Project Story: SCCM Implementation for Mstile

Background: Mstile has experienced rapid growth and now needs an efficient system to manage their computers and IT resources. Microsoft recommends System Center Configuration Manager (SCCM) as a comprehensive solution for both client and server management.

Objective: Mstile would like us to set up a demo environment to showcase how SCCM works and how it can streamline their IT management.

Preparations:

1. **Active Directory Server:**
    - Install and configure an Active Directory server to handle domain control and authentication.
2. **SCCM Server:**
    - Install Windows Server 2019 on a server that will be used for the SCCM installation.
3. **Applications:**
    - Download all necessary applications and installation files from Google Drive to prepare for the SCCM setup and configuration.
4. **Client Machine:**
    - Create a virtual machine with Windows 10 to serve as the client machine in the demo environment.

By completing these preparations, we will create a functional demo environment that demonstrates SCCM's capabilities and how it can enhance Mstile's IT management.

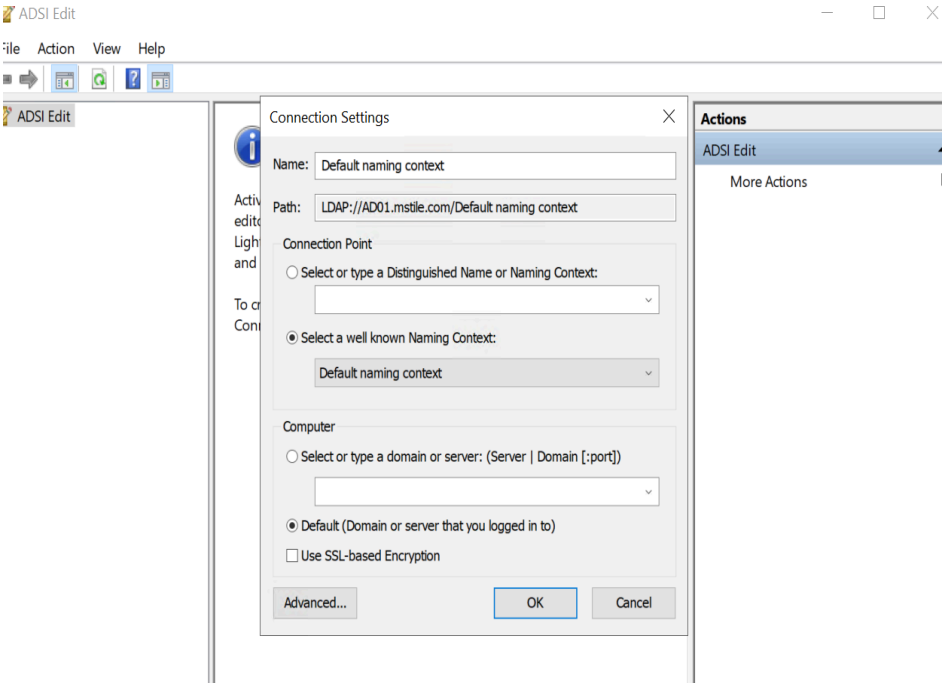
DEL 1:

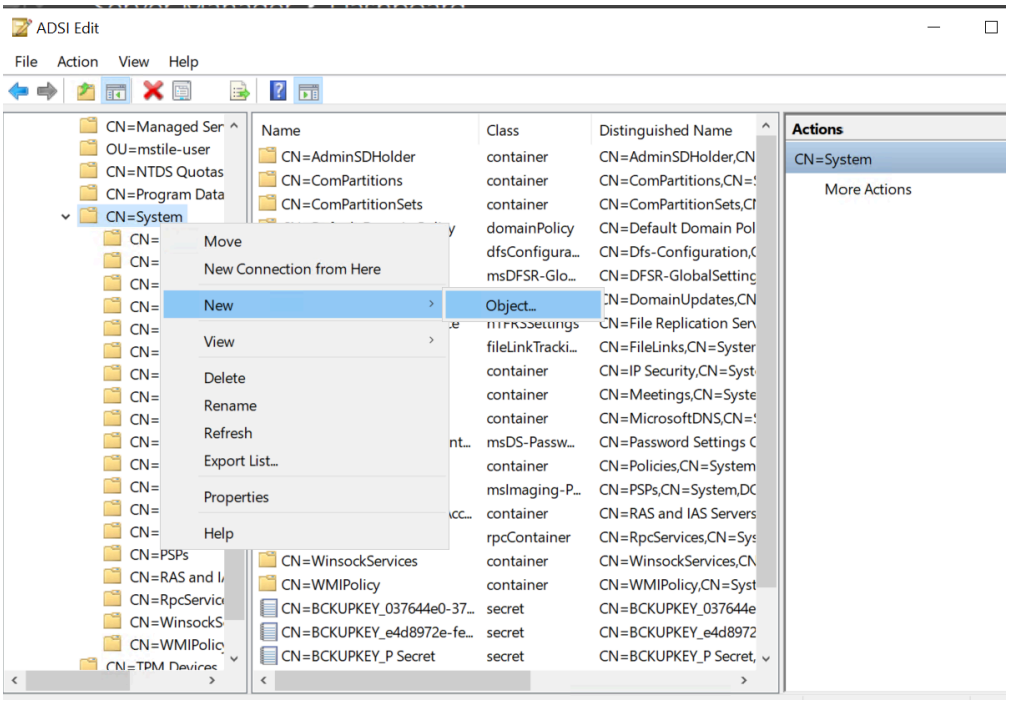
Via PowerShell, I installed the Active Directory (AD) server with the IP address `192.168.100.10`, then set up the AD server and used the domain name `Mstile.com`.

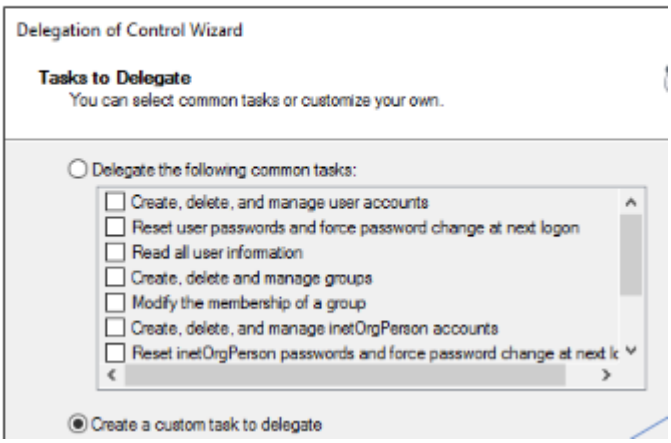
SCCM Installation:

For this deployment, we need an AD server where we install the AD role and connect it to the router. After completing the AD role installation, follow these steps in **ADSI Edit** to create a system container:

1. Open **ADSI Edit**.
2. Connect to the **Default Naming Context**.
3. Select a well-known naming context and choose **Default Domain**, then click **OK**.
4. Expand **Default Naming Context**.
5. Right-click on **Object**, select **Create Object**, and choose **Container**.
6. For the **Value** field, enter `SYSTEM MANAGEMENT`, then click **OK**.


ADSI Edit
File Action View Help
ADSI Edit
Connection Settings
Name: Default naming context
Path: LDAP://AD01.mstile.com/Default naming context
Connection Point
Select or type a Distinguished Name or Naming Context:
Select a well known Naming Context:
Default naming context
Computer
Select or type a domain or server: (Server | Domain [:port])
Default (Domain or server that you logged in to)
Use SSL-based Encryption
Advanced...
OK
Cancel
Actions
ADSI Edit
More Actions


ADSI Edit
File Action View Help
CN=Managed Ser
OU=mstile-user
CN=NTDS Quotas
CN=Program Data
CN=System
Move
New Connection from Here
New
View
Delete
Rename
Refresh
Export List...
Properties
Help
Object...
Name
Class
Distinguished Name
CN=AdminSDHolder container CN=AdminSDHolder,CN
CN=ComPartitions container CN=ComPartitions,CN=
CN=ComPartitionSets container CN=ComPartitionSets,CN
CN=WinsockServices container CN=WinsockServices,CN
CN=WMIPolicy container CN=WMIPolicy,CN=Syst
CN=BCKUPKEY_037644e0-37... secret CN=BCKUPKEY_037644e
CN=BCKUPKEY_e4d8972e-fe... secret CN=BCKUPKEY_e4d8972
CN=BCKUPKEY_P Secret secret CN=BCKUPKEY_P Secret,
Actions
CN=System
More Actions



Delegating Control of the System Management Container

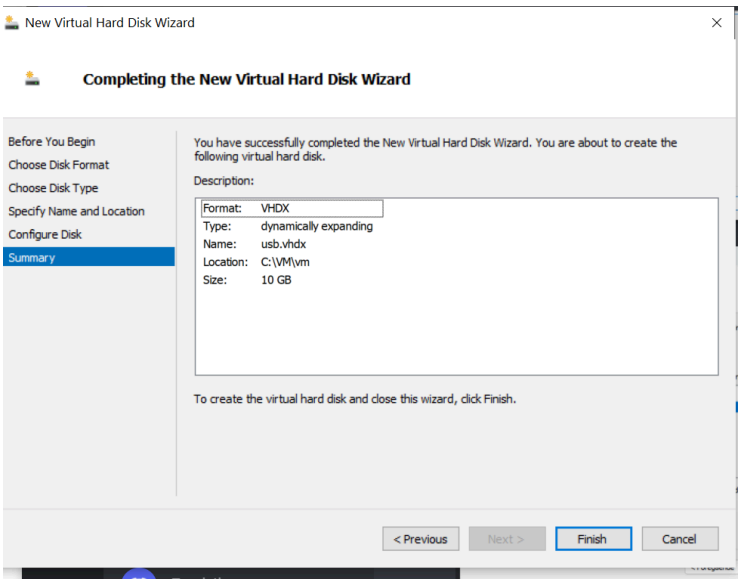
1. **Open Active Directory Users and Computers**:
   - In **Active Directory Users and Computers**, go to the **View** menu and select **Advanced Features**.
2. **Locate the System Management Container**:
   - Expand the **System** node in the console tree.
   - You should see the **System Management** container.
3. **Delegate Control**:
   - Right-click on the **System Management** container and select **Delegate Control**.
   - Click **Next** to start the Delegation of Control Wizard.
4. **Add the SCCM Server**:
   - Click **Add** to specify which object will be granted delegated control.
   - Change the **Location** if needed, and click **Object Types**.
   - Check **Computer** (note: by default, computer objects are not included in AD, so you need to enable this option).
   - In the **Object** field, type the name of the SCCM server computer (e.g., `SCCM`), and click **OK**.
5. **Create a Custom Task**:
   - You should now see the SCCM server (e.g., `SCCM (mstile/SCCM)`).
   - Select **Create a custom task to delegate**, and click **Next**.
   - Choose **Delegate control**, then click **Next**.
6. **Set Permissions**:
   - In the permissions section, select **Full Control** or **Everything** to grant the SCCM server all necessary permissions.
   - Click **Next** to complete the delegation process.
7. **Finish**:
   - Review the summary and click **Finish** to apply the delegation.

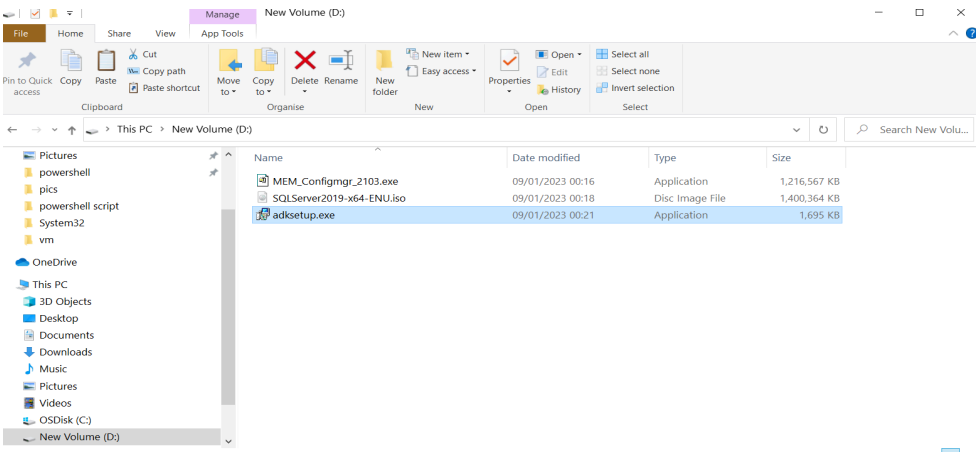
The System Management container is now successfully delegated, and the SCCM server has the necessary rights to manage it.

!

AD Schema Setup

1. **Create a Virtual Hard Disk in Hyper-V**:
    - Open **Hyper-V Manager**.
    - Select the appropriate virtual machine (VM) where you want to add the new hard disk.
    - Right-click the VM and select **Settings**.
    - Under **Hardware**, click **Add Hard Disk**.
    - Choose **Virtual Hard Disk** and click **Next**.
    - Select **Dynamic** as the disk type and set the size to **10 GB**.
    - Click **Next**, review your settings, and click **Finish**.
2. **Initialize and Format the New Disk**:
    - Go to **Computer Management** on your host machine (you can access it via **Control Panel** > **Administrative Tools** > **Computer Management**).
    - Select **Disk Management** under **Storage**.
    - You should see the new 10 GB disk listed as unallocated. Right-click on it and choose **Initialize Disk**.
    - Create a new volume by right-clicking the unallocated space and selecting **New Simple Volume**.
    - Follow the wizard to format the disk (choose NTFS as the file system) and assign a drive letter.
3. **Prepare the Disk for Application and ISO Files**:
    - Once formatted, open the newly created drive.
    - Download all necessary applications and ISO files for Windows Server 2019.
    - Copy these files to the new drive.
4. **Eject the Disk from the Host**:
    - Ensure that all files have been copied and no applications are using the disk.
    - Right-click the drive in **Disk Management** and select **Remove** to safely eject it, or simply shut down the VM to detach the virtual disk.
5. **Attach the Disk to the AD Server VM**:
    - In **Hyper-V Manager**, right-click on the AD server VM and select **Settings**.
    - Under **Hardware**, click **Add Hard Disk**.
    - Choose **Existing** and browse to the location where the virtual disk file was saved.
    - Attach the disk to the VM.
6. **Start the AD Server VM**:
    - Start the AD server VM from **Hyper-V Manager**.
    - Log in to the VM and verify that the new drive is visible and accessible in **File Explorer**.





Initializing the New Disk and Installing SCCM Schema

1. **Initialize the New Disk on the AD Server**:
    - Open **Computer Management** on the AD server.
    - Go to **Disk Management** under **Storage**.
    - You should see the new disk listed as uninitialized. Right-click on the disk and select **Initialize Disk**.
    - Follow the prompts to initialize the disk.
2. **Unzip and Install SCCM Schema**:
    - Unzip the file `Mem-configmgr` to the C: drive of the AD server.
    - Navigate to the location: `C:\bin\x64`.
    - Find the file named `extadsch` and open **File Explorer** to this location.
    - Click the **Home** tab in **File Explorer** and select **Copy path** to copy the full path of the `extadsch` file.
3. **Run the Schema Extension Tool**:
    - Open **Command Prompt** as an Administrator.

- Paste the copied path of `extadsch` into the Command Prompt and press **Enter**.
- This command will run the schema extension tool and install the SCCM schema updates.

4. **Turn Off the AD Server**:
   - Once the schema installation is complete, shut down the AD server.

Creating the SCCM Server

1. **Create and Configure the SCCM Server**:
   - Open **PowerPoint** to create a new presentation. This seems unusual, but if it's required for documentation or a planning purpose, use PowerPoint to prepare any relevant slides or diagrams.
   - Set up the SCCM server with the following network configuration:
     - **IP Address**: `192.168.100.11`
     - **Default Gateway**: `192.168.100.10`
   - Connect the SCCM server to the domain `mstile.com`.
2. **Complete SCCM Server Setup**:
   - Make sure the SCCM server is properly connected to the domain and verify network settings.
   - Follow any additional steps required for SCCM installation and configuration as per your organization's guidelines.

Here are the detailed and corrected steps for configuring IIS on the SCCM server, including using the USB drive to provide the necessary installation files:

Configuration of IIS on SCCM Server

1. **Prepare the USB Drive**:
   - **Delete the old USB drive/hard disk** from the SCCM server if it was previously used.
   - **Attach the USB drive** to the SCCM server.

2. **Start the SCCM Server**:
   - Boot up the SCCM server if it is not already running.

3. **Add Roles in SCCM Server**:
   - Open **Server Manager** on the SCCM server.
   - Click on **Manage** and select **Add Roles and Features**.

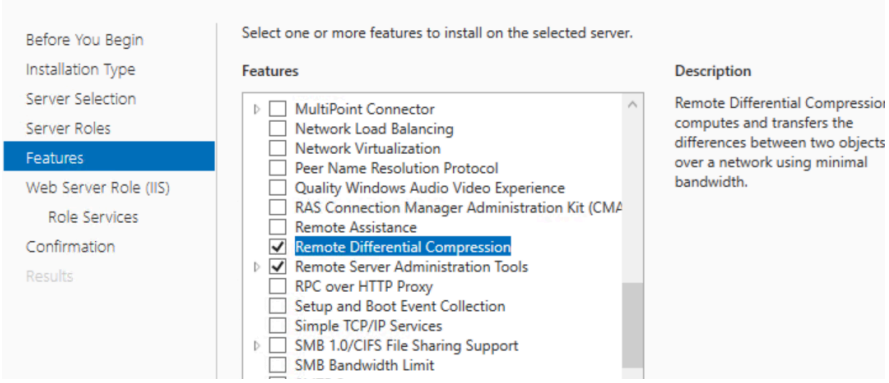
4. **Install IIS**:
   - Proceed through the wizard until you reach the **Select features** section.
   - Check **Web Server (IIS)** and click **Next**.

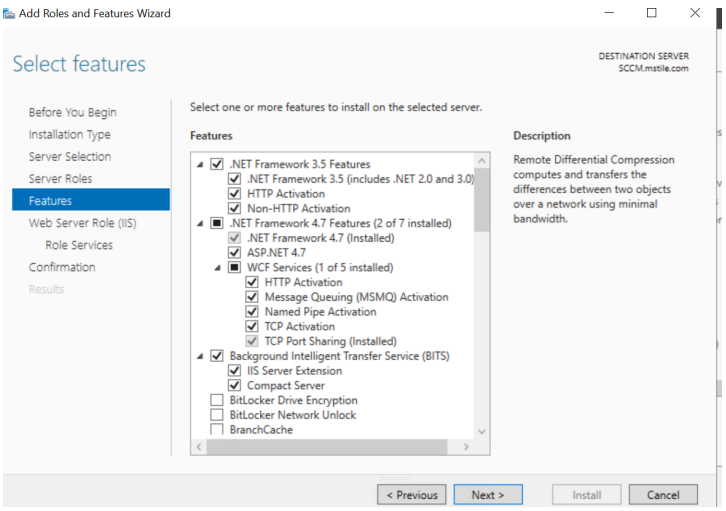
5. **Provide Source Files for IIS**:
   - When prompted to specify the source files for IIS, you need to point to the Windows Server installation files on the USB drive.
   - Navigate to the USB drive and locate the ISO file for Windows Server 2019.
   - Mount the ISO file or open the drive to access the installation files.
   - Go to the `sources\sxs` directory on the USB drive.
   - Copy the `sxs` folder to the desktop for easier access.
   - After copying, open the `sxs` folder and **copy the path** of this directory.

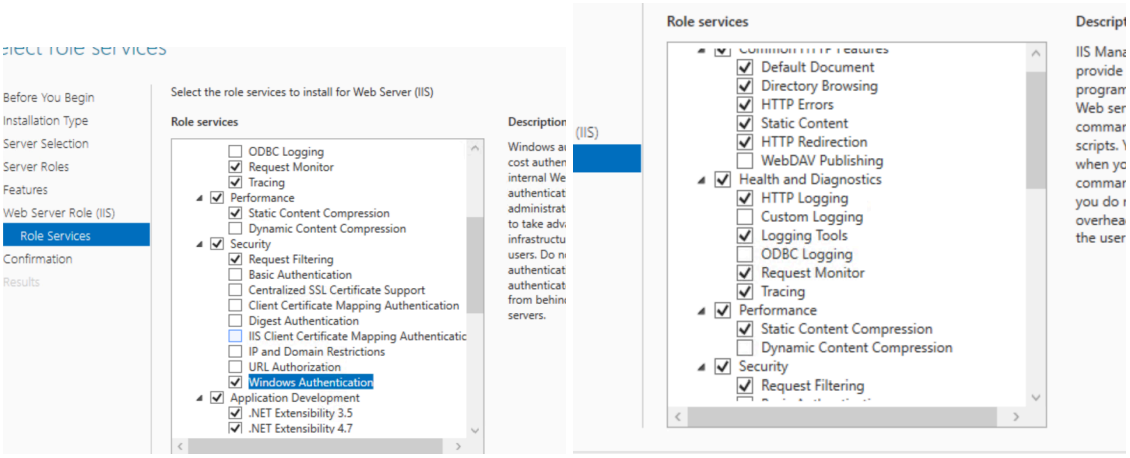
6. **Specify the Path During IIS Installation**:
   - In the **Add Roles and Features Wizard**, when you are asked to specify the source path for IIS files, paste the copied path to the `sxs` directory.
   - The path should look something like `C:\Users\[YourUsername]\Desktop\sxs`.

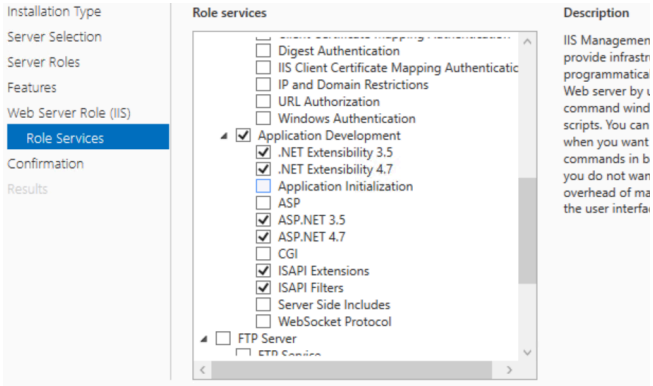
7. **Complete the Installation**:
   - Click **OK** to confirm the path and continue with the installation of IIS.
   - Follow the remaining prompts to complete the installation process.

By following these steps, you should successfully configure IIS on your SCCM server.

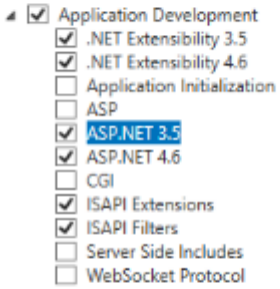


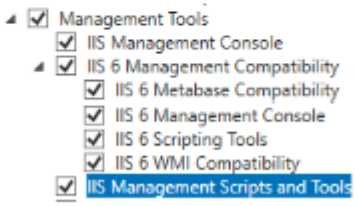



Select the role services to install for Web Server (IIS)
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Web Server Role (IIS)
Role Services
Confirmation
Results
Role services
ODBC Logging
Request Monitor
Tracing
Performance
Static Content Compression
Dynamic Content Compression
Security
Request Filtering
Basic Authentication
Centralized SSL Certificate Support
Client Certificate Mapping Authentication
Digest Authentication
IIS Client Certificate Mapping Authenticatic
IP and Domain Restrictions
URL Authorization
Windows Authentication
Application Development
.NET Extensibility 3.5
.NET Extensibility 4.7
Description
Role services
Default Document
Directory Browsing
HTTP Errors
Static Content
HTTP Redirection
WebDAV Publishing
Health and Diagnostics
HTTP Logging
Custom Logging
Logging Tools
ODBC Logging
Request Monitor
Tracing
Performance
Static Content Compression
Dynamic Content Compression
Security
Request Filtering


Installation Type
Server Selection
Server Roles
Features
Web Server Role (IIS)
Role Services
Confirmation
Results
Role services
Description
Digest Authentication
IIS Client Certificate Mapping Authenticatic
IP and Domain Restrictions
URL Authorization
Windows Authentication
Application Development
.NET Extensibility 3.5
.NET Extensibility 4.7
Application Initialization
ASP
ASP.NET 3.5
ASP.NET 4.7
CGI
ISAPI Extensions
ISAPI Filters
Server Side Includes
WebSocket Protocol
FTP Server


Security
Request Filtering
Basic Authentication
Centralized SSL Certificate Support
Client Certificate Mapping Authentication
Digest Authentication
IIS Client Certificate Mapping Authenticatic
IP and Domain Restrictions
URL Authorization
Windows Authentication

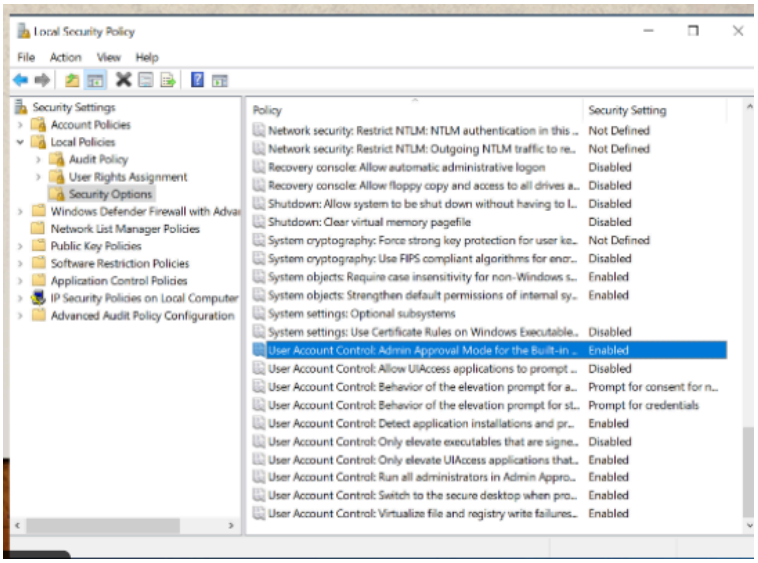

Application Development
.NET Extensibility 3.5
.NET Extensibility 4.6
Application Initialization
ASP
ASP.NET 3.5
ASP.NET 4.6
CGI
ISAPI Extensions
ISAPI Filters
Server Side Includes
WebSocket Protocol

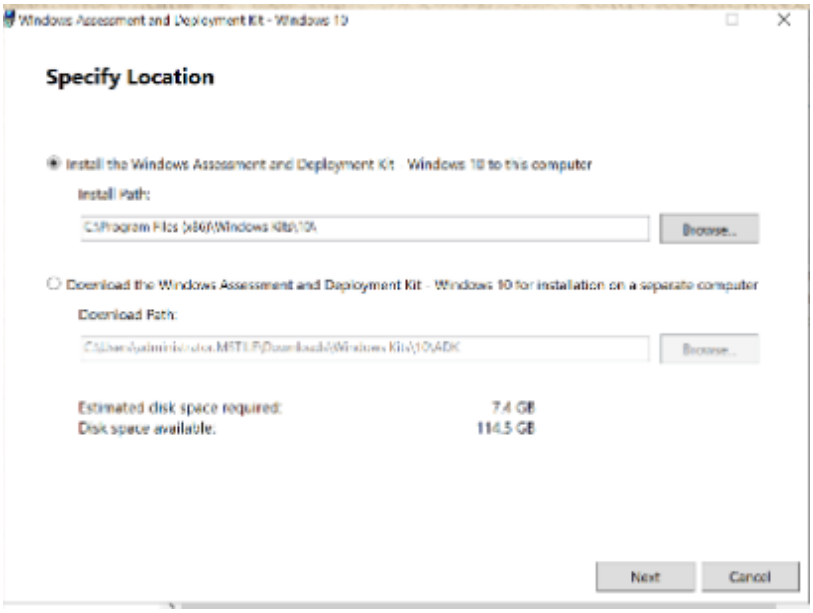

Management Tools
IIS Management Console
IIS 6 Management Compatibility
IIS 6 Metabase Compatibility
IIS 6 Management Console
IIS 6 Scripting Tools
IIS 6 WMI Compatibility
IIS Management Scripts and Tools

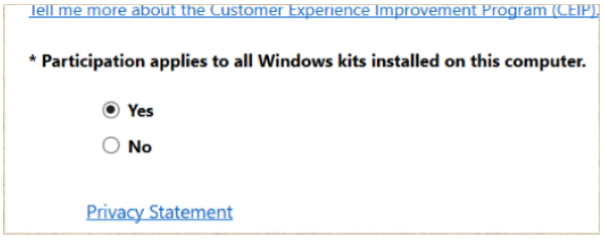
Installing Windows ADK on SCCM Server

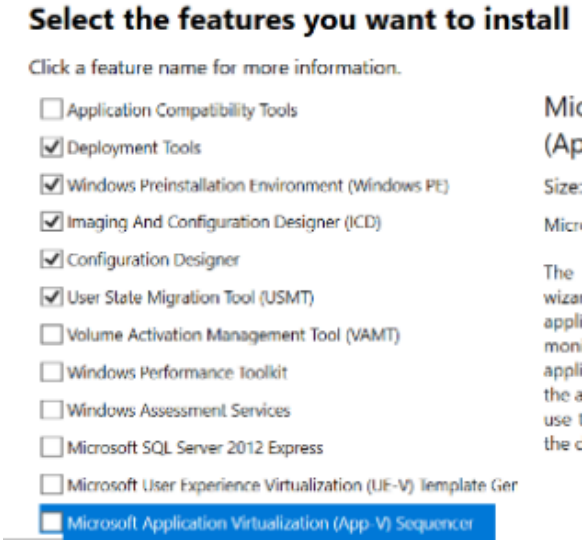
1. **Prepare the USB Drive**:
    - Ensure that the USB drive with the Windows ADK setup files is connected to the SCCM server.
2. **Open File Explorer**:
    - On the SCCM server, open **File Explorer**.
3. **Navigate to the USB Drive**:
    - Locate and open the USB drive in **File Explorer**.
4. **Run the ADK Setup**:
    - Find the `adksetup.exe` file on the USB drive and double-click to run it.
5. **Specify Installation Location**:
    - During the setup process, you will be prompted to specify the installation location for Windows ADK. Choose a suitable location if needed, or use the default location provided.
6. **Select Features to Install**:
    - When prompted to select the features you want to install, choose the following based on your requirements:
        - **Deployment Tools**: For general deployment capabilities.
        - **Windows Preinstallation Environment (WinPE)**: For creating bootable WinPE media.
        - **Imaging and Configuration Designer (ICD)**: For creating and customizing Windows images.
        - Select any additional features you need for your deployment scenario.
7. **Complete the Installation**:
    - After selecting the features, click **Install** to begin the installation process.
    - Wait for the installation to complete.
8. **Verify Installation**:
    - Once installed, you can verify the installation by checking the installed programs list or using the tools provided by Windows ADK.

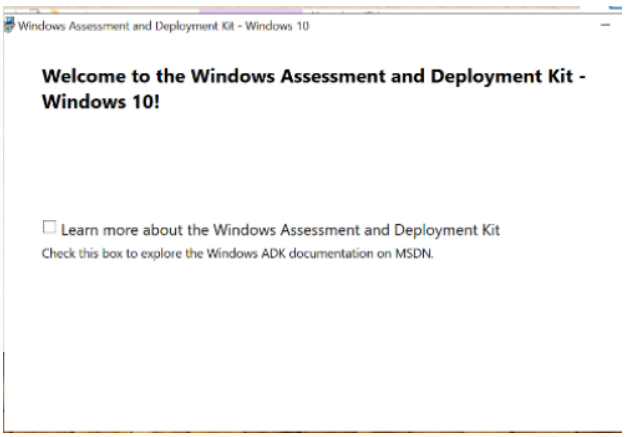
This will install the necessary Windows ADK components on your SCCM server, which are crucial for deployment and image management tasks


Local Security Policy
File Action View Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Computer
Advanced Audit Policy Configuration
Policy
Security Setting
Network security: Restrict NTLM: NTLM authentication in this ... Not Defined
Network security: Restrict NTLM: Outgoing NTLM traffic to re... Not Defined
Recovery console: Allow automatic administrative logon Disabled
Recovery console: Allow floppy copy and access to all drives a... Disabled
Shutdown: Allow system to be shut down without having to l... Disabled
Shutdown: Clear virtual memory pagefile Disabled
System cryptography: Force strong key protection for user ke... Not Defined
System cryptography: Use FIPS compliant algorithms for encr... Disabled
System objects: Require case insensitivity for non-Windows s... Enabled
System objects: Strengthen default permissions of internal sy... Enabled
System settings: Optional subsystems
System settings: Use Certificate Rules on Windows Executable... Disabled
User Account Control: Admin Approval Mode for the Built-in ... Enabled
User Account Control: Allow UIAccess applications to prompt ... Disabled
User Account Control: Behavior of the elevation prompt for a... Prompt for consent for n...
User Account Control: Behavior of the elevation prompt for st... Prompt for credentials
User Account Control: Detect application installations and pr... Enabled
User Account Control: Only elevate executables that are signe... Disabled
User Account Control: Only elevate UIAccess applications that... Enabled
User Account Control: Run all administrators in Admin Appro... Enabled
User Account Control: Switch to the secure desktop when pro... Enabled
User Account Control: Virtualize file and registry write failures... Enabled


Windows Assessment and Deployment Kit - Windows 10
Specify Location
Install the Windows Assessment and Deployment Kit - Windows 10 to this computer
Install Path:
C:\Program Files (x86)\Windows Kits\10\
Browse...
Download the Windows Assessment and Deployment Kit - Windows 10 for installation on a separate computer
Download Path:
Browse...
Estimated disk space required: 7.4 GB
Disk space available: 114.5 GB
Next
Cancel


Tell me more about the Customer Experience Improvement Program (CEIP)
* Participation applies to all Windows kits installed on this computer.
Yes
No
Privacy Statement


Select the features you want to install
Click a feature name for more information.
Application Compatibility Tools
Deployment Tools
Windows Preinstallation Environment (Windows PE)
Imaging And Configuration Designer (ICD)
Configuration Designer
User State Migration Tool (USMT)
Volume Activation Management Tool (VAMT)
Windows Performance Toolkit
Windows Assessment Services
Microsoft SQL Server 2012 Express
Microsoft User Experience Virtualization (UE-V) Template Ger
Microsoft Application Virtualization (App-V) Sequencer



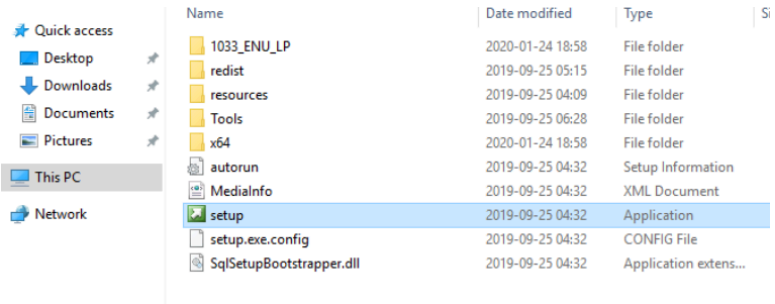
Installing SQL Server 2019

1. **Prepare for Installation**:
    - Go to **Drive D** on the server.
    - Navigate to the folder: `SQL Server 2019` > `x64` > `setup.exe`.
2. **Start SQL Server Installation**:
    - Run `setup.exe` to launch the SQL Server Installation Center.
3. **Begin New SQL Server Installation**:
    - In the SQL Server Installation Center, click on **Installation** in the left-hand menu.
    - Click **New SQL Server stand-alone installation or add feature to an existing installation**.
4. **Choose Evaluation Edition**:
    - Select **Evaluation** as the edition to install.
    - Click **Next**.
5. **Configure Microsoft Update**:
    - On the **Microsoft Update** screen, do not check the option to **Use Microsoft Update**.
    - Click **Next**.
6. **Install Setup Files**:
    - SQL Server will install setup files. Wait for this process to complete and click **Next**.
7. **Configure SQL Server Setup**:
    - On the **SQL Server License Terms** screen, review and accept the license terms. Click **Next**.
8. **SQL Server Feature Selection**:
    - On the **Feature Selection** screen, select the features you want to install. For a basic setup, ensure that **Database Engine Services** is checked.
    - Click **Next**.
9. **Instance Configuration**:
    - On the **Instance Configuration** screen, select **Default instance** or specify a named instance if needed.
    - The default instance ID is `MSSQLSERVER`. You can leave it as is or specify a different instance ID.

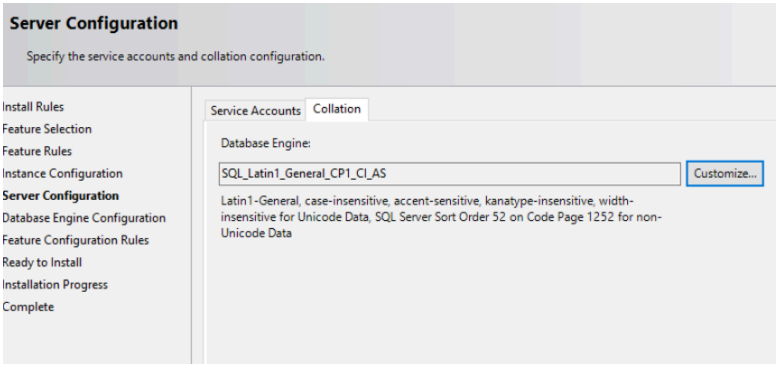
- Click **Next**.

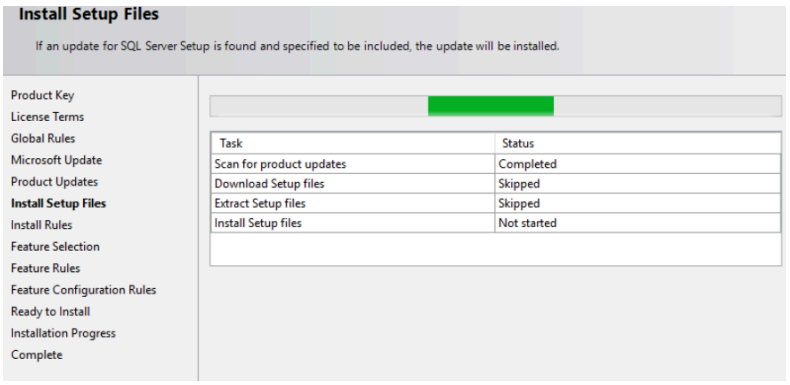
10. **Server Configuration**:
    - On the **Server Configuration** screen, choose the appropriate service accounts for SQL Server services. For basic setup, you can use the default accounts or specify custom accounts as required.
    - Click **Next**.
11. **Collation Settings**:
    - On the **Collation** screen, click **Customize**.
    - Set the **SQL collation** to `SQL_Latin1_General_CP1_CI_AS`.
    - Click **Next**.
12. **Database Engine Configuration**:
    - On the **Database Engine Configuration** screen, choose the authentication mode:
        - **Windows Authentication Mode**: SQL Server will use Windows user accounts for authentication.
        - **Mixed Mode (SQL Server authentication and Windows authentication)**: You will need to provide a SQL Server administrator password if choosing this option.
    - Add SQL Server administrators as needed by clicking **Add Current User** or specifying other users.
    - Click **Next**.
13. **Ready to Install**:
    - Review the summary of your installation choices on the **Ready to Install** screen.
    - Click **Install** to begin the installation process.
14. **Complete Installation**:
    - Wait for the installation to complete. Once it's done, click **Next** and then **Close** to exit the setup wizard.

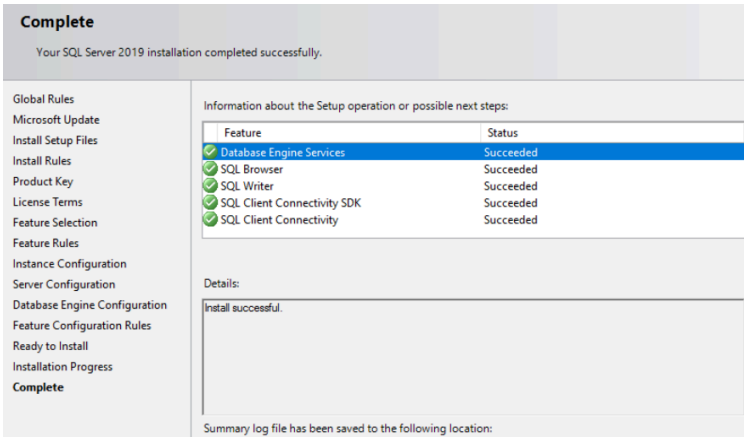
This will set up SQL Server 2019 on your server, configured with the specified settings




SQL Server Installation Center
Planning
Installation
Maintenance
New SQL Server stand-alone installation or add features to an existing installation
Launch a wizard to install SQL Server 2019 in a non-clustered environment or to ad
features to an existing SQL Server 2019 instance.
Product Key
Specify the edition of SQL Server 2019 to install.
Product Key
License Terms
Global Rules
Microsoft Update
Product Updates
Install Setup Files
Install Rules
Feature Selection
Feature Rules
Feature Configuration Rules
Ready to Install
Installation Progress
Complete
Validate this instance of SQL Server 2019 by enterin
of authenticity or product packaging. You can also
Evaluation, or Express. Evaluation has the largest se
Books Online, and is activated with a 180-day expir
has the same set of features found in Evaluation, bu
development only. To upgrade from one installed e
Specify a free edition:
Evaluation
Enter the product key:
Microsoft Update
Use Microsoft Update to check for important updates
Product Key
License Terms
Global Rules
Microsoft Update
Product Updates
Install Setup Files
Install Rules
Feature Selection
Feature Rules
Feature Configuration Rules
Ready to Install
Installation Progress
Complete
Microsoft Update offers securit
software, including SQL Server
the Microsoft Update website.
Use Microsoft Update to che
Microsoft Update FAQ
Microsoft Update Privacy State





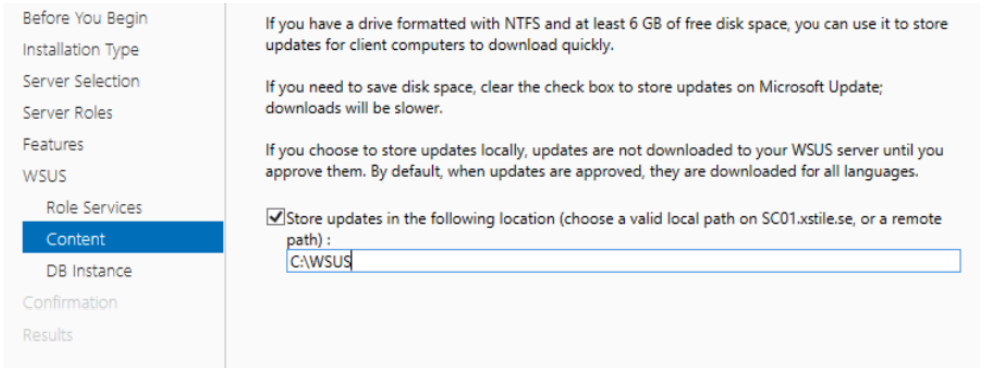


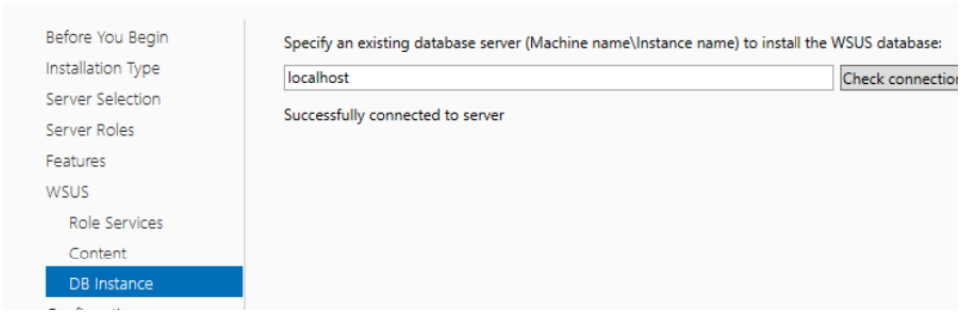
Installing and Configuring WSUS

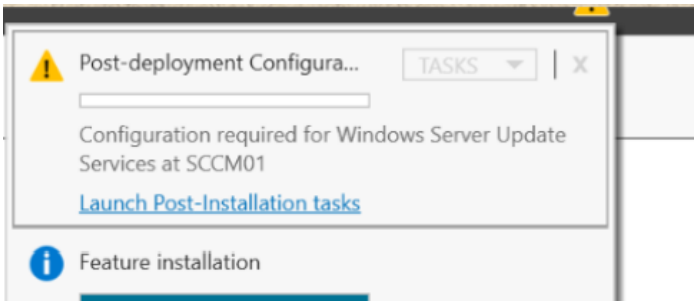
1. **Prepare for WSUS Installation**:
    - Create a folder where WSUS will store updates. For example, create a folder `C:\WSUS` on your server.
2. **Install WSUS**:
    - On the SCCM server, open **Server Manager**.
    - Click on **Manage** and select **Add Roles and Features**.
3. **Role Installation Wizard**:
    - Proceed through the wizard until you reach the **Select server roles** section.
    - Check the box for **Windows Server Update Services**.
    - Click **Next**.
4. **Select Features**:

    - On the **Select features** screen, you can leave the default selections or add additional features if needed.
    - Click **Next**.
5. **WSUS Role Services**:
    - On the **Select role services** screen, check the following:
        - **WSUS Services**
        - **Database**
    - Make sure that **WSUS Services** and **SQL Server Database** (if required) are selected.
    - Click **Next**.
6. **Configure WSUS**:
    - On the **WSUS Configuration** screen:
        - **Content Location**: Specify the folder you created earlier (`C:\WSUS`).
        - Check the **Use existing database** option if you are using an existing WSUS database or **Install a new WSUS database** if this is a fresh installation.
        - Ensure that **Localhost** is selected as the WSUS server to manage updates from.
        - Check **Connect** to ensure the server can reach WSUS.
    - Click **Next**.
7. **Finish Installation**:
    - Review your selections and click **Install** to begin the installation process.
    - Wait for the installation to complete.
8. **Post-Installation Configuration**:
    - Once the installation is complete, click **Close**.
9. **Open WSUS Console**:
    - Click on the flag icon in the top right corner of the Server Manager window.
    - Select **Launch Post-Installation Tasks** to complete the WSUS setup.
10. **Configure WSUS**:
    - After the post-installation tasks are complete, open the **WSUS Console** to further configure WSUS settings, including synchronization with Microsoft Update and approval of updates.

This process will install and configure WSUS on your server, allowing it to manage and deploy updates.





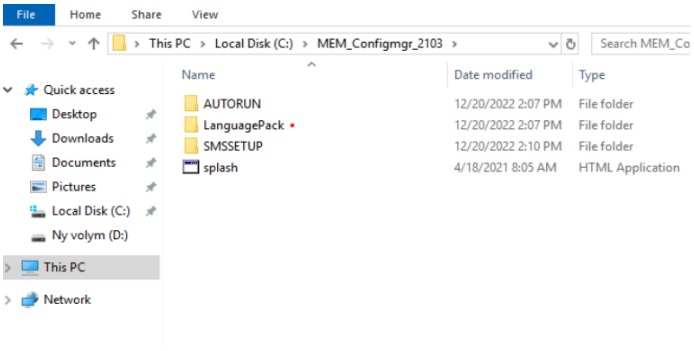


Installing SCCM

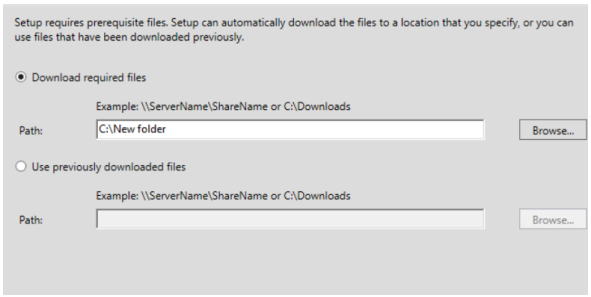
1. **Prepare Installation Files**:
    - Navigate to **Drive D**.
    - Open the folder `MEM_configmgr_2103`.
2. **Start Installation**:
    - Locate and double-click the `splash.hta` file to launch the Configuration Manager setup.
3. **Begin Setup**:
    - Click **Install** to start the installation process.
    - On the **Setup Wizard** screen, click **Next**.
4. **Select Installation Type**:
    - Choose **Install Configuration Manager**.
    - Select the option for a **Typical installation**.
    - Click **Next**.
5. **Evaluation Version**:
    - When prompted to install the evaluation version, click **Yes**.
    - Click **Next** to continue.
6. **License Terms**:

    - Review and select all the license terms.
    - Click **Next**.
7. **Download and Save Files**:
    - In the **Download Files** section:
        - Click **Browse** to choose the location where the installation files will be saved.
        - Create a new folder if necessary (e.g., `C:\NEW FOLDER`).
        - Select this folder and click **Next**.
8. **Wait for Download**:
    - The installation files will be downloaded to the specified folder.
    - Wait for the download process to complete.
9. **Proceed with Installation**:
    - Once the files are downloaded, follow any additional prompts to complete the installation of Configuration Manager.

These steps will guide you through the installation of SCCM using the `MEM_configmgr_2103` package.



i

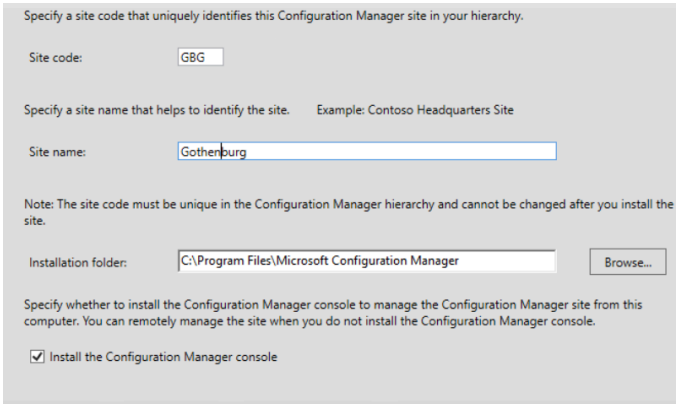


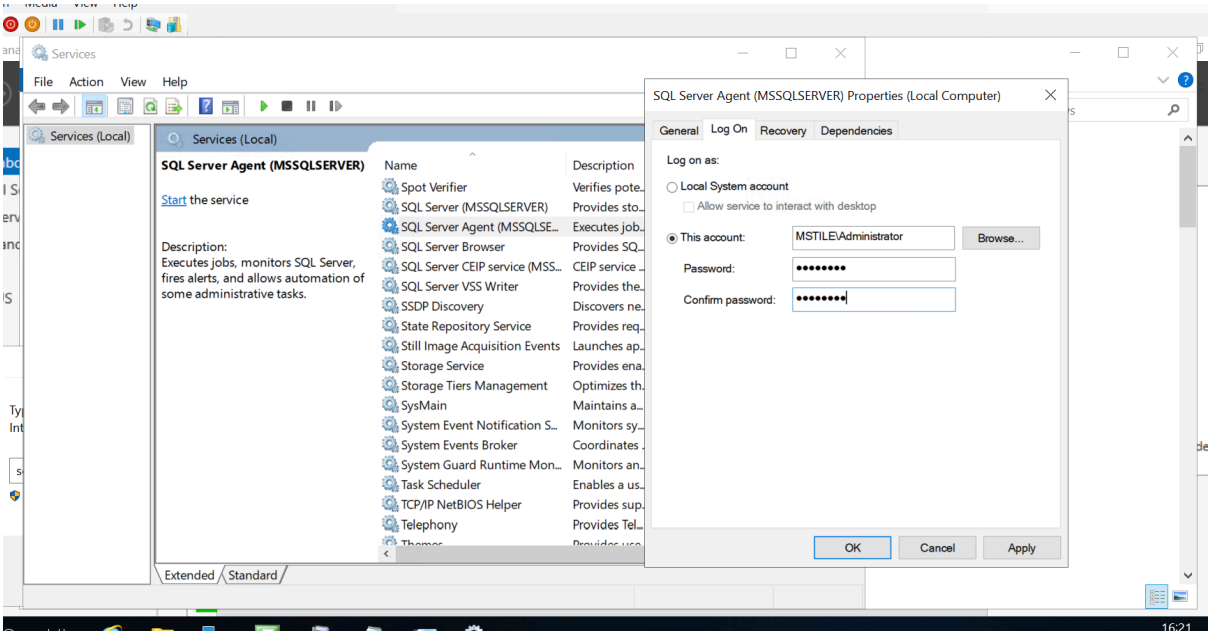
Site and Installation Settings

1. **Start Configuration Manager Setup**:
    - If not already running, launch the Configuration Manager setup wizard.
2. **Proceed to Site and Installation Settings**:
    - Navigate to the **Site and Installation Settings** section.
    - Click **Next** to continue.
3. **Configure SQL Server Properties**:

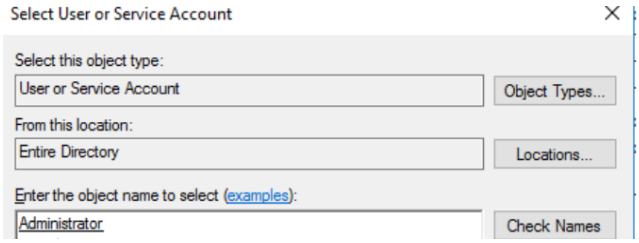
    - Before proceeding with the installation of SQL Server and SQL Agent, you need to set the properties for these services.
    - On the **Service Configuration** screen:
        - **SQL Server**: Specify the SQL Server instance where SCCM will install its database.
        - **SQL Agent**: Specify the SQL Server Agent account if it will be used for SCCM-related tasks.
4. **Specify SQL Server Instance**:
    - Provide the name of the SQL Server instance where SCCM will store its database.
    - If SQL Server is installed on the same machine, you can use `localhost` or the name of the SQL Server instance.
5. **SQL Server Agent Configuration**:
    - Configure the SQL Server Agent settings if needed. Typically, this will involve specifying the service account used by SQL Server Agent.
6. **Continue Installation**:
    - Click **Next** to proceed with the installation after setting the SQL Server and SQL Agent properties.

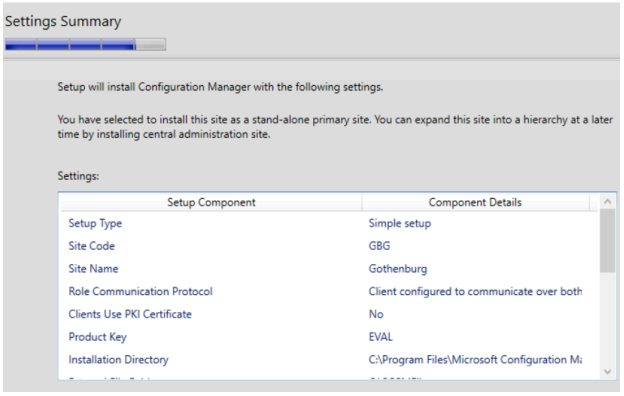
These steps ensure that SCCM is correctly configured to use the SQL Server for its database and set up SQL Server Agent for scheduled tasks.

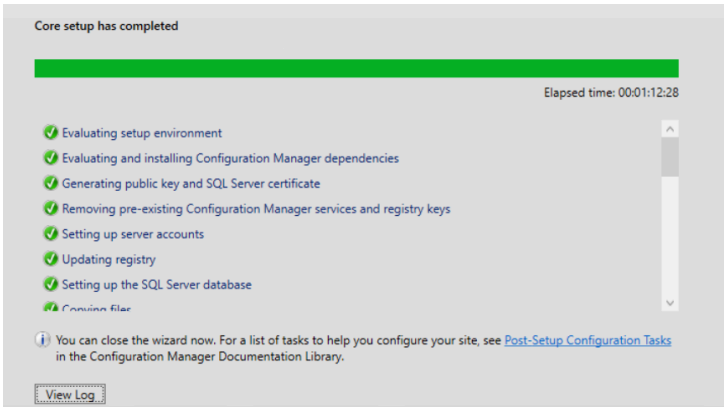

Specify a site code that uniquely identifies this Configuration Manager site in your hierarchy.
Site code:
GBG
Specify a site name that helps to identify the site.
Example: Contoso Headquarters Site
Site name:
Gothenburg
Note: The site code must be unique in the Configuration Manager hierarchy and cannot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


Services
File Action View Help
Services (Local)
SQL Server Agent (MSSQLSERVER)
Start the service
Description:
Executes jobs, monitors SQL Server, fires alerts, and allows automation of some administrative tasks.
Name
Description
Spot Verifier
SQL Server (MSSQLSERVER)
SQL Server Agent (MSSQLSE...
SQL Server Browser
SQL Server CEIP service (MSS...
SQL Server VSS Writer
SSDP Discovery
State Repository Service
Still Image Acquisition Events
Storage Service
Storage Tiers Management
SysMain
System Event Notification S...
System Events Broker
System Guard Runtime Mon...
Task Scheduler
TCP/IP NetBIOS Helper
Telephony
Extended
Standard
SQL Server Agent (MSSQLSERVER) Properties (Local Computer)
General
Log On
Recovery
Dependencies
Log on as:
Local System account
Allow service to interact with desktop
This account:
MSTILE\Administrator
Browse...
Password:
Confirm password:
OK
Cancel
Apply

>next



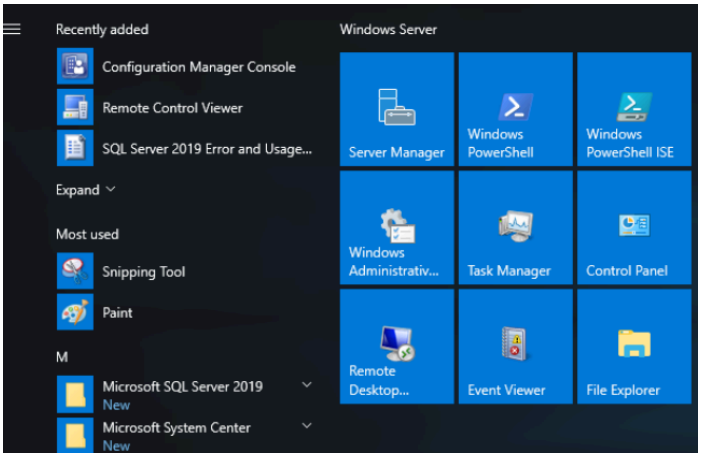


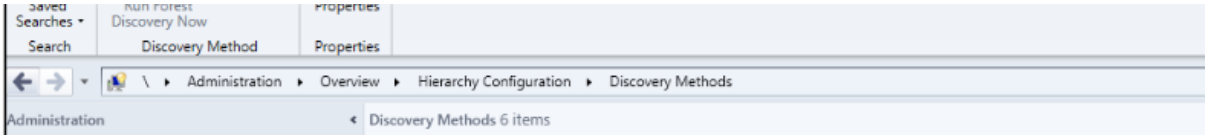


Configuration of SCCM

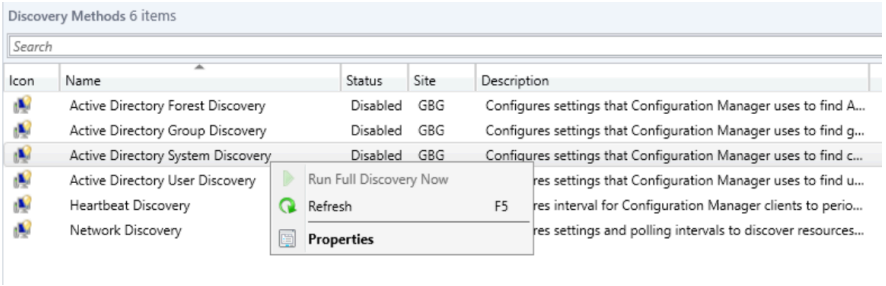
1. **Open Configuration Manager Console**:
    - Launch the **Configuration Manager Console**. The console will open with various features and options.
2. **Configure Active Directory Discovery**:
    - Go to the **Administrator** workspace.
    - In the **Administration** section, navigate to **Hierarchy Configuration** and then **Discovery Methods**.
3. **Open Properties for Discovery Methods**:
    - Select **Active Directory Forest Discovery** (or the relevant discovery method).
    - Click **Properties**.
    - Go to the **General** tab and click on the yellow icon to initiate the search for devices.
4. **Search for Devices**:
    - Click **Browse** to select and search for the device you want to configure.

    - Locate the desired device and click **OK**.
5. **Configure Polling Schedule**:
    - Under the **Polling Schedule** tab:
        - Click on **Discovery**.
        - Ensure that **Recurring the AD** is selected.
        - Choose **Use the computer account** for the discovery.
        - Set the polling interval according to your needs.
        - Click **OK**.
6. **Configure Active Directory Attributes**:
    - Go to **Active Directory Attributes**.
    - Ensure that all necessary attributes are configured correctly.
    - Click **Option** to configure attributes if needed.
    - Click **OK** to apply the changes.
7. **Configure Boundaries**:
    - Go to the **Administration** workspace.
    - Navigate to **Hierarchy Configuration** and then **Boundaries**.
    - Click **Create Boundary**.
8. **Create a New Boundary**:
    - Enter a description for the boundary (e.g., `GBG`).
    - Set **Type** to **IP Subnet**.
    - Enter the following details:
        - **Network**: `192.168.10.0`
        - **Subnet Mask**: `255.255.255.0`
        - **Gateway**: `192.168.10.0`
    - Click **OK** to create the IP subnet boundary.
9. **Configure Boundary Groups**:
    - In the **Boundaries** section, open the properties of the **Boundary Groups**.
    - Click **Create Boundary Group**.
    - Name the boundary group (e.g., `GBG`).
    - Click **Add** to add boundaries to the group.
    - Reference the boundaries created earlier by selecting and adding them to the group.
    - Click **OK** to apply the settings.

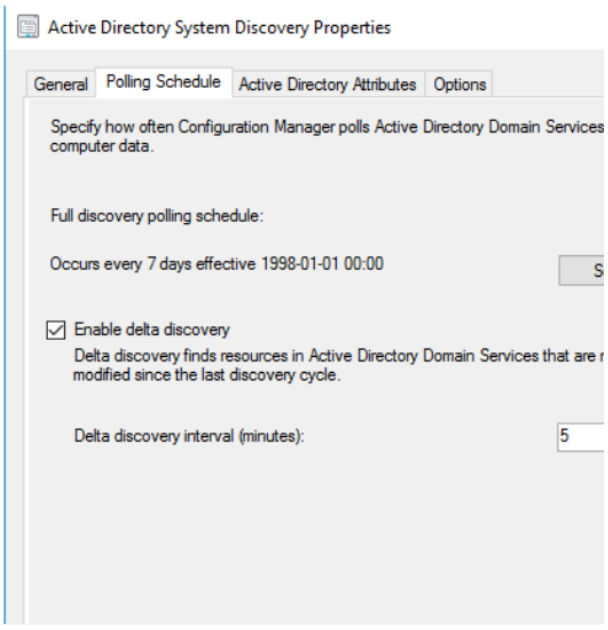

Recently added
Configuration Manager Console
Remote Control Viewer
SQL Server 2019 Error and Usage...
Expand
Most used
Snipping Tool
Paint
M
Microsoft SQL Server 2019
New
Microsoft System Center
New
Windows Server
Server Manager
Windows PowerShell
Windows PowerShell ISE
Windows Administrativ...
Task Manager
Control Panel
Remote Desktop...
Event Viewer
File Explorer

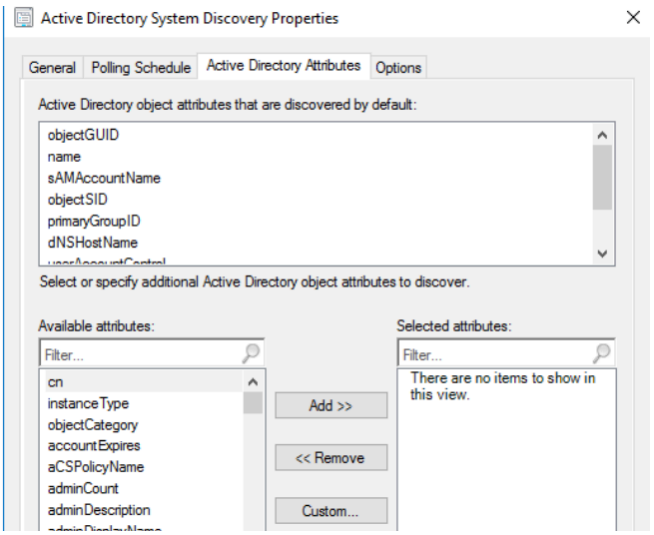

Saved Searches
Run Forest Discovery Now
Properties
Search
Discovery Method
Properties
Administration
Overview
Hierarchy Configuration
Discovery Methods
Administration
Discovery Methods 6 items

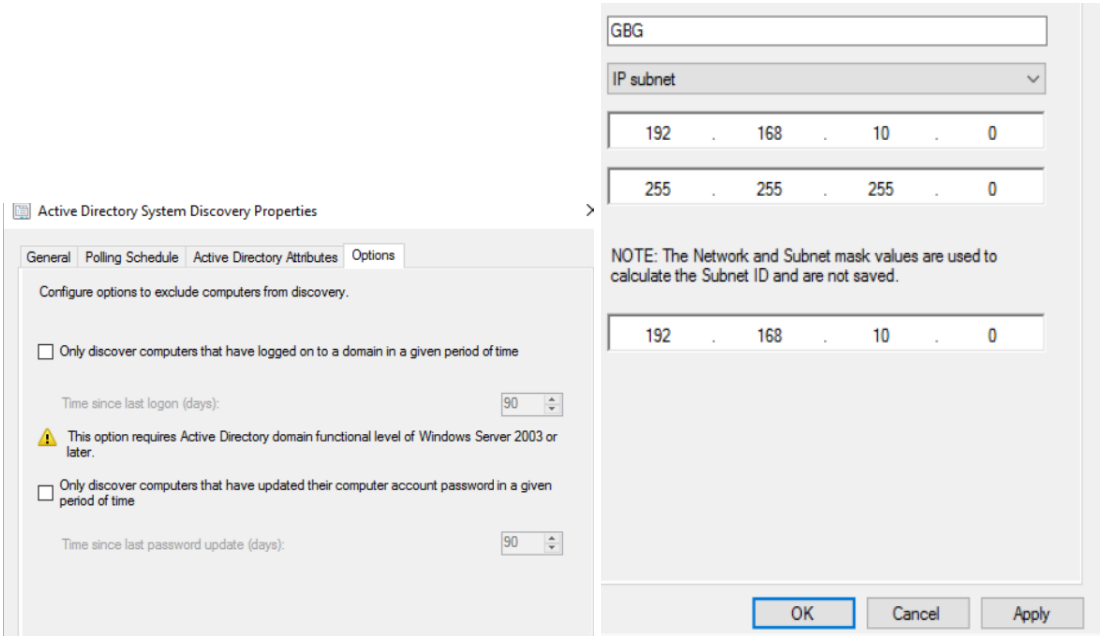
then>

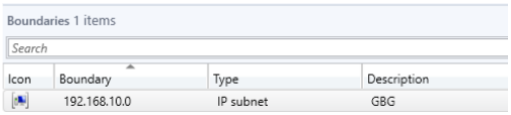

Discovery Methods 6 items
Search
Icon
Name
Status
Site
Description
Active Directory Forest Discovery
Disabled
GBG
Configures settings that Configuration Manager uses to find A...
Active Directory Group Discovery
Disabled
GBG
Configures settings that Configuration Manager uses to find g...
Active Directory System Discovery
Disabled
GBG
Configures settings that Configuration Manager uses to find c...
Active Directory User Discovery
Heartbeat Discovery
Network Discovery
Run Full Discovery Now
Refresh
F5
Properties

>


Active Directory System Discovery Properties
General
Polling Schedule
Active Directory Attributes
Options
Specify how often Configuration Manager polls Active Directory Domain Services
computer data.
Full discovery polling schedule:
Occurs every 7 days effective 1998-01-01 00:00
Enable delta discovery
Delta discovery finds resources in Active Directory Domain Services that are
modified since the last discovery cycle.
Delta discovery interval (minutes):
5







Configure Firewall

1. **Open Firewall Settings**:
    - Open **Control Panel**.
    - Go to **System and Security** and then **Windows Defender Firewall**.
    - Click on **Advanced settings**.
2. **Modify Firewall Properties**:
    - In the **Windows Firewall with Advanced Security** window, go to **Properties**.
    - For each profile (Domain, Private, Public), ensure that the firewall is set to **Allow** connections as necessary.
    - Click **OK** to apply the changes.

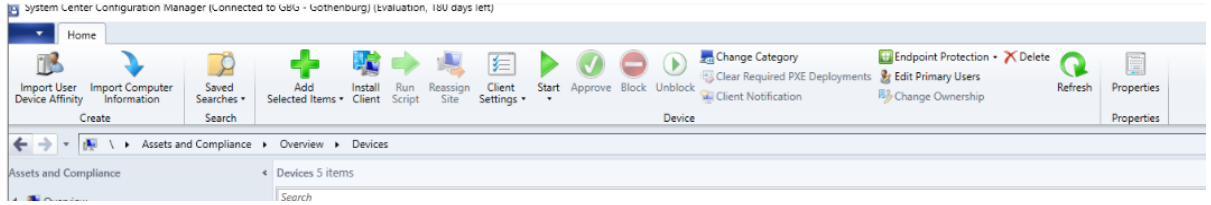
Install SCCM Client

1. **View Devices**:
    - Open the **Configuration Manager Console**.
    - Go to **Assets and Compliance** > **Overview** > **Devices**.
    - Here you should see a list of all devices.
2. **Install SCCM Client**:
    - Select the devices where you want to install the client.
    - Right-click on the selected device(s) and choose **Install Client**.
    - The installation process will begin. Click **Next** to proceed.
3. **Configure Installation Options**:
    - On the **Installation Options** screen:
        - Select **Allow the client software to be installed on domain computers**.
        - Choose **Install the client on the specific site** and select the site (e.g., `gbg-GOTHENBURG`).
    - Click **Next** to continue.
4. **Client Installation Setting**:
    - Go to **Administration** > **Site Configuration** > **Sites**.
    - Click on **Client Installation Settings** and then **Client Push Installation**.
    - In the **General** tab, check **Enable automatic site-wide client push**.
    - Check **Allow connections**.
    - Click **OK** to apply the settings.
5. **Create a New Account for Client Push**:
    - Click on the **yellow exclamation mark** or **Create Account** button.
    - Click **New Account** to add a domain/user account for client push installation.
    - Enter the **Domain/User** details and click **OK**.
6. **Update Boundary Group**:
    - Go to **Administration** > **Hierarchy Configuration** > **Boundary Groups**.
    - Open the properties of the **GBG BG** boundary group.
    - Ensure that the boundary group is set to be used for the assignment.
    - Click **Add** to include necessary boundaries.
    - Click **OK** to save the changes.

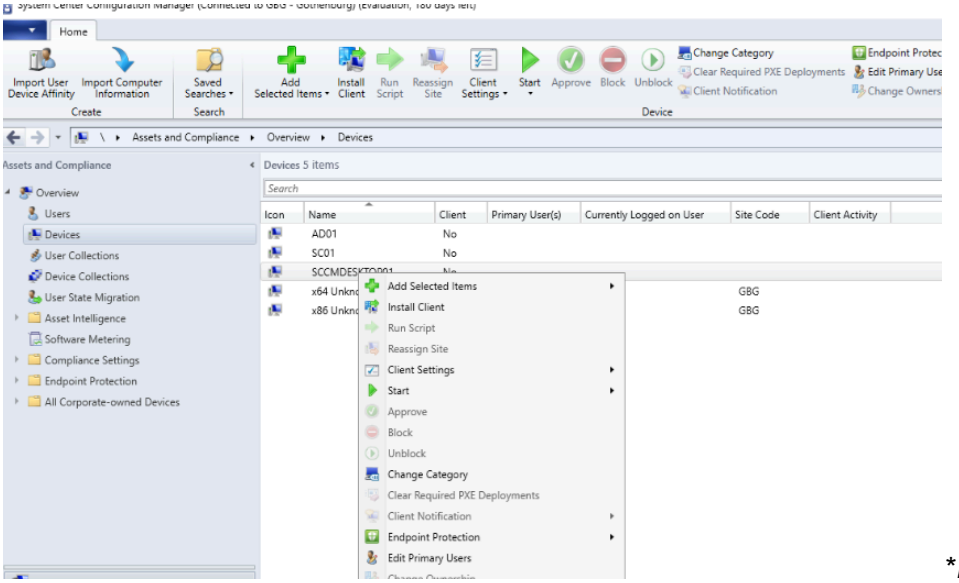
Final Step: Verify Client Installation

1. **Check Configuration Manager Client on the Device**:
    - Once the client installation is complete, go to the client machine.
    - Open **Control Panel**.
    - Look for **Configuration Manager** to verify that the client is installed.
2. **Verify SCCM Client Properties**:
    - On the client machine, open **Configuration Manager** from the Control Panel.
    - Check the **General** tab to see information about the SCCM client and ensure it's properly configured.

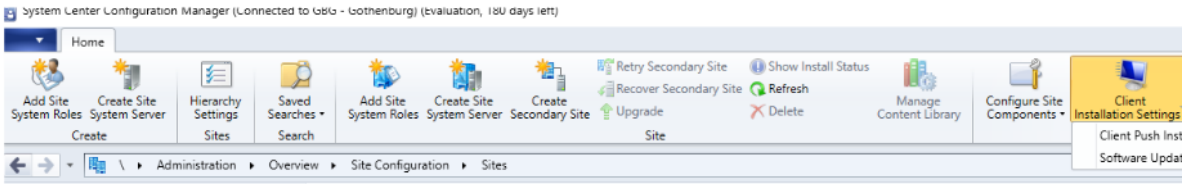
These steps will ensure that the SCCM client is installed and properly configured on your devices.



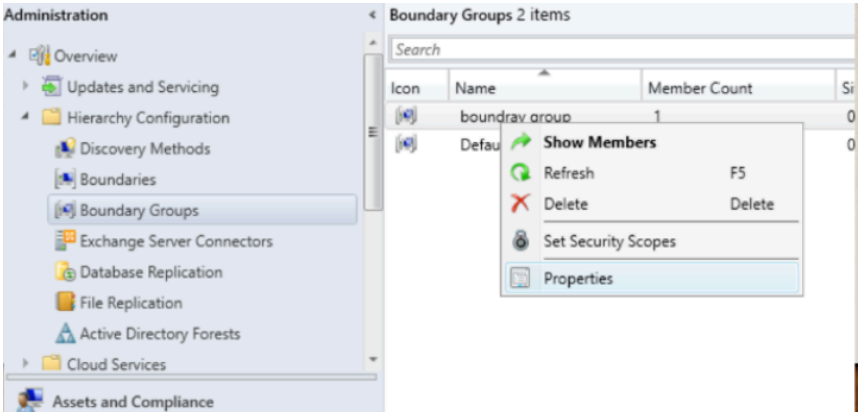
now go to Assets and compliance>overview>devices.´(here you see your all devices)
*in case you find /see the error correct the error by viewing its warning



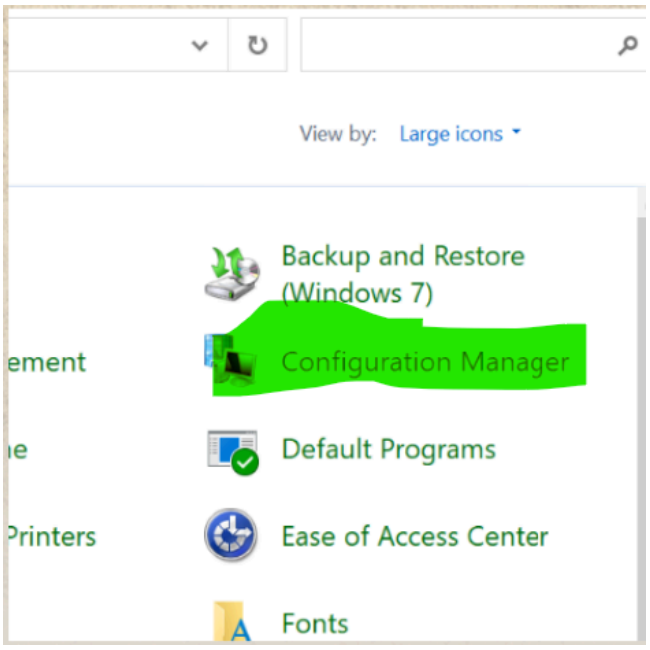
here we see the devices so now click left and there you will click on install client>installation process begin>click next>in installation option click"ALLOW THE CLIENT SOFTWARE TO BE INSTALLED ON DOMAIN">(*) CLICK ON INSTALL THE CLIENT ON THE SPECIFIC SITE:gbg-GOTHENBURG>next>cilent is being pushed to windows 10 VM>

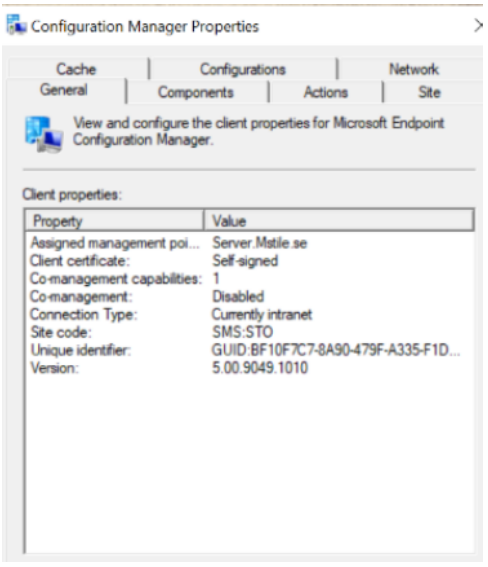


*go to client installation setting and click on CLIENT PUSH INSTALLATION.>general click on enable>click on allow connections>ok>click on yellow button>create "new account">domain/user to be added>ok.
now go to Boundry group >GBG BG properties>click on use this boundary group to this assignment.>click add>now here we see the SCCM client is installed.*



Final step

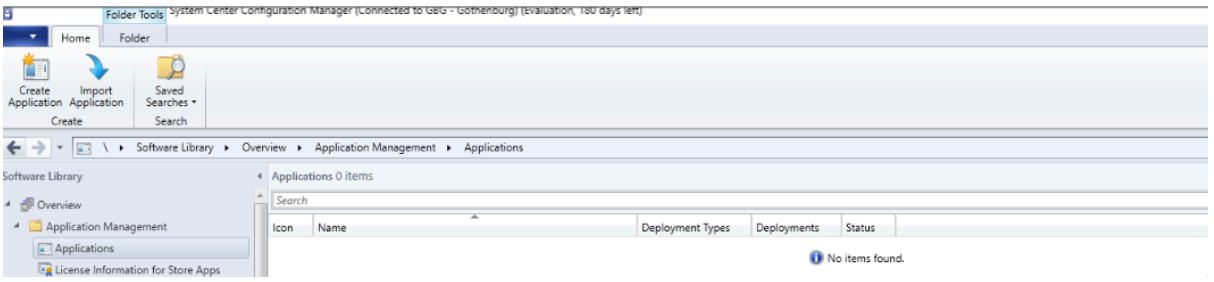


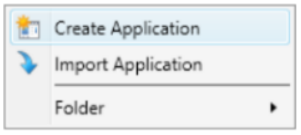


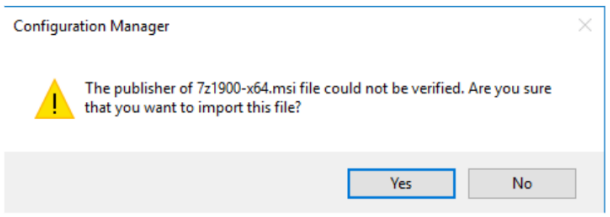
Creating and Installing an Application in SCCM

1. **Open SCCM Console**:
    a. Launch the **Configuration Manager Console**.
2. **Navigate to Software Library**:
    a. Go to **Software Library** in the left-hand navigation pane.
    b. Expand **Application Management** and select **Applications**.
3. **Create a New Application**:
    a. Click **Create Application** in the ribbon at the top.
4. **Specify Application Type**:
    a. In the **Create Application Wizard**, choose **Automatically detect information about this application from installation files**.
    b. Click **Next**.

5. **Select Application Type**:
    a. Select **Windows Installer (*.msi file)** as the application type.
    b. Click **Next**.
6. **Specify Source File Location**:
    a. Enter the path to the MSI file for the application. For example, if your file is located on a network share, enter: `\\sccm\app\googlechrome.msi`.
    b. Click **Next**.
7. **Application Information**:
    a. The wizard will detect the application information from the MSI file. Verify or enter the application details as needed, such as:
        i. **Name**: Google Chrome
        ii. **Publisher**: Google
        iii. **Version**: [Version Number]
    b. Click **Next**.
8. **Deployment Type**:
    a. Specify the deployment type settings for the application. Typically, the default settings for the MSI package will be sufficient.
    b. Click **Next**.
9. **Content Location**:
    a. Confirm or modify the content location where the source files are stored. This is usually the network path you specified earlier.
    b. Click **Next**.
10. **Detection Method**:
    a. Configure the detection method to determine if the application is already installed. SCCM usually detects this automatically from the MSI file, but you can modify the detection rules if needed.
    b. Click **Next**.
11. **User Experience**:
    a. Configure user experience settings such as installation behavior, whether the application should be installed in the background, and if users should see any installation progress.
    b. Click **Next**.
12. **Requirements**:
    a. Define any system requirements that must be met for the application to be installed.
    b. Click **Next**.
13. **Dependencies**:
    a. Specify any dependencies required for the application to function correctly, if applicable.
    b. Click **Next**.
14. **Summary**:
    a. Review the summary of your application settings and configurations.
    b. Click **Next** to create the application.
15. **Complete the Wizard**:
    a. Click **Close** to finish the application creation process.

16. 
Folder Tools
Home
Folder
Create Application
Import Application
Saved Searches
Create
Search
Software Library
Overview
Application Management
Applications
Software Library
Overview
Application Management
Applications
License Information for Store Apps
Applications 0 items
Search
Icon
Name
Deployment Types
Deployments
Status
No items found.

17. 
Create Application
Import Application
Folder

18. 
Configuration Manager
The publisher of 7z1900-x64.msi file could not be verified. Are you sure that you want to import this file?
Yes
No