select the collection that contains the devices from which you want to uninstall the application.
   - In the Content section, ensure that the content is distributed to the distribution points.
   - In the Deployment Settings section, select Uninstall in the Action dropdown.
   - Configure the scheduling and user experience settings as needed.
   - Complete the wizard to create the uninstall deployment.

2. Monitor the Uninstall Deployment

1. **Navigate to Monitoring**:
   - Go to Monitoring -> Overview -> Deployments.
2. **Check the Status**:
   - Locate the deployment you just created and monitor the status to ensure the application is being uninstalled from the targeted devices.
   - Review the Asset Details tab for detailed information on the success and failure of the uninstallation process.

3. Remove Application from SCCM Console (Optional)

1. **Navigate to Applications**:
   - Go back to Software Library -> Overview -> Application Management -> Applications.
2. **Delete the Application**:
   - Right-click on the application and select Delete.
   - Confirm the deletion to remove the application from the SCCM console. Note that this step will remove the application metadata from SCCM, but not from the distribution points.

4. Remove Content from Distribution Points (Optional)

1. **Navigate to Content Locations**:
   - Go to Monitoring -> Overview -> Distribution Status -> Content Status.
2. **Select the Application Content**:
   - Locate the content associated with the application you deleted.

---

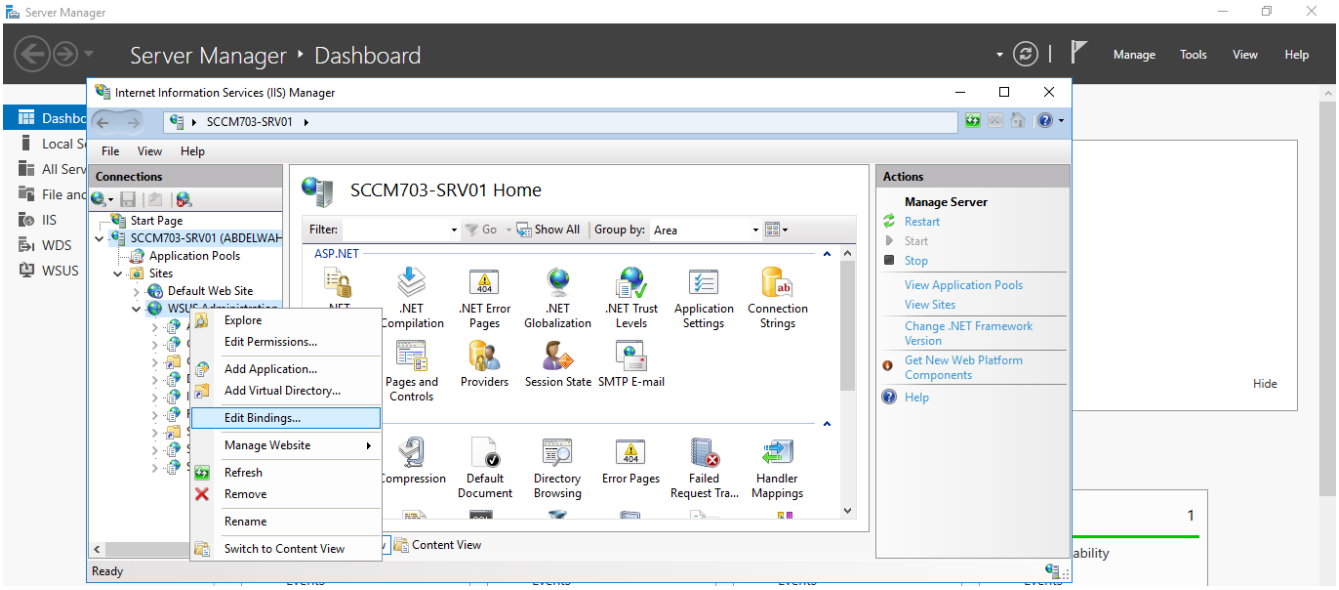
3. **Remove the Content**:
    - Right-click on the content and select Remove to delete it from the distribution points.
    - Confirm the removal.

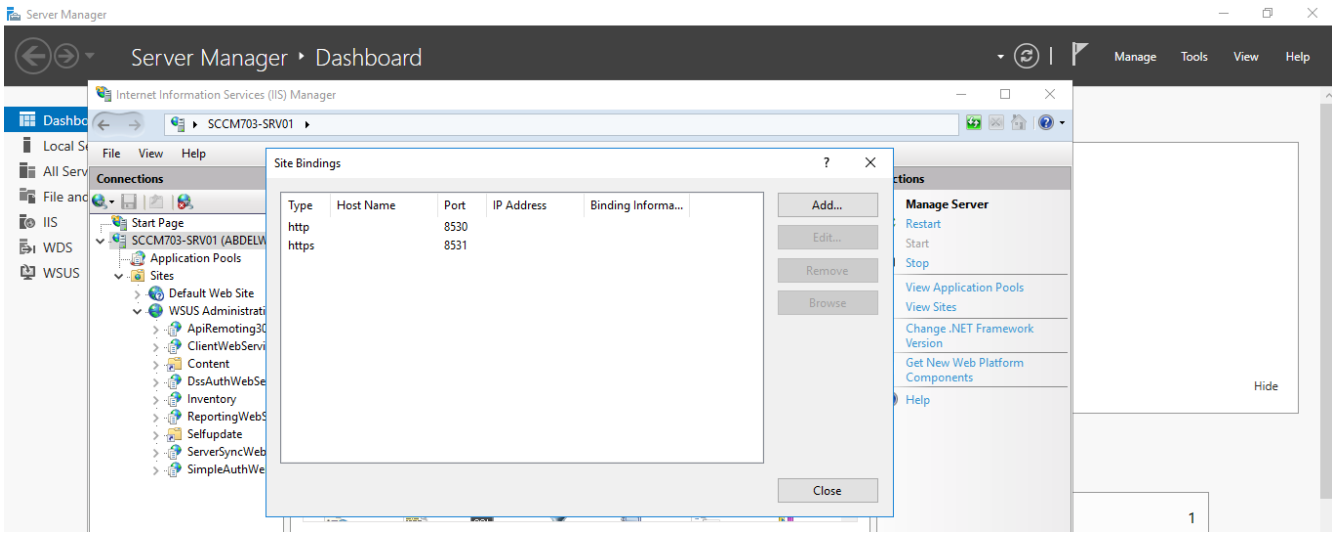
Example Scenario: Uninstalling Microsoft Office

1. **Create an Uninstall Deployment for Microsoft Office**:
    - Navigate to Software Library -> Overview -> Application Management -> Applications.
    - Select Microsoft Office and right-click to Deploy.
    - Choose the collection of devices from which you want to uninstall Microsoft Office.
    - In the Deploy Software Wizard, set Action to Uninstall.
    - Configure other settings as needed and complete the wizard.
2. **Monitor the Uninstall Process**:
    - Navigate to Monitoring -> Overview -> Deployments.
    - Monitor the deployment status to ensure Microsoft Office is being uninstalled.
3. **Remove Application from SCCM Console (Optional)**:
    - Navigate to Software Library -> Overview -> Application Management -> Applications.
    - Right-click Microsoft Office and select Delete.
4. **Remove Content from Distribution Points (Optional)**:
    - Navigate to Monitoring -> Overview -> Distribution Status -> Content Status.
    - Locate the content for Microsoft Office, right-click, and select Remove.

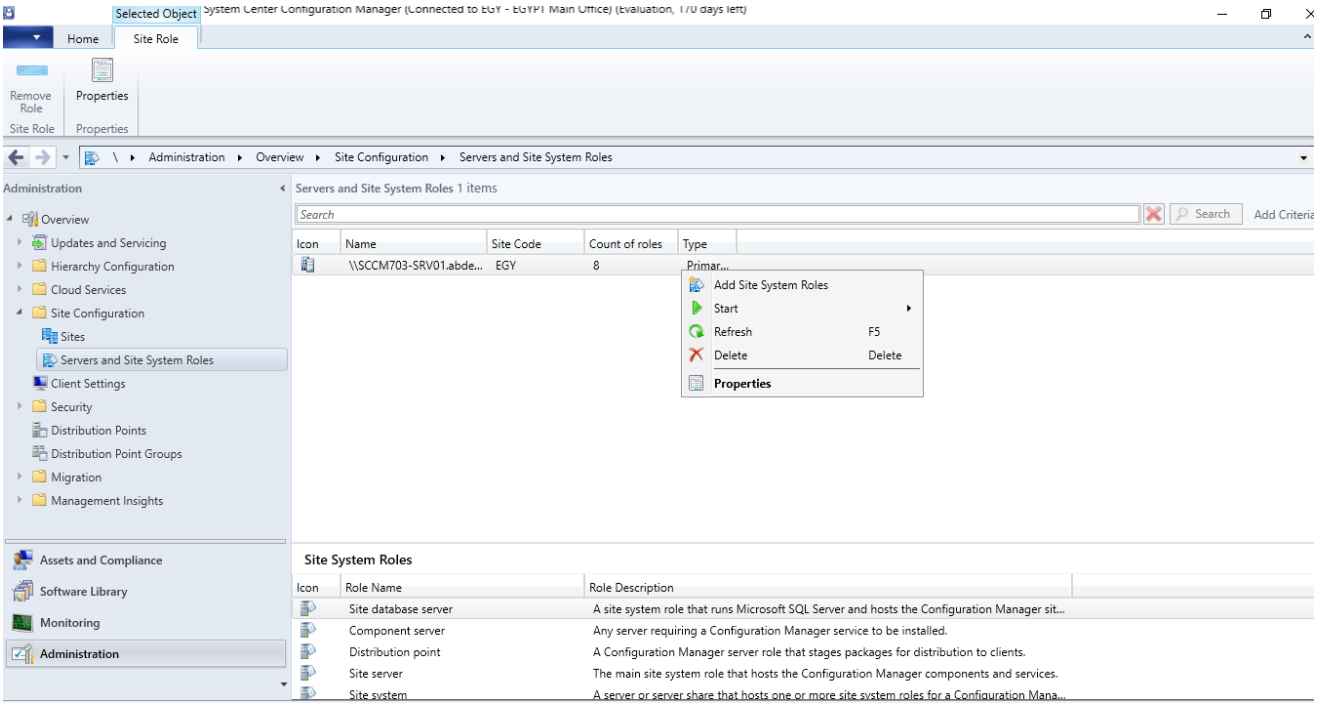
Install and configure a software update point

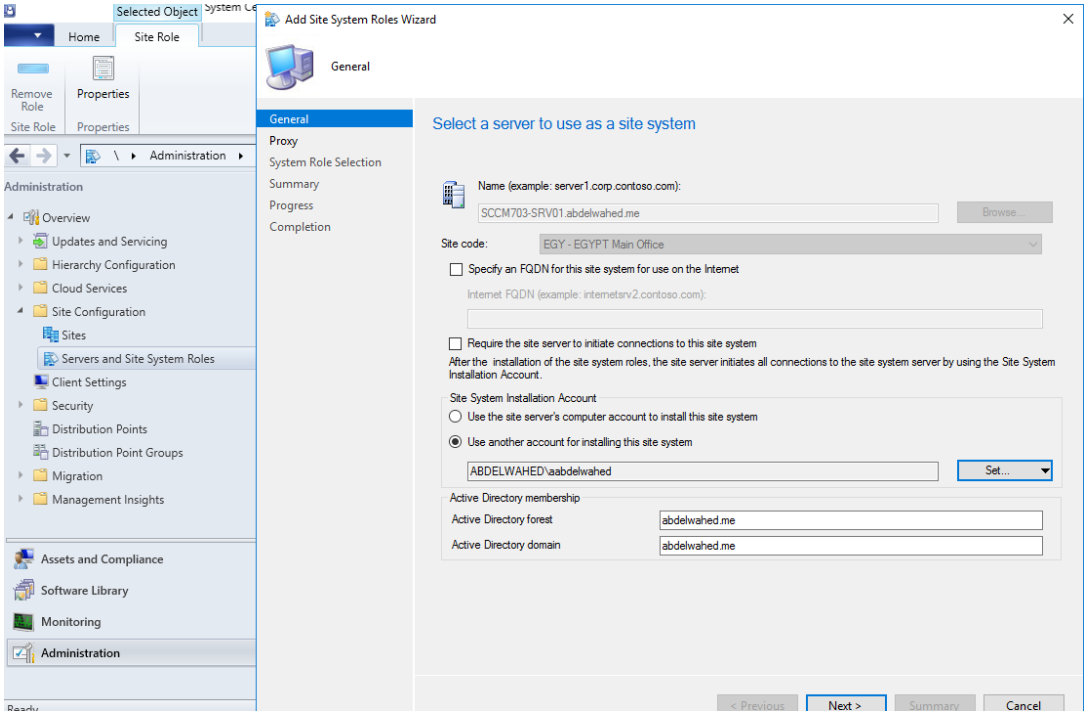
When setting up a software update point in SCCM, it's essential to be aware of the HTTP and HTTPS ports your WSUS server uses. To find these ports, open the WSUS Administration Console, go to "Update Source and Proxy Server" settings, and note the ports specified for the upstream server and proxy server updates. Typically, WSUS uses port 8530 for HTTP and 8531 for HTTPS by default.

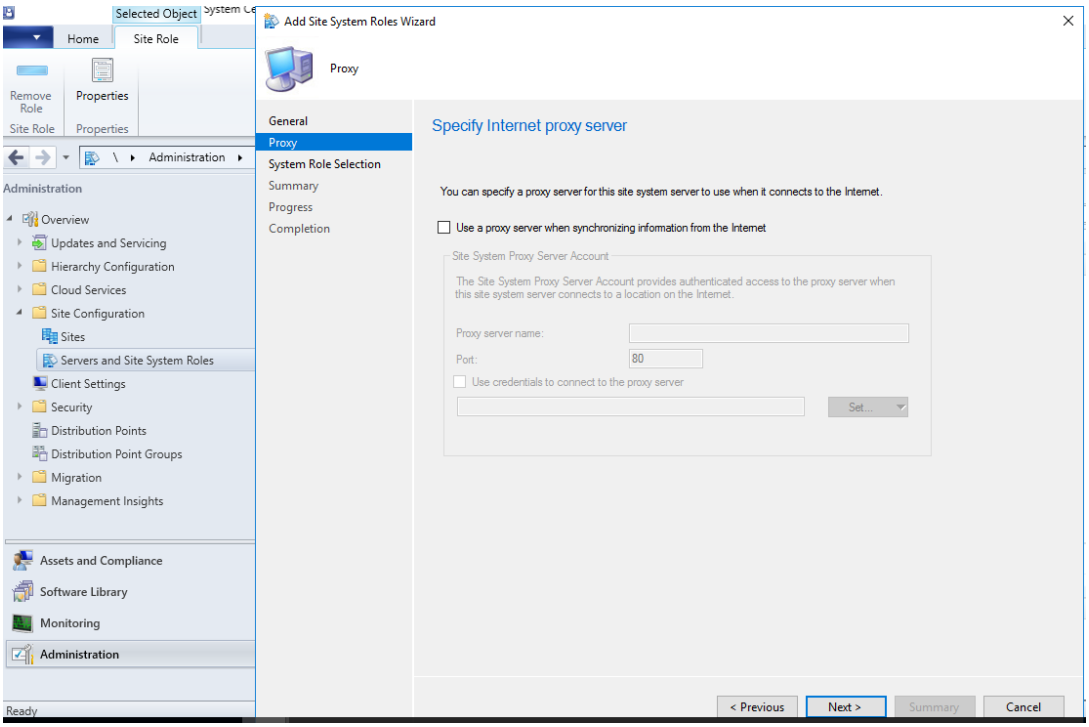


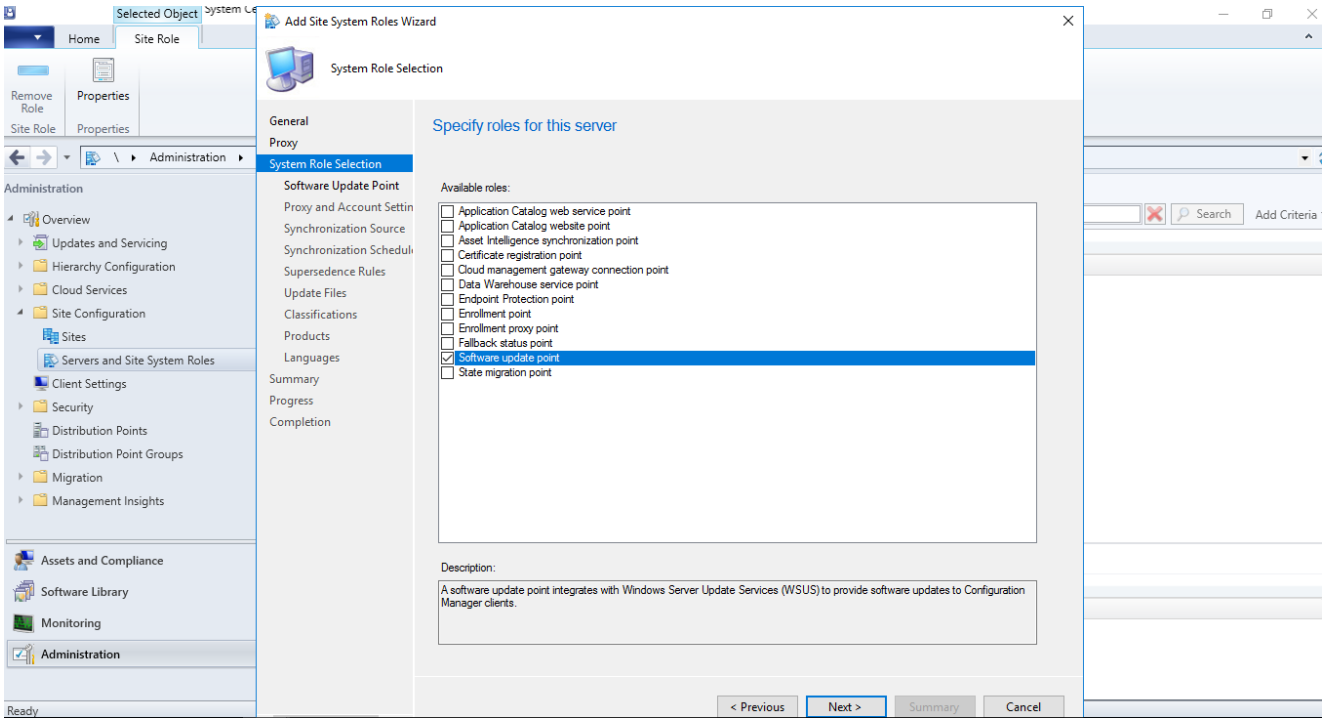


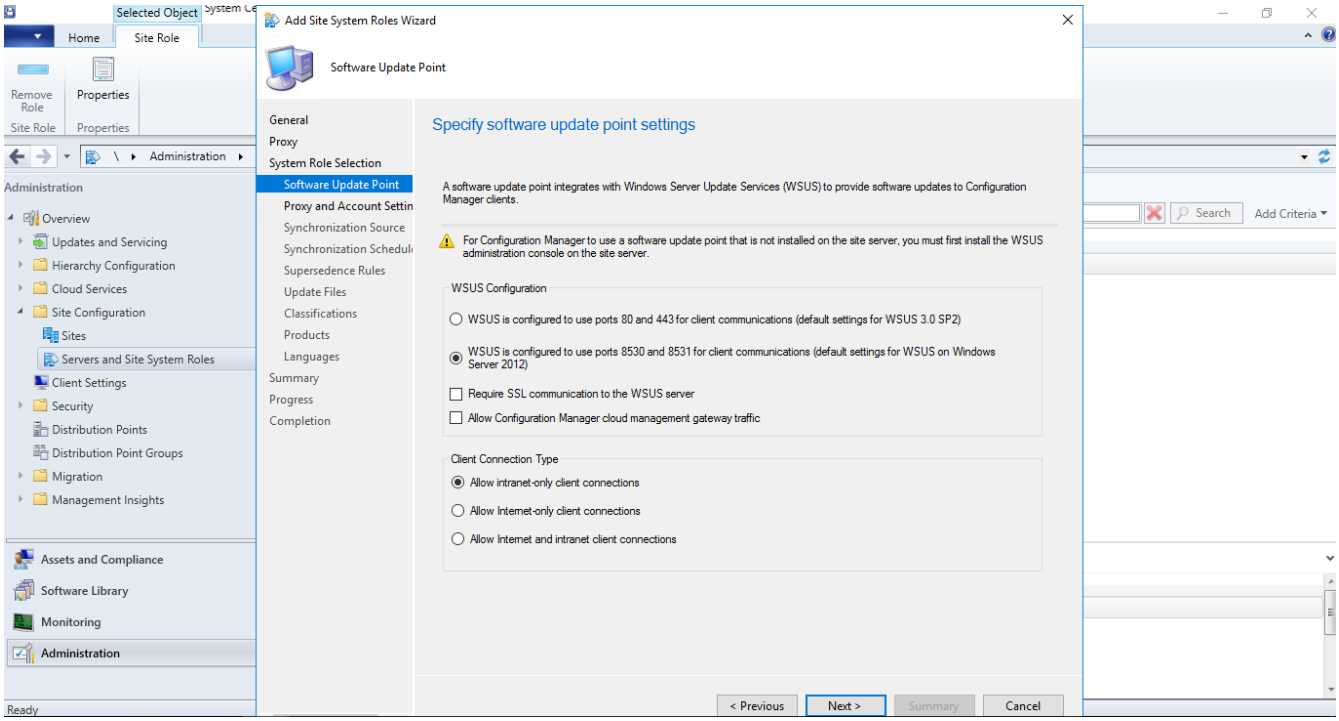
Add site role (software update point)

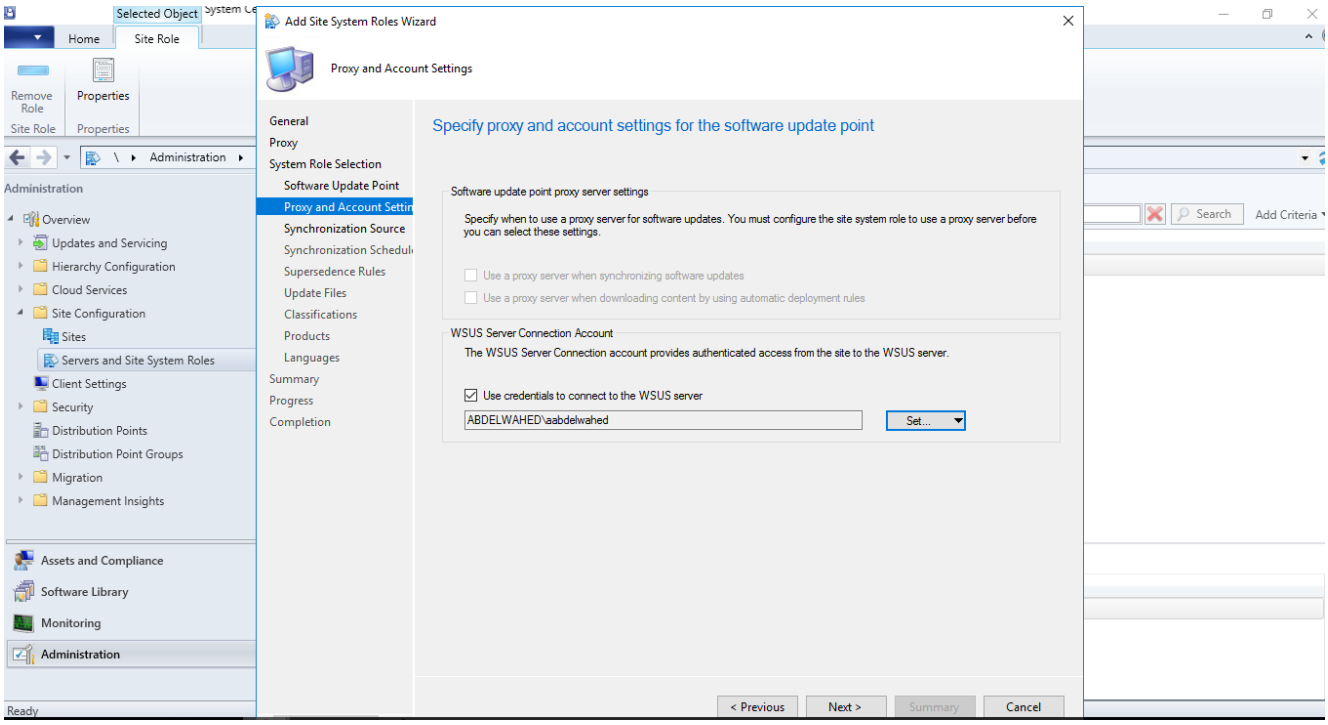


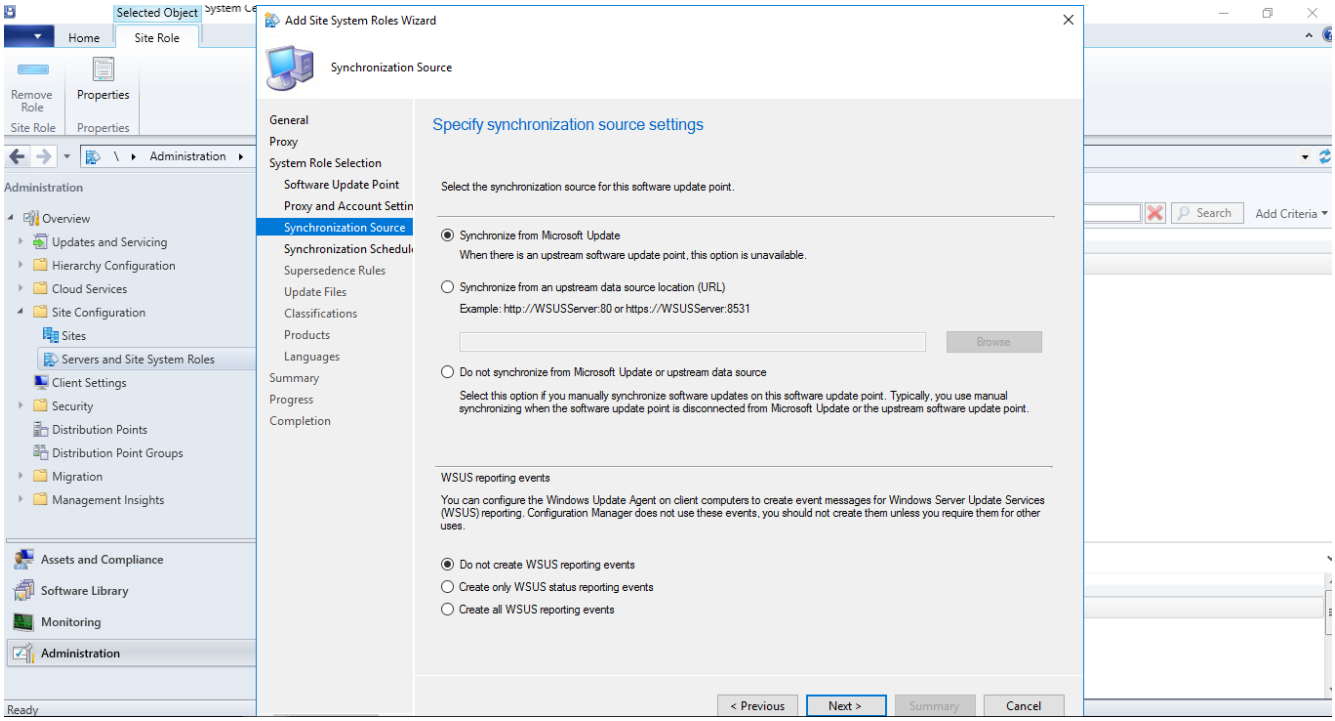


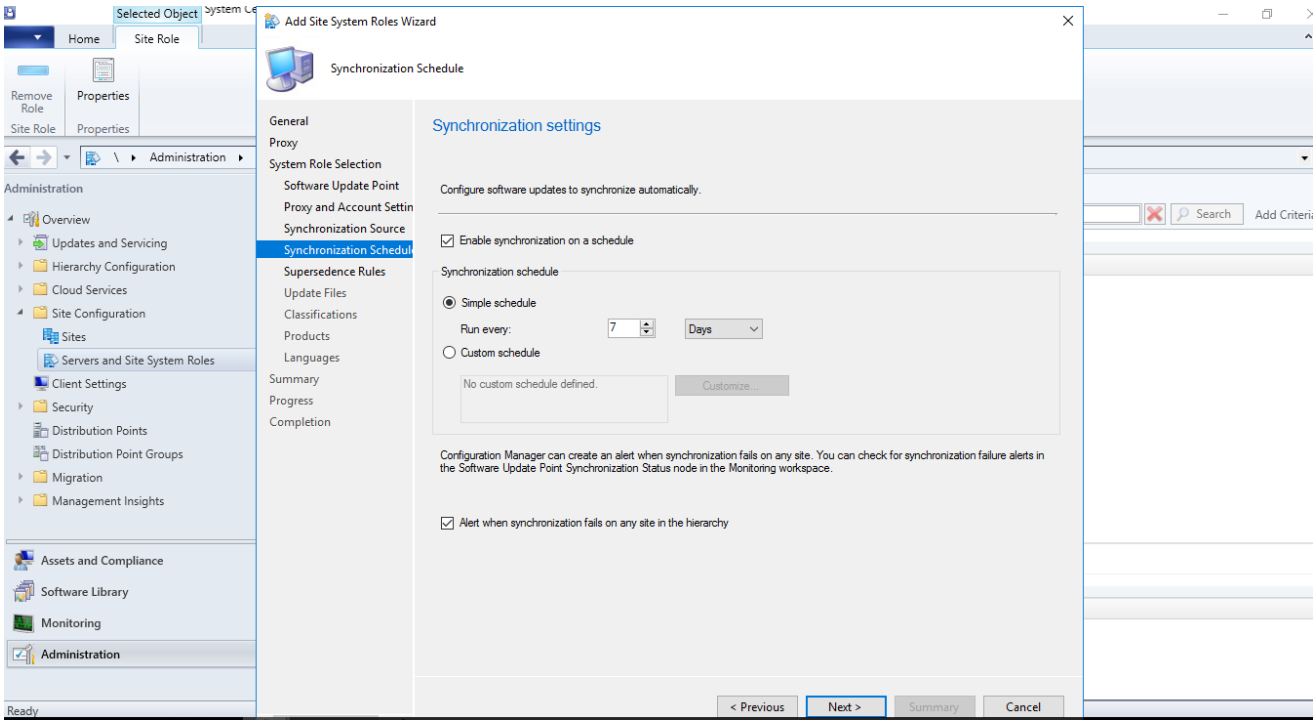

Selected Object
Home
Site Role
Remove Role
Properties
Site Role
Properties
Administration
Overview
Updates and Servicing
Hierarchy Configuration
Cloud Services
Site Configuration
Sites
Servers and Site System Roles
Client Settings
Security
Distribution Points
Distribution Point Groups
Migration
Management Insights
Assets and Compliance
Software Library
Monitoring
Administration
Ready
Add Site System Roles Wizard
Proxy
General
Proxy
System Role Selection
Summary
Progress
Completion
Specify Internet proxy server
You can specify a proxy server for this site system server to use when it connects to the Internet.
Use a proxy server when synchronizing information from the Internet
Site System Proxy Server Account
The Site System Proxy Server Account provides authenticated access to the proxy server when this site system server connects to a location on the Internet.
Proxy server name:
Port:
80
Use credentials to connect to the proxy server
Set...
< Previous
Next >
Summary
Cancel

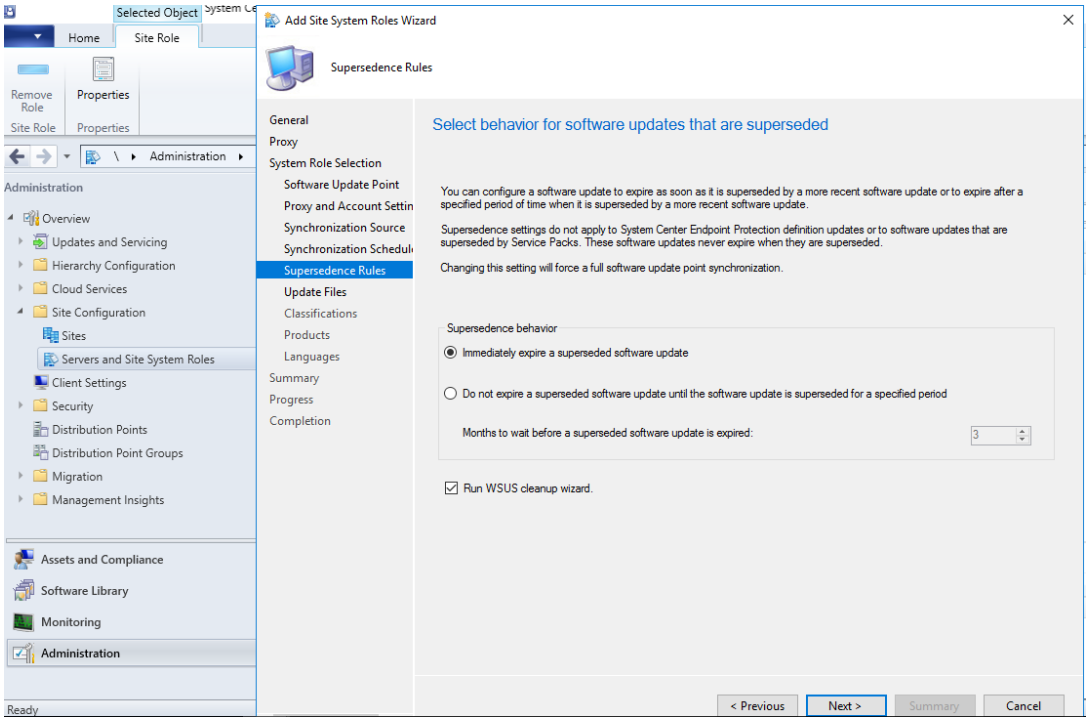

Selected Object
Home
Site Role
Remove Role
Properties
Site Role
Properties
Administration
Overview
Updates and Servicing
Hierarchy Configuration
Cloud Services
Site Configuration
Sites
Servers and Site System Roles
Client Settings
Security
Distribution Points
Distribution Point Groups
Migration
Management Insights
Assets and Compliance
Software Library
Monitoring
Administration
Ready
Add Site System Roles Wizard
System Role Selection
General
Proxy
System Role Selection
Software Update Point
Proxy and Account Settin
Synchronization Source
Synchronization Schedul
Supersedence Rules
Update Files
Classifications
Products
Languages
Summary
Progress
Completion
Specify roles for this server
Available roles:
Application Catalog web service point
Application Catalog website point
Asset Intelligence synchronization point
Certificate registration point
Cloud management gateway connection point
Data Warehouse service point
Endpoint Protection point
Enrollment point
Enrollment proxy point
Fallback status point
Software update point
State migration point
Description:
A software update point integrates with Windows Server Update Services (WSUS) to provide software updates to Configuration Manager clients.
< Previous
Next >
Summary
Cancel
Search
Add Criteria

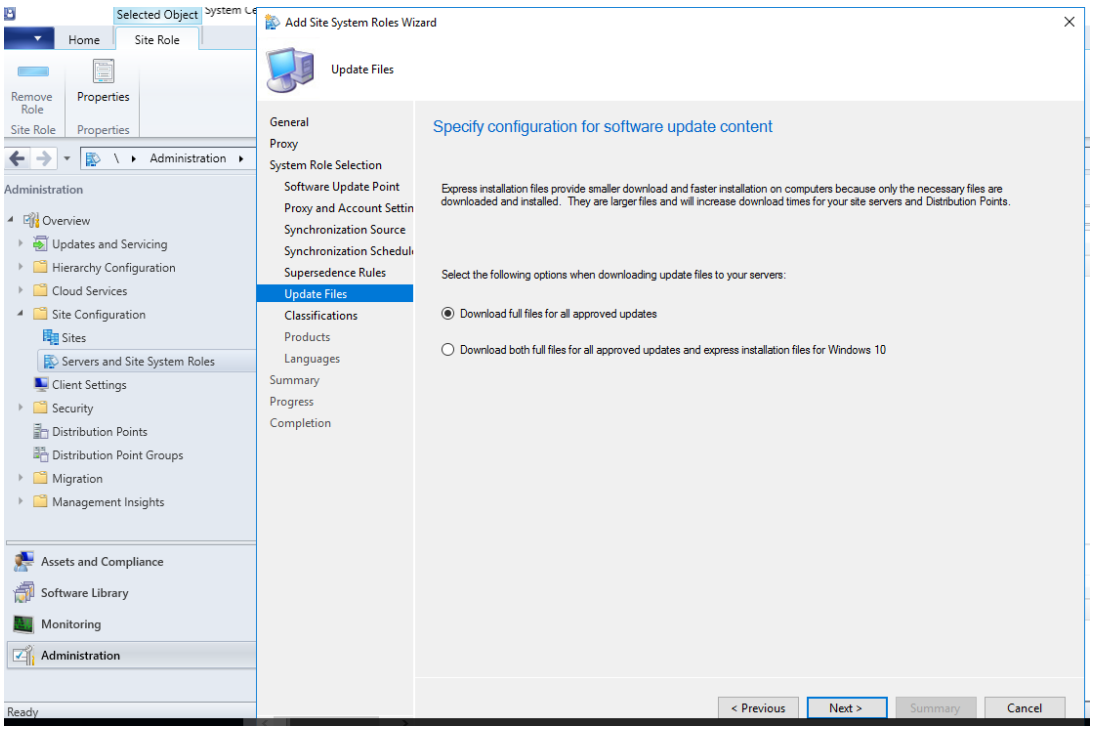

Add Site System Roles Wizard
Software Update Point
General
Proxy
System Role Selection
Software Update Point
Proxy and Account Settin
Synchronization Source
Synchronization Schedul
Supersedence Rules
Update Files
Classifications
Products
Languages
Summary
Progress
Completion
Specify software update point 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
Allow Configuration Manager cloud management gateway traffic
Client Connection Type
Allow intranet-only client connections
Allow Internet-only client connections
Allow Internet and intranet client connections
< Previous
Next >
Summary
Cancel

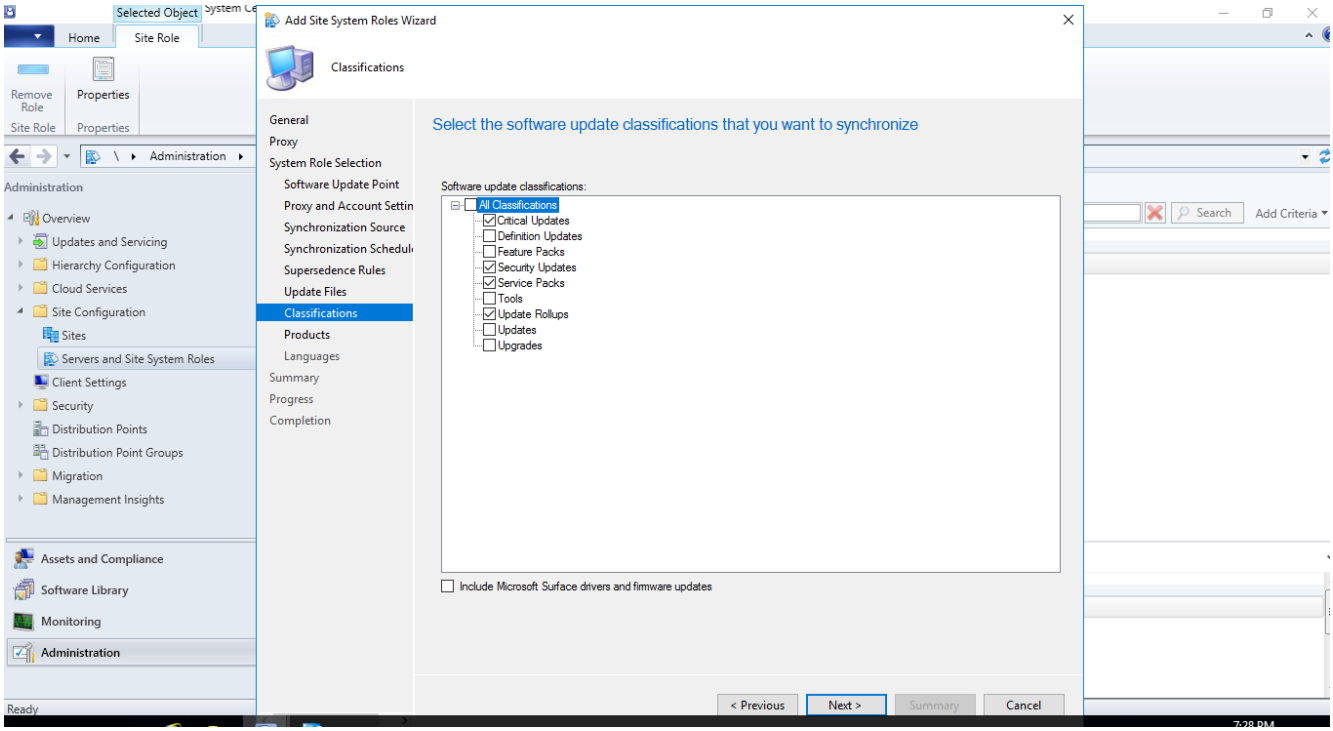

Add Site System Roles Wizard
Proxy and Account Settings
General
Proxy
System Role Selection
Software Update Point
Proxy and Account Settin
Synchronization Source
Synchronization Schedul
Supersedence Rules
Update Files
Classifications
Products
Languages
Summary
Progress
Completion
Specify proxy and account settings for the software update point
Software update point proxy server settings
Specify when to use a proxy server for software updates. You must configure the site system role to use a proxy server before you can select these settings.
Use a proxy server when synchronizing software updates
Use a proxy server when downloading content by using automatic deployment rules
WSUS Server Connection Account
The WSUS Server Connection account provides authenticated access from the site to the WSUS server.
Use credentials to connect to the WSUS server
ABDELWAHED\aabdelwahed
Set...
< Previous
Next >
Summary
Cancel

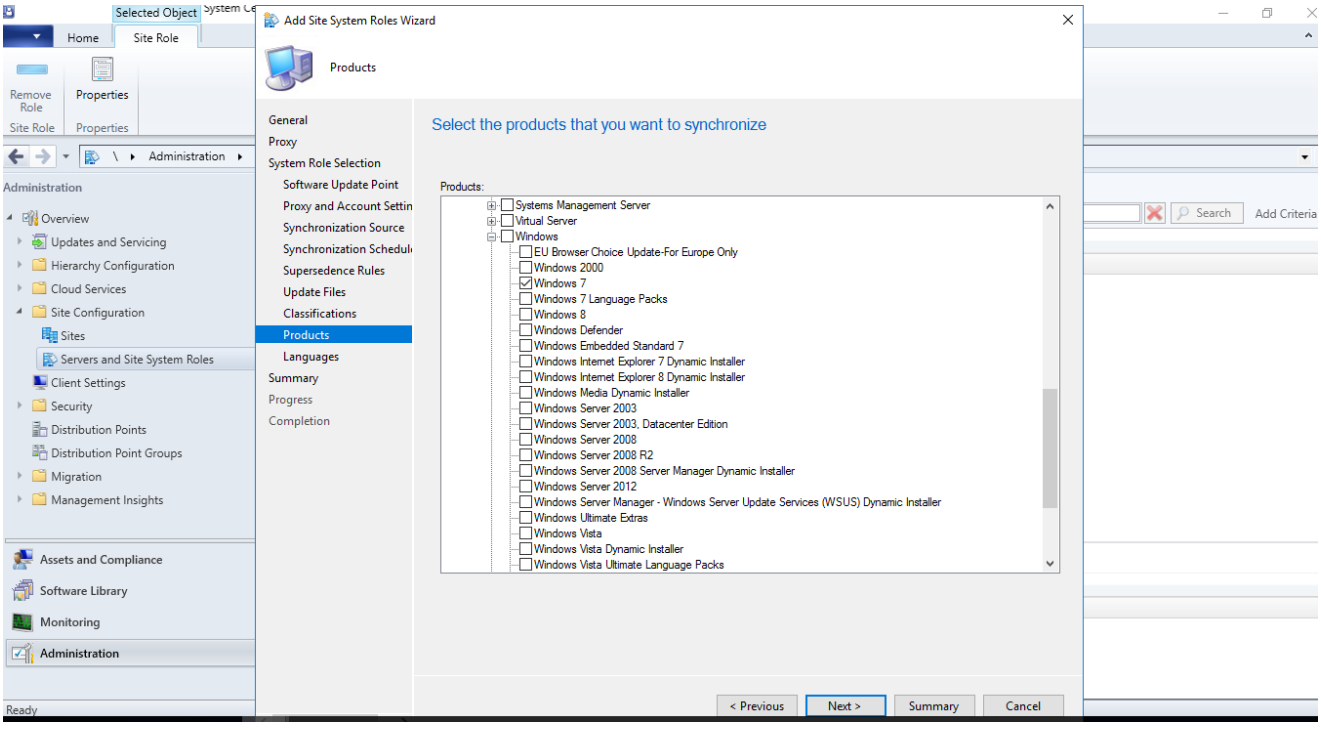

Add Site System Roles Wizard
Synchronization Source
General
Proxy
System Role Selection
Software Update Point
Proxy and Account Settin
Synchronization Source
Synchronization Schedul
Supersedence Rules
Update Files
Classifications
Products
Languages
Summary
Progress
Completion
Specify synchronization 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
< Previous
Next >
Summary
Cancel
Selected Object
Home
Site Role
Remove Role
Properties
Site Role
Properties
Administration
Overview
Updates and Servicing
Hierarchy Configuration
Cloud Services
Site Configuration
Sites
Servers and Site System Roles
Client Settings
Security
Distribution Points
Distribution Point Groups
Migration
Management Insights
Assets and Compliance
Software Library
Monitoring
Administration
Ready
Search
Add Criteria

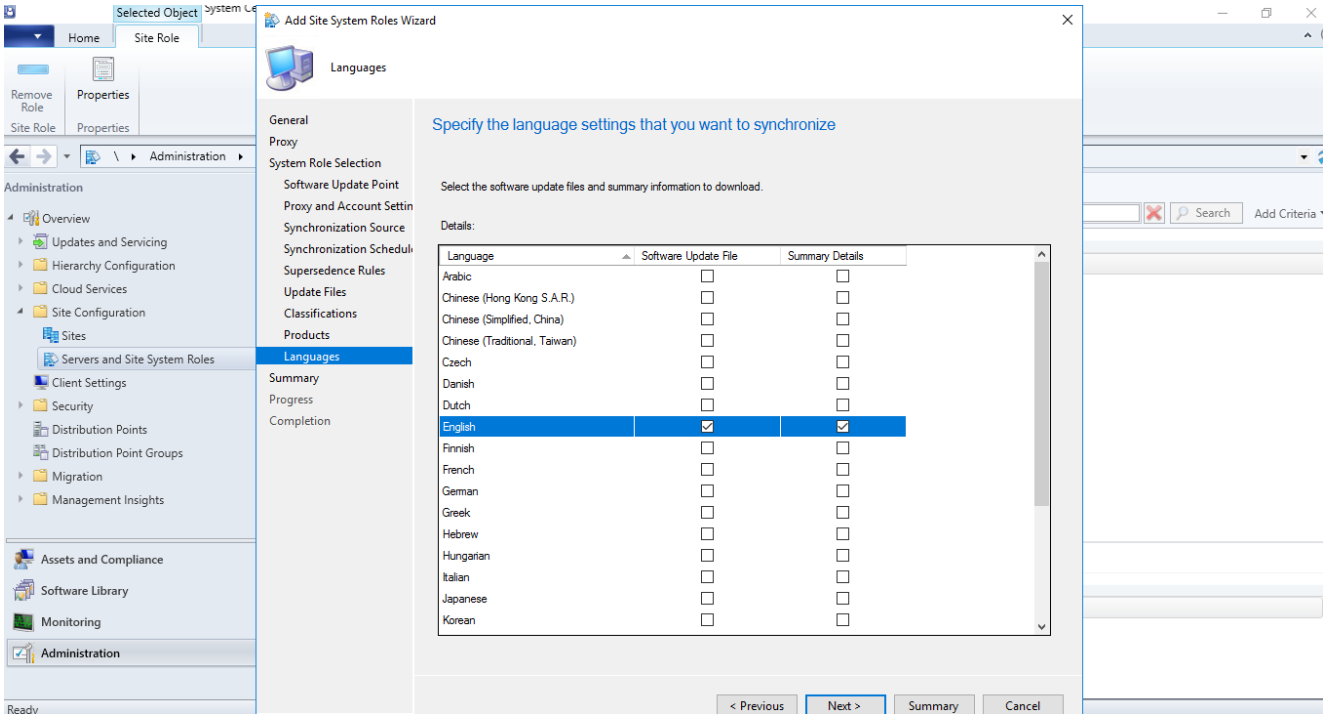

Add Site System Roles Wizard
Synchronization Schedule
General
Proxy
System Role Selection
Software Update Point
Proxy and Account Settin
Synchronization Source
Synchronization Schedul
Supersedence Rules
Update Files
Classifications
Products
Languages
Summary
Progress
Completion
Synchronization settings
Configure software updates to synchronize automatically.
Enable synchronization on a schedule
Synchronization schedule
Simple schedule
Run every:
7
Days
Custom schedule
No custom schedule defined.
Customize...
Configuration Manager can create an alert when synchronization fails on any site. You can check for synchronization failure alerts in the Software Update Point Synchronization Status node in the Monitoring workspace.
Alert when synchronization fails on any site in the hierarchy
< Previous
Next >
Summary
Cancel
Selected Object
Home
Site Role
Remove Role
Properties
Site Role
Properties
Administration
Overview
Updates and Servicing
Hierarchy Configuration
Cloud Services
Site Configuration
Sites
Servers and Site System Roles
Client Settings
Security
Distribution Points
Distribution Point Groups
Migration
Management Insights
Assets and Compliance
Software Library
Monitoring
Administration
Ready
Search
Add Criteria

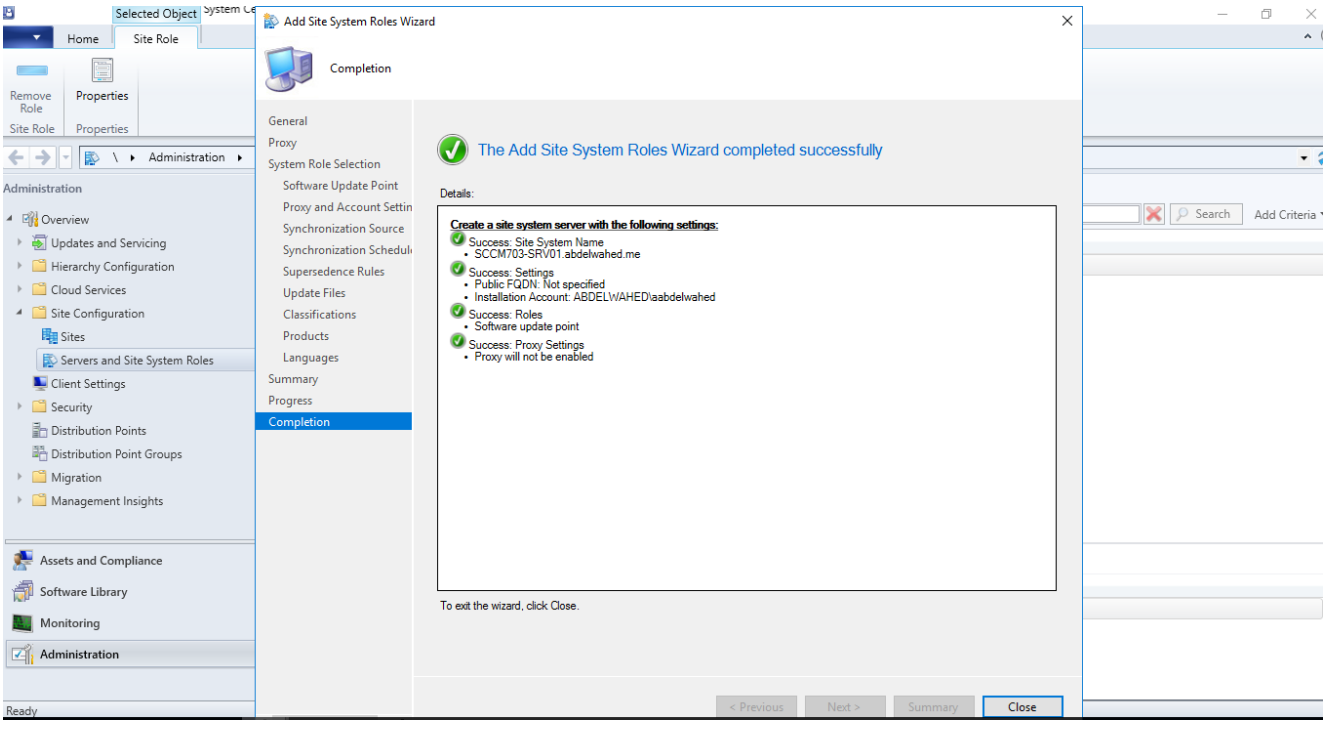

Selected Object
Home
Site Role
Remove Role
Properties
Site Role
Properties
Administration
Administration
Overview
Updates and Servicing
Hierarchy Configuration
Cloud Services
Site Configuration
Sites
Servers and Site System Roles
Client Settings
Security
Distribution Points
Distribution Point Groups
Migration
Management Insights
Assets and Compliance
Software Library
Monitoring
Administration
Ready
Add Site System Roles Wizard
Supersedence Rules
General
Proxy
System Role Selection
Software Update Point
Proxy and Account Settin
Synchronization Source
Synchronization Schedul
Supersedence Rules
Update Files
Classifications
Products
Languages
Summary
Progress
Completion
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.
< Previous
Next >
Summary
Cancel


Selected Object
Home
Site Role
Remove Role
Properties
Site Role
Properties
Administration
Administration
Overview
Updates and Servicing
Hierarchy Configuration
Cloud Services
Site Configuration
Sites
Servers and Site System Roles
Client Settings
Security
Distribution Points
Distribution Point Groups
Migration
Management Insights
Assets and Compliance
Software Library
Monitoring
Administration
Ready
Add Site System Roles Wizard
Update Files
General
Proxy
System Role Selection
Software Update Point
Proxy and Account Settin
Synchronization Source
Synchronization Schedul
Supersedence Rules
Update Files
Classifications
Products
Languages
Summary
Progress
Completion
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
< Previous
Next >
Summary
Cancel

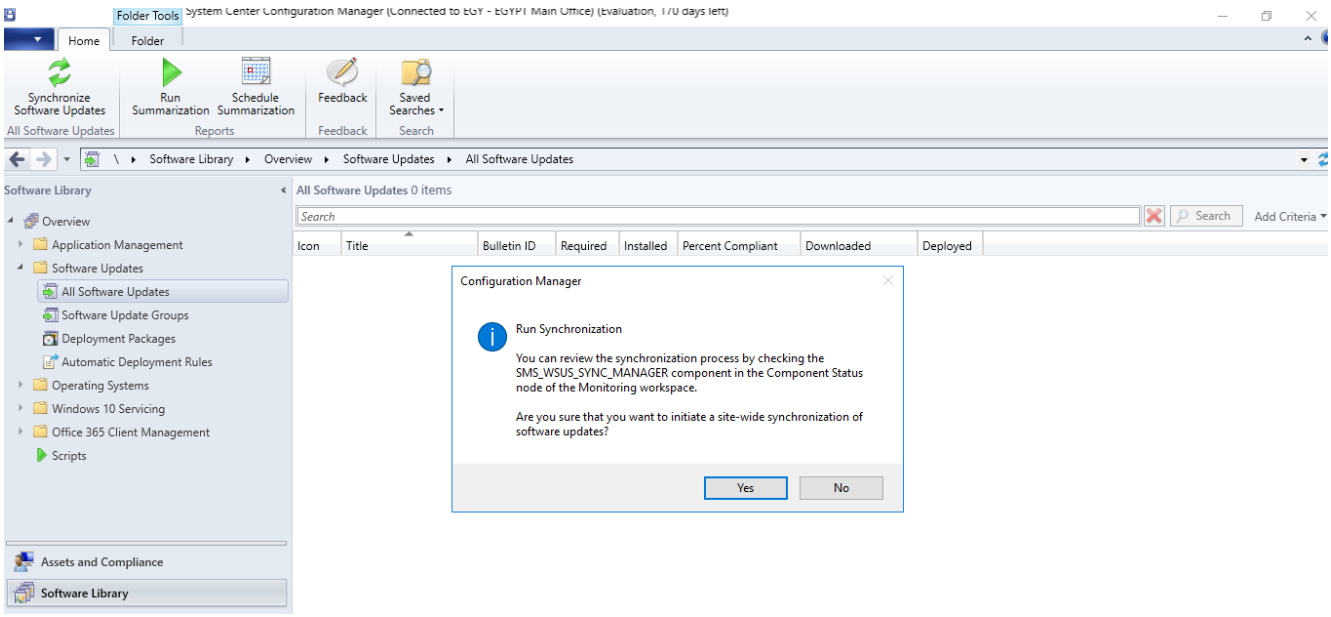

Add Site System Roles Wizard
Classifications
Select the software update classifications that you want to synchronize
Software update classifications:
All Classifications
Critical Updates
Definition Updates
Feature Packs
Security Updates
Service Packs
Tools
Update Rollups
Updates
Upgrades
Include Microsoft Surface drivers and firmware updates
General
Proxy
System Role Selection
Software Update Point
Proxy and Account Settin
Synchronization Source
Synchronization Schedul
Supersedence Rules
Update Files
Classifications
Products
Languages
Summary
Progress
Completion
< Previous
Next >
Summary
Cancel


Add Site System Roles Wizard
Products
Select the products that you want to synchronize
Products:
Systems Management Server
Virtual Server
Windows
EU Browser Choice Update-For Europe Only
Windows 2000
Windows 7
Windows 7 Language Packs
Windows 8
Windows Defender
Windows Embedded Standard 7
Windows Internet Explorer 7 Dynamic Installer
Windows Internet Explorer 8 Dynamic Installer
Windows Media Dynamic Installer
Windows Server 2003
Windows Server 2003, Datacenter Edition
Windows Server 2008
Windows Server 2008 R2
Windows Server 2008 Server Manager Dynamic Installer
Windows Server 2012
Windows Server Manager - Windows Server Update Services (WSUS) Dynamic Installer
Windows Ultimate Extras
Windows Vista
Windows Vista Dynamic Installer
Windows Vista Ultimate Language Packs
General
Proxy
System Role Selection
Software Update Point
Proxy and Account Settin
Synchronization Source
Synchronization Schedul
Supersedence Rules
Update Files
Classifications
Products
Languages
Summary
Progress
Completion
< Previous
Next >
Summary
Cancel


Add Site System Roles Wizard
Languages
Specify the language settings that you want to synchronize
Select the software update files and summary information to download.
Details:
Language
Software Update File
Summary Details
Arabic
Chinese (Hong Kong S.A.R.)
Chinese (Simplified, China)
Chinese (Traditional, Taiwan)
Czech
Danish
Dutch
English
Finnish
French
German
Greek
Hebrew
Hungarian
Italian
Japanese
Korean
General
Proxy
System Role Selection
Software Update Point
Proxy and Account Settin
Synchronization Source
Synchronization Schedul
Supersedence Rules
Update Files
Classifications
Products
Languages
Summary
Progress
Completion
< Previous
Next >
Summary
Cancel


Add Site System Roles Wizard
Completion
The Add Site System Roles Wizard completed successfully
Details:
Create a site system server with the following settings:
Success: Site System Name
SCCM703-SRV01.abdelwahed.me
Success: Settings
Public FQDN: Not specified
Installation Account: ABDELWAHED\aabdelwahed
Success: Roles
Software update point
Success: Proxy Settings
Proxy will not be enabled
To exit the wizard, click Close.
Close

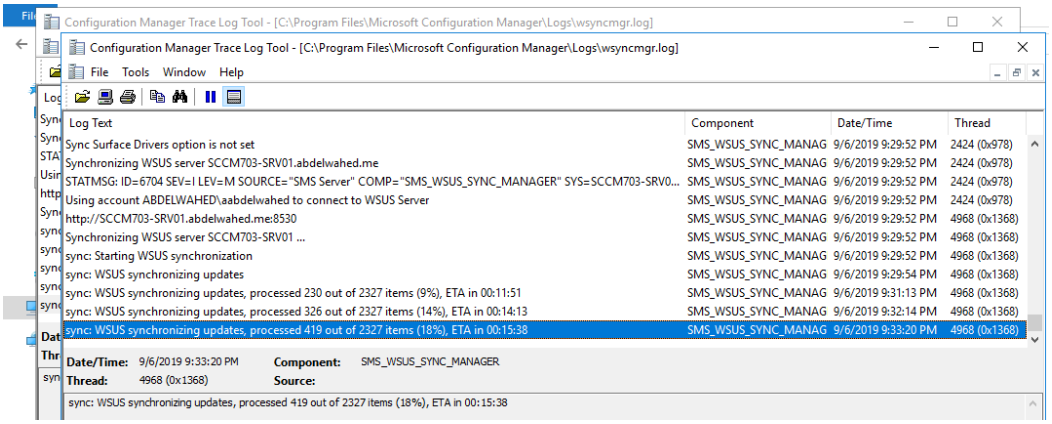
Now Synchronize Software Updates

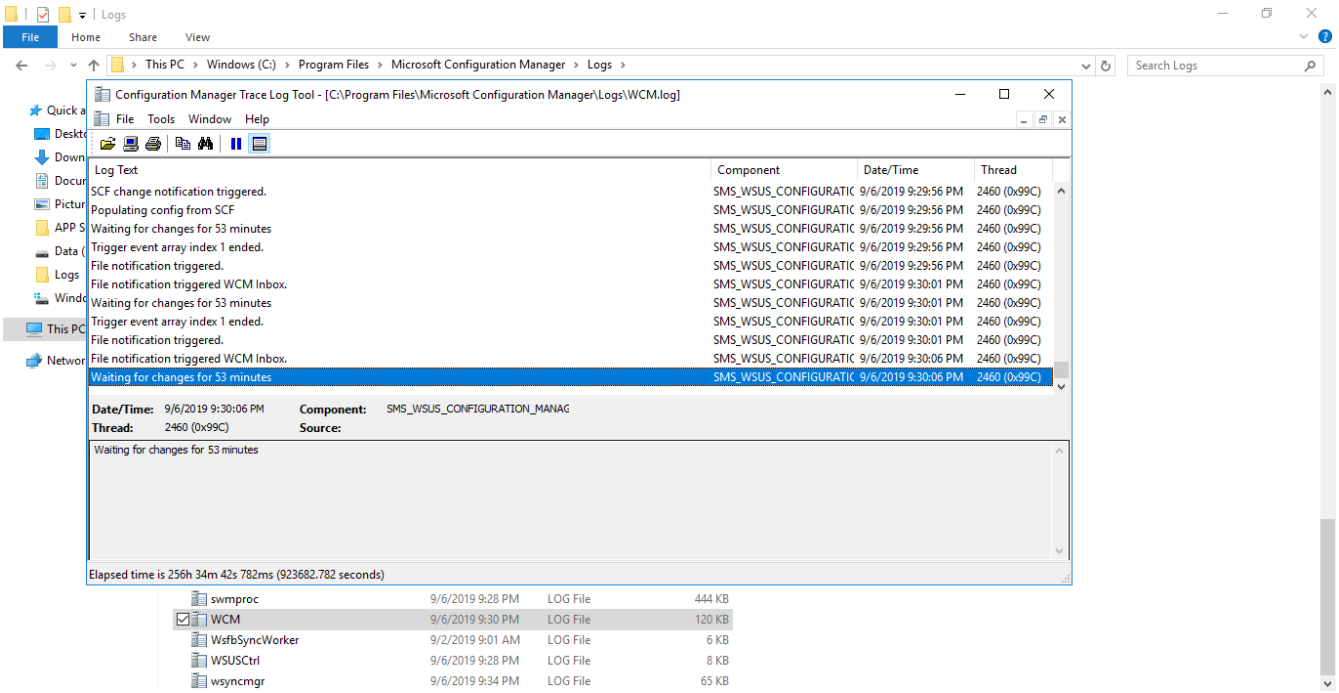


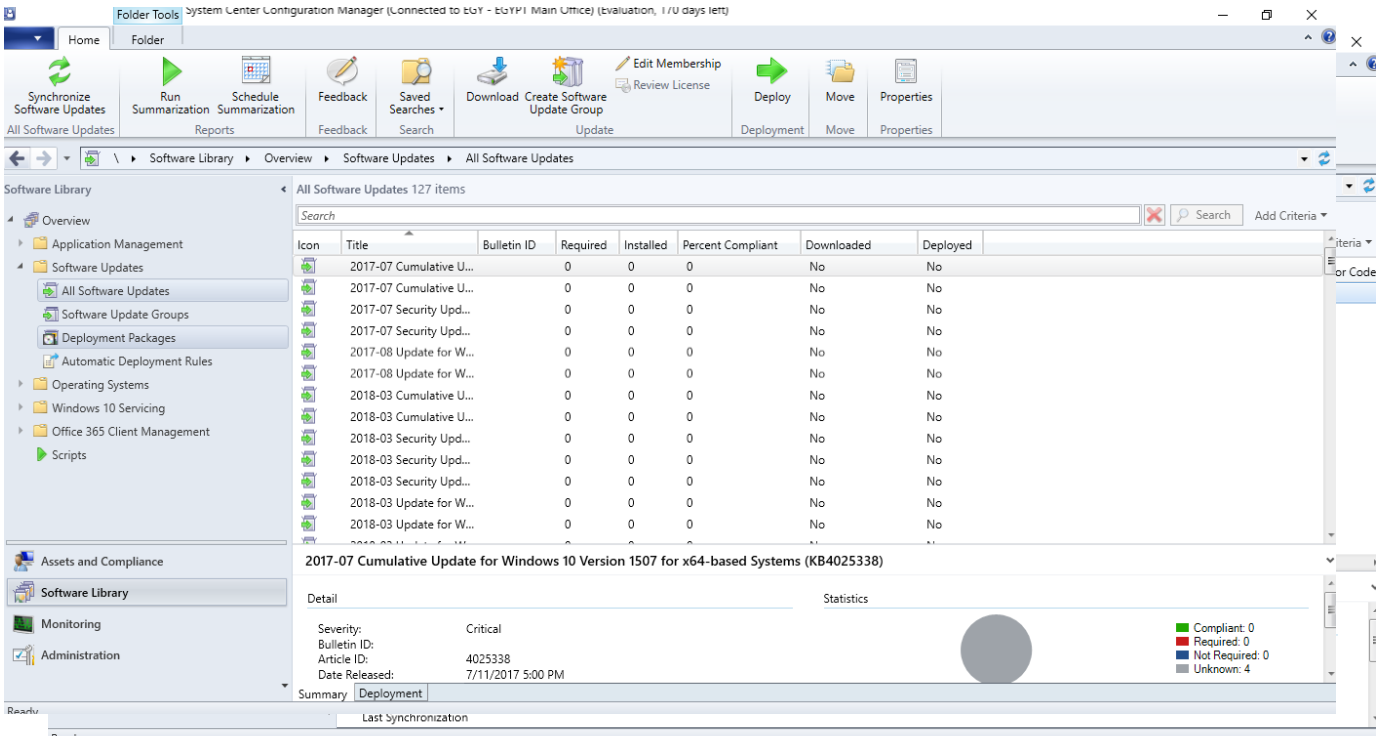
Once you've set up the software update point with Configuration Manager, monitor the sync progress of software updates by heading to the Monitoring workspace and clicking on the Software Update Points Synchronization Status node. You'll see how the synchronization is going, along with any errors or alerts that might have popped up.

Besides checking the sync status, you should examine the logs in the C:\Program Files\Microsoft Configuration Manager\Logs directory to resolve problems. The wsyncmgr.log details the sync process and records errors or warnings, while the WCM.log reports on software update point configurations and modifications.

Examining these records can assist in pinpointing potential complications in the software update point setup, including troubles with connection, authorization dilemmas, or disruptions in sync. Recognizing these problems allows you to take suitable measures to rectify them, confirming that the software update point is accurately configured and functioning efficiently.




Logs
File Home Share View
This PC › Windows (C:) › Program Files › Microsoft Configuration Manager › Logs ›
Search Logs
Configuration Manager Trace Log Tool - [C:\Program Files\Microsoft Configuration Manager\Logs\WCM.log]
File Tools Window Help
Log Text Component Date/Time Thread
SCF change notification triggered. SMS_WSUS_CONFIGURATIC 9/6/2019 9:29:56 PM 2460 (0x99C)
Populating config from SCF SMS_WSUS_CONFIGURATIC 9/6/2019 9:29:56 PM 2460 (0x99C)
Waiting for changes for 53 minutes SMS_WSUS_CONFIGURATIC 9/6/2019 9:29:56 PM 2460 (0x99C)
Trigger event array index 1 ended. SMS_WSUS_CONFIGURATIC 9/6/2019 9:29:56 PM 2460 (0x99C)
File notification triggered. SMS_WSUS_CONFIGURATIC 9/6/2019 9:29:56 PM 2460 (0x99C)
File notification triggered WCM Inbox. SMS_WSUS_CONFIGURATIC 9/6/2019 9:30:01 PM 2460 (0x99C)
Waiting for changes for 53 minutes SMS_WSUS_CONFIGURATIC 9/6/2019 9:30:01 PM 2460 (0x99C)
Trigger event array index 1 ended. SMS_WSUS_CONFIGURATIC 9/6/2019 9:30:01 PM 2460 (0x99C)
File notification triggered. SMS_WSUS_CONFIGURATIC 9/6/2019 9:30:01 PM 2460 (0x99C)
File notification triggered WCM Inbox. SMS_WSUS_CONFIGURATIC 9/6/2019 9:30:06 PM 2460 (0x99C)
Waiting for changes for 53 minutes SMS_WSUS_CONFIGURATIC 9/6/2019 9:30:06 PM 2460 (0x99C)
Date/Time: 9/6/2019 9:30:06 PM Component: SMS_WSUS_CONFIGURATION_MANAG
Thread: 2460 (0x99C) Source:
Waiting for changes for 53 minutes
Elapsed time is 256h 34m 42s 782ms (923682.782 seconds)
swmproc 9/6/2019 9:28 PM LOG File 444 KB
WCM 9/6/2019 9:30 PM LOG File 120 KB
WsfbSyncWorker 9/2/2019 9:01 AM LOG File 6 KB
WSUSCtrl 9/6/2019 9:28 PM LOG File 8 KB
wsyncmgr 9/6/2019 9:34 PM LOG File 65 KB


Folder Tools
Home Folder
Synchronize Software Updates
Run Summarization
Schedule Summarization
Feedback
Saved Searches
Download
Create Software Update Group
Edit Membership
Review License
Deploy
Move
Properties
All Software Updates
Reports
Feedback
Search
Update
Deployment
Move
Properties
Software Library › Overview › Software Updates › All Software Updates
Software Library
Overview
Application Management
Software Updates
All Software Updates
Software Update Groups
Deployment Packages
Automatic Deployment Rules
Operating Systems
Windows 10 Servicing
Office 365 Client Management
Scripts
Assets and Compliance
Software Library
Monitoring
Administration
All Software Updates 127 items
Search
Add Criteria
Icon Title Bulletin ID Required Installed Percent Compliant Downloaded Deployed
2017-07 Cumulative U... 0 0 0 No No
2017-07 Security Upd... 0 0 0 No No
2017-08 Update for W... 0 0 0 No No
2018-03 Cumulative U... 0 0 0 No No
2018-03 Security Upd... 0 0 0 No No
2018-03 Update for W... 0 0 0 No No
2017-07 Cumulative Update for Windows 10 Version 1507 for x64-based Systems (KB4025338)
Detail
Severity: Critical
Bulletin ID:
Article ID: 4025338
Date Released: 7/11/2017 5:00 PM
Statistics
Compliant: 0
Required: 0
Not Required: 0
Unknown: 4
Summary Deployment
Ready
Last Synchronization

Steps to Create and Deploy Software Update Packages in SCCM

Applying software updates in SCCM involves creating a deployment package and specifying which updates should be included in the deployment. Here's a step-by-step guide to creating a software update deployment:

1. Navigate to Software Updates

- Open the Configuration Manager console.
- Navigate to Software Library -> Software Updates.

2. Select Updates for Deployment

- Use criteria such as product, classification, or severity to select the updates you want to deploy.
- Alternatively, create a custom search query to find specific updates.

3. Create Deployment Package

- Right-click the selected updates and choose Create Deployment Package.

4. Create Deployment Package Wizard

- **Package Information**:
  - Provide a name and description for the package.
  - Select the distribution points where the package will be deployed.
  - Specify other deployment settings as needed.
- **Deployment Schedule**:
  - Configure the start time, deadline, and other scheduling options.
- **User Experience**:
  - Configure notifications, installation behavior, and reboot options.
- **Summary and Finish**:
  - Review the summary of the deployment package.
  - Click Finish to create the deployment package.

5. Deploy the Updates

- After the deployment package is created, right-click the deployment package and select Deploy.

6. Deploy Software Updates Wizard

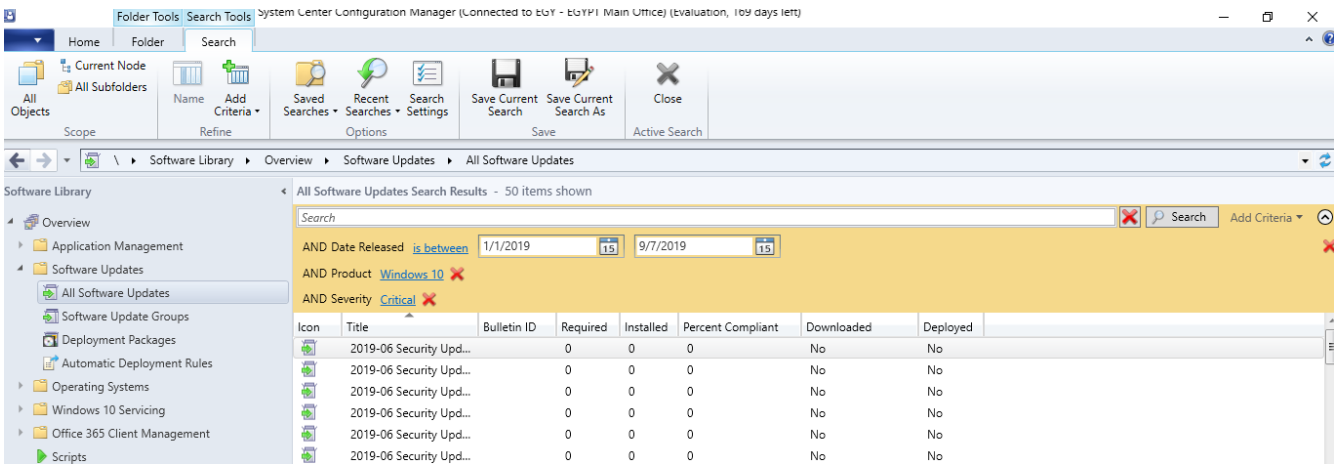
- **Target Collection**:
  - Select the collection of client computers to deploy the updates to.
- **Installation Settings**:
  - Specify installation settings and configure other deployment options.
- **Deployment Schedule**:
  - Configure the start time, deadline, and other scheduling options.
- **User Experience**:
  - Configure notifications, installation behavior, and reboot options.
- **Summary and Finish**:
  - Review the summary of the deployment settings.
  - Click Finish to deploy the updates to the selected collection of client computers.

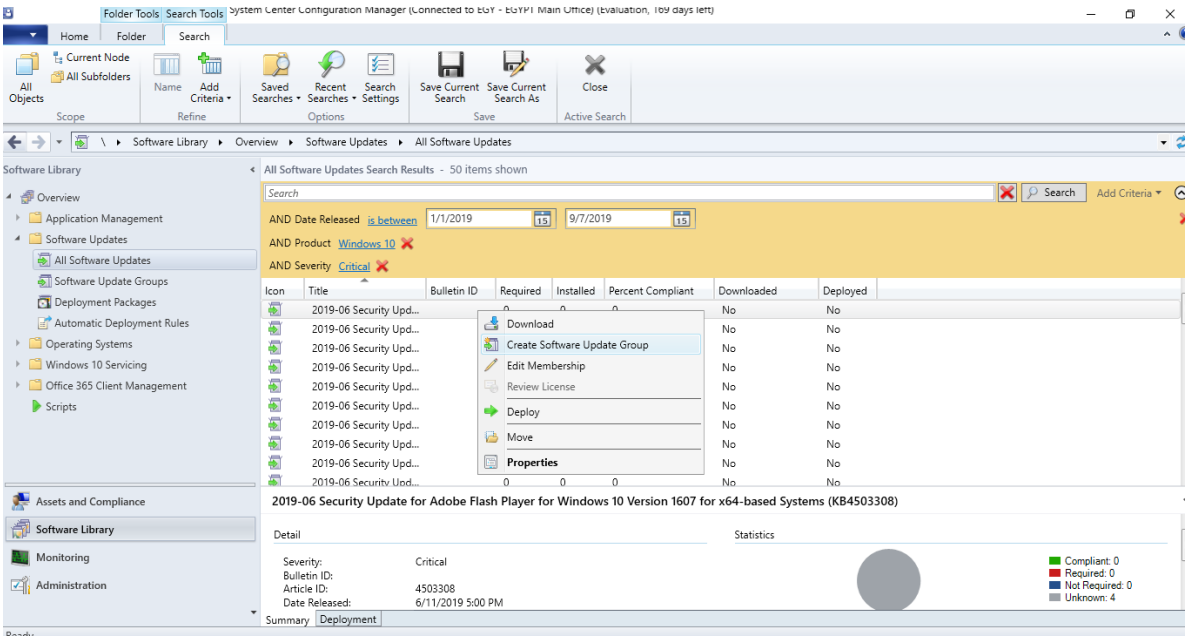
Example Scenario: Deploying Critical Updates

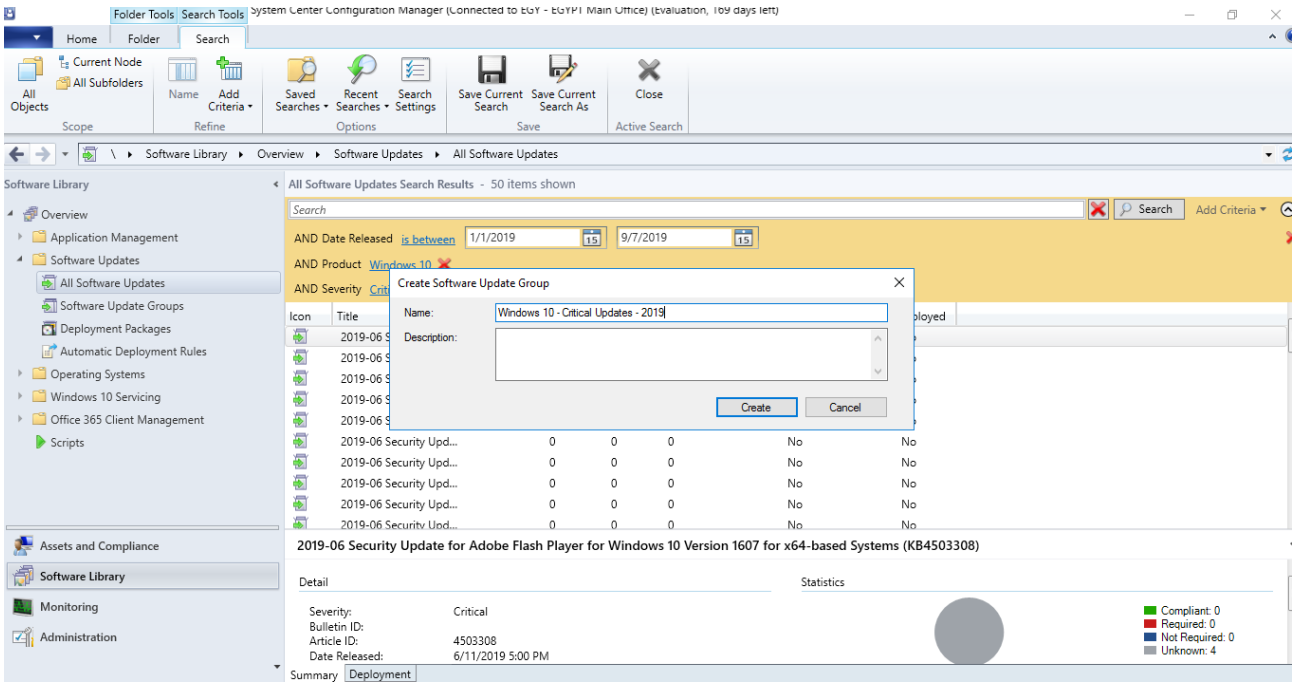
Scenario: You need to deploy critical updates for Windows 10.

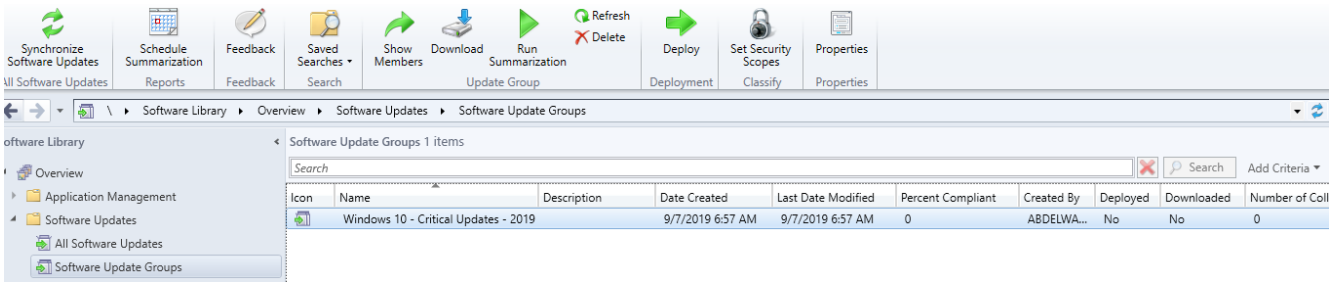
Steps:

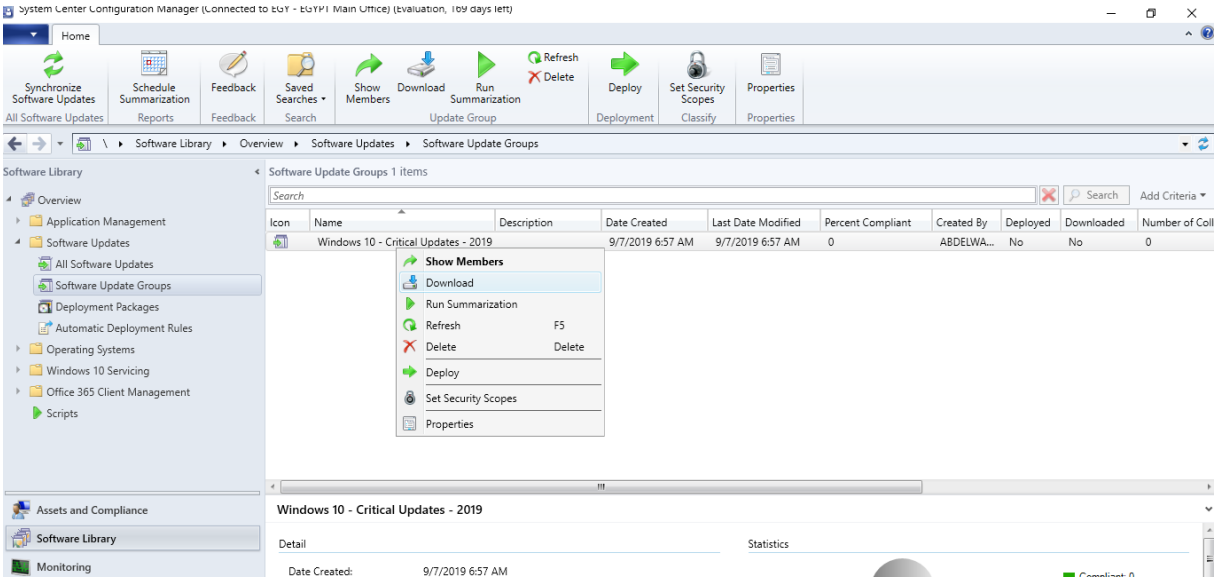
1. **Navigate to Software Updates**:
   - Open the SCCM console.
   - Go to Software Library -> Software Updates.
2. **Select Updates**:
   - Use the criteria to filter updates by Product: Windows 10 and Classification: Critical Updates.
   - Select the relevant updates.
3. **Create Deployment Package**:
   - Right-click the selected updates and choose Create Deployment Package.
   - Name the package "Windows 10 Critical Updates".
   - Select the appropriate distribution points.
   - Configure other settings as needed.
4. **Configure Deployment Package Wizard**:
   - Set the deployment schedule to start immediately and set a deadline.
   - Configure the user experience to notify users and allow them to schedule the installation within the deadline.
   - Review and finish the package creation.
5. **Deploy the Updates**:
   - Right-click the newly created deployment package and select Deploy.
   - Choose the collection containing all Windows 10 client computers.
6. **Deploy Software Updates Wizard**:
   - Configure installation settings to install updates during maintenance windows if available.
   - Set the deployment schedule to enforce the deadline.
   - Configure user experience settings to ensure users are notified of the pending updates.
   - Review and finish the deployment.

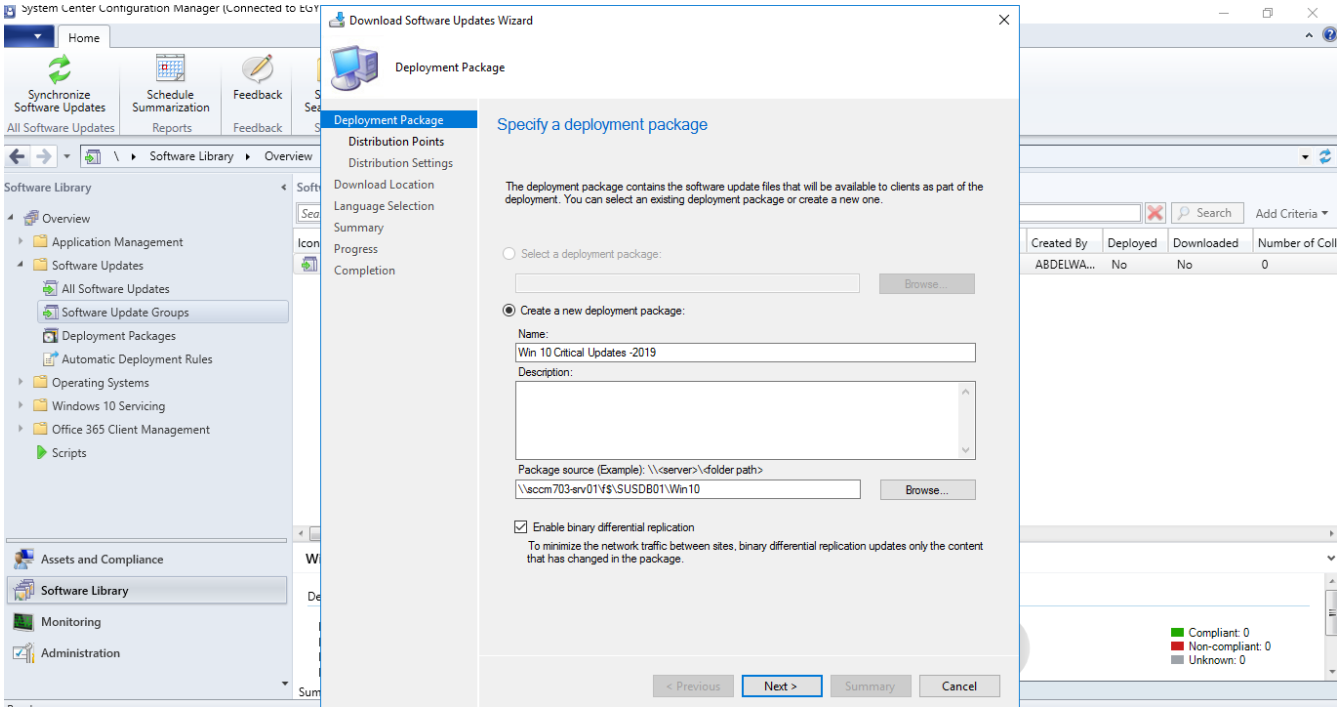


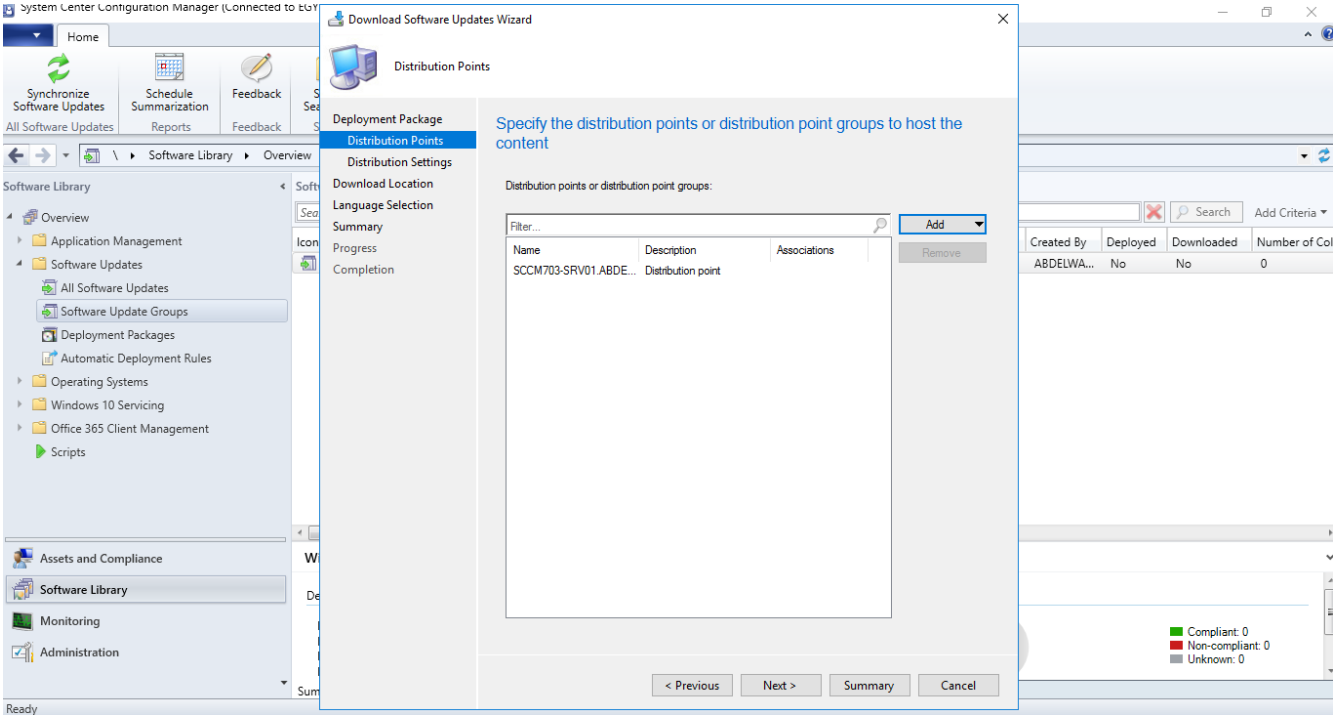

Folder Tools
Search Tools
Home
Folder
Search
All Objects
Current Node
All Subfolders
Name
Add Criteria
Saved Searches
Recent Searches
Search Settings
Save Current Search
Save Current Search As
Close
Scope
Refine
Options
Save
Active Search
Software Library
Overview
Application Management
Software Updates
All Software Updates
Software Update Groups
Deployment Packages
Automatic Deployment Rules
Operating Systems
Windows 10 Servicing
Office 365 Client Management
Scripts
Assets and Compliance
Software Library
Monitoring
Administration
All Software Updates Search Results - 50 items shown
AND Date Released is between 1/1/2019 9/7/2019
AND Product Windows 10
AND Severity Critical
Add Criteria
Icon
Title
Bulletin ID
Required
Installed
Percent Compliant
Downloaded
Deployed
2019-06 Security Upd...
Download
Create Software Update Group
Edit Membership
Review License
Deploy
Move
Properties
2019-06 Security Update for Adobe Flash Player for Windows 10 Version 1607 for x64-based Systems (KB4503308)
Detail
Severity: Critical
Bulletin ID:
Article ID: 4503308
Date Released: 6/11/2019 5:00 PM
Statistics
Compliant: 0
Required: 0
Not Required: 0
Unknown: 4
Summary
Deployment

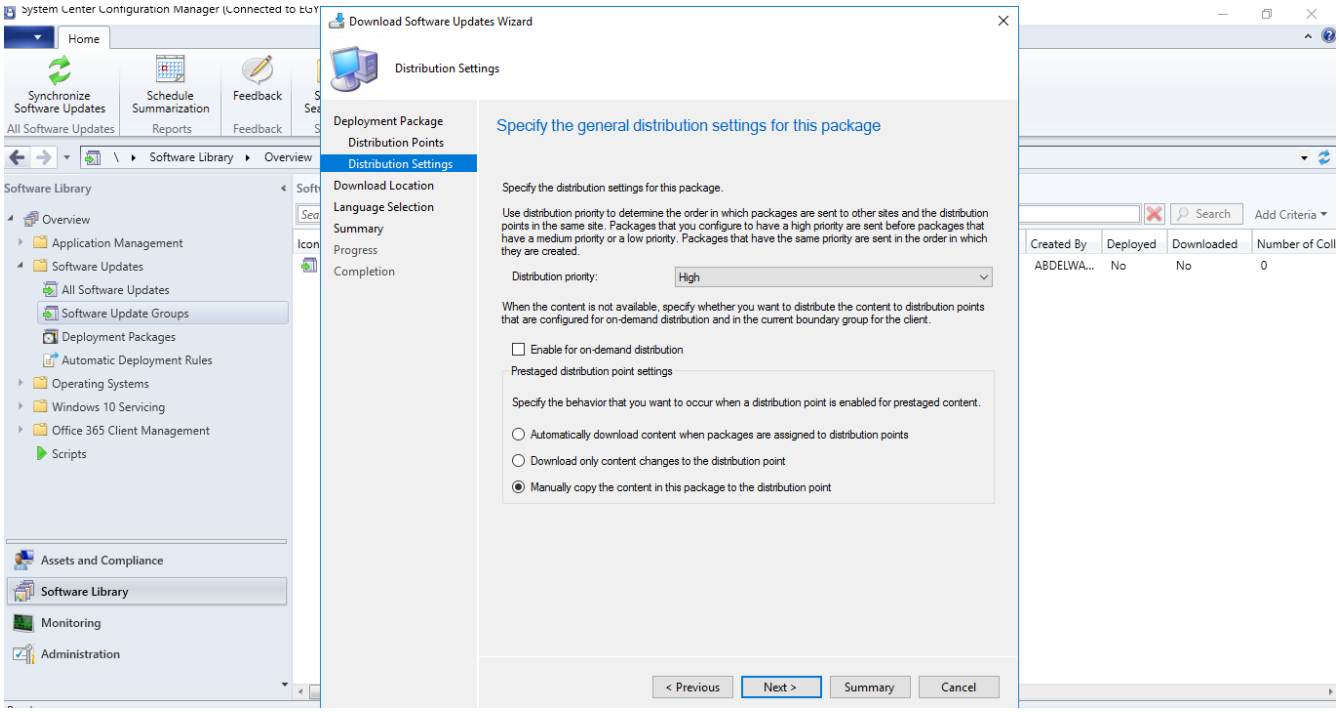

Create Software Update Group
Name:
Windows 10 - Critical Updates - 2019
Description:
Create
Cancel
2019-06 Security Update for Adobe Flash Player for Windows 10 Version 1607 for x64-based Systems (KB4503308)

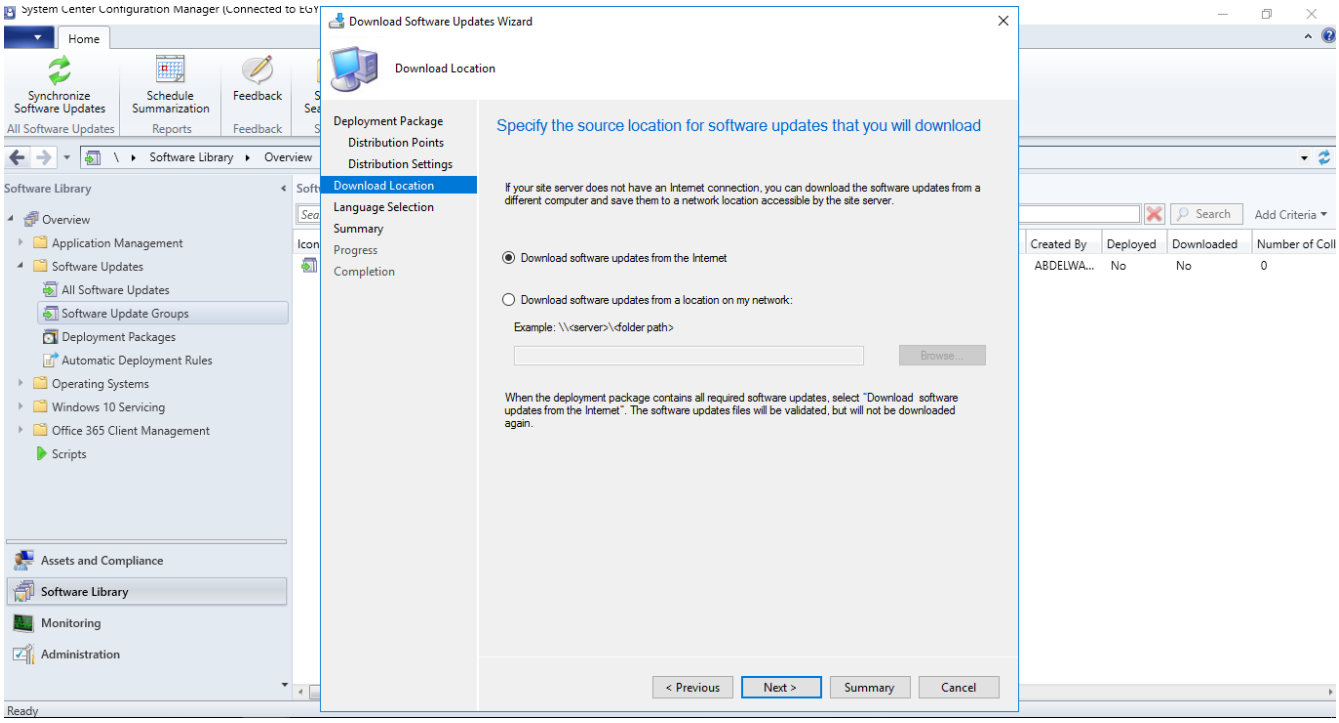

Software Update Groups 1 items
Windows 10 - Critical Updates - 2019

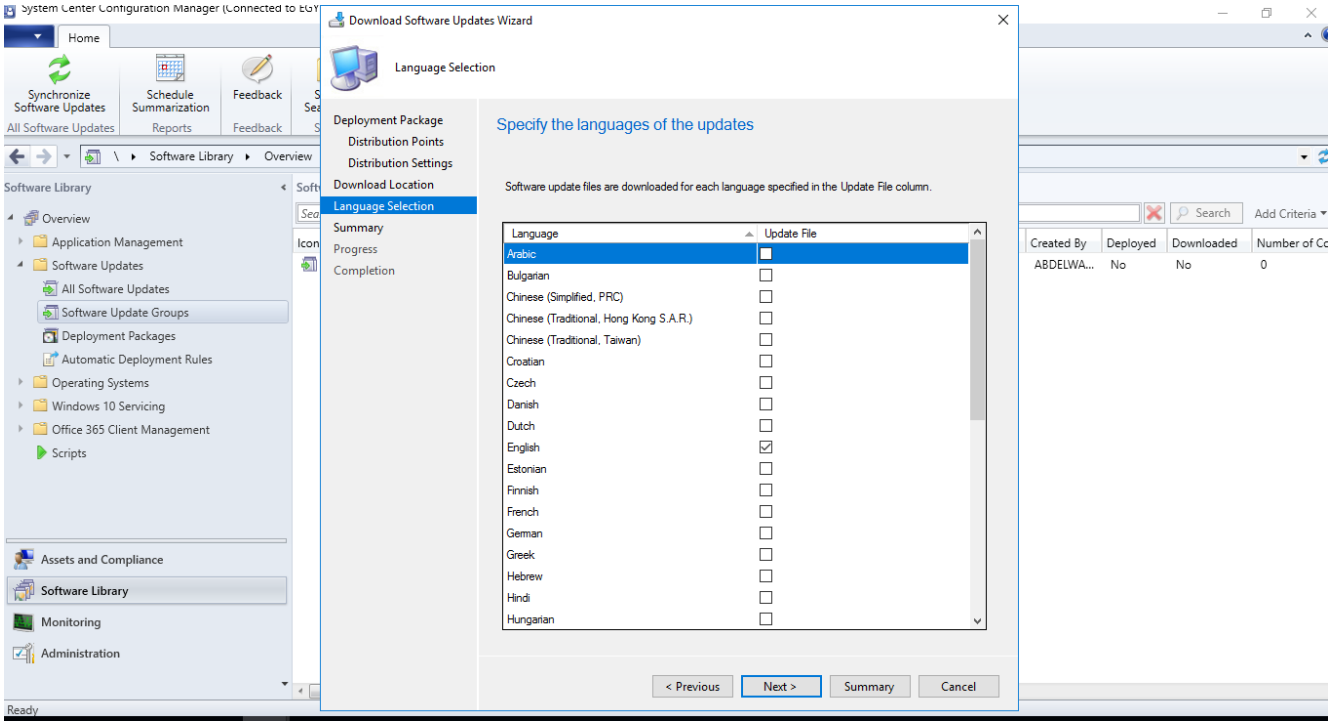

Show Members
Download
Run Summarization
Refresh F5
Delete Delete
Deploy
Set Security Scopes
Properties
Windows 10 - Critical Updates - 2019

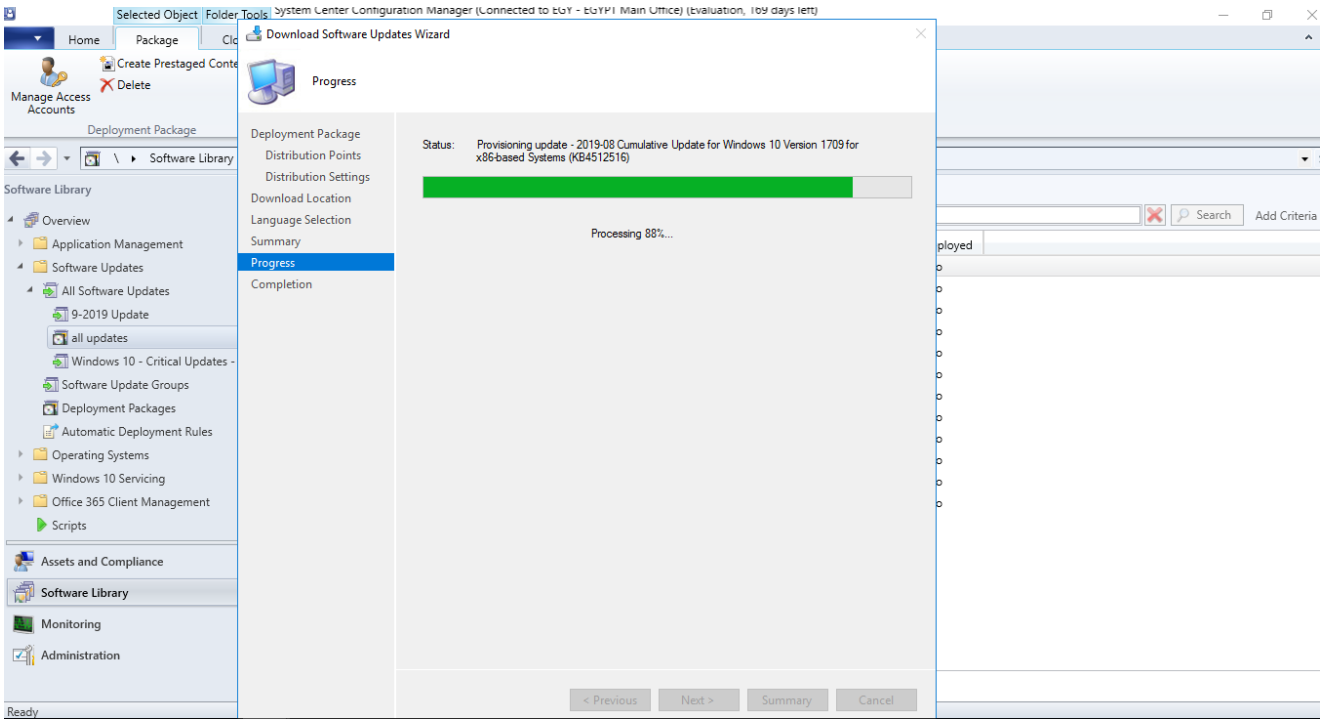

Download Software Updates Wizard
Deployment Package
Deployment Package
Distribution Points
Distribution Settings
Download Location
Language Selection
Summary
Progress
Completion
Specify a deployment package
The deployment package contains the software update files that will be available to clients as 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:
Win 10 Critical Updates -2019
Description:
Package source (Example): \\<server>\<folder path>
\\sccm703-srv01\f$\SUSDB01\Win10
Browse...
Enable binary differential replication
To minimize the network traffic between sites, binary differential replication updates only the content that has changed in the package.
< Previous
Next >
Summary
Cancel

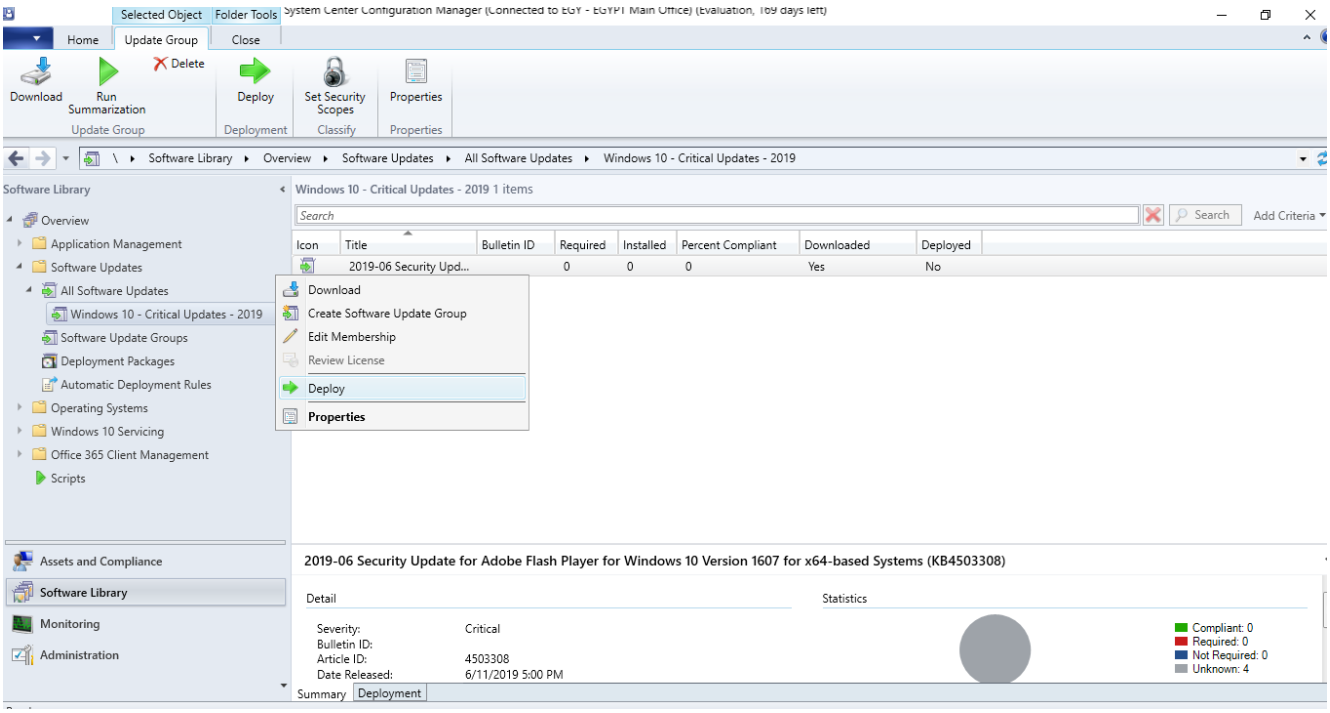

Download Software Updates Wizard
Distribution Points
Deployment Package
Distribution Points
Distribution Settings
Download Location
Language Selection
Summary
Progress
Completion
Specify the distribution points or distribution point groups to host the content
Distribution points or distribution point groups:
Filter...
Add
Remove
Name
Description
Associations
SCCM703-SRV01.ABDE...
Distribution point
< Previous
Next >
Summary
Cancel

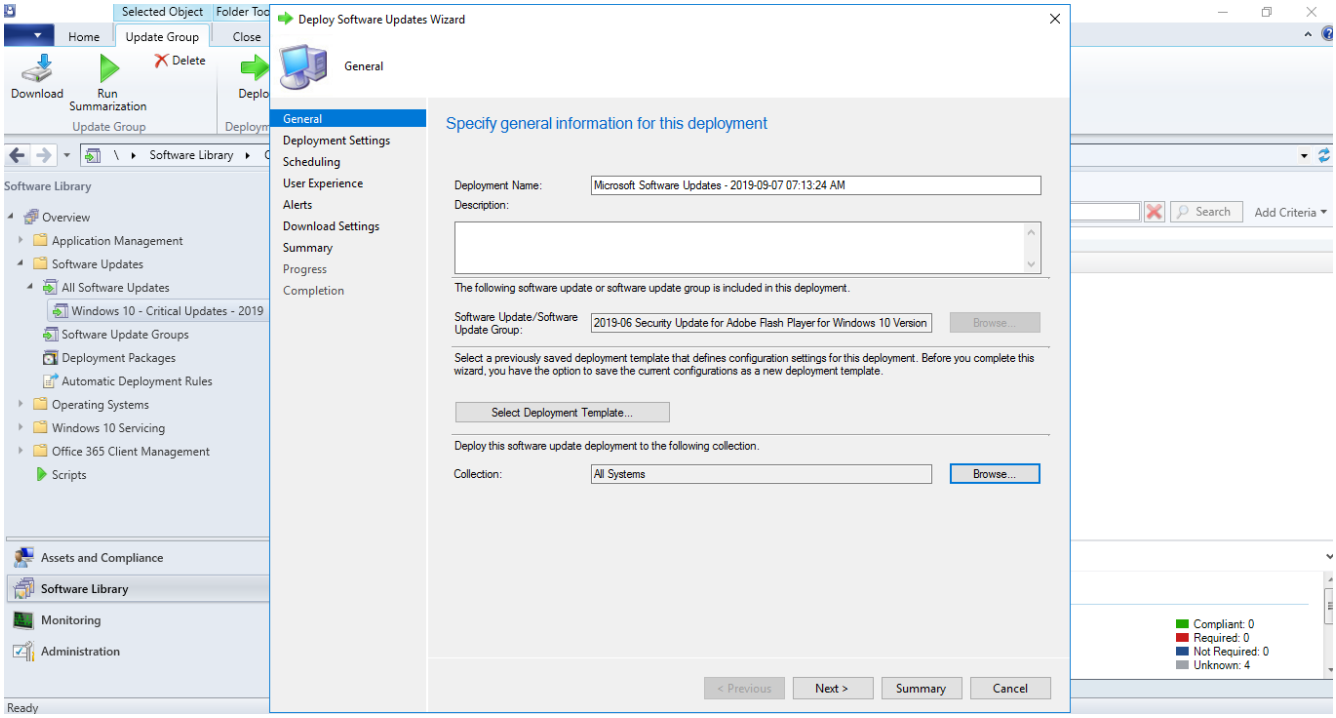

Download Software Updates Wizard
Distribution Settings
Deployment Package
Distribution Points
Distribution Settings
Download Location
Language Selection
Summary
Progress
Completion
Specify the general distribution settings for this package
Specify the distribution settings for this package.
Use distribution priority to determine the order in which packages are sent to other sites and the distribution points in the same site. Packages that you configure to have a high priority are sent before packages that have a medium priority or a low priority. Packages that have the same priority are sent in the order in which they are created.
Distribution priority:
High
When the content is not available, specify whether you want to distribute the content to distribution points that are configured for on-demand distribution and in the current boundary group for the client.
Enable for on-demand distribution
Prestaged distribution point settings
Specify the behavior that you want to occur when a distribution point is enabled for prestaged content.
Automatically download content when packages are assigned to distribution points
Download only content changes to the distribution point
Manually copy the content in this package to the distribution point
< Previous
Next >
Summary
Cancel
Home
Synchronize Software Updates
Schedule Summarization
Feedback
Software Library
Overview
Application Management
Software Updates
All Software Updates
Software Update Groups
Deployment Packages
Automatic Deployment Rules
Operating Systems
Windows 10 Servicing
Office 365 Client Management
Scripts
Assets and Compliance
Software Library
Monitoring
Administration
Search
Add Criteria
Created By
Deployed
Downloaded
Number of Coll
ABDELWA...
No
No
0

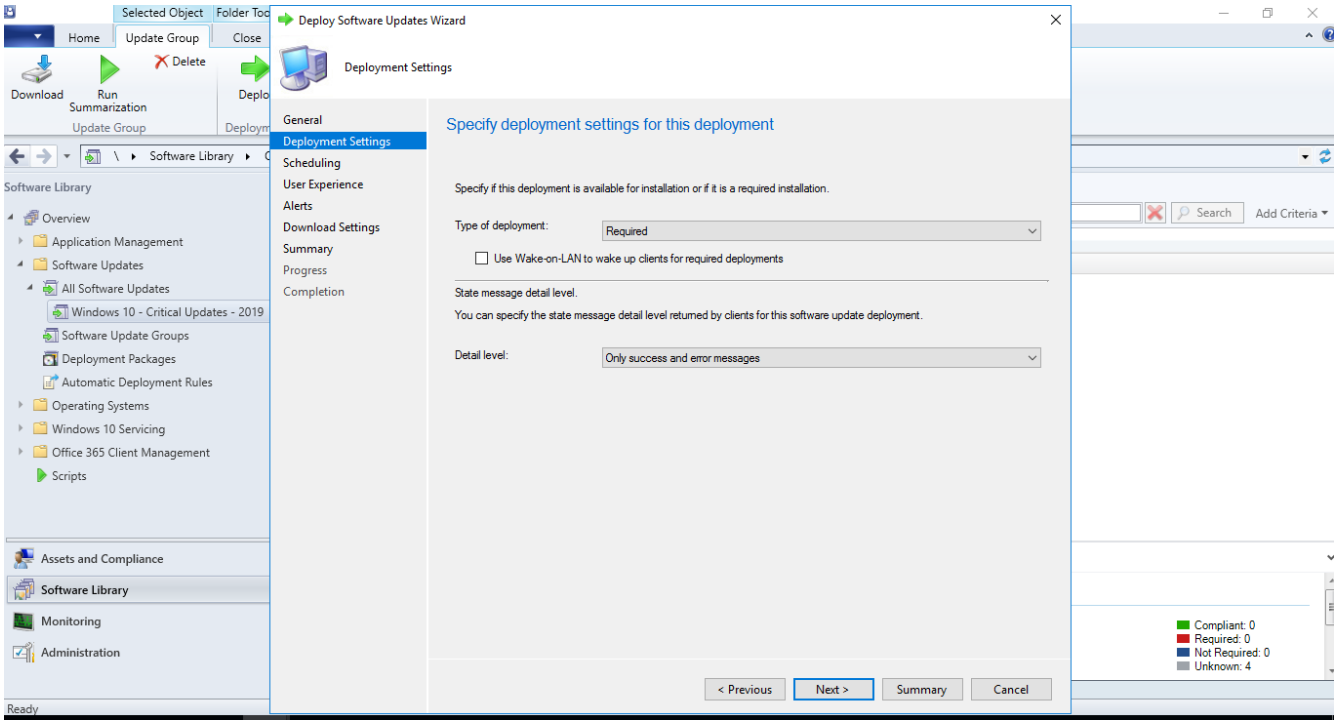

Download Software Updates Wizard
Download Location
Deployment Package
Distribution Points
Distribution Settings
Download Location
Language Selection
Summary
Progress
Completion
Specify the source location for software updates that you will download
If your site server does not have an Internet connection, you can download the software updates from a different computer and save them to a network location accessible by the site server.
Download software updates from the Internet
Download software updates from a location on my network:
Example: \\<server>\<folder path>
Browse...
When the deployment package contains all required software updates, select "Download software updates from the Internet". The software updates files will be validated, but will not be downloaded again.
< Previous
Next >
Summary
Cancel
Home
Synchronize Software Updates
Schedule Summarization
Feedback
Software Library
Overview
Application Management
Software Updates
All Software Updates
Software Update Groups
Deployment Packages
Automatic Deployment Rules
Operating Systems
Windows 10 Servicing
Office 365 Client Management
Scripts
Assets and Compliance
Software Library
Monitoring
Administration
Search
Add Criteria
Created By
Deployed
Downloaded
Number of Coll
ABDELWA...
No
No
0
Ready

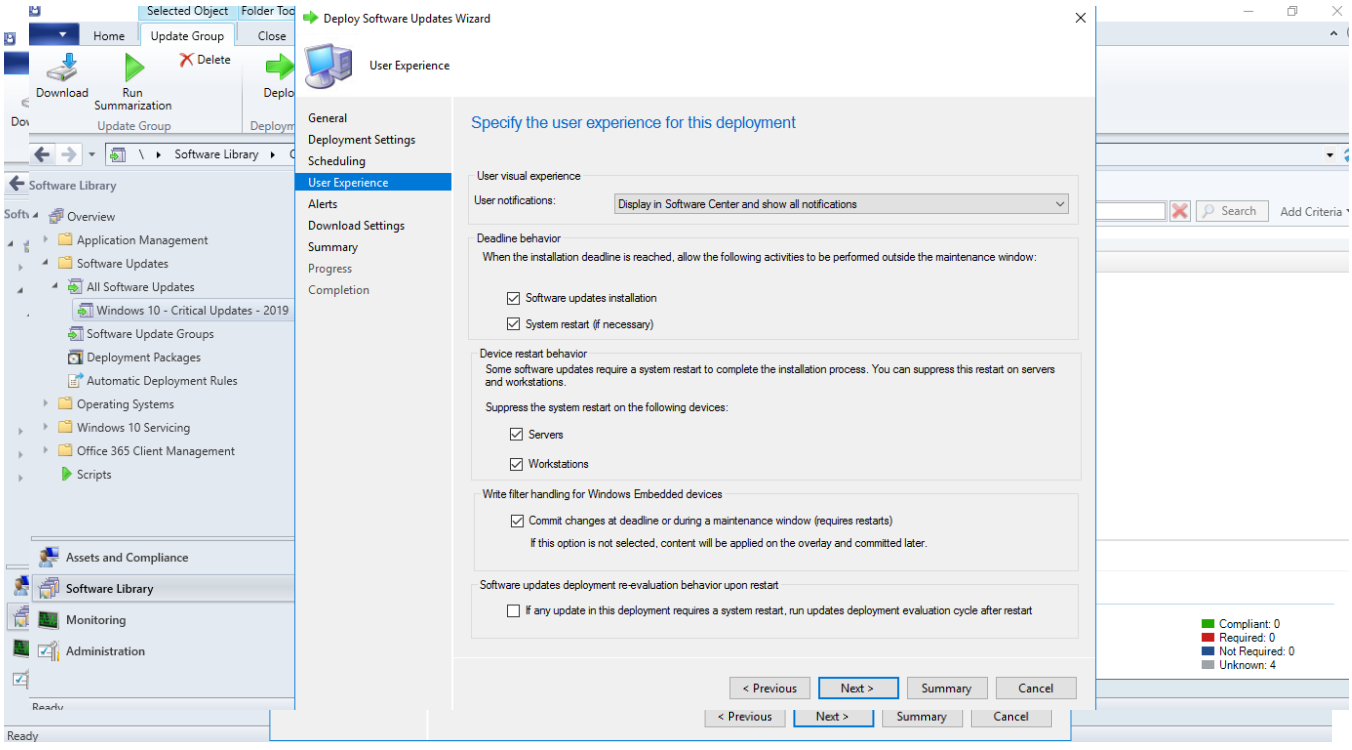

Download Software Updates Wizard
Language Selection
Deployment Package
Distribution Points
Distribution Settings
Download Location
Language Selection
Summary
Progress
Completion
Specify the languages of the updates
Software update files are downloaded for each language specified in the Update File column.
Language
Update File
Arabic
Bulgarian
Chinese (Simplified, PRC)
Chinese (Traditional, Hong Kong S.A.R.)
Chinese (Traditional, Taiwan)
Croatian
Czech
Danish
Dutch
English
Estonian
Finnish
French
German
Greek
Hebrew
Hindi
Hungarian
< Previous
Next >
Summary
Cancel
Software Library
Overview
Application Management
Software Updates
All Software Updates
Software Update Groups
Deployment Packages
Automatic Deployment Rules
Operating Systems
Windows 10 Servicing
Office 365 Client Management
Scripts
Assets and Compliance
Monitoring
Administration
Ready

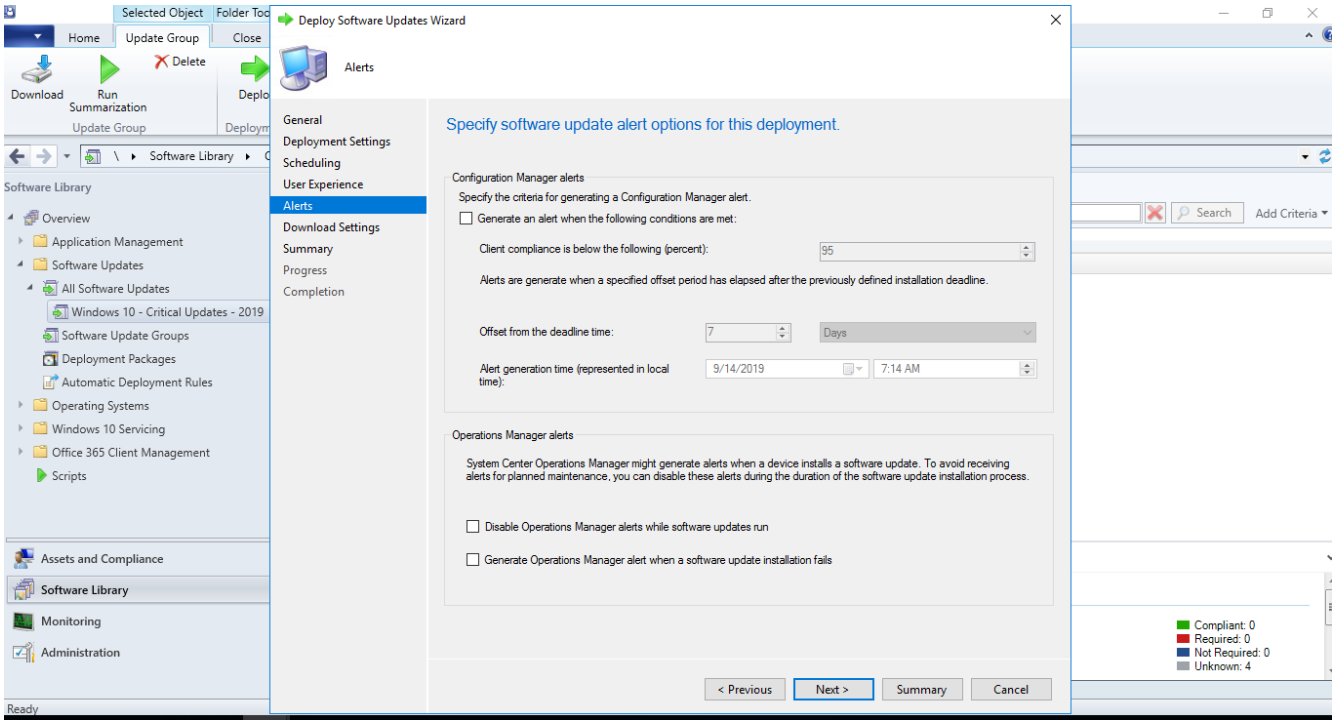

Download Software Updates Wizard
Progress
Deployment Package
Distribution Points
Distribution Settings
Download Location
Language Selection
Summary
Progress
Completion
Status: Provisioning update - 2019-08 Cumulative Update for Windows 10 Version 1709 for x86-based Systems (KB4512516)
Processing 88%...
< Previous
Next >
Summary
Cancel
Software Library
Overview
Application Management
Software Updates
All Software Updates
9-2019 Update
all updates
Windows 10 - Critical Updates -
Software Update Groups
Deployment Packages
Automatic Deployment Rules
Operating Systems
Windows 10 Servicing
Office 365 Client Management
Scripts
Assets and Compliance
Monitoring
Administration
Ready

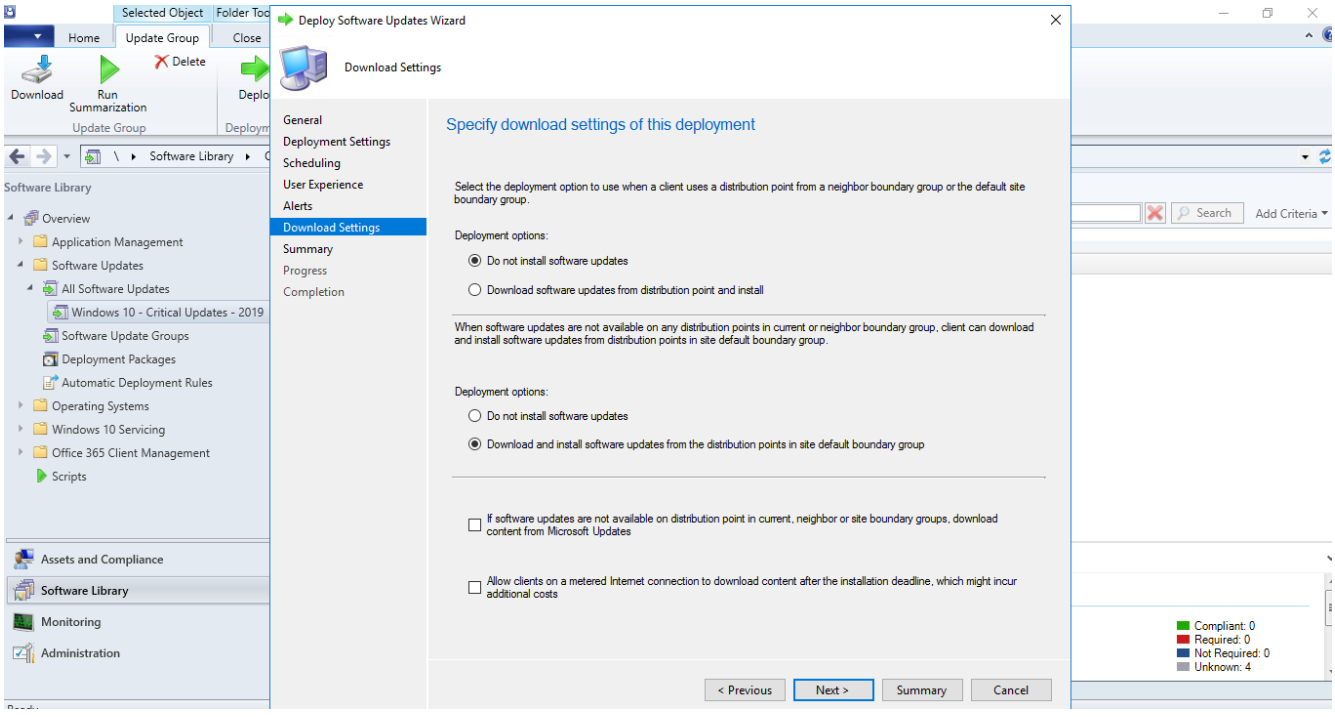

Selected Object
Folder Tools
Home
Update Group
Close
Download
Run Summarization
Delete
Deploy
Set Security Scopes
Properties
Update Group
Deployment
Classify
Properties
Software Library
Overview
Application Management
Software Updates
All Software Updates
Windows 10 - Critical Updates - 2019
Software Update Groups
Deployment Packages
Automatic Deployment Rules
Operating Systems
Windows 10 Servicing
Office 365 Client Management
Scripts
Windows 10 - Critical Updates - 2019 1 items
Search
Add Criteria
Icon
Title
Bulletin ID
Required
Installed
Percent Compliant
Downloaded
Deployed
2019-06 Security Upd...
0
0
0
Yes
No
Download
Create Software Update Group
Edit Membership
Review License
Deploy
Properties
Assets and Compliance
Software Library
Monitoring
Administration
2019-06 Security Update for Adobe Flash Player for Windows 10 Version 1607 for x64-based Systems (KB4503308)
Detail
Severity: Critical
Bulletin ID:
Article ID: 4503308
Date Released: 6/11/2019 5:00 PM
Statistics
Compliant: 0
Required: 0
Not Required: 0
Unknown: 4
Summary
Deployment

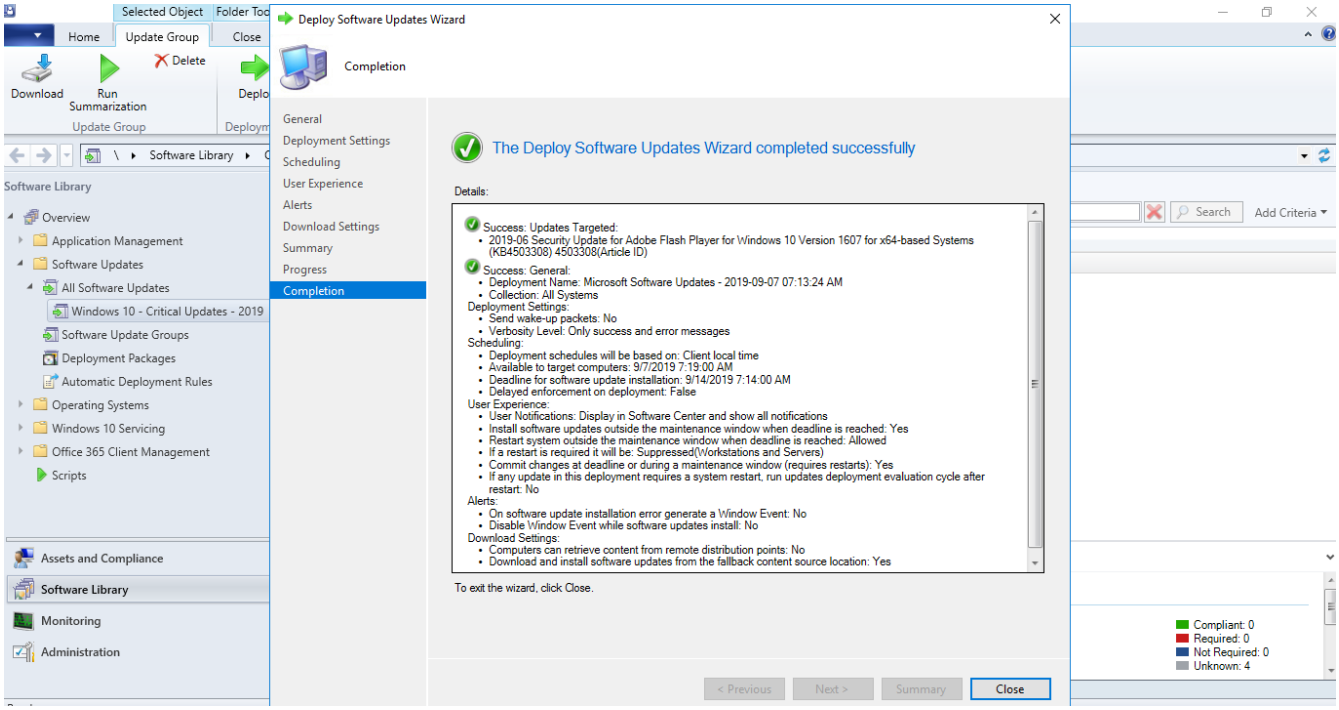

Deploy Software Updates Wizard
General
General
Deployment Settings
Scheduling
User Experience
Alerts
Download Settings
Summary
Progress
Completion
Specify general information for this deployment
Deployment Name: Microsoft Software Updates - 2019-09-07 07:13:24 AM
Description:
The following software update or software update group is included in this deployment.
Software Update/Software Update Group: 2019-06 Security Update for Adobe Flash Player for Windows 10 Version
Browse...
Select a previously saved deployment template that defines configuration settings for this deployment. Before you complete this wizard, you have the option to save the current configurations as a new deployment template.
Select Deployment Template...
Deploy this software update deployment to the following collection.
Collection: All Systems
Browse...
< Previous
Next >
Summary
Cancel
Ready

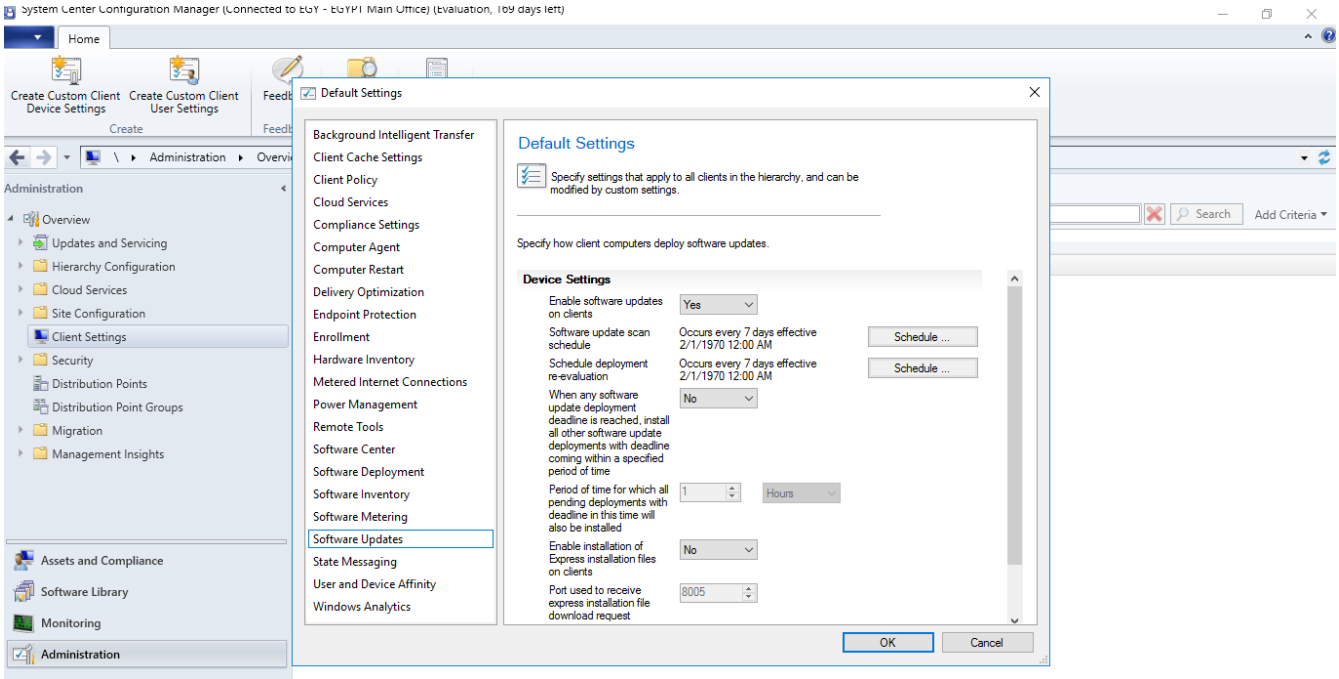

Deploy Software Updates Wizard
Deployment Settings
General
Deployment Settings
Scheduling
User Experience
Alerts
Download Settings
Summary
Progress
Completion
Specify deployment settings for this deployment
Specify if this deployment is available for installation or if it is a required installation.
Type of deployment:
Required
Use Wake-on-LAN to wake up clients for required deployments
State message detail level.
You can specify the state message detail level returned by clients for this software update deployment.
Detail level:
Only success and error messages
< Previous
Next >
Summary
Cancel
Software Library
Assets and Compliance
Monitoring
Administration
Compliant: 0
Required: 0
Not Required: 0
Unknown: 4

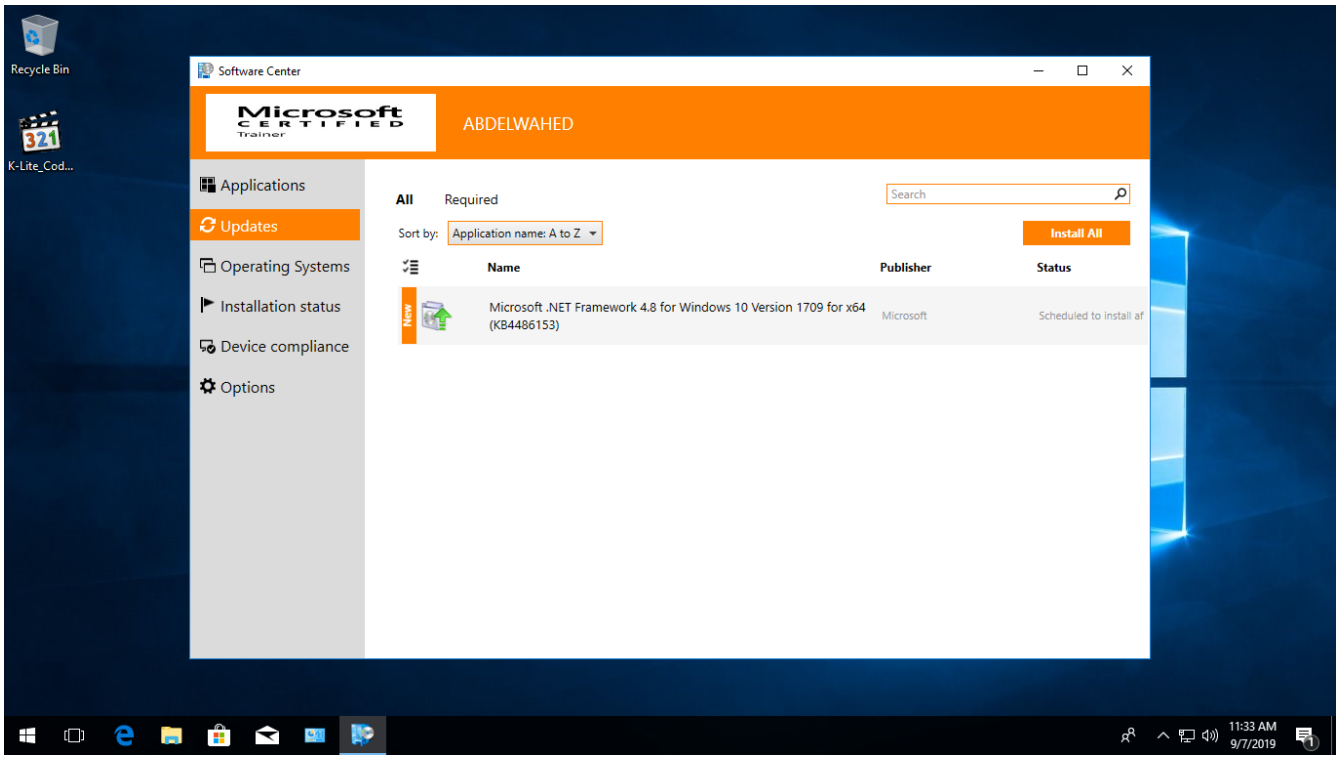

Deploy Software Updates Wizard
User Experience
General
Deployment Settings
Scheduling
User Experience
Alerts
Download Settings
Summary
Progress
Completion
Specify the user experience for this deployment
User visual experience
User notifications:
Display in Software Center and show all notifications
Deadline behavior
When the installation deadline is reached, allow the following activities to be performed outside the maintenance window:
Software updates 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
< Previous
Next >
Summary
Cancel
Software Library
Assets and Compliance
Monitoring
Administration
Compliant: 0
Required: 0
Not Required: 0
Unknown: 4

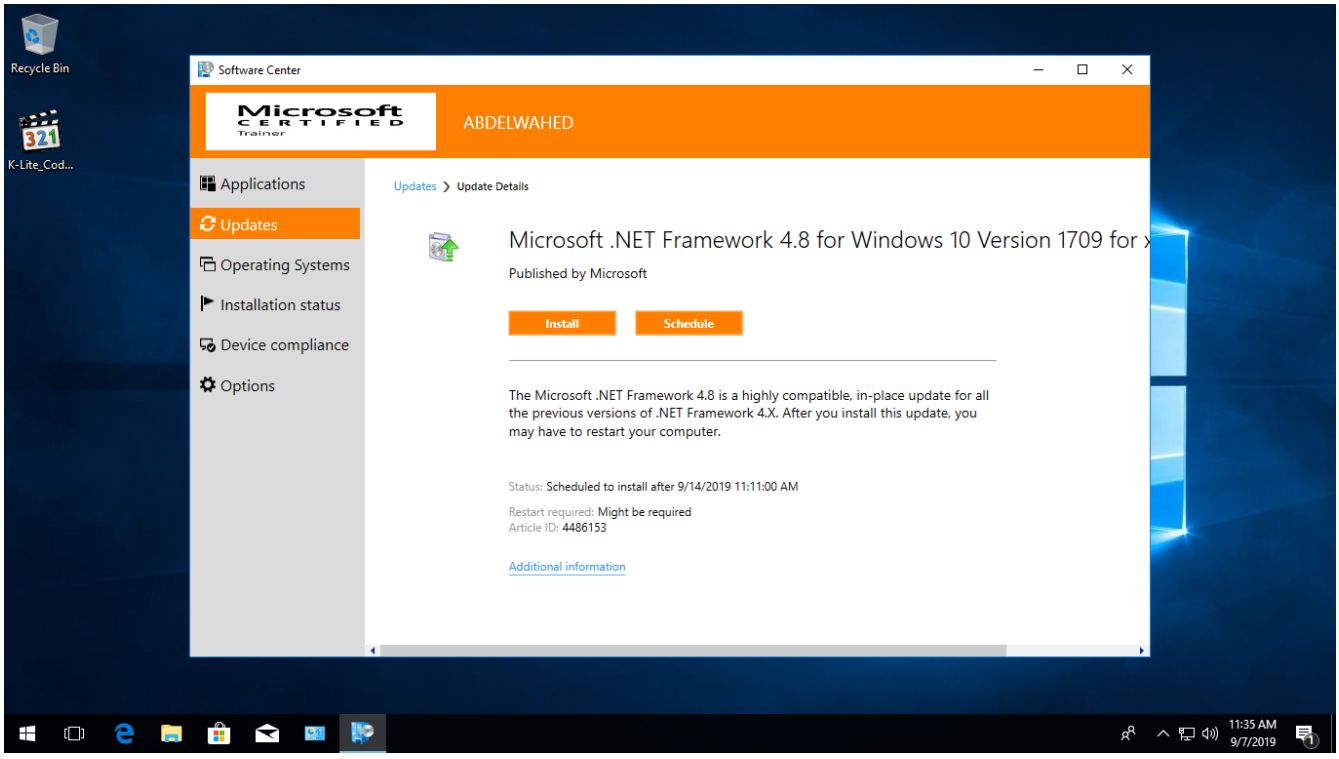

Deploy Software Updates Wizard
Alerts
General
Deployment Settings
Scheduling
User Experience
Alerts
Download Settings
Summary
Progress
Completion
Specify software update alert options for this deployment.
Configuration Manager alerts
Specify the criteria for generating a Configuration Manager alert.
Generate an alert when the following conditions are met:
Client compliance is below the following (percent):
95
Alerts are generate when a specified offset period has elapsed after the previously defined installation deadline.
Offset from the deadline time:
7
Days
Alert generation time (represented in local time):
9/14/2019
7:14 AM
Operations Manager alerts
System Center Operations Manager might generate alerts when a device installs a software update. To avoid receiving alerts for planned maintenance, you can disable these alerts during the duration of the software update installation process.
Disable Operations Manager alerts while software updates run
Generate Operations Manager alert when a software update installation fails
< Previous
Next >
Summary
Cancel


Deploy Software Updates Wizard
Download Settings
General
Deployment Settings
Scheduling
User Experience
Alerts
Download Settings
Summary
Progress
Completion
Specify download settings of this deployment
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
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
< Previous
Next >
Summary
Cancel


Deploy Software Updates Wizard
Completion
General
Deployment Settings
Scheduling
User Experience
Alerts
Download Settings
Summary
Progress
Completion
The Deploy Software Updates Wizard completed successfully
Details:
Success: Updates Targeted:
2019-06 Security Update for Adobe Flash Player for Windows 10 Version 1607 for x64-based Systems (KB4503308) 4503308(Article ID)
Success: General:
Deployment Name: Microsoft Software Updates - 2019-09-07 07:13:24 AM
Collection: All Systems
Deployment Settings:
Send wake-up packets: No
Verbosity Level: Only success and error messages
Scheduling:
Deployment schedules will be based on: Client local time
Available to target computers: 9/7/2019 7:19:00 AM
Deadline for software update installation: 9/14/2019 7:14:00 AM
Delayed enforcement on deployment: False
User Experience:
User Notifications: Display in Software Center and show all notifications
Install software updates outside the maintenance window when deadline is reached: Yes
Restart system outside the maintenance window when deadline is reached: Allowed
If a restart is required it will be: Suppressed(Workstations and Servers)
Commit changes at deadline or during a maintenance window (requires restarts): Yes
If any update in this deployment requires a system restart, run updates deployment evaluation cycle after restart: No
Alerts:
On software update installation error generate a Window Event: No
Disable Window Event while software updates install: No
Download Settings:
Computers can retrieve content from remote distribution points: No
Download and install software updates from the fallback content source location: Yes
To exit the wizard, click Close.
< Previous
Next >
Summary
Close
Software Library
Overview
Application Management
Software Updates
All Software Updates
Windows 10 - Critical Updates - 2019
Software Update Groups
Deployment Packages
Automatic Deployment Rules
Operating Systems
Windows 10 Servicing
Office 365 Client Management
Scripts
Assets and Compliance
Software Library
Monitoring
Administration
Compliant: 0
Required: 0
Not Required: 0
Unknown: 4


Default Settings
Background Intelligent Transfer
Client Cache Settings
Client Policy
Cloud Services
Compliance Settings
Computer Agent
Computer Restart
Delivery Optimization
Endpoint Protection
Enrollment
Hardware Inventory
Metered Internet Connections
Power Management
Remote Tools
Software Center
Software Deployment
Software Inventory
Software Metering
Software Updates
State Messaging
User and Device Affinity
Windows Analytics
Default Settings
Specify settings that apply to all clients in the hierarchy, and can be modified by custom settings.
Specify how client computers deploy software updates.
Device Settings
Enable software updates on clients
Yes
Software update scan schedule
Occurs every 7 days effective 2/1/1970 12:00 AM
Schedule ...
Schedule deployment re-evaluation
Occurs every 7 days effective 2/1/1970 12:00 AM
Schedule ...
When any software update deployment deadline is reached, install all other software update deployments with deadline coming within a specified period of time
No
Period of time for which all pending deployments with deadline in this time will also be installed
1
Hours
Enable installation of Express installation files on clients
No
Port used to receive express installation file download request
8005
OK
Cancel
Create Custom Client Device Settings
Create Custom Client User Settings
Create
Administration
Overview
Updates and Servicing
Hierarchy Configuration
Cloud Services
Site Configuration
Client Settings
Security
Distribution Points
Distribution Point Groups
Migration
Management Insights
Assets and Compliance
Software Library
Monitoring
Administration


Recycle Bin
K-Lite_Cod...
Software Center
Microsoft CERTIFIED Trainer
ABDELWAHED
Applications
Updates
Operating Systems
Installation status
Device compliance
Options
All
Required
Search
Sort by:
Application name: A to Z
Install All
Name
Publisher
Status
New
Microsoft .NET Framework 4.8 for Windows 10 Version 1709 for x64 (KB4486153)
Microsoft
Scheduled to install af
11:33 AM
9/7/2019


Recycle Bin
K-Lite_Cod...
Software Center
Microsoft CERTIFIED Trainer
ABDELWAHED
Applications
Updates
Operating Systems
Installation status
Device compliance
Options
Updates > Update Details
Microsoft .NET Framework 4.8 for Windows 10 Version 1709 for x
Published by Microsoft
Install
Schedule
The Microsoft .NET Framework 4.8 is a highly compatible, in-place update for all the previous versions of .NET Framework 4.X. After you install this update, you may have to restart your computer.
Status: Scheduled to install after 9/14/2019 11:11:00 AM
Restart required: Might be required
Article ID: 4486153
Additional information
11:35 AM
9/7/2019

Deploy OS

Deploying OS with Bare Metal Installation using SCCM

Deploying an OS using SCCM for a bare metal installation involves several steps, from configuring network access and boot images to creating and deploying task sequences. Here is a detailed guide:

1. Configure Network Access Account

- **Purpose**: Allows SCCM to access the network location where installation files are stored.
    - Navigate to Administration -> Overview -> Site Configuration -> Sites.
    - Select your site, and in the ribbon, click Configure Site Components -> Software Distribution.
    - In the Network Access Account tab, specify an account that has read access to the network share containing the OS installation files.

2. Configure Boot Images

- **Check Boot Image Properties**:
    - Navigate to Software Library -> Overview -> Operating Systems -> Boot Images.
    - Right-click the boot image (x86 or x64) and select Properties.
    - In the Data Source tab, check Deploy this boot image from the PXE-enabled distribution point.
- **Customize Boot Image**:
    - In the Customization tab, enable Enable command support (testing only) to allow opening a command prompt by pressing F8 during boot.
    - Add necessary network drivers under the Drivers tab if required.
- **Distribute Boot Images**:
    - Right-click the boot image and select Distribute Content.
    - Follow the wizard to distribute the boot images to the distribution points.

3. Prepare Operating System Image

- **Use Default Image**:
    - Obtain the install.wim file from Windows 10 Business Edition or another version and place it in a shared network location.
    - Navigate to Software Library -> Overview -> Operating Systems -> Operating System Images.
    - Right-click and select Add Operating System Image, specifying the network path to install.wim.
- **Optional: Schedule Updates**:
    - After adding the OS image, right-click it and select Schedule Updates to integrate updates from WSUS if available.

4. Create and Customize Task Sequence

- **Add Task Sequence**:
    - Navigate to Software Library -> Overview -> Operating Systems -> Task Sequences.
    - Right-click and select Create Task Sequence to create a new task sequence for the OS deployment.
- **Edit Task Sequence**:
    - Select the created task sequence and click Edit.
    - Configure the task sequence steps, such as Apply Operating System, Apply Device Drivers, and Setup Windows and ConfigMgr.

- **Task Sequence Types**:
  - Choose appropriate task sequence types, such as bare metal deployment or in-place upgrade (e.g., from Windows 10 build 1511 to build 1902).

5. Distribute Task Sequence

- **Distribute Task Sequence**:
  - Right-click the task sequence and select Distribute Content.
  - Follow the wizard to distribute the task sequence to the distribution points.

6. Deploy Task Sequence

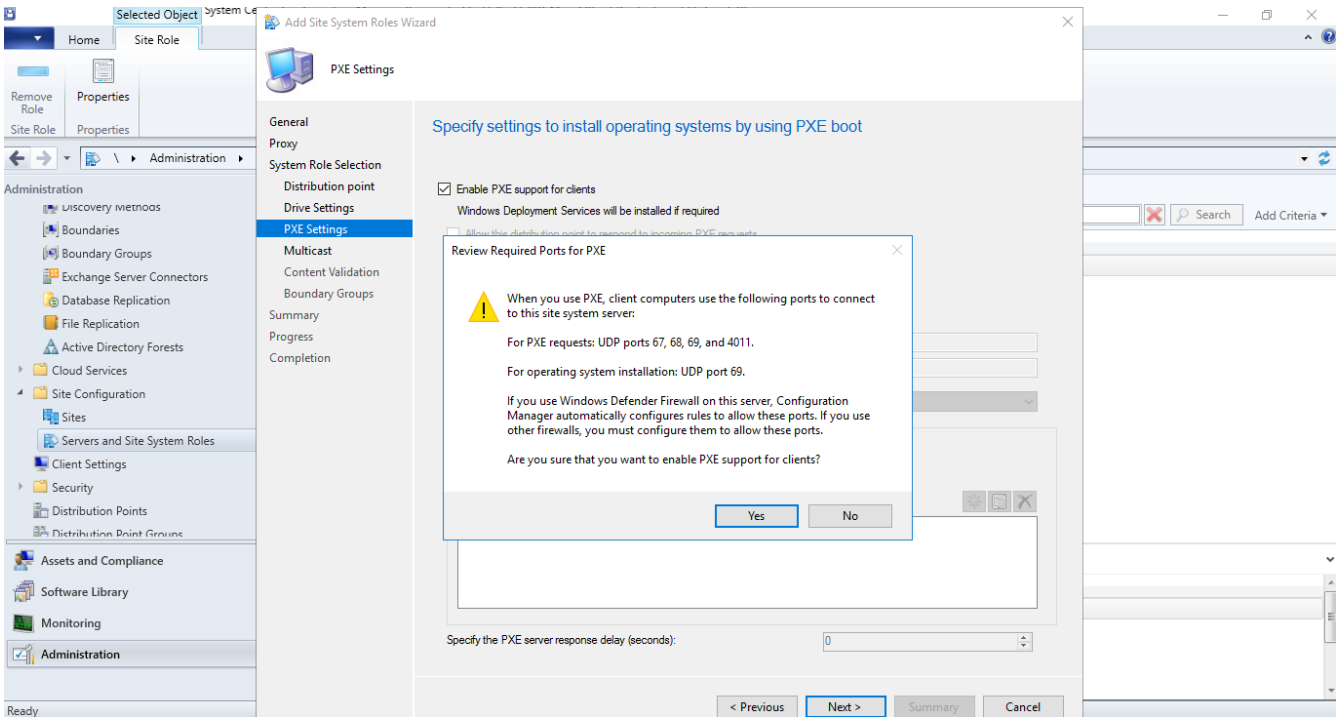
- **Deploy to Client Computers**:
  - Right-click the task sequence and select Deploy.
  - Choose the collection of target client computers. If deploying to new or non-SCCM clients, select Unknown Computers.
- **Deployment Settings**:
  - Configure deployment settings, such as making the deployment available or required, and schedule the deployment.

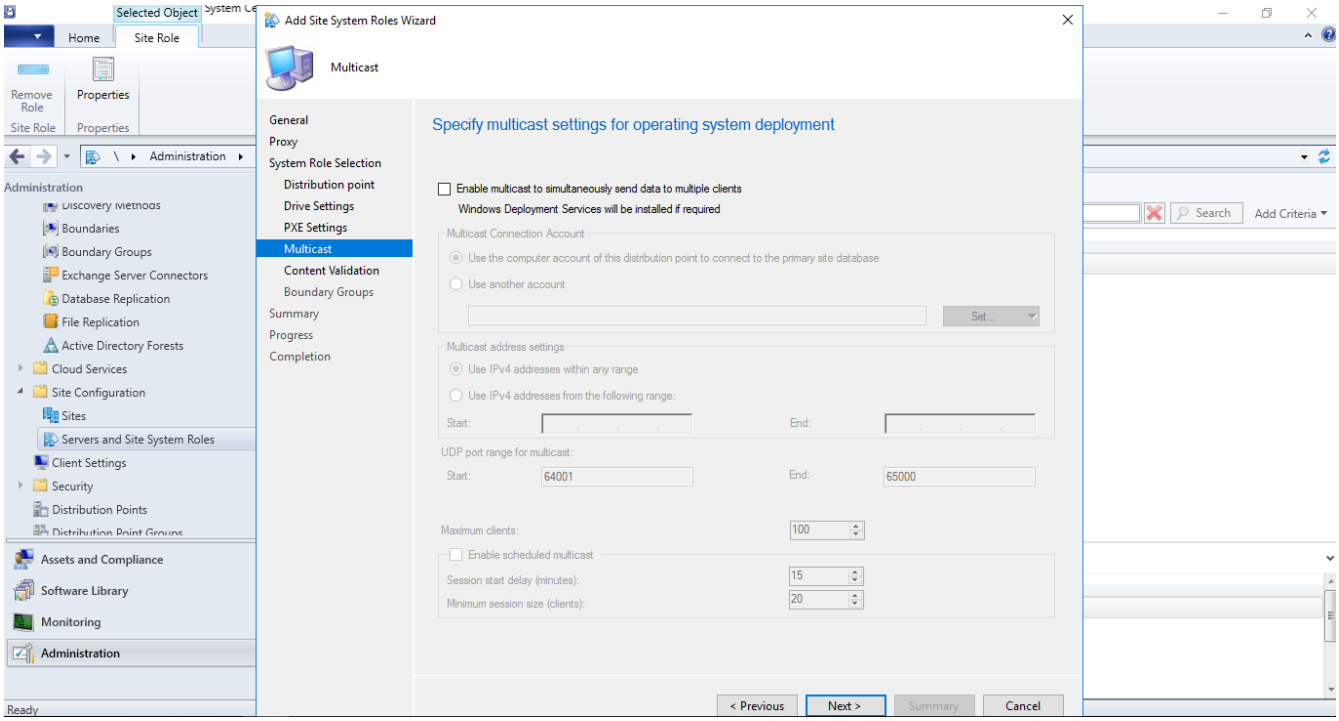
Example Scenario: Deploying Windows 10 Bare Metal Installation

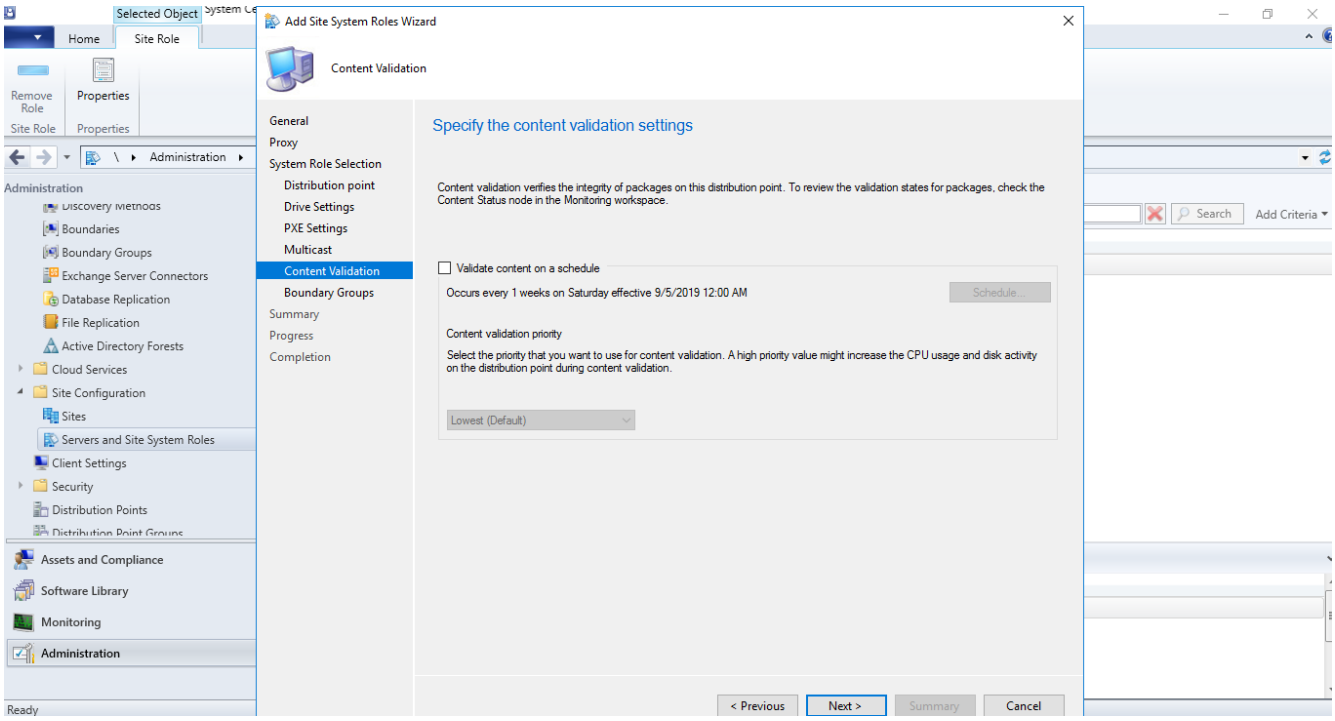
Scenario: You need to perform a bare metal installation of Windows 10 on unknown computers.

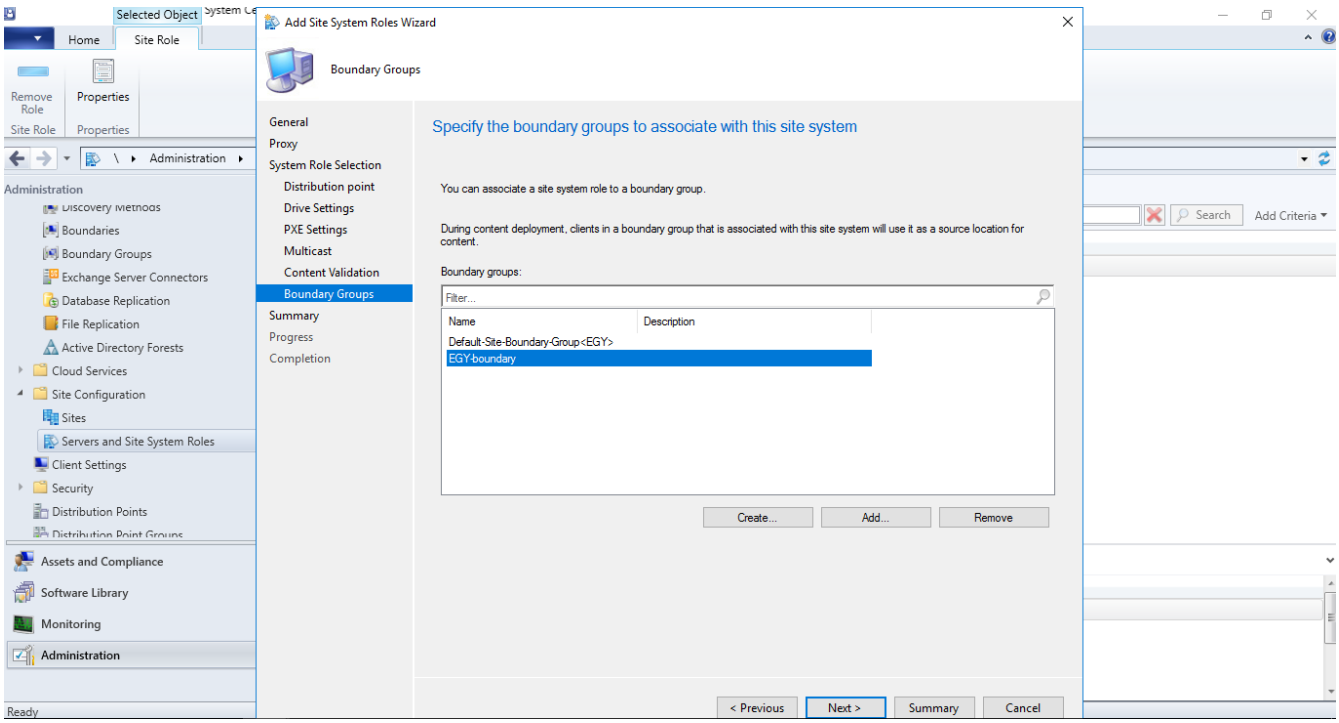
1. **Configure Network Access Account**:
   - Go to Administration -> Site Configuration -> Sites.
   - Select the site, and configure the Network Access Account.
2. **Configure Boot Images:**
   - Go to Software Library -> Operating Systems -> Boot Images.
   - Select the x64 boot image, enable command support, and deploy from PXE-enabled distribution points.
   - Distribute the boot image to distribution points.
3. **Prepare OS Image:**
   - Add the install.wim from Windows 10 Business Edition.
   - (Optional) Schedule updates if using WSUS.
4. **Create Task Sequence:**
   - Navigate to Software Library -> Operating Systems -> Task Sequences.
   - Create a new task sequence for Windows 10 deployment.
   - Edit the task sequence to include steps like applying the OS image and configuring the SCCM client.
5. **Distribute Task Sequence:**
   - Distribute the task sequence to the distribution points.
6. **Deploy Task Sequence:**
   - Deploy the task sequence to the Unknown Computers collection to allow installation on new devices.
   - Configure deployment settings to make it available for PXE boot.

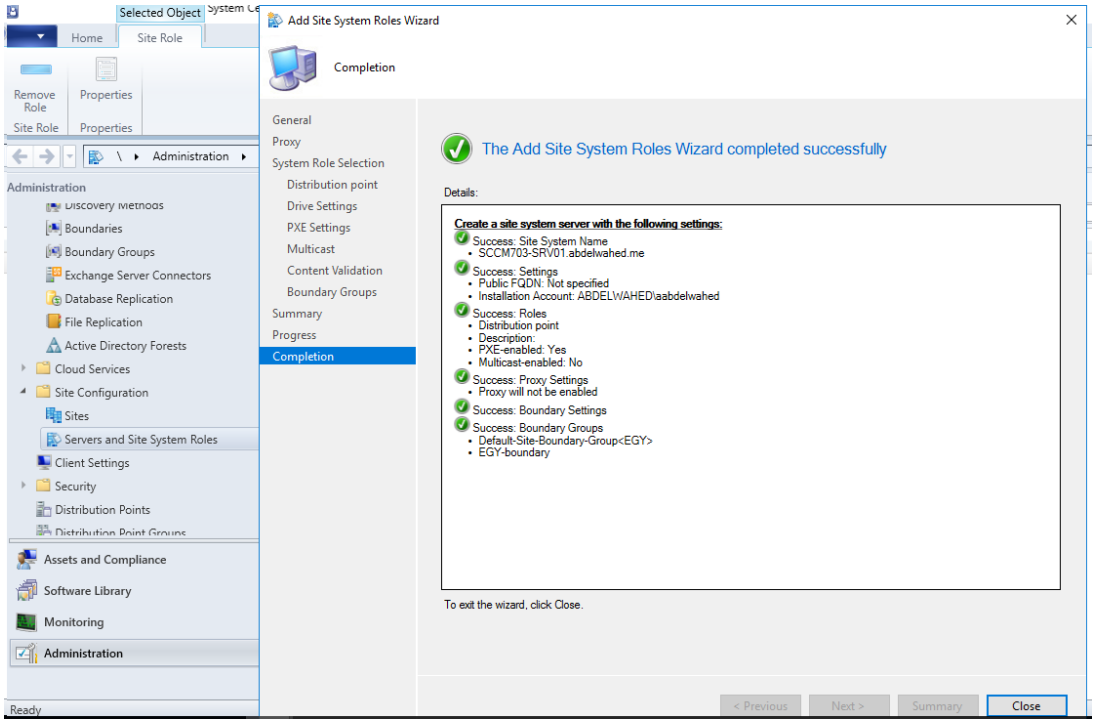
When adding the distribution point role in OS deployment



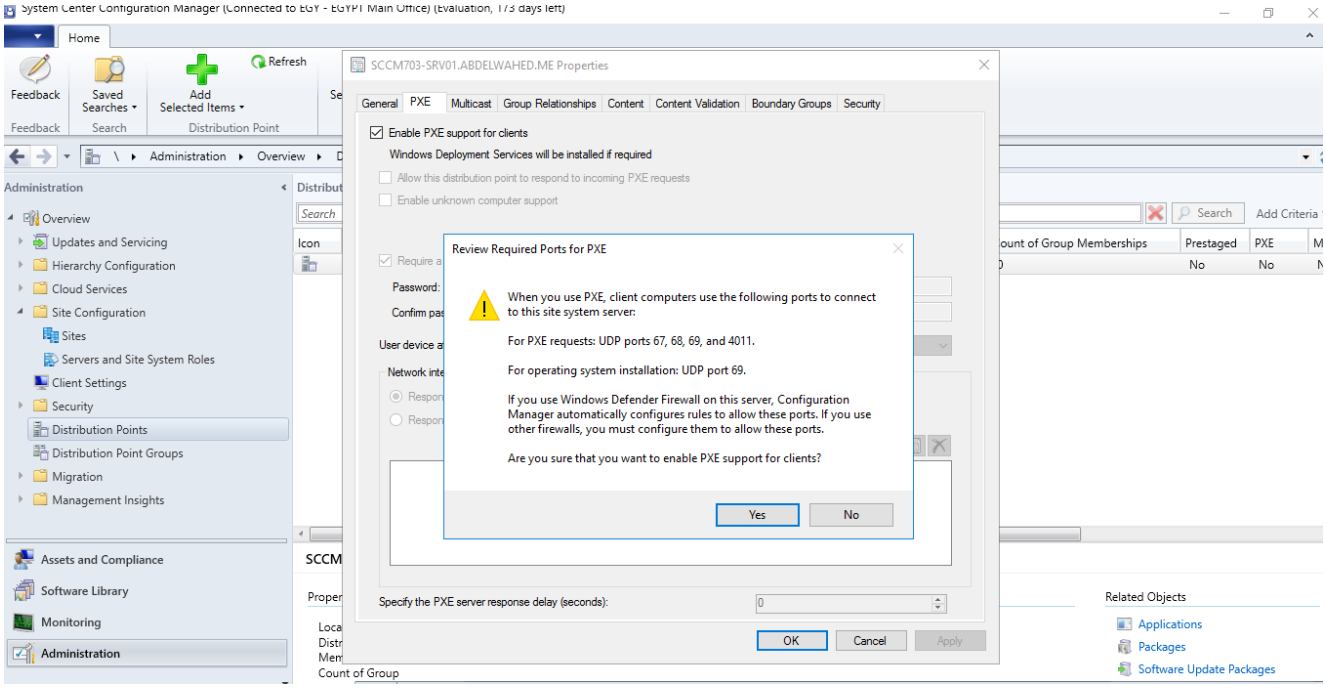



Add Site System Roles Wizard
Content Validation
General
Proxy
System Role Selection
Distribution point
Drive Settings
PXE Settings
Multicast
Content Validation
Boundary Groups
Summary
Progress
Completion
Specify the content validation settings
Content validation verifies the integrity of packages on this distribution point. To review the validation states for packages, check the Content Status node in the Monitoring workspace.
Validate content on a schedule
Occurs every 1 weeks on Saturday effective 9/5/2019 12:00 AM
Schedule...
Content validation priority
Select the priority that you want to use for content validation. A high priority value might increase the CPU usage and disk activity on the distribution point during content validation.
Lowest (Default)
< Previous
Next >
Summary
Cancel
Selected Object
Home
Site Role
Remove Role
Properties
Site Role
Properties
Administration
Boundaries
Boundary Groups
Exchange Server Connectors
Database Replication
File Replication
Active Directory Forests
Cloud Services
Site Configuration
Sites
Servers and Site System Roles
Client Settings
Security
Distribution Points
Assets and Compliance
Software Library
Monitoring
Administration
Search
Add Criteria
Ready

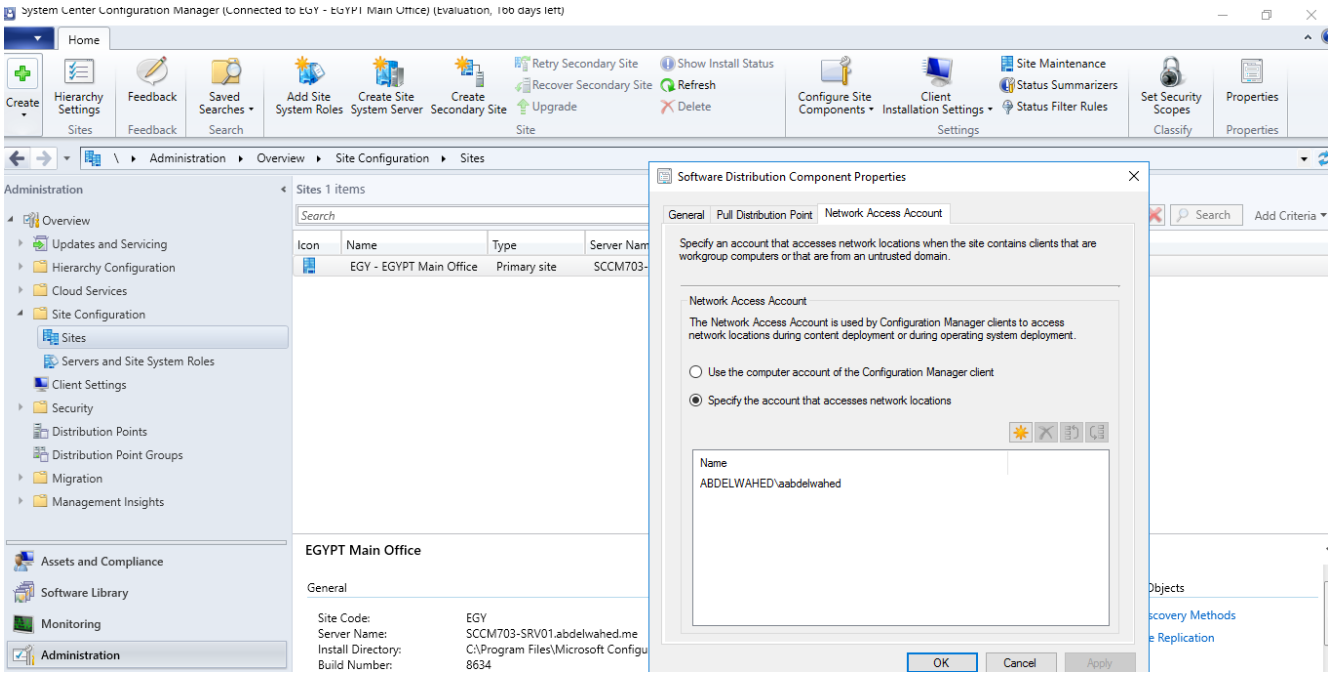

Add Site System Roles Wizard
Boundary Groups
General
Proxy
System Role Selection
Distribution point
Drive Settings
PXE Settings
Multicast
Content Validation
Boundary Groups
Summary
Progress
Completion
Specify the boundary groups to associate with this site system
You can associate a site system role to a boundary group.
During content deployment, clients in a boundary group that is associated with this site system will use it as a source location for content.
Boundary groups:
Filter...
Name
Description
Default-Site-Boundary-Group<EGY>
EGY-boundary
Create...
Add...
Remove
< Previous
Next >
Summary
Cancel
Selected Object
Home
Site Role
Remove Role
Properties
Site Role
Properties
Administration
Boundaries
Boundary Groups
Exchange Server Connectors
Database Replication
File Replication
Active Directory Forests
Cloud Services
Site Configuration
Sites
Servers and Site System Roles
Client Settings
Security
Distribution Points
Assets and Compliance
Software Library
Monitoring
Administration
Search
Add Criteria
Ready



Activating PXE or multicast options on a server-configured distribution point will automatically trigger the installation of the Windows Deployment Services (WDS) server role on that server.



Add network access account to allow CM to access the network location



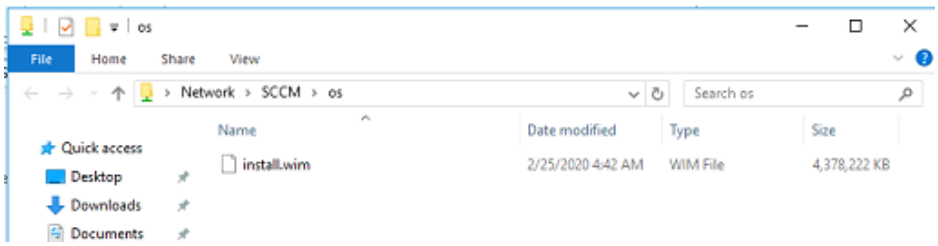
Adjust the properties of boot images for x86:

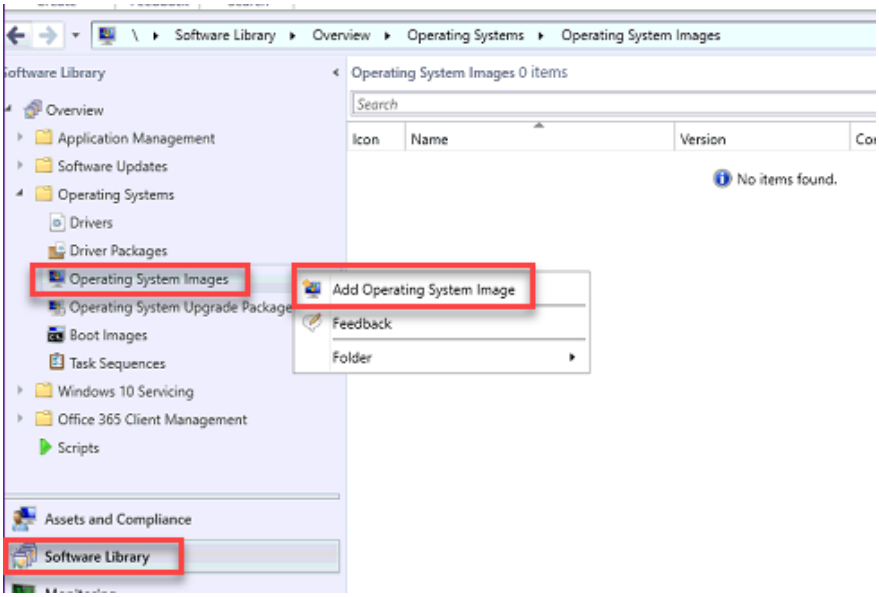
- Customization: Include a command line option to access the cmd by pressing F8 when the boot image appears.
- Data Source: Ensure this boot image is available from PXE-enabled deployment.
- Drivers: Add any required network drivers, making sure to add the driver's package first.

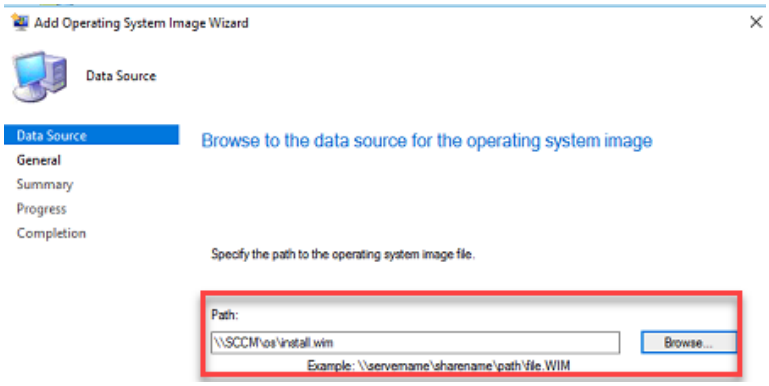
Distribute both of the boot images to the distribution point.

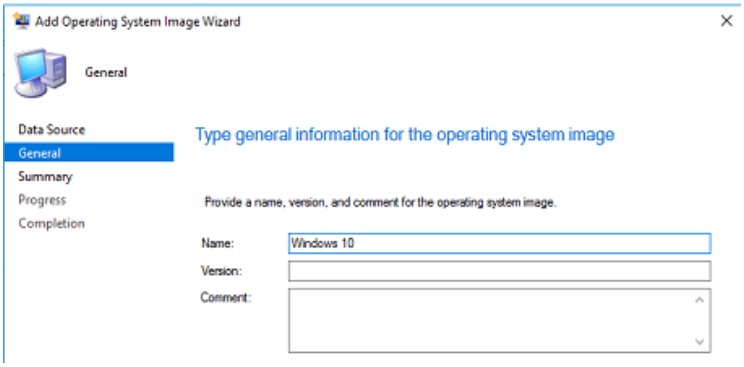
For Operating System Images:

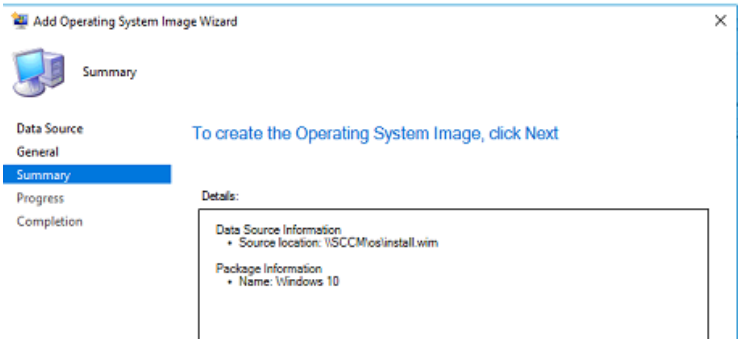
Transfer the install.wim file from the Windows OS CD to the shared folder.

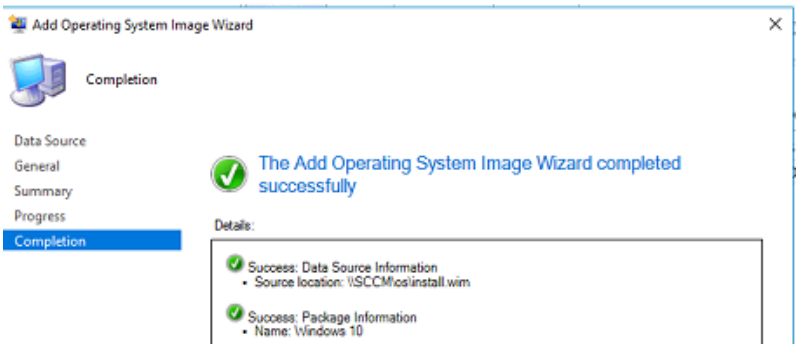


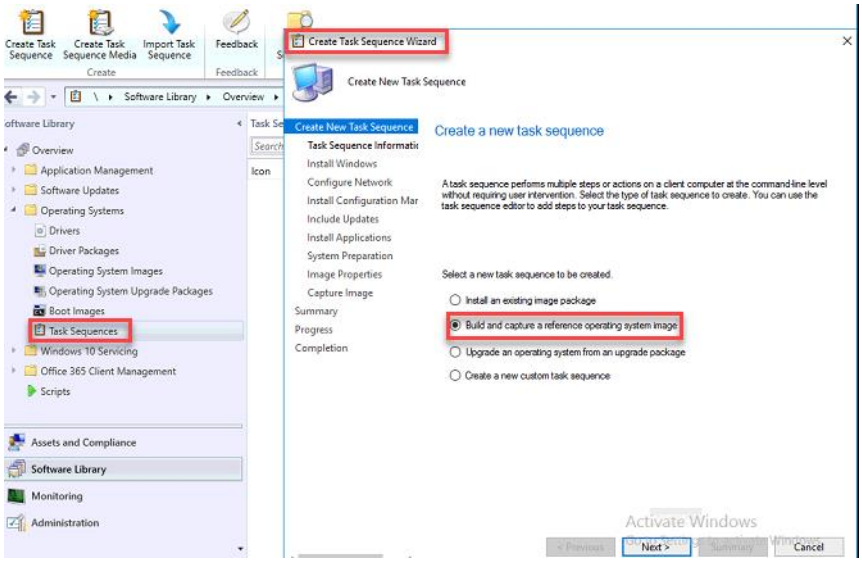

Software Library
Overview
Operating Systems
Operating System Images
Operating System Images 0 items
Search
Icon
Name
Version
No items found.
Application Management
Software Updates
Operating Systems
Drivers
Driver Packages
Operating System Images
Operating System Upgrade Packages
Boot Images
Task Sequences
Windows 10 Servicing
Office 365 Client Management
Scripts
Add Operating System Image
Feedback
Folder
Assets and Compliance
Software Library

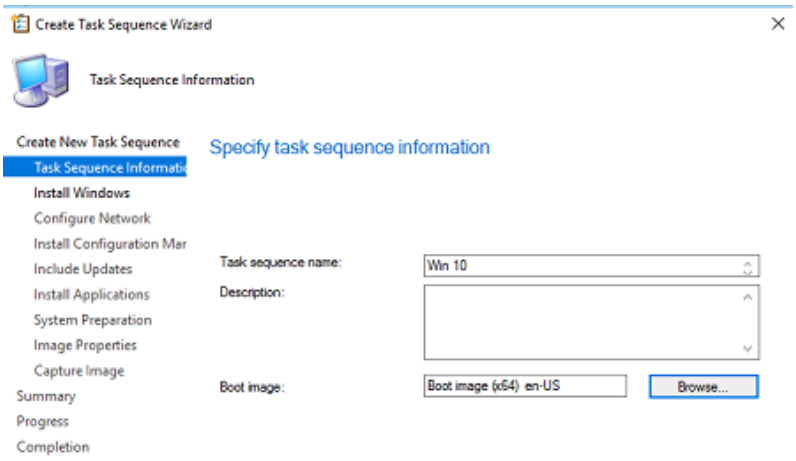

Add Operating System Image Wizard
Data Source
Data Source
General
Summary
Progress
Completion
Browse to the data source for the operating system image
Specify the path to the operating system image file.
Path:
\\SCCM\os\install.wim
Browse...
Example: \\servername\sharename\path\file.WIM

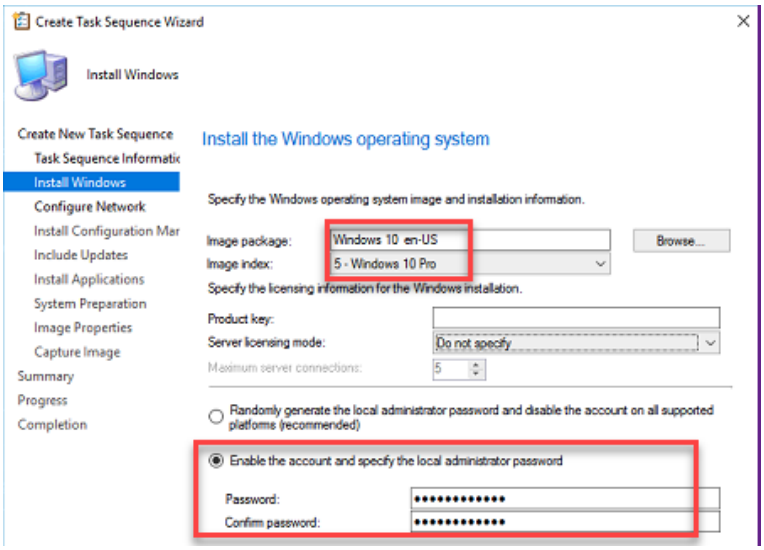

Add Operating System Image Wizard
General
Data Source
General
Summary
Progress
Completion
Type general information for the operating system image
Provide a name, version, and comment for the operating system image.
Name:
Windows 10
Version:
Comment:

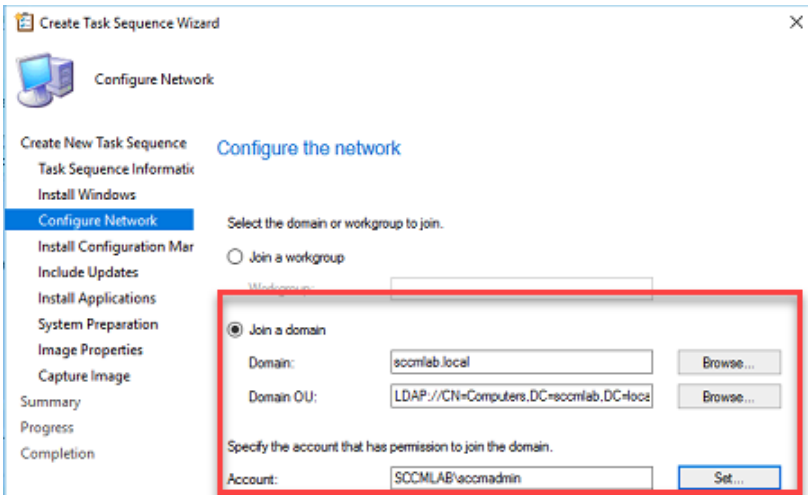

Add Operating System Image Wizard
Summary
Data Source
General
Summary
Progress
Completion
To create the Operating System Image, click Next
Details:
Data Source Information
• Source location: \\SCCM\os\install.wim
Package Information
• Name: Windows 10

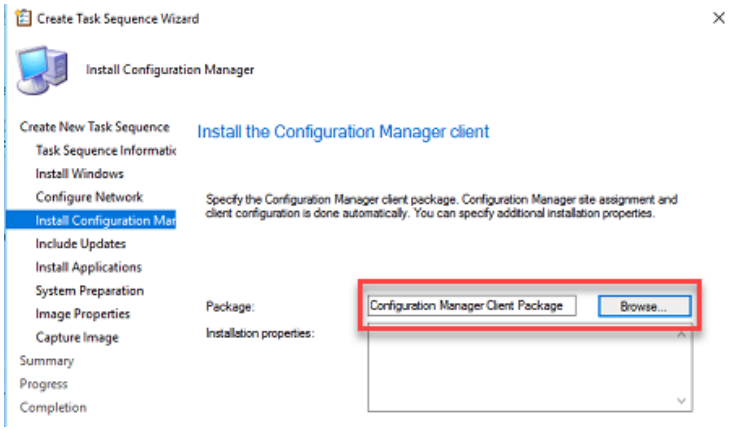

Add Operating System Image Wizard
Completion
Data Source
General
Summary
Progress
Completion
The Add Operating System Image Wizard completed successfully
Details:
Success: Data Source Information
• Source location: \\SCCM\os\install.wim
Success: Package Information
• Name: Windows 10

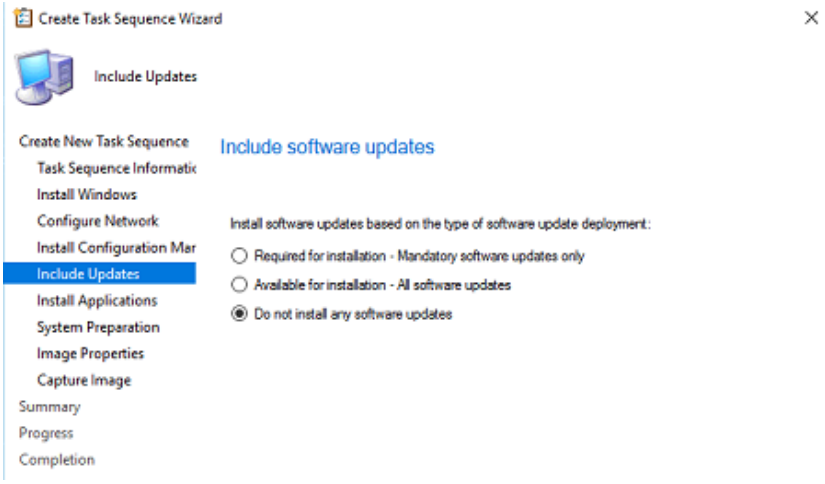

Create Task Sequence
Create Task Sequence Media
Import Task Sequence
Feedback
Create
Feedback
Create Task Sequence Wizard
Create New Task Sequence
Create a new task sequence
Task Sequences
Boot Images
Operating System Images
Operating System Upgrade Packages
Drivers
Driver Packages
Scripts
Assets and Compliance
Software Library
Monitoring
Administration
Install an existing image package
Build and capture a reference operating system image
Upgrade an operating system from an upgrade package
Create a new custom task sequence
Next >
Cancel

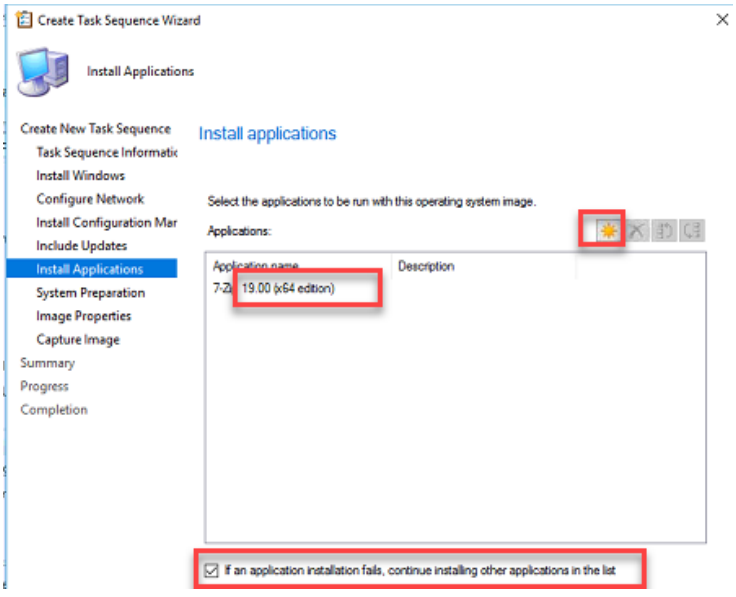

Create Task Sequence Wizard
Task Sequence Information
Create New Task Sequence
Task Sequence Informatic
Install Windows
Configure Network
Install Configuration Mar
Include Updates
Install Applications
System Preparation
Image Properties
Capture Image
Summary
Progress
Completion
Specify task sequence information
Task sequence name:
Win 10
Description:
Boot image:
Boot image (x64) en-US
Browse...

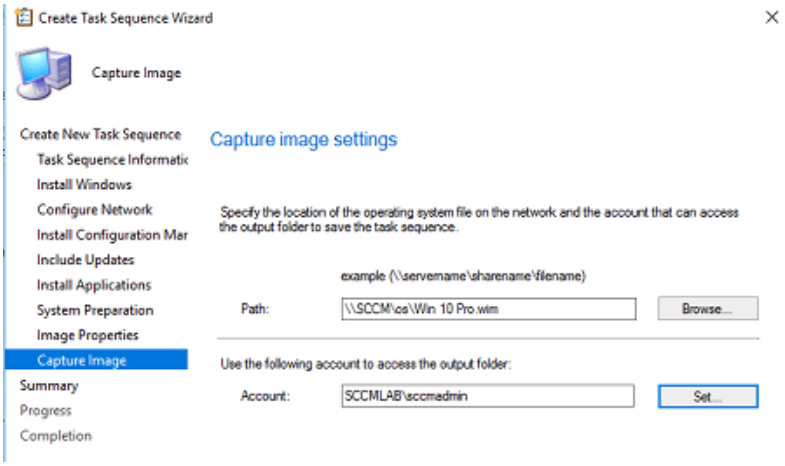

Create Task Sequence Wizard
Install Windows
Create New Task Sequence
Task Sequence Informatic
Install Windows
Configure Network
Install Configuration Mar
Include Updates
Install Applications
System Preparation
Image Properties
Capture Image
Summary
Progress
Completion
Install the Windows operating system
Specify the Windows operating system image and installation information.
Image package:
Windows 10 en-US
Image index:
5 - Windows 10 Pro
Browse...
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:

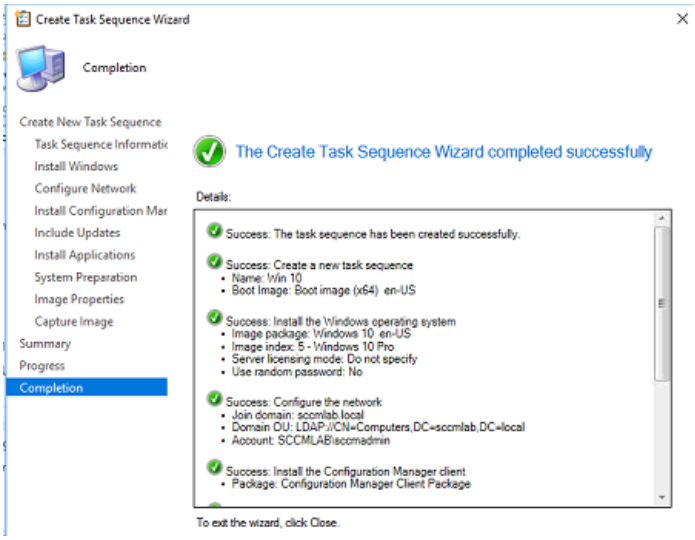

Create Task Sequence Wizard
Configure Network
Create New Task Sequence
Task Sequence Informatic
Install Windows
Configure Network
Install Configuration Mar
Include Updates
Install Applications
System Preparation
Image Properties
Capture Image
Summary
Progress
Completion
Configure the network
Select the domain or workgroup to join.
Join a workgroup
Join a domain
Domain:
sccmlab.local
Browse...
Domain OU:
LDAP://CN=Computers,DC=sccmlab,DC=loca
Browse...
Specify the account that has permission to join the domain.
Account:
SCCMLAB\sccmadmin
Set...


Create Task Sequence Wizard
Install Configuration Manager
Create New Task Sequence
Task Sequence Informatic
Install Windows
Configure Network
Install Configuration Mar
Include Updates
Install Applications
System Preparation
Image Properties
Capture Image
Summary
Progress
Completion
Install the Configuration Manager client
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:


Create Task Sequence Wizard
Include Updates
Create New Task Sequence
Task Sequence Informatic
Install Windows
Configure Network
Install Configuration Mar
Include Updates
Install Applications
System Preparation
Image Properties
Capture Image
Summary
Progress
Completion
Include software updates
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


Create Task Sequence Wizard
Install Applications
Create New Task Sequence
Task Sequence Informatic
Install Windows
Configure Network
Install Configuration Mar
Include Updates
Install Applications
System Preparation
Image Properties
Capture Image
Summary
Progress
Completion
Install applications
Select the applications to be run with this operating system image.
Applications:
Application name
Description
19.00 (x64 edition)
If an application installation fails, continue installing other applications in the list

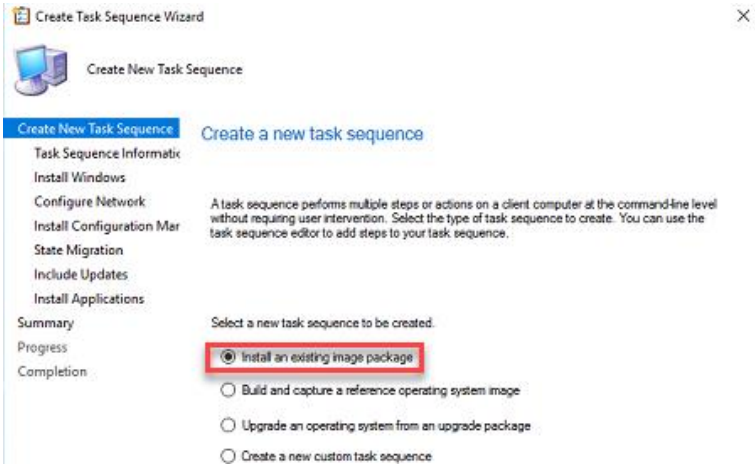


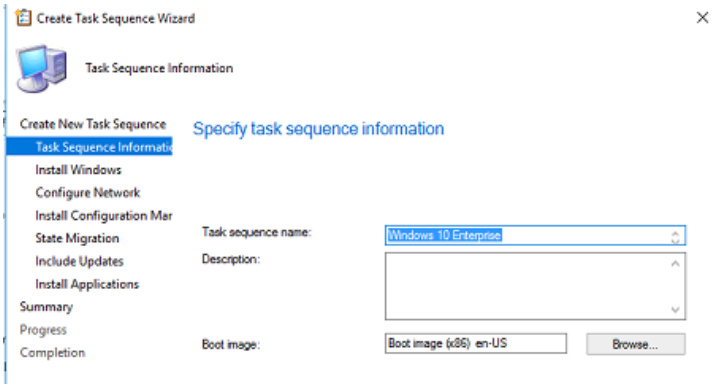


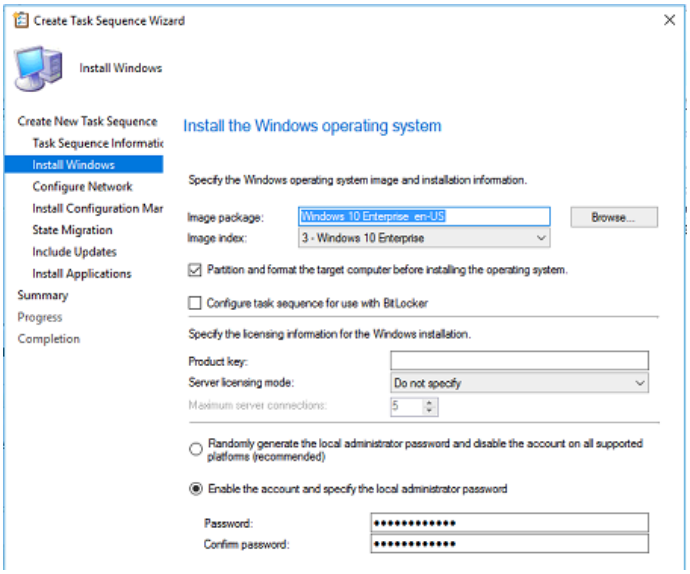
1- Proceed to release it on a distribution point and then deploy it to an unidentified computer to allow for network installation.
2- Ensure the task is distributed to the distribution point and set up deployment targeting the unknown client if necessary to support Non-CM clients.

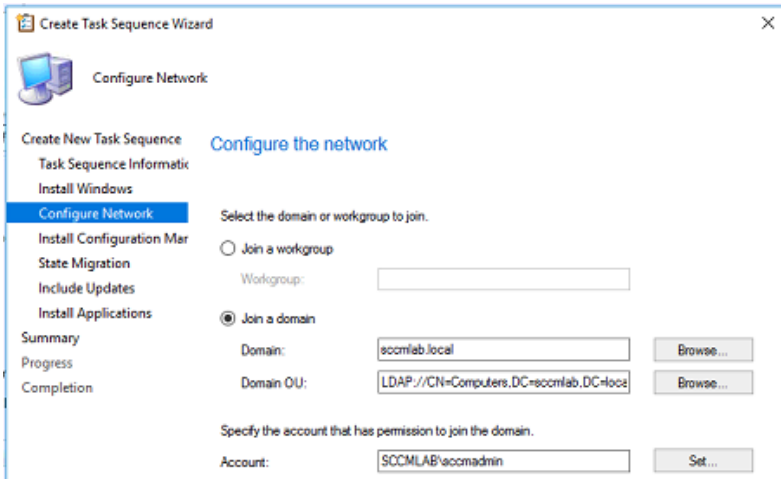
Deploy Windows 10 Enterprise without capture

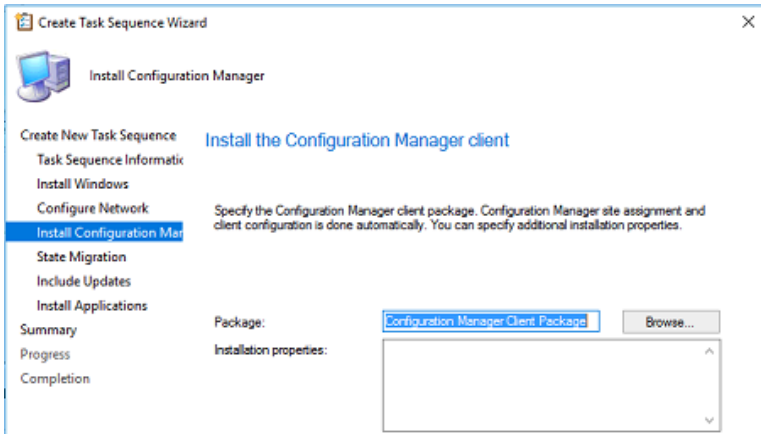
Create Windows 10 Image for 10 Enterprise then follow steps down:

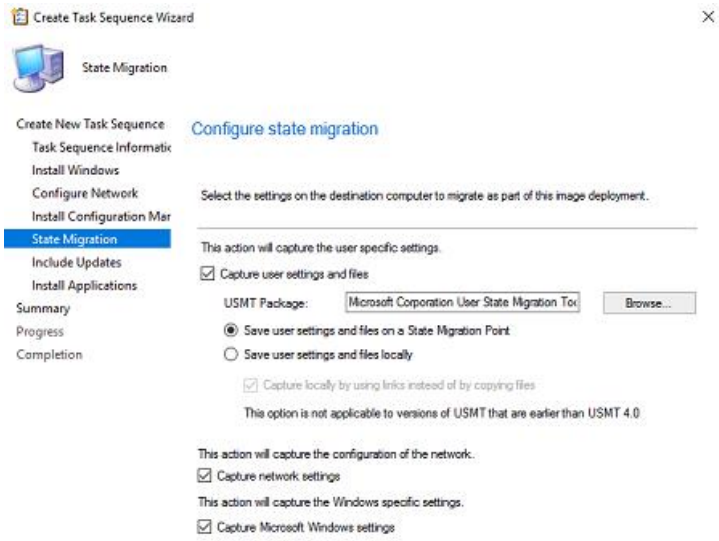


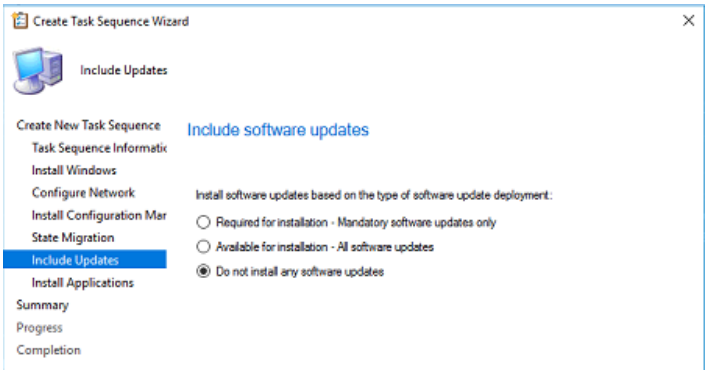


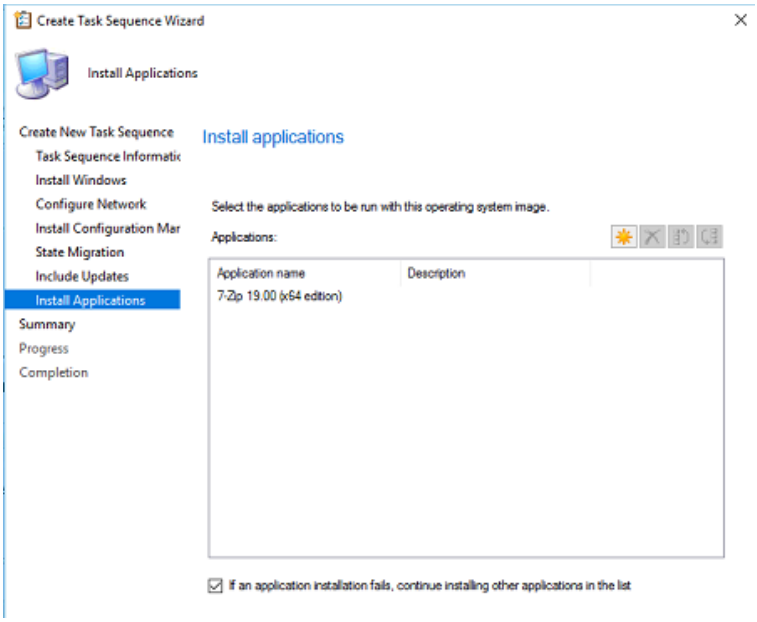


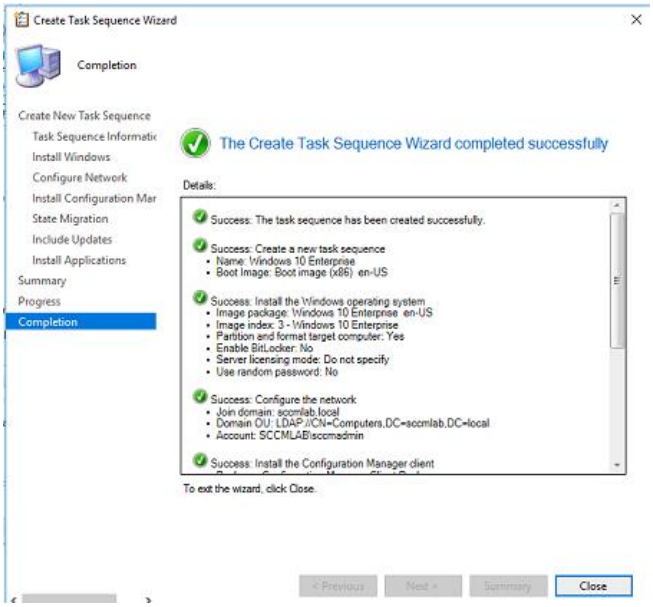

Create Task Sequence Wizard
Configure Network
Create New Task Sequence
Task Sequence Informatic
Install Windows
Configure Network
Install Configuration Mar
State Migration
Include Updates
Install Applications
Summary
Progress
Completion
Configure the network
Select the domain or workgroup to join.
Join a workgroup
Workgroup:
Join a domain
Domain:
sccmlab.local
Browse...
Domain OU:
LDAP://CN=Computers,DC=sccmlab,DC=loca
Browse...
Specify the account that has permission to join the domain.
Account:
SCCMLAB\sccmadmin
Set...


Create Task Sequence Wizard
Install Configuration Manager
Create New Task Sequence
Task Sequence Informatic
Install Windows
Configure Network
Install Configuration Mar
State Migration
Include Updates
Install Applications
Summary
Progress
Completion
Install the Configuration Manager client
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:

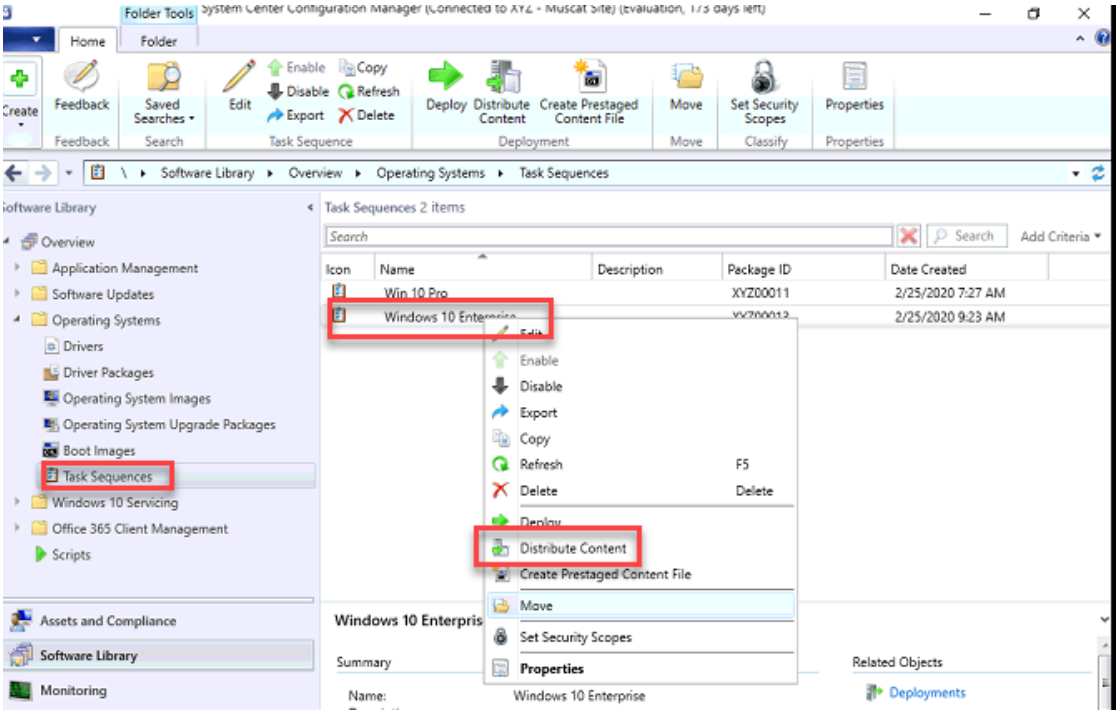

Create Task Sequence Wizard
State Migration
Create New Task Sequence
Task Sequence Informatic
Install Windows
Configure Network
Install Configuration Mar
State Migration
Include Updates
Install Applications
Summary
Progress
Completion
Configure state migration
Select the settings on the destination computer 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

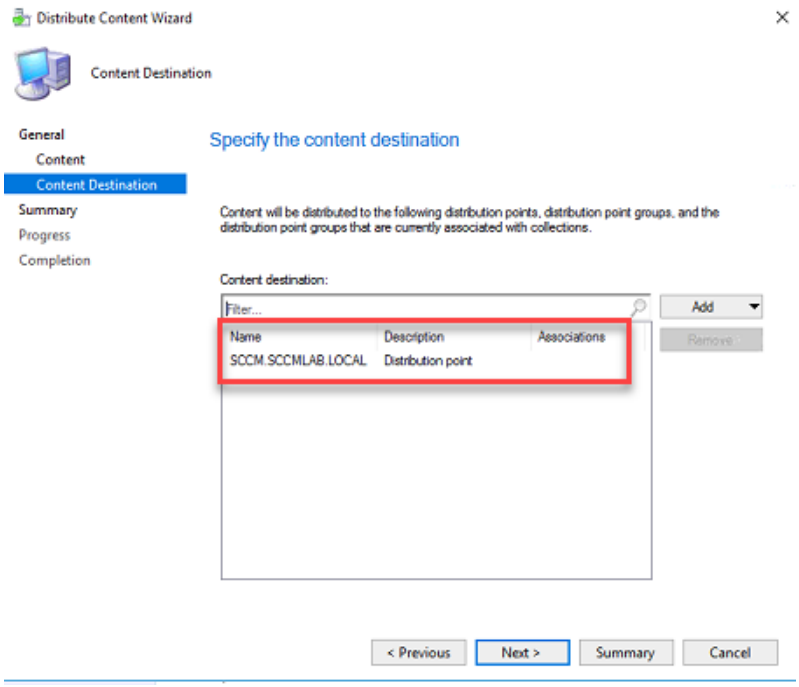

Create Task Sequence Wizard
Include Updates
Create New Task Sequence
Task Sequence Informatic
Install Windows
Configure Network
Install Configuration Mar
State Migration
Include Updates
Install Applications
Summary
Progress
Completion
Include software updates
Install software updates based on the type of software update deployment:
Required for installation - Mandatory software updates only
Available for installation - All software updates
Do not install any software updates

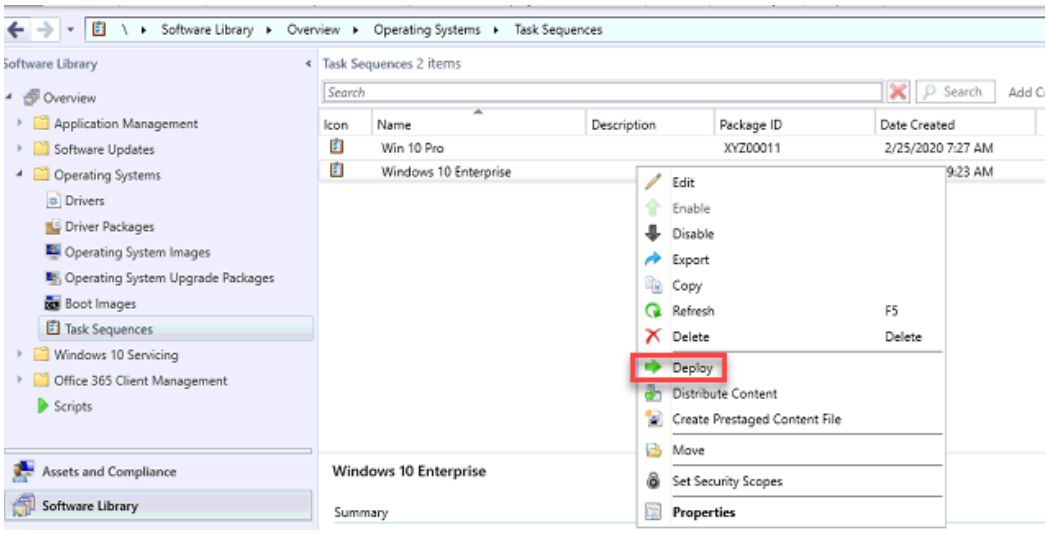

Create Task Sequence Wizard
Install Applications
Create New Task Sequence
Task Sequence Informatic
Install Windows
Configure Network
Install Configuration Mar
State Migration
Include Updates
Install Applications
Summary
Progress
Completion
Install applications
Select the applications to be run with this operating system image.
Applications:
Application name
Description
7-Zip 19.00 (x64 edition)
If an application installation fails, continue installing other applications in the list

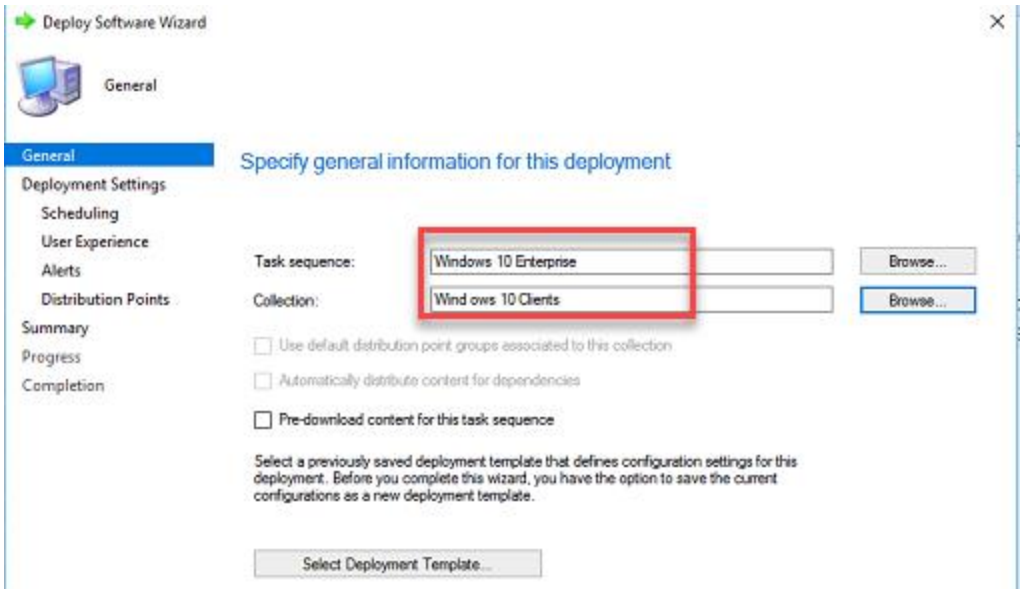

Create Task Sequence Wizard
Completion
Create New Task Sequence
Task Sequence Informatic
Install Windows
Configure Network
Install Configuration Mar
State Migration
Include Updates
Install Applications
Summary
Progress
Completion
The Create Task Sequence Wizard completed successfully
Details:
Success: The task sequence has been created successfully.
Success: Create a new task sequence
Name: Windows 10 Enterprise
Boot Image: Boot image (x86) en-US
Success: Install the Windows operating system
Image package: Windows 10 Enterprise en-US
Image index: 3 - Windows 10 Enterprise
Partition and format target computer: Yes
Enable BitLocker: No
Server licensing mode: Do not specify
Use random password: No
Success: Configure the network
Join domain: scomlab.local
Domain OU: LDAP://CN=Computers,DC=scomlab,DC=local
Account: SCCMLAB\sccmadmin
Success: Install the Configuration Manager client
To exit the wizard, click Close.
< Previous
Next >
Summary
Close

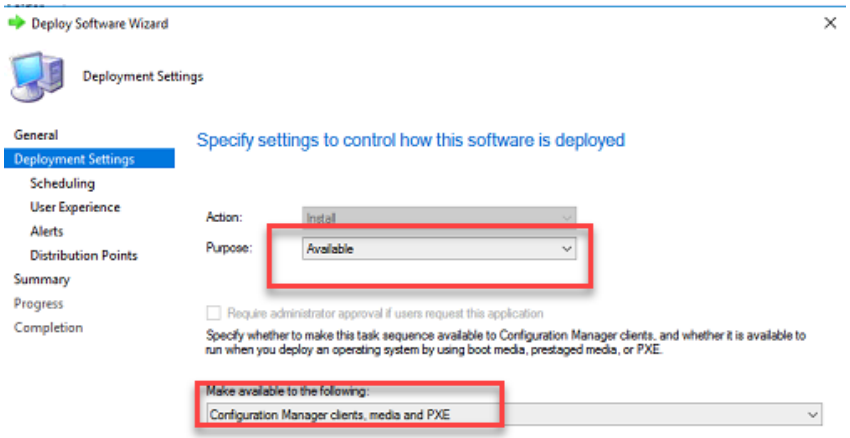
Distribute and Deploy

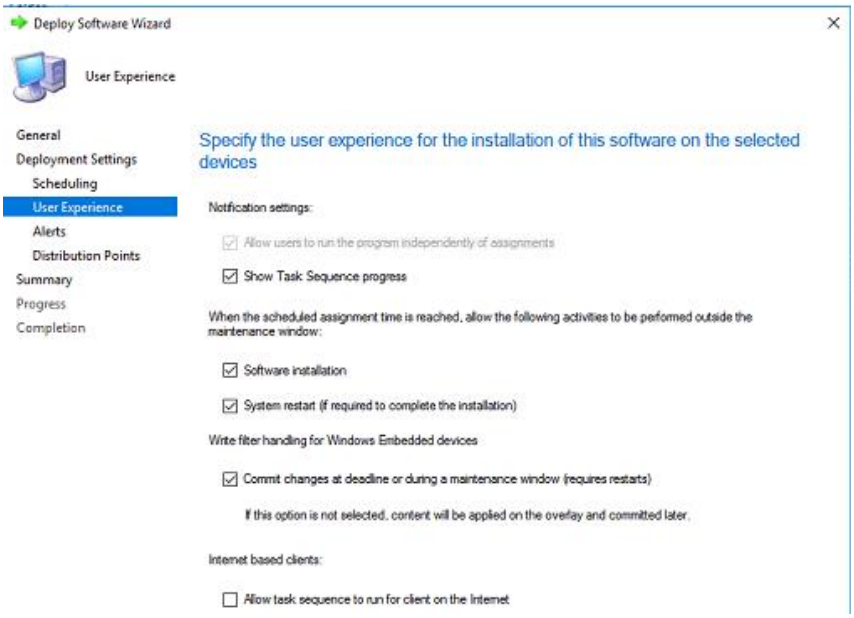


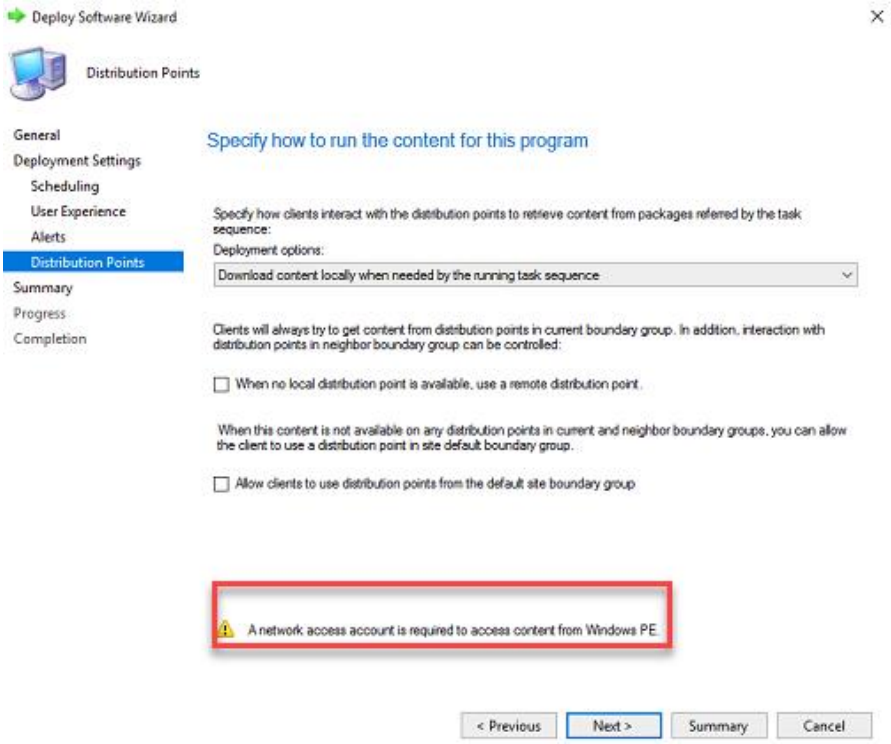


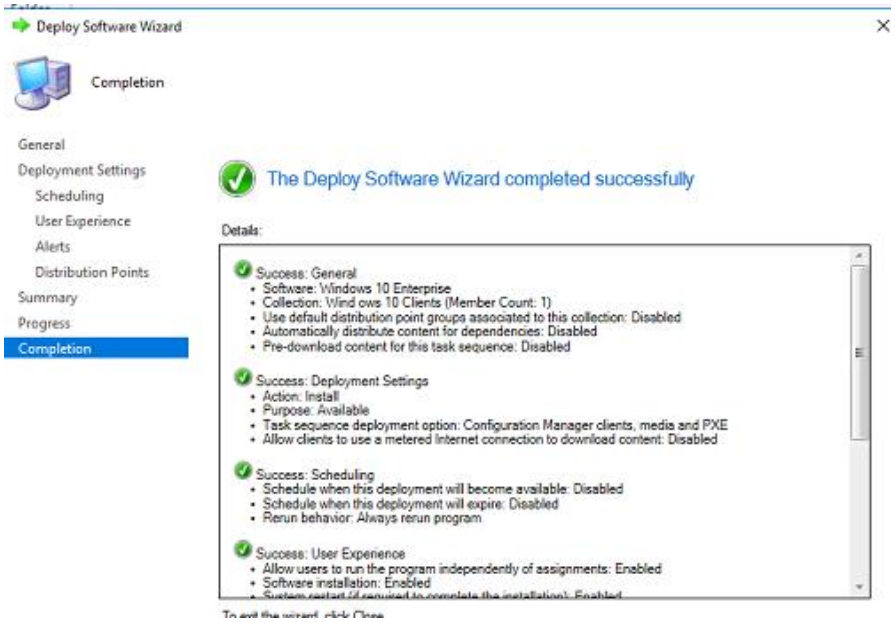

Software Library ▸ Overview ▸ Operating Systems ▸ Task Sequences
Software Library
Overview
Application Management
Software Updates
Operating Systems
Drivers
Driver Packages
Operating System Images
Operating System Upgrade Packages
Boot Images
Task Sequences
Windows 10 Servicing
Office 365 Client Management
Scripts
Assets and Compliance
Software Library
Task Sequences 2 items
Search
Icon
Name
Description
Package ID
Date Created
Win 10 Pro
XYZ00011
2/25/2020 7:27 AM
Windows 10 Enterprise
9:23 AM
Edit
Enable
Disable
Export
Copy
Refresh
F5
Delete
Delete
Deploy
Distribute Content
Create Prestaged Content File
Move
Set Security Scopes
Properties
Windows 10 Enterprise
Summary

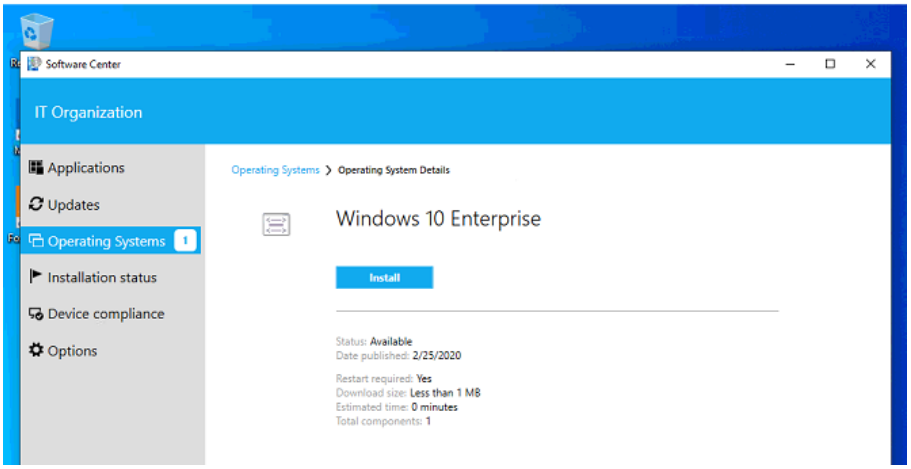

Deploy Software Wizard
General
General
Deployment Settings
Scheduling
User Experience
Alerts
Distribution Points
Summary
Progress
Completion
Specify general information for this deployment
Task sequence:
Windows 10 Enterprise
Browse...
Collection:
Wind ows 10 Clients
Browse...
Use default distribution point groups associated to this collection
Automatically distribute content for dependencies
Pre-download content for this task sequence
Select a previously saved deployment template that defines configuration settings for this deployment. Before you complete this wizard, you have the option to save the current configurations as a new deployment template.
Select Deployment Template...

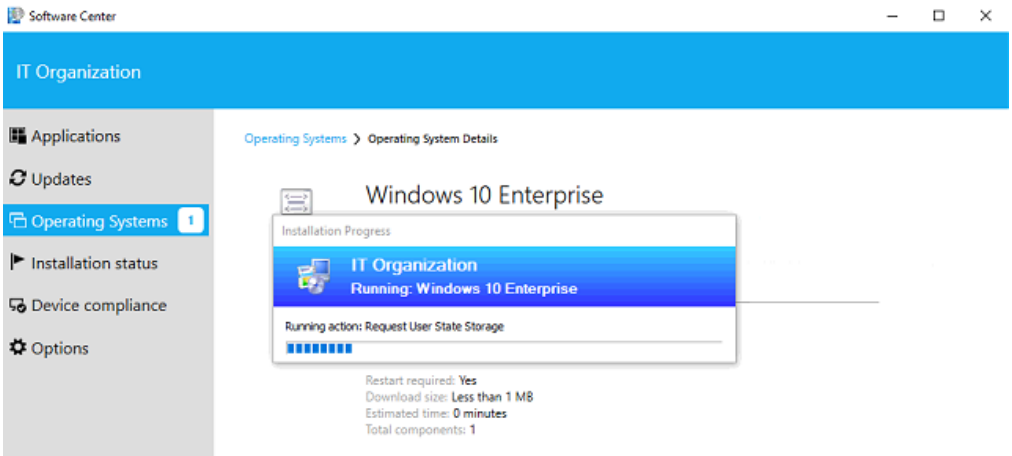

Deploy Software Wizard
Deployment Settings
General
Deployment Settings
Scheduling
User Experience
Alerts
Distribution Points
Summary
Progress
Completion
Specify settings to control how this software is deployed
Action:
Install
Purpose:
Available
Require administrator approval if users request this application
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:
Configuration Manager clients, media and PXE


Deploy Software Wizard
User Experience
General
Deployment Settings
Scheduling
User Experience
Alerts
Distribution Points
Summary
Progress
Completion
Specify the user experience for the installation of this software on the selected devices
Notification settings:
Allow users to run the program independently of assignments
Show Task Sequence progress
When the scheduled assignment time 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.
Internet based clients:
Allow task sequence to run for client on the Internet


Deploy Software Wizard
Distribution Points
General
Deployment Settings
Scheduling
User Experience
Alerts
Distribution Points
Summary
Progress
Completion
Specify how to run the content for this program
Specify how clients interact with the distribution points to retrieve content from packages referred by the task sequence:
Deployment options:
Download content locally when needed by the running task sequence
Clients will always try to get content from distribution points in current boundary group. In addition, interaction with distribution points in neighbor boundary group can be controlled:
When no local distribution point is available, use a remote distribution point.
When this content is not available on any distribution points in current and neighbor boundary groups, you can allow the client to use a distribution point in site default boundary group.
Allow clients to use distribution points from the default site boundary group
A network access account is required to access content from Windows PE.
< Previous
Next >
Summary
Cancel


Deploy Software Wizard
Completion
General
Deployment Settings
Scheduling
User Experience
Alerts
Distribution Points
Summary
Progress
Completion
The Deploy Software Wizard completed successfully
Details:
Success: General
Software: Windows 10 Enterprise
Collection: Wind ows 10 Clients (Member Count: 1)
Use default distribution point groups associated to this collection: Disabled
Automatically distribute content for dependencies: Disabled
Pre-download content for this task sequence: Disabled
Success: Deployment Settings
Action: Install
Purpose: Available
Task sequence deployment option: Configuration Manager clients, media and PXE
Allow clients to use a metered Internet connection to download content: Disabled
Success: Scheduling
Schedule when this deployment will become available: Disabled
Schedule when this deployment will expire: Disabled
Rerun behavior: Always rerun program
Success: User Experience
Allow users to run the program independently of assignments: Enabled
Software installation: Enabled


Software Center
IT Organization
Applications
Updates
Operating Systems 1
Installation status
Device compliance
Options
Operating Systems > Operating System Details
Windows 10 Enterprise
Install
Status: Available
Date published: 2/25/2020
Restart required: Yes
Download size: Less than 1 MB
Estimated time: 0 minutes
Total components: 1


Software Center
IT Organization
Applications
Updates
Operating Systems 1
Installation status
Device compliance
Options
Operating Systems > Operating System Details
Windows 10 Enterprise
Installation Progress
IT Organization
Running: Windows 10 Enterprise
Running action: Request User State Storage
Restart required: Yes
Download size: Less than 1 MB
Estimated time: 0 minutes
Total components: 1

Installing with User State Migration using Microsoft Deployment Toolkit (MDT) and SCCM

Performing an installation with user state migration involves integrating Microsoft Deployment Toolkit (MDT) with System Center Configuration Manager (SCCM) and configuring the necessary settings to capture and restore user state. Here are the detailed steps:

1. Download and Install MDT

- **Download MDT**:
  - Download the latest version of Microsoft Deployment Toolkit from the Microsoft Download Center.
- **Install MDT on the SCCM Server**:
  - Run the MDT installer on the SCCM server.
  - During the installation, select the option "Install the MDT extensions for Configuration Manager" to integrate MDT with SCCM.

2. Configure SCCM with MDT Extensions

- **Close and Reopen SCCM Console**:
  - Close the SCCM console and reopen it to ensure that the MDT extensions are loaded.

3. Create MDT Task Sequence in SCCM

- **Navigate to Task Sequences**:
  - In the SCCM console, go to Software Library -> Overview -> Operating Systems -> Task Sequences.
- **Create MDT Task Sequence**:
  - In the left-hand pane, select Create MDT Task Sequence.
  - This will open the Create MDT Task Sequence wizard.

4. Configure MDT Task Sequence

- **Select Deployment Share**:
  - In the wizard, select the deployment share where the MDT files are stored.
- **Select Operating System and Architecture**:
  - Choose the operating system (e.g., Windows 10) and the architecture (e.g., x64) that you want to install.
- **Configure Task Sequence Settings**:
  - Configure various task sequence settings, such as task sequence name, description, and boot image.

5. Configure User State Migration

- **User State Capture and Restore**:
  - In the task sequence wizard, configure the user state migration settings:
    - **Capture User State**: Select options to capture the user state during the deployment process.
    - **Restore User State**: Select options to restore the user state after the operating system installation.
- **Specify User State Store Location**:
  - Define the network location or local storage where the user state data will be temporarily stored.

---

6. Additional Task Sequence Settings

- **Network Settings**:
  - Specify network settings, such as IP configuration and DNS settings.
- **Computer Name and Domain Join Information**:
  - Configure the computer name settings and domain join information.

7. Review and Finish

  - Review the summary of the task sequence settings.
  - Click Finish to create the MDT task sequence.

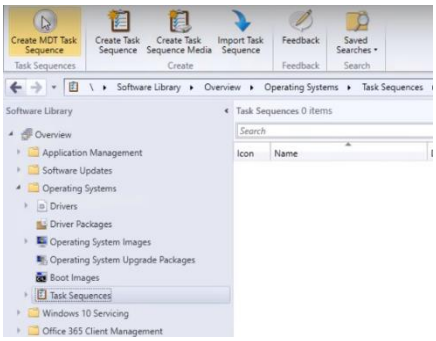
8. Deploy Task Sequence

- **Deploy to Target Clients**:
  - After creating the MDT task sequence, deploy it to the target client computers:
    - Right-click the task sequence and select Deploy.
    - Choose the collection of client computers that you want to target.
- **Deployment Settings**:
  - Configure deployment settings, such as making the deployment available or required, and schedule the deployment.

Example Scenario: Deploying Windows 10 with User State Migration

Scenario: You need to deploy Windows 10 to client computers while capturing and restoring user state.

1. **Download and Install MDT**:
   - Download MDT from the Microsoft Download Center and install it on the SCCM server.
   - Select "Install the MDT extensions for Configuration Manager" during installation.
2. **Configure SCCM with MDT Extensions:**
   - Close and reopen the SCCM console to load the MDT extensions.
3. **Create MDT Task Sequence:**
   - In SCCM, go to Software Library -> Operating Systems -> Task Sequences.
   - Select Create MDT Task Sequence and follow the wizard.
4. **Configure Task Sequence:**
   - Select the MDT deployment share.
   - Choose Windows 10 (x64) as the operating system.
   - Configure user state migration to capture and restore user state.
   - Define network settings, computer name, and domain join information.
   - Review and finish the task sequence creation.



5. **Deploy Task Sequence:**
   - Right-click the MDT task sequence and select Deploy.
   - Target the appropriate collection of client computers.
   - Configure deployment settings and schedule.

Upgrading Microsoft Endpoint Configuration Manager

Upgrading Microsoft Endpoint Configuration Manager (ConfigMgr) ensures your organization maintains security, functionality, support, compatibility, and performance. Here's a comprehensive guide to upgrade ConfigMgr:

1. Plan the Upgrade

- **Review the Release Notes**:
  - Understand new features, functionalities, and changes in the new version of ConfigMgr.
- **Check Requirements**:
  - Ensure your hardware, software, and network infrastructure meet the new version's requirements.
- **Review Customizations**:
  - Check if your customizations will be compatible with the new version.
- **Determine Upgrade Strategy**:
  - Decide between an in-place upgrade (simpler) or a side-by-side migration (less risky, more flexible).
- **Create an Upgrade Plan**:
  - List tasks, timelines, and responsibilities in detail.

2. Prepare for the Upgrade

- **Backup the Configuration Manager Database**:
  - Backup the ConfigMgr database to protect against any issues during the upgrade.
- **Install Prerequisite Software**:
  - Install any additional software required by the new ConfigMgr version (e.g., .NET Framework, SQL Server).
- **Download Installation Media**:
  - Obtain the installation media for the new ConfigMgr version.
- **Run the Prerequisite Checker Tool**:
  - Ensure all prerequisites are met and resolve any highlighted issues.

3. Upgrade the Site Server

- **Run the Setup Program**:
  - Start the setup program and follow the wizard to upgrade the site server.
- **Choose Upgrade Option**:
  - Select between an in-place upgrade or side-by-side migration.
- **Enter Product Key**:
  - Enter the product key for the new ConfigMgr version.
- **Choose Installation Location**:
  - Specify where to install the new ConfigMgr version.
- **Follow the Wizard**:
  - Complete the wizard to finish the site server upgrade.

---

4. Upgrade Client Agents

- **Automatic Client Upgrade**:
  - Use the automatic client upgrade feature to upgrade client agents during a specified maintenance window.
- **Software Update Deployment**:
  - Deploy a software update containing the new ConfigMgr client to client computers.
- **Script or Group Policy**:
  - Use a script or group policy to install the new ConfigMgr client on client computers.

5. Verify the Upgrade

- **Check the Configuration Manager Console**:
  - Verify that all ConfigMgr components (site server, management points, distribution points, reporting services) are functioning correctly.
- **Check Client Status**:
  - Ensure all client agents have been successfully upgraded and are reporting to the new version of ConfigMgr.

6. Update Configuration Manager Clients

- **Take Advantage of New Features**:
  - Update the ConfigMgr client on each managed computer to use new features.
  - This can be done using automatic client upgrades, software update deployments, scripts, or group policies.

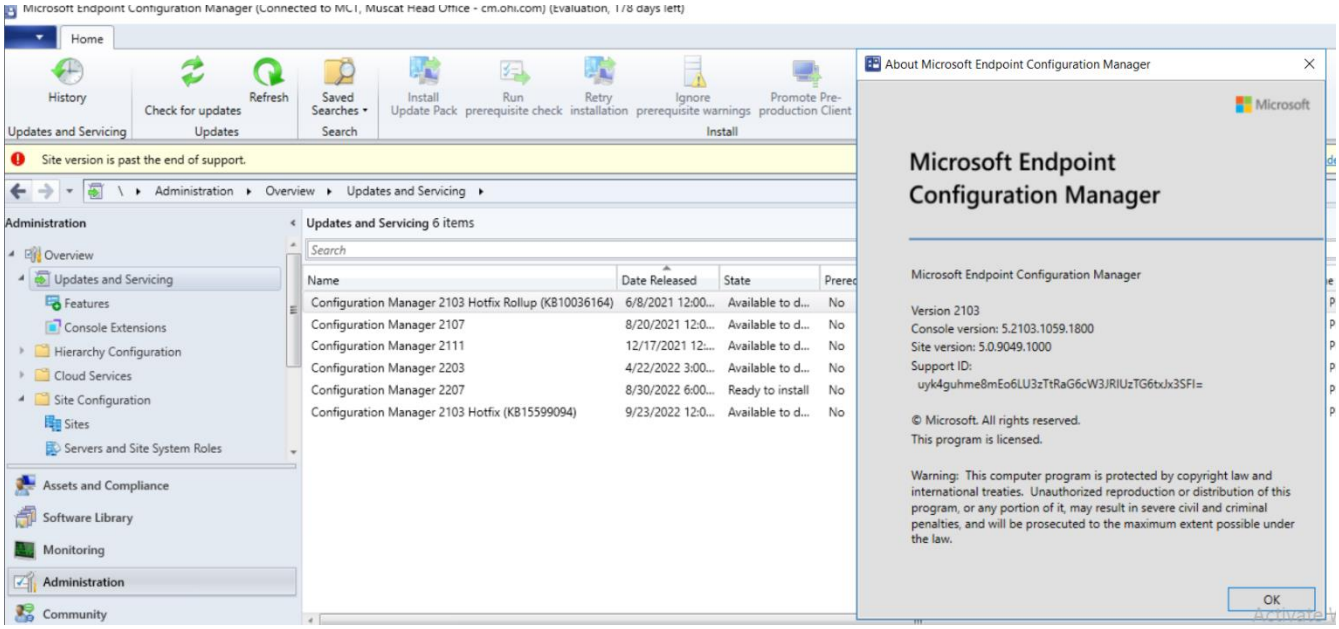
Example Scenario: Upgrading ConfigMgr

Scenario: You need to upgrade ConfigMgr from version 2002 to version 2103.

1. **Plan the Upgrade**:
   - Review release notes for ConfigMgr version 2103.
   - Check that your infrastructure meets the requirements for version 2103.
   - Review customizations and decide to perform an in-place upgrade.
   - Create a detailed upgrade plan.
2. **Prepare for the Upgrade:**
   - Backup the ConfigMgr database.
   - Ensure .NET Framework and SQL Server are updated to required versions.
   - Download ConfigMgr 2103 installation media.
   - Run the prerequisite checker tool and resolve any issues.
3. **Upgrade the Site Server:**
   - Run the ConfigMgr setup program.
   - Select in-place upgrade.
   - Enter the product key for version 2103.
   - Specify the installation location.
   - Follow the wizard to complete the site server upgrade.

---

4. **Upgrade Client Agents:**
    - Configure automatic client upgrade during a maintenance window.
    - Deploy the ConfigMgr 2103 client as a software update to all client computers.
    - Optionally, use a script or group policy for additional coverage.
5. **Verify the Upgrade:**
    - Check the ConfigMgr console to ensure all components are functioning.
    - Verify client status and confirm that all client agents report to ConfigMgr 2103.
6. **Update Configuration Manager Clients:**
    - Ensure all managed computers have the ConfigMgr 2103 client installed to leverage new features.



Backup and Restore Site System Data in SCCM

Backing up and restoring site system data in System Center Configuration Manager (SCCM) is crucial for data protection and disaster recovery. Here's a detailed guide on how to perform these tasks:

Backup Site System Data

1. **Open SCCM Console**:
   - Navigate to Administration -> Site Configuration -> Sites.
2. **Access Site Maintenance:**
   - Right-click on the site you want to back up and select Site Maintenance.
3. **Select Backup Option:**
   - In the "Site Maintenance" dialog box, select Backup ConfigMgr Site Server and click Next.
4. **Specify Backup Location:**
   - On the "Backup Site Server" screen, select the backup location.
   - Enter the credentials for accessing the backup location (network share or local drive).
5. **Choose Data to Backup:**
   - On the "Backup Settings" screen, choose to back up the site database, SCCM installation folder, or both.
6. **Set Backup Schedule:**
   - On the "Schedule" screen, select the backup schedule.
   - Choose to run the backup immediately or schedule it for a specific time.
7. **Review and Start Backup:**
   - Click Next to review the backup settings.
   - Click Next again to start the backup process.
8. **Verify Backup:**
   - Once the backup is complete, verify the backup by checking the backup location for the backup files.

Restore Site System Data

1. **Open SCCM Console**:
   - Navigate to Administration -> Site Configuration -> Sites.
2. **Access Site Maintenance:**
   - Right-click on the site you want to restore and select Site Maintenance.
3. **Select Restore Option:**
   - In the "Site Maintenance" dialog box, select Restore ConfigMgr Site Server and click Next.
4. **Specify Restore Location:**
   - On the "Restore Site Server" screen, select the backup location.
   - Enter the credentials for accessing the backup location.
5. **Choose Data to Restore:**
   - On the "Backup Selection" screen, select the backup files you want to restore (site database, SCCM installation folder, or both).

6. **Set Restore Options:**
    - On the "Restore Settings" screen, choose to overwrite the existing site data or restore the data to a new location.
7. **Set Restore Schedule:**
    - On the "Schedule" screen, select the restore schedule.
    - Choose to restore the backup immediately or schedule it for a specific time.
8. **Review and Start Restore:**
    - Click Next to review the restore settings.
    - Click Next again to start the restore process.

Example Scenario: Backing Up and Restoring SCCM Site Data

Scenario: You need to back up and restore your SCCM site data to ensure data protection and prepare for disaster recovery.

1. **Open SCCM Console**:
    - Go to Administration -> Site Configuration -> Sites.
2. **Site Maintenance**:
    - Right-click your site and select Site Maintenance.
    - Choose Backup ConfigMgr Site Server and click Next.
3. **Backup Location**:
    - Select a network share (e.g., \\backupserver\backups) and provide credentials.
    - Choose to back up both the site database and the SCCM installation folder.
4. **Schedule Backup**:
    - Schedule the backup to run daily at 2 AM.
    - Review and confirm settings, then start the backup.
5. **Verify**:
    - Check \\backupserver\backups for backup files to ensure the backup completed successfully.

Steps to Restore:

2. **Open SCCM Console**:
    - Go to Administration -> Site Configuration -> Sites.
3. **Site Maintenance**:
    - Right-click your site and select Site Maintenance.
    - Choose Restore ConfigMgr Site Server and click Next.
4. **Restore Location**:
    - Enter \\backupserver\backups and provide credentials.
    - Select the backup files for both the site database and the SCCM installation folder.
5. **Restore Settings**:
    - Choose to overwrite existing site data.
    - Schedule the restore to run immediately.
6. **Review and Confirm**:
    - Review the restore settings.
    - Start the restore process.