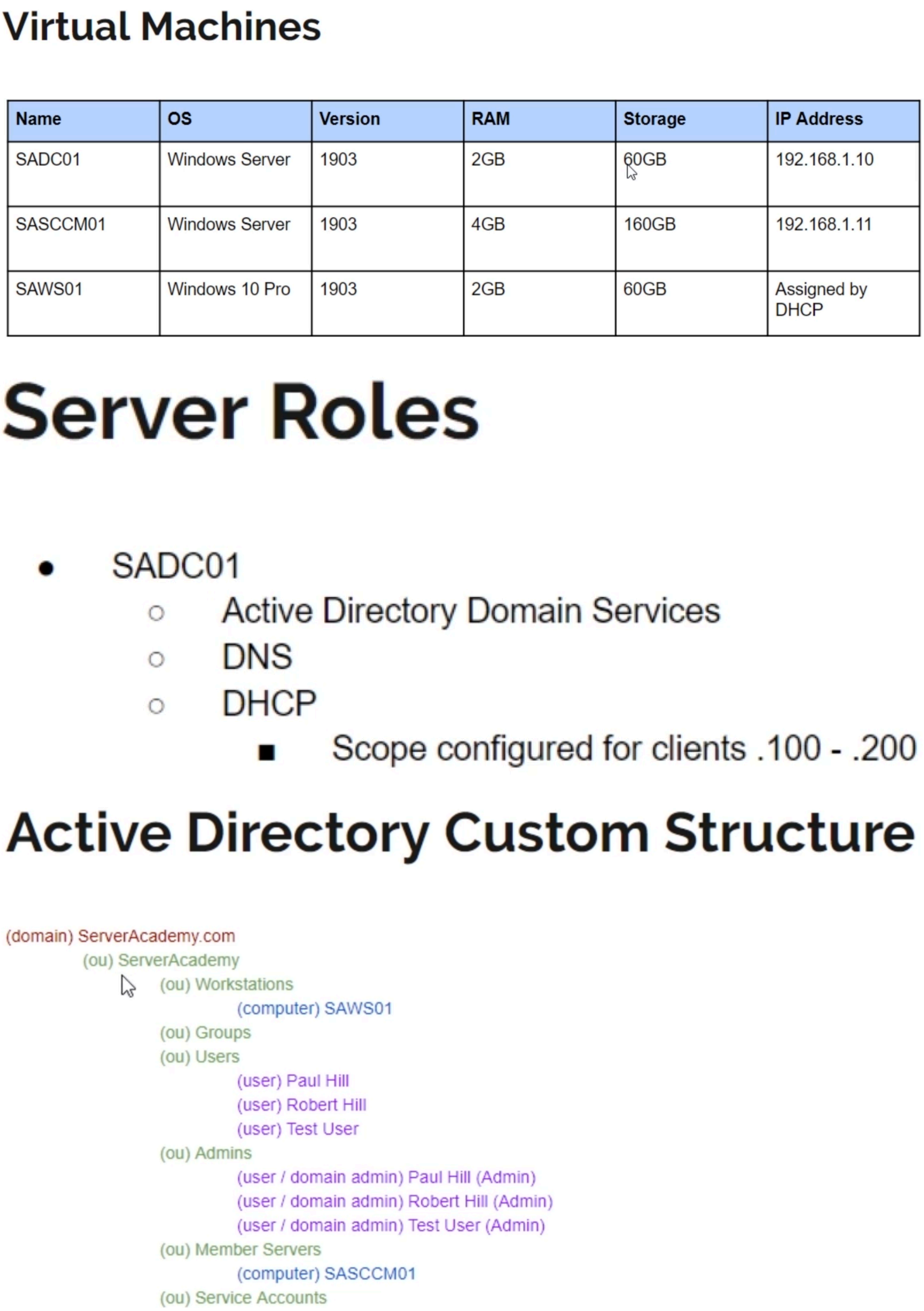


Virtual Machines

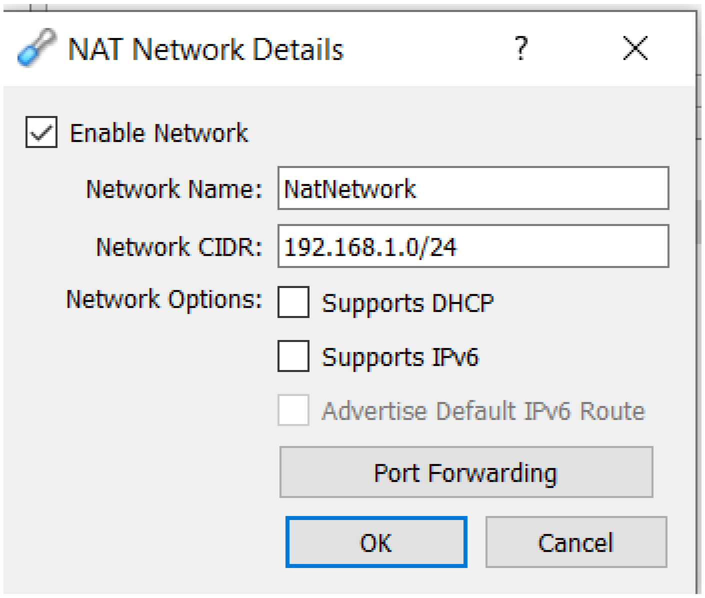
Name	OS	Version	RAM	Storage	IP Address
SADC01	Windows Server	1903	2GB	60GB	192.168.1.10
SASCCM01	Windows Server	1903	4GB	160GB	192.168.1.11
SAWS01	Windows 10 Pro	1903	2GB	60GB	Assigned by DHCP

Server Roles

- SADC01
  - Active Directory Domain Services
  - DNS
  - DHCP
    - Scope configured for clients .100 - .200

Active Directory Custom Structure

- (domain) ServerAcademy.com
  - (ou) ServerAcademy
    - (ou) Workstations
      - (computer) SAWS01
    - (ou) Groups
    - (ou) Users
      - (user) Paul Hill
      - (user) Robert Hill
      - (user) Test User
    - (ou) Admins
      - (user / domain admin) Paul Hill (Admin)
      - (user / domain admin) Robert Hill (Admin)
      - (user / domain admin) Test User (Admin)
    - (ou) Member Servers
      - (computer) SASCCM01
    - (ou) Service Accounts



NAT Network Details

☑ Enable Network

Network Name: NatNetwork

Network CIDR: 192.168.1.0/24

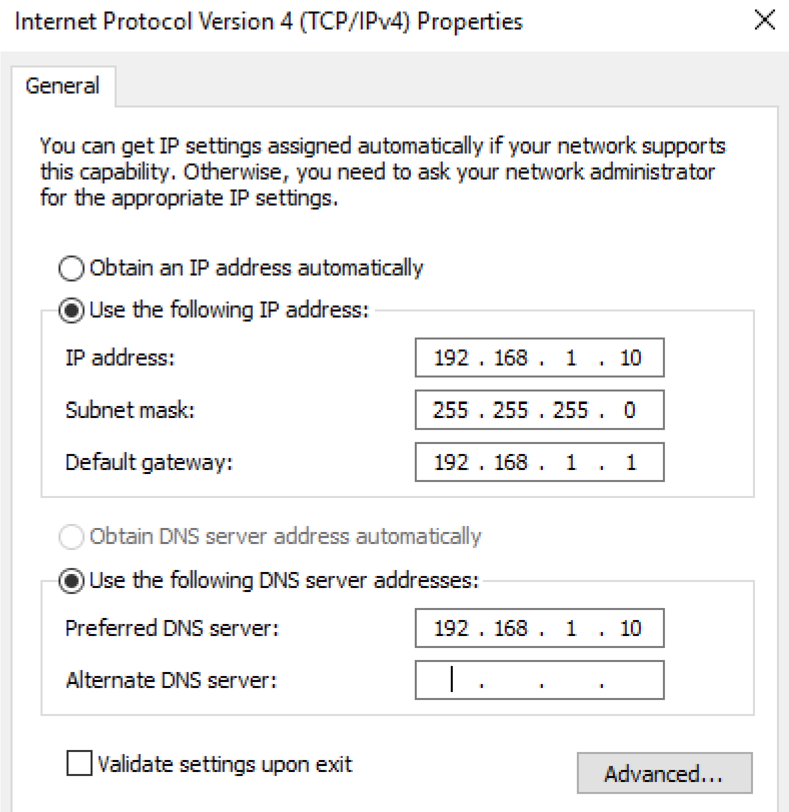
Network Options: □ Supports DHCP

□ Supports IPv6

□ Advertise Default IPv6 Route

E:\Users\Tanner
C:\Users\Tanner\VirtualBox VMs
E:\Users\Tanner\VirtualBox VMs

SADC01 Server Configuration (Domain Controller)



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 10

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 1 . 1

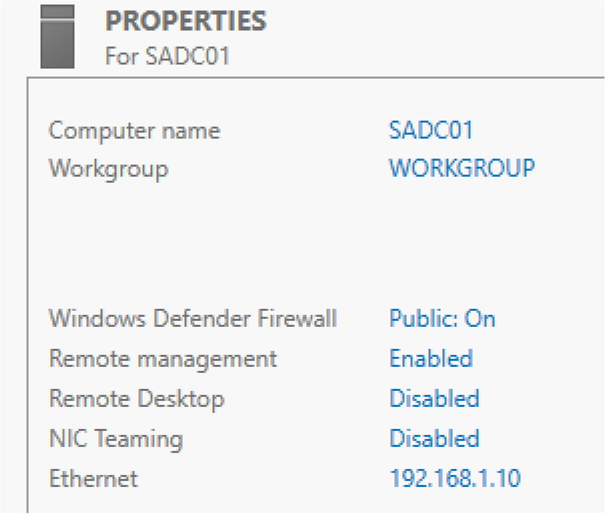
○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 1 . 10

Alternate DNS server: . . .

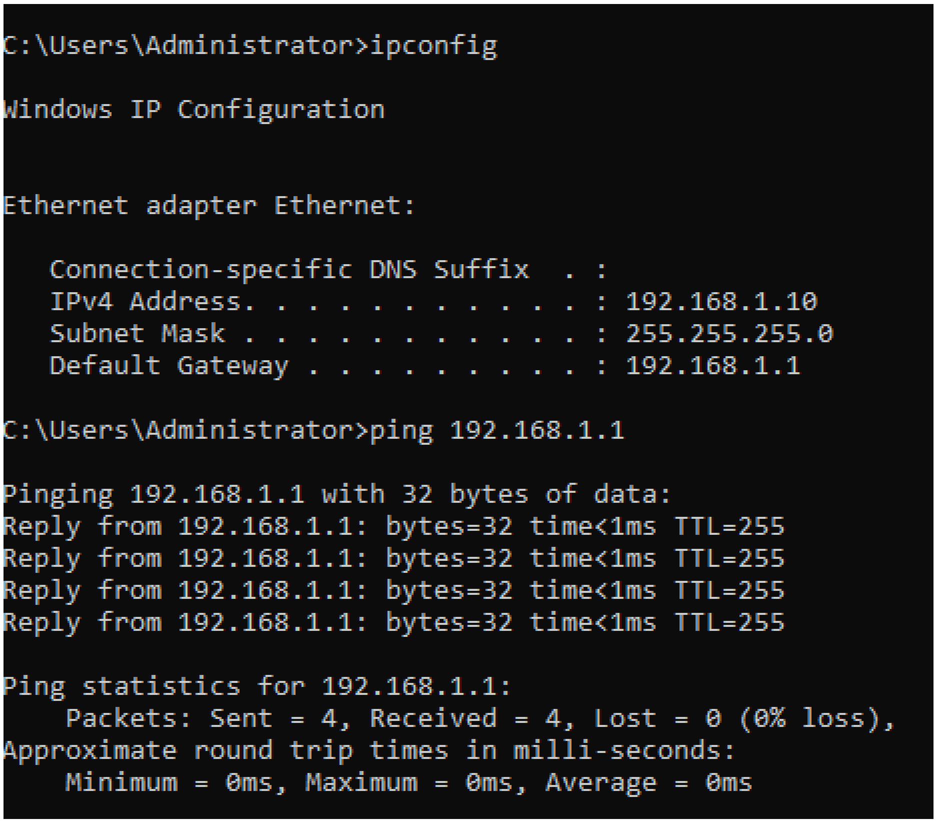
□ Validate settings upon exit



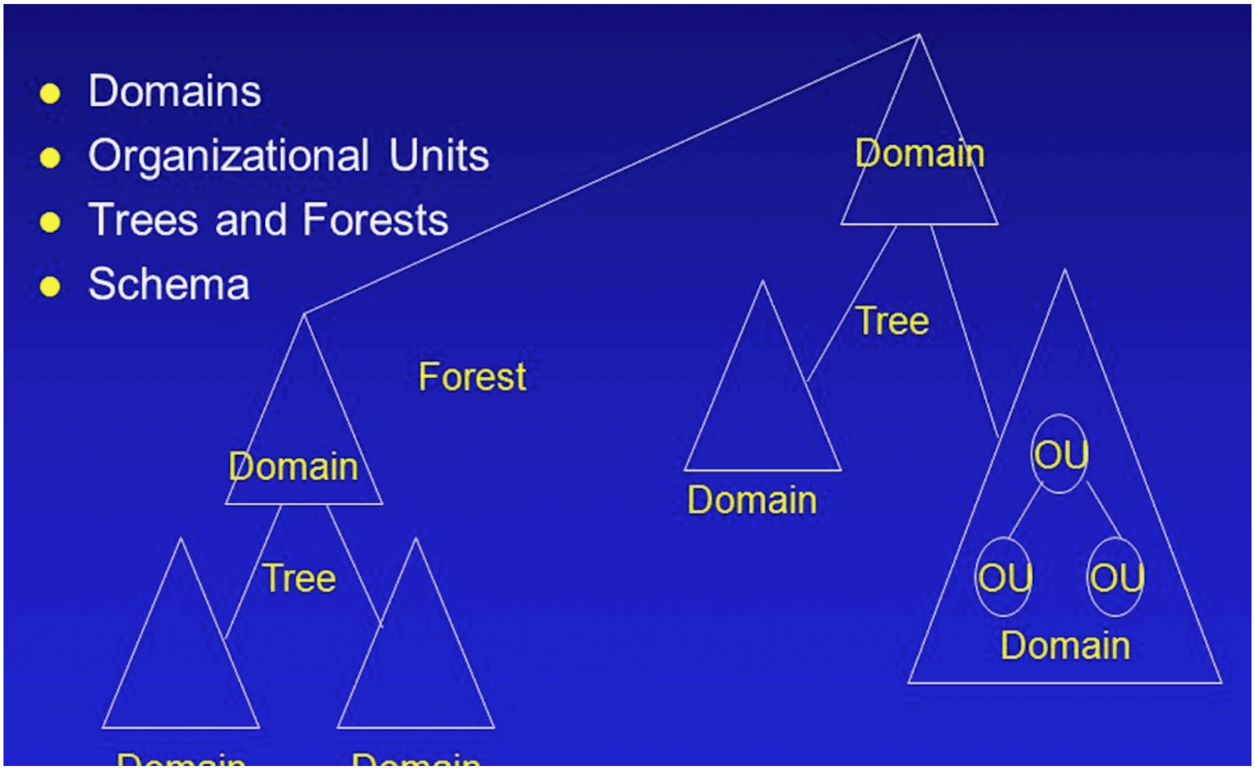
PROPERTIES
For SADC01

Computer name	SADC01
Workgroup	WORKGROUP
Windows Defender Firewall	Public: On
Remote management	Enabled
Remote Desktop	Disabled
NIC Teaming	Disabled
Ethernet	192.168.1.10

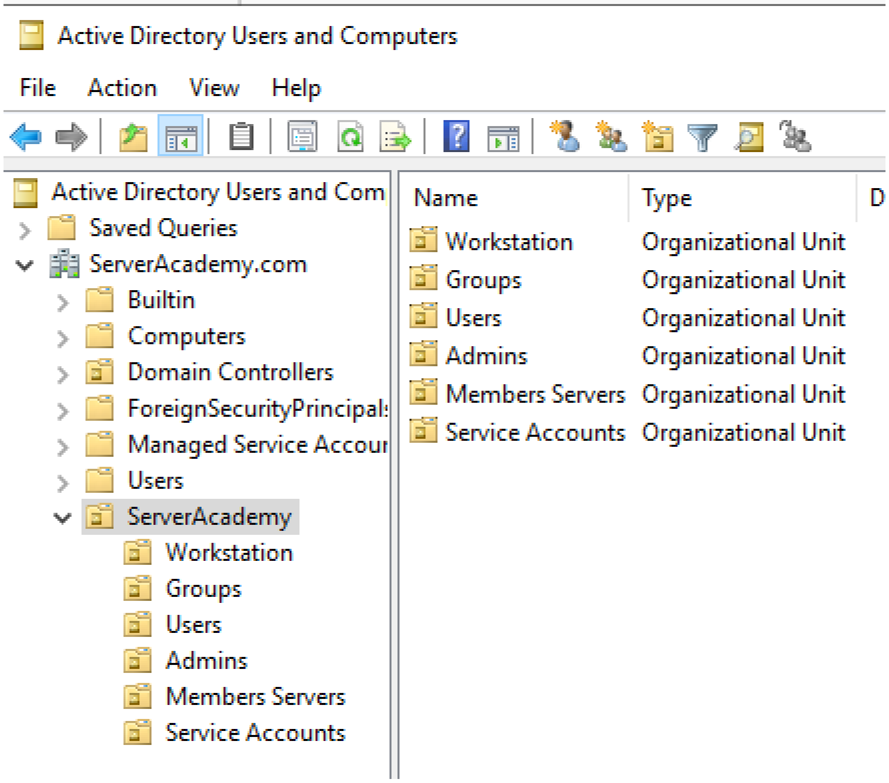
Pinging the Gateway



```
C:\Users\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.1.10
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

C:\Users\Administrator>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

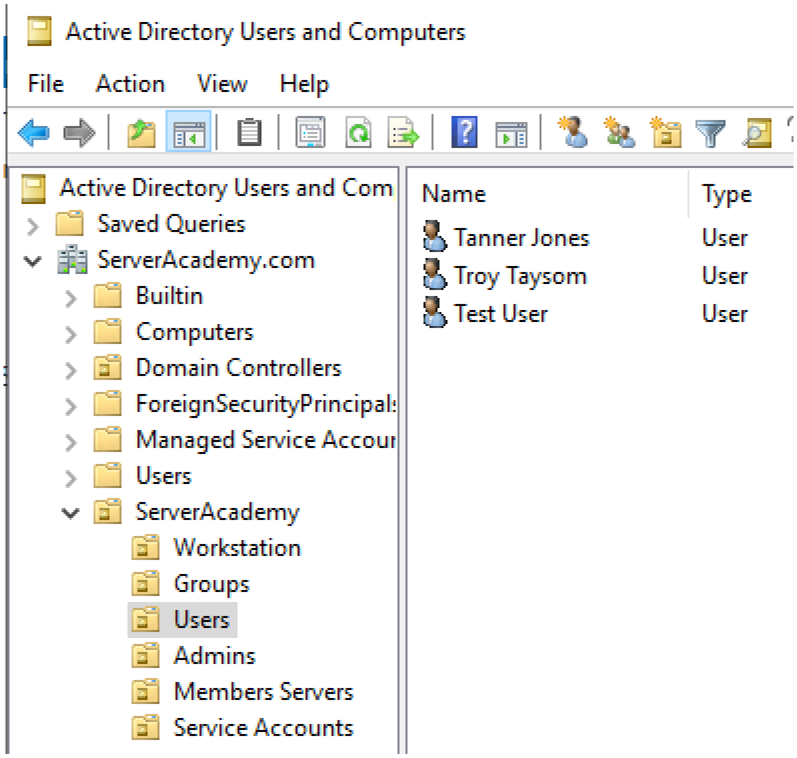


- Domains
- Organizational Units
- Trees and Forests
- Schema

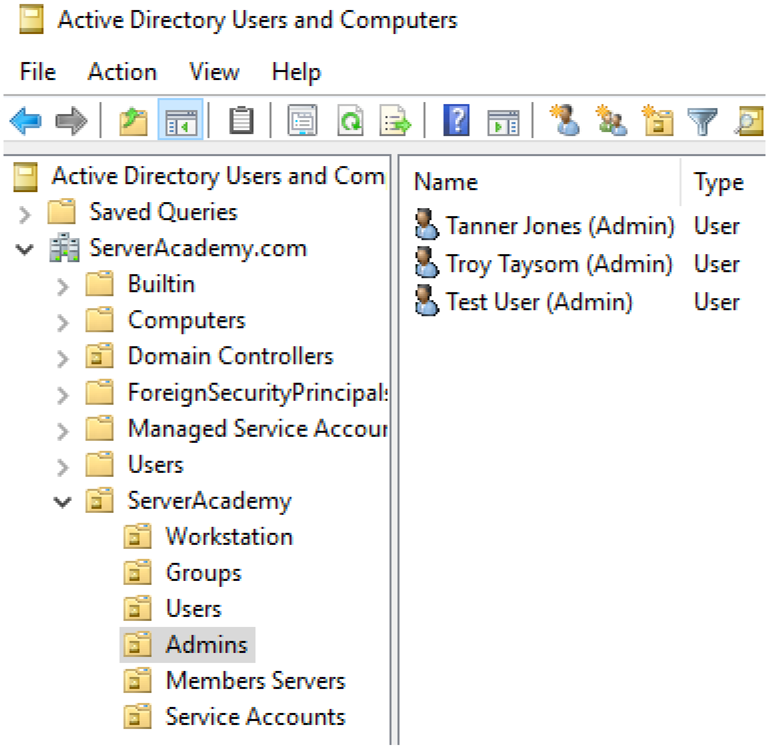


- Active Directory Users and Com
  - Saved Queries
  - ServerAcademy.com
    - Builtin
    - Computers
    - Domain Controllers
    - ForeignSecurityPrincipal:
    - Managed Service Accour
    - Users
    - ServerAcademy
      - Workstation
      - Groups
      - Users
      - Admins
      - Members Servers
      - Service Accounts

Name	Type	D
Workstation	Organizational Unit	
Groups	Organizational Unit	
Users	Organizational Unit	
Admins	Organizational Unit	
Members Servers	Organizational Unit	
Service Accounts	Organizational Unit	

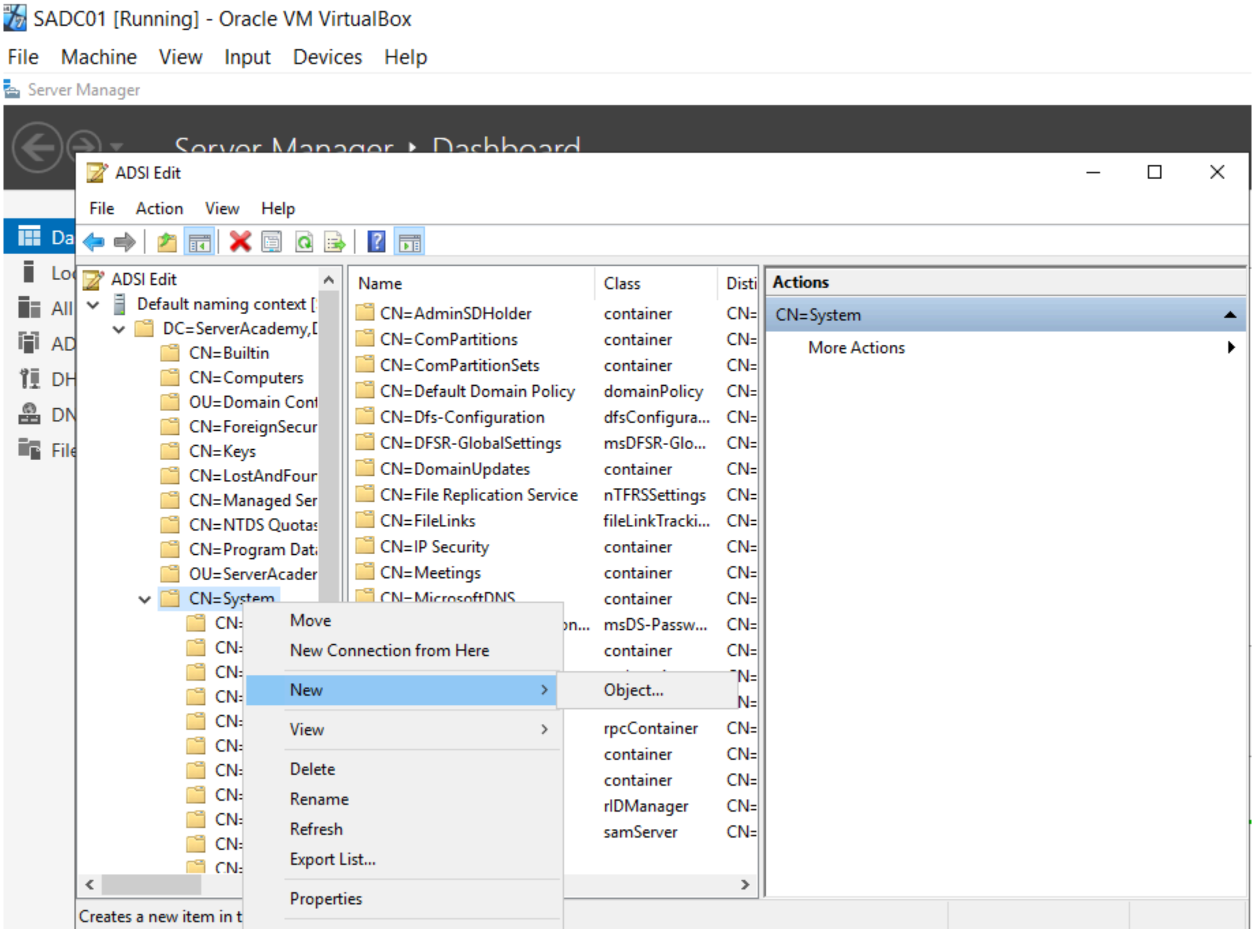


Name	Type
Tanner Jones	User
Troy Taysom	User
Test User	User



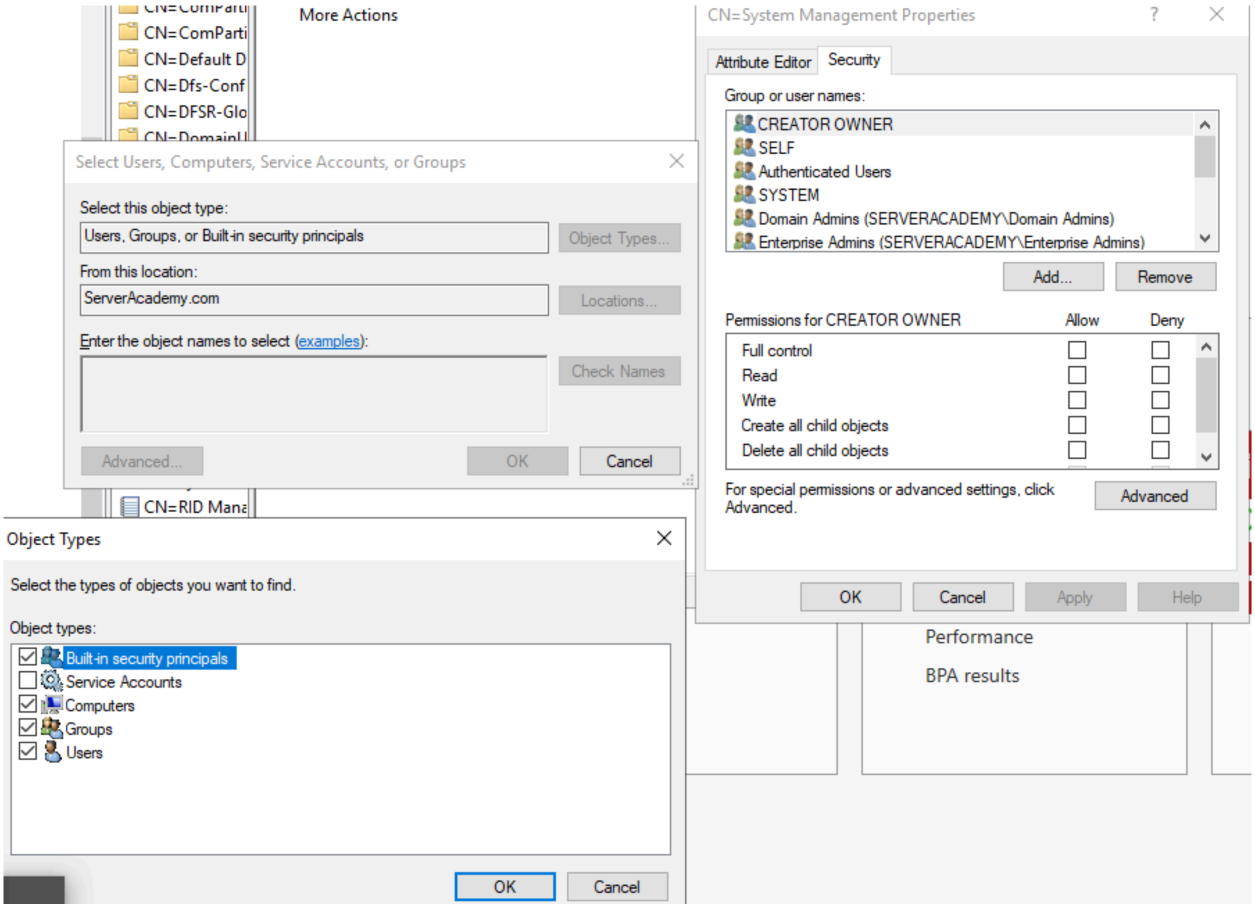
Name	Type
Tanner Jones (Admin)	User
Troy Taysom (Admin)	User
Test User (Admin)	User

Container Creation within Domain Controller



Name	Class	Disti
CN=AdminSDHolder	container	CN=
CN=ComPartitions	container	CN=
CN=ComPartitionSets	container	CN=
CN=Default Domain Policy	domainPolicy	CN=
CN=Dfs-Configuration	dfsConfigura...	CN=
CN=DFSR-GlobalSettings	msDFSR-Glo...	CN=
CN=DomainUpdates	container	CN=
CN=File Replication Service	nTFRSSettings	CN=
CN=FileLinks	fileLinkTracki...	CN=
CN=IP Security	container	CN=
CN=Meetings	container	CN=
CN=MicrosoftDNS	container	CN=
...n...	msDS-Passw...	CN=
	container	CN=
		N=
		N=
	rpcContainer	CN=
	container	CN=
	container	CN=
	rIDManager	CN=
	samServer	CN=

Security Configuration of New Container (DC)



Select Users, Computers, Service Accounts, or Groups

Select this object type:
Users, Groups, or Built-in security principals

From this location:
ServerAcademy.com

Enter the object names to select (examples):

Object Types

Select the types of objects you want to find.

Object types:

- ☑ Built-in security principals
- ☐ Service Accounts
- ☑ Computers
- ☑ Groups
- ☑ Users

CN=System Management Properties

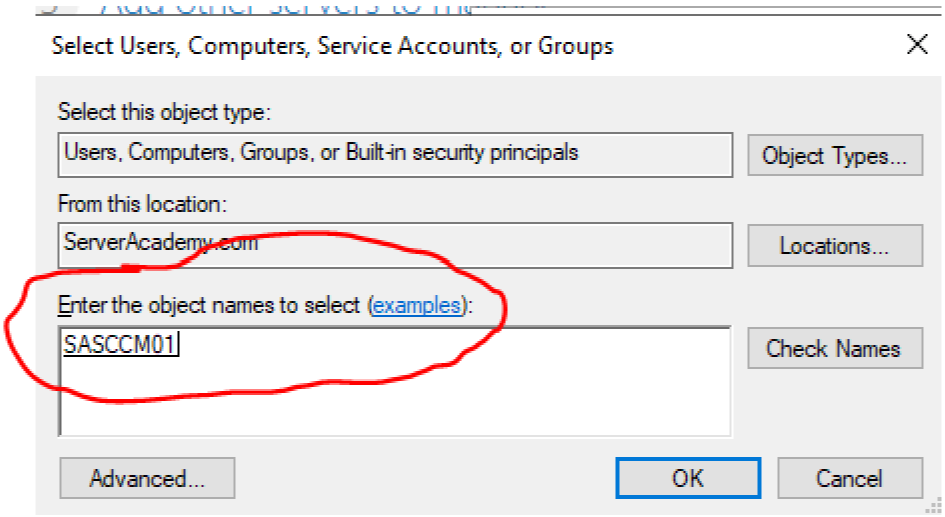
Group or user names:

- CREATOR OWNER
- SELF
- Authenticated Users
- SYSTEM
- Domain Admins (SERVERACADEMY\Domain Admins)
- Enterprise Admins (SERVERACADEMY\Enterprise Admins)

Permissions for CREATOR OWNER	Allow	Deny
Full control	□	□
Read	□	□
Write	□	□
Create all child objects	□	□
Delete all child objects	□	□

For special permissions or advanced settings, click Advanced.

Adding SASCCM Server to groups within container



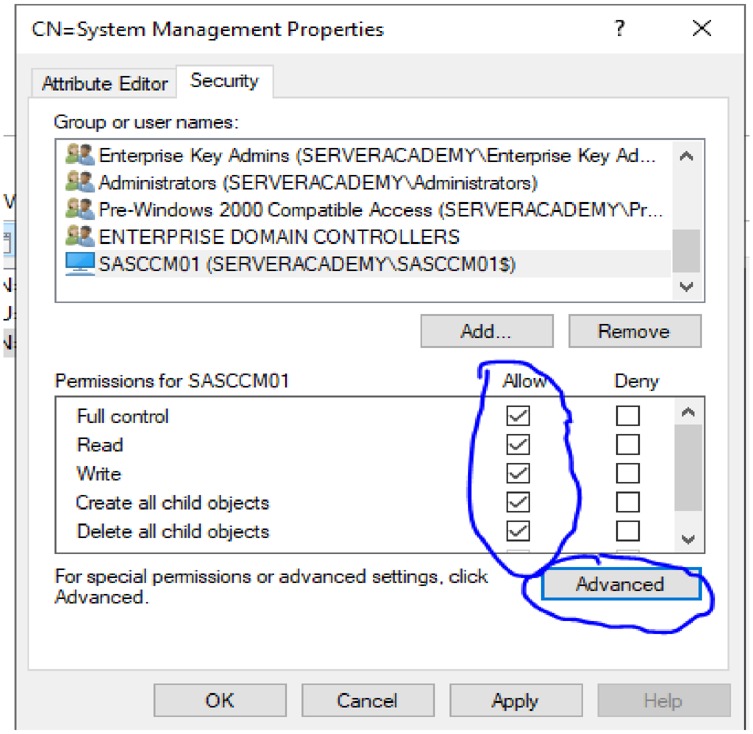
Select Users, Computers, Service Accounts, or Groups

Select this object type:
Users, Computers, Groups, or Built-in security principals

From this location:
ServerAcademy.com

Enter the object names to select (examples):
SASCCM01

Granting full permissions to SASCCM

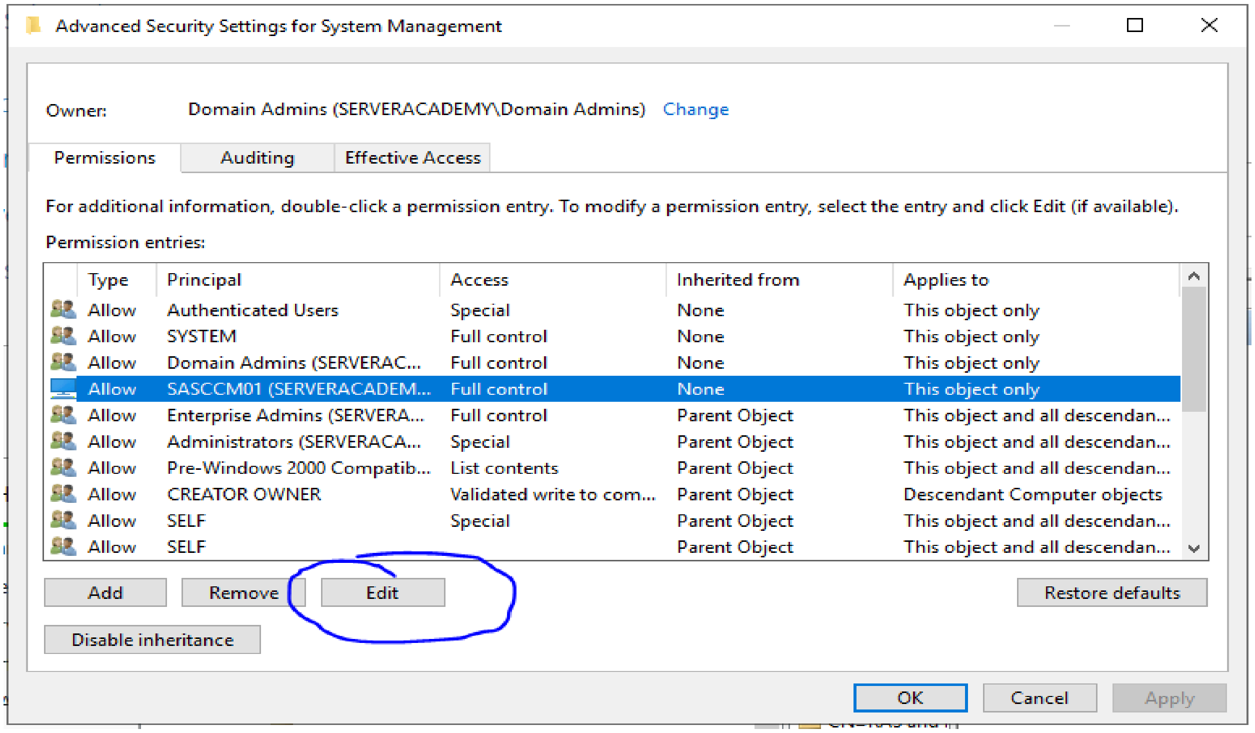

CN=System Management Properties

Group or user names:

- Enterprise Key Admins (SERVERACADEMY\Enterprise Key Ad...
- Administrators (SERVERACADEMY\Administrators)
- Pre-Windows 2000 Compatible Access (SERVERACADEMY\Pr...
- ENTERPRISE DOMAIN CONTROLLERS
- SASCCM01 (SERVERACADEMY\SASCCM01$)

Permissions for SASCCM01	Allow	Deny
Full control	☑	□
Read	☑	□
Write	☑	□
Create all child objects	☑	□
Delete all child objects	☑	□

For special permissions or advanced settings, click Advanced.


Advanced Security Settings for System Management

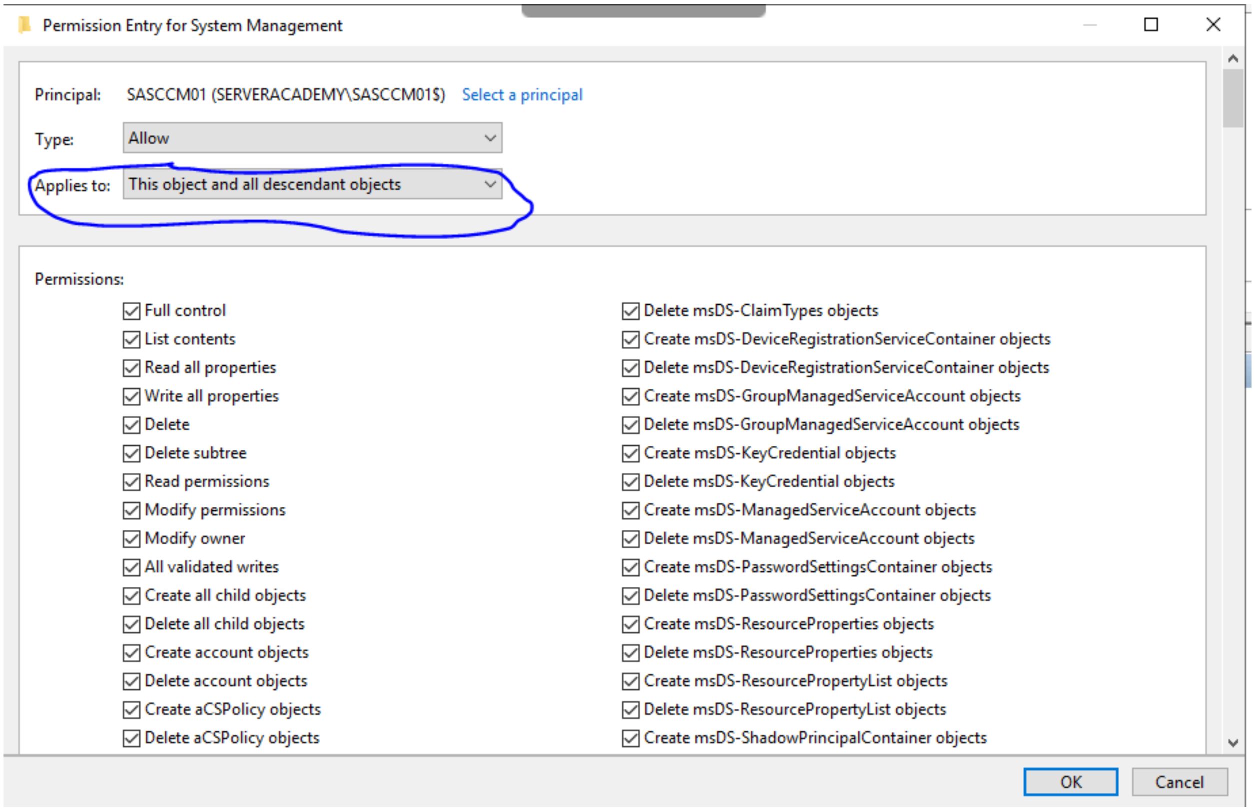
Owner: Domain Admins (SERVERACADEMY\Domain Admins) Change

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Principal	Access	Inherited from	Applies to
Allow	Authenticated Users	Special	None	This object only
Allow	SYSTEM	Full control	None	This object only
Allow	Domain Admins (SERVERAC...	Full control	None	This object only
Allow	SASCCM01 (SERVERACADEM...	Full control	None	This object only
Allow	Enterprise Admins (SERVERA...	Full control	Parent Object	This object and all descendan...
Allow	Administrators (SERVERACA...	Special	Parent Object	This object and all descendan...
Allow	Pre-Windows 2000 Compatib...	List contents	Parent Object	This object and all descendan...
Allow	CREATOR OWNER	Validated write to com...	Parent Object	Descendant Computer objects
Allow	SELF	Special	Parent Object	This object and all descendan...
Allow	SELF		Parent Object	This object and all descendan...

Granting permissions to descendant objects of SASCCM



Principal: SASCCM01 (SERVERACADEMY\SASCCM01$) Select a principal

Type: Allow

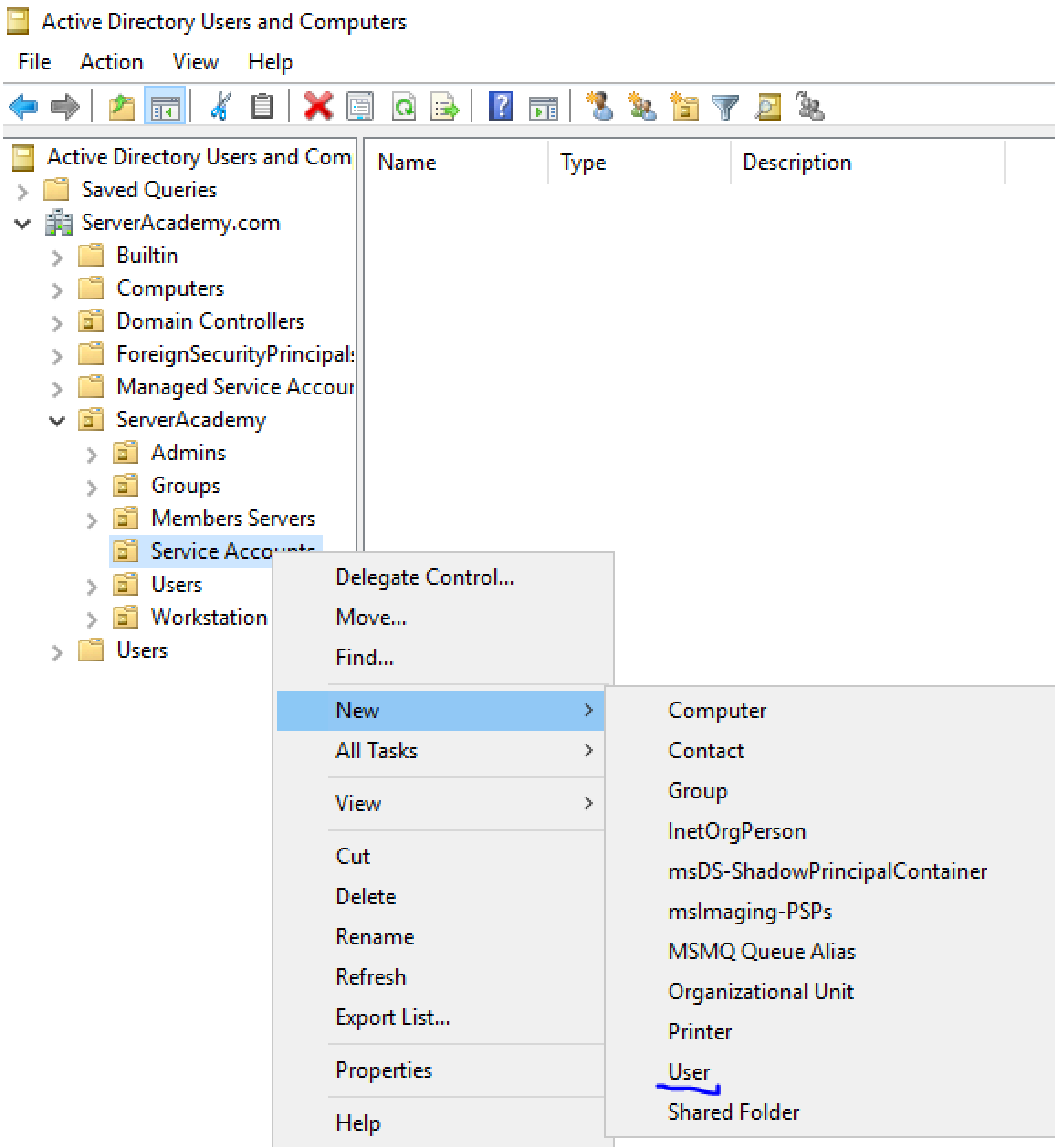
Applies to: This object and all descendant objects

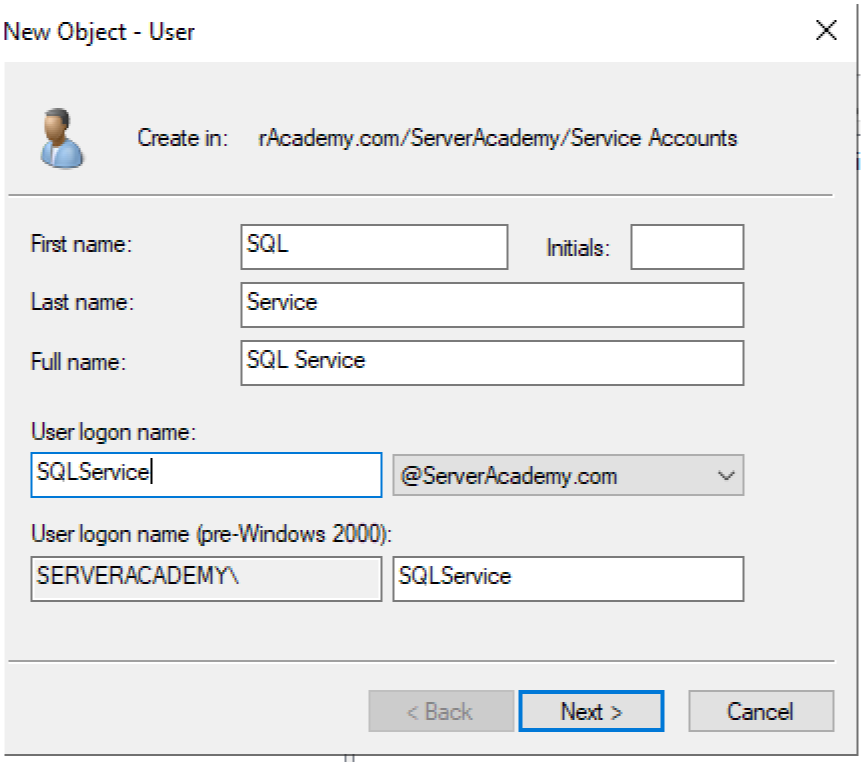
Permissions:

☑ Full control
☑ List contents
☑ Read all properties
☑ Write all properties
☑ Delete
☑ Delete subtree
☑ Read permissions
☑ Modify permissions
☑ Modify owner
☑ All validated writes
☑ Create all child objects
☑ Delete all child objects
☑ Create account objects
☑ Delete account objects
☑ Create aCSPolicy objects
☑ Delete aCSPolicy objects

☑ Delete msDS-ClaimTypes objects
☑ Create msDS-DeviceRegistrationServiceContainer objects
☑ Delete msDS-DeviceRegistrationServiceContainer objects
☑ Create msDS-GroupManagedServiceAccount objects
☑ Delete msDS-GroupManagedServiceAccount objects
☑ Create msDS-KeyCredential objects
☑ Delete msDS-KeyCredential objects
☑ Create msDS-ManagedServiceAccount objects
☑ Delete msDS-ManagedServiceAccount objects
☑ Create msDS-PasswordSettingsContainer objects
☑ Delete msDS-PasswordSettingsContainer objects
☑ Create msDS-ResourceProperties objects
☑ Delete msDS-ResourceProperties objects
☑ Create msDS-ResourcePropertyList objects
☑ Delete msDS-ResourcePropertyList objects
☑ Create msDS-ShadowPrincipalContainer objects

Creating SQL Service within Service Accounts




New Object - User

Create in: rAcademy.com/ServerAcademy/Service Accounts

First name: SQL

Initials:

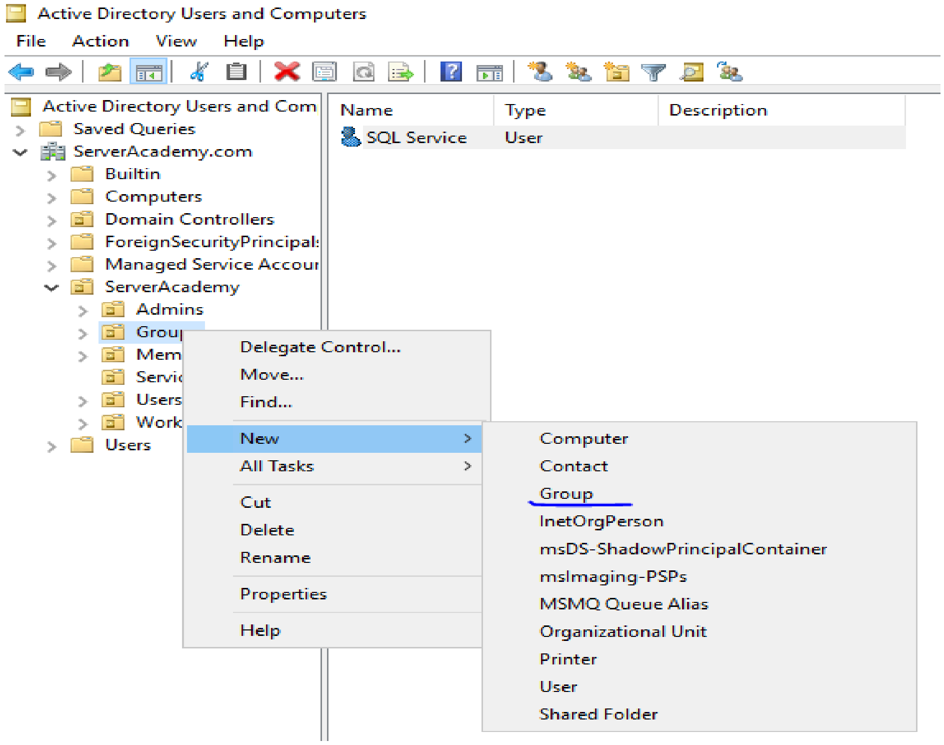
Last name: Service

Full name: SQL Service

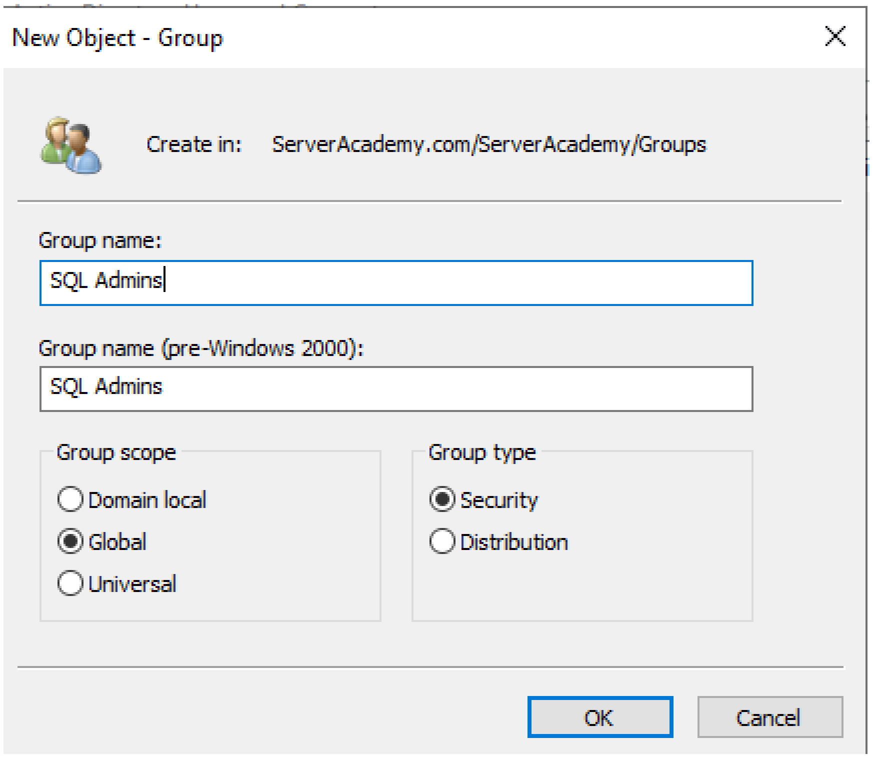
User logon name: SQLService @ServerAcademy.com

User logon name (pre-Windows 2000): SERVERACADEMY\ SQLService

Creating Admin Groups within ServerAcademy


Active Directory Users and Computers

Name	Type	Description
SQL Service	User	



New Object - Group

Create in: ServerAcademy.com/ServerAcademy/Groups

Group name: SQL Admins

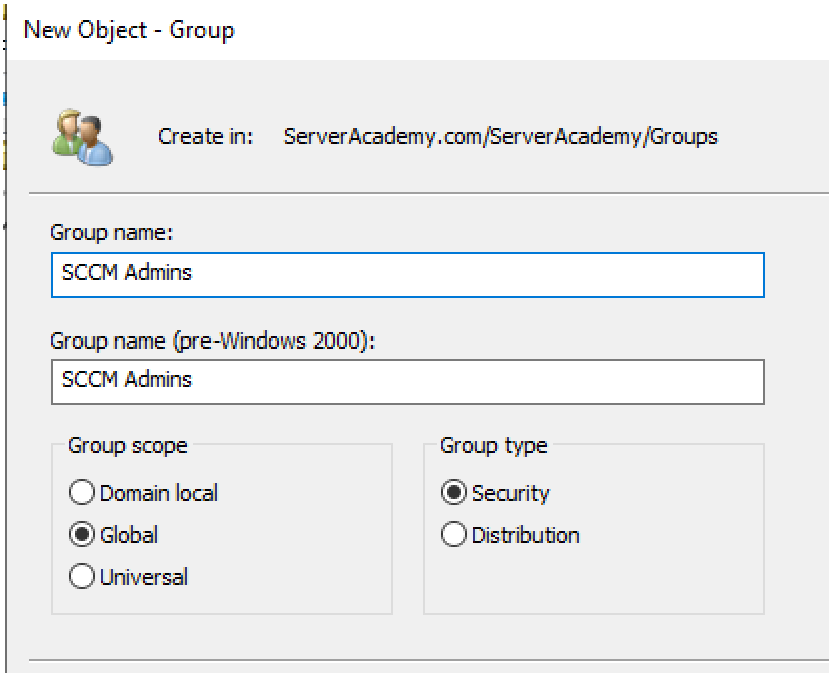
Group name (pre-Windows 2000): SQL Admins

Group scope

○ Domain local
● Global
○ Universal

Group type

● Security
○ Distribution



New Object - Group

Create in: ServerAcademy.com/ServerAcademy/Groups

Group name: SCCM Admins

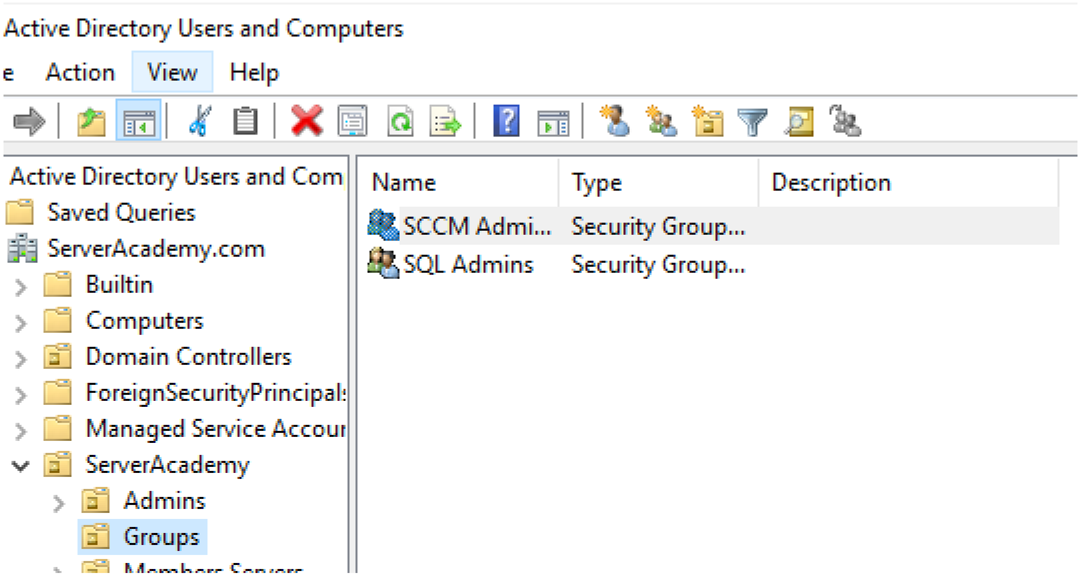
Group name (pre-Windows 2000): SCCM Admins

Group scope

○ Domain local
● Global
○ Universal

Group type

● Security
○ Distribution

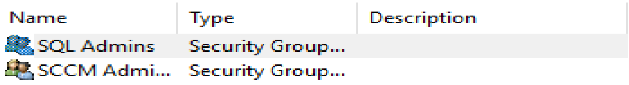


Active Directory Users and Computers

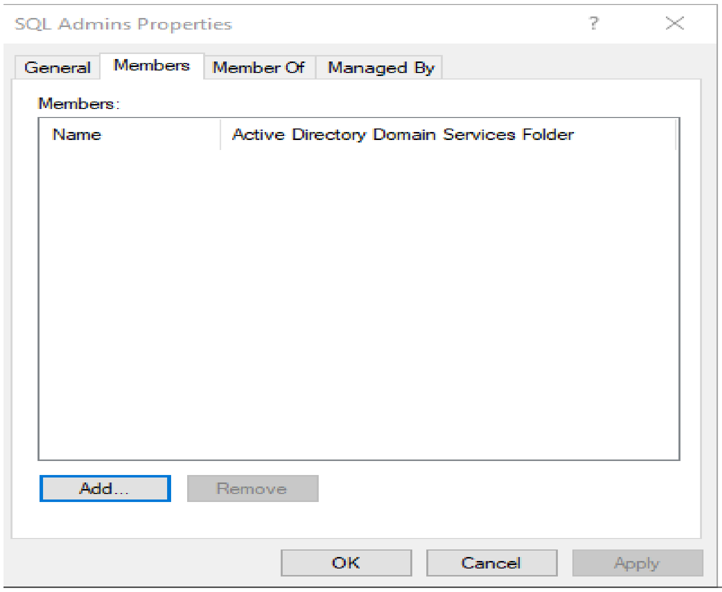
Active Directory Users and Com
Saved Queries
ServerAcademy.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipal:
Managed Service Accour
ServerAcademy
Admins
Groups
Members Servers

Name	Type	Description
SCCM Admi...	Security Group...	
SQL Admins	Security Group...	

Adding Users to the Created Groups



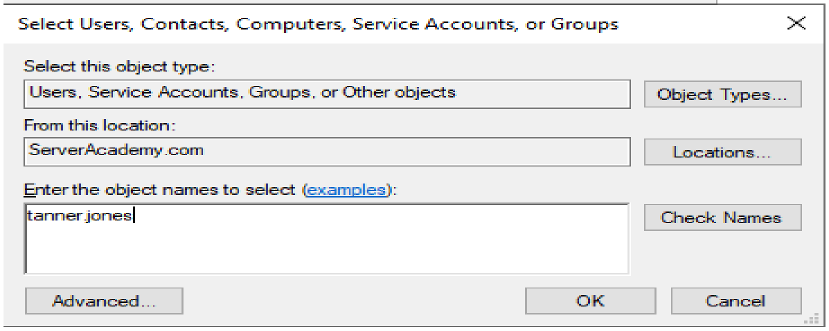
Name	Type	Description
SQL Admins	Security Group...	
SCCM Admi...	Security Group...	



SQL Admins Properties

Members:

Name	Active Directory Domain Services Folder

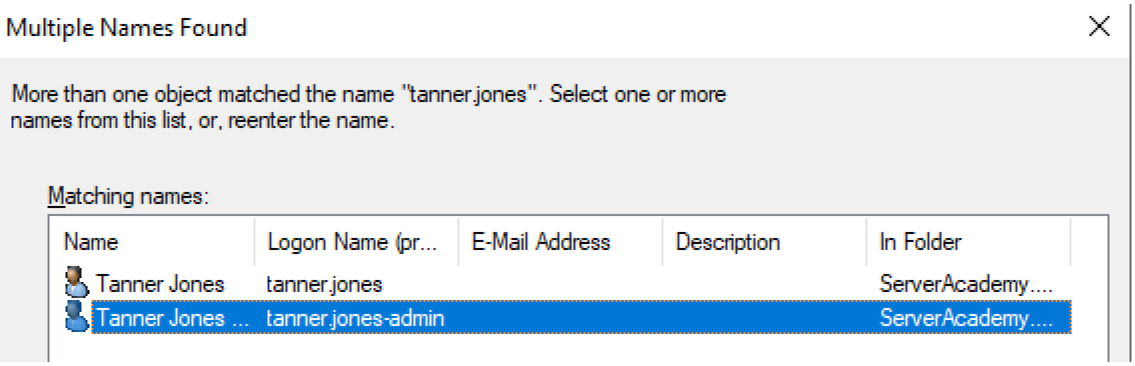


Select Users, Contacts, Computers, Service Accounts, or Groups

Select this object type:
Users, Service Accounts, Groups, or Other objects

From this location:
ServerAcademy.com

Enter the object names to select (examples):
tanner.jones

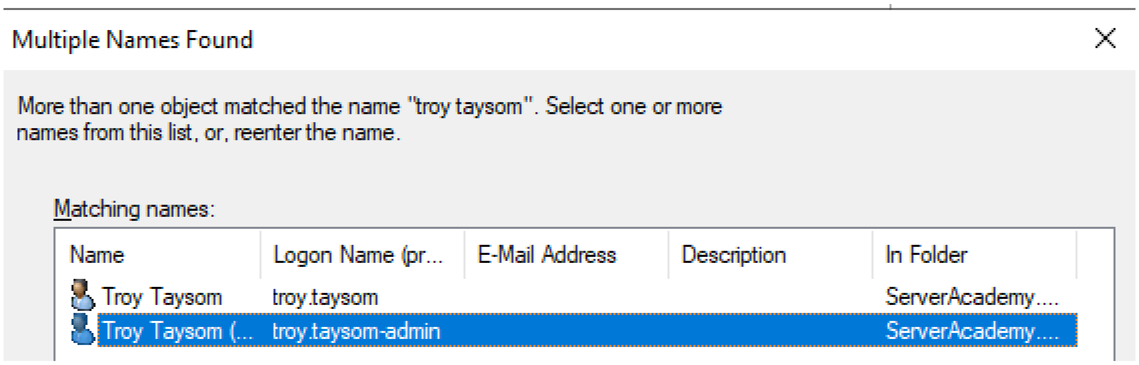


Multiple Names Found

More than one object matched the name "tanner.jones". Select one or more names from this list, or, reenter the name.

Matching names:

Name	Logon Name (pr...	E-Mail Address	Description	In Folder
Tanner Jones	tanner.jones			ServerAcademy....
Tanner Jones ...	tanner.jones-admin			ServerAcademy....

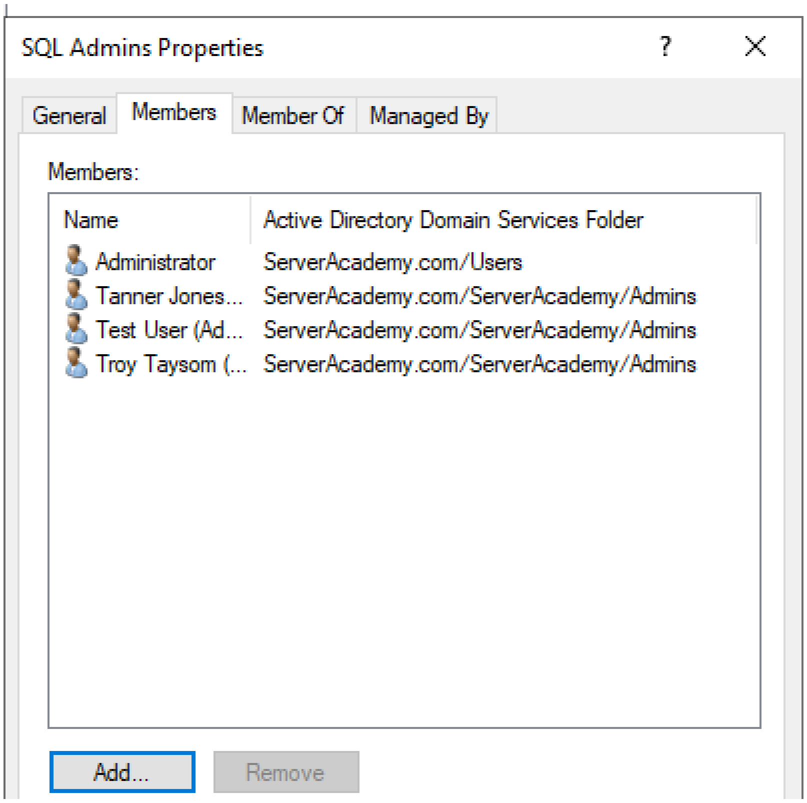


Multiple Names Found

More than one object matched the name "troy.taysom". Select one or more names from this list, or, reenter the name.

Matching names:

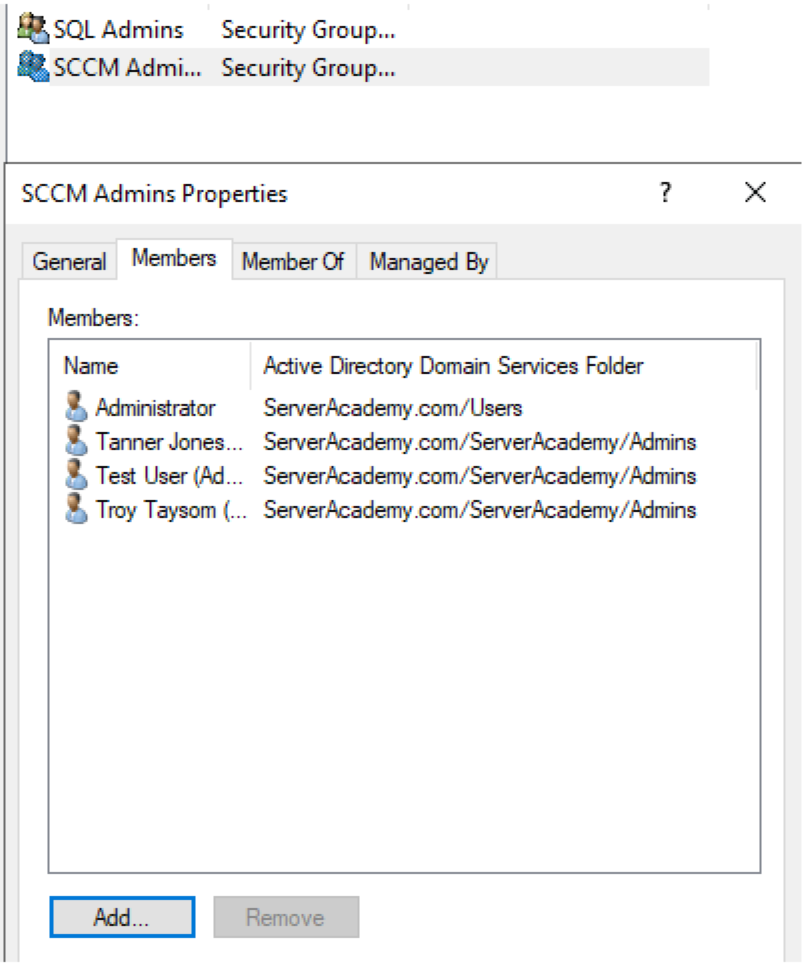
Name	Logon Name (pr...	E-Mail Address	Description	In Folder
Troy Taysom	troy.taysom			ServerAcademy....
Troy Taysom (...	troy.taysom-admin			ServerAcademy....



SQL Admins Properties

Members:

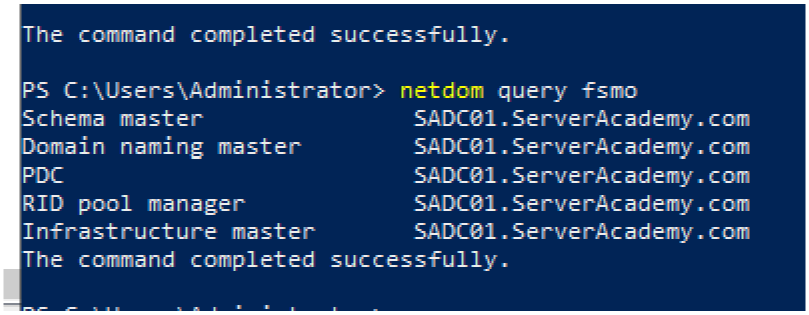
Name	Active Directory Domain Services Folder
Administrator	ServerAcademy.com/Users
Tanner Jones...	ServerAcademy.com/ServerAcademy/Admins
Test User (Ad...	ServerAcademy.com/ServerAcademy/Admins
Troy Taysom (...	ServerAcademy.com/ServerAcademy/Admins



SQL Admins	Security Group...
SCCM Admi...	Security Group...

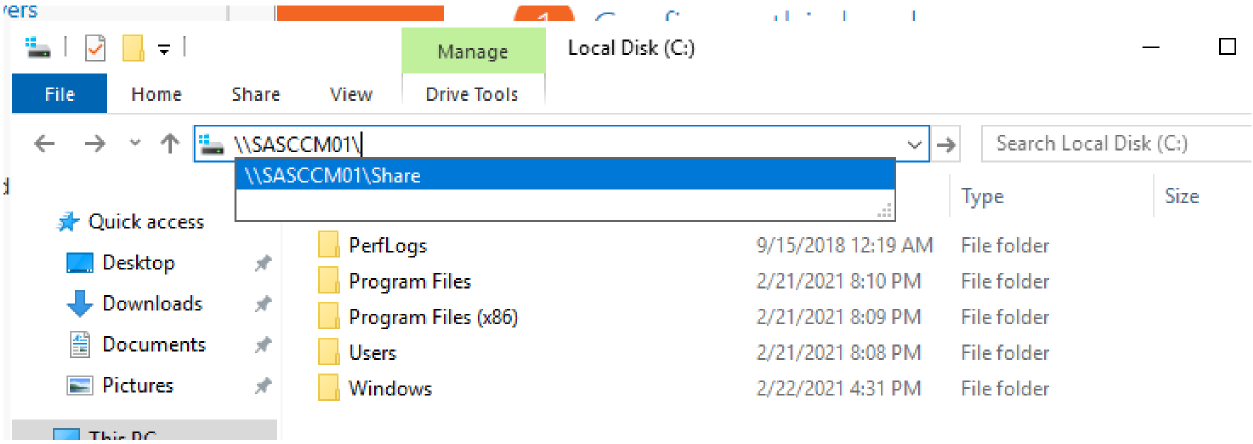
Name	Active Directory Domain Services Folder
Administrator	ServerAcademy.com/Users
Tanner Jones...	ServerAcademy.com/ServerAcademy/Admins
Test User (Ad...	ServerAcademy.com/ServerAcademy/Admins
Troy Taysom (...	ServerAcademy.com/ServerAcademy/Admins

Extending the Active Directory Schema (DC)



```
The command completed successfully.

PS C:\Users\Administrator> netdom query fsmo
Schema master               SADC01.ServerAcademy.com
Domain naming master        SADC01.ServerAcademy.com
PDC                         SADC01.ServerAcademy.com
RID pool manager            SADC01.ServerAcademy.com
Infrastructure master       SADC01.ServerAcademy.com
The command completed successfully.
```

Accessing the shared file from SADC01

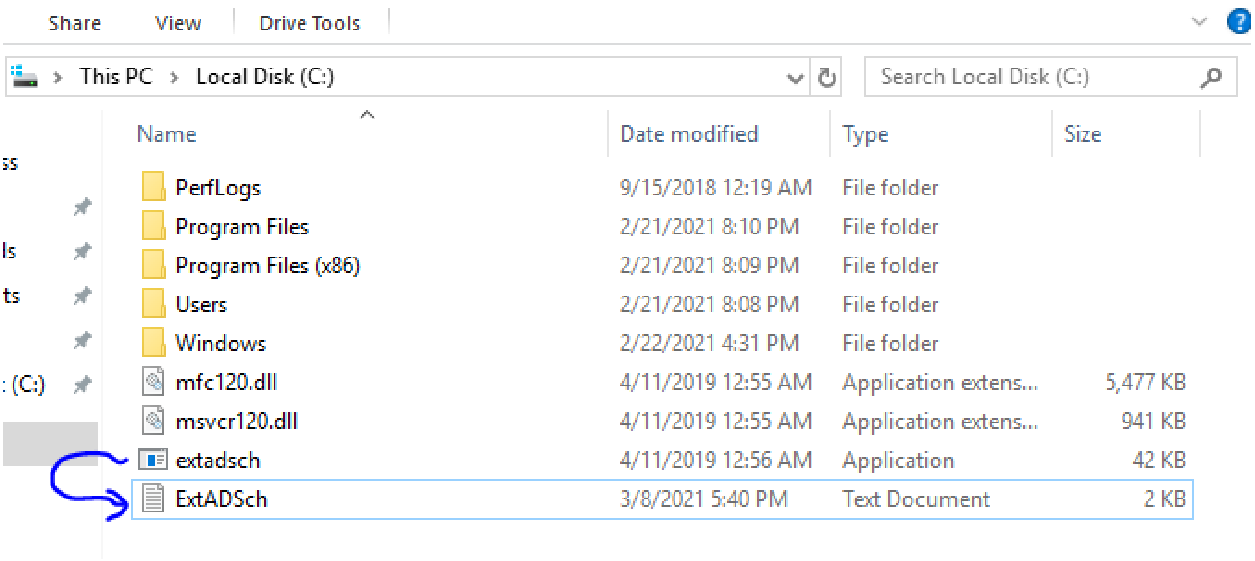


\\SASCCM01\

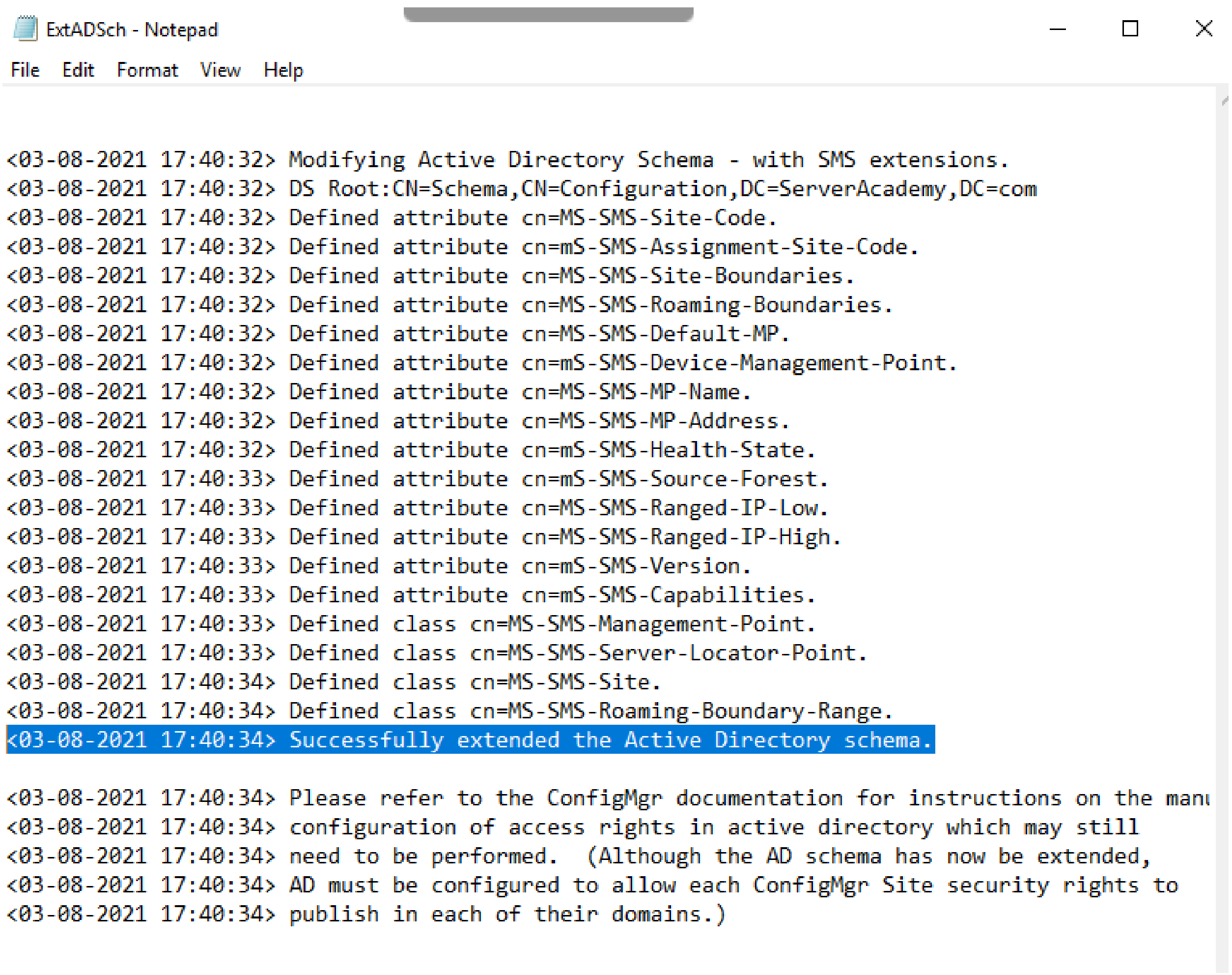
\\SASCCM01\Share

Name	Date modified	Type	Size
PerfLogs	9/15/2018 12:19 AM	File folder	
Program Files	2/21/2021 8:10 PM	File folder	
Program Files (x86)	2/21/2021 8:09 PM	File folder	
Users	2/21/2021 8:08 PM	File folder	
Windows	2/22/2021 4:31 PM	File folder	

Ran extadsch as admin to create text document

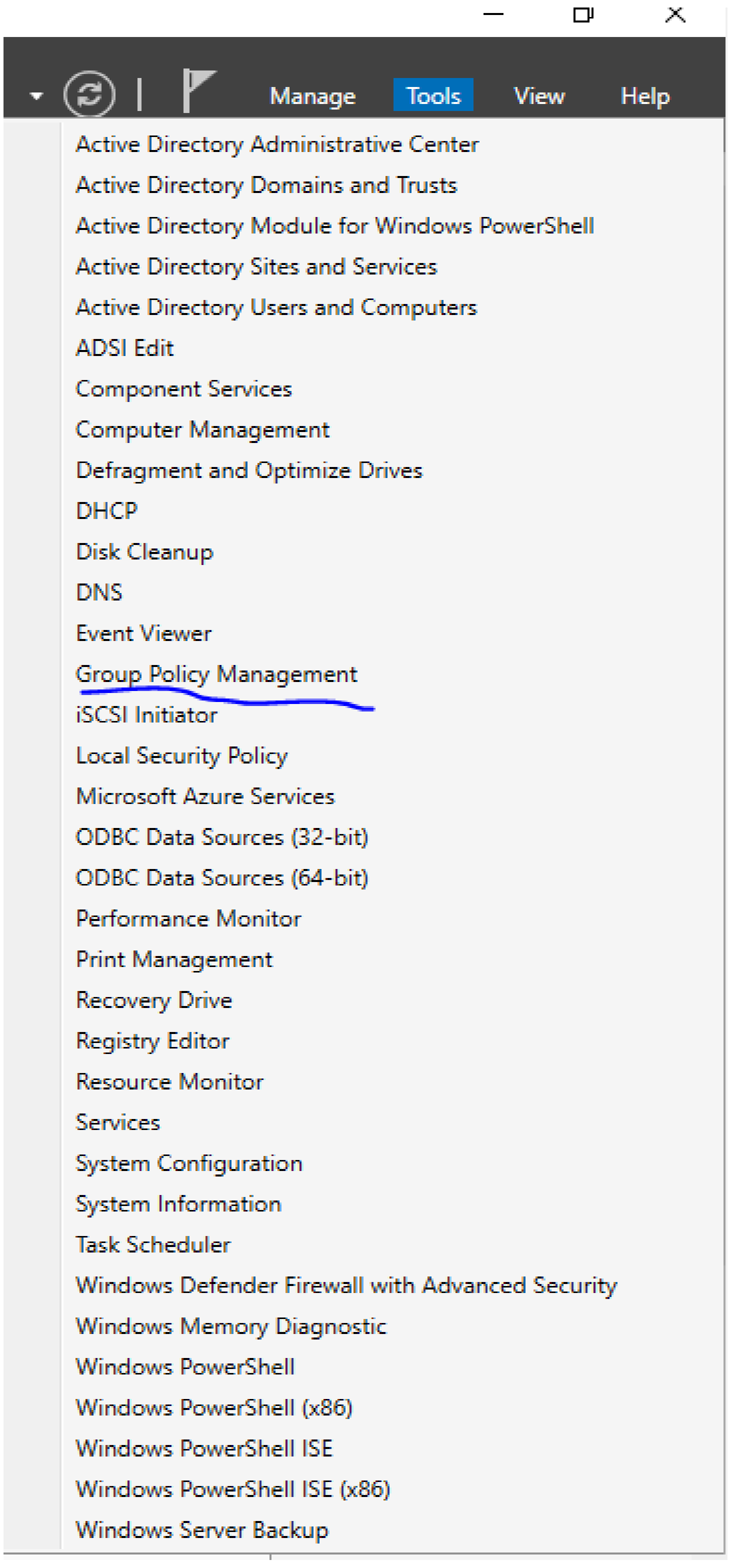


Name	Date modified	Type	Size
PerfLogs	9/15/2018 12:19 AM	File folder	
Program Files	2/21/2021 8:10 PM	File folder	
Program Files (x86)	2/21/2021 8:09 PM	File folder	
Users	2/21/2021 8:08 PM	File folder	
Windows	2/22/2021 4:31 PM	File folder	
mfc120.dll	4/11/2019 12:55 AM	Application extens...	5,477 KB
msvcr120.dll	4/11/2019 12:55 AM	Application extens...	941 KB
extadsch	4/11/2019 12:56 AM	Application	42 KB
ExtADSch	3/8/2021 5:40 PM	Text Document	2 KB

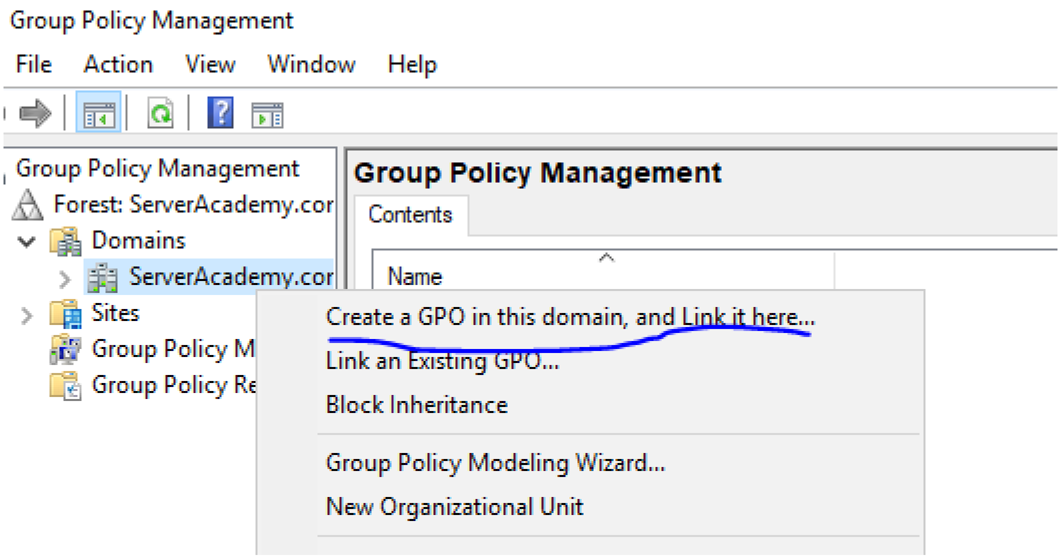


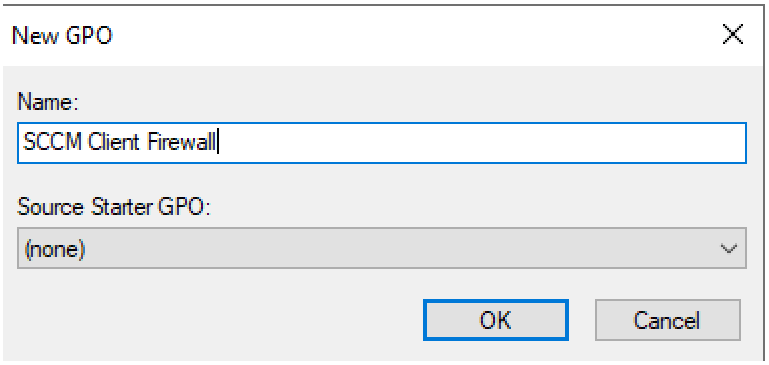
```
<03-08-2021 17:40:32> Modifying Active Directory Schema - with SMS extensions.
<03-08-2021 17:40:32> DS Root:CN=Schema,CN=Configuration,DC=ServerAcademy,DC=com
<03-08-2021 17:40:32> Defined attribute cn=MS-SMS-Site-Code.
<03-08-2021 17:40:32> Defined attribute cn=mS-SMS-Assignment-Site-Code.
<03-08-2021 17:40:32> Defined attribute cn=MS-SMS-Site-Boundaries.
<03-08-2021 17:40:32> Defined attribute cn=MS-SMS-Roaming-Boundaries.
<03-08-2021 17:40:32> Defined attribute cn=MS-SMS-Default-MP.
<03-08-2021 17:40:32> Defined attribute cn=mS-SMS-Device-Management-Point.
<03-08-2021 17:40:32> Defined attribute cn=MS-SMS-MP-Name.
<03-08-2021 17:40:32> Defined attribute cn=MS-SMS-MP-Address.
<03-08-2021 17:40:32> Defined attribute cn=mS-SMS-Health-State.
<03-08-2021 17:40:33> Defined attribute cn=mS-SMS-Source-Forest.
<03-08-2021 17:40:33> Defined attribute cn=MS-SMS-Ranged-IP-Low.
<03-08-2021 17:40:33> Defined attribute cn=MS-SMS-Ranged-IP-High.
<03-08-2021 17:40:33> Defined attribute cn=mS-SMS-Version.
<03-08-2021 17:40:33> Defined attribute cn=mS-SMS-Capabilities.
<03-08-2021 17:40:33> Defined class cn=MS-SMS-Management-Point.
<03-08-2021 17:40:33> Defined class cn=MS-SMS-Server-Locator-Point.
<03-08-2021 17:40:34> Defined class cn=MS-SMS-Site.
<03-08-2021 17:40:34> Defined class cn=MS-SMS-Roaming-Boundary-Range.
<03-08-2021 17:40:34> Successfully extended the Active Directory schema.

<03-08-2021 17:40:34> Please refer to the ConfigMgr documentation for instructions on the manu
<03-08-2021 17:40:34> configuration of access rights in active directory which may still
<03-08-2021 17:40:34> need to be performed.  (Although the AD schema has now be extended,
<03-08-2021 17:40:34> AD must be configured to allow each ConfigMgr Site security rights to
<03-08-2021 17:40:34> publish in each of their domains.)
```

Configuring Firewall with Group Policy



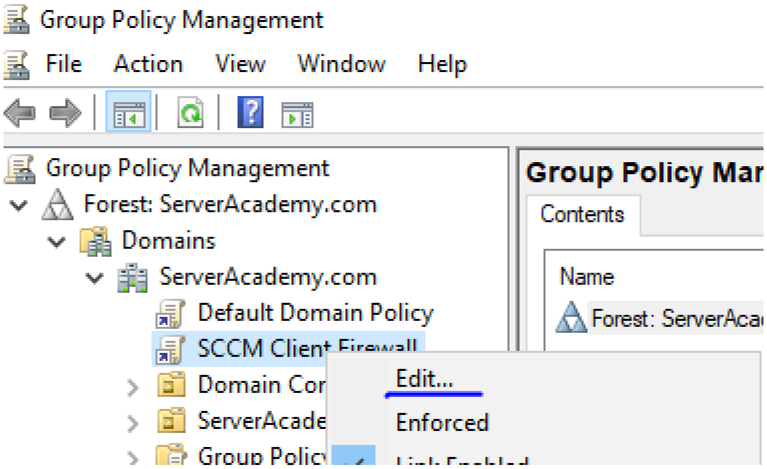
Applying Firewall rules to every computer in domain

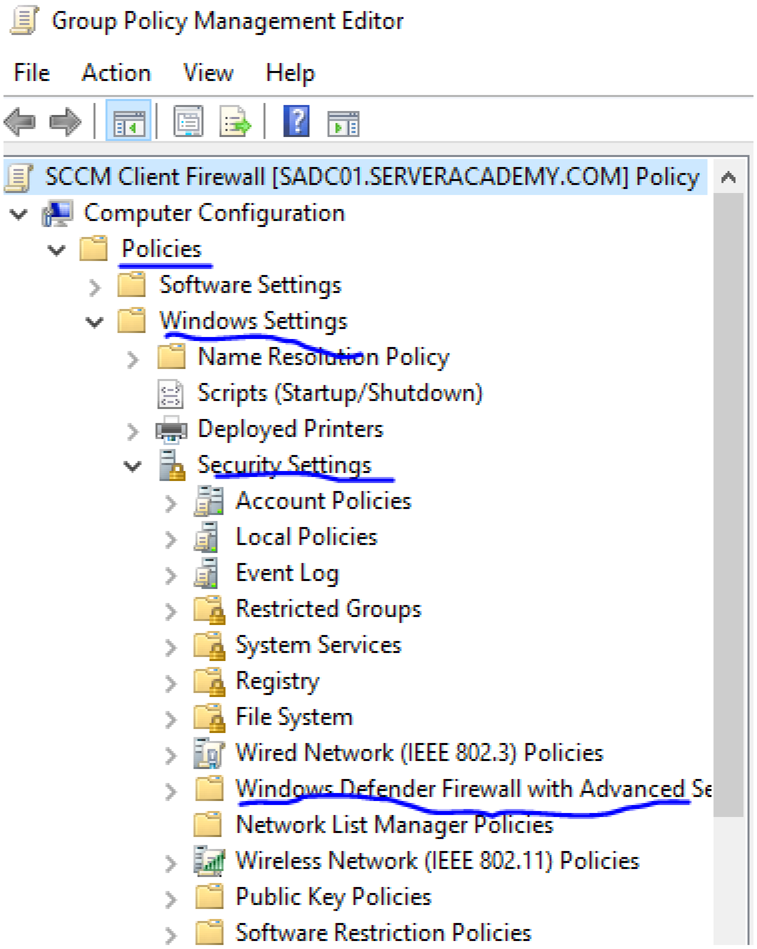


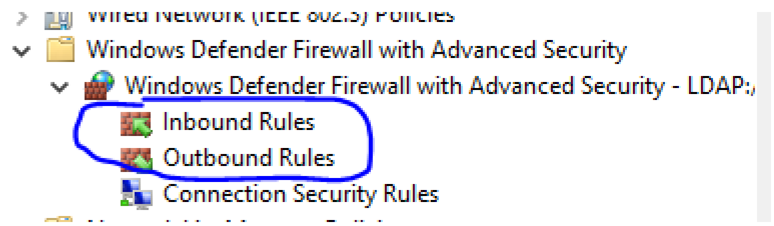


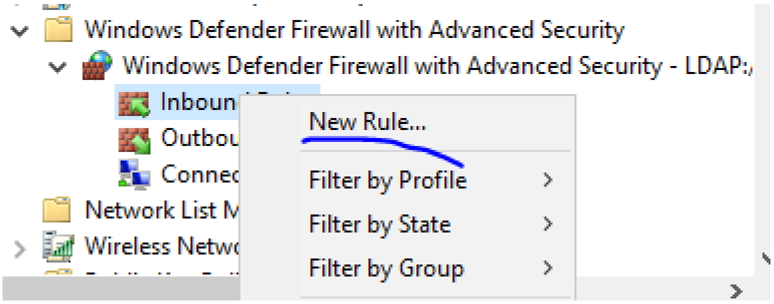
Name: SCCM Client Firewall

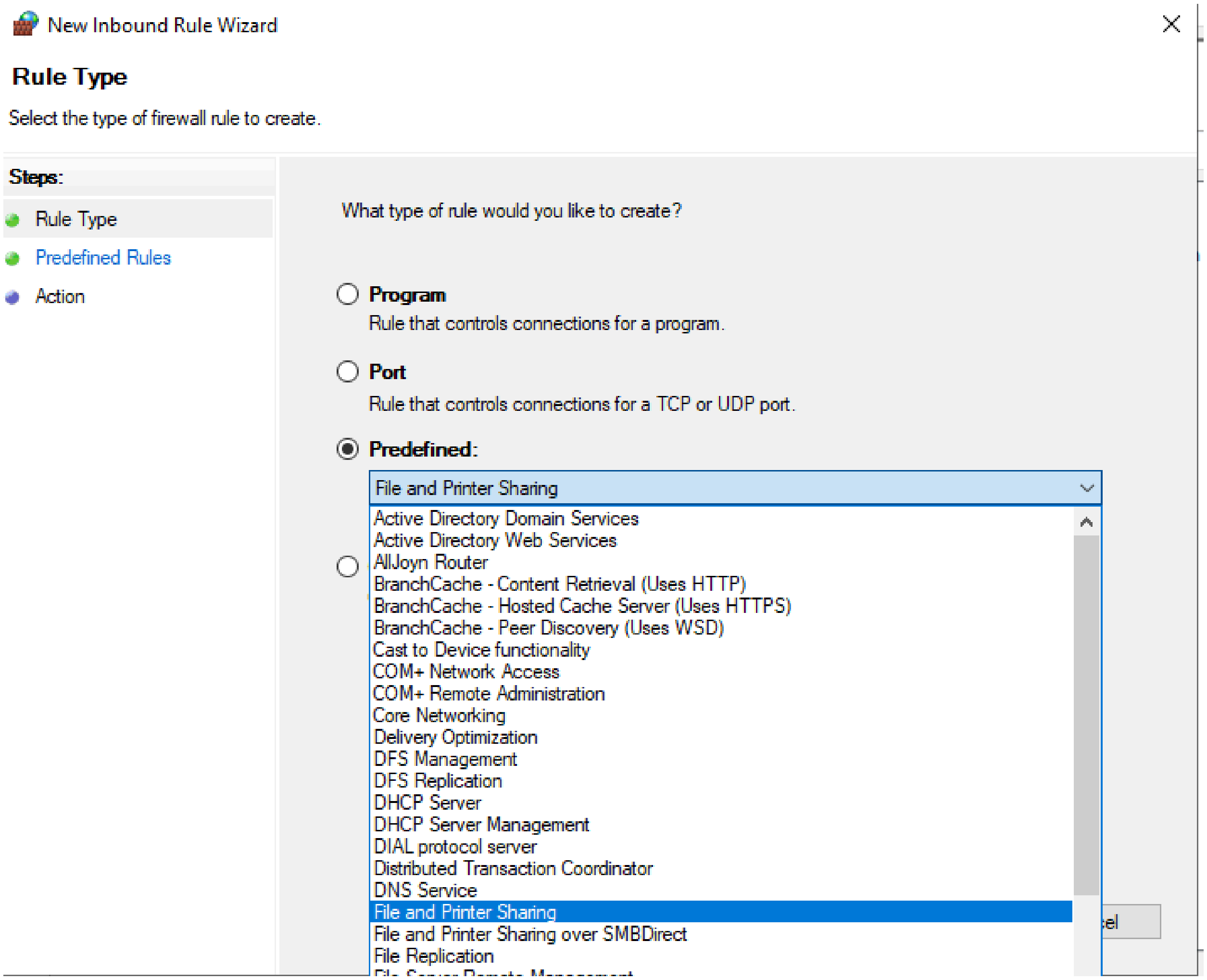
Source Starter GPO: (none)




Group Policy Management Editor
File
Action
View
Help
SCCM Client Firewall [SADC01.SERVERACADEMY.COM] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Defender Firewall with Advanced Se
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies


Wired Network (IEEE 802.3) Policies
Windows Defender Firewall with Advanced Security
Windows Defender Firewall with Advanced Security - LDAP:/
Inbound Rules
Outbound Rules
Connection Security Rules


Windows Defender Firewall with Advanced Security
Windows Defender Firewall with Advanced Security - LDAP:/
Inboun
Outbou
Connec
Network List M
Wireless Netwo
New Rule...
Filter by Profile
Filter by State
Filter by Group



New Inbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

Steps:

- Rule Type
- Predefined Rules
- Action

What type of rule would you like to create?

○ **Program**

Rule that controls connections for a program.

○ **Port**

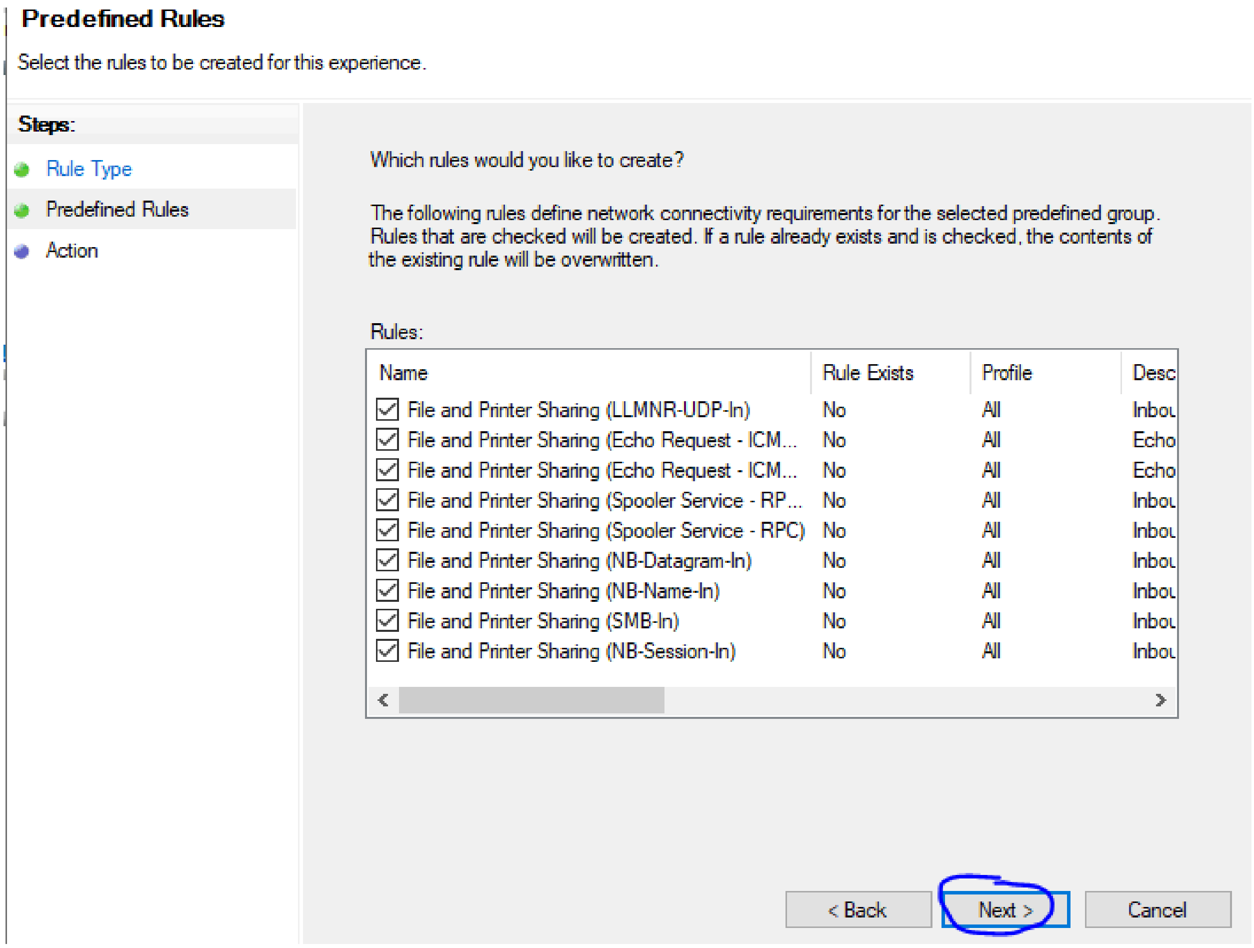
Rule that controls connections for a TCP or UDP port.

● **Predefined:**

File and Printer Sharing

Active Directory Domain Services
Active Directory Web Services
AllJoyn Router
BranchCache - Content Retrieval (Uses HTTP)
BranchCache - Hosted Cache Server (Uses HTTPS)
BranchCache - Peer Discovery (Uses WSD)
Cast to Device functionality
COM+ Network Access
COM+ Remote Administration
Core Networking
Delivery Optimization
DFS Management
DFS Replication
DHCP Server
DHCP Server Management
DIAL protocol server
Distributed Transaction Coordinator
DNS Service
File and Printer Sharing
File and Printer Sharing over SMBDirect
File Replication
File Server Remote Management

○



Predefined Rules

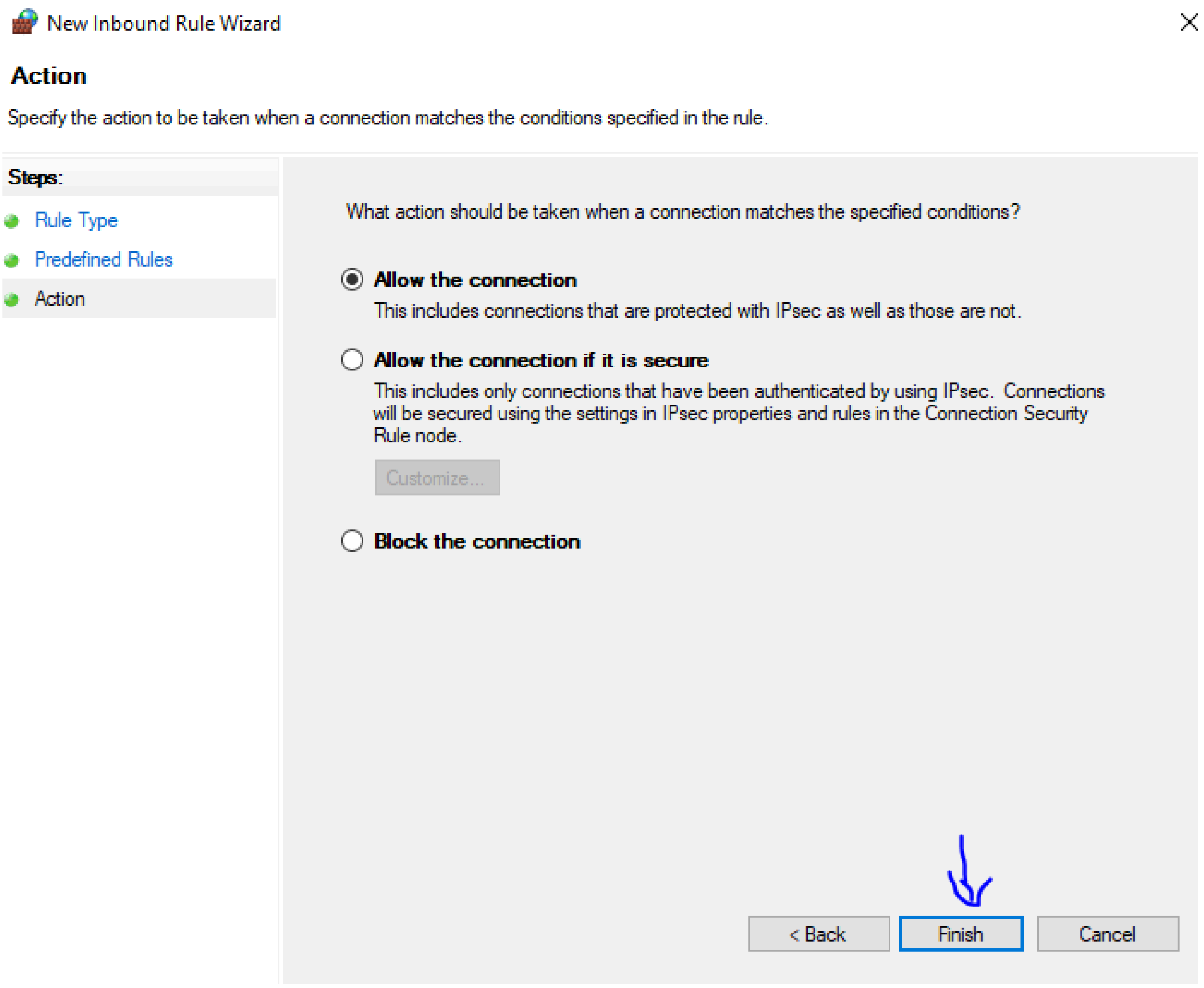
Select the rules to be created for this experience.

Which rules would you like to create?

The following rules define network connectivity requirements for the selected predefined group. Rules that are checked will be created. If a rule already exists and is checked, the contents of the existing rule will be overwritten.

Rules:

Name	Rule Exists	Profile	Desc
☑ File and Printer Sharing (LLMNR-UDP-In)	No	All	Inbou
☑ File and Printer Sharing (Echo Request - ICM...	No	All	Echo
☑ File and Printer Sharing (Echo Request - ICM...	No	All	Echo
☑ File and Printer Sharing (Spooler Service - RP...	No	All	Inbou
☑ File and Printer Sharing (Spooler Service - RPC)	No	All	Inbou
☑ File and Printer Sharing (NB-Datagram-In)	No	All	Inbou
☑ File and Printer Sharing (NB-Name-In)	No	All	Inbou
☑ File and Printer Sharing (SMB-In)	No	All	Inbou
☑ File and Printer Sharing (NB-Session-In)	No	All	Inbou



New Inbound Rule Wizard

Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

Steps:

- Rule Type
- Predefined Rules
- Action

What action should be taken when a connection matches the specified conditions?

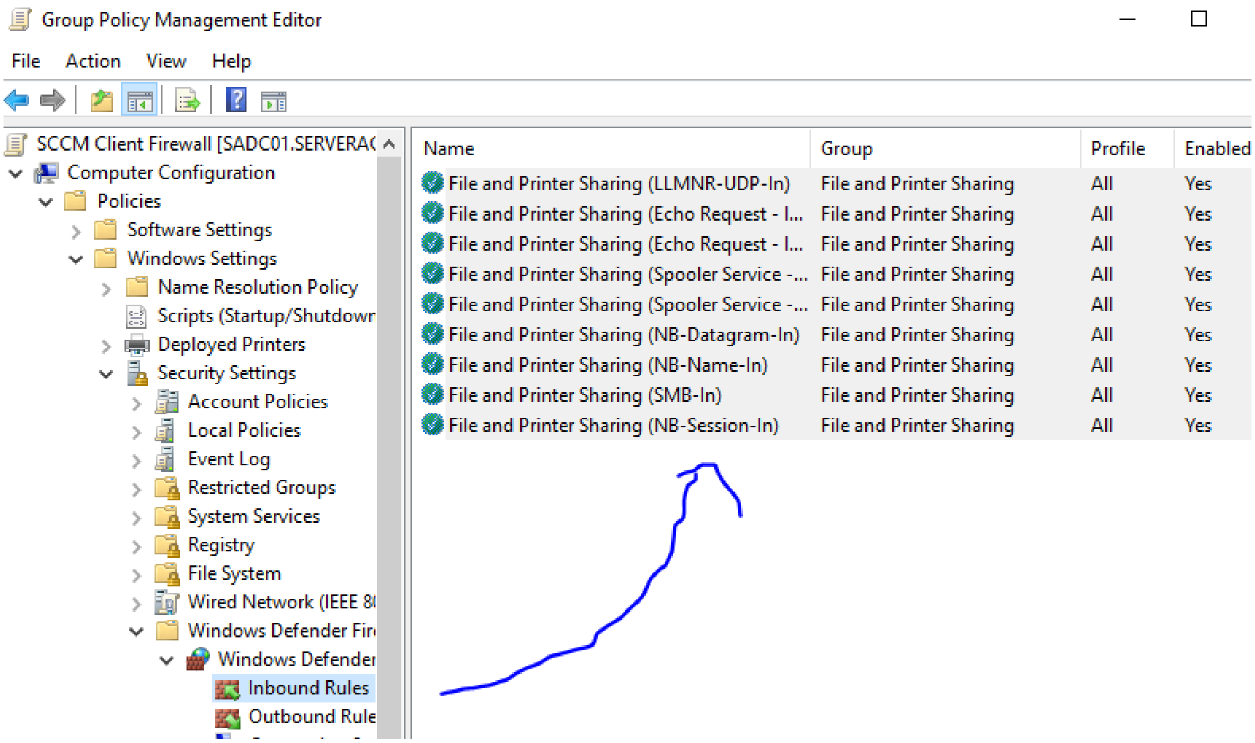
● **Allow the connection**

This includes connections that are protected with IPsec as well as those are not.

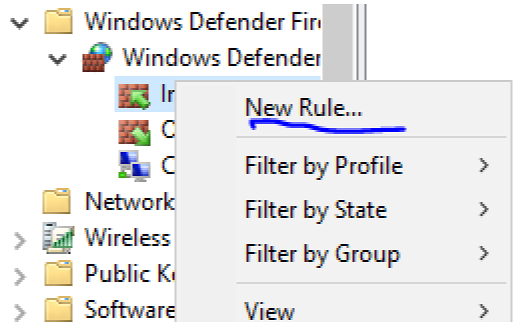
○ **Allow the connection if it is secure**

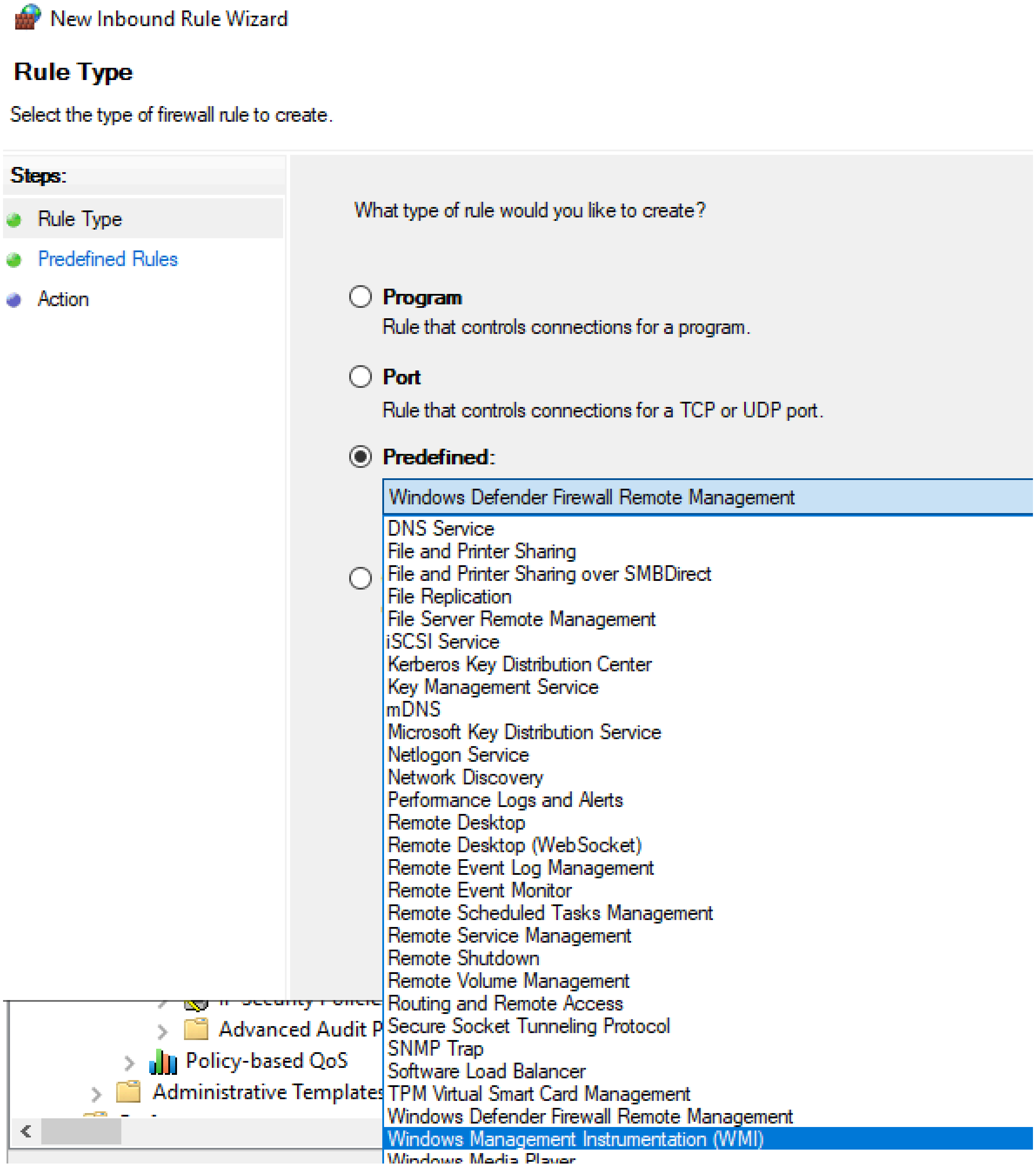
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

○ **Block the connection**



Name	Group	Profile	Enabled
File and Printer Sharing (LLMNR-UDP-In)	File and Printer Sharing	All	Yes
File and Printer Sharing (Echo Request - I...	File and Printer Sharing	All	Yes
File and Printer Sharing (Echo Request - I...	File and Printer Sharing	All	Yes
File and Printer Sharing (Spooler Service -...	File and Printer Sharing	All	Yes
File and Printer Sharing (Spooler Service -...	File and Printer Sharing	All	Yes
File and Printer Sharing (NB-Datagram-In)	File and Printer Sharing	All	Yes
File and Printer Sharing (NB-Name-In)	File and Printer Sharing	All	Yes
File and Printer Sharing (SMB-In)	File and Printer Sharing	All	Yes
File and Printer Sharing (NB-Session-In)	File and Printer Sharing	All	Yes





New Inbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

What type of rule would you like to create?

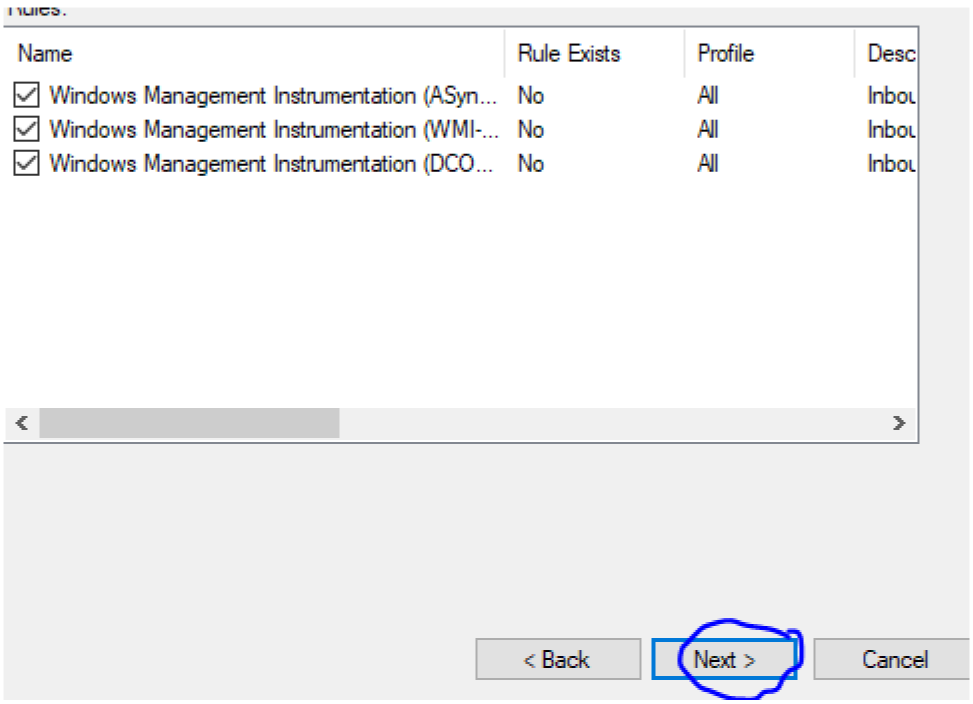
○ **Program**
Rule that controls connections for a program.

○ **Port**
Rule that controls connections for a TCP or UDP port.

● **Predefined:**

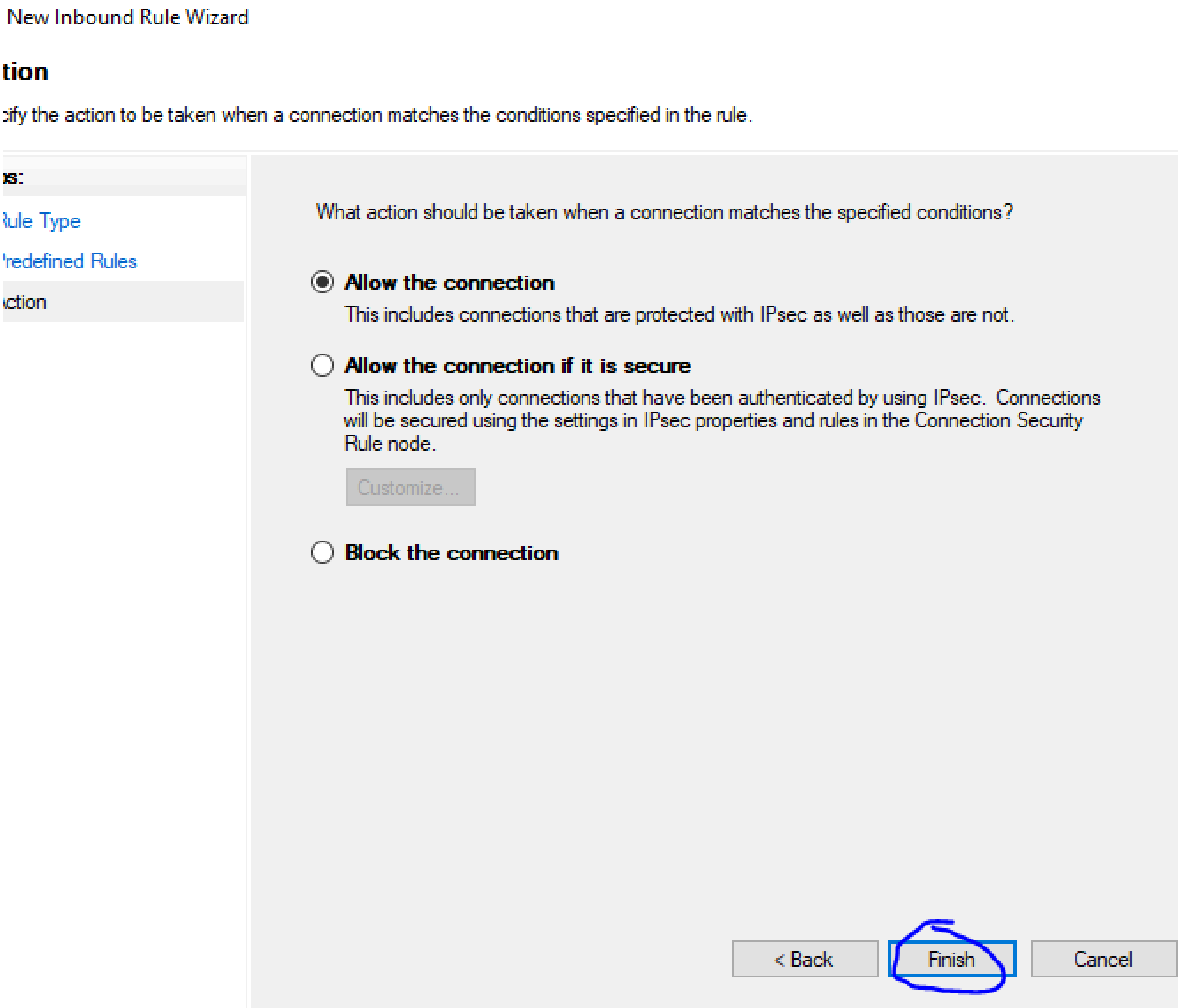
Windows Defender Firewall Remote Management

DNS Service
File and Printer Sharing
File and Printer Sharing over SMBDirect
File Replication
File Server Remote Management
iSCSI Service
Kerberos Key Distribution Center
Key Management Service
mDNS
Microsoft Key Distribution Service
Netlogon Service
Network Discovery
Performance Logs and Alerts
Remote Desktop
Remote Desktop (WebSocket)
Remote Event Log Management
Remote Event Monitor
Remote Scheduled Tasks Management
Remote Service Management
Remote Shutdown
Remote Volume Management
Routing and Remote Access
Secure Socket Tunneling Protocol
SNMP Trap
Software Load Balancer
TPM Virtual Smart Card Management
Windows Defender Firewall Remote Management
Windows Management Instrumentation (WMI)
Windows Media Player



Rules:

Name	Rule Exists	Profile	Desc
☑ Windows Management Instrumentation (ASyn...	No	All	Inbou
☑ Windows Management Instrumentation (WMI-...	No	All	Inbou
☑ Windows Management Instrumentation (DCO...	No	All	Inbou



New Inbound Rule Wizard

tion

:ify the action to be taken when a connection matches the conditions specified in the rule.

What action should be taken when a connection matches the specified conditions?

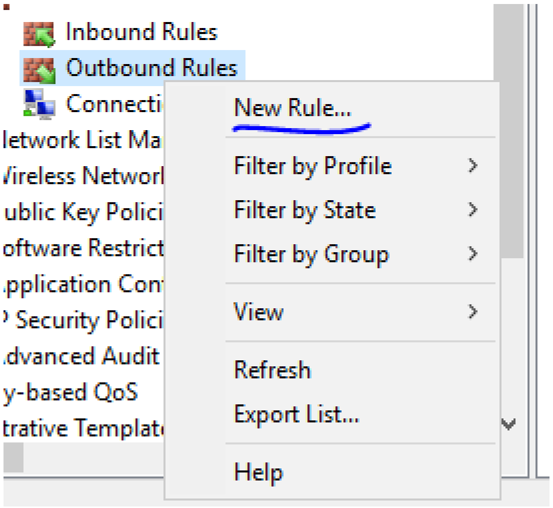
● **Allow the connection**

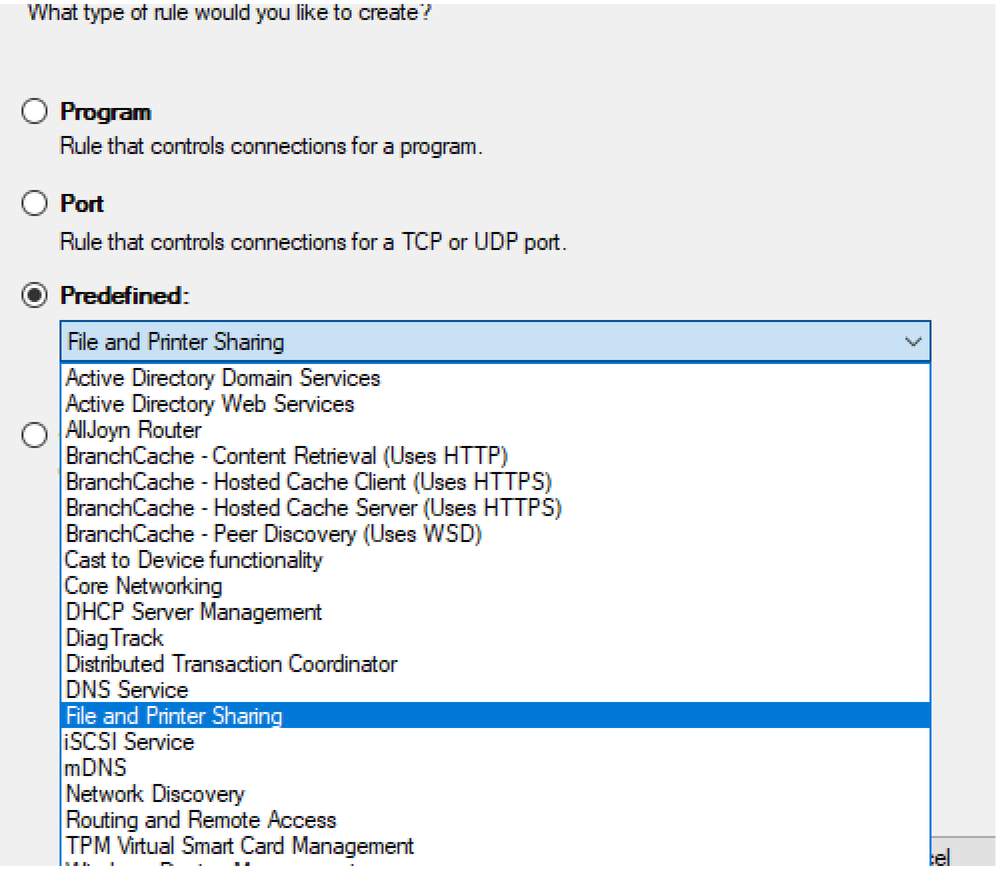
This includes connections that are protected with IPsec as well as those are not.

○ **Allow the connection if it is secure**

This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

○ **Block the connection**





What type of rule would you like to create?

○ **Program**

Rule that controls connections for a program.

○ **Port**

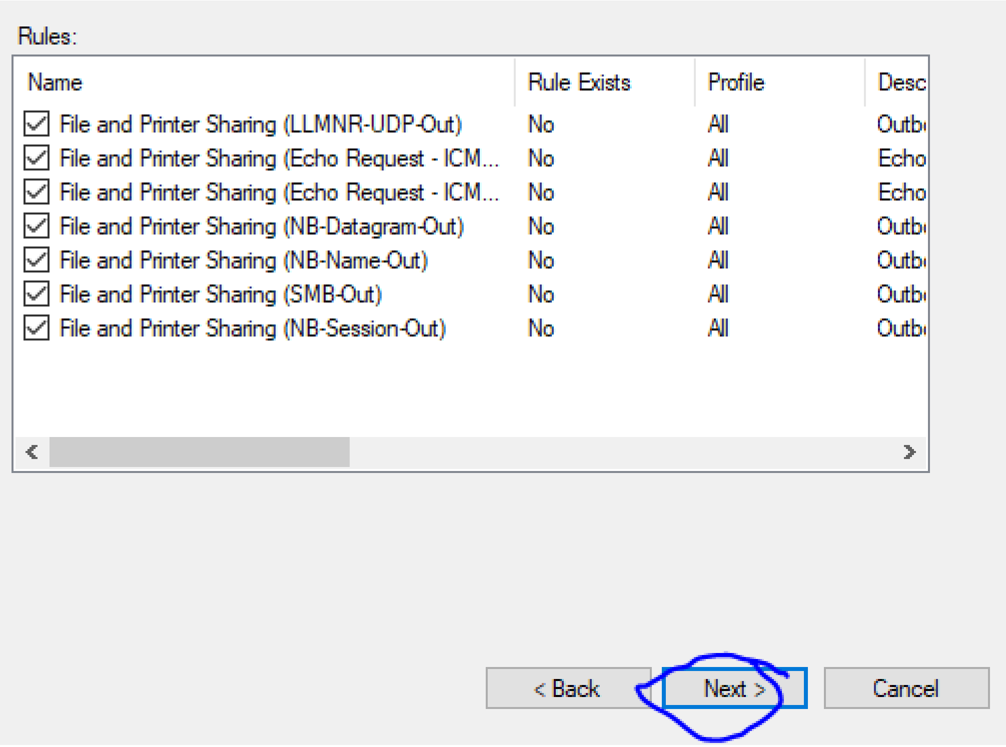
Rule that controls connections for a TCP or UDP port.

● **Predefined:**

File and Printer Sharing

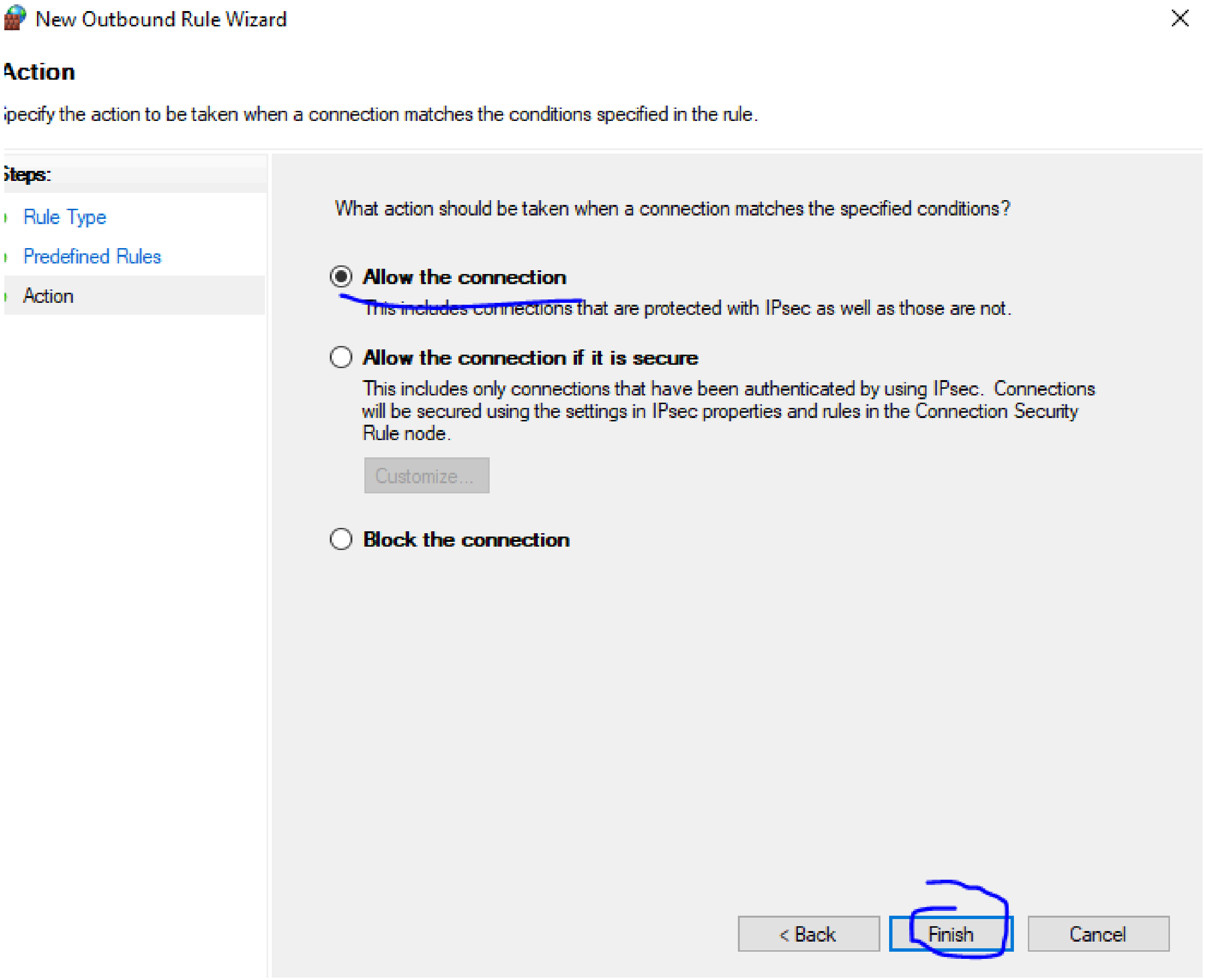
Active Directory Domain Services
Active Directory Web Services
AllJoyn Router
BranchCache - Content Retrieval (Uses HTTP)
BranchCache - Hosted Cache Client (Uses HTTPS)
BranchCache - Hosted Cache Server (Uses HTTPS)
BranchCache - Peer Discovery (Uses WSD)
Cast to Device functionality
Core Networking
DHCP Server Management
Diag Track
Distributed Transaction Coordinator
DNS Service
File and Printer Sharing
iSCSI Service
mDNS
Network Discovery
Routing and Remote Access
TPM Virtual Smart Card Management

○



Rules:

	Name	Rule Exists	Profile	Desc
☑	File and Printer Sharing (LLMNR-UDP-Out)	No	All	Outb
☑	File and Printer Sharing (Echo Request - ICM...	No	All	Echo
☑	File and Printer Sharing (Echo Request - ICM...	No	All	Echo
☑	File and Printer Sharing (NB-Datagram-Out)	No	All	Outb
☑	File and Printer Sharing (NB-Name-Out)	No	All	Outb
☑	File and Printer Sharing (SMB-Out)	No	All	Outb
☑	File and Printer Sharing (NB-Session-Out)	No	All	Outb



New Outbound Rule Wizard

Action

ꞏpecify the action to be taken when a connection matches the conditions specified in the rule.

ꞏteps:

- Rule Type
- Predefined Rules
- Action

What action should be taken when a connection matches the specified conditions?

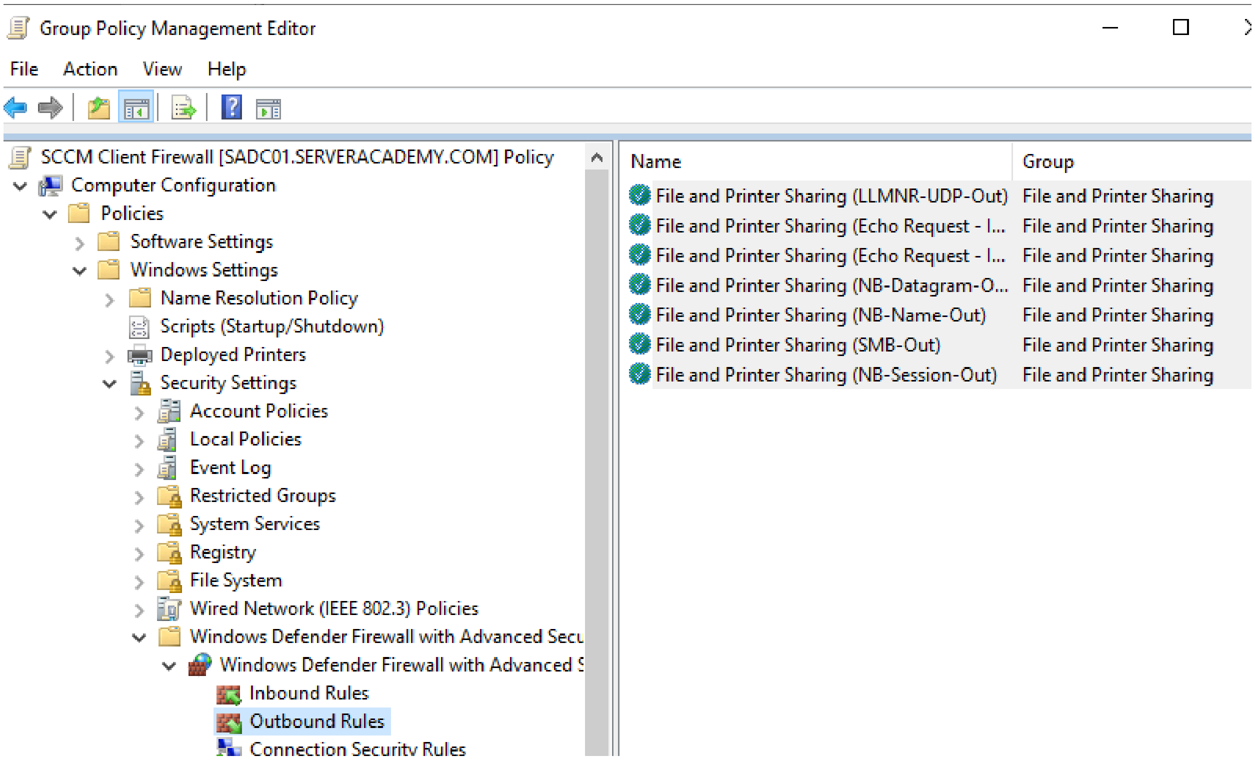
● **Allow the connection**

This includes connections that are protected with IPsec as well as those are not.

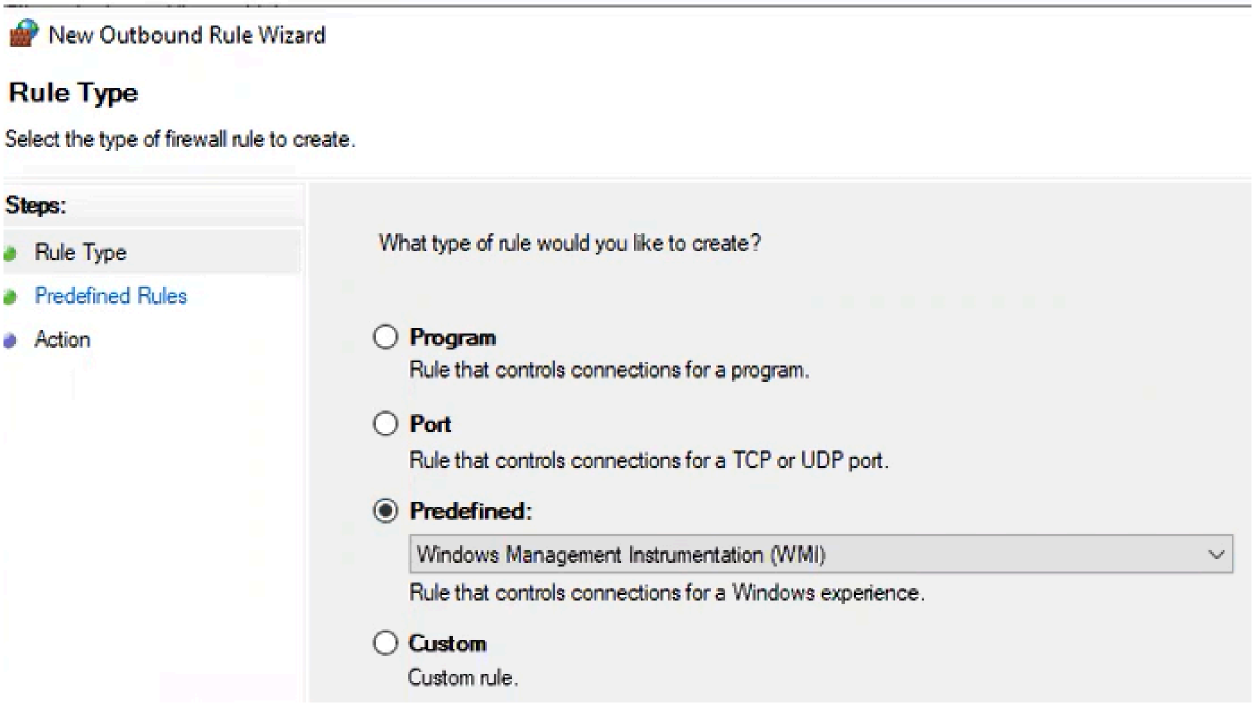
○ **Allow the connection if it is secure**

This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

○ **Block the connection**


Group Policy Management Editor
File
Action
View
Help
SCCM Client Firewall [SADC01.SERVERACADEMY.COM] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Defender Firewall with Advanced Secu
Windows Defender Firewall with Advanced S
Inbound Rules
Outbound Rules
Connection Security Rules

Name	Group
File and Printer Sharing (LLMNR-UDP-Out)	File and Printer Sharing
File and Printer Sharing (Echo Request - I...	File and Printer Sharing
File and Printer Sharing (Echo Request - I...	File and Printer Sharing
File and Printer Sharing (NB-Datagram-O...	File and Printer Sharing
File and Printer Sharing (NB-Name-Out)	File and Printer Sharing
File and Printer Sharing (SMB-Out)	File and Printer Sharing
File and Printer Sharing (NB-Session-Out)	File and Printer Sharing



Rule Type

Select the type of firewall rule to create.

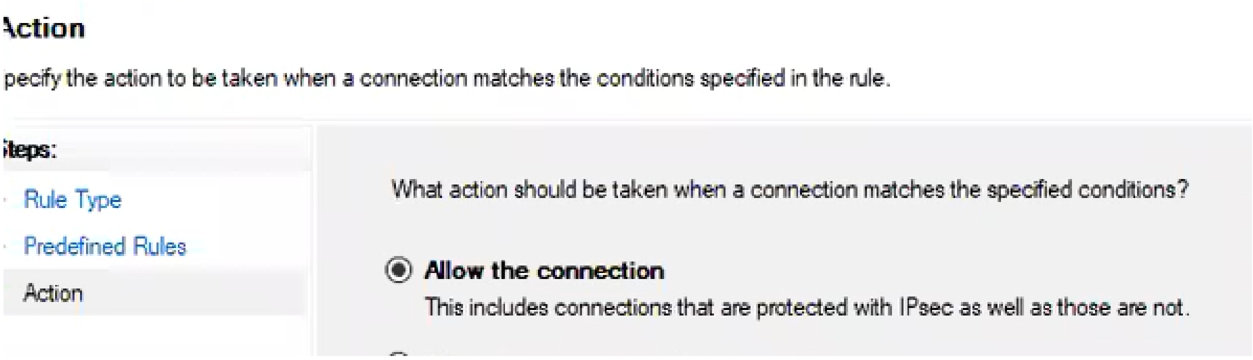
What type of rule would you like to create?

○ **Program**
Rule that controls connections for a program.

○ **Port**
Rule that controls connections for a TCP or UDP port.

● **Predefined:**
Windows Management Instrumentation (WMI)
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.



\ction

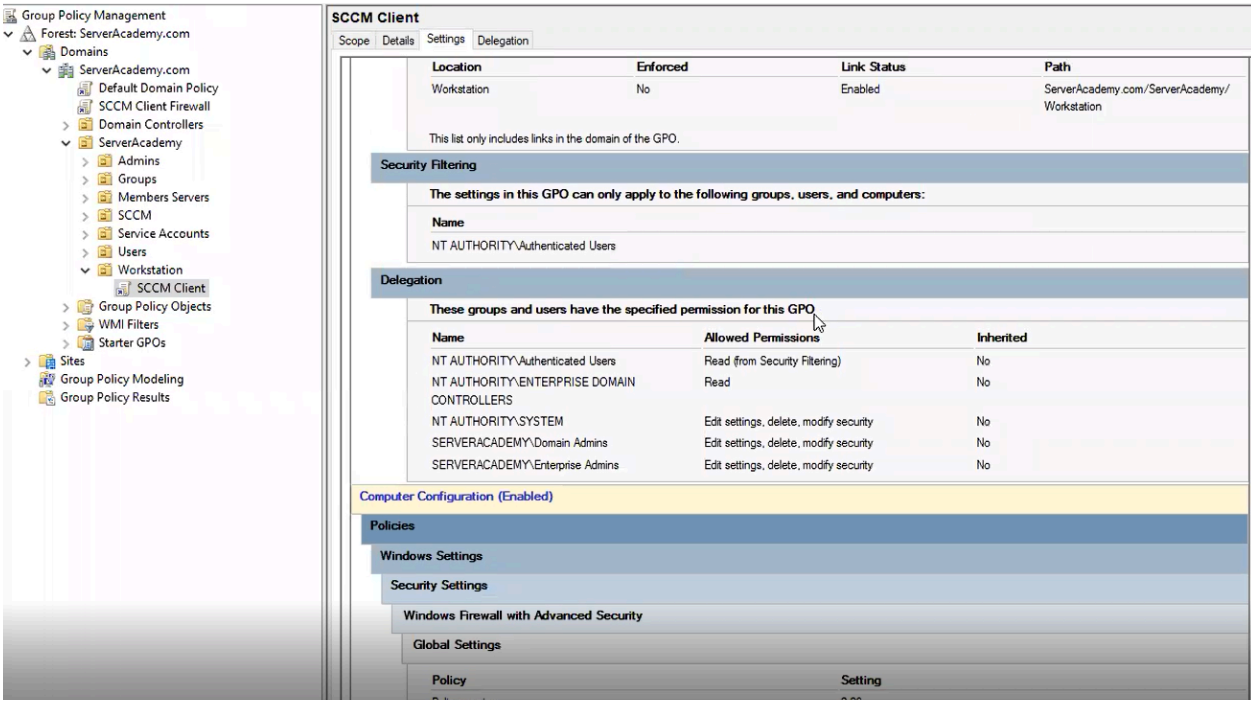
pecify the action to be taken when a connection matches the conditions specified in the rule.

What action should be taken when a connection matches the specified conditions?

● Allow the connection

This includes connections that are protected with IPsec as well as those are not.

SCCM Client Group Policy Settings



Location	Enforced	Link Status	Path
Workstation	No	Enabled	ServerAcademy.com/ServerAcademy/ Workstation

This list only includes links in the domain of the GPO.

Security Filtering

The settings in this GPO can only apply to the following groups, users, and computers:

Name
NT AUTHORITY\Authenticated Users

Delegation

These groups and users have the specified permission for this GPO

Name	Allowed Permissions	Inherited
NT AUTHORITY\Authenticated Users	Read (from Security Filtering)	No
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Read	No
NT AUTHORITY\SYSTEM	Edit settings, delete, modify security	No
SERVERACADEMY\Domain Admins	Edit settings, delete, modify security	No
SERVERACADEMY\Enterprise Admins	Edit settings, delete, modify security	No

Computer Configuration (Enabled)

Policies

Windows Settings

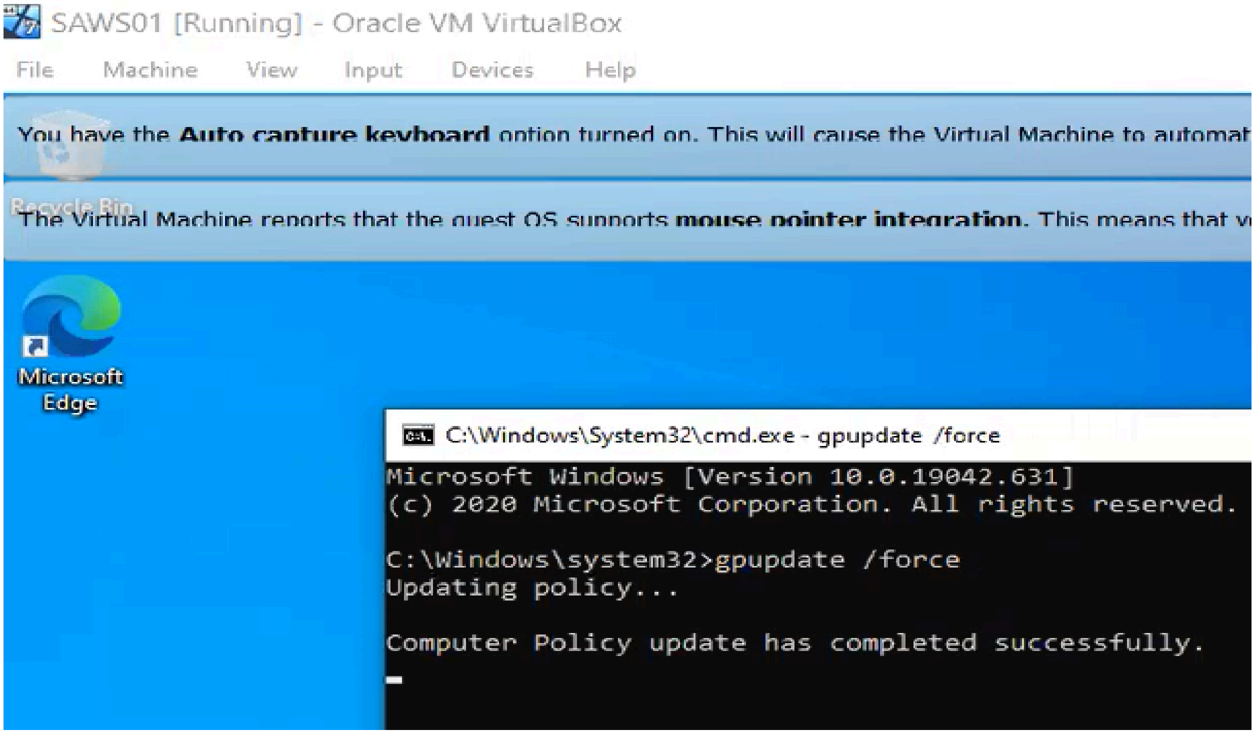
Security Settings

Windows Firewall with Advanced Security

Global Settings

Policy	Setting

Running gpupdate /force to update client



SAWS01 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Microsoft Edge
Recycle Bin

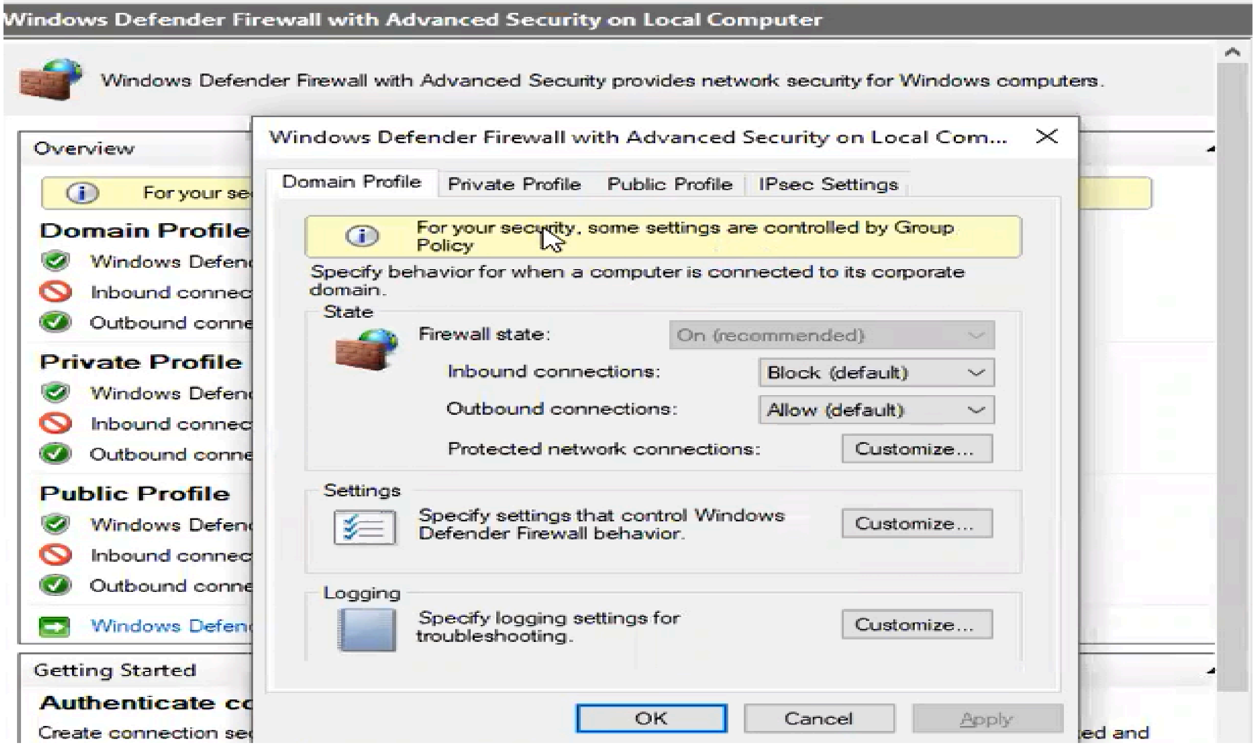
You have the **Auto capture keyboard** option turned on. This will cause the Virtual Machine to automat

The Virtual Machine reports that the guest OS supports **mouse pointer integration**. This means that v

C:\Windows\System32\cmd.exe - gpupdate /force

```
Microsoft Windows [Version 10.0.19042.631]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Windows\system32>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
```

Checking Firewall Changes on Client Machine



Windows Defender Firewall with Advanced Security on Local Computer

Windows Defender Firewall with Advanced Security provides network security for Windows computers.

Windows Defender Firewall with Advanced Security on Local Com...

For your security, some settings are controlled by Group Policy

Specify behavior for when a computer is connected to its corporate domain.

State

Firewall state: On (recommended)

Inbound connections: Block (default)

Outbound connections: Allow (default)

Protected network connections: Customize...

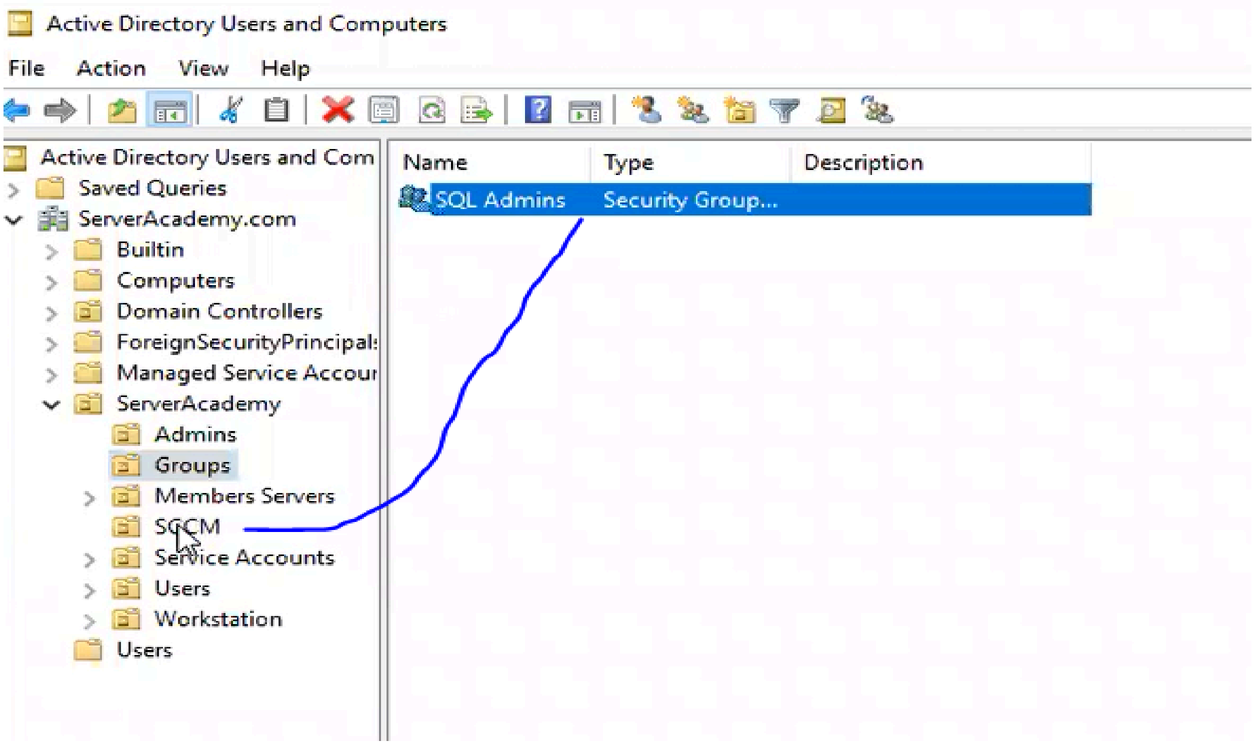
Settings

Specify settings that control Windows Defender Firewall behavior. Customize...

Logging

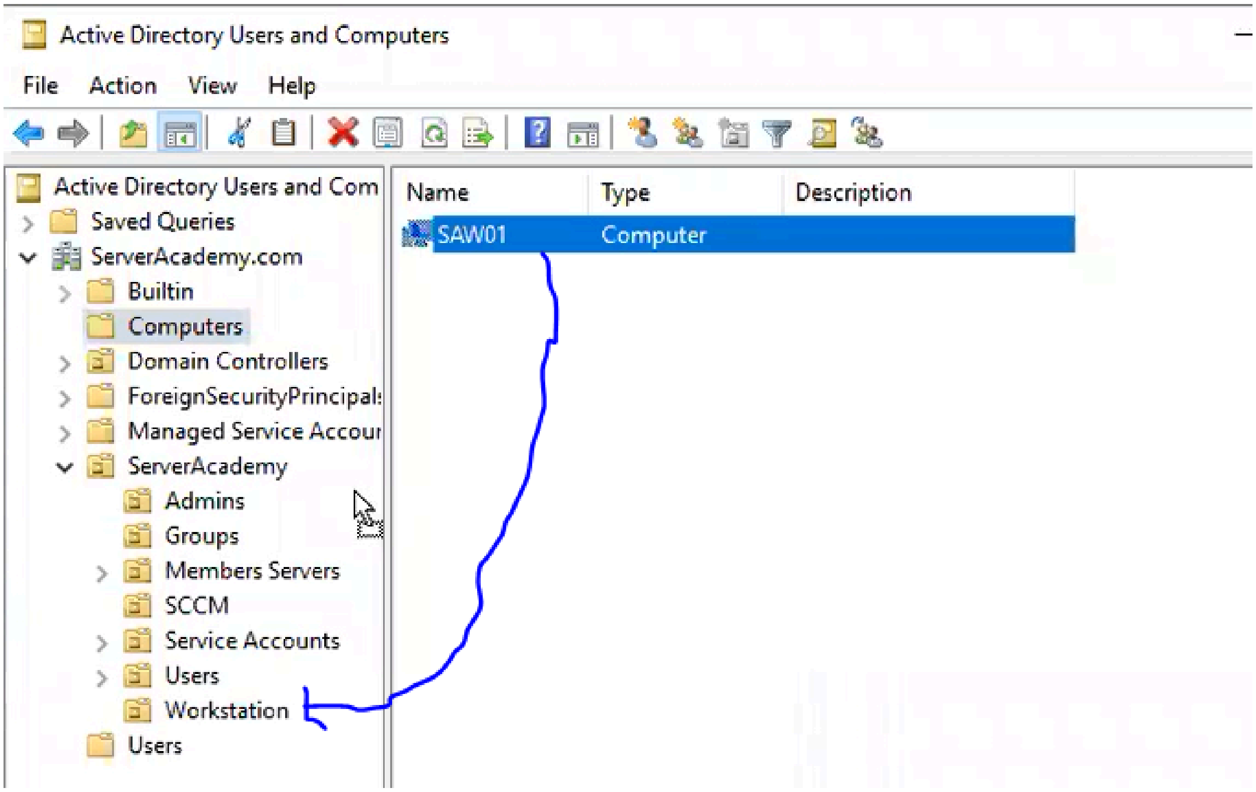
Specify logging settings for troubleshooting. Customize...

Moving SQL Admins to SCCM OU



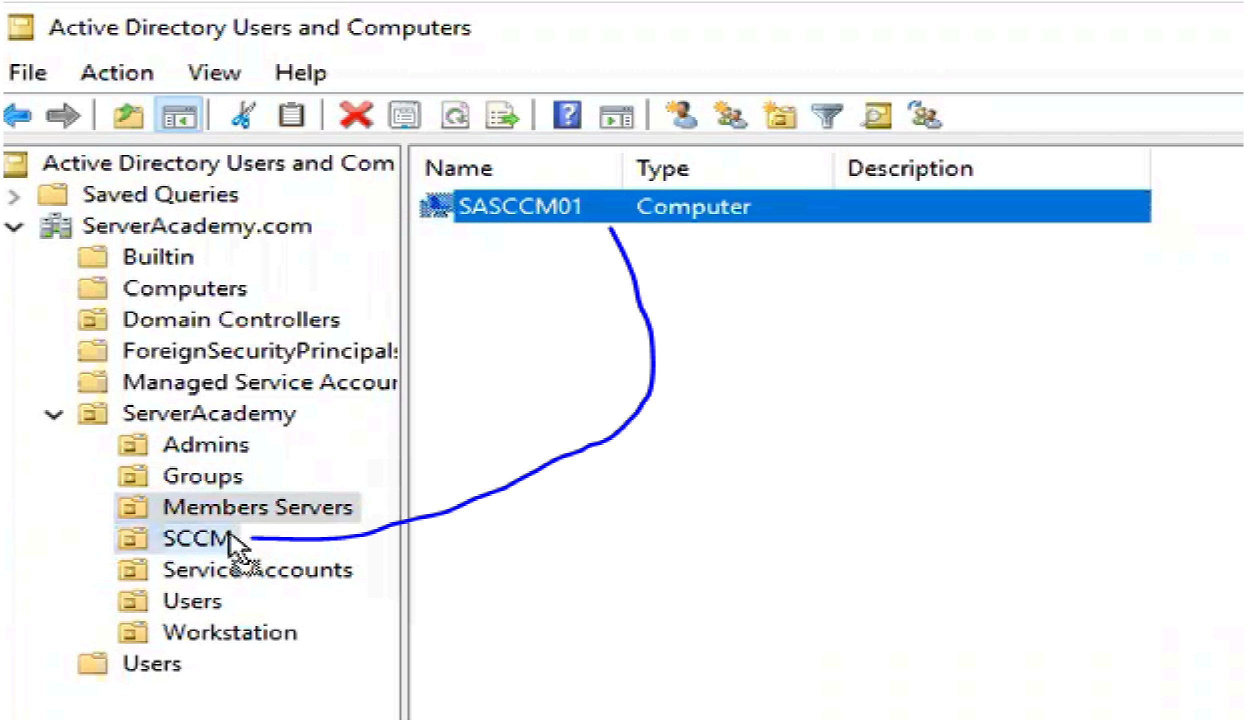
Name	Type	Description
SQL Admins	Security Group...	

Moving SAW01 Client to Workstation OU



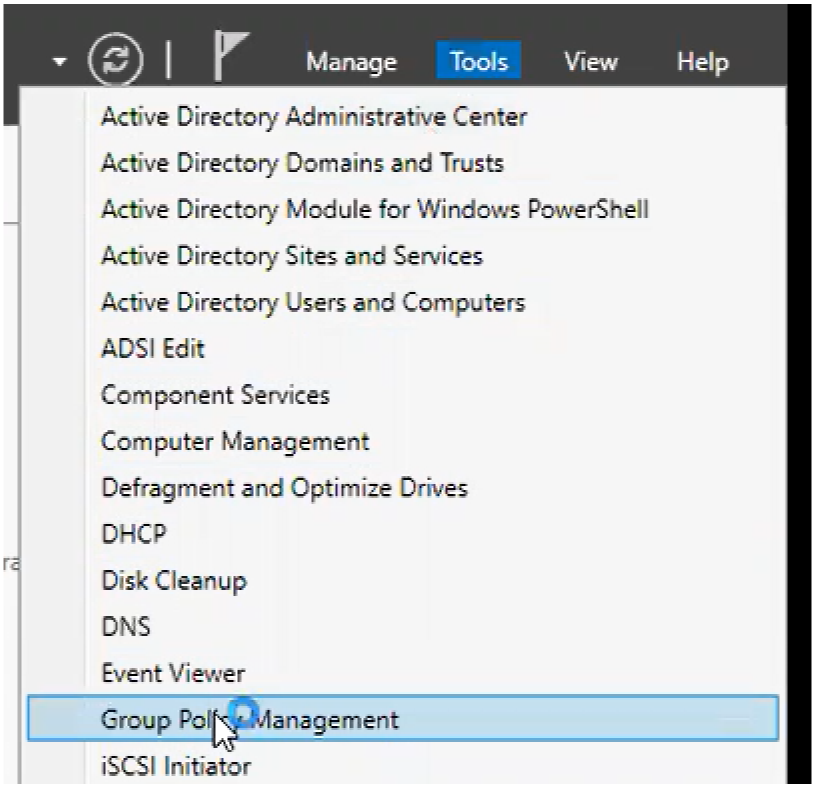
Name	Type	Description
SAW01	Computer	

Moving SASCCM01 Server to SCCM OU

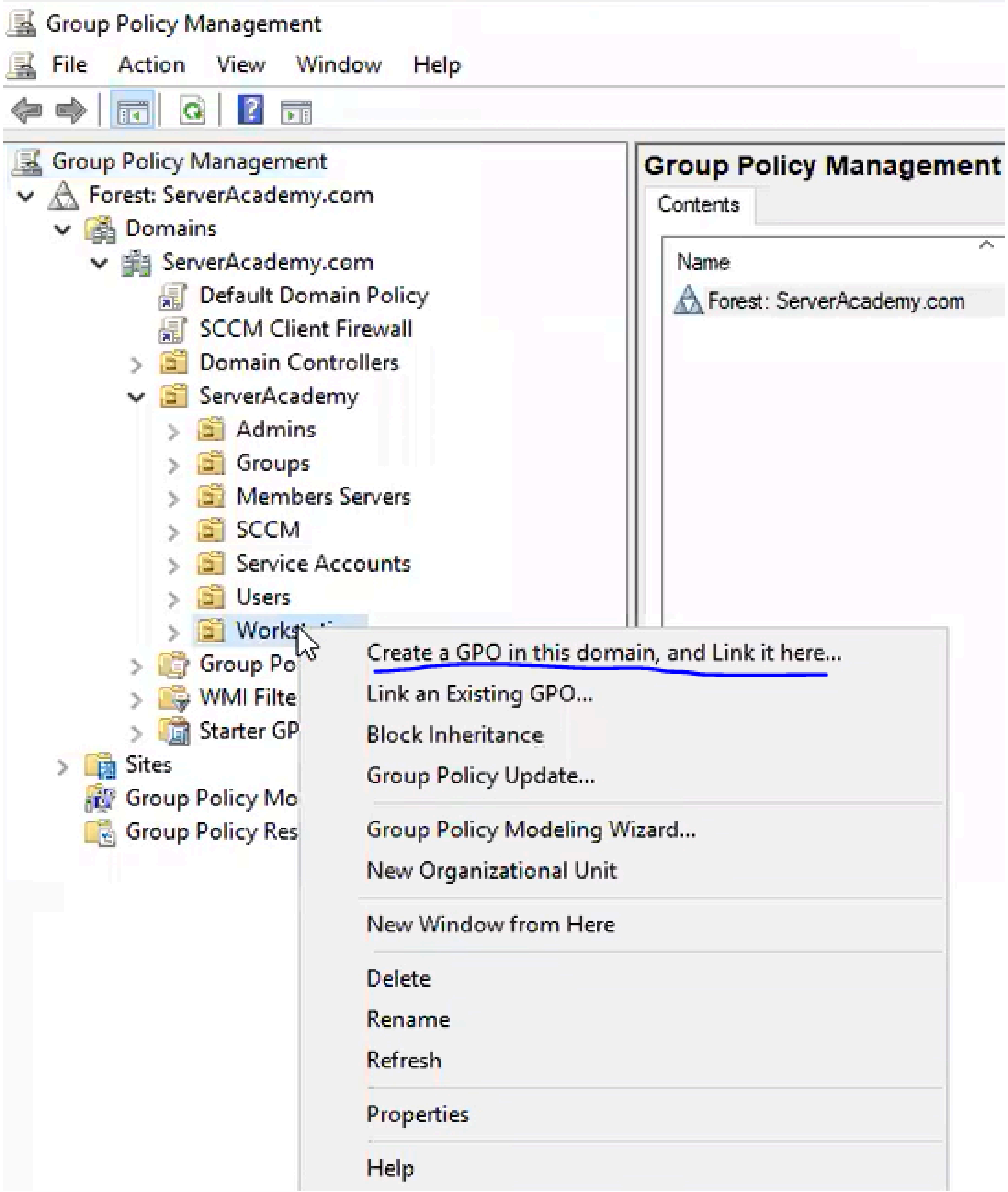


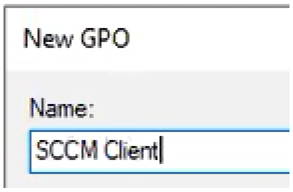
Name	Type	Description
SASCCM01	Computer	

Group Policy Management

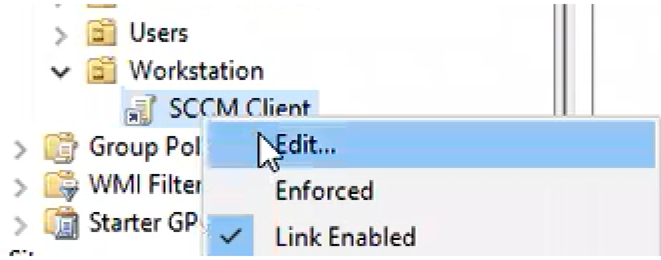

Manage
Tools
View
Help
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit
Component Services
Computer Management
Defragment and Optimize Drives
DHCP
Disk Cleanup
DNS
Event Viewer
Group Policy Management
iSCSI Initiator

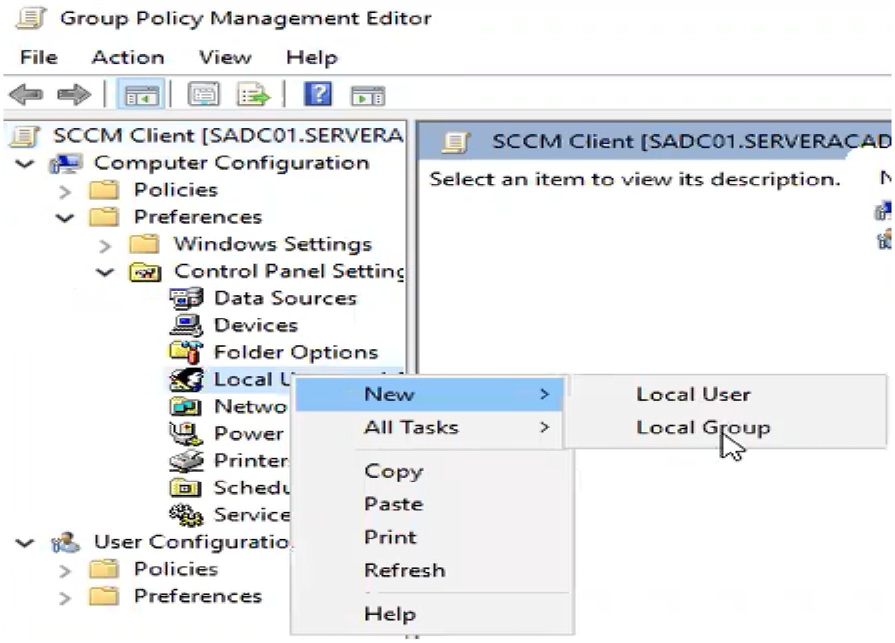
Creating a Group Policy Object for Workstations

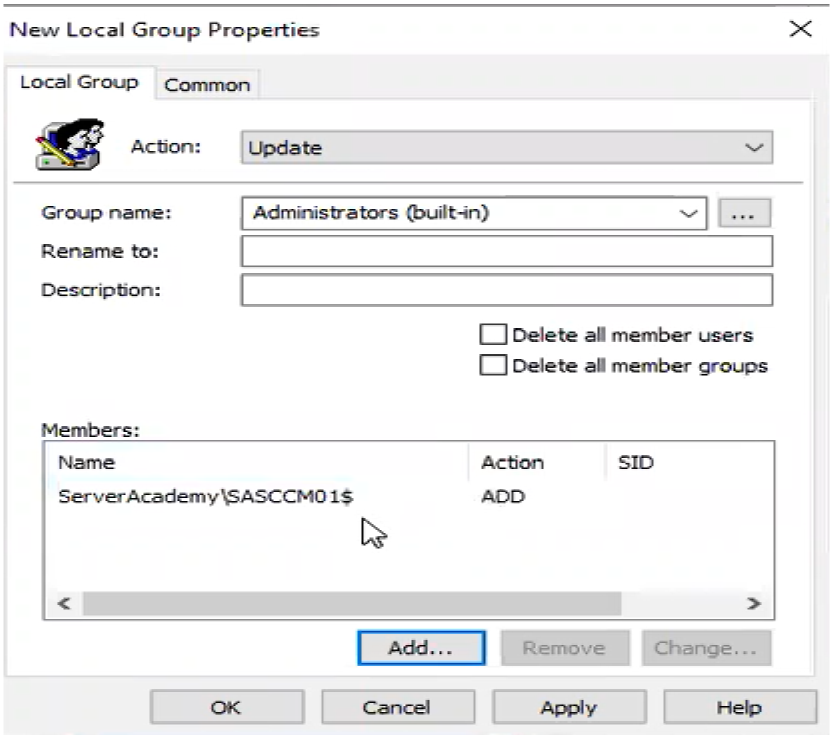




Name: SCCM Client







Action: Update

Group name: Administrators (built-in)

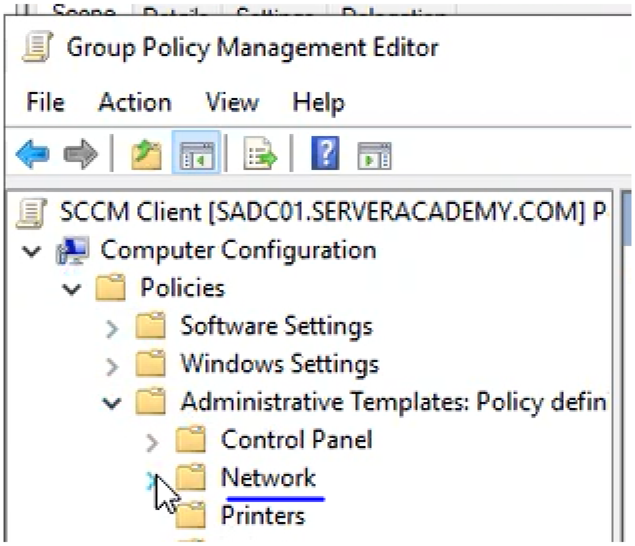
Rename to:

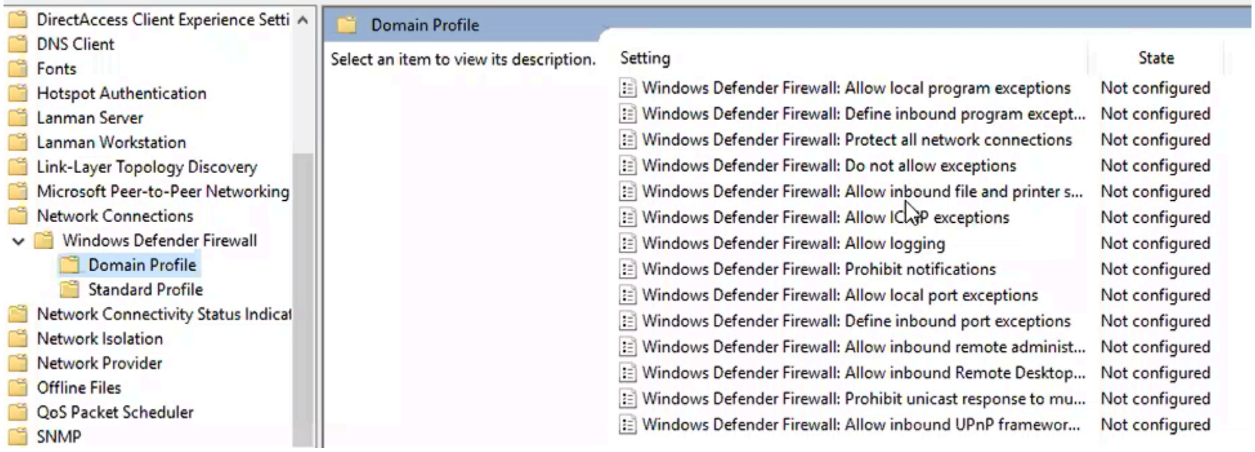
Description:

□ Delete all member users
□ Delete all member groups

Members:

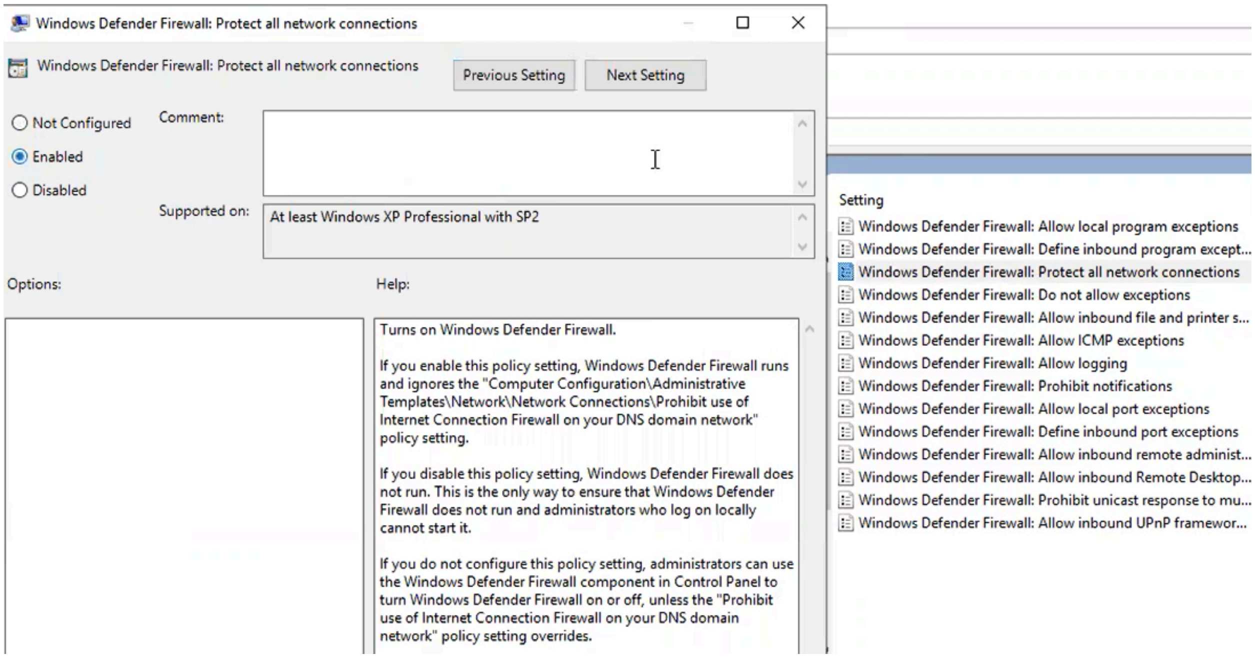
Name	Action	SID
ServerAcademy\SASCCM01$	ADD	


Scope Details Settings Delegation
Group Policy Management Editor
File Action View Help
SCCM Client [SADC01.SERVERACADEMY.COM] P
Computer Configuration
Policies
Software Settings
Windows Settings
Administrative Templates: Policy defin
Control Panel
Network
Printers



Select an item to view its description.

Setting	State
Windows Defender Firewall: Allow local program exceptions	Not configured
Windows Defender Firewall: Define inbound program except...	Not configured
Windows Defender Firewall: Protect all network connections	Not configured
Windows Defender Firewall: Do not allow exceptions	Not configured
Windows Defender Firewall: Allow inbound file and printer s...	Not configured
Windows Defender Firewall: Allow ICMP exceptions	Not configured
Windows Defender Firewall: Allow logging	Not configured
Windows Defender Firewall: Prohibit notifications	Not configured
Windows Defender Firewall: Allow local port exceptions	Not configured
Windows Defender Firewall: Define inbound port exceptions	Not configured
Windows Defender Firewall: Allow inbound remote administ...	Not configured
Windows Defender Firewall: Allow inbound Remote Desktop...	Not configured
Windows Defender Firewall: Prohibit unicast response to mu...	Not configured
Windows Defender Firewall: Allow inbound UPnP framewor...	Not configured


Windows Defender Firewall: Protect all network connections
Windows Defender Firewall: Protect all network connections
Previous Setting
Next Setting

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows XP Professional with SP2

Options:

Help:

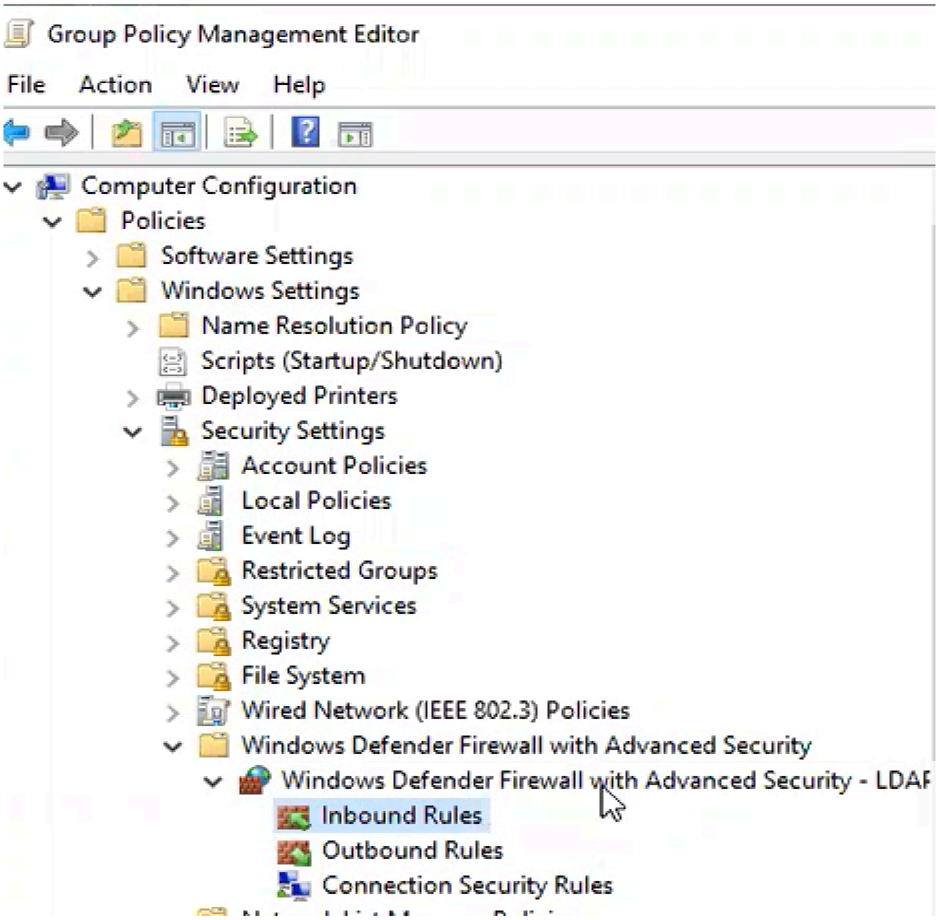
Turns on Windows Defender Firewall.

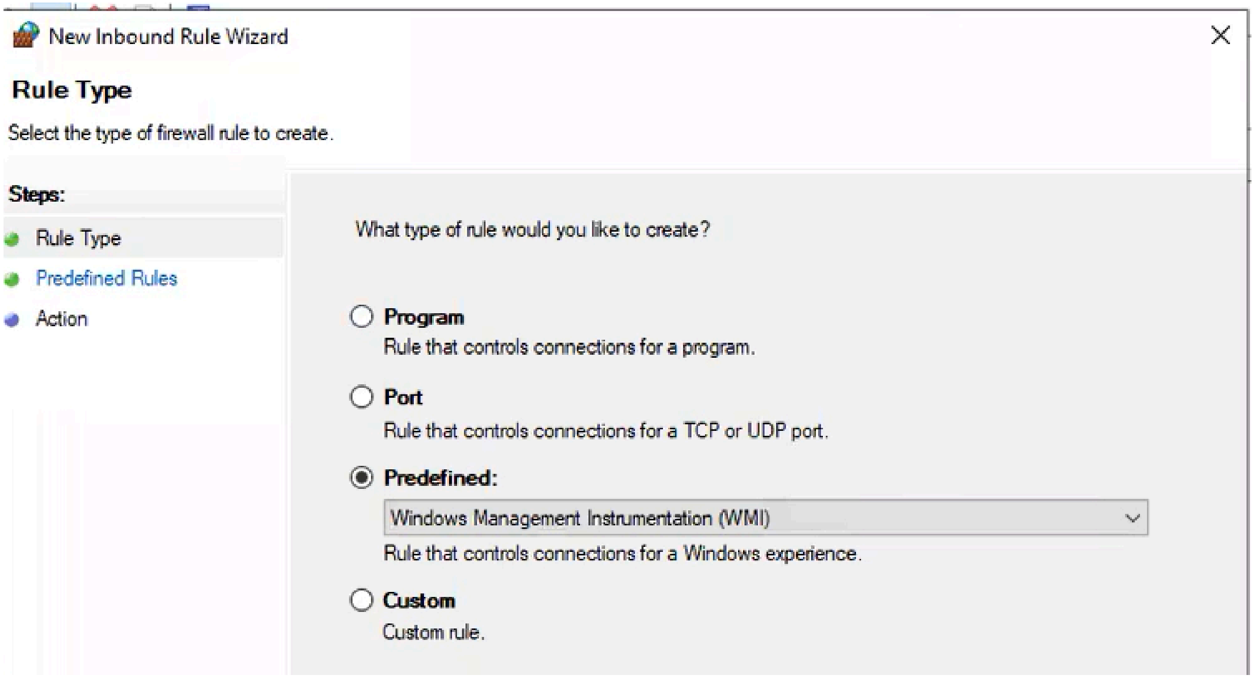
If you enable this policy setting, Windows Defender Firewall runs and ignores the "Computer Configuration\Administrative Templates\Network\Network Connections\Prohibit use of Internet Connection Firewall on your DNS domain network" policy setting.

If you disable this policy setting, Windows Defender Firewall does not run. This is the only way to ensure that Windows Defender Firewall does not run and administrators who log on locally cannot start it.

If you do not configure this policy setting, administrators can use the Windows Defender Firewall component in Control Panel to turn Windows Defender Firewall on or off, unless the "Prohibit use of Internet Connection Firewall on your DNS domain network" policy setting overrides.

Setting
Windows Defender Firewall: Allow local program exceptions
Windows Defender Firewall: Define inbound program except...
Windows Defender Firewall: Protect all network connections
Windows Defender Firewall: Do not allow exceptions
Windows Defender Firewall: Allow inbound file and printer s...
Windows Defender Firewall: Allow ICMP exceptions
Windows Defender Firewall: Allow logging
Windows Defender Firewall: Prohibit notifications
Windows Defender Firewall: Allow local port exceptions
Windows Defender Firewall: Define inbound port exceptions
Windows Defender Firewall: Allow inbound remote administ...
Windows Defender Firewall: Allow inbound Remote Desktop...
Windows Defender Firewall: Prohibit unicast response to mu...
Windows Defender Firewall: Allow inbound UPnP framewor...





New Inbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

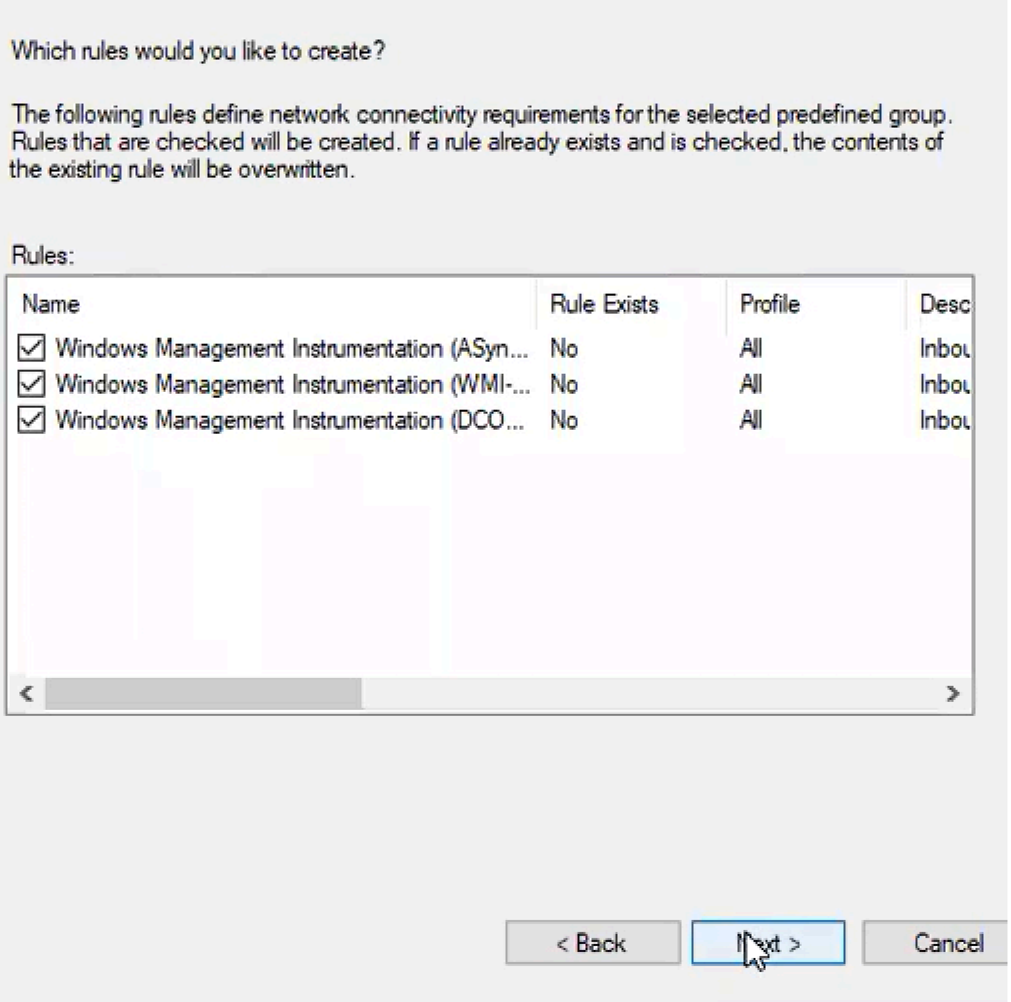
What type of rule would you like to create?

○ **Program**
Rule that controls connections for a program.

○ **Port**
Rule that controls connections for a TCP or UDP port.

● **Predefined:**
Windows Management Instrumentation (WMI)
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.

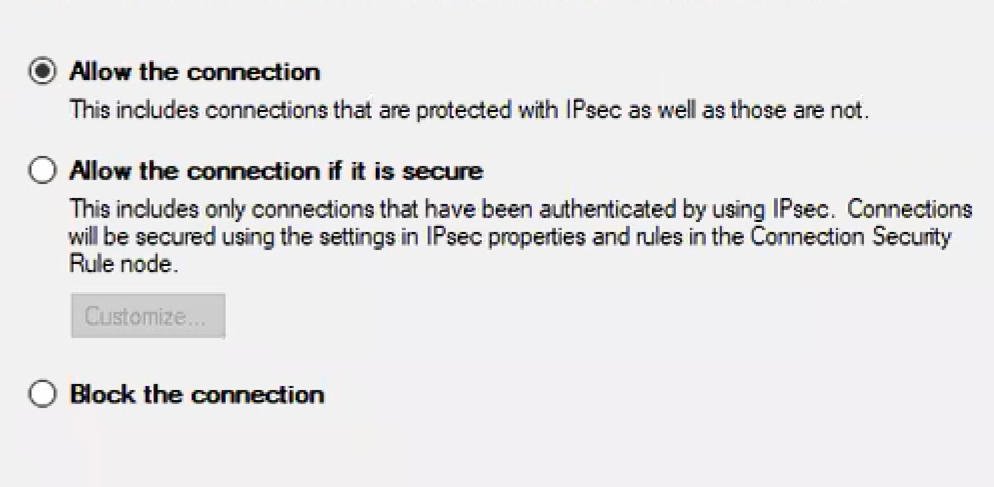


Which rules would you like to create?

The following rules define network connectivity requirements for the selected predefined group. Rules that are checked will be created. If a rule already exists and is checked, the contents of the existing rule will be overwritten.

Rules:

Name	Rule Exists	Profile	Desc
☑ Windows Management Instrumentation (ASyn...	No	All	Inbou
☑ Windows Management Instrumentation (WMI-...	No	All	Inbou
☑ Windows Management Instrumentation (DCO...	No	All	Inbou



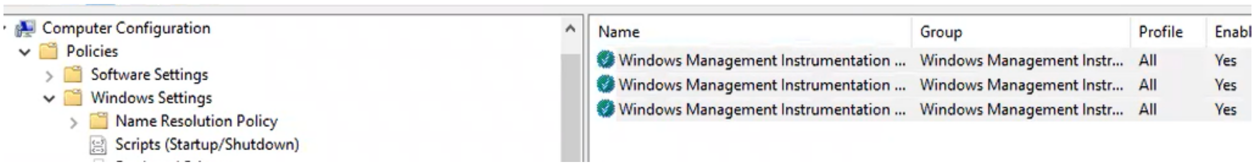
● **Allow the connection**

This includes connections that are protected with IPsec as well as those are not.

○ **Allow the connection if it is secure**

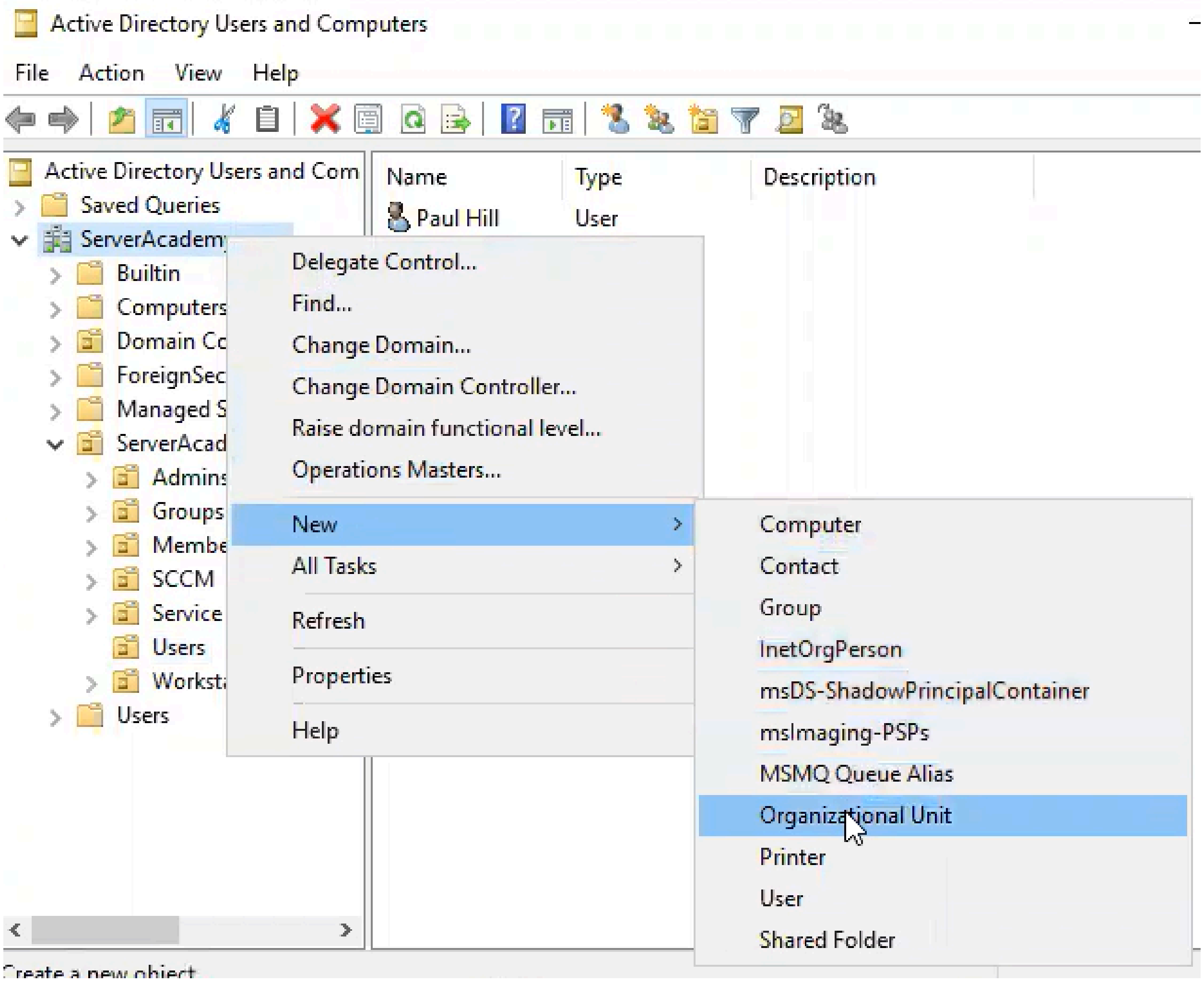
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

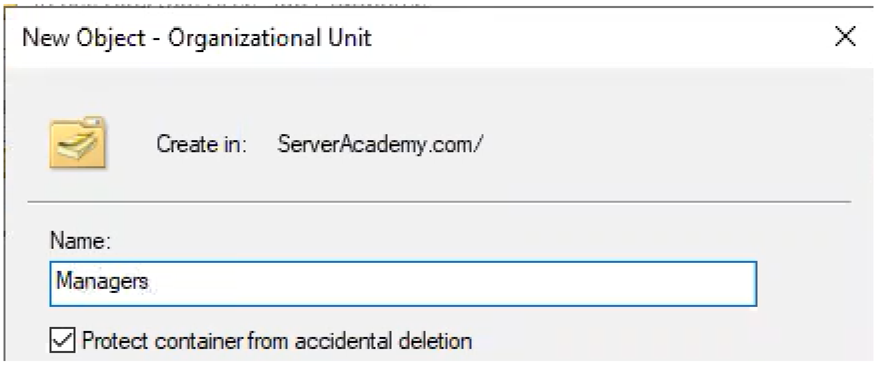
○ **Block the connection**



Name	Group	Profile	Enabl
Windows Management Instrumentation ...	Windows Management Instr...	All	Yes
Windows Management Instrumentation ...	Windows Management Instr...	All	Yes
Windows Management Instrumentation ...	Windows Management Instr...	All	Yes

Creating a Managers OU

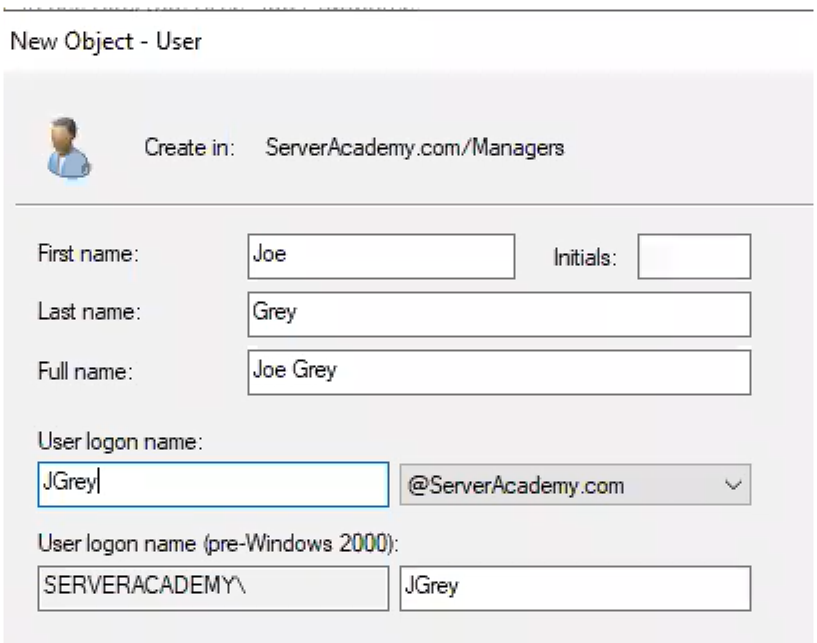




Create in: ServerAcademy.com/

Name: Managers

☑ Protect container from accidental deletion



New Object - User

Create in: ServerAcademy.com/Managers

First name: Joe

Initials:

Last name: Grey

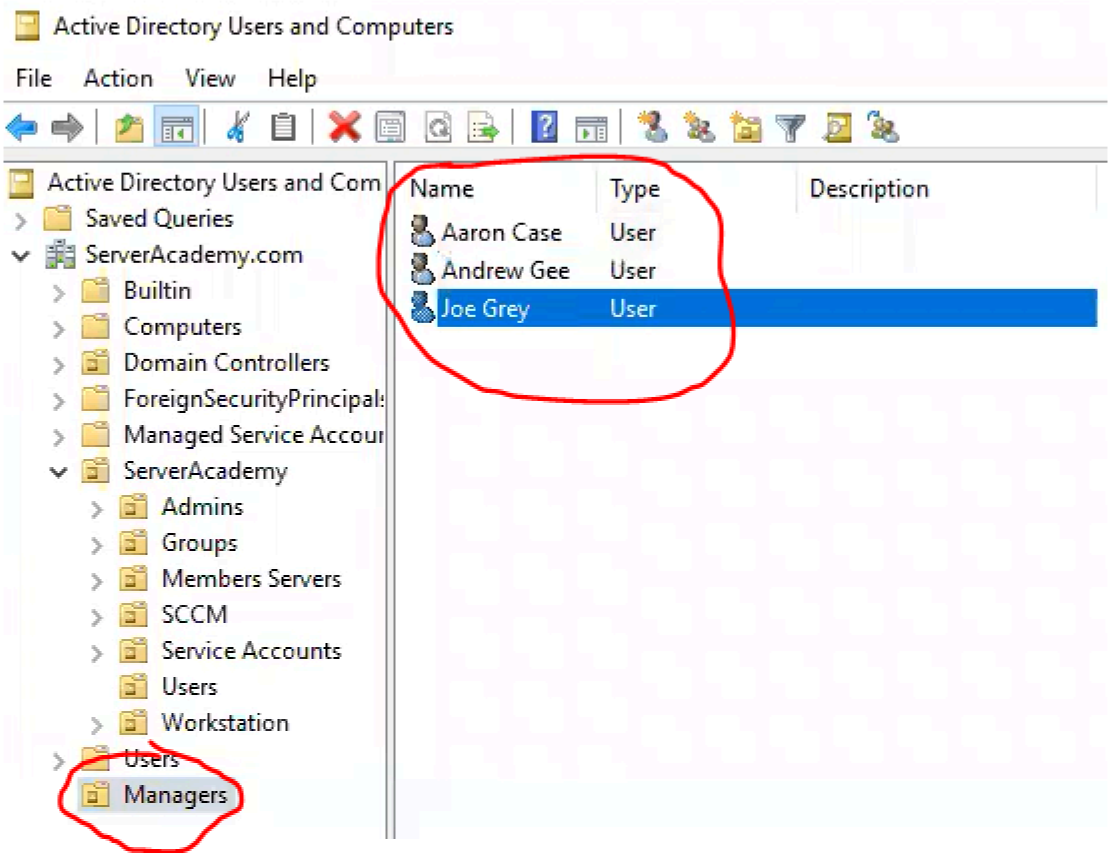
Full name: Joe Grey

User logon name:

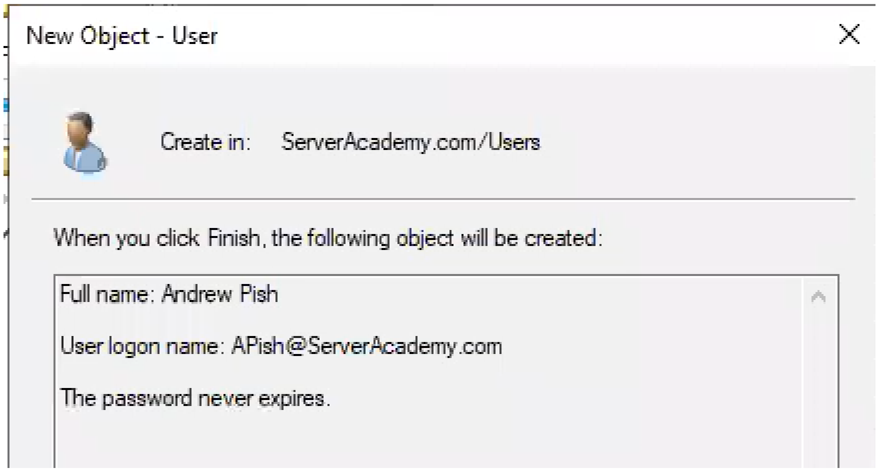
JGrey @ServerAcademy.com

User logon name (pre-Windows 2000):

SERVERACADEMY\ JGrey



Name	Type	Description
Aaron Case	User	
Andrew Gee	User	
Joe Grey	User	



New Object - User

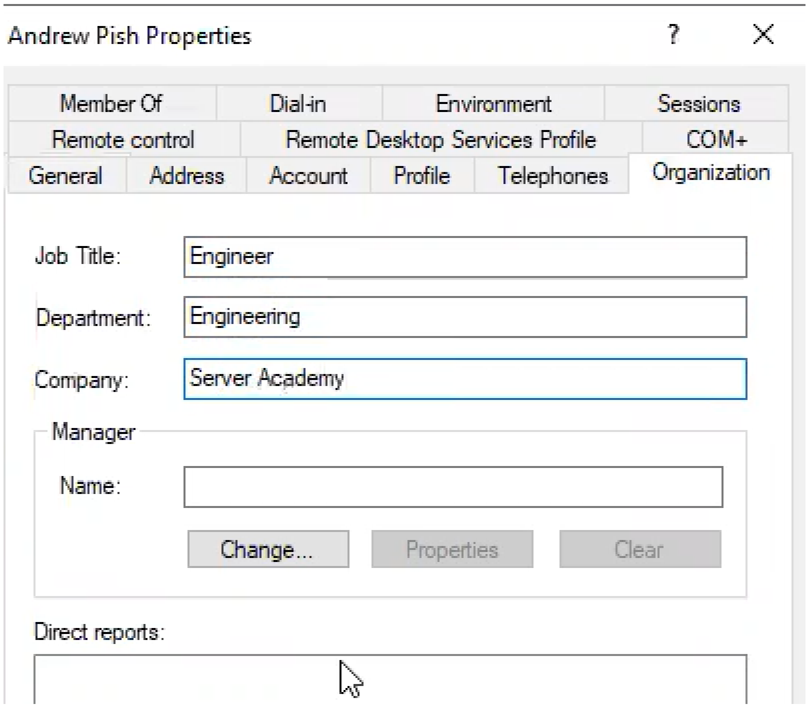
Create in: ServerAcademy.com/Users

When you click Finish, the following object will be created:

Full name: Andrew Pish

User logon name: APish@ServerAcademy.com

The password never expires.



Andrew Pish Properties

Job Title: Engineer

Department: Engineering

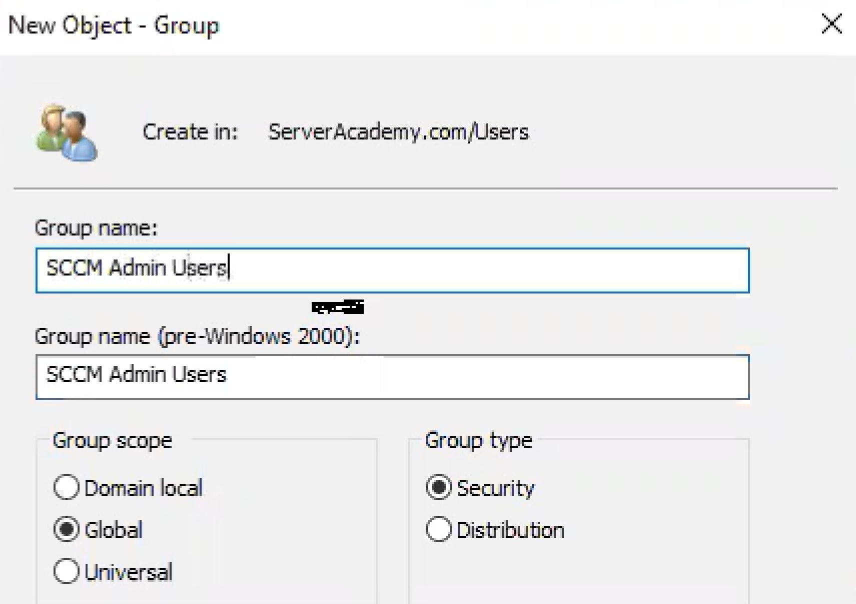
Company: Server Academy

Manager

Name:

Direct reports:

Creating a Group Object



New Object - Group

Create in: ServerAcademy.com/Users

Group name:

SCCM Admin Users

Group name (pre-Windows 2000):

SCCM Admin Users

Group scope

○ Domain local

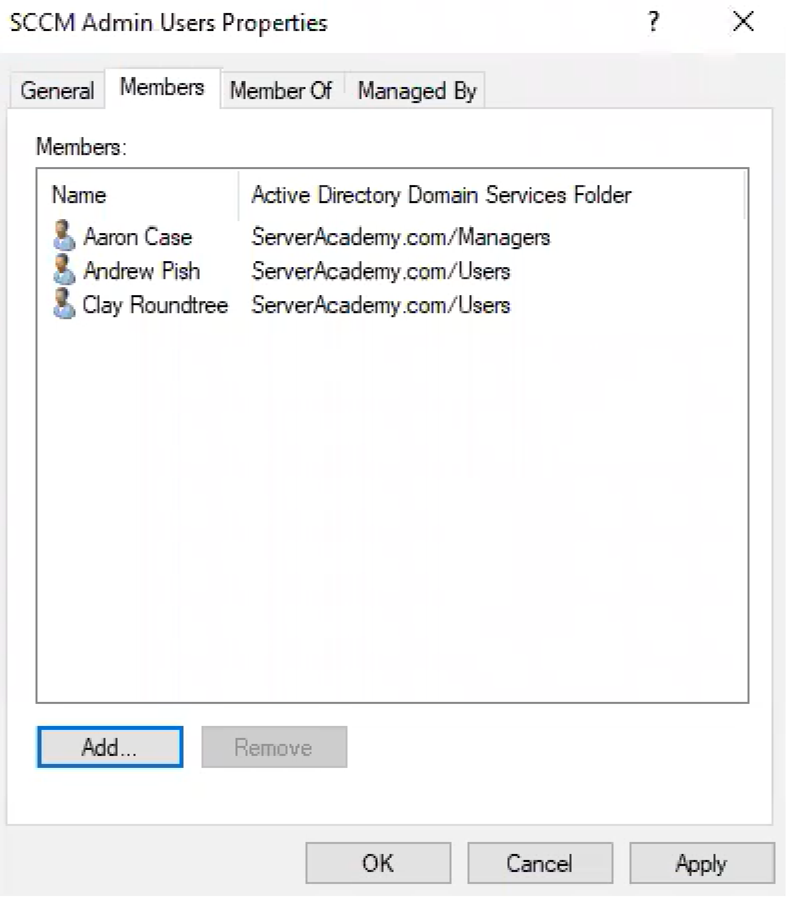
● Global

○ Universal

Group type

● Security

○ Distribution

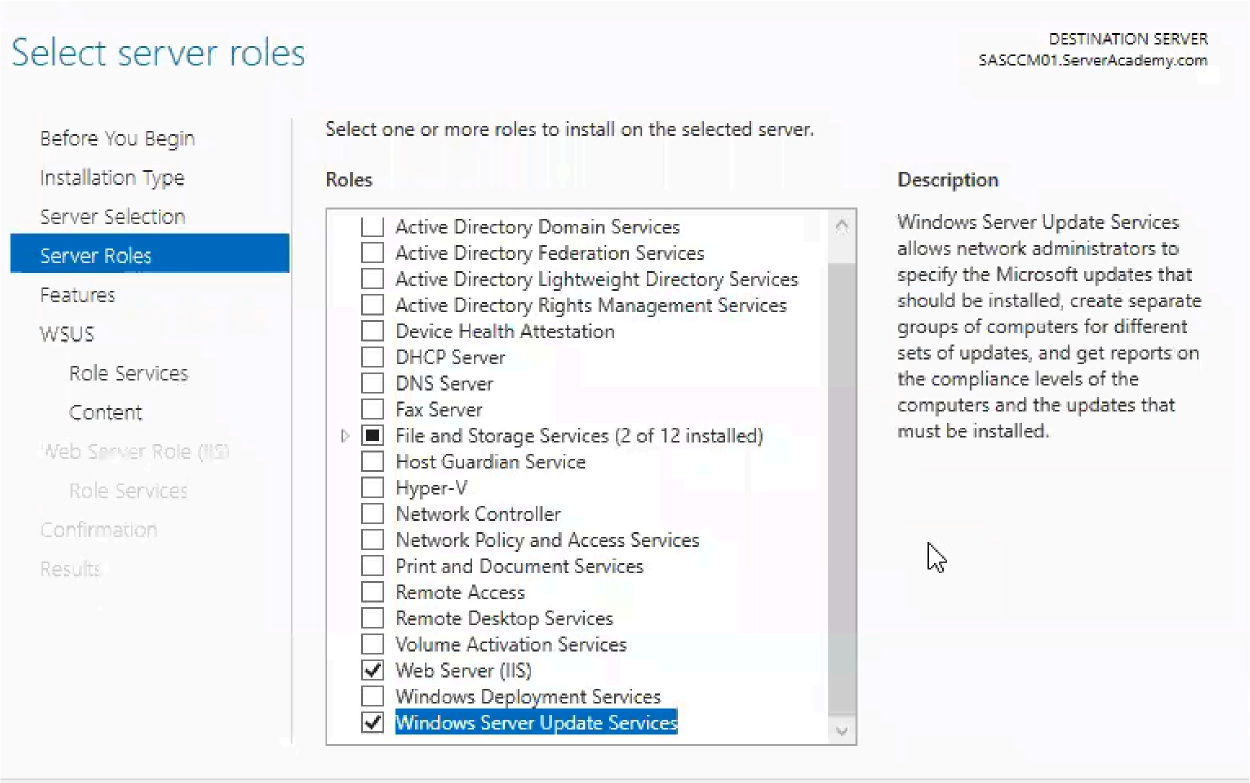


SCCM Admin Users Properties

Members:

Name	Active Directory Domain Services Folder
Aaron Case	ServerAcademy.com/Managers
Andrew Pish	ServerAcademy.com/Users
Clay Roundtree	ServerAcademy.com/Users

Installing SCCM Dependent Roles



Select server roles

DESTINATION SERVER
SASCCM01.ServerAcademy.com

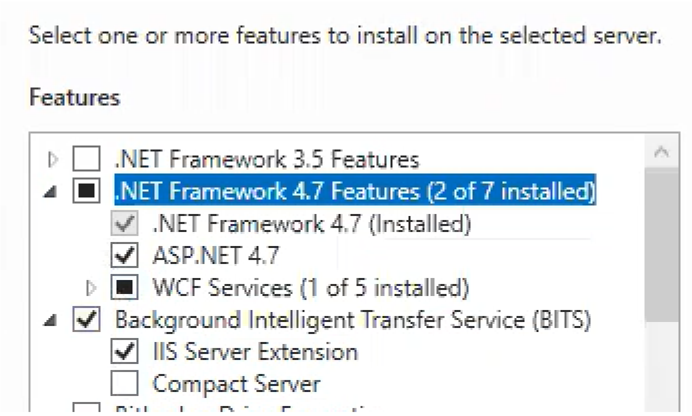
Select one or more roles to install on the selected server.

Roles

- ☐ Active Directory Domain Services
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Device Health Attestation
- ☐ DHCP Server
- ☐ DNS Server
- ☐ Fax Server
- ■ File and Storage Services (2 of 12 installed)
- ☐ Host Guardian Service
- ☐ Hyper-V
- ☐ Network Controller
- ☐ Network Policy and Access Services
- ☐ Print and Document Services
- ☐ Remote Access
- ☐ Remote Desktop Services
- ☐ Volume Activation Services
- ☑ Web Server (IIS)
- ☐ Windows Deployment Services
- ☑ Windows Server Update Services

Description

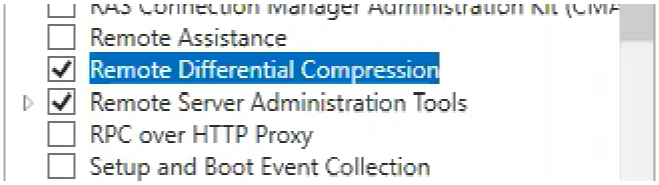
Windows Server Update Services allows network administrators to specify the Microsoft updates that should be installed, create separate groups of computers for different sets of updates, and get reports on the compliance levels of the computers and the updates that must be installed.



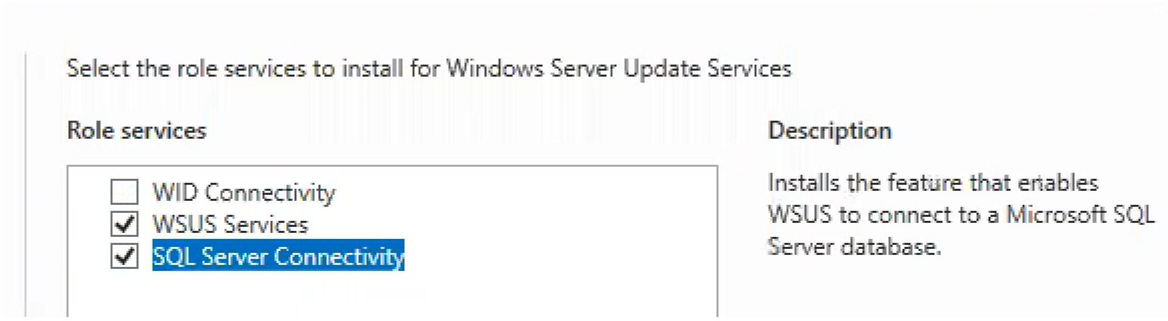
Select one or more features to install on the selected server.

Features

- ☐ .NET Framework 3.5 Features
- ■ .NET Framework 4.7 Features (2 of 7 installed)
  - ☑ .NET Framework 4.7 (Installed)
  - ☑ ASP.NET 4.7
  - ■ WCF Services (1 of 5 installed)
- ☑ Background Intelligent Transfer Service (BITS)
  - ☑ IIS Server Extension
  - ☐ Compact Server



- ☐ RAS Connection Manager Administration Kit (CMA
- ☐ Remote Assistance
- ☑ Remote Differential Compression
- ☑ Remote Server Administration Tools
- ☐ RPC over HTTP Proxy
- ☐ Setup and Boot Event Collection



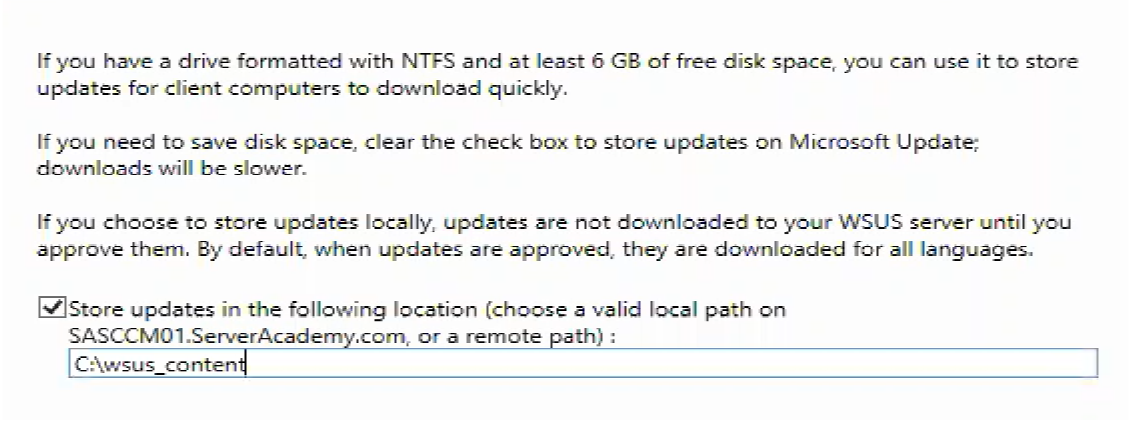
Select the role services to install for Windows Server Update Services

Role services

□ WID Connectivity
☑ WSUS Services
☑ SQL Server Connectivity

Description

Installs the feature that enables WSUS to connect to a Microsoft SQL Server database.



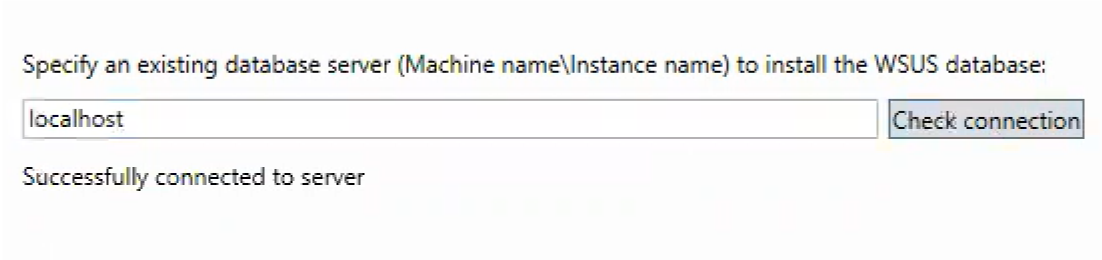
If you have a drive formatted with NTFS and at least 6 GB of free disk space, you can use it to store updates for client computers to download quickly.

If you need to save disk space, clear the check box to store updates on Microsoft Update; downloads will be slower.

If you choose to store updates locally, updates are not downloaded to your WSUS server until you approve them. By default, when updates are approved, they are downloaded for all languages.

☑ Store updates in the following location (choose a valid local path on SASCCM01.ServerAcademy.com, or a remote path) :

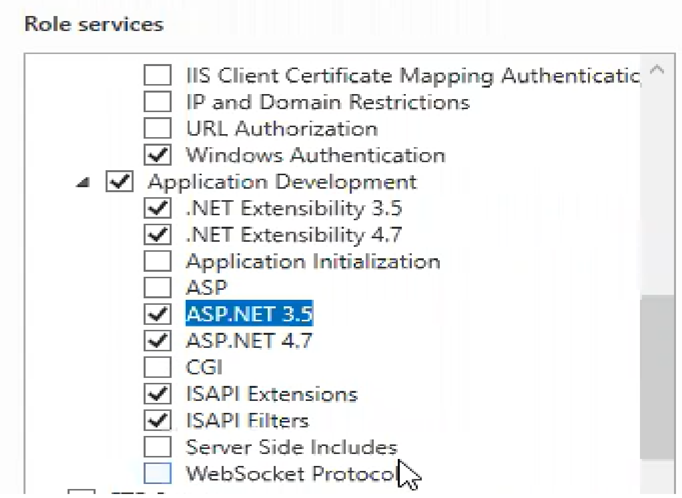
C:\wsus_content



Specify an existing database server (Machine name\Instance name) to install the WSUS database:

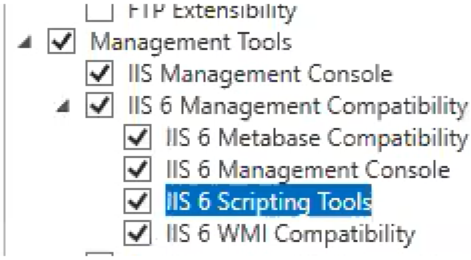
localhost

Successfully connected to server

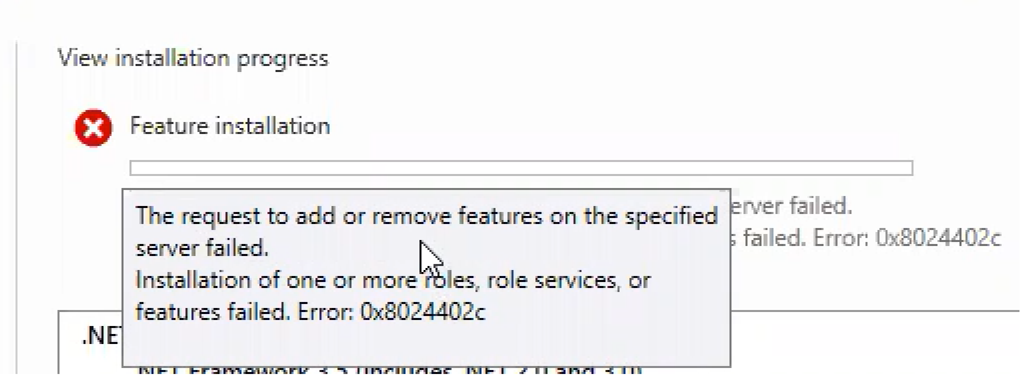


Role services

- □ 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 Extensibility
- ☑ Management Tools
  - ☑ IIS Management Console
  - ☑ IIS 6 Management Compatibility
    - ☑ IIS 6 Metabase Compatibility
    - ☑ IIS 6 Management Console
    - ☑ IIS 6 Scripting Tools
    - ☑ IIS 6 WMI Compatibility

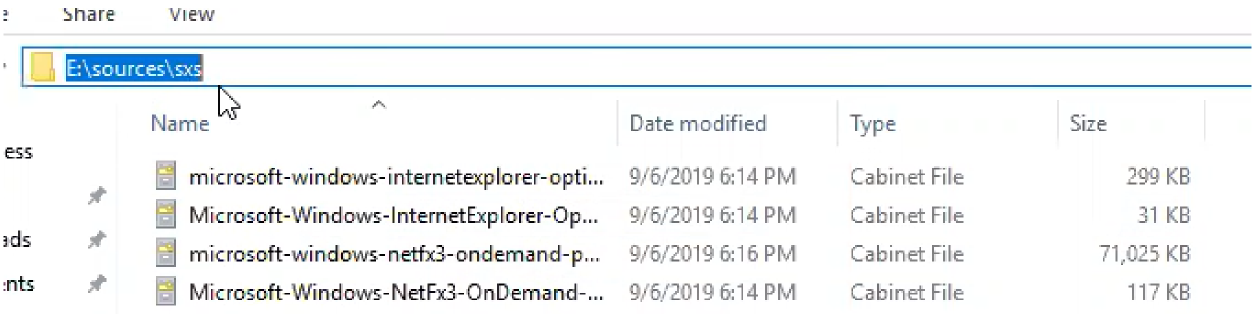


View installation progress

Feature installation

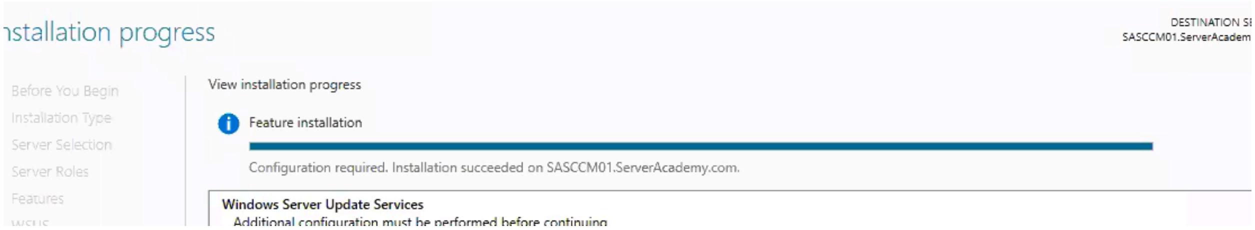
The request to add or remove features on the specified server failed.
Installation of one or more roles, role services, or features failed. Error: 0x8024402c

Needed to mount an Preconfigured Windows ISO image to Hypervisor to Complete Install (E:)



E:\sources\sxs

Name	Date modified	Type	Size
microsoft-windows-internetexplorer-opti...	9/6/2019 6:14 PM	Cabinet File	299 KB
Microsoft-Windows-InternetExplorer-Op...	9/6/2019 6:14 PM	Cabinet File	31 KB
microsoft-windows-netfx3-ondemand-p...	9/6/2019 6:16 PM	Cabinet File	71,025 KB
Microsoft-Windows-NetFx3-OnDemand-...	9/6/2019 6:14 PM	Cabinet File	117 KB



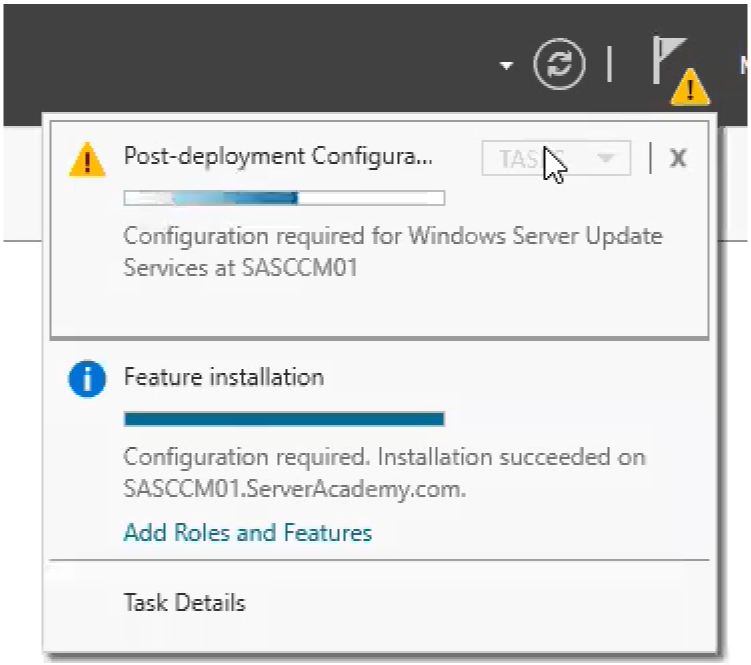
View installation progress

Feature installation

Configuration required. Installation succeeded on SASCCM01.ServerAcademy.com.

Windows Server Update Services

Additional configuration must be performed before continuing



Post-deployment Configura...

Configuration required for Windows Server Update Services at SASCCM01

Feature installation

Configuration required. Installation succeeded on SASCCM01.ServerAcademy.com.

!!

!!

DOMAIN CONTROLLER CONFIGURATION ENDS

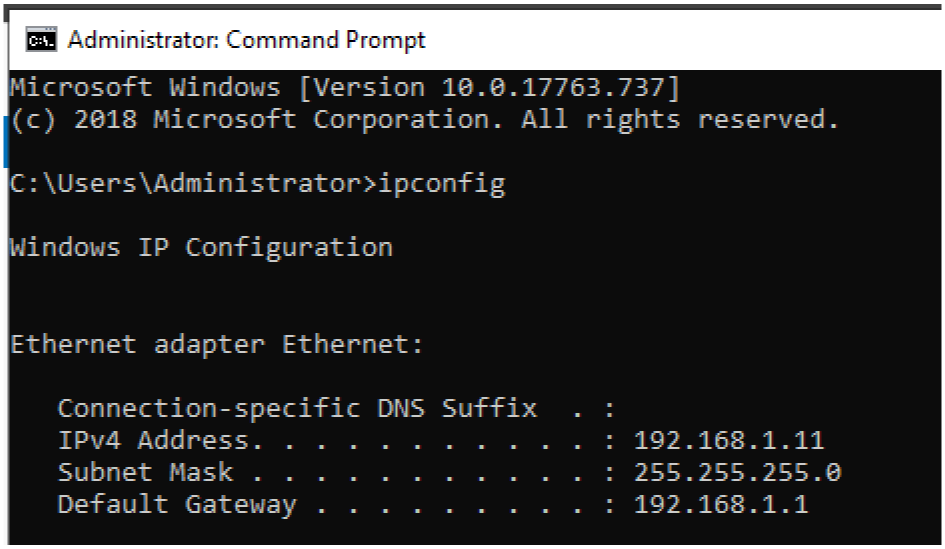
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!**HERE**!!

!!

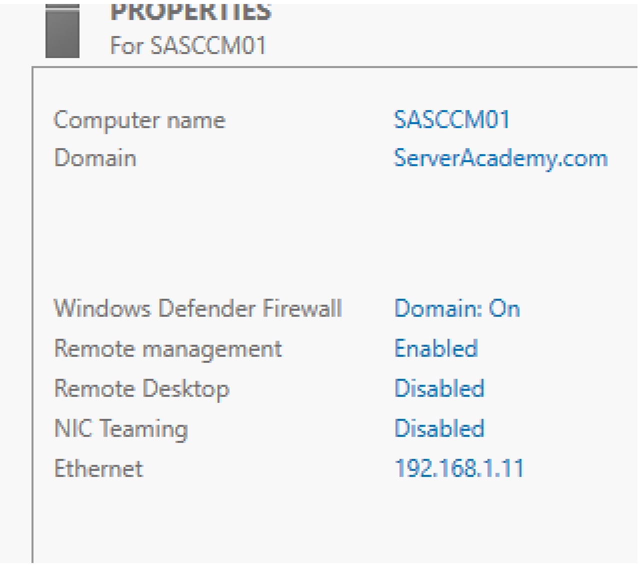
!!

!!!!!!!-- SASCCM01 Server Configuration --!!!!!!!!

!!

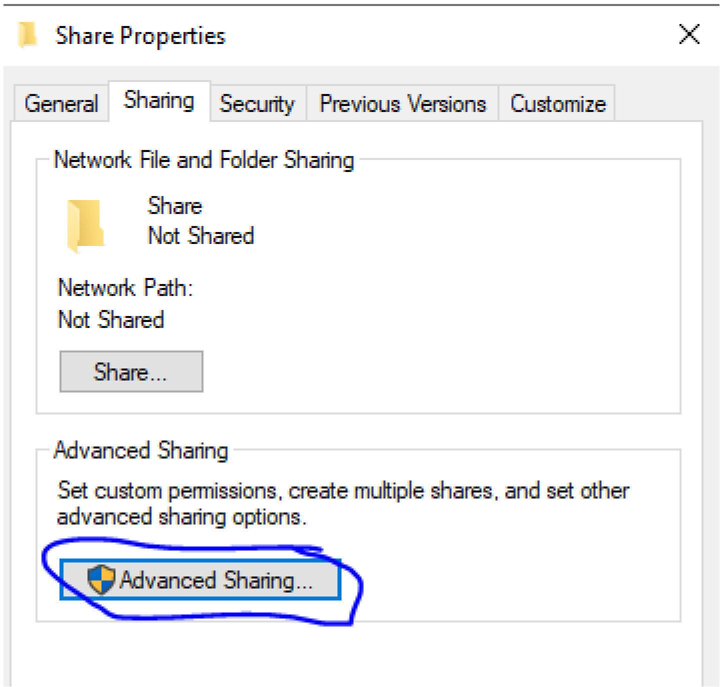


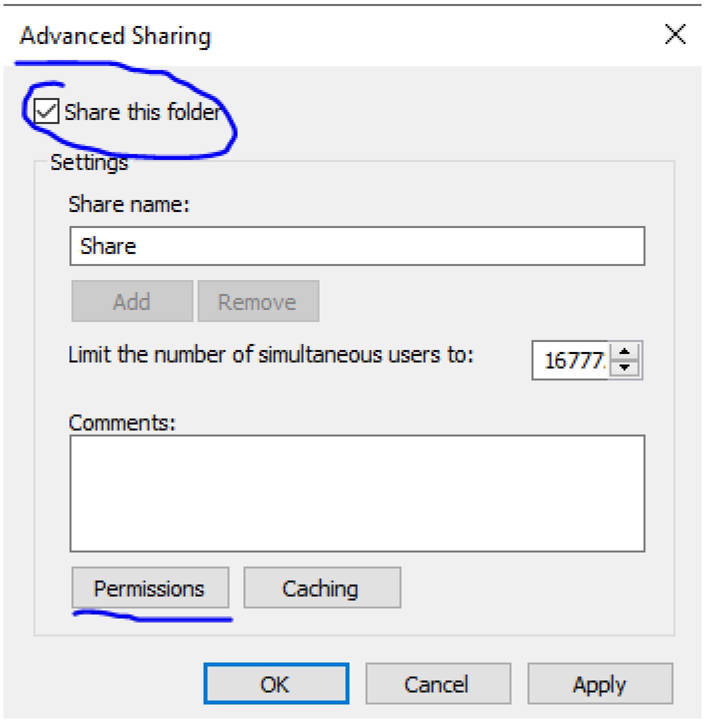
```
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : 192.168.1.11
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1
```

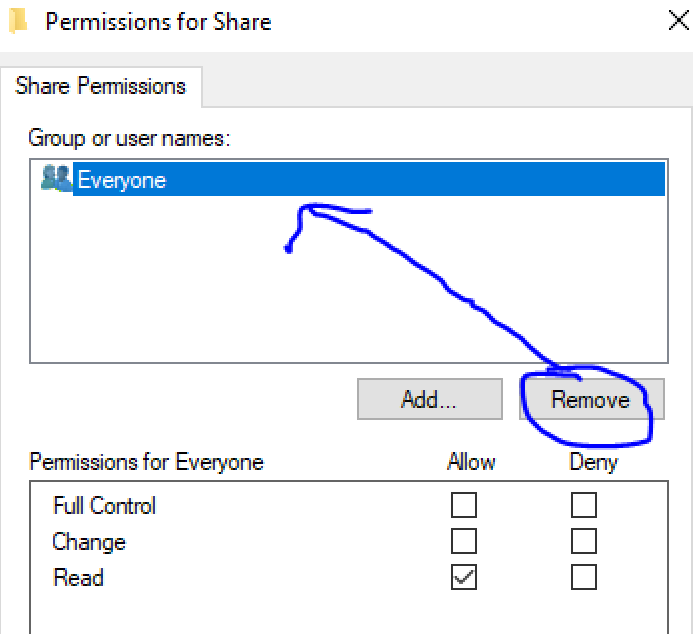

PROPERTIES
For SASCCM01

Computer name	SASCCM01
Domain	ServerAcademy.com
Windows Defender Firewall	Domain: On
Remote management	Enabled
Remote Desktop	Disabled
NIC Teaming	Disabled
Ethernet	192.168.1.11

Create a shared folder in SASCCM C: Disk



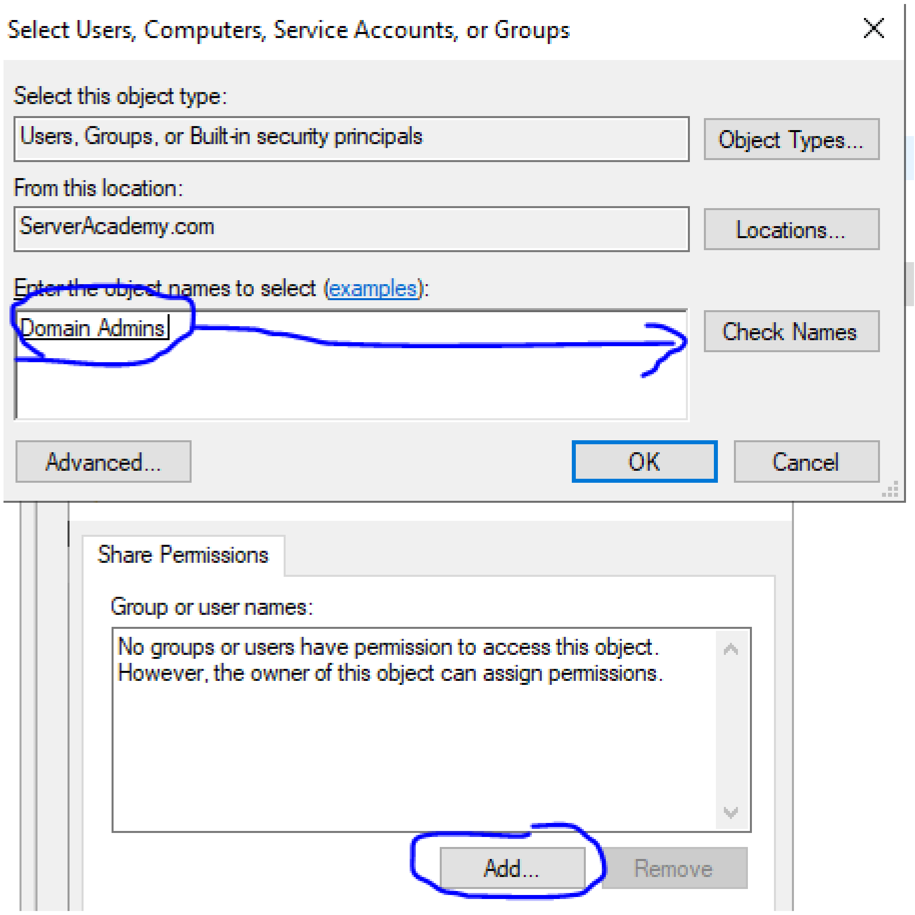




Group or user names:
Everyone

Permissions for Everyone

	Allow	Deny
Full Control	□	□
Change	□	□
Read	☑	□

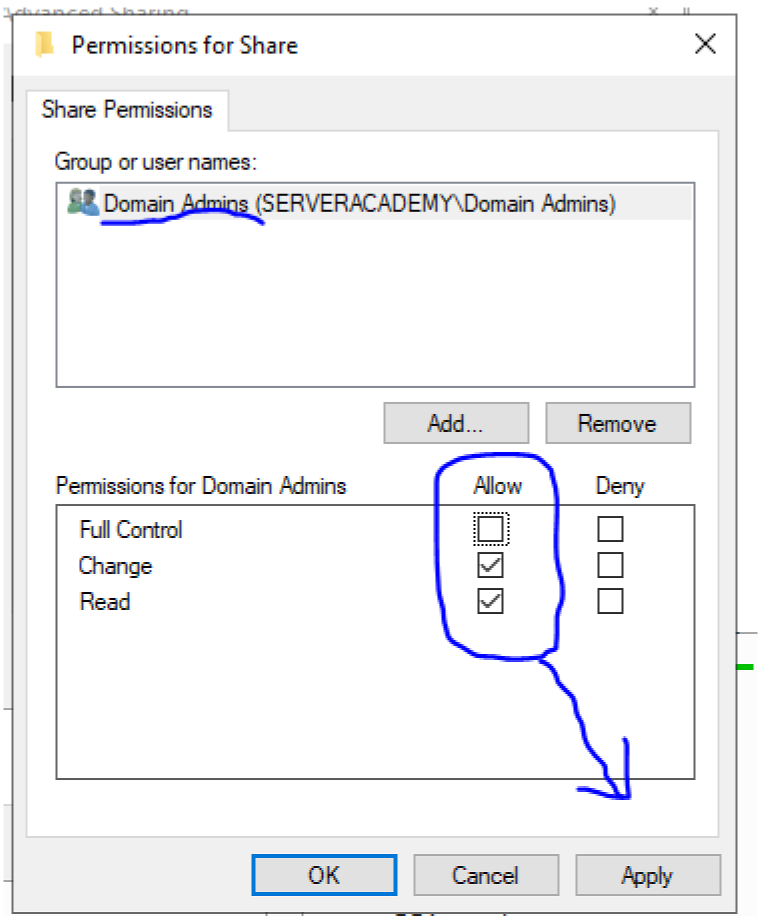


Select this object type:
Users, Groups, or Built-in security principals

From this location:
ServerAcademy.com

Enter the object names to select (examples):
Domain Admins

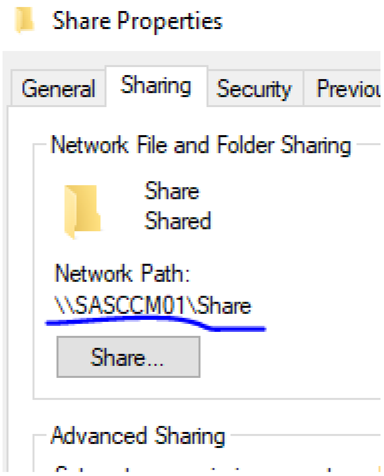
Group or user names:
No groups or users have permission to access this object.
However, the owner of this object can assign permissions.



Group or user names:

Domain Admins (SERVERACADEMY\Domain Admins)

Permissions for Domain Admins	Allow	Deny
Full Control	□	□
Change	☑	□
Read	☑	□

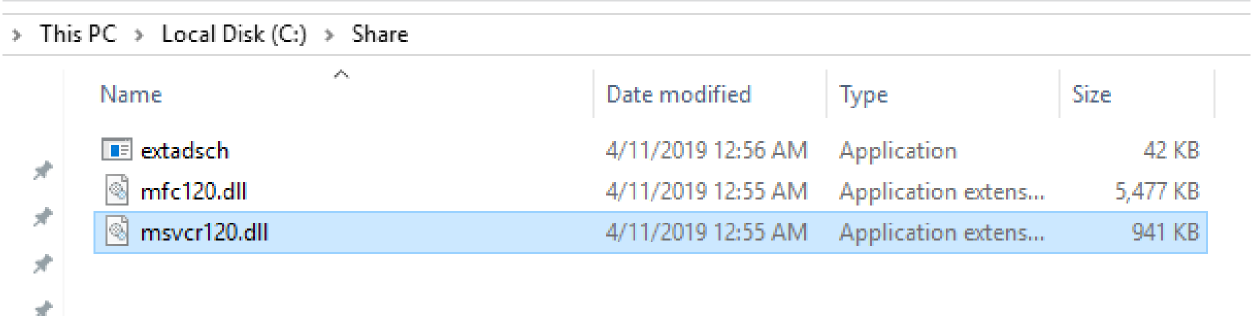


Network File and Folder Sharing

Share
Shared

Network Path:
\\SASCCM01\Share

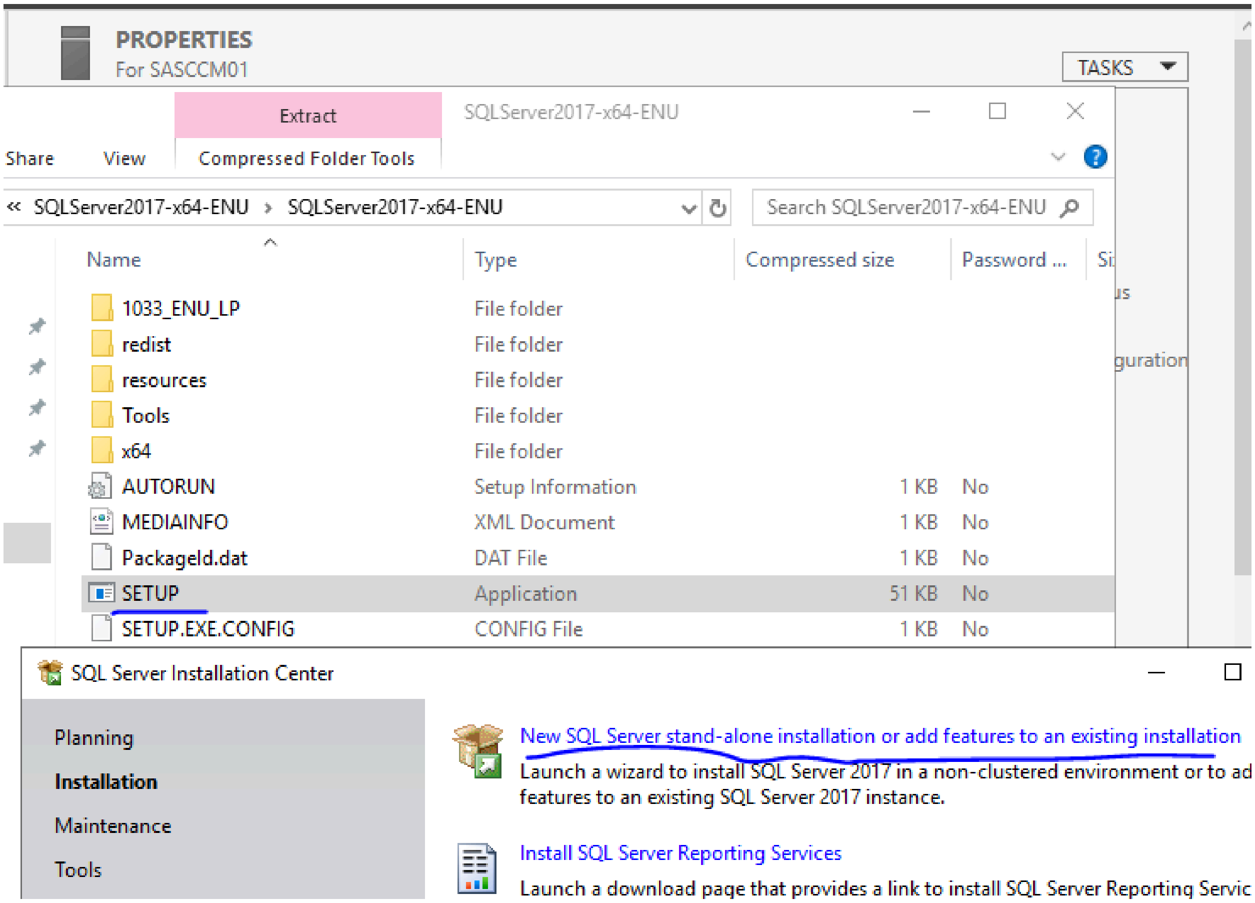
Shared files



This PC > Local Disk (C:) > Share

Name	Date modified	Type	Size
extadsch	4/11/2019 12:56 AM	Application	42 KB
mfc120.dll	4/11/2019 12:55 AM	Application extens...	5,477 KB
msvcr120.dll	4/11/2019 12:55 AM	Application extens...	941 KB

Installing SQLServer on SASCCM



« SQLServer2017-x64-ENU > SQLServer2017-x64-ENU

Name	Type	Compressed size	Password ...
1033_ENU_LP	File folder		
redist	File folder		
resources	File folder		
Tools	File folder		
x64	File folder		
AUTORUN	Setup Information	1 KB	No
MEDIAINFO	XML Document	1 KB	No
PackageId.dat	DAT File	1 KB	No
SETUP	Application	51 KB	No
SETUP.EXE.CONFIG	CONFIG File	1 KB	No

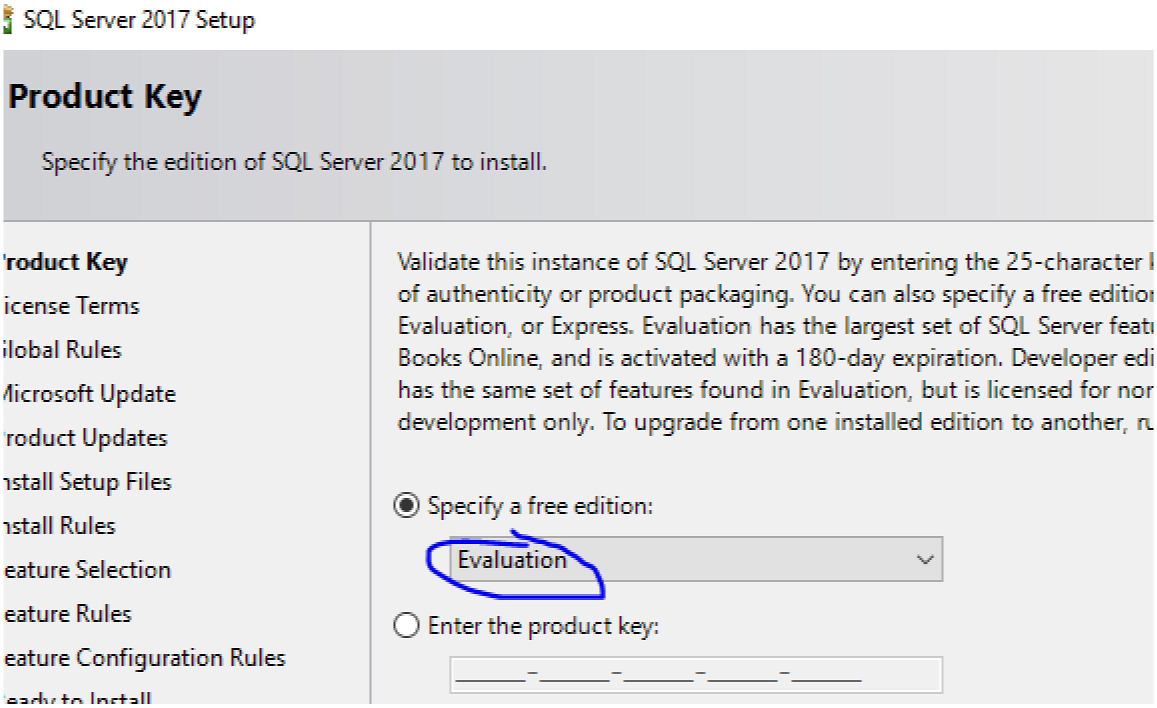
SQL Server Installation Center

New SQL Server stand-alone installation or add features to an existing installation

Launch a wizard to install SQL Server 2017 in a non-clustered environment or to ad features to an existing SQL Server 2017 instance.

Install SQL Server Reporting Services

Launch a download page that provides a link to install SQL Server Reporting Servic



SQL Server 2017 Setup

Product Key

Specify the edition of SQL Server 2017 to install.

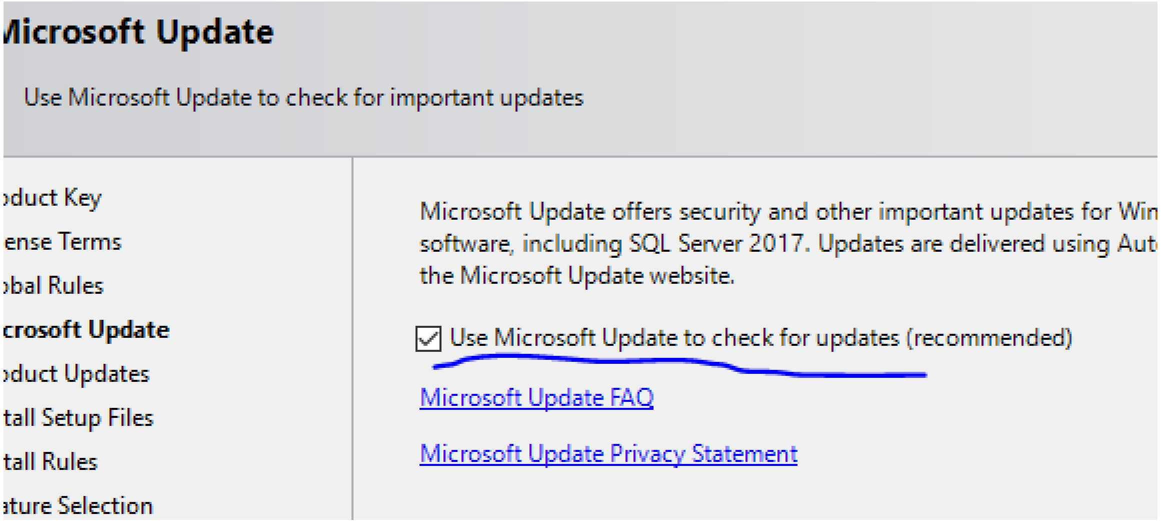
Validate this instance of SQL Server 2017 by entering the 25-character k
of authenticity or product packaging. You can also specify a free editio
Evaluation, or Express. Evaluation has the largest set of SQL Server feat
Books Online, and is activated with a 180-day expiration. Developer edi
has the same set of features found in Evaluation, but is licensed for nor
development only. To upgrade from one installed edition to another, ru

● Specify a free edition:

Evaluation

○ Enter the product key:

_____-_____-_____-_____-_____



Microsoft Update

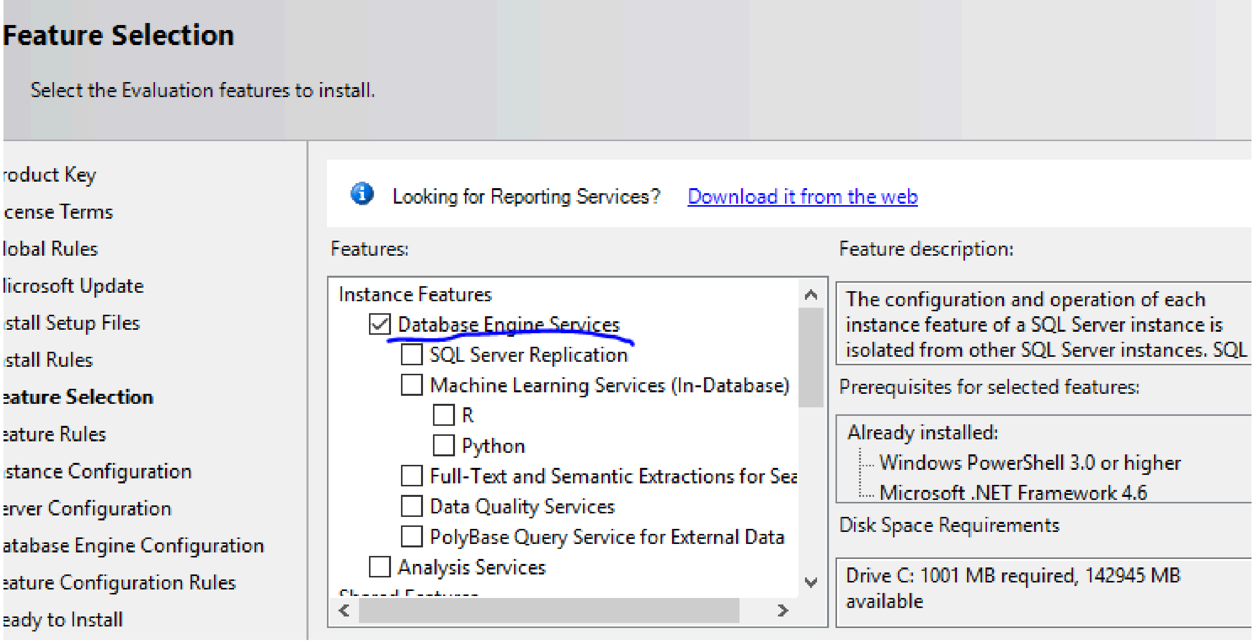
Use Microsoft Update to check for important updates

Microsoft Update offers security and other important updates for Win
software, including SQL Server 2017. Updates are delivered using Aut
the Microsoft Update website.

☑ Use Microsoft Update to check for updates (recommended)

Microsoft Update FAQ

Microsoft Update Privacy Statement



Feature Selection

Select the Evaluation features to install.

- roduct Key
- cense Terms
- lobal Rules
- licrosoft Update
- stall Setup Files
- stall Rules
- **eature Selection**
- eature Rules
- stance Configuration
- erver Configuration
- atabase Engine Configuration
- eature Configuration Rules
- eady to Install

Looking for Reporting Services? Download it from the web

Features:

Instance Features
- ☑ Database Engine Services
  - □ SQL Server Replication
  - □ Machine Learning Services (In-Database)
    - □ R
    - □ Python
  - □ Full-Text and Semantic Extractions for Sea
  - □ Data Quality Services
  - □ PolyBase Query Service for External Data
- □ Analysis Services

Shared Features

Feature description:

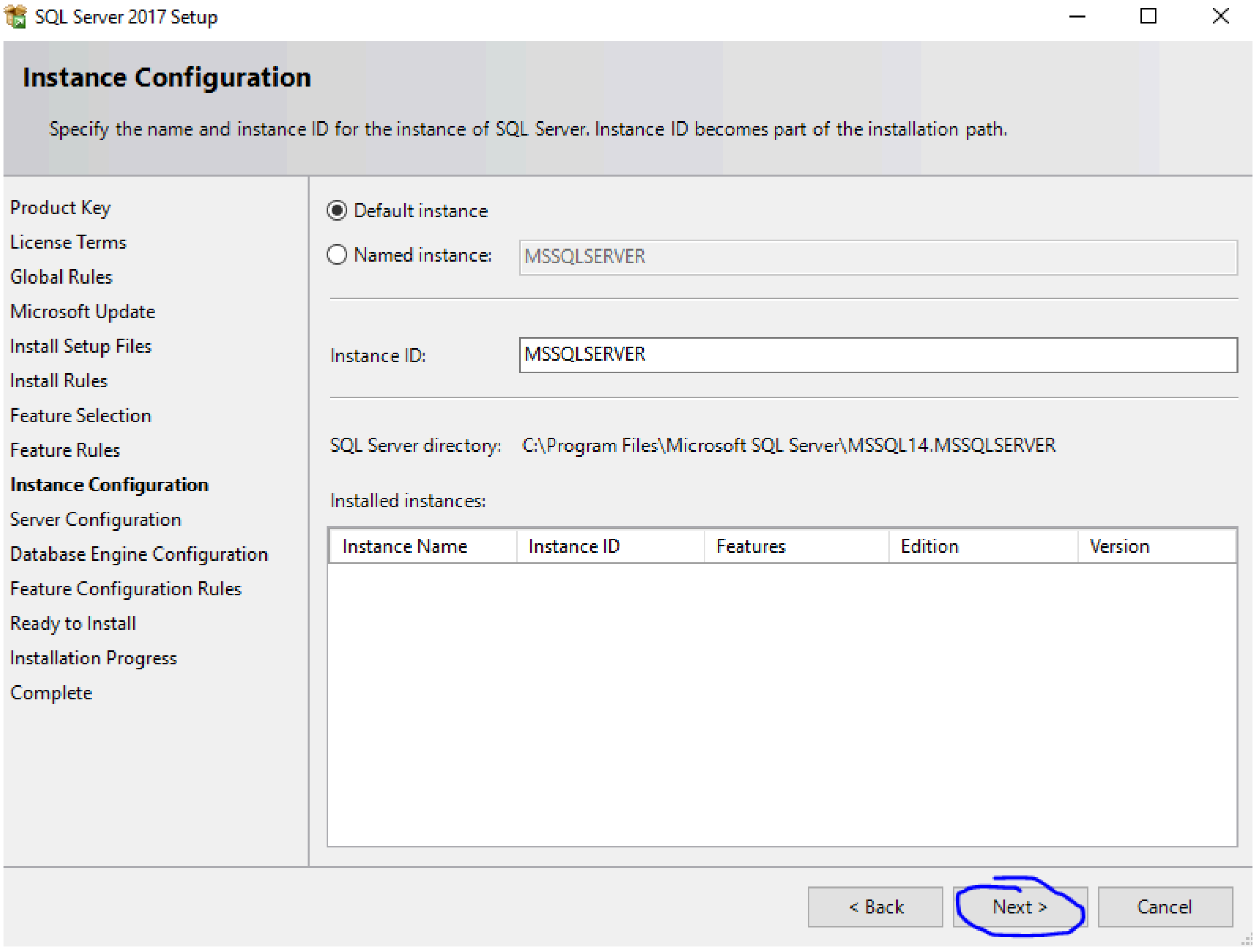
The configuration and operation of each instance feature of a SQL Server instance is isolated from other SQL Server instances. SQL

Prerequisites for selected features:

Already installed:
- Windows PowerShell 3.0 or higher
- Microsoft .NET Framework 4.6

Disk Space Requirements

Drive C: 1001 MB required, 142945 MB available



SQL Server 2017 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
- Install Setup Files
- Install Rules
- Feature Selection
- Feature Rules
- **Instance Configuration**
- Server Configuration
- Database Engine Configuration
- Feature Configuration Rules
- Ready to Install
- Installation Progress
- Complete

● Default instance

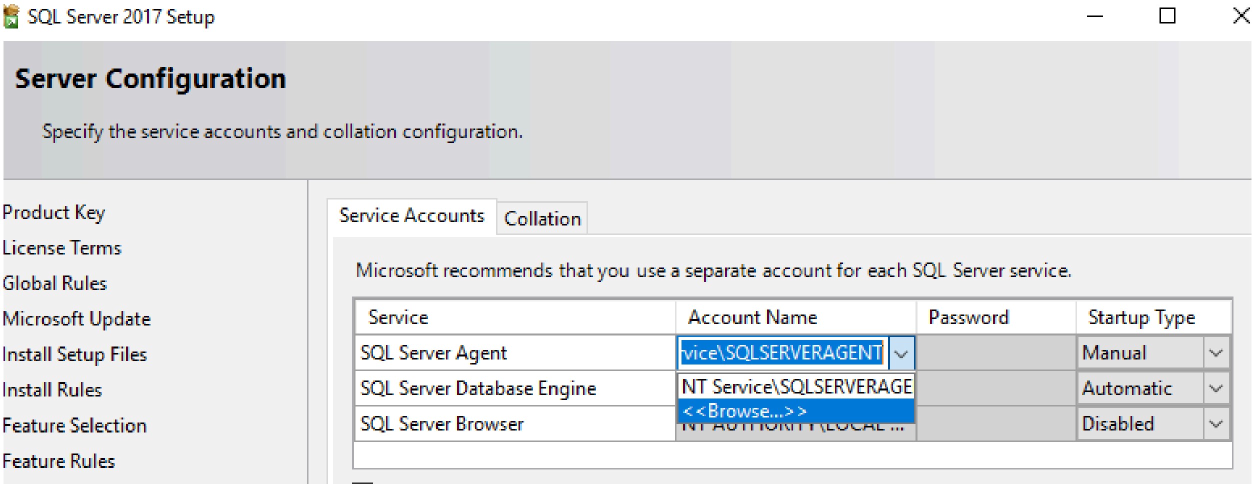
○ Named instance: MSSQLSERVER

Instance ID: MSSQLSERVER

SQL Server directory: C:\Program Files\Microsoft SQL Server\MSSQL14.MSSQLSERVER

Installed instances:

Instance Name	Instance ID	Features	Edition	Version



SQL Server 2017 Setup

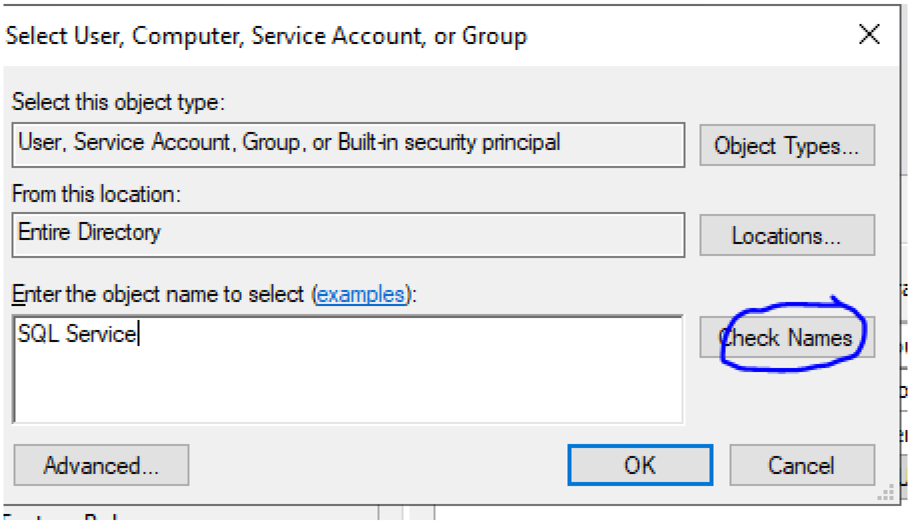
Server Configuration

Specify the service accounts and collation configuration.

- Product Key
- License Terms
- Global Rules
- Microsoft Update
- Install Setup Files
- Install Rules
- Feature Selection
- Feature Rules

Microsoft recommends that you use a separate account for each SQL Server service.

Service	Account Name	Password	Startup Type
SQL Server Agent	vice\SQLSERVERAGENT		Manual
SQL Server Database Engine			Automatic
SQL Server Browser	NT AUTHORITY\LOCAL ...		Disabled



Select User, Computer, Service Account, or Group

Select this object type:

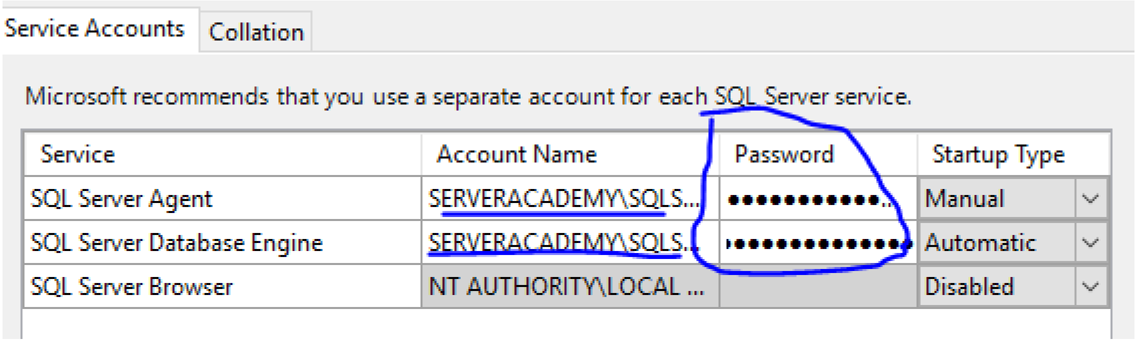
User, Service Account, Group, or Built-in security principal

From this location:

Entire Directory

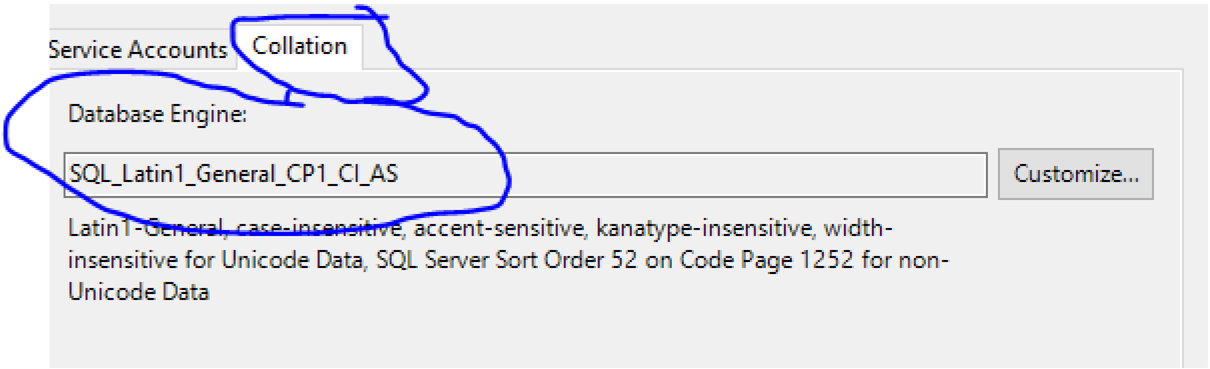
Enter the object name to select (examples):

SQL Service



Microsoft recommends that you use a separate account for each SQL Server service.

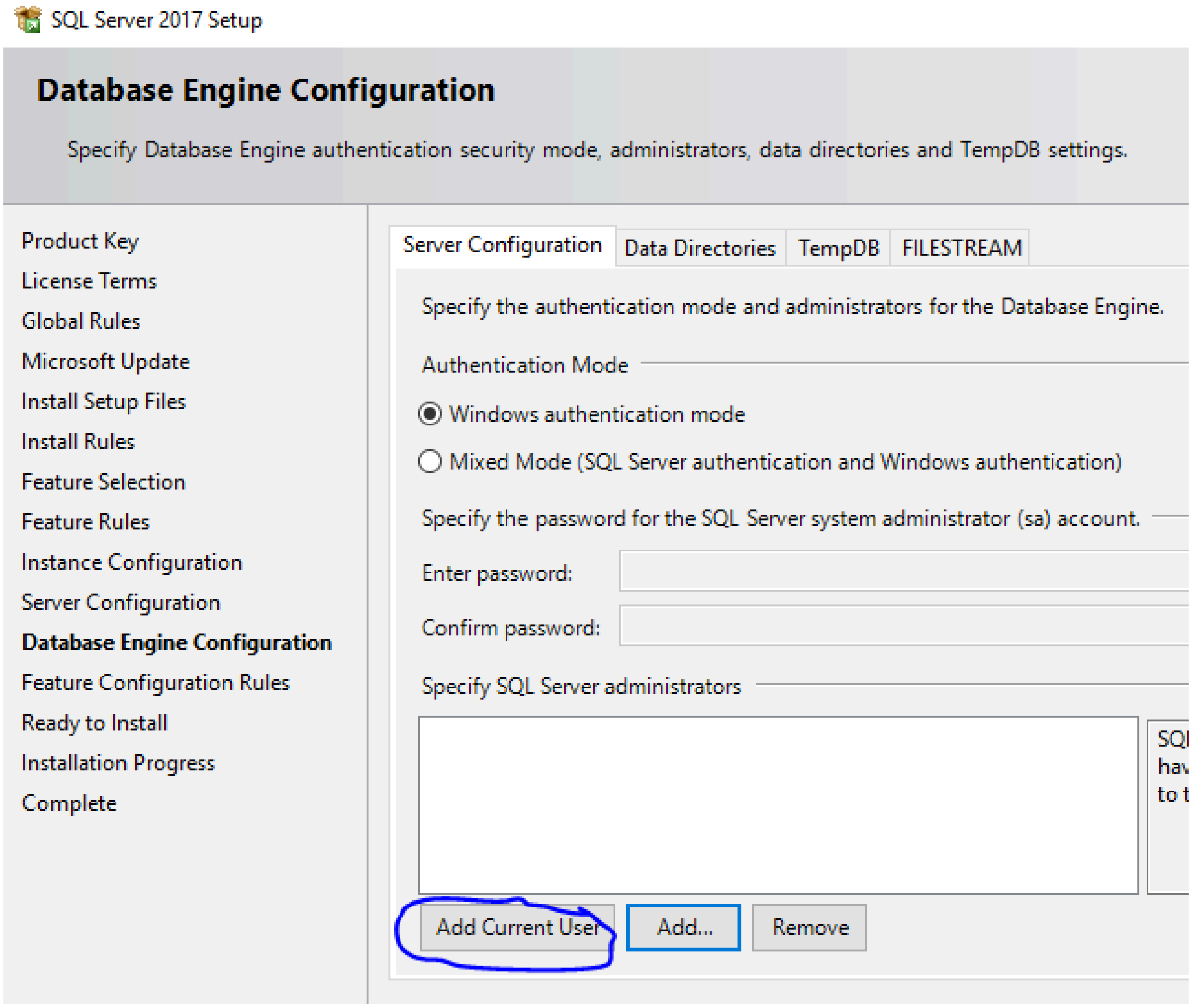
Service	Account Name	Password	Startup Type
SQL Server Agent	SERVERACADEMY\SQLS...	●●●●●●●●●●●●	Manual
SQL Server Database Engine	SERVERACADEMY\SQLS...	●●●●●●●●●●●●●	Automatic
SQL Server Browser	NT AUTHORITY\LOCAL ...		Disabled



Database Engine:

SQL_Latin1_General_CP1_CI_AS

Latin1-General, case-insensitive, accent-sensitive, kanatype-insensitive, width-insensitive for Unicode Data, SQL Server Sort Order 52 on Code Page 1252 for non-Unicode Data



Database Engine Configuration

Specify Database Engine authentication security mode, administrators, data directories and TempDB settings.

Specify the authentication mode and administrators for the Database Engine.

Authentication Mode

● Windows authentication mode

○ Mixed Mode (SQL Server authentication and Windows authentication)

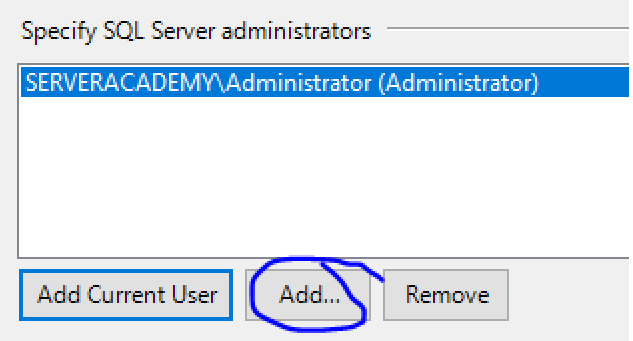
Specify the password for the SQL Server system administrator (sa) account.

Enter password:

Confirm password:

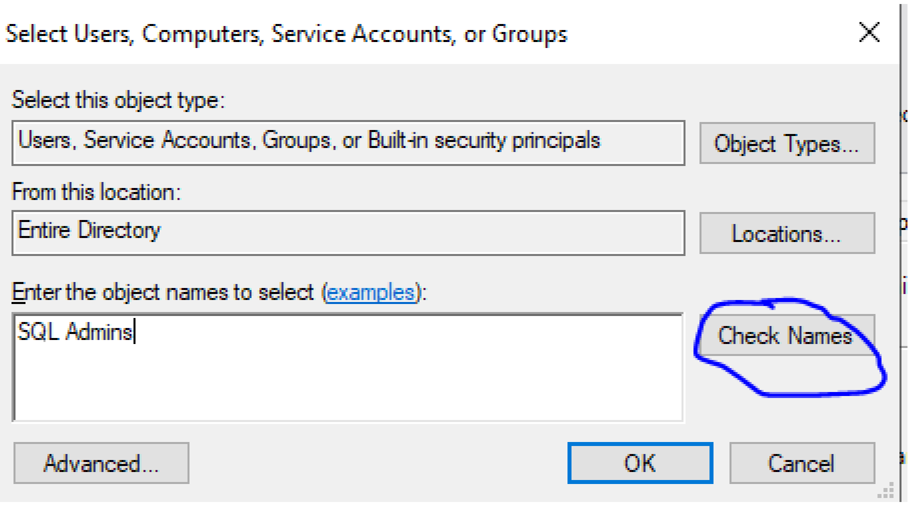
Specify SQL Server administrators

SQl
hav
to t



Specify SQL Server administrators

SERVERACADEMY\Administrator (Administrator)

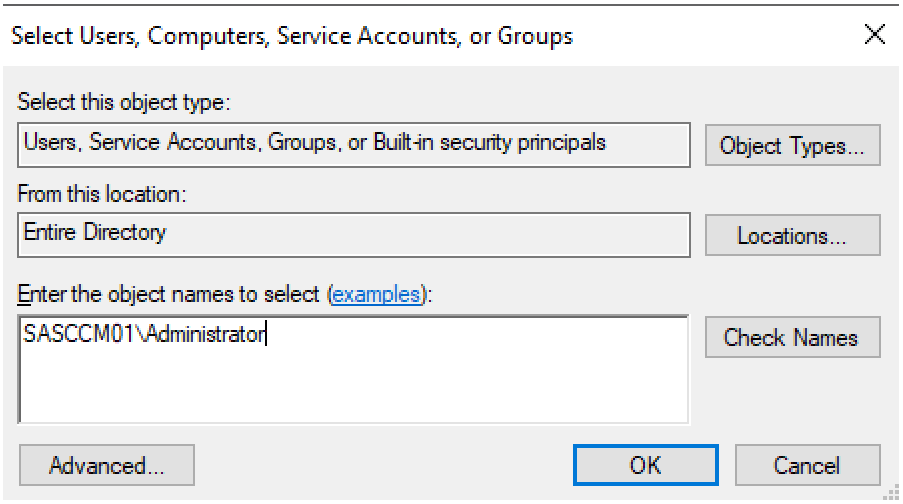


Select Users, Computers, Service Accounts, or Groups

Select this object type:
Users, Service Accounts, Groups, or Built-in security principals

From this location:
Entire Directory

Enter the object names to select (examples):
SQL Admins

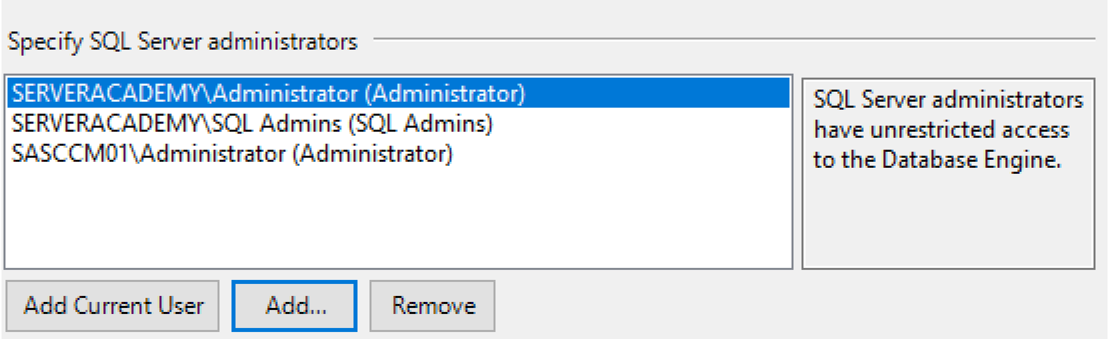


Select Users, Computers, Service Accounts, or Groups

Select this object type:
Users, Service Accounts, Groups, or Built-in security principals

From this location:
Entire Directory

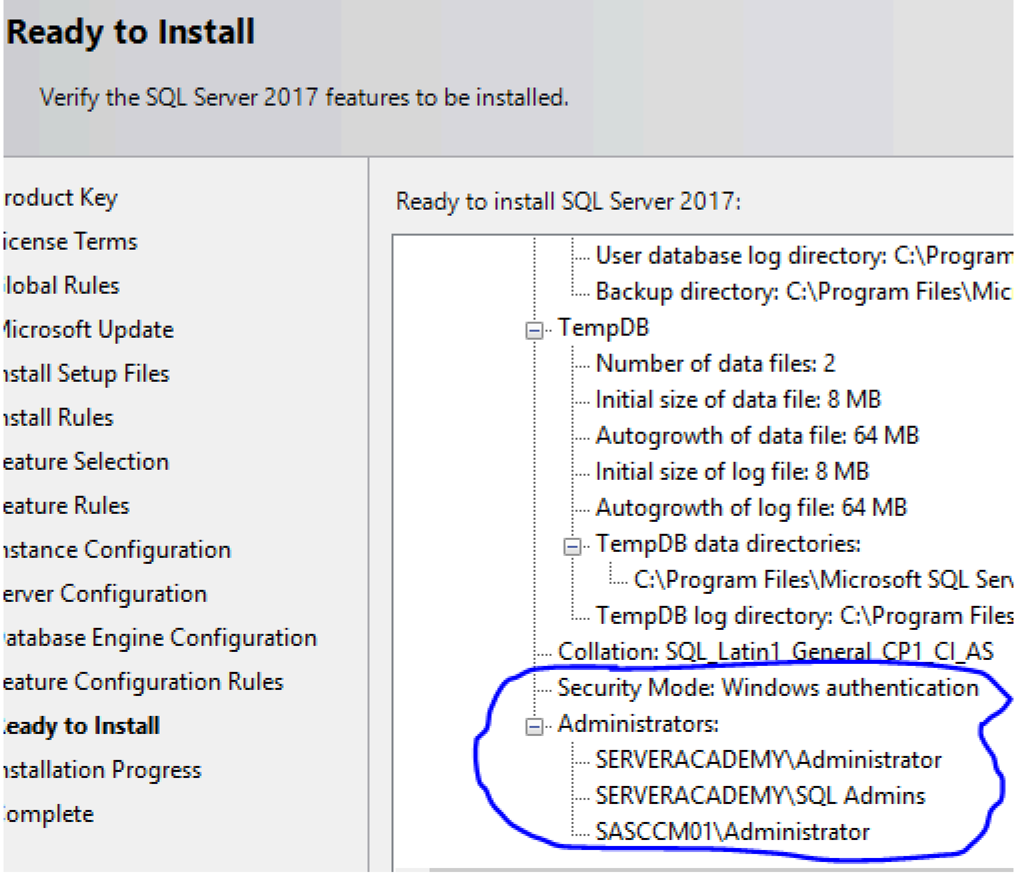
Enter the object names to select (examples):
SASCCM01\Administrator



Specify SQL Server administrators

SERVERACADEMY\Administrator (Administrator)
SERVERACADEMY\SQL Admins (SQL Admins)
SASCCM01\Administrator (Administrator)

SQL Server administrators have unrestricted access to the Database Engine.



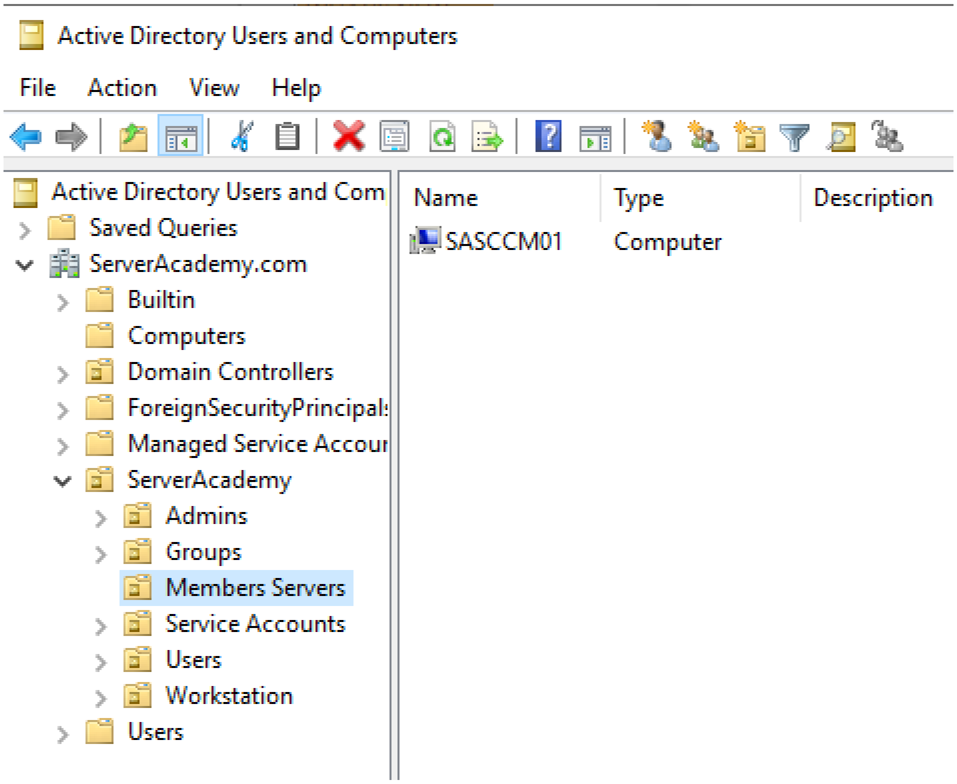
Ready to Install

Verify the SQL Server 2017 features to be installed.

Ready to install SQL Server 2017:

```
        User database log directory: C:\Program
        Backup directory: C:\Program Files\Mic
    TempDB
        Number of data files: 2
        Initial size of data file: 8 MB
        Autogrowth of data file: 64 MB
        Initial size of log file: 8 MB
        Autogrowth of log file: 64 MB
        TempDB data directories:
            C:\Program Files\Microsoft SQL Serv
        TempDB log directory: C:\Program Files
    Collation: SQL_Latin1_General_CP1_CI_AS
    Security Mode: Windows authentication
    Administrators:
        SERVERACADEMY\Administrator
        SERVERACADEMY\SQL Admins
        SASCCM01\Administrator
```

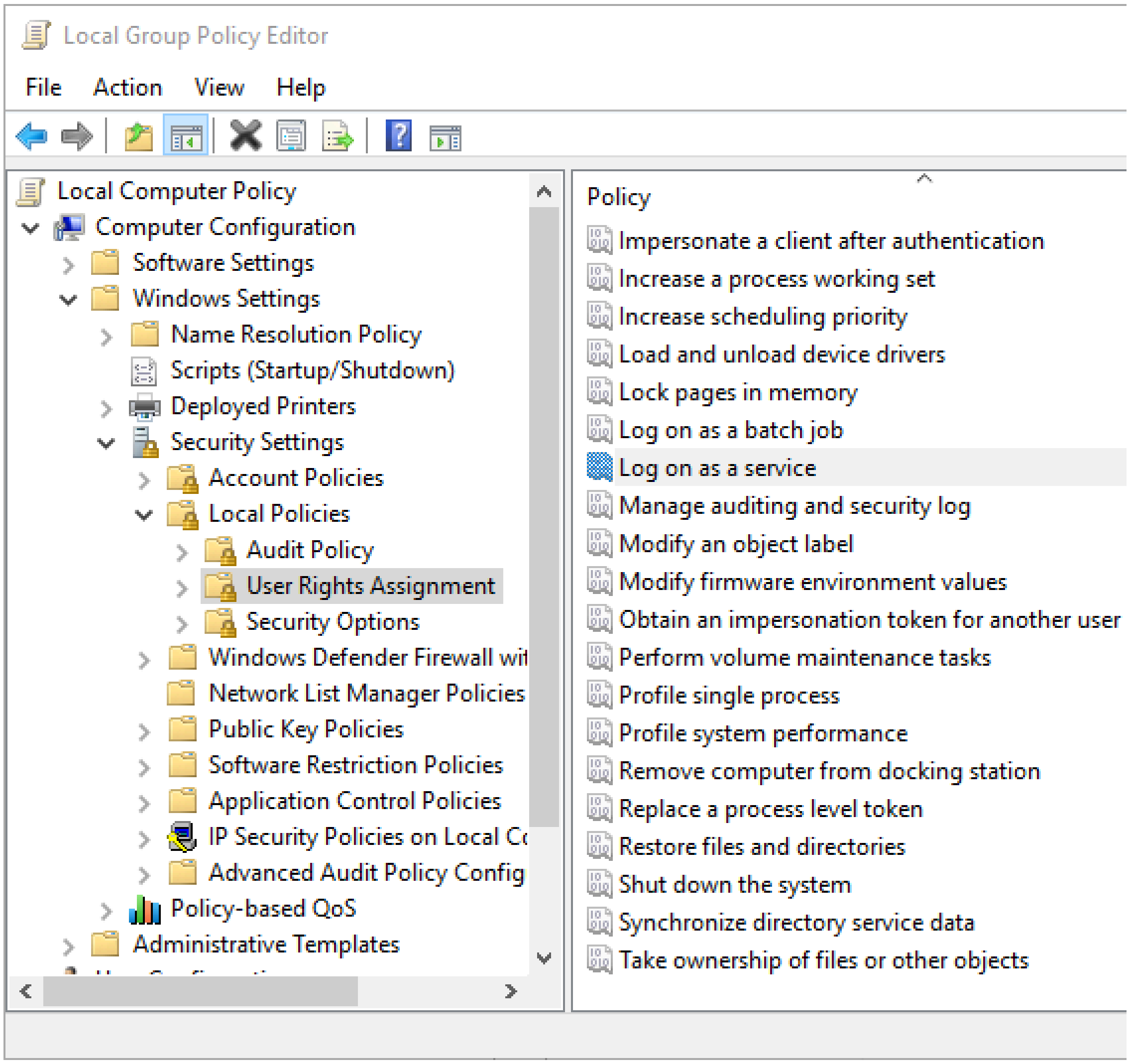
SADC01 Server Configuration (Domain Controller)



- Active Directory Users and Com
  - Saved Queries
  - ServerAcademy.com
    - Builtin
    - Computers
    - Domain Controllers
    - ForeignSecurityPrincipal:
    - Managed Service Accour
    - ServerAcademy
      - Admins
      - Groups
      - Members Servers
      - Service Accounts
      - Users
      - Workstation
    - Users

Name	Type	Description
SASCCM01	Computer	

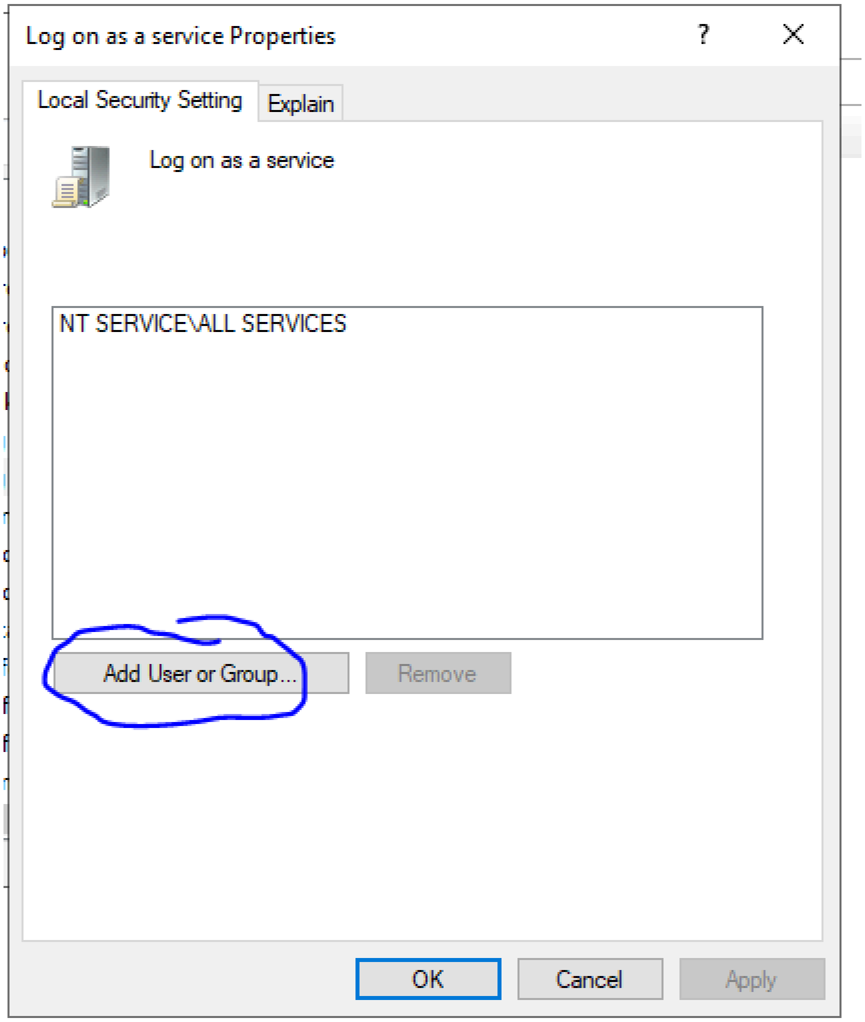
SASCCM01 Creating Domain User Accounts



- Local Computer Policy
  - Computer Configuration
    - Software Settings
    - Windows Settings
      - Name Resolution Policy
      - Scripts (Startup/Shutdown)
      - Deployed Printers
      - Security Settings
        - Account Policies
        - Local Policies
          - Audit Policy
          - User Rights Assignment
          - Security Options
        - Windows Defender Firewall wi
        - Network List Manager Policies
        - Public Key Policies
        - Software Restriction Policies
        - Application Control Policies
        - IP Security Policies on Local C
        - Advanced Audit Policy Config
      - Policy-based QoS
    - Administrative Templates

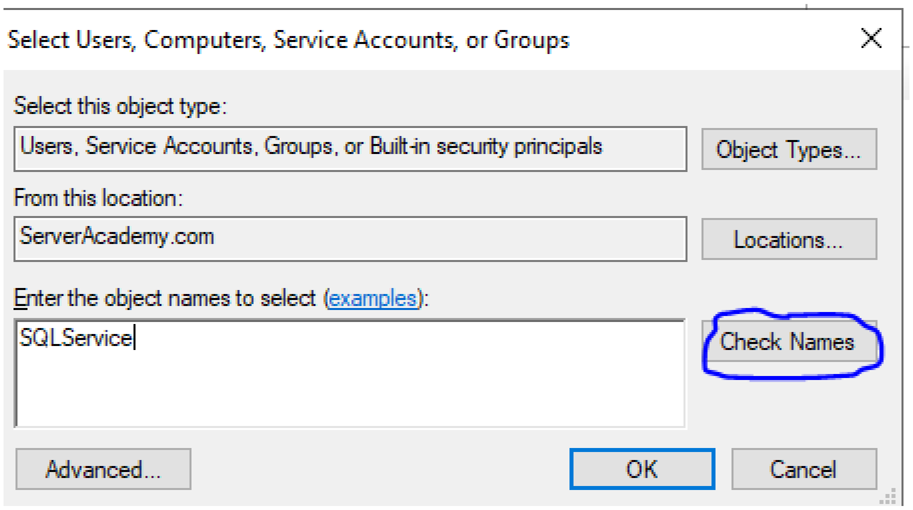
Policy

- Impersonate a client after authentication
- Increase a process working set
- Increase scheduling priority
- Load and unload device drivers
- Lock pages in memory
- Log on as a batch job
- Log on as a service
- Manage auditing and security log
- Modify an object label
- Modify firmware environment values
- Obtain an impersonation token for another user
- Perform volume maintenance tasks
- Profile single process
- Profile system performance
- Remove computer from docking station
- Replace a process level token
- Restore files and directories
- Shut down the system
- Synchronize directory service data
- Take ownership of files or other objects



Log on as a service

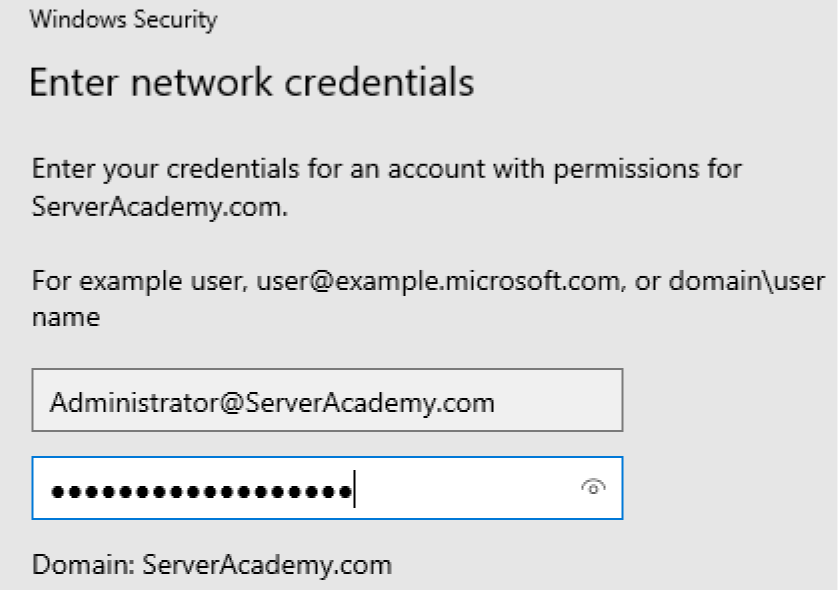
NT SERVICE\ALL SERVICES



Select this object type:
Users, Service Accounts, Groups, or Built-in security principals

From this location:
ServerAcademy.com

Enter the object names to select (examples):
SQLService



Windows Security

Enter network credentials

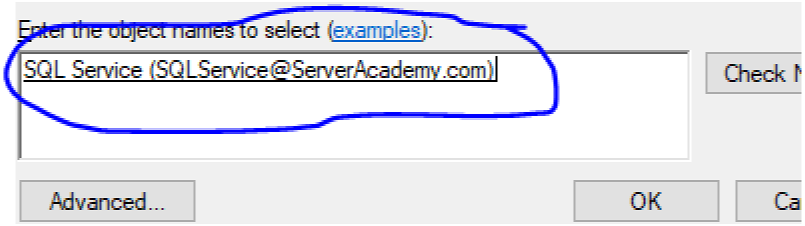
Enter your credentials for an account with permissions for ServerAcademy.com.

For example user, user@example.microsoft.com, or domain\user name

Administrator@ServerAcademy.com

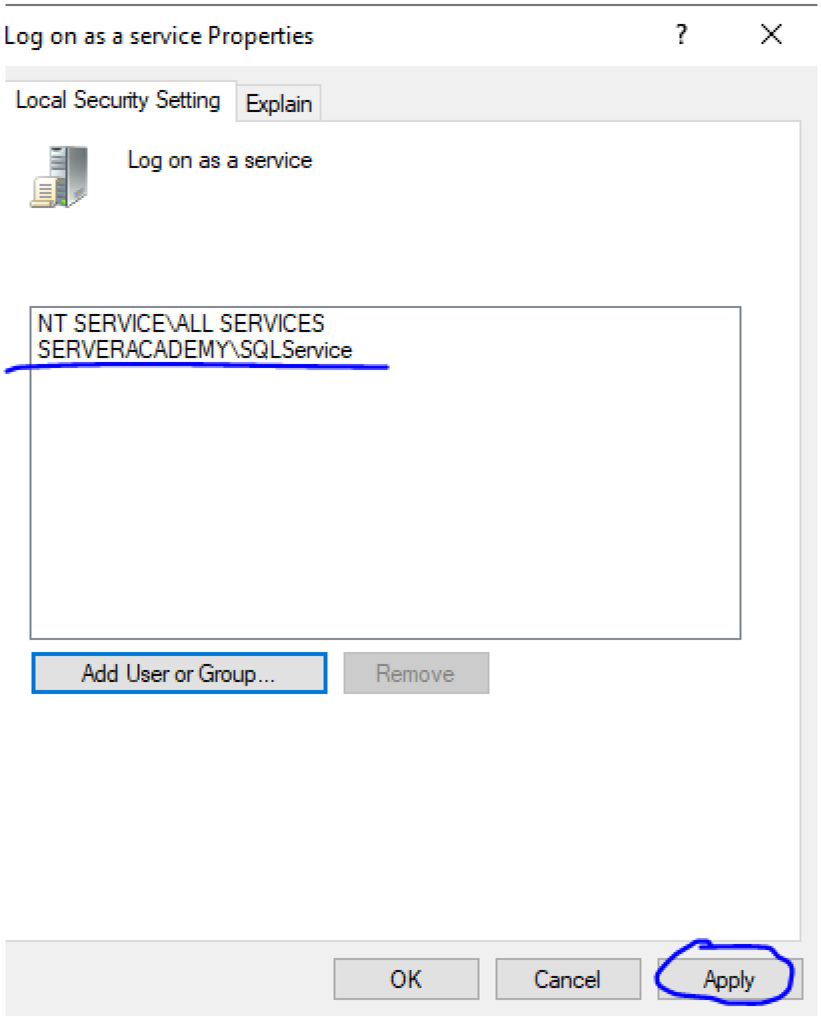
•••••••••••••••••

Domain: ServerAcademy.com

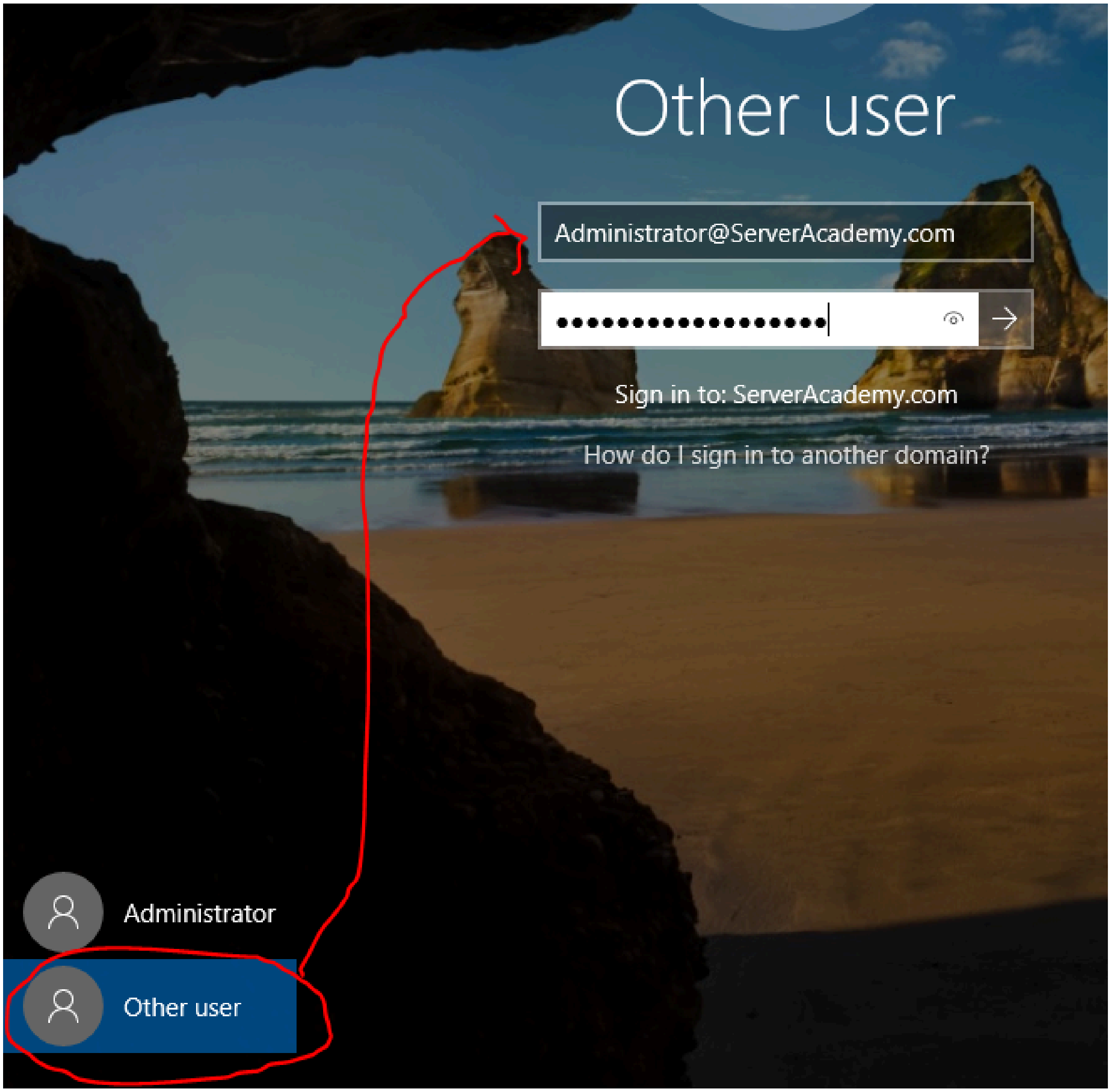


Enter the object names to select (examples):

SQL Service (SQLService@ServerAcademy.com)

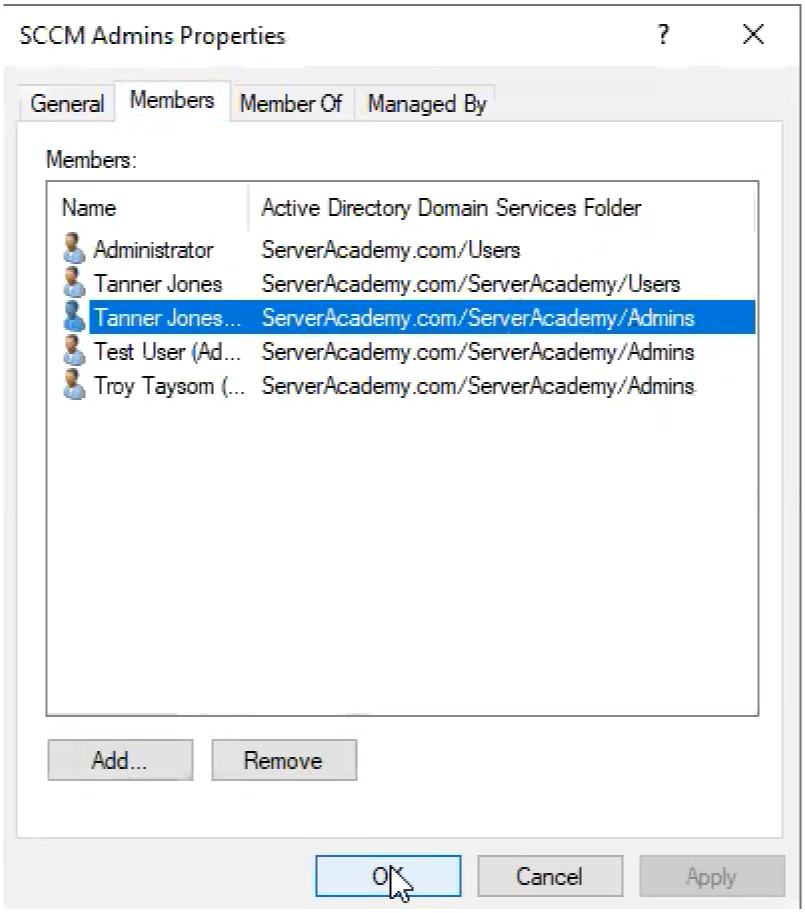


NT SERVICE\ALL SERVICES
SERVERACADEMY\SQLService



Other user
Administrator@ServerAcademy.com
●●●●●●●●●●●●●●●●●●
Sign in to: ServerAcademy.com
How do I sign in to another domain?
Administrator
Other user

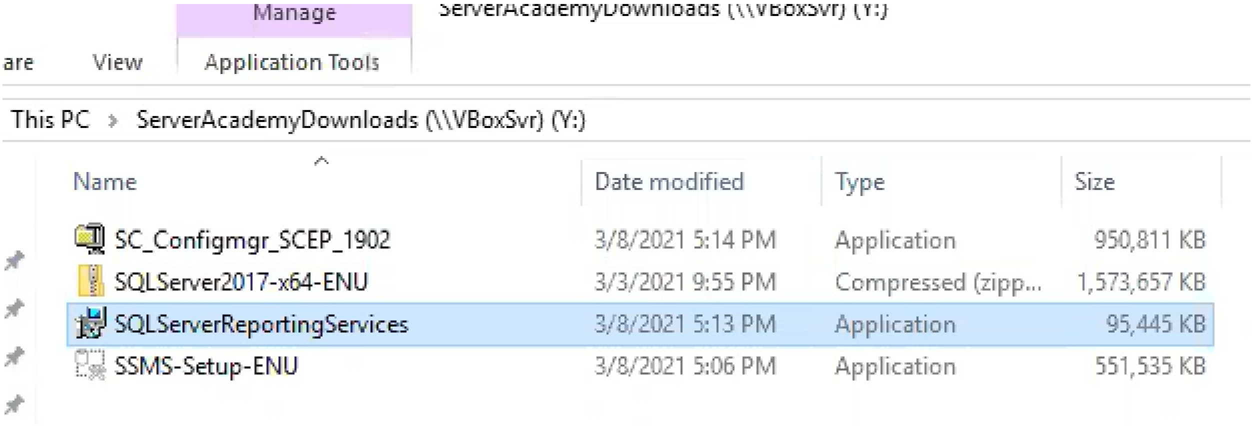
SCCM Admins Group in ServerAcademy OU



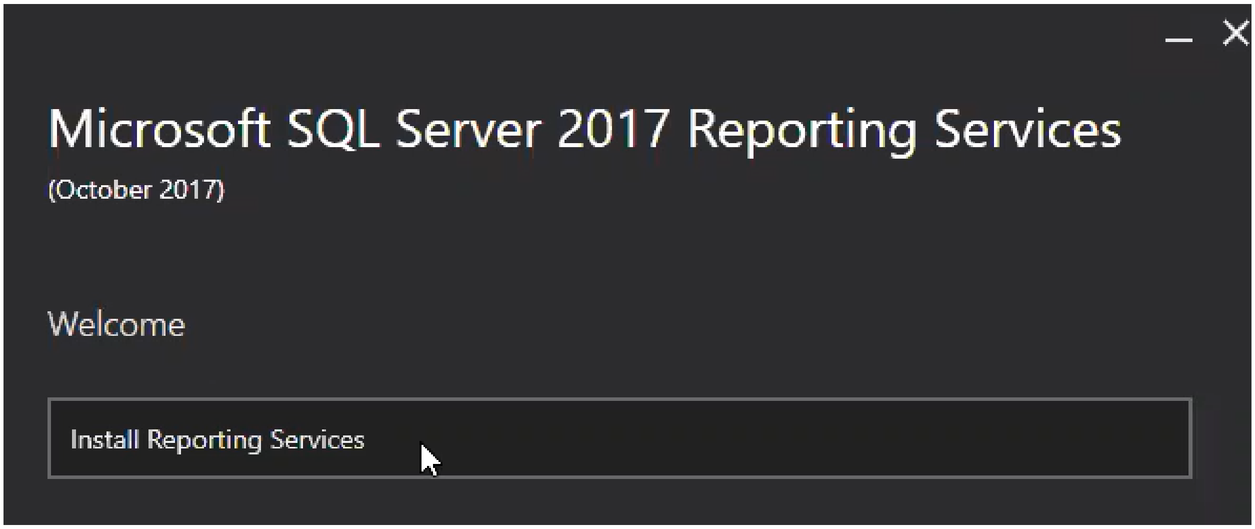
Members:

Name	Active Directory Domain Services Folder
Administrator	ServerAcademy.com/Users
Tanner Jones	ServerAcademy.com/ServerAcademy/Users
Tanner Jones...	ServerAcademy.com/ServerAcademy/Admins
Test User (Ad...	ServerAcademy.com/ServerAcademy/Admins
Troy Taysom (...	ServerAcademy.com/ServerAcademy/Admins

Installing SQL Server 2017

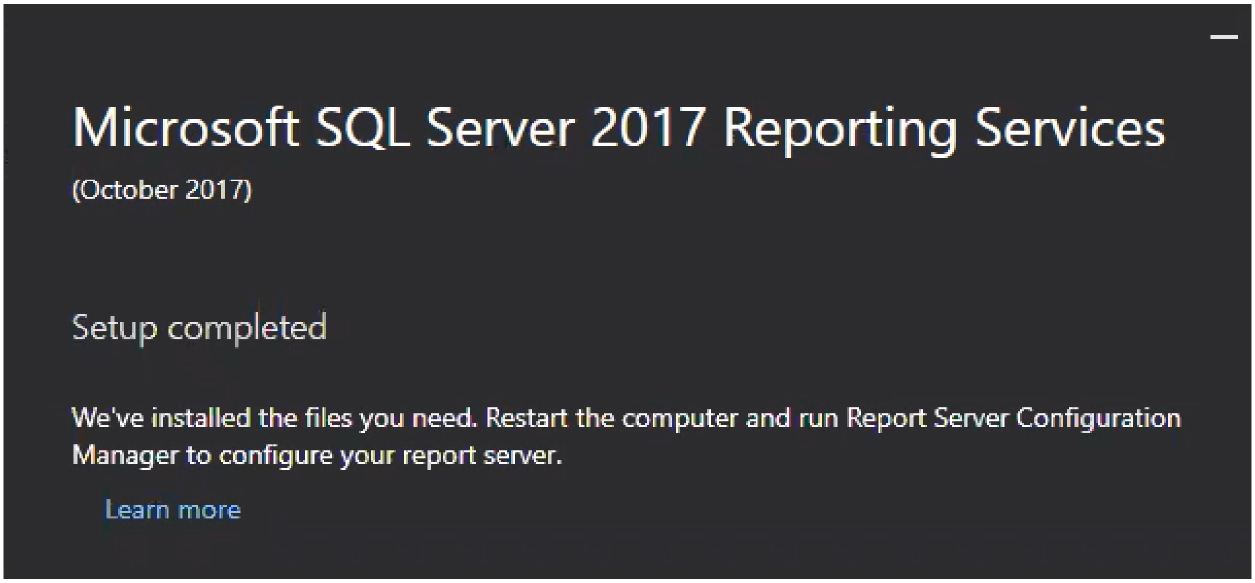

Manage
ServerAcademyDownloads (\\VBoxSvr) (Y:)
are
View
Application Tools
This PC › ServerAcademyDownloads (\\VBoxSvr) (Y:)

Name	Date modified	Type	Size
SC_Configmgr_SCEP_1902	3/8/2021 5:14 PM	Application	950,811 KB
SQLServer2017-x64-ENU	3/3/2021 9:55 PM	Compressed (zipp...	1,573,657 KB
SQLServerReportingServices	3/8/2021 5:13 PM	Application	95,445 KB
SSMS-Setup-ENU	3/8/2021 5:06 PM	Application	551,535 KB


Microsoft SQL Server 2017 Reporting Services

(October 2017)

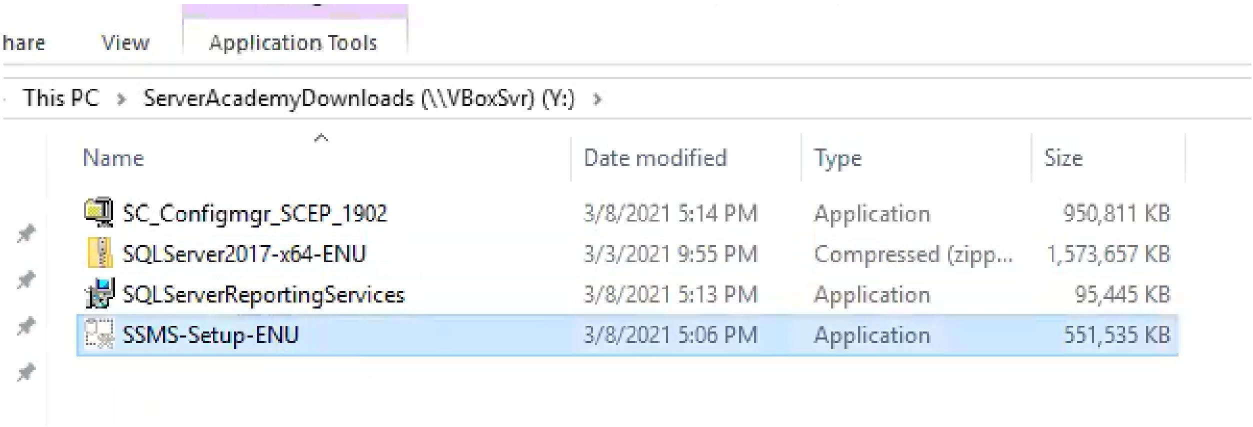
Welcome


Microsoft SQL Server 2017 Reporting Services

(October 2017)

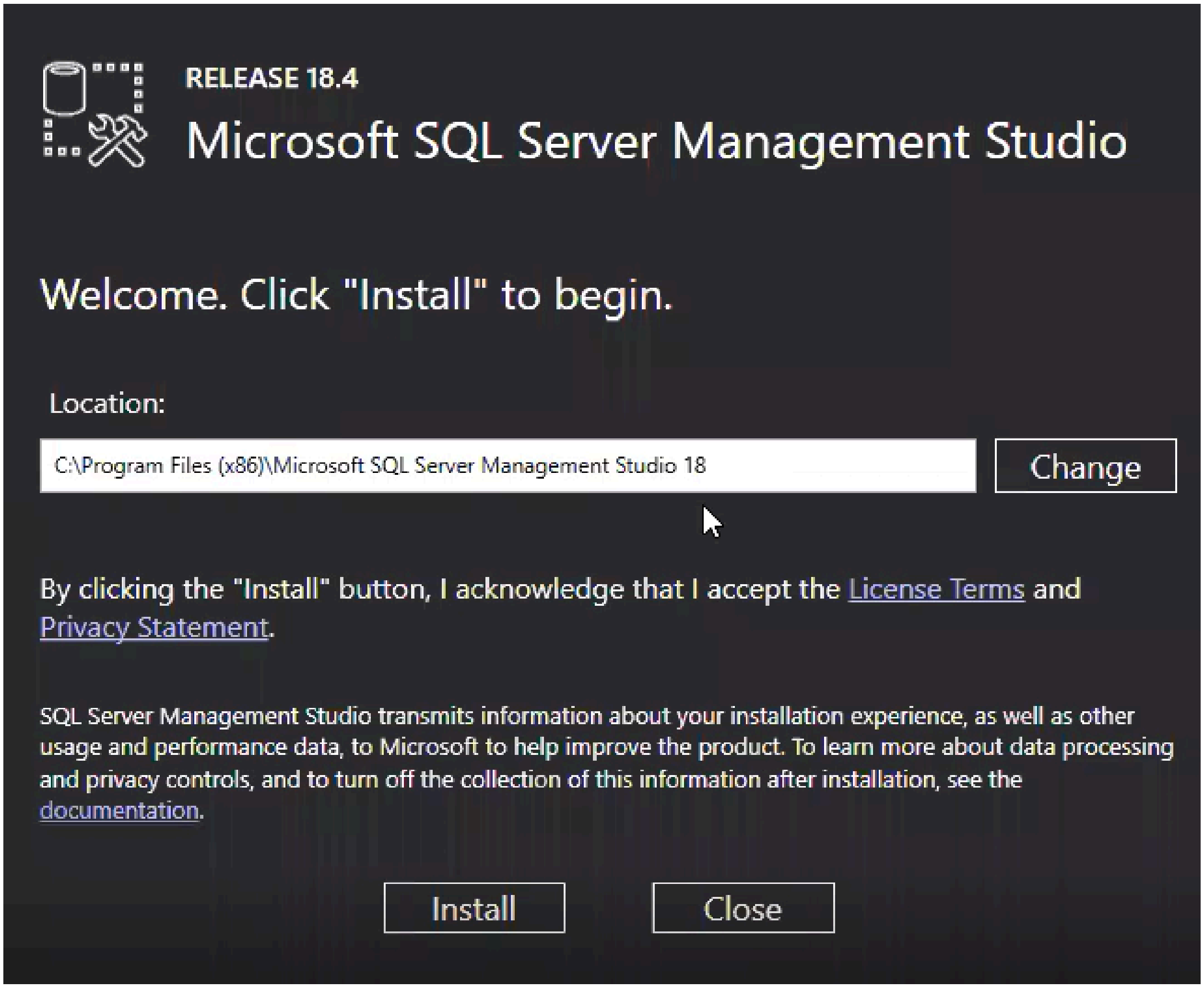
Setup completed

We've installed the files you need. Restart the computer and run Report Server Configuration Manager to configure your report server.



This PC › ServerAcademyDownloads (\\VBoxSvr) (Y:) ›

Name	Date modified	Type	Size
SC_Configmgr_SCEP_1902	3/8/2021 5:14 PM	Application	950,811 KB
SQLServer2017-x64-ENU	3/3/2021 9:55 PM	Compressed (zipp...	1,573,657 KB
SQLServerReportingServices	3/8/2021 5:13 PM	Application	95,445 KB
SSMS-Setup-ENU	3/8/2021 5:06 PM	Application	551,535 KB



RELEASE 18.4

Microsoft SQL Server Management Studio

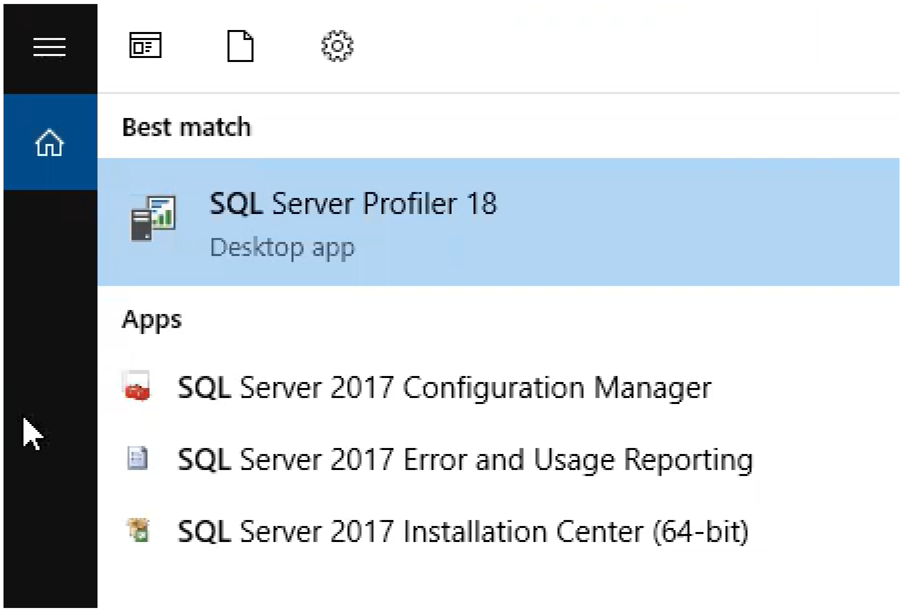
Welcome. Click "Install" to begin.

Location:

C:\Program Files (x86)\Microsoft SQL Server Management Studio 18

By clicking the "Install" button, I acknowledge that I accept the License Terms and Privacy Statement.

SQL Server Management Studio transmits information about your installation experience, as well as other usage and performance data, to Microsoft to help improve the product. To learn more about data processing and privacy controls, and to turn off the collection of this information after installation, see the documentation.



Best match

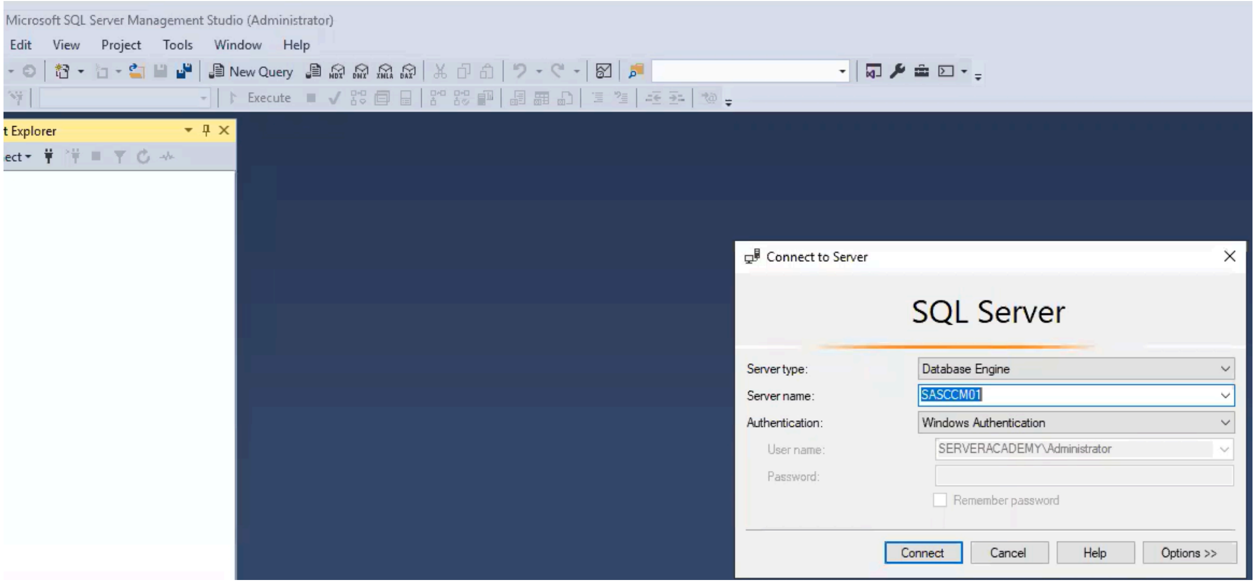
SQL Server Profiler 18
Desktop app

Apps

SQL Server 2017 Configuration Manager

SQL Server 2017 Error and Usage Reporting

SQL Server 2017 Installation Center (64-bit)

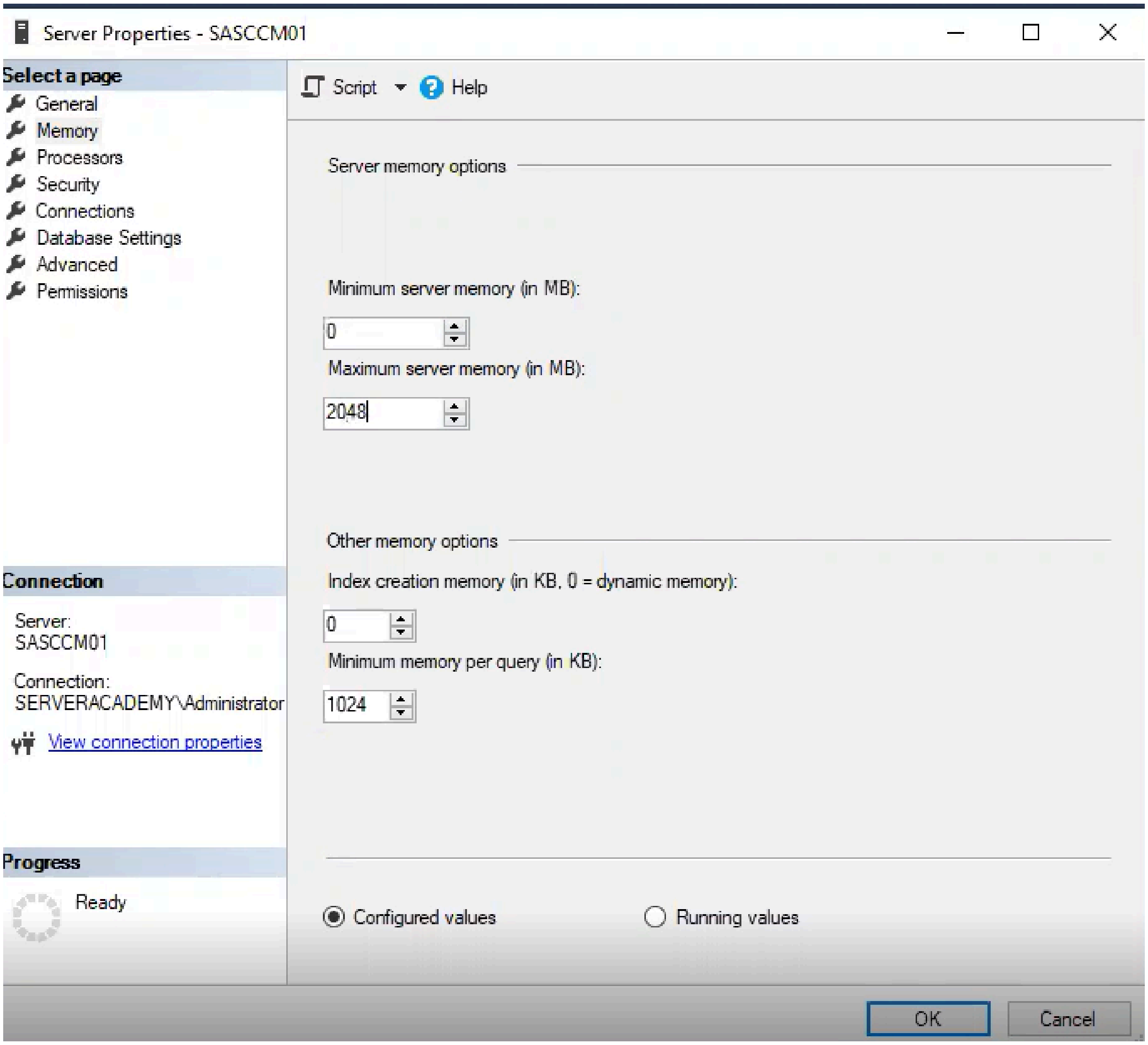


Microsoft SQL Server Management Studio (Administrator)

Connect to Server

SQL Server

Server type: Database Engine
Server name: SASCCM01
Authentication: Windows Authentication
User name: SERVERACADEMY\Administrator
Password:
□ Remember password



Server Properties - SASCCM01

Server memory options

Minimum server memory (in MB): 0

Maximum server memory (in MB): 2048

Other memory options

Index creation memory (in KB, 0 = dynamic memory): 0

Minimum memory per query (in KB): 1024

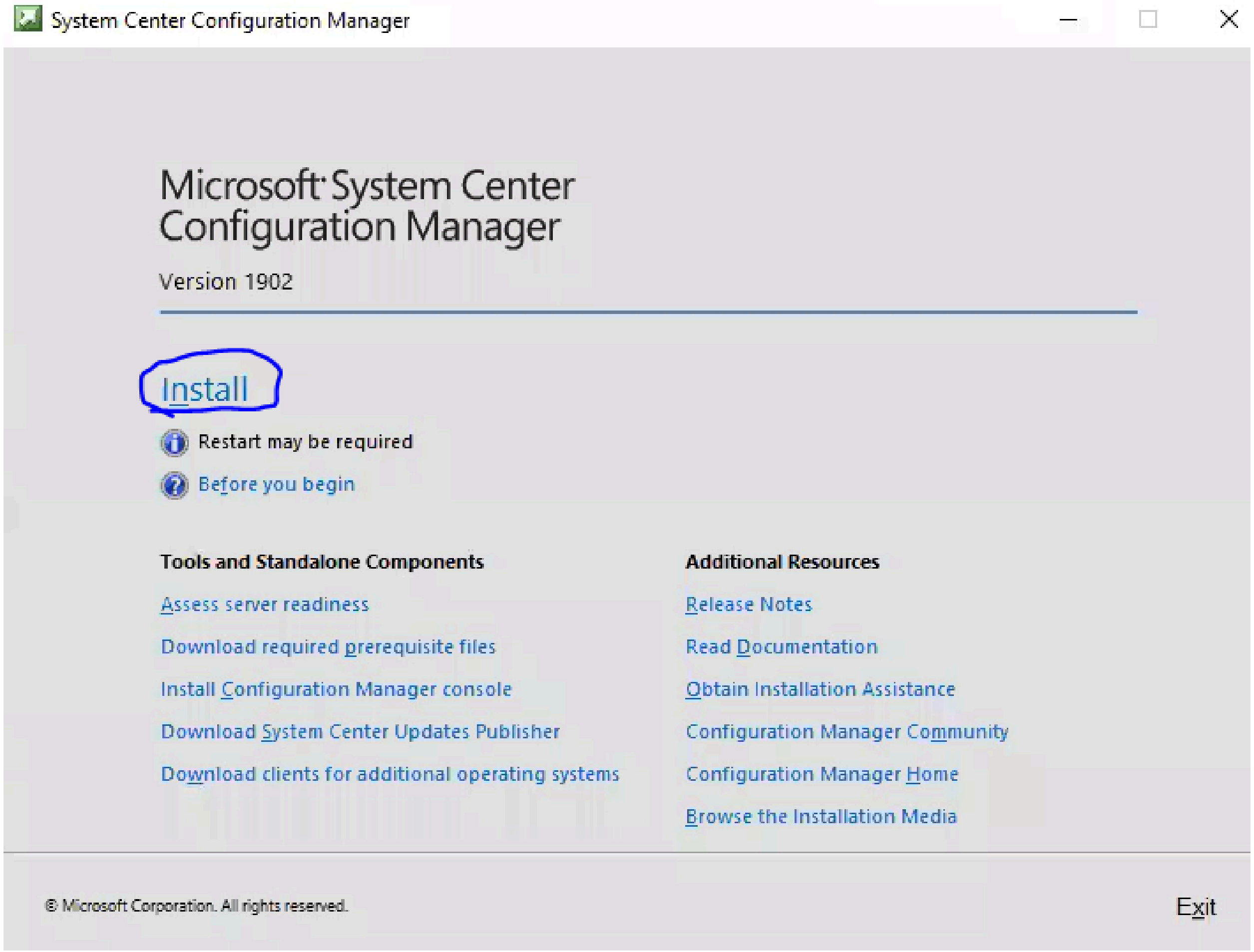
Connection

Server:
SASCCM01

Connection:
SERVERACADEMY\Administrator

● Configured values ○ Running values

Installing Configuration Manager on SCCM01



System Center Configuration Manager

Microsoft System Center
Configuration Manager

Version 1902

Install

Restart may be required

Before you begin

Tools and Standalone Components

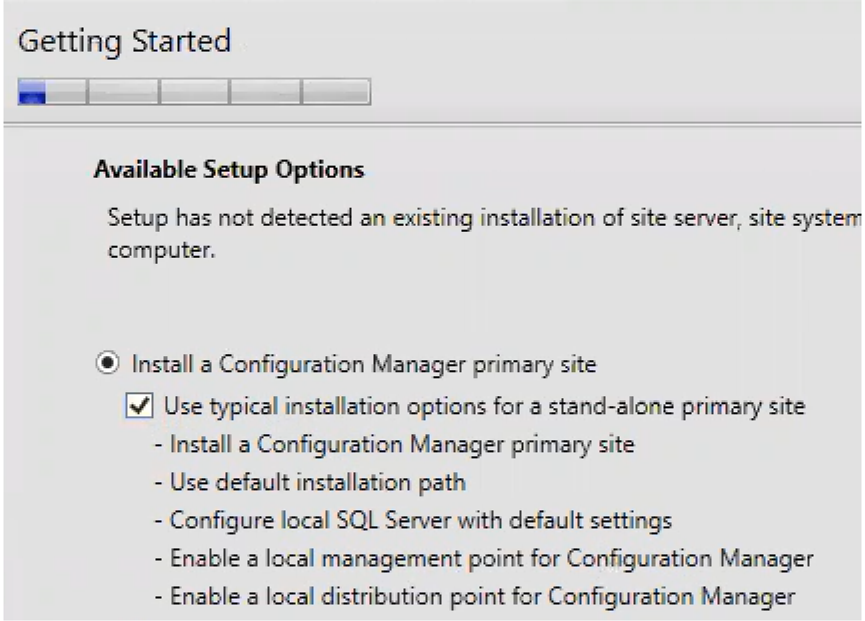
- Assess server readiness
- Download required prerequisite files
- Install Configuration Manager console
- Download System Center Updates Publisher
- Download clients for additional operating systems

Additional Resources

- Release Notes
- Read Documentation
- Obtain Installation Assistance
- Configuration Manager Community
- Configuration Manager Home
- Browse the Installation Media

© Microsoft Corporation. All rights reserved.

Exit



Getting Started

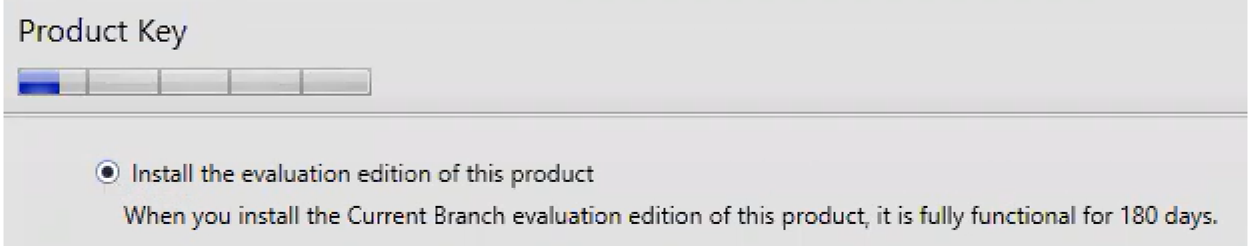
Available Setup Options

Setup has not detected an existing installation of site server, site system
computer.

● Install a Configuration Manager primary site

☑ Use typical installation options for a stand-alone primary site

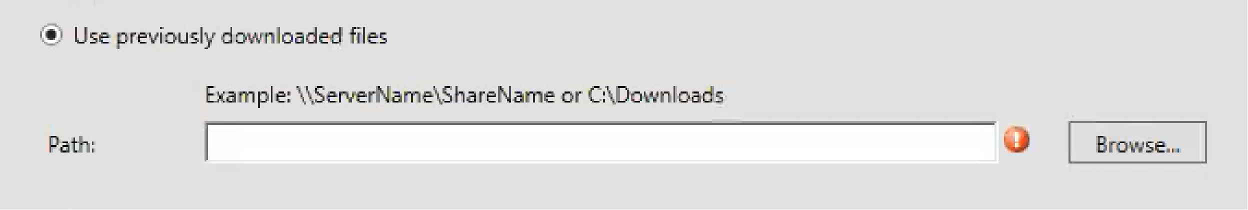
- Install a Configuration Manager primary site
- Use default installation path
- Configure local SQL Server with default settings
- Enable a local management point for Configuration Manager
- Enable a local distribution point for Configuration Manager



Product Key

● Install the evaluation edition of this product

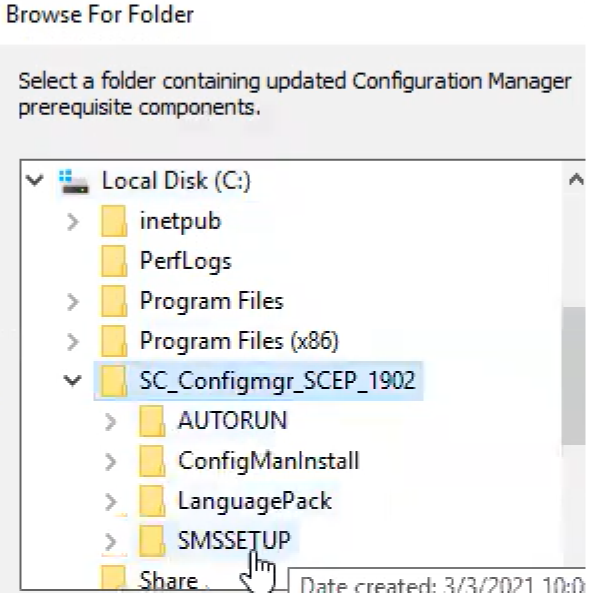
When you install the Current Branch evaluation edition of this product, it is fully functional for 180 days.



● Use previously downloaded files

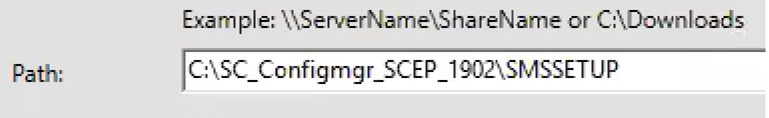
Example: \\ServerName\ShareName or C:\Downloads

Path:



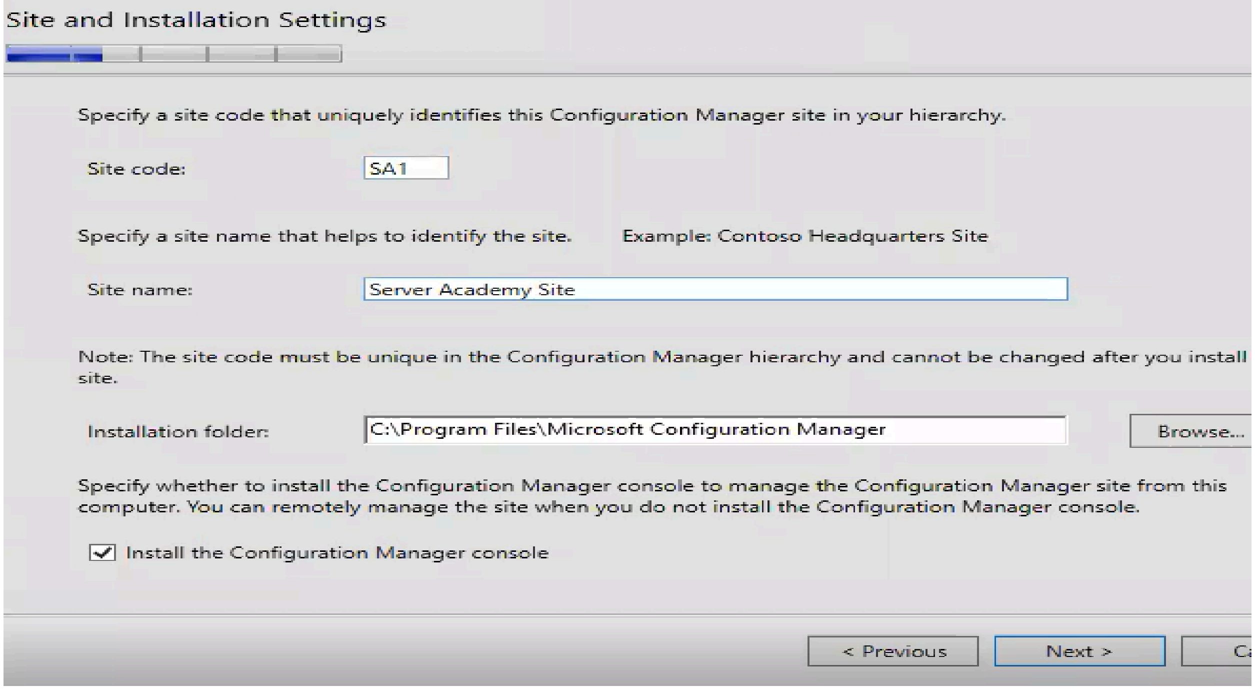
Browse For Folder

Select a folder containing updated Configuration Manager prerequisite components.



Example: \\ServerName\ShareName or C:\Downloads

Path: C:\SC_Configmgr_SCEP_1902\SMSSETUP



Site and Installation Settings

Specify a site code that uniquely identifies this Configuration Manager site in your hierarchy.

Site code: SA1

Specify a site name that helps to identify the site. Example: Contoso Headquarters Site

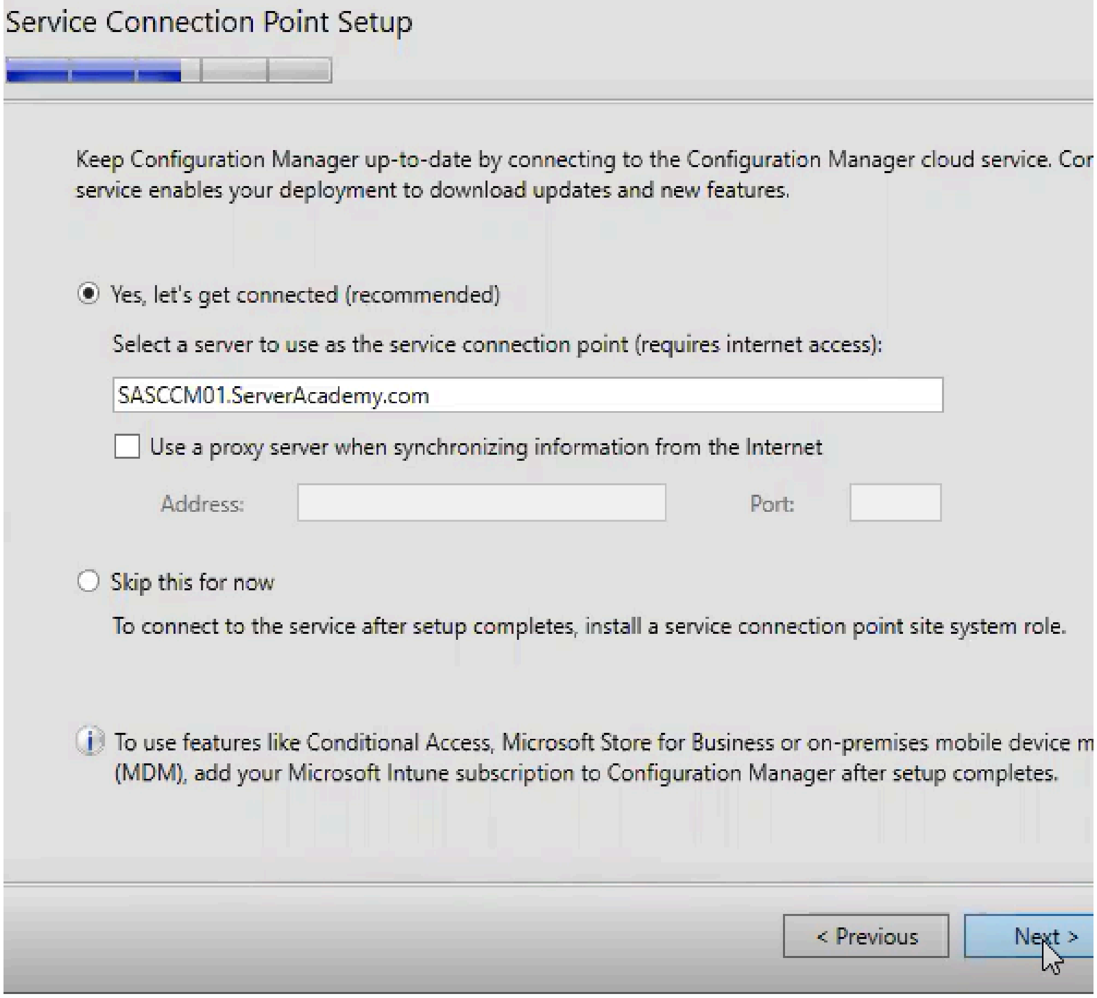
Site name: Server Academy Site

Note: The site code must be unique in the Configuration Manager hierarchy and cannot be changed after you install site.

Installation folder: C:\Program Files\Microsoft Configuration Manager

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



Service Connection Point Setup

Keep Configuration Manager up-to-date by connecting to the Configuration Manager cloud service. Cor 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):

SASCCM01.ServerAcademy.com

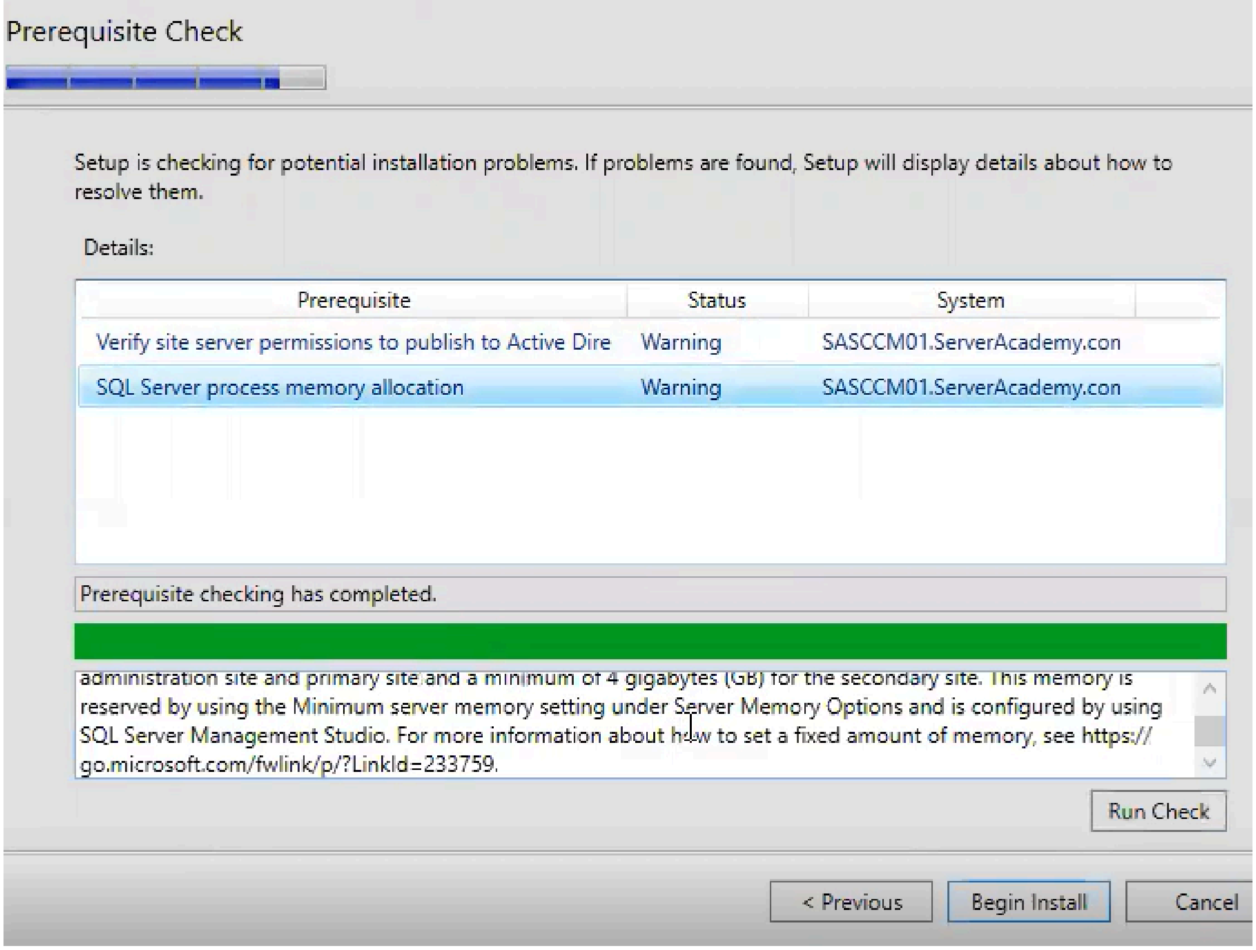
□ Use a proxy server when synchronizing information from the Internet

Address: Port:

○ Skip this for now

To connect to the service after setup completes, install a service connection point site system role.

To use features like Conditional Access, Microsoft Store for Business or on-premises mobile device m (MDM), add your Microsoft Intune subscription to Configuration Manager after setup completes.



Prerequisite Check

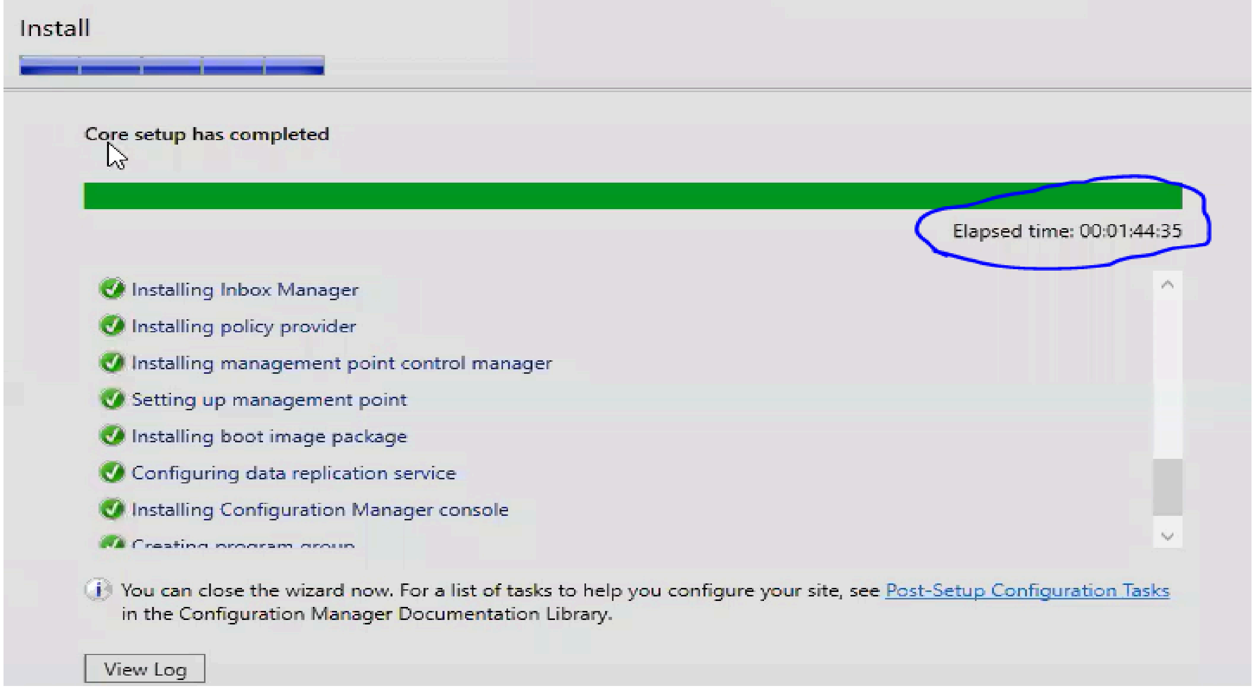
Setup is checking for potential installation problems. If problems are found, Setup will display details about how to resolve them.

Details:

Prerequisite	Status	System
Verify site server permissions to publish to Active Dire	Warning	SASCCM01.ServerAcademy.con
SQL Server process memory allocation	Warning	SASCCM01.ServerAcademy.con

Prerequisite checking has completed.

administration site and primary site and a minimum of 4 gigabytes (GB) for the secondary site. This memory is reserved by using the Minimum server memory setting under Server Memory Options and is configured by using SQL Server Management Studio. For more information about how to set a fixed amount of memory, see https://go.microsoft.com/fwlink/p/?LinkId=233759.



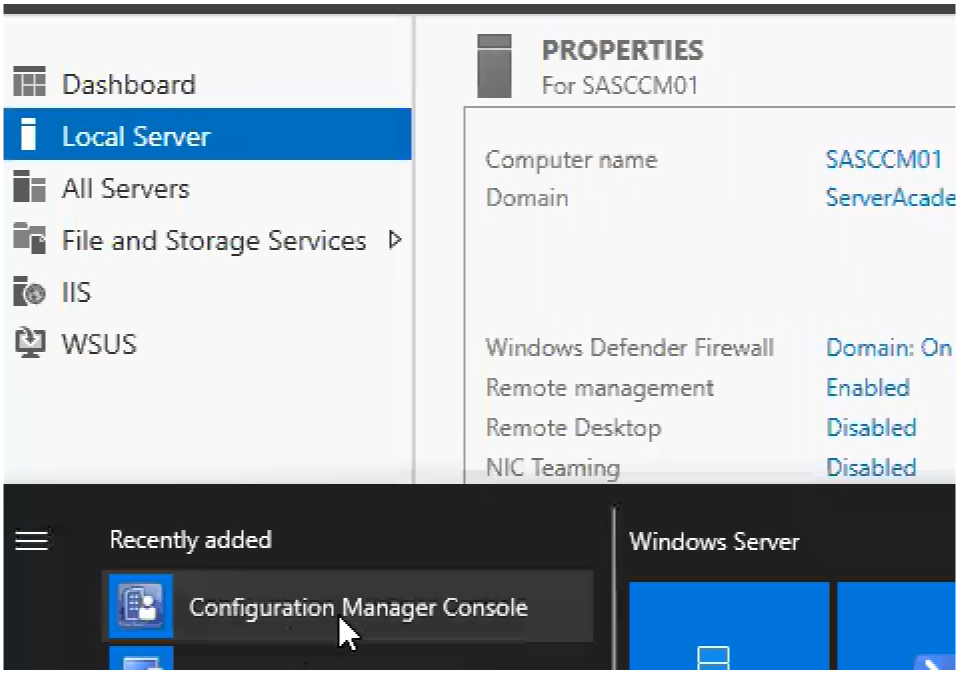
Install

Core setup has completed

Elapsed time: 00:01:44:35

- ✓ Installing Inbox Manager
- ✓ Installing policy provider
- ✓ Installing management point control manager
- ✓ Setting up management point
- ✓ Installing boot image package
- ✓ Configuring data replication service
- ✓ Installing Configuration Manager console
- ✓ Creating program group

You can close the wizard now. For a list of tasks to help you configure your site, see Post-Setup Configuration Tasks in the Configuration Manager Documentation Library.

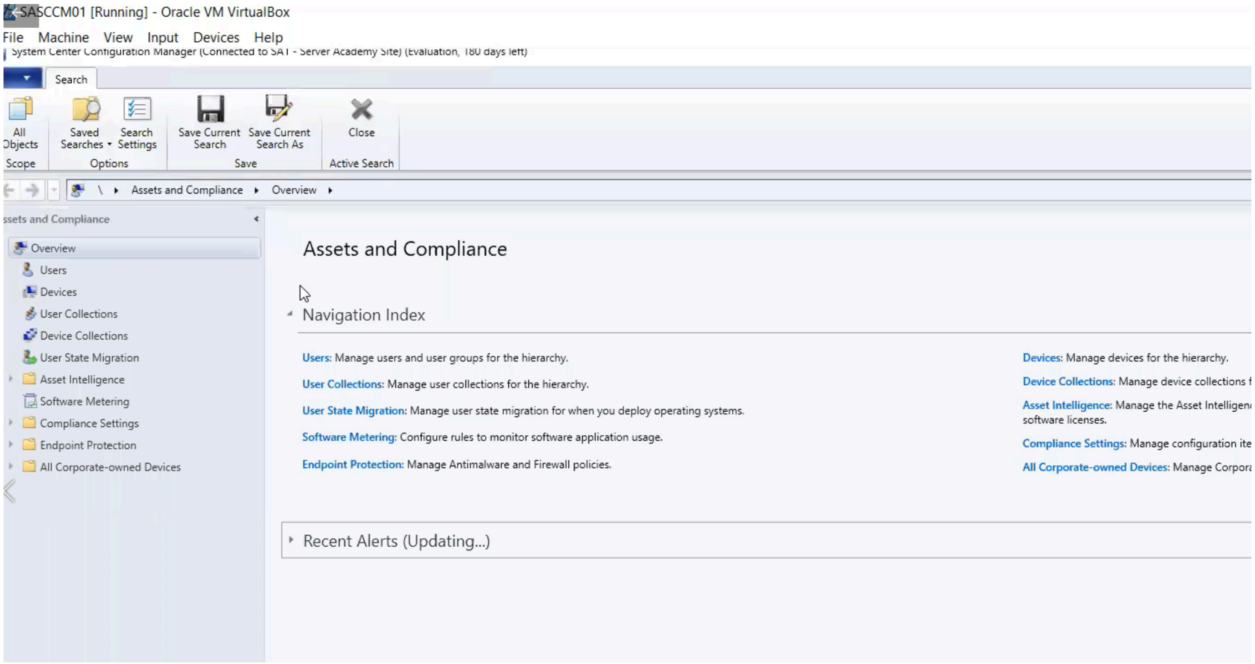


PROPERTIES
For SASCCM01

Computer name SASCCM01
Domain ServerAcade

Windows Defender Firewall Domain: On
Remote management Enabled
Remote Desktop Disabled
NIC Teaming Disabled

Installed Successfully



System Center Configuration Manager (Connected to SA1 - Server Academy Site) (Evaluation, 180 days left)

Assets and Compliance

Navigation Index

Users: Manage users and user groups for the hierarchy.

User Collections: Manage user collections for the hierarchy.

User State Migration: Manage user state migration for when you deploy operating systems.

Software Metering: Configure rules to monitor software application usage.

Endpoint Protection: Manage Antimalware and Firewall policies.

Devices: Manage devices for the hierarchy.

Device Collections: Manage device collections f

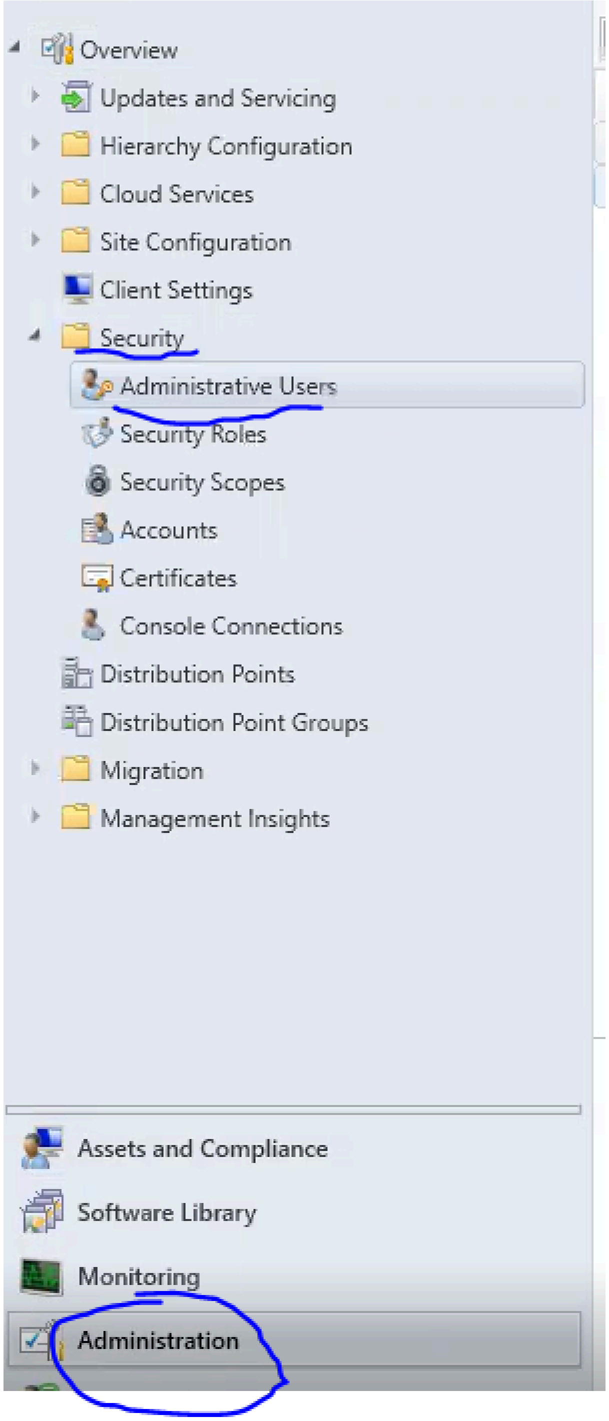
Asset Intelligence: Manage the Asset Intelligen
software licenses.

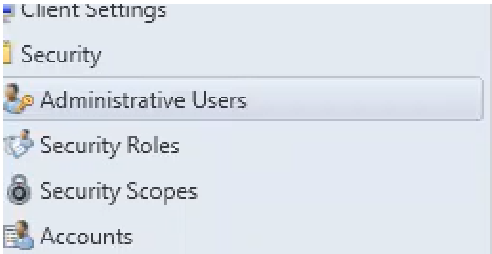
Compliance Settings: Manage configuration ite

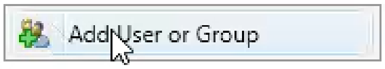
All Corporate-owned Devices: Manage Corpora

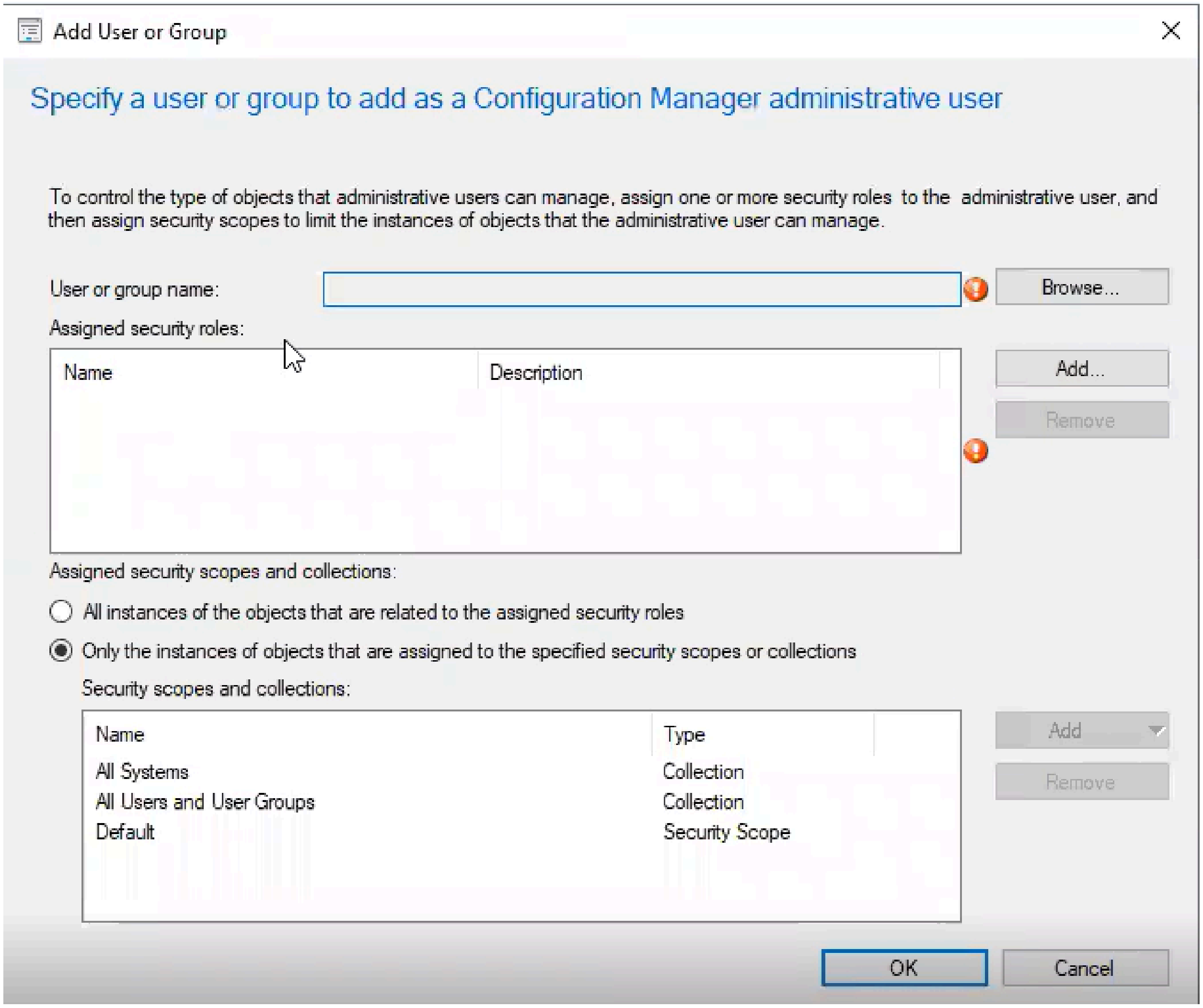
Recent Alerts (Updating...)

Creating/Adding Security Groups In SCCM









Add User or Group

Specify a user or group to add as a Configuration Manager administrative user

To control the type of objects that administrative users can manage, assign one or more security roles to the administrative user, and then assign security scopes to limit the instances of objects that the administrative user can manage.

User or group name: [Browse...]

Assigned security roles:

Name	Description

[Add...] [Remove]

Assigned security scopes and collections:

○ All instances of the objects that are related to the assigned security roles

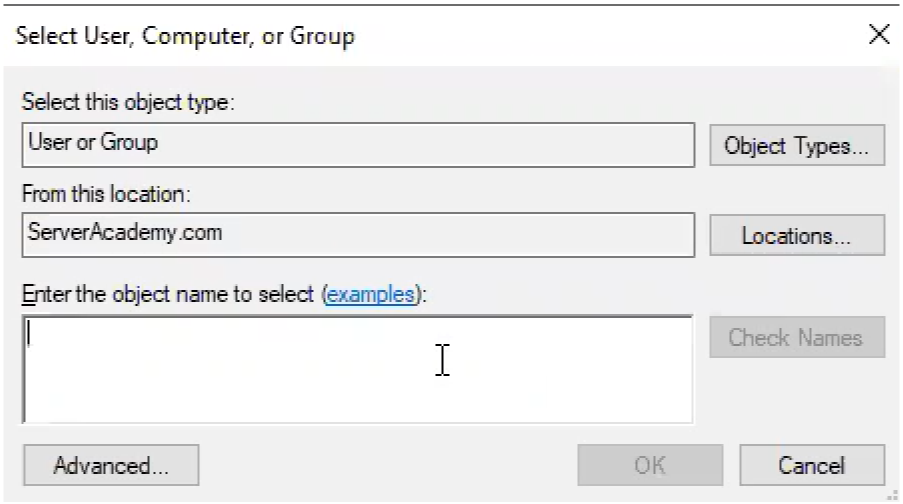
● Only the instances of objects that are assigned to the specified security scopes or collections

Security scopes and collections:

Name	Type
All Systems	Collection
All Users and User Groups	Collection
Default	Security Scope

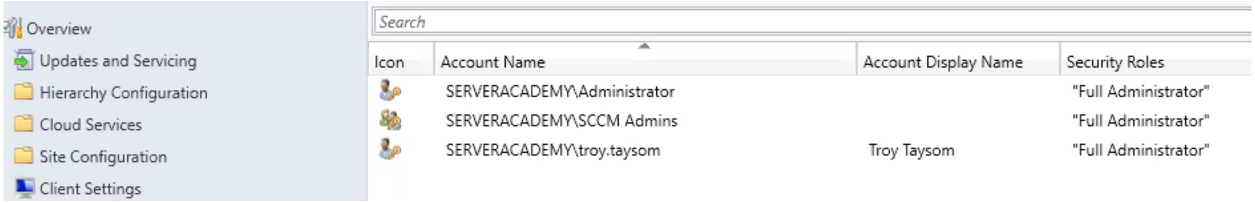
[Add] [Remove]

[OK] [Cancel]


Select User, Computer, or Group
Object Types...
Locations...
Enter the object name to select (examples):
Check Names
Advanced...
OK
Cancel

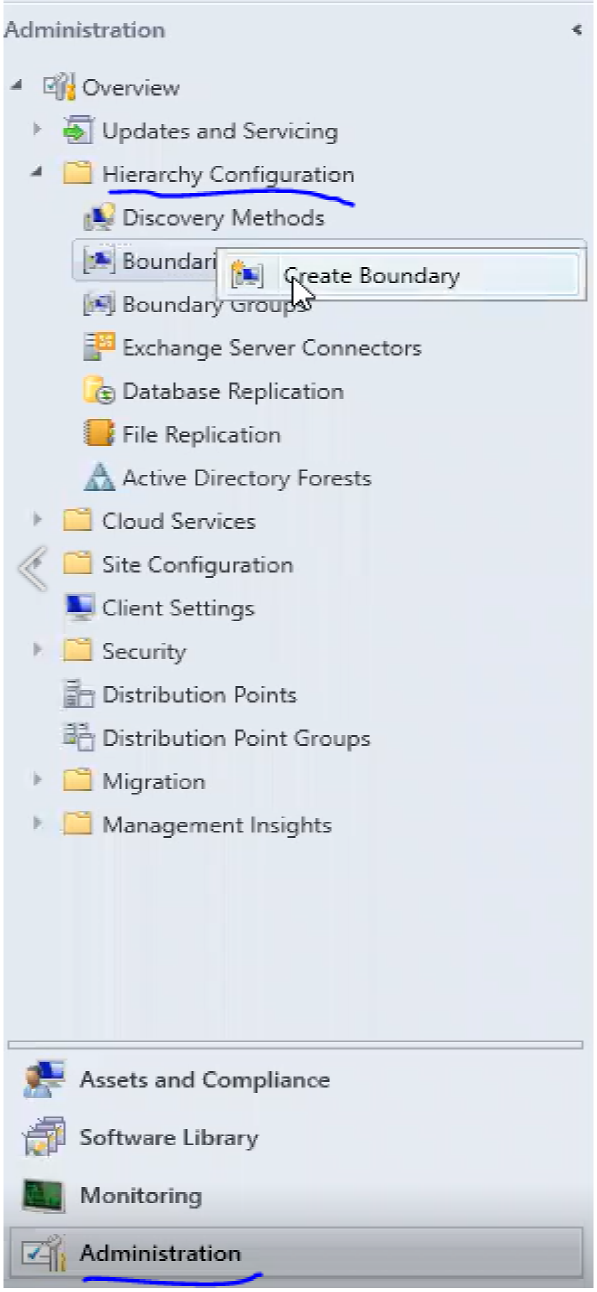
Select this object type: User or Group

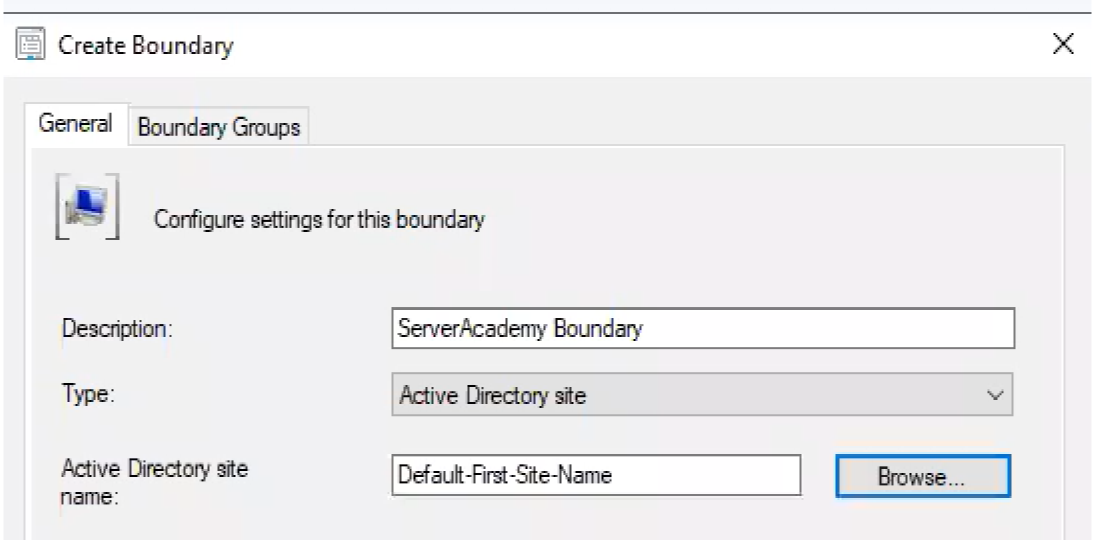
From this location: ServerAcademy.com



Icon	Account Name	Account Display Name	Security Roles
	SERVERACADEMY\Administrator		"Full Administrator"
	SERVERACADEMY\SCCM Admins		"Full Administrator"
	SERVERACADEMY\troy.taysom	Troy Taysom	"Full Administrator"

Creating Boundary Groups in SCCM



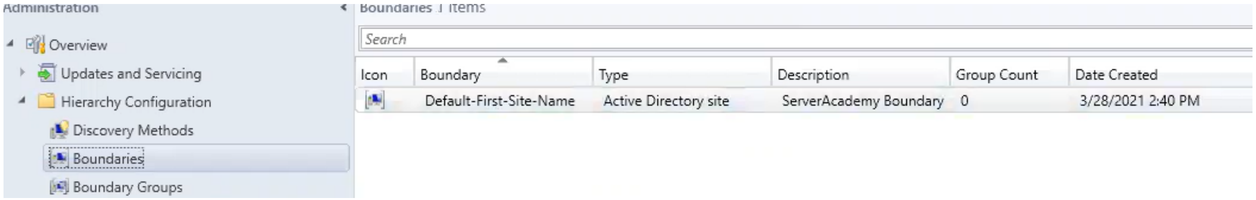


Configure settings for this boundary

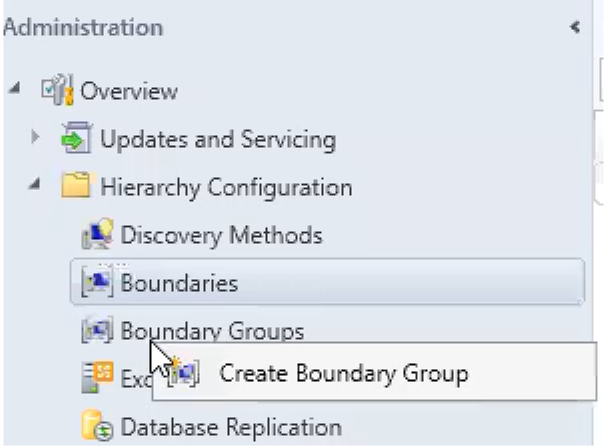
Description: ServerAcademy Boundary

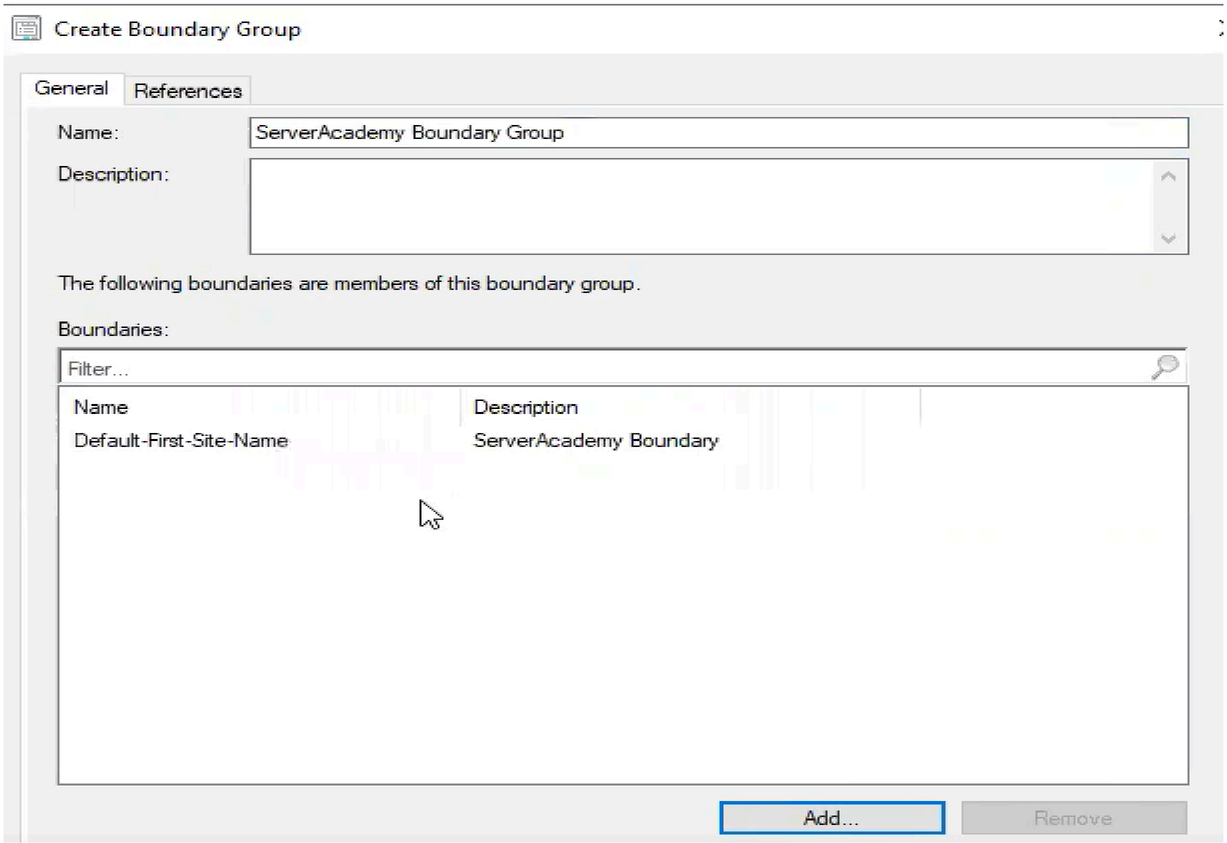
Type: Active Directory site

Active Directory site name: Default-First-Site-Name



Icon	Boundary	Type	Description	Group Count	Date Created
	Default-First-Site-Name	Active Directory site	ServerAcademy Boundary	0	3/28/2021 2:40 PM





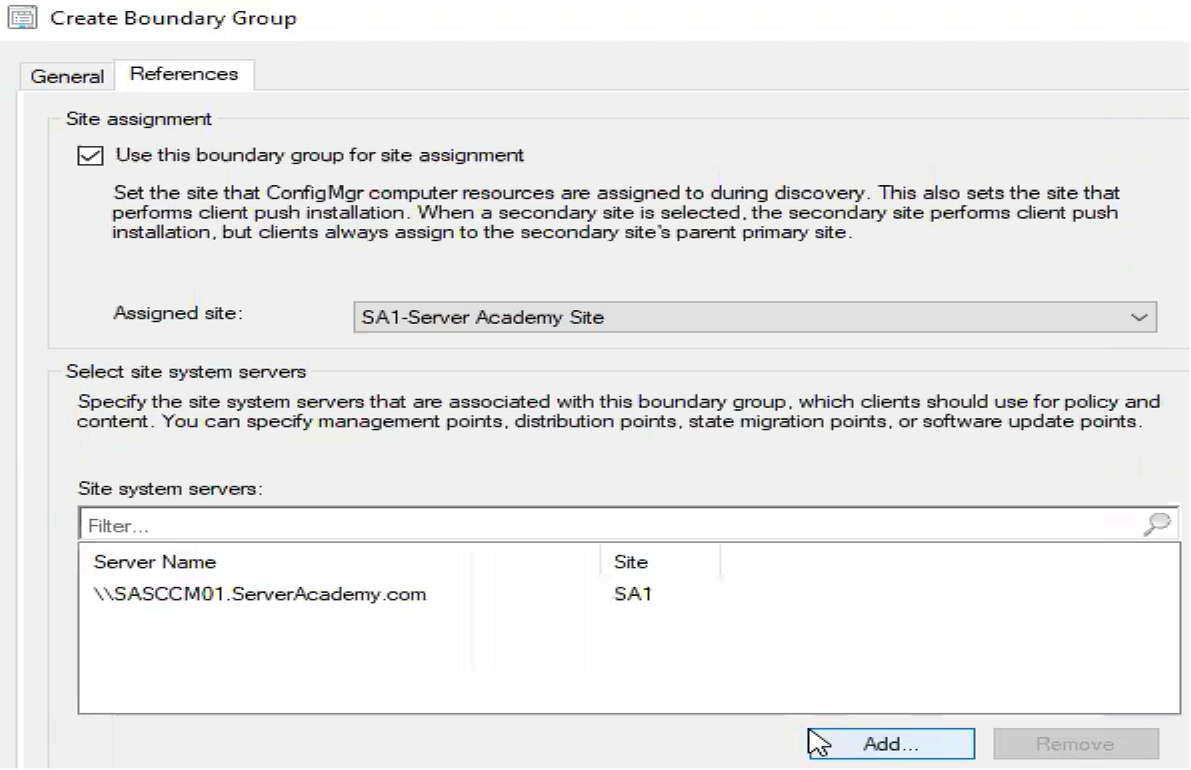
Name: ServerAcademy Boundary Group

Description:

The following boundaries are members of this boundary group.

Boundaries:

Name	Description
Default-First-Site-Name	ServerAcademy Boundary



Site assignment

☑ Use this boundary group for site assignment

Set the site that ConfigMgr computer resources are assigned to during discovery. This also sets the site that performs client push installation. When a secondary site is selected, the secondary site performs client push installation, but clients always assign to the secondary site's parent primary site.

Assigned site: SA1-Server Academy Site

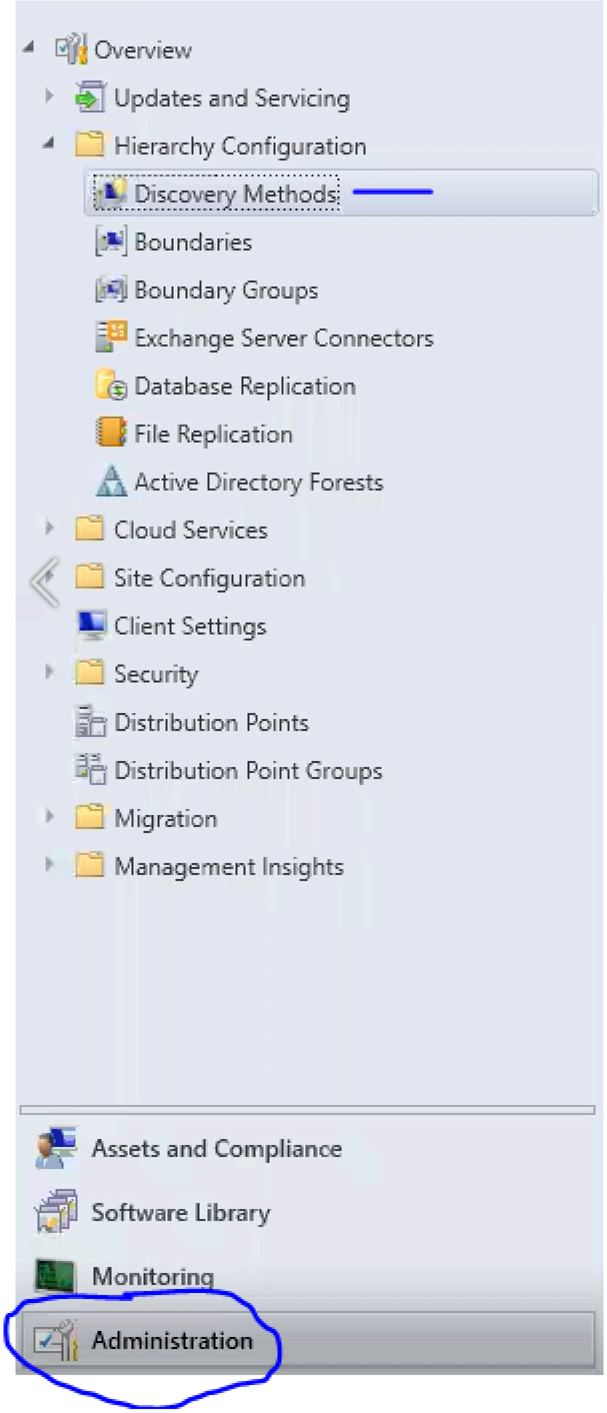
Select site system servers

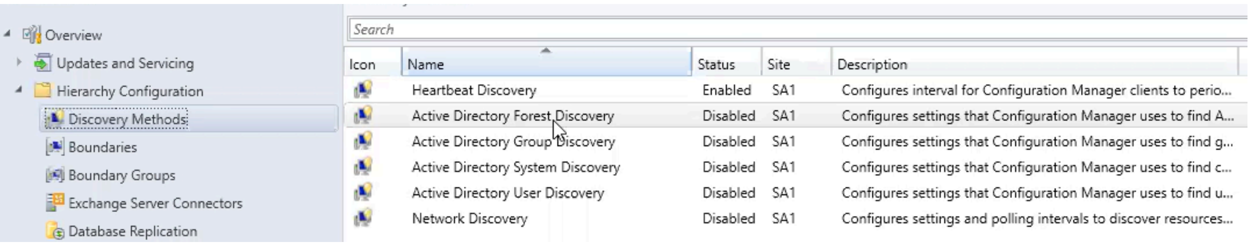
Specify the site system servers that are associated with this boundary group, which clients should use for policy and content. You can specify management points, distribution points, state migration points, or software update points.

Site system servers:

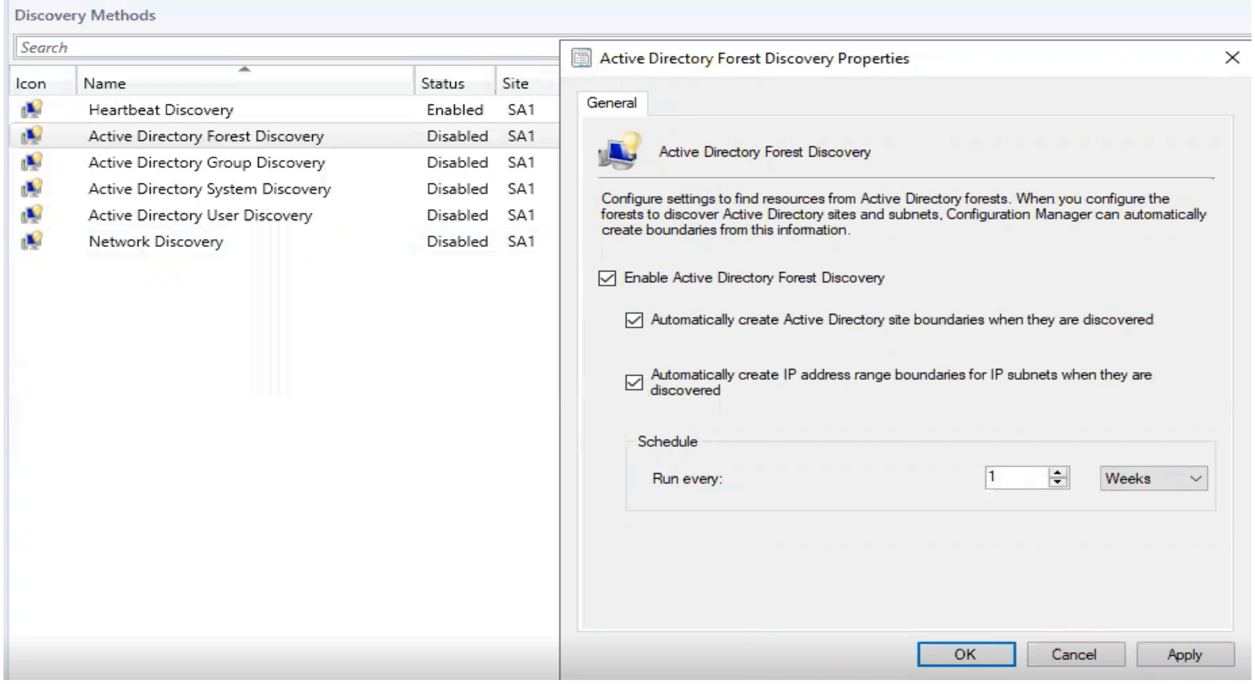
Server Name	Site
\\SASCCM01.ServerAcademy.com	SA1

Enabling Client and User Discovery on SCCM





Icon	Name	Status	Site	Description
	Heartbeat Discovery	Enabled	SA1	Configures interval for Configuration Manager clients to perio...
	Active Directory Forest Discovery	Disabled	SA1	Configures settings that Configuration Manager uses to find A...
	Active Directory Group Discovery	Disabled	SA1	Configures settings that Configuration Manager uses to find g...
	Active Directory System Discovery	Disabled	SA1	Configures settings that Configuration Manager uses to find c...
	Active Directory User Discovery	Disabled	SA1	Configures settings that Configuration Manager uses to find u...
	Network Discovery	Disabled	SA1	Configures settings and polling intervals to discover resources...



Icon	Name	Status	Site
	Heartbeat Discovery	Enabled	SA1
	Active Directory Forest Discovery	Disabled	SA1
	Active Directory Group Discovery	Disabled	SA1
	Active Directory System Discovery	Disabled	SA1
	Active Directory User Discovery	Disabled	SA1
	Network Discovery	Disabled	SA1

Active Directory Forest Discovery Properties

General

Active Directory Forest Discovery

Configure settings to find resources from Active Directory forests. When you configure the forests to discover Active Directory sites and subnets, Configuration Manager can automatically create boundaries from this information.

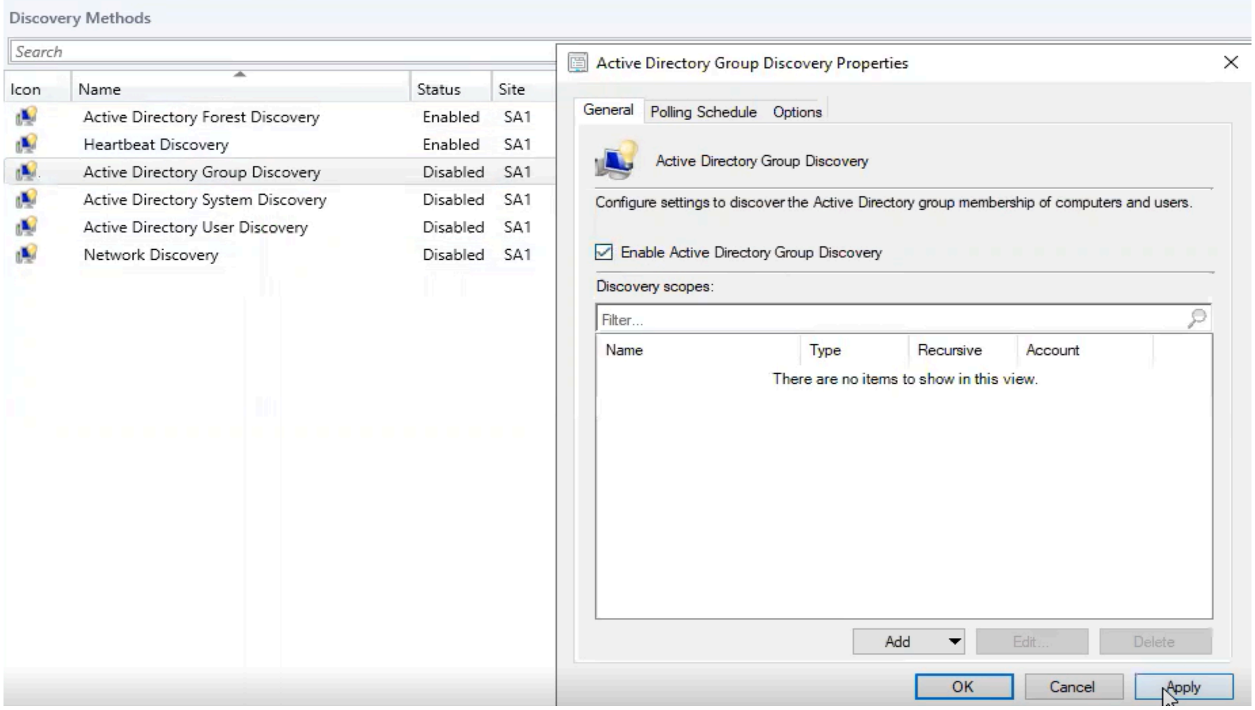
☑ Enable Active Directory Forest Discovery

☑ Automatically create Active Directory site boundaries when they are discovered

☑ Automatically create IP address range boundaries for IP subnets when they are discovered

Schedule

Run every: 1 Weeks



Icon	Name	Status	Site
	Active Directory Forest Discovery	Enabled	SA1
	Heartbeat Discovery	Enabled	SA1
	Active Directory Group Discovery	Disabled	SA1
	Active Directory System Discovery	Disabled	SA1
	Active Directory User Discovery	Disabled	SA1
	Network Discovery	Disabled	SA1

Active Directory Group Discovery Properties

General | Polling Schedule | Options

Active Directory Group Discovery

Configure settings to discover the Active Directory group membership of computers and users.

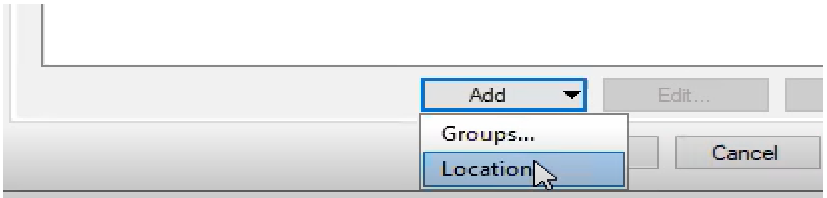
☑ Enable Active Directory Group Discovery

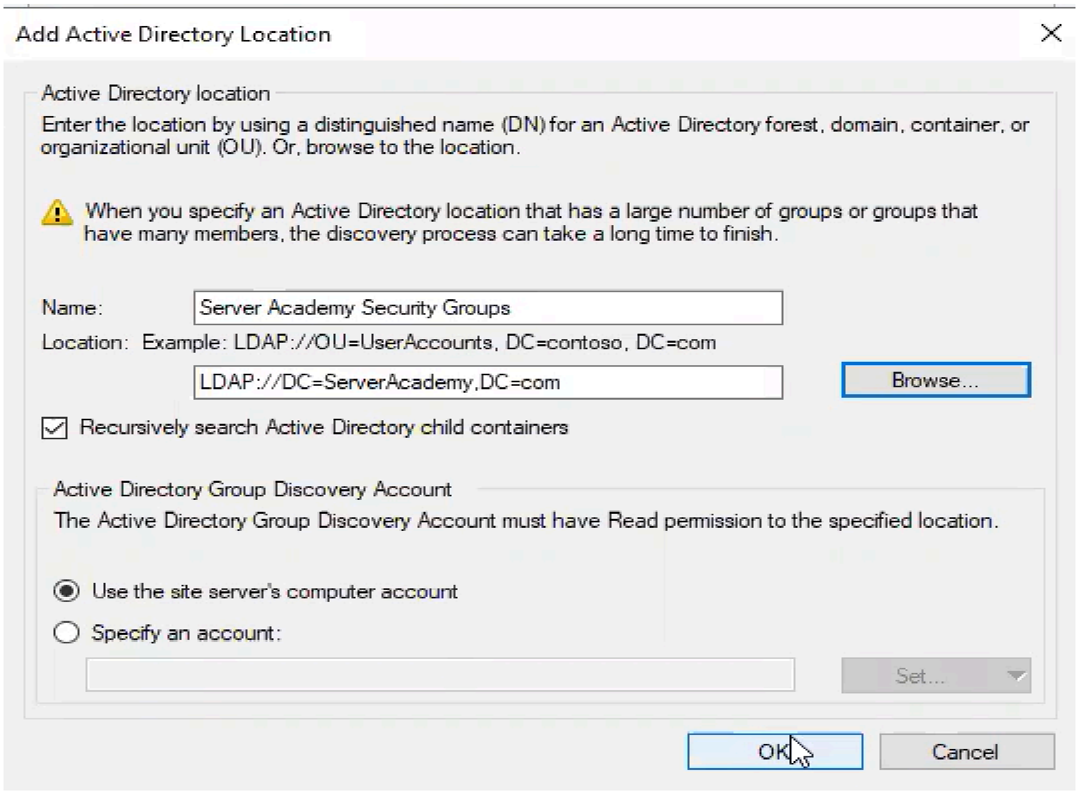
Discovery scopes:

Filter...

Name	Type	Recursive	Account

There are no items to show in this view.





Add Active Directory Location

Active Directory location

Enter the location by using a distinguished name (DN) for an Active Directory forest, domain, container, or organizational unit (OU). Or, browse to the location.

⚠ When you specify an Active Directory location that has a large number of groups or groups that have many members, the discovery process can take a long time to finish.

Name: Server Academy Security Groups

Location: Example: LDAP://OU=UserAccounts, DC=contoso, DC=com

LDAP://DC=ServerAcademy,DC=com

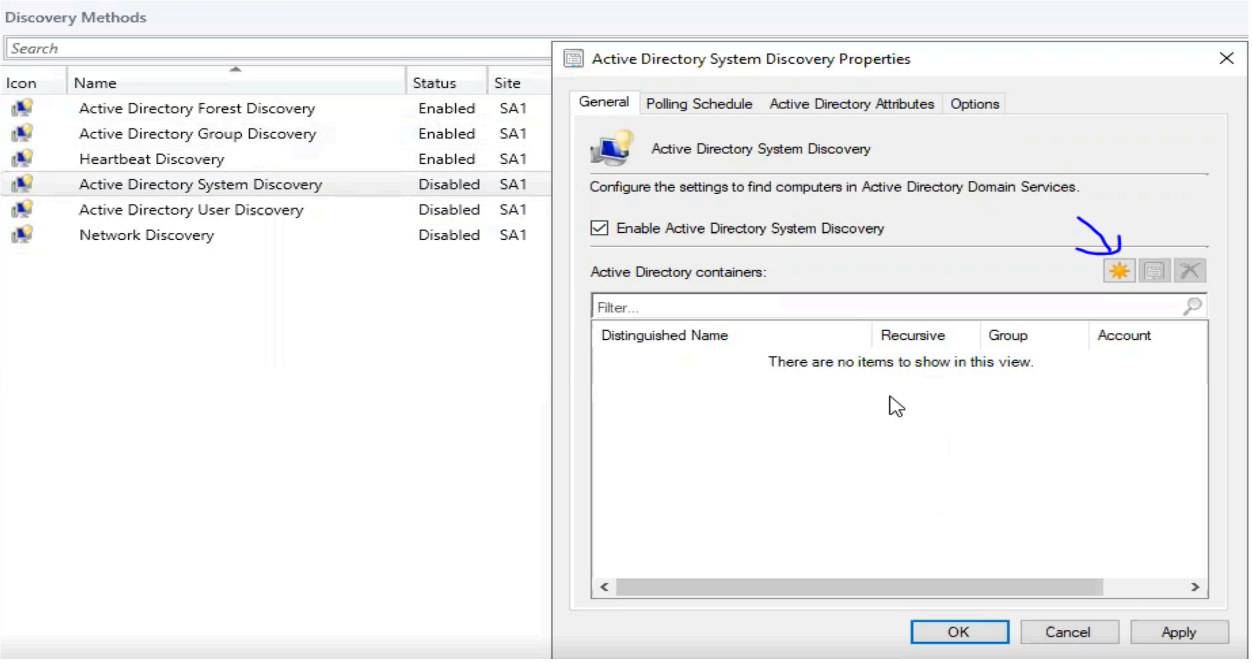
☑ Recursively search Active Directory child containers

Active Directory Group Discovery Account

The Active Directory Group Discovery Account must have Read permission to the specified location.

● Use the site server's computer account

○ Specify an account:



Discovery Methods

Icon	Name	Status	Site
	Active Directory Forest Discovery	Enabled	SA1
	Active Directory Group Discovery	Enabled	SA1
	Heartbeat Discovery	Enabled	SA1
	Active Directory System Discovery	Disabled	SA1
	Active Directory User Discovery	Disabled	SA1
	Network Discovery	Disabled	SA1

Active Directory System Discovery Properties

Active Directory System Discovery

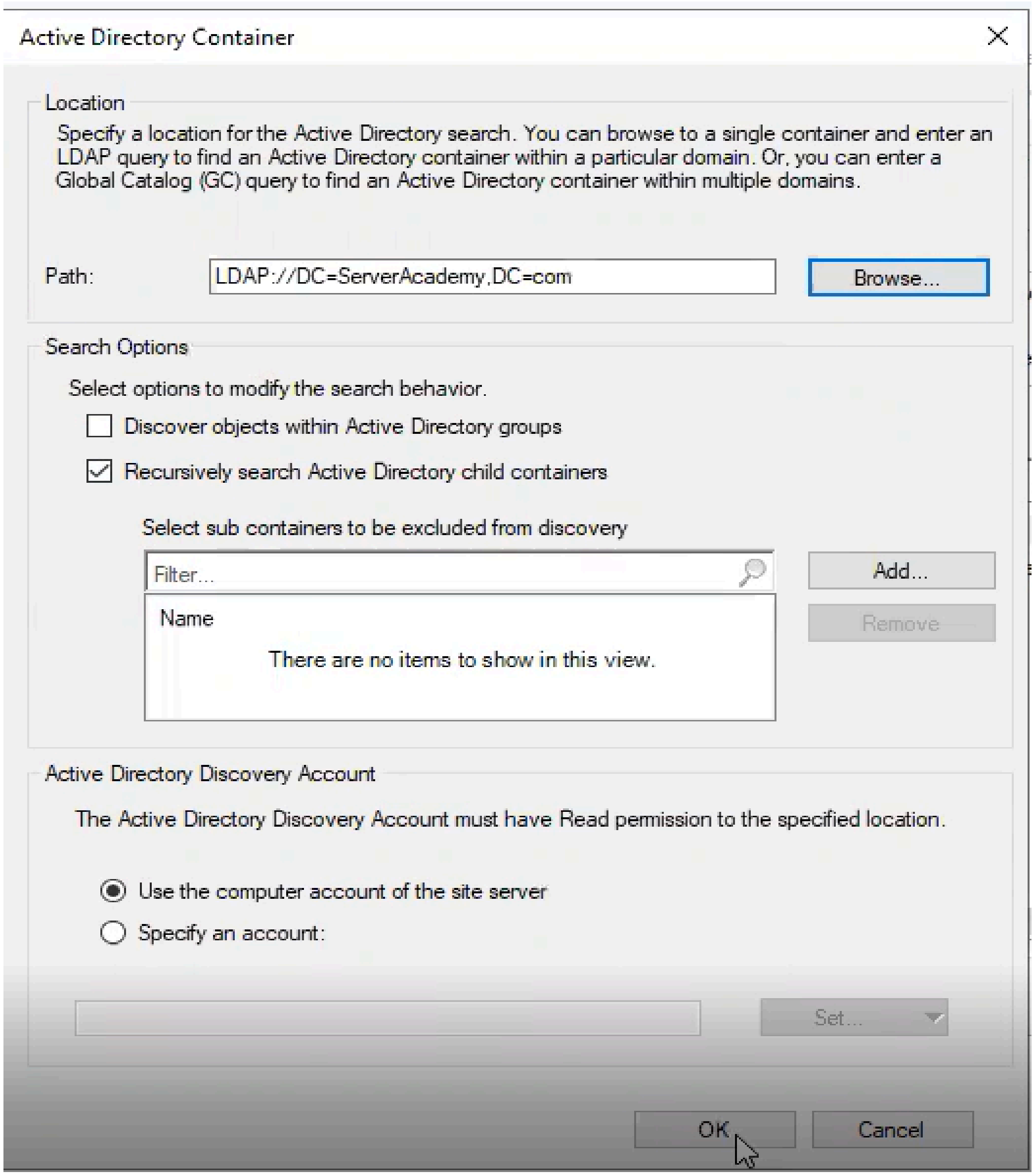
Configure the settings to find computers in Active Directory Domain Services.

☑ Enable Active Directory System Discovery

Active Directory containers:

Distinguished Name	Recursive	Group	Account

There are no items to show in this view.



Active Directory Container

Location

Specify a location for the Active Directory search. You can browse to a single container and enter an LDAP query to find an Active Directory container within a particular domain. Or, you can enter a Global Catalog (GC) query to find an Active Directory container within multiple domains.

Path: LDAP://DC=ServerAcademy,DC=com

Search Options

Select options to modify the search behavior.

□ Discover objects within Active Directory groups

☑ Recursively search Active Directory child containers

Select sub containers to be excluded from discovery

Name

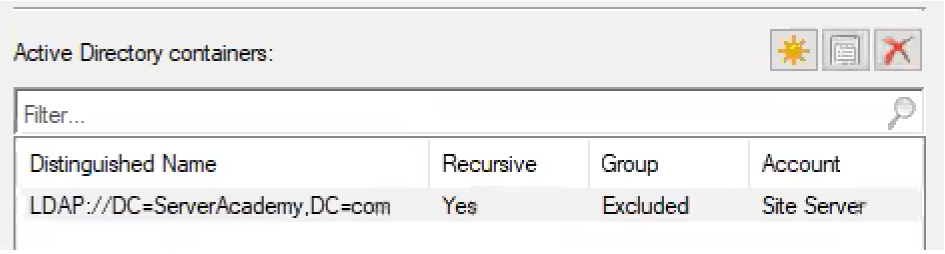
There are no items to show in this view.

Active Directory Discovery Account

The Active Directory Discovery Account must have Read permission to the specified location.

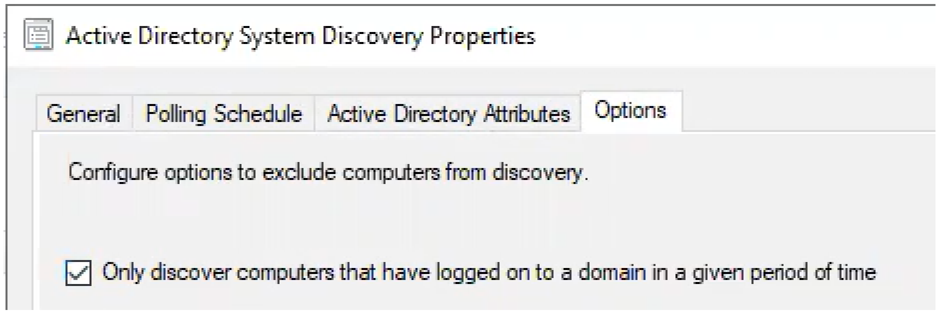
● Use the computer account of the site server

○ Specify an account:



Active Directory containers:

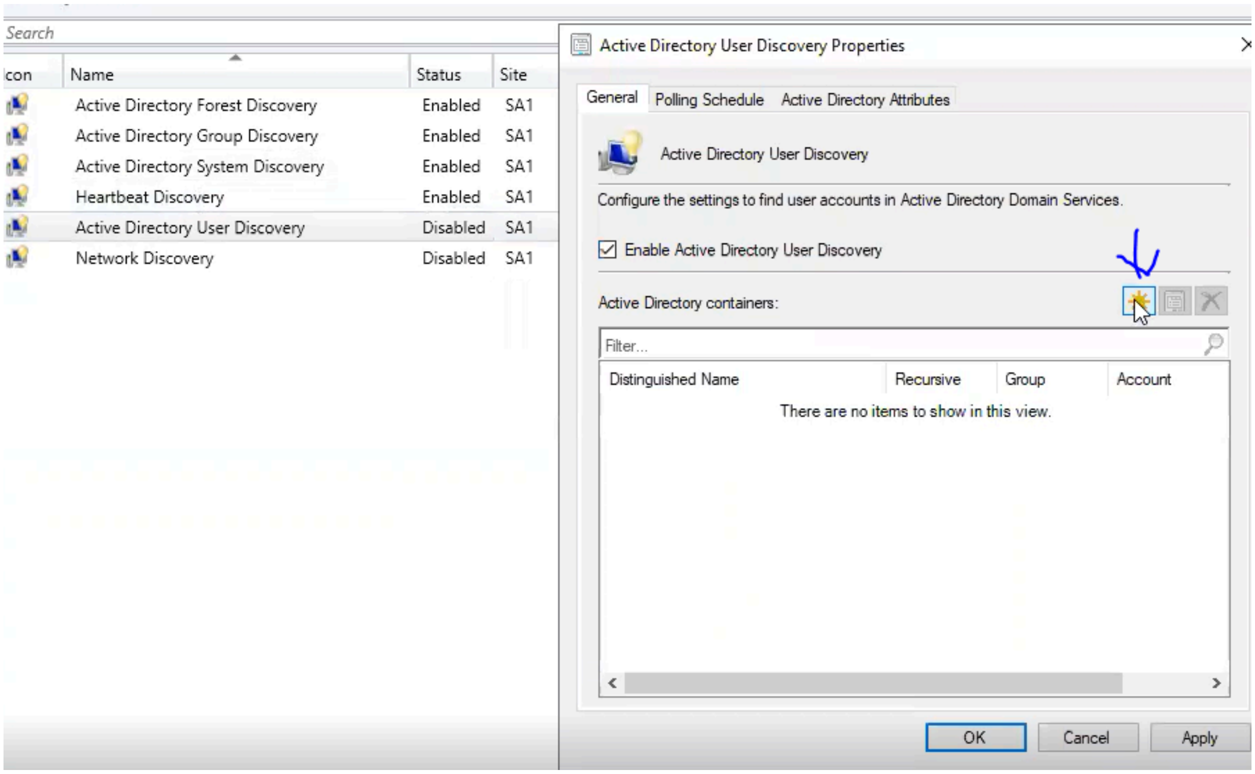
Distinguished Name	Recursive	Group	Account
LDAP://DC=ServerAcademy,DC=com	Yes	Excluded	Site Server



Active Directory System Discovery Properties

Configure options to exclude computers from discovery.

☑ Only discover computers that have logged on to a domain in a given period of time



Icon	Name	Status	Site
	Active Directory Forest Discovery	Enabled	SA1
	Active Directory Group Discovery	Enabled	SA1
	Active Directory System Discovery	Enabled	SA1
	Heartbeat Discovery	Enabled	SA1
	Active Directory User Discovery	Disabled	SA1
	Network Discovery	Disabled	SA1

Active Directory User Discovery Properties

Active Directory User Discovery

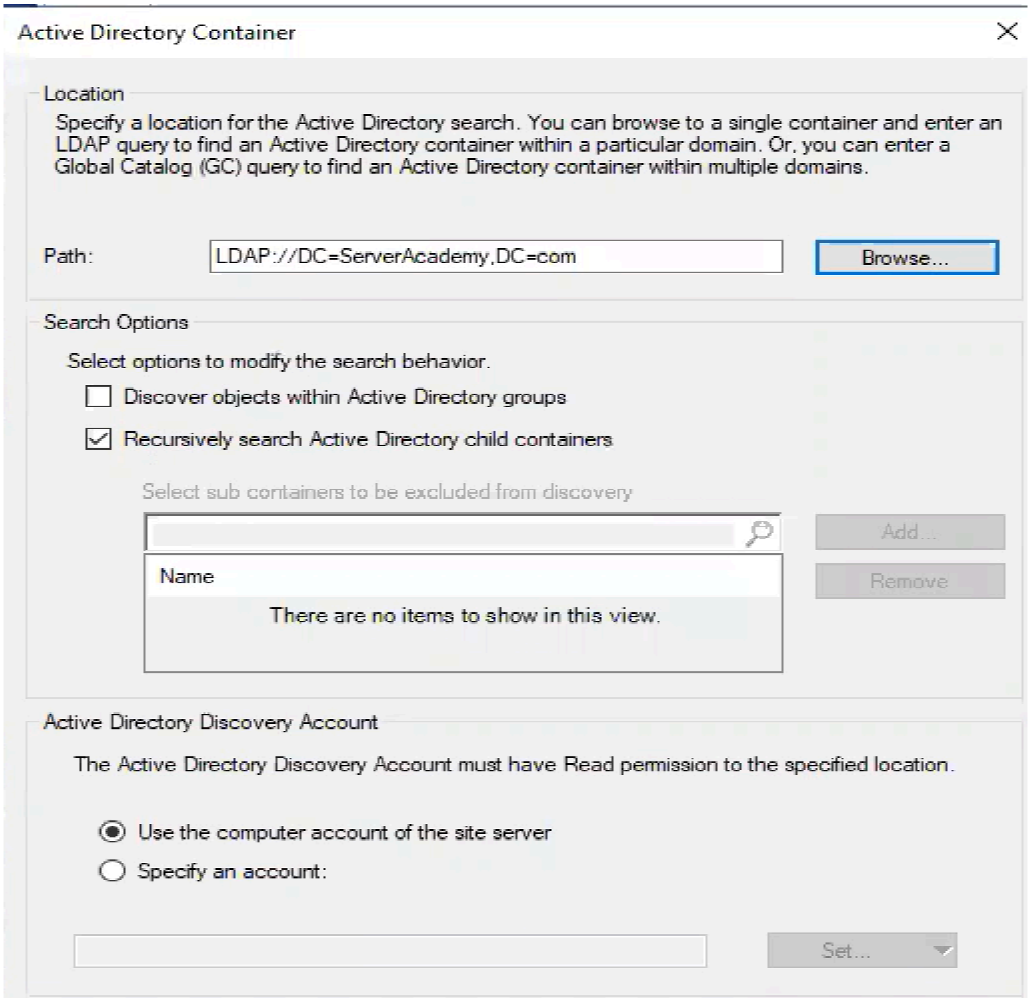
Configure the settings to find user accounts in Active Directory Domain Services.

☑ Enable Active Directory User Discovery

Active Directory containers:

Distinguished Name	Recursive	Group	Account

There are no items to show in this view.



Active Directory Container

Location

Specify a location for the Active Directory search. You can browse to a single container and enter an LDAP query to find an Active Directory container within a particular domain. Or, you can enter a Global Catalog (GC) query to find an Active Directory container within multiple domains.

Path: LDAP://DC=ServerAcademy,DC=com

Search Options

Select options to modify the search behavior.

☐ Discover objects within Active Directory groups

☑ Recursively search Active Directory child containers

Select sub containers to be excluded from discovery

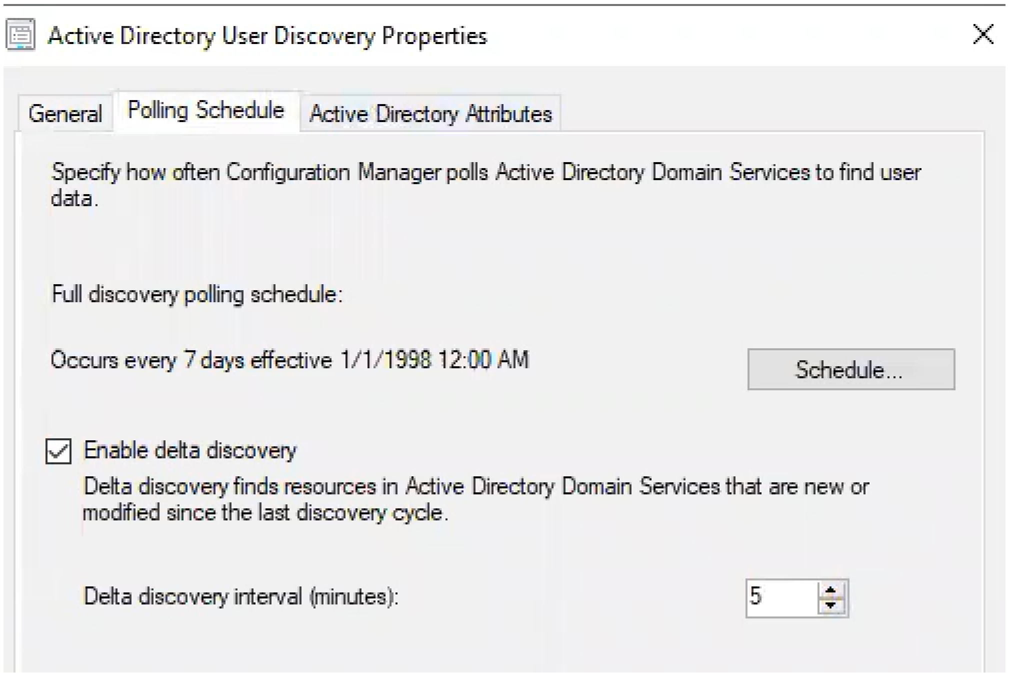
There are no items to show in this view.

Active Directory Discovery Account

The Active Directory Discovery Account must have Read permission to the specified location.

● Use the computer account of the site server

○ Specify an account:



Active Directory User Discovery Properties

Specify how often Configuration Manager polls Active Directory Domain Services to find user data.

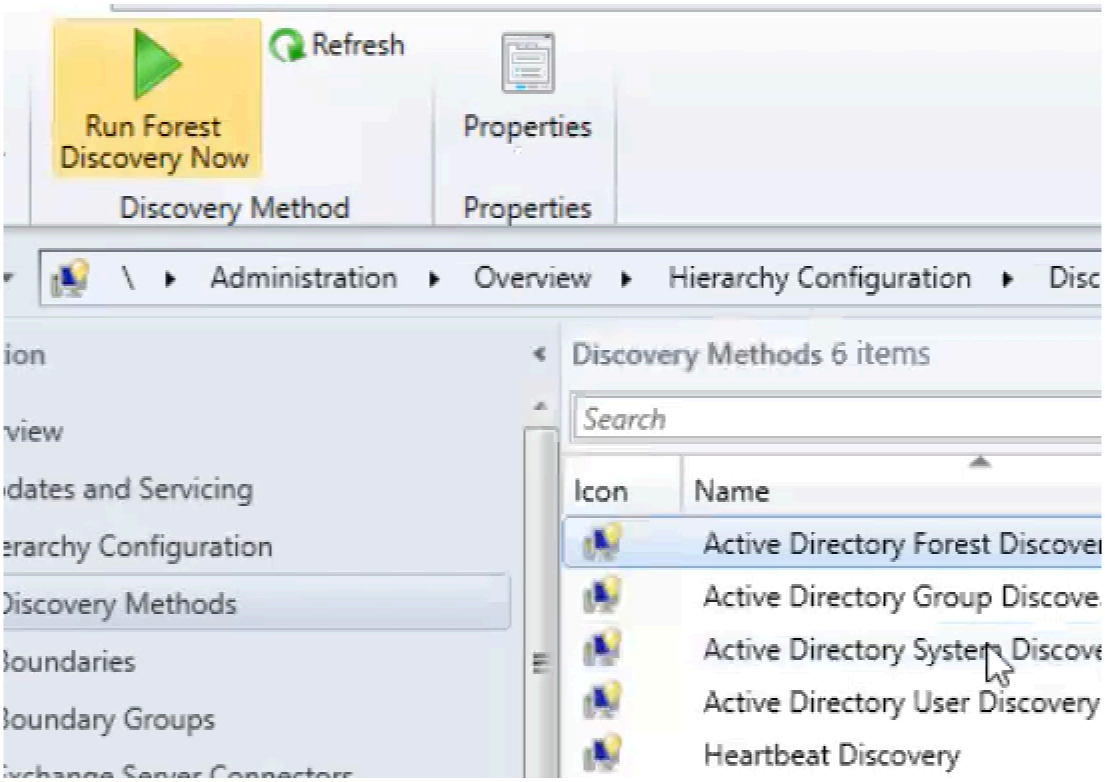
Full discovery polling schedule:

Occurs every 7 days effective 1/1/1998 12:00 AM

☑ Enable delta discovery

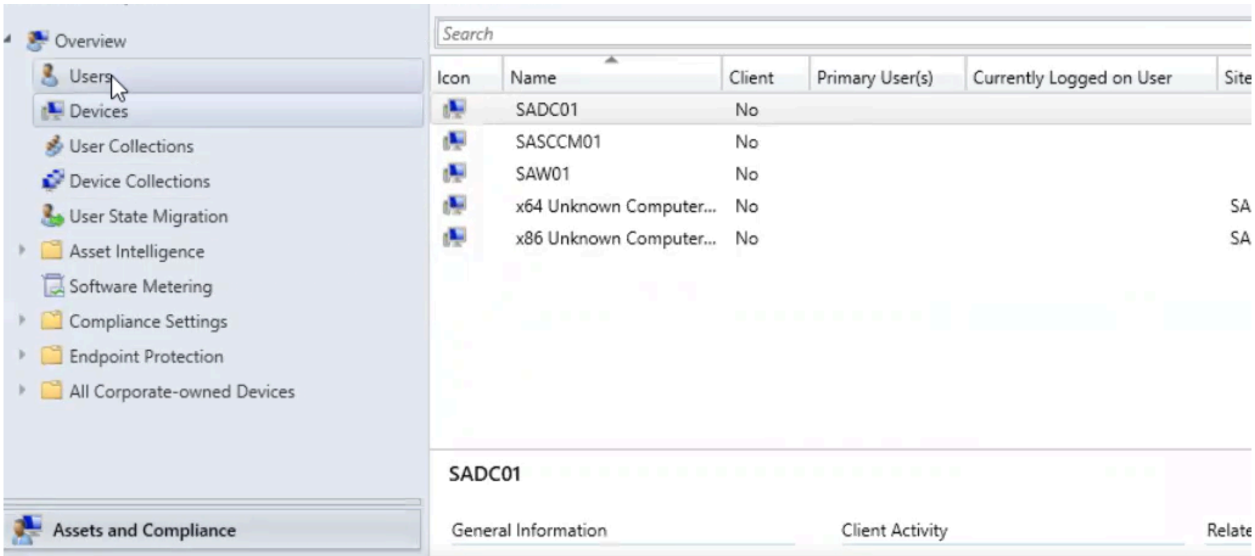
Delta discovery finds resources in Active Directory Domain Services that are new or modified since the last discovery cycle.

Delta discovery interval (minutes): 5

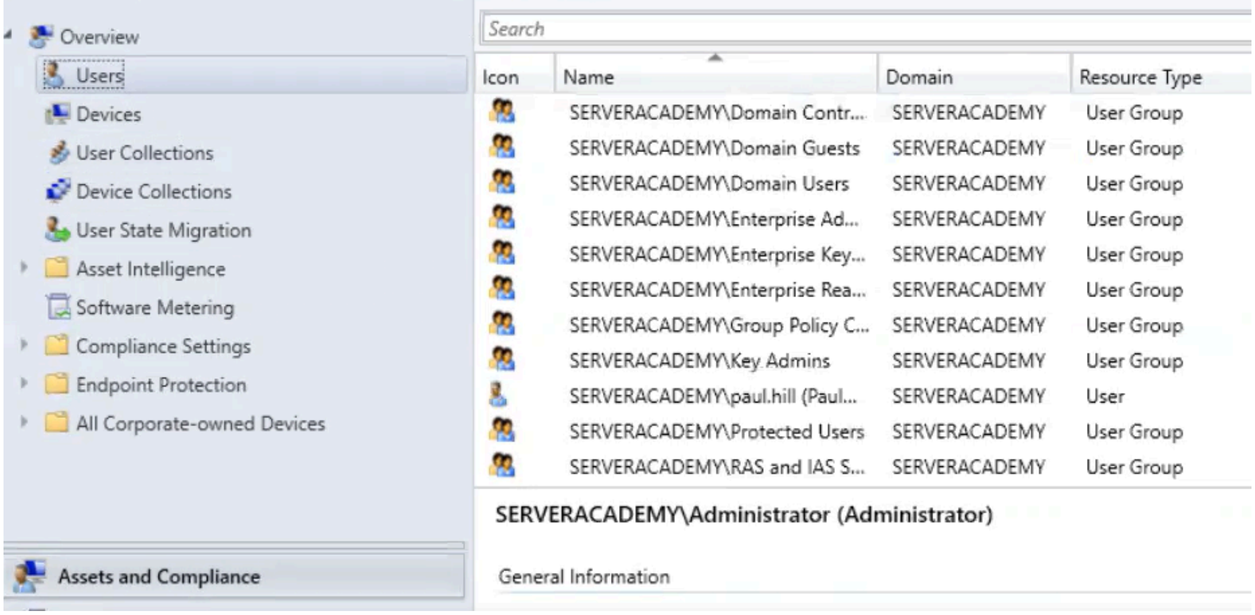


Icon	Name
	Active Directory Forest Discover
	Active Directory Group Discove
	Active Directory System Discove
	Active Directory User Discovery
	Heartbeat Discovery

Clients and Devices on Network Successfully Discovered



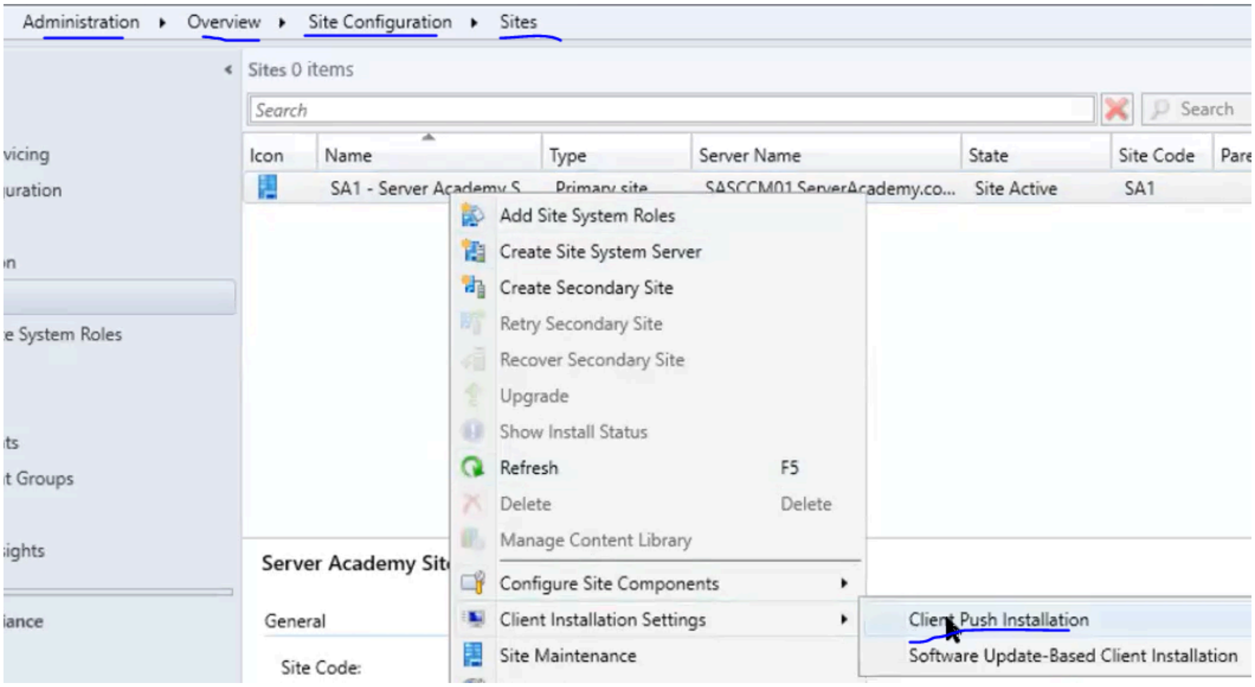
Icon	Name	Client	Primary User(s)	Currently Logged on User	Site
	SADC01	No			
	SASCCM01	No			
	SAW01	No			
	x64 Unknown Computer...	No			SA
	x86 Unknown Computer...	No			SA



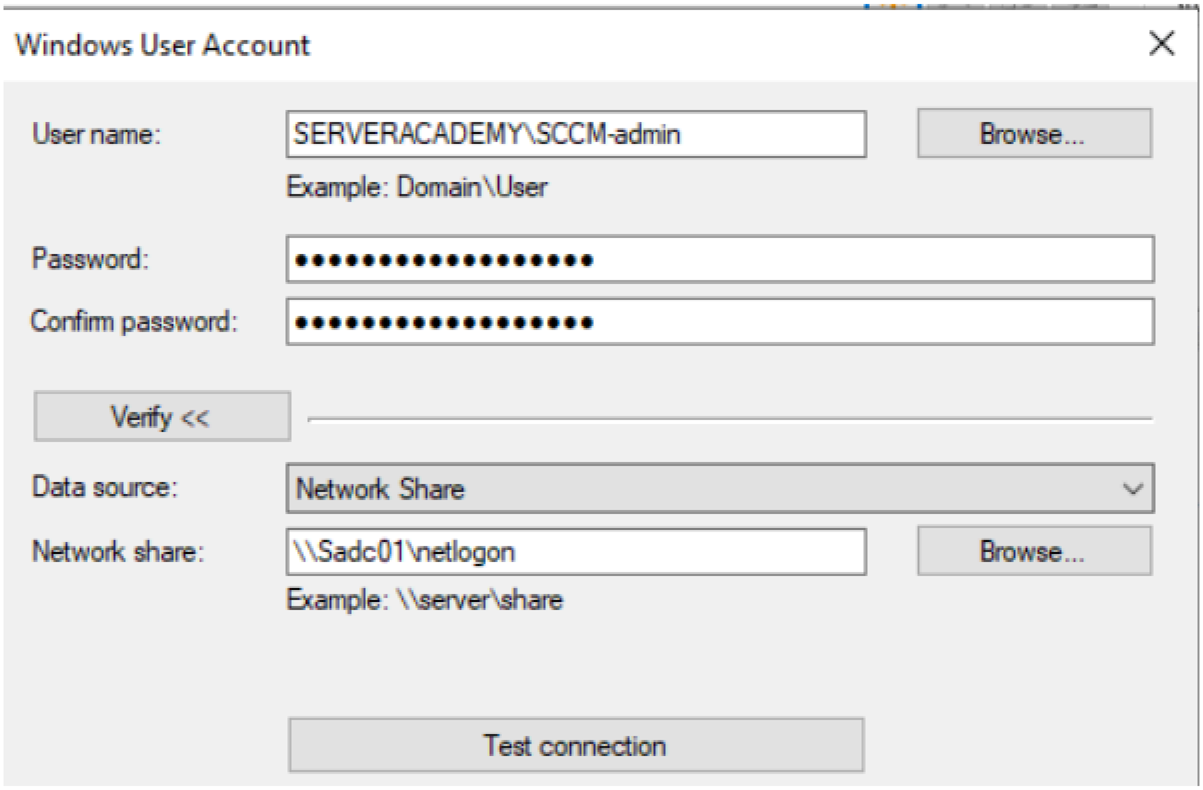
Icon	Name	Domain	Resource Type
	SERVERACADEMY\Domain Contr...	SERVERACADEMY	User Group
	SERVERACADEMY\Domain Guests	SERVERACADEMY	User Group
	SERVERACADEMY\Domain Users	SERVERACADEMY	User Group
	SERVERACADEMY\Enterprise Ad...	SERVERACADEMY	User Group
	SERVERACADEMY\Enterprise Key...	SERVERACADEMY	User Group
	SERVERACADEMY\Enterprise Rea...	SERVERACADEMY	User Group
	SERVERACADEMY\Group Policy C...	SERVERACADEMY	User Group
	SERVERACADEMY\Key Admins	SERVERACADEMY	User Group
	SERVERACADEMY\paul.hill (Paul...	SERVERACADEMY	User
	SERVERACADEMY\Protected Users	SERVERACADEMY	User Group
	SERVERACADEMY\RAS and IAS S...	SERVERACADEMY	User Group

SERVERACADEMY\Administrator (Administrator)

Client Push Installation



Icon	Name	Type	Server Name	State	Site Code	Pare
	SA1 - Server Academy S...	Primary site	SASCCM01.ServerAcademy.co...	Site Active	SA1	



Windows User Account

User name: SERVERACADEMY\SCCM-admin

Example: Domain\User

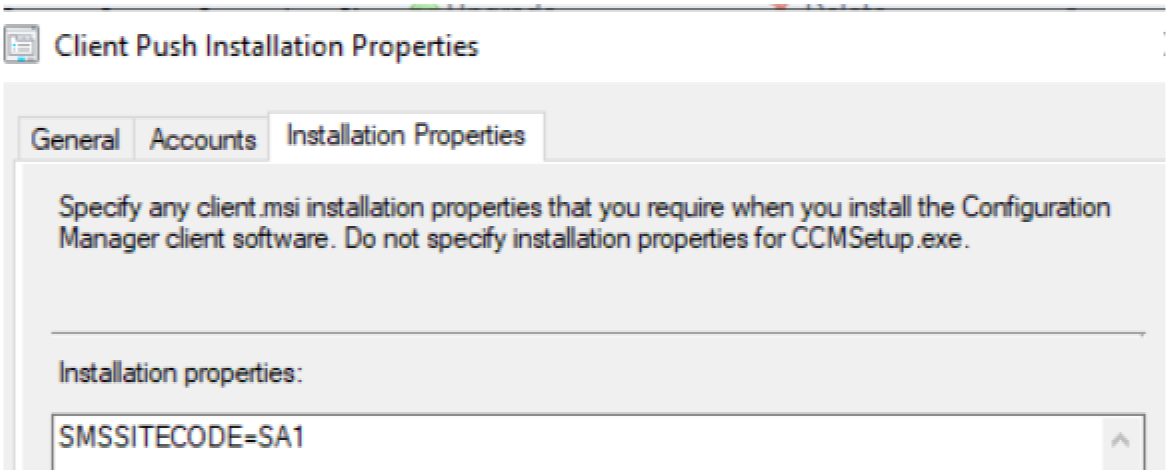
Password: ••••••••••••••••••

Confirm password: ••••••••••••••••••

Data source: Network Share

Network share: \\Sadc01\netlogon

Example: \\server\share

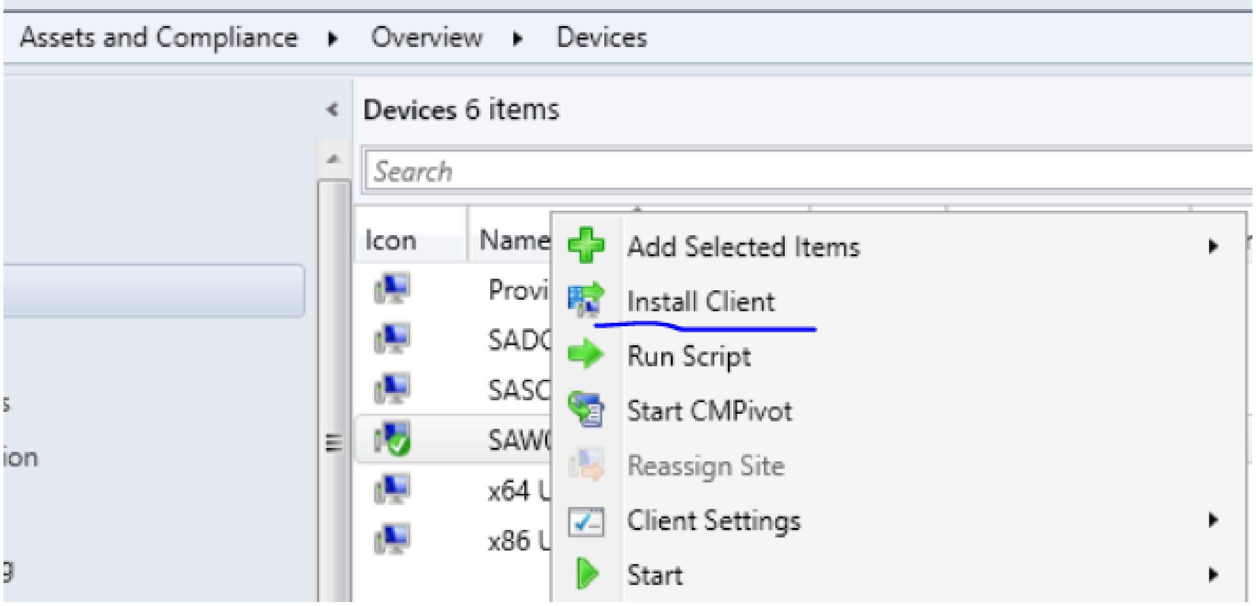


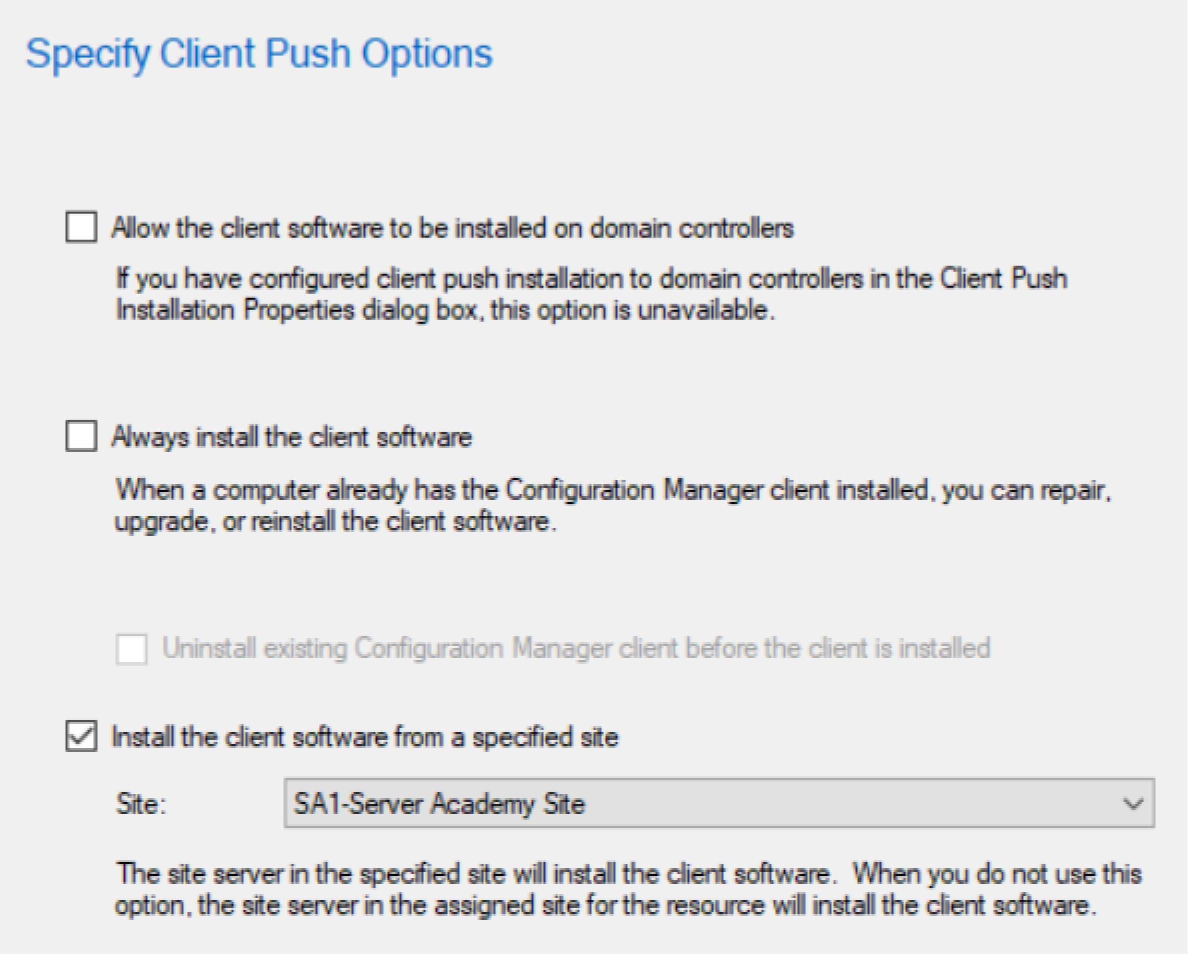
Client Push Installation Properties

Specify any client.msi installation properties that you require when you install the Configuration Manager client software. Do not specify installation properties for CCMSetup.exe.

Installation properties:

SMSSITECODE=SA1





Specify Client Push Options

□ Allow the client software to be installed on domain controllers

If you have configured client push installation to domain controllers in the Client Push Installation Properties dialog box, this option is unavailable.

□ Always install the client software

When a computer already has the Configuration Manager client installed, you can repair, upgrade, or reinstall the client software.

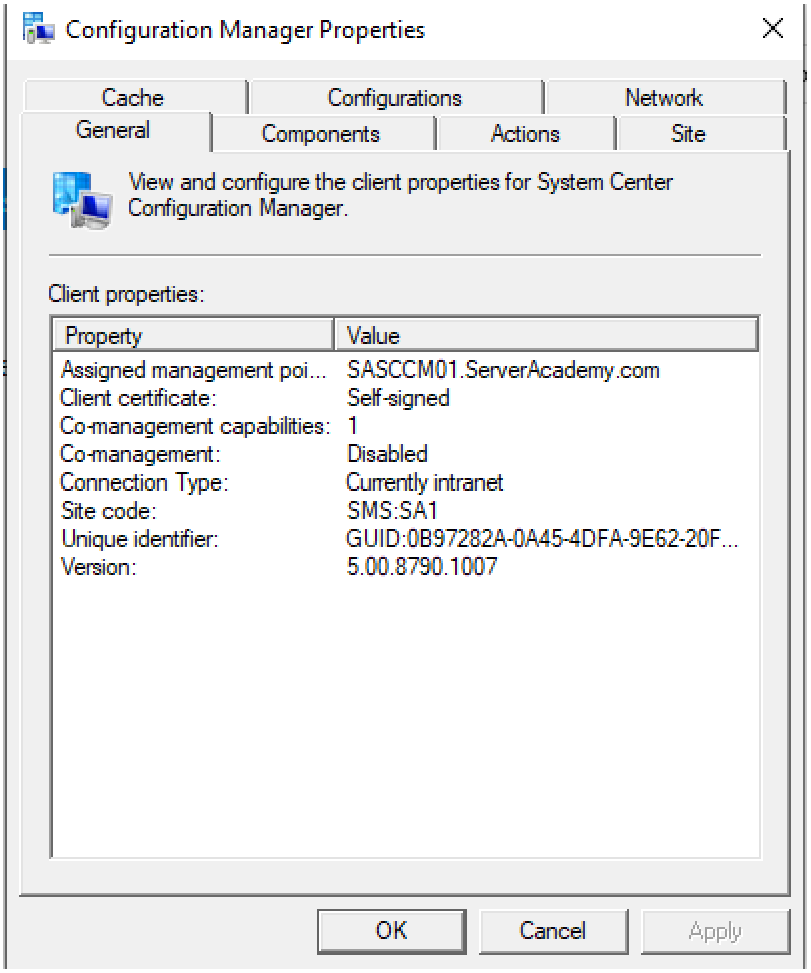
□ Uninstall existing Configuration Manager client before the client is installed

☑ Install the client software from a specified site

Site: SA1-Server Academy Site

The site server in the specified site will install the client software. When you do not use this option, the site server in the assigned site for the resource will install the client software.

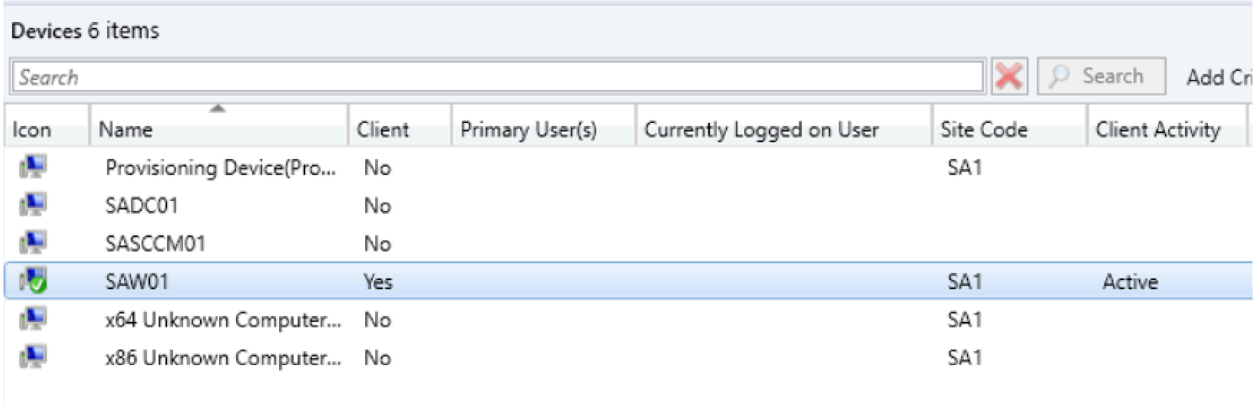
Verifying SCCM is Installed on Client



View and configure the client properties for System Center Configuration Manager.

Client properties:

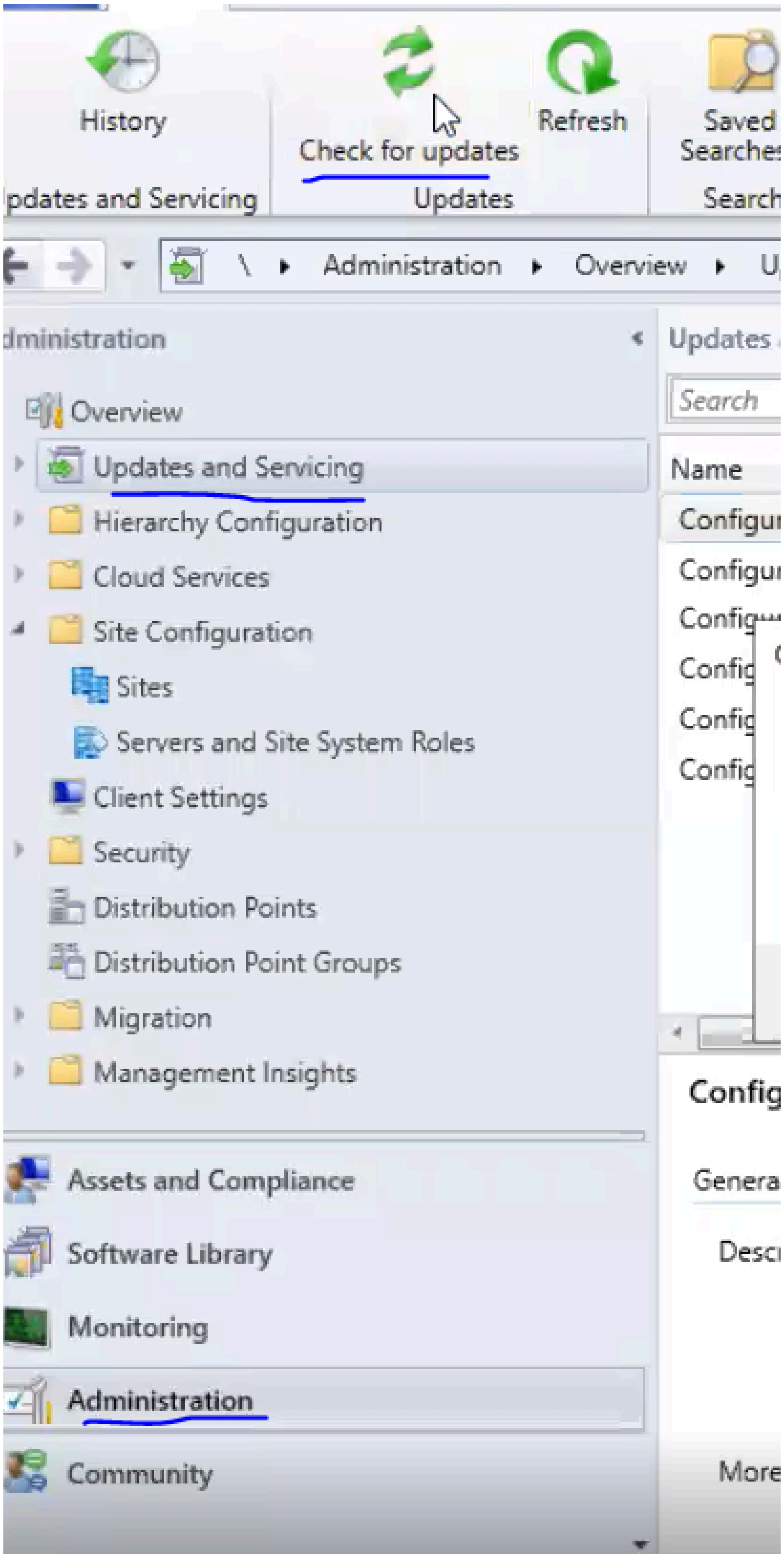
Property	Value
Assigned management poi...	SASCCM01.ServerAcademy.com
Client certificate:	Self-signed
Co-management capabilities:	1
Co-management:	Disabled
Connection Type:	Currently intranet
Site code:	SMS:SA1
Unique identifier:	GUID:0B97282A-0A45-4DFA-9E62-20F...
Version:	5.00.8790.1007



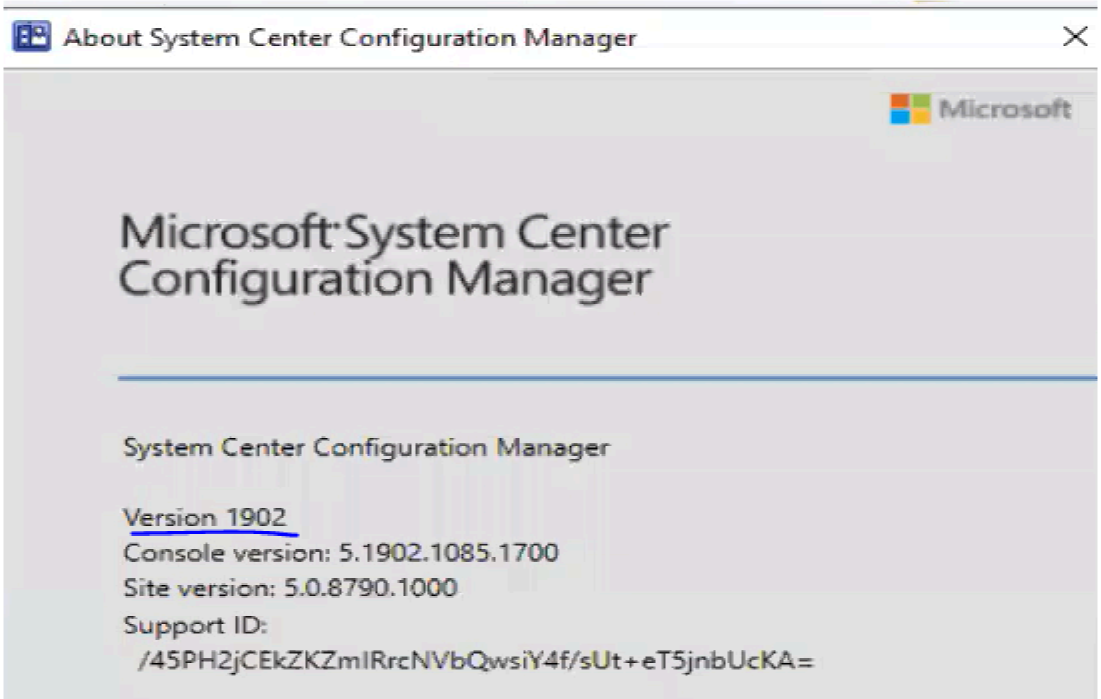
Devices 6 items

Icon	Name	Client	Primary User(s)	Currently Logged on User	Site Code	Client Activity
	Provisioning Device(Pro...	No			SA1	
	SADC01	No				
	SASCCM01	No				
✓	SAW01	Yes			SA1	Active
	x64 Unknown Computer...	No			SA1	
	x86 Unknown Computer...	No			SA1	

Updating SCCM to Latest Version



Older version 1902 being updated



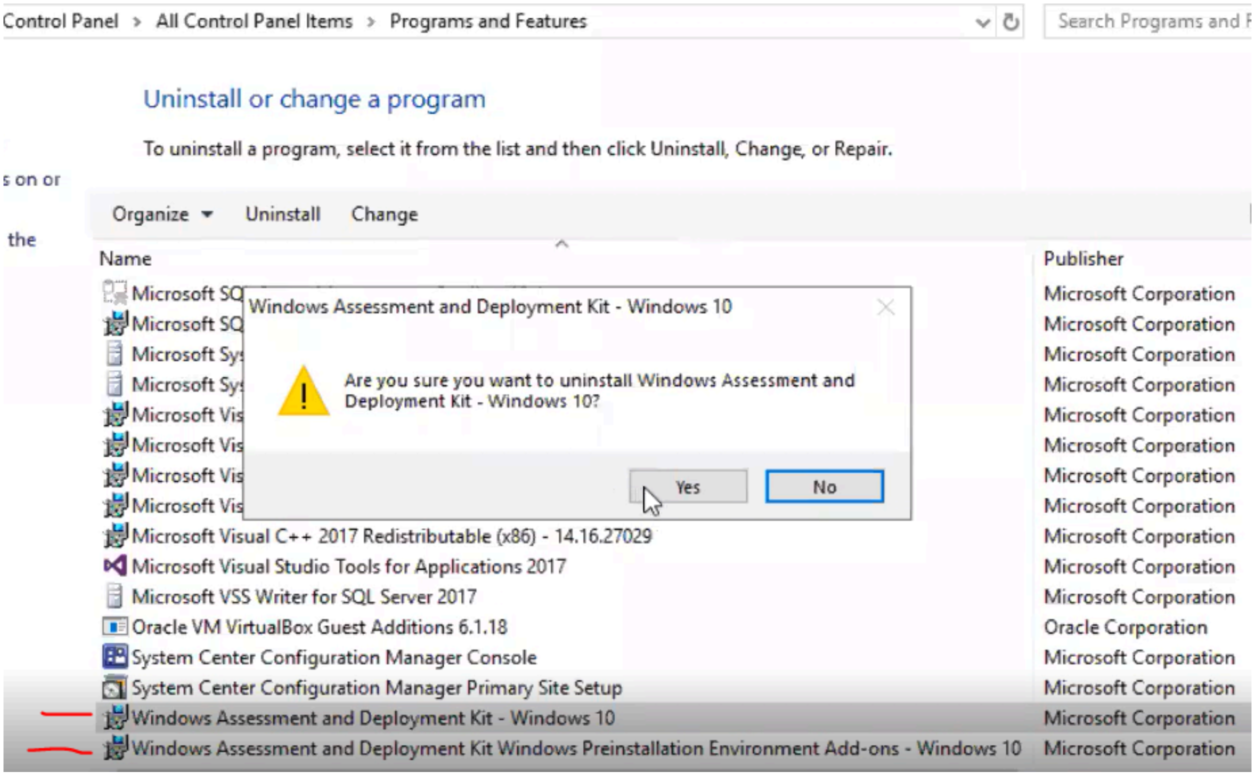
About System Center Configuration Manager

Microsoft System Center Configuration Manager

System Center Configuration Manager

Version 1902
Console version: 5.1902.1085.1700
Site version: 5.0.8790.1000
Support ID:
/45PH2jCEkZKZmIRrcNVbQwsiY4f/sUt+eT5jnbUcKA=

Uninstalling Both Assessment and Deployment Kits



Control Panel > All Control Panel Items > Programs and Features
Search Programs and F
s on or
the
Organize
Uninstall
Change

Uninstall or change a program

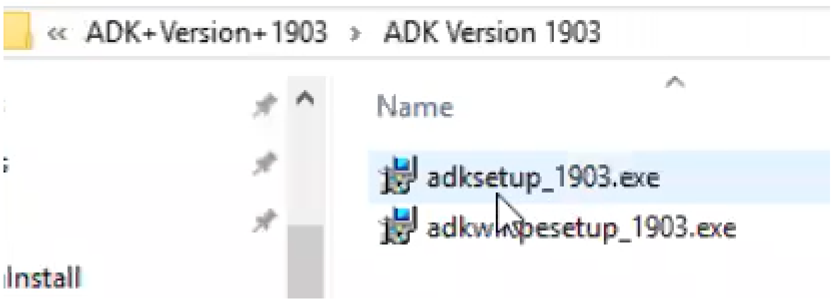
To uninstall a program, select it from the list and then click Uninstall, Change, or Repair.

Name	Publisher
Microsoft SQ	Microsoft Corporation
Microsoft SQ	Microsoft Corporation
Microsoft Sys	Microsoft Corporation
Microsoft Sys	Microsoft Corporation
Microsoft Vis	Microsoft Corporation
Microsoft Vis	Microsoft Corporation
Microsoft Vis	Microsoft Corporation
Microsoft Vis	Microsoft Corporation
Microsoft Visual C++ 2017 Redistributable (x86) - 14.16.27029	Microsoft Corporation
Microsoft Visual Studio Tools for Applications 2017	Microsoft Corporation
Microsoft VSS Writer for SQL Server 2017	Microsoft Corporation
Oracle VM VirtualBox Guest Additions 6.1.18	Oracle Corporation
System Center Configuration Manager Console	Microsoft Corporation
System Center Configuration Manager Primary Site Setup	Microsoft Corporation
Windows Assessment and Deployment Kit - Windows 10	Microsoft Corporation
Windows Assessment and Deployment Kit Windows Preinstallation Environment Add-ons - Windows 10	Microsoft Corporation

Windows Assessment and Deployment Kit - Windows 10

Are you sure you want to uninstall Windows Assessment and Deployment Kit - Windows 10?

Reinstalling Assessment and Deployment Kit



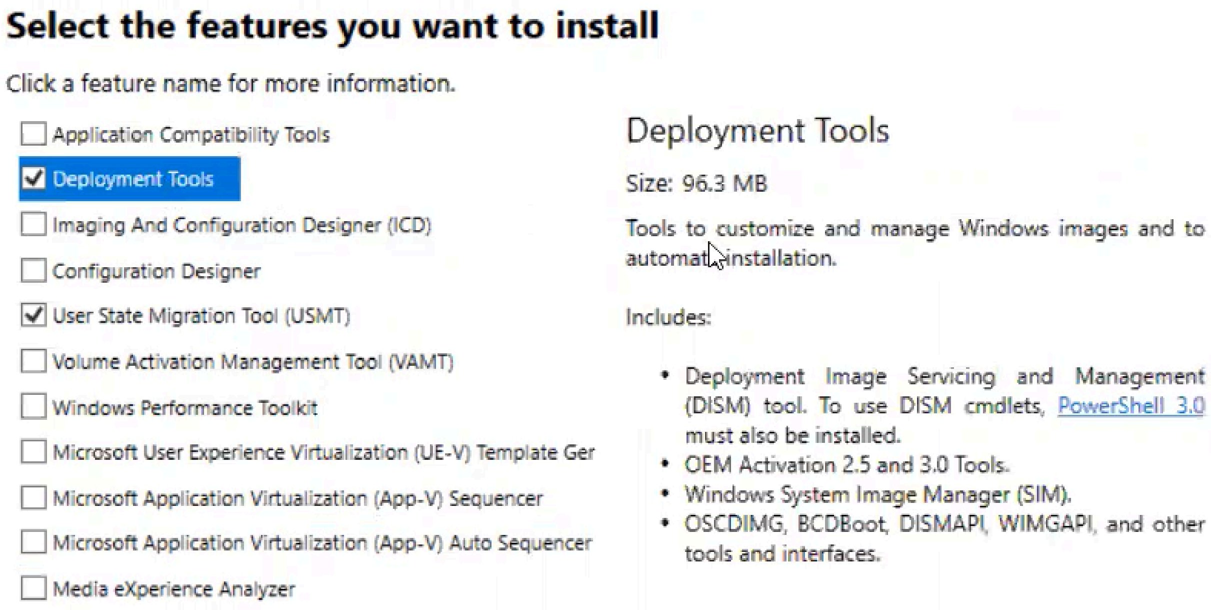
« ADK+Version+1903 › ADK Version 1903

Name

adksetup_1903.exe

adkwinpesetup_1903.exe

Install



Select the features you want to install

Click a feature name for more information.

- □ Application Compatibility Tools
- ☑ Deployment Tools
- □ Imaging And Configuration Designer (ICD)
- □ Configuration Designer
- ☑ User State Migration Tool (USMT)
- □ Volume Activation Management Tool (VAMT)
- □ Windows Performance Toolkit
- □ Microsoft User Experience Virtualization (UE-V) Template Ger
- □ Microsoft Application Virtualization (App-V) Sequencer
- □ Microsoft Application Virtualization (App-V) Auto Sequencer
- □ Media eXperience Analyzer

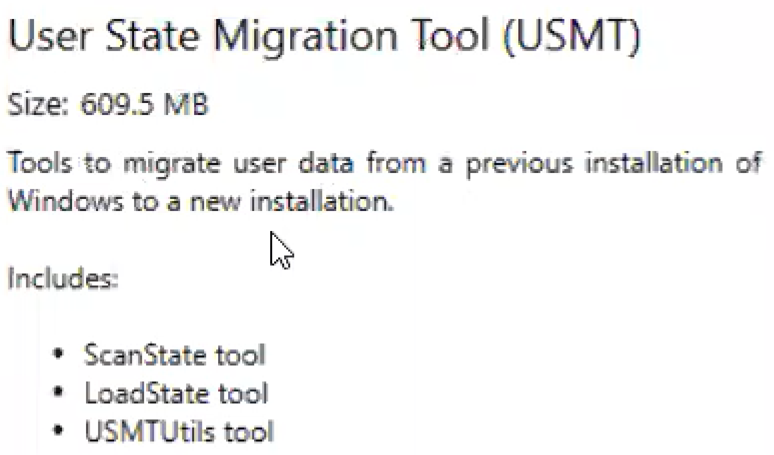
Deployment Tools

Size: 96.3 MB

Tools to customize and manage Windows images and to automate installation.

Includes:

- Deployment Image Servicing and Management (DISM) tool. To use DISM cmdlets, PowerShell 3.0 must also be installed.
- OEM Activation 2.5 and 3.0 Tools.
- Windows System Image Manager (SIM).
- OSCDIMG, BCDBoot, DISMAPI, WIMGAPI, and other tools and interfaces.



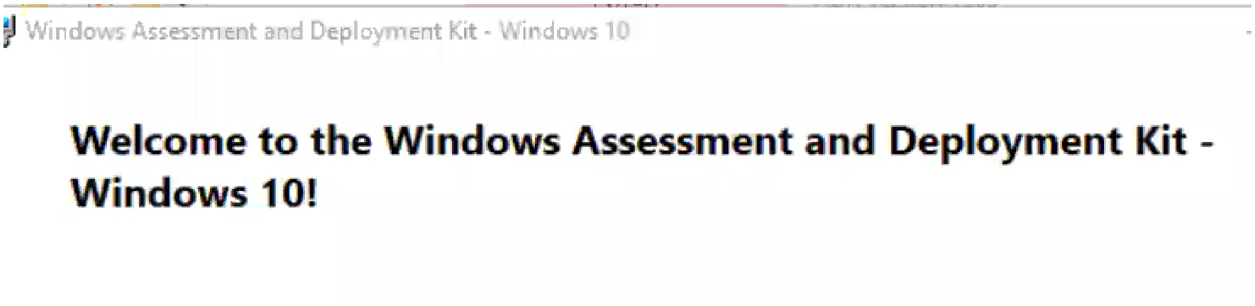
User State Migration Tool (USMT)

Size: 609.5 MB

Tools to migrate user data from a previous installation of Windows to a new installation.

Includes:

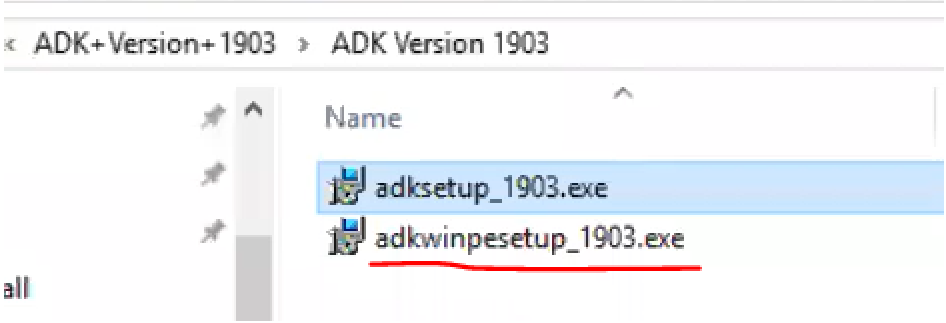
- ScanState tool
- LoadState tool
- USMTUtils tool



Windows Assessment and Deployment Kit - Windows 10

Welcome to the Windows Assessment and Deployment Kit - Windows 10!

Launching the WinPE Setup



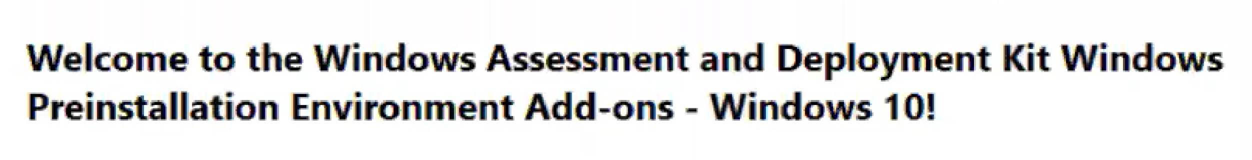
ADK+Version+1903 › ADK Version 1903

Name

adksetup_1903.exe

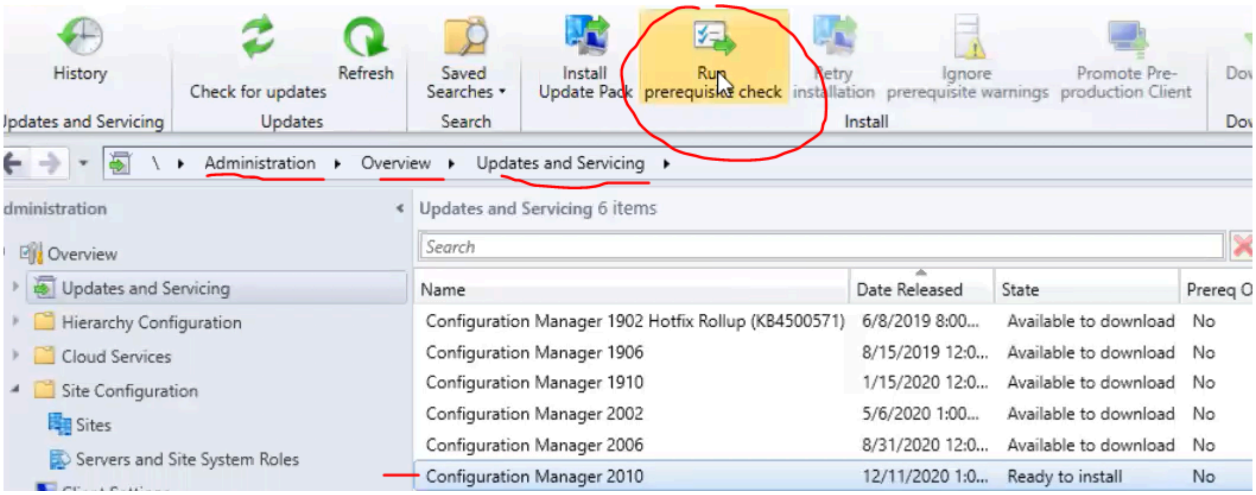
adkwinpesetup_1903.exe

all



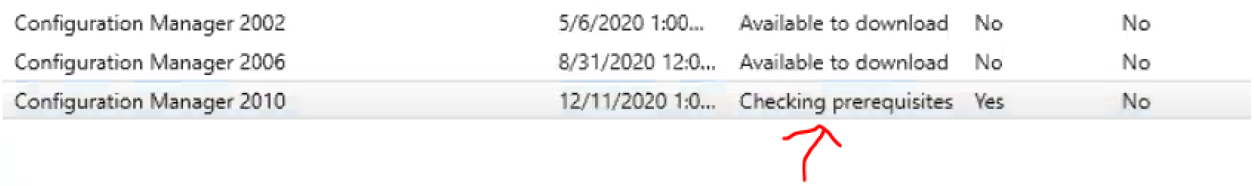
Welcome to the Windows Assessment and Deployment Kit Windows Preinstallation Environment Add-ons - Windows 10!

Running Prerequisite Checks Before Updating

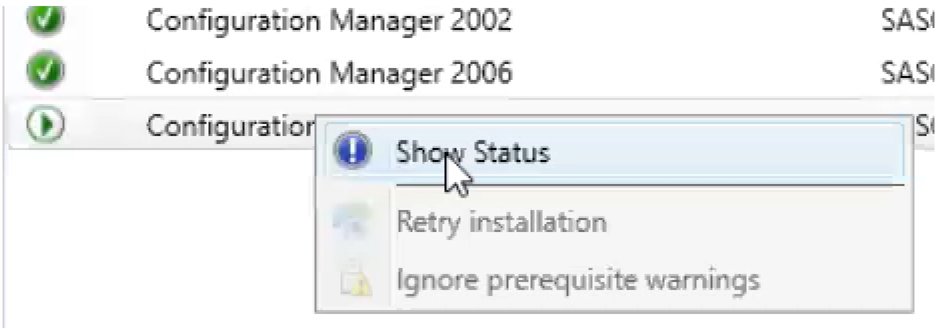


Updates and Servicing 6 items

Name	Date Released	State	Prereq O
Configuration Manager 1902 Hotfix Rollup (KB4500571)	6/8/2019 8:00...	Available to download	No
Configuration Manager 1906	8/15/2019 12:0...	Available to download	No
Configuration Manager 1910	1/15/2020 12:0...	Available to download	No
Configuration Manager 2002	5/6/2020 1:00...	Available to download	No
Configuration Manager 2006	8/31/2020 12:0...	Available to download	No
Configuration Manager 2010	12/11/2020 1:0...	Ready to install	No

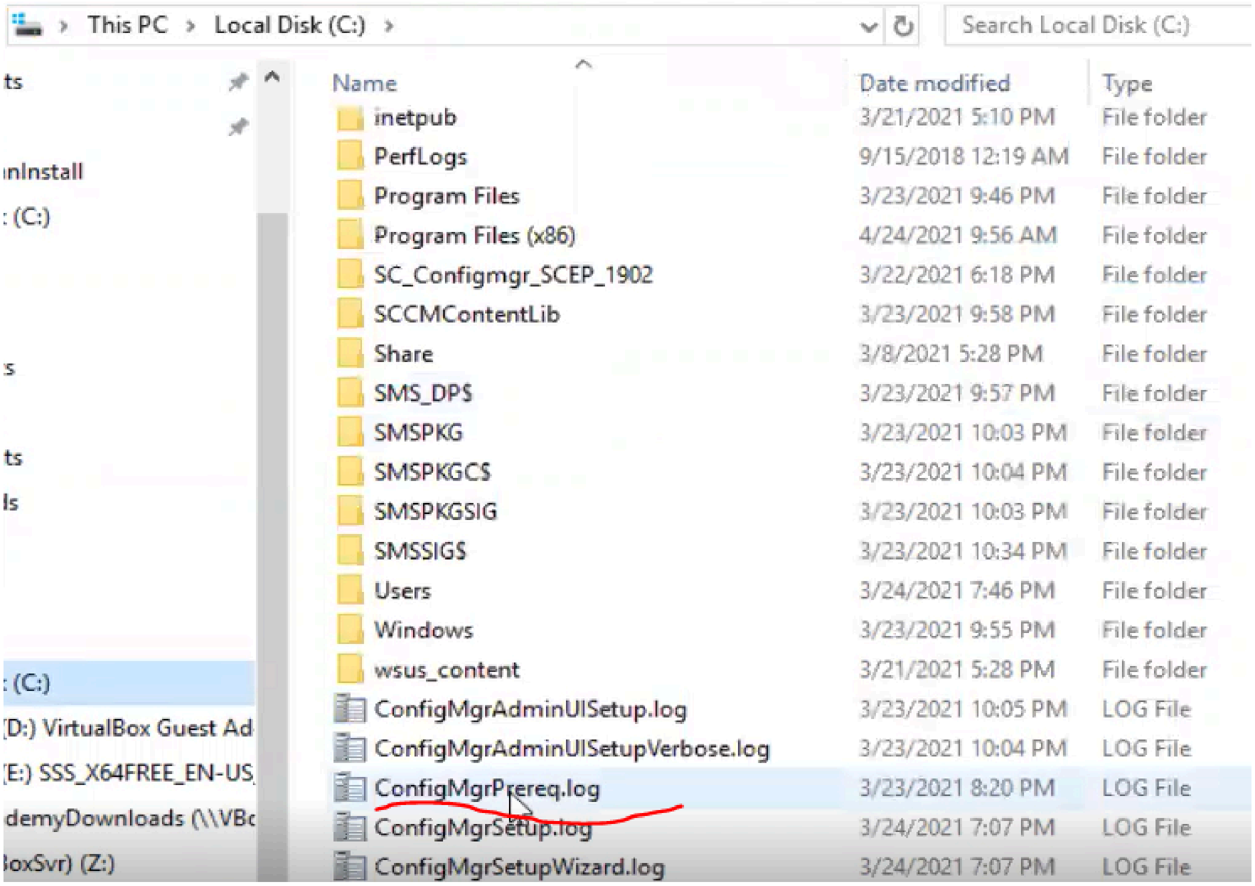


Configuration Manager 2002	5/6/2020 1:00...	Available to download	No	No
Configuration Manager 2006	8/31/2020 12:0...	Available to download	No	No
Configuration Manager 2010	12/11/2020 1:0...	Checking prerequisites	Yes	No

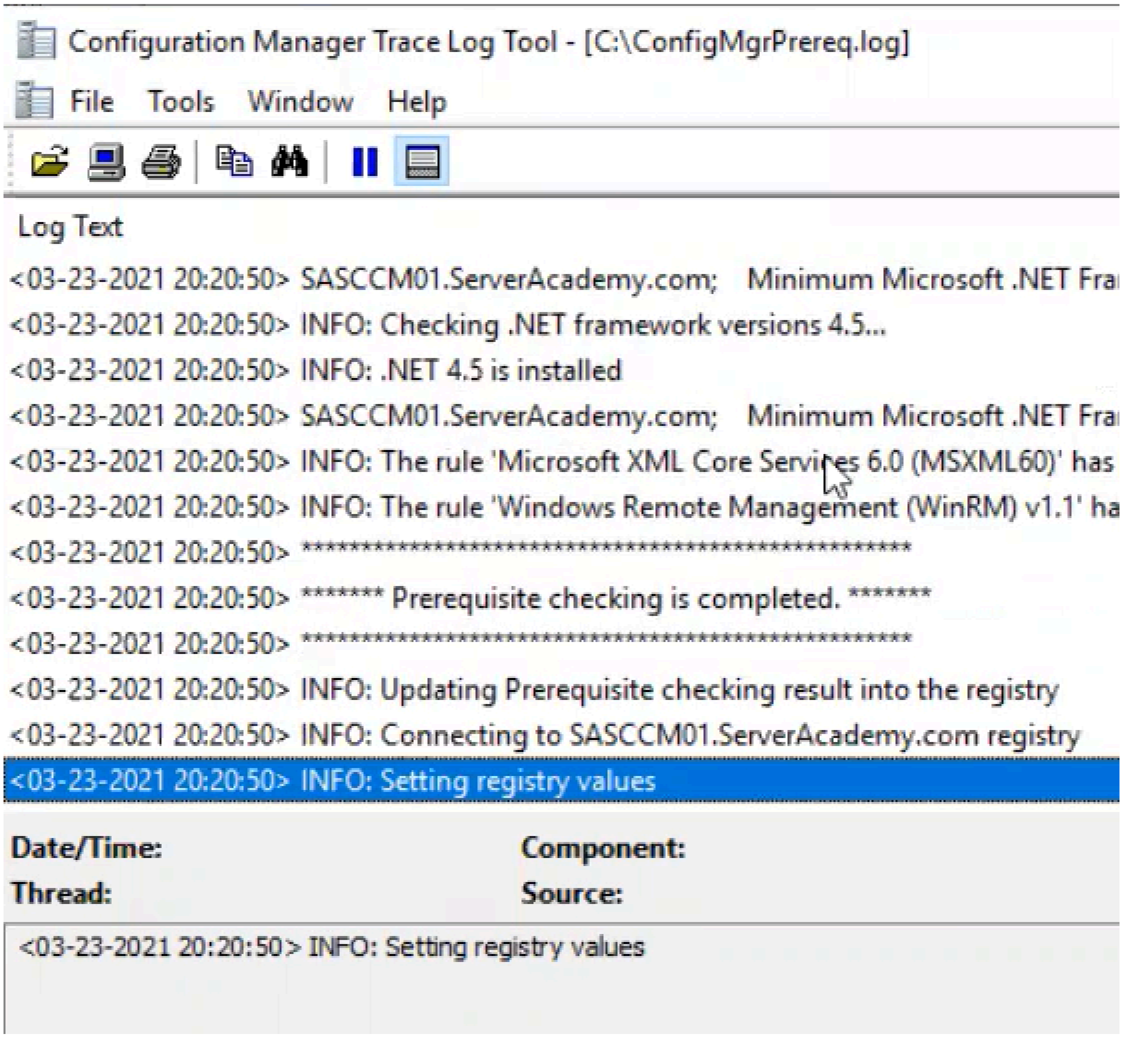


Configuration Manager 2002	SAS
Configuration Manager 2006	SAS
Configuratior	S

Checking Prerequisites log file with the CMTrace Tool



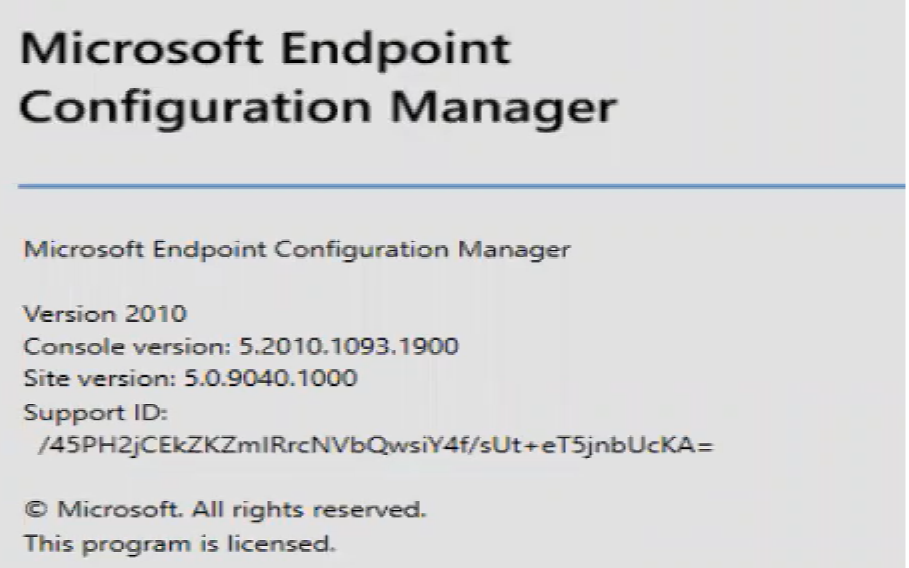
Name	Date modified	Type
inetpub	3/21/2021 5:10 PM	File folder
PerfLogs	9/15/2018 12:19 AM	File folder
Program Files	3/23/2021 9:46 PM	File folder
Program Files (x86)	4/24/2021 9:56 AM	File folder
SC_Configmgr_SCEP_1902	3/22/2021 6:18 PM	File folder
SCCMContentLib	3/23/2021 9:58 PM	File folder
Share	3/8/2021 5:28 PM	File folder
SMS_DP$	3/23/2021 9:57 PM	File folder
SMSPKG	3/23/2021 10:03 PM	File folder
SMSPKGC$	3/23/2021 10:04 PM	File folder
SMSPKGSIG	3/23/2021 10:03 PM	File folder
SMSSIG$	3/23/2021 10:34 PM	File folder
Users	3/24/2021 7:46 PM	File folder
Windows	3/23/2021 9:55 PM	File folder
wsus_content	3/21/2021 5:28 PM	File folder
ConfigMgrAdminUISetup.log	3/23/2021 10:05 PM	LOG File
ConfigMgrAdminUISetupVerbose.log	3/23/2021 10:04 PM	LOG File
ConfigMgrPrereq.log	3/23/2021 8:20 PM	LOG File
ConfigMgrSetup.log	3/24/2021 7:07 PM	LOG File
ConfigMgrSetupWizard.log	3/24/2021 7:07 PM	LOG File



Configuration Manager Trace Log Tool - [C:\ConfigMgrPrereq.log]
File
Tools
Window
Help
Log Text
Date/Time:
Component:
Thread:
Source:

```
<03-23-2021 20:20:50> SASCCM01.ServerAcademy.com;    Minimum Microsoft .NET Fra
<03-23-2021 20:20:50> INFO: Checking .NET framework versions 4.5...
<03-23-2021 20:20:50> INFO: .NET 4.5 is installed
<03-23-2021 20:20:50> SASCCM01.ServerAcademy.com;    Minimum Microsoft .NET Fra
<03-23-2021 20:20:50> INFO: The rule 'Microsoft XML Core Services 6.0 (MSXML60)' has
<03-23-2021 20:20:50> INFO: The rule 'Windows Remote Management (WinRM) v1.1' ha
<03-23-2021 20:20:50> ***************************************************
<03-23-2021 20:20:50> ******* Prerequisite checking is completed. *******
<03-23-2021 20:20:50> ***************************************************
<03-23-2021 20:20:50> INFO: Updating Prerequisite checking result into the registry
<03-23-2021 20:20:50> INFO: Connecting to SASCCM01.ServerAcademy.com registry
<03-23-2021 20:20:50> INFO: Setting registry values
```

```
<03-23-2021 20:20:50> INFO: Setting registry values
```



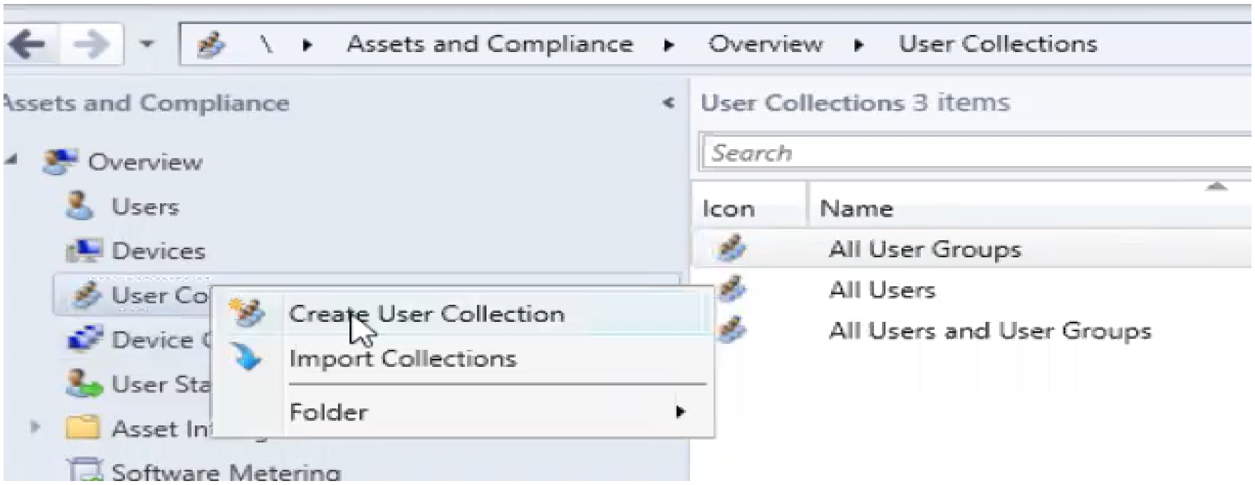
Microsoft Endpoint Configuration Manager

Microsoft Endpoint Configuration Manager

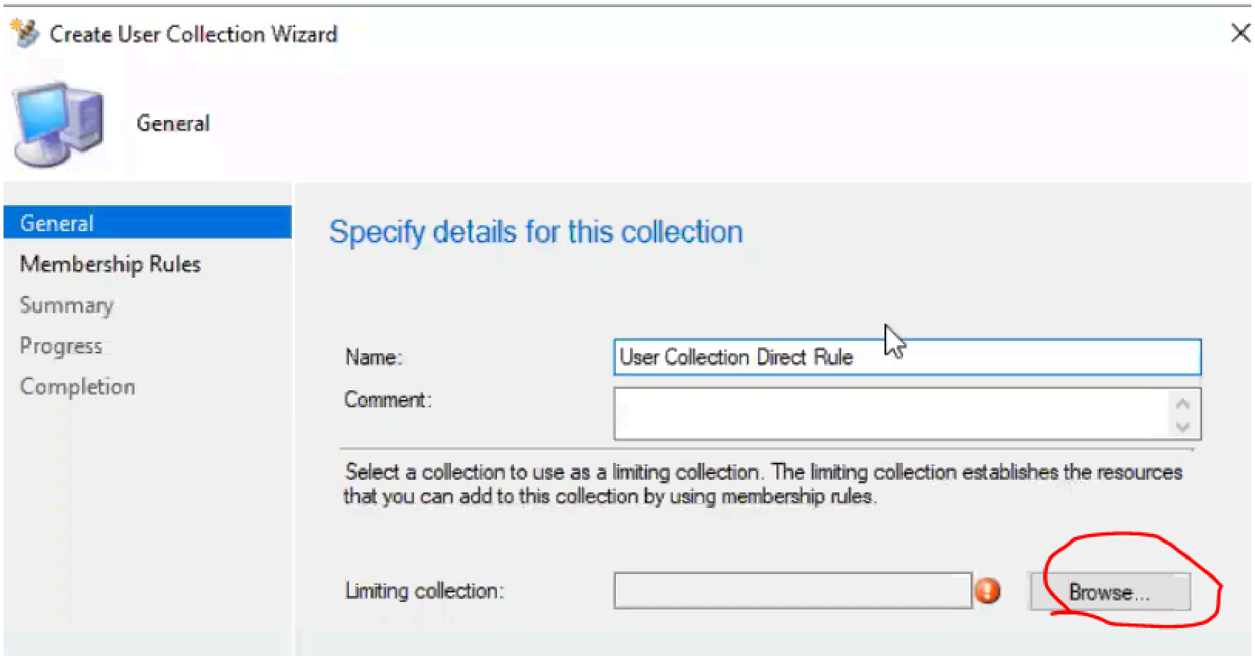
Version 2010
Console version: 5.2010.1093.1900
Site version: 5.0.9040.1000
Support ID:
/45PH2jCEkZKZmIRrcNVbQwsiY4f/sUt+eT5jnbUcKA=

© Microsoft. All rights reserved.
This program is licensed.

Creating a Collection



Icon	Name
	All User Groups
	All Users
	All Users and User Groups



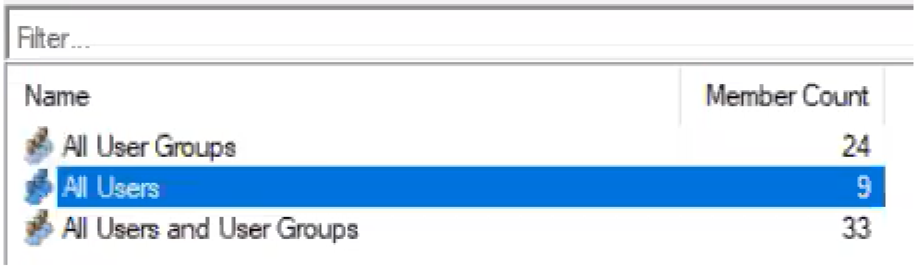
Specify details for this collection

Name: User Collection Direct Rule

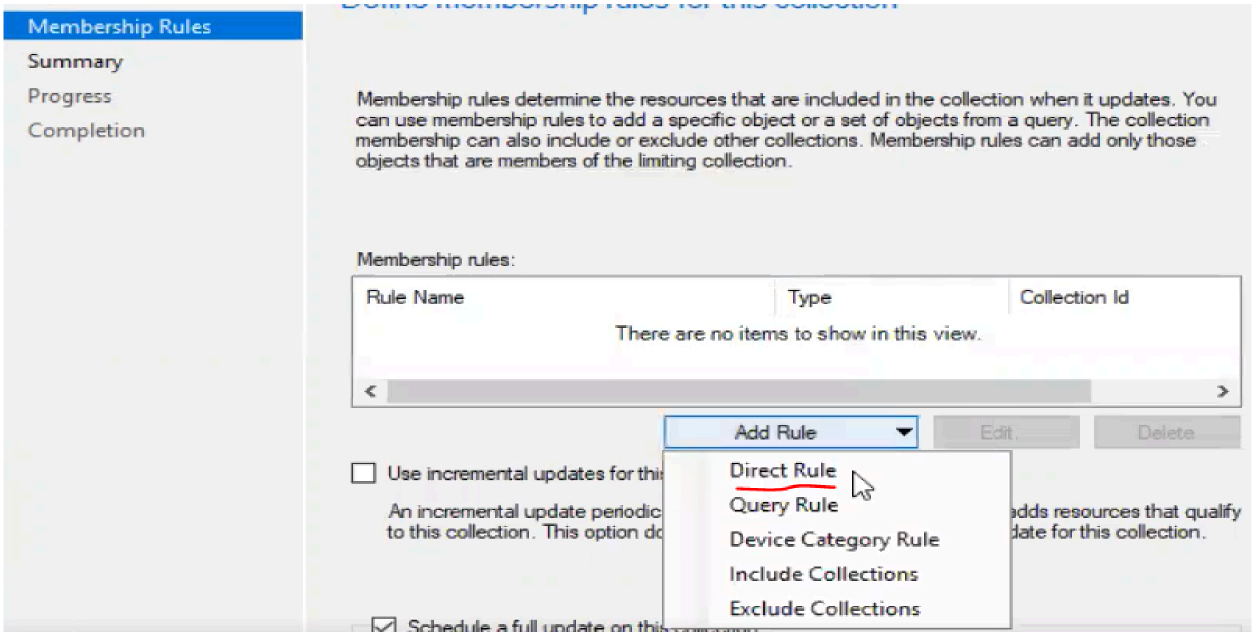
Comment:

Select a collection to use as a limiting collection. The limiting collection establishes the resources that you can add to this collection by using membership rules.

Limiting collection:



Name	Member Count
All User Groups	24
All Users	9
All Users and User Groups	33



- 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.

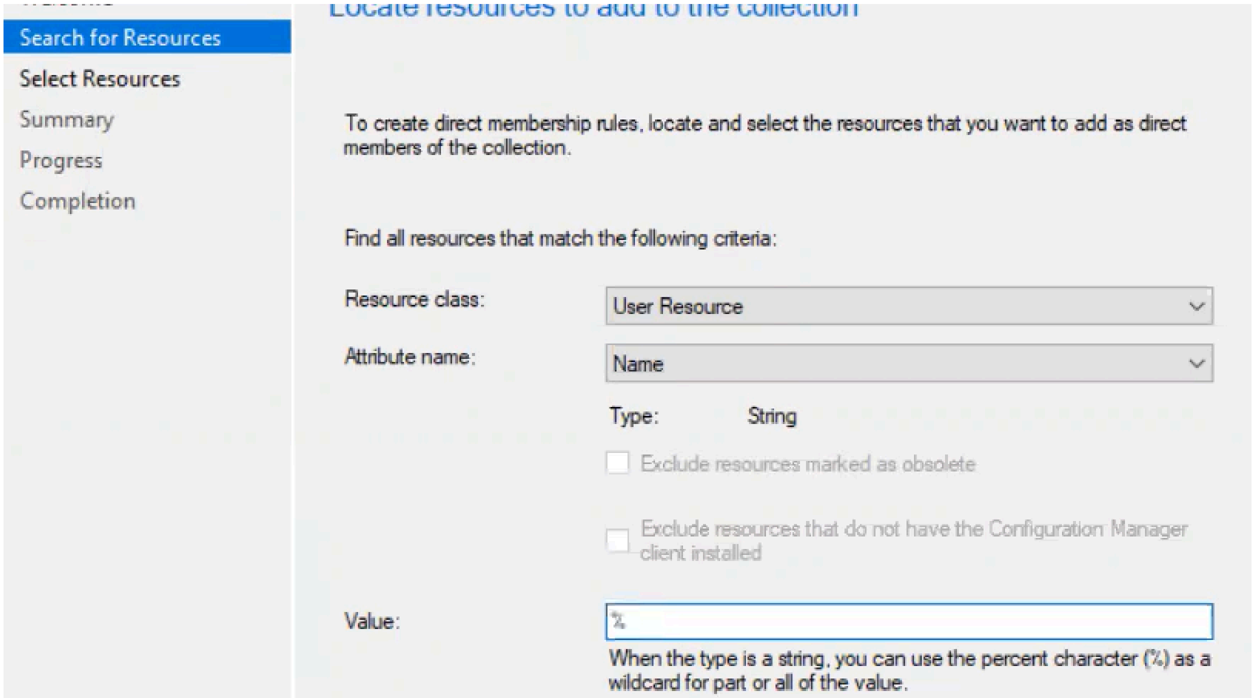
Membership rules:

Rule Name	Type	Collection Id
There are no items to show in this view.		

□ Use incremental updates for thi

An incremental update periodic ... adds resources that qualify to this collection. This option do ... date for this collection.

☑ Schedule a full update on this collection



- Welcome
- Search for Resources
- Select Resources
- Summary
- Progress
- Completion

Locate resources to add to the collection

To create direct membership rules, locate and select the resources that you want to add as direct members of the collection.

Find all resources that match the following criteria:

Resource class: User Resource

Attribute name: Name

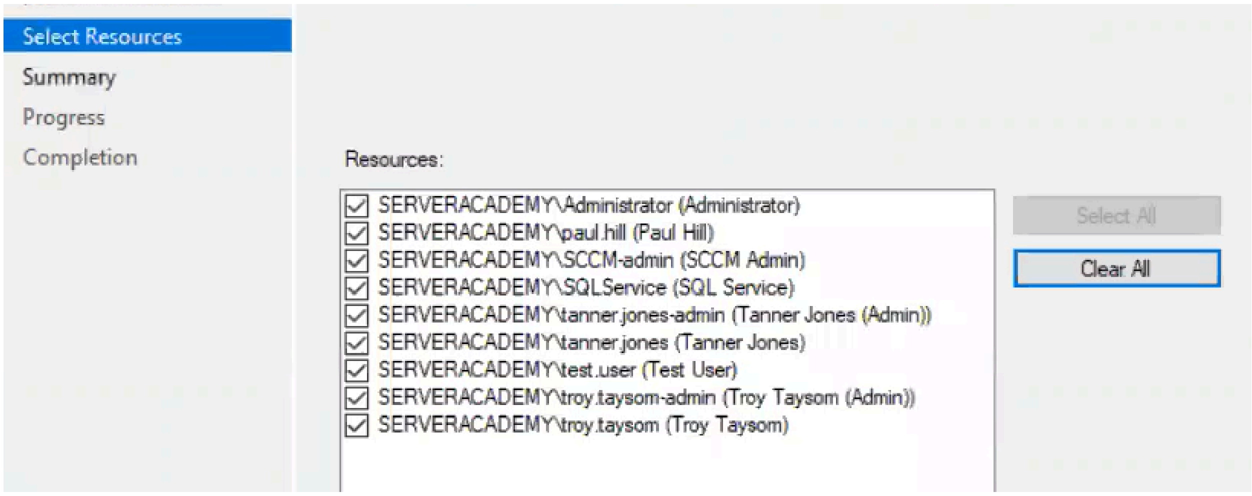
Type: String

□ Exclude resources marked as obsolete

□ Exclude resources that do not have the Configuration Manager client installed

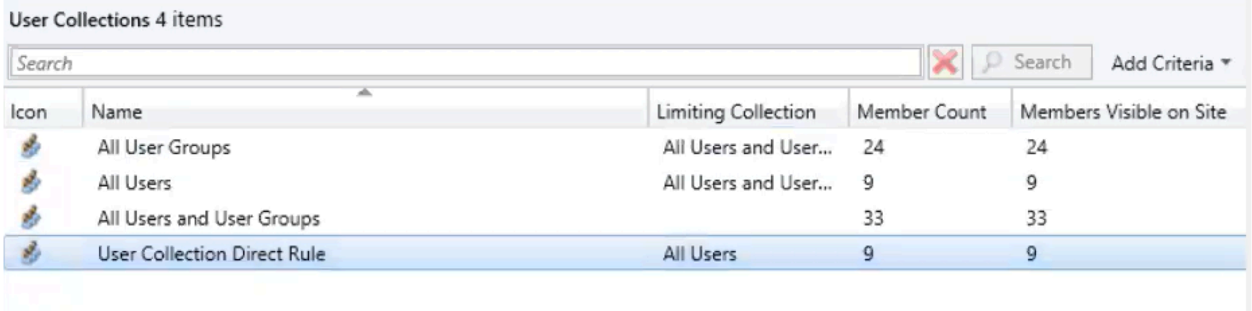
Value: %

When the type is a string, you can use the percent character (%) as a wildcard for part or all of the value.



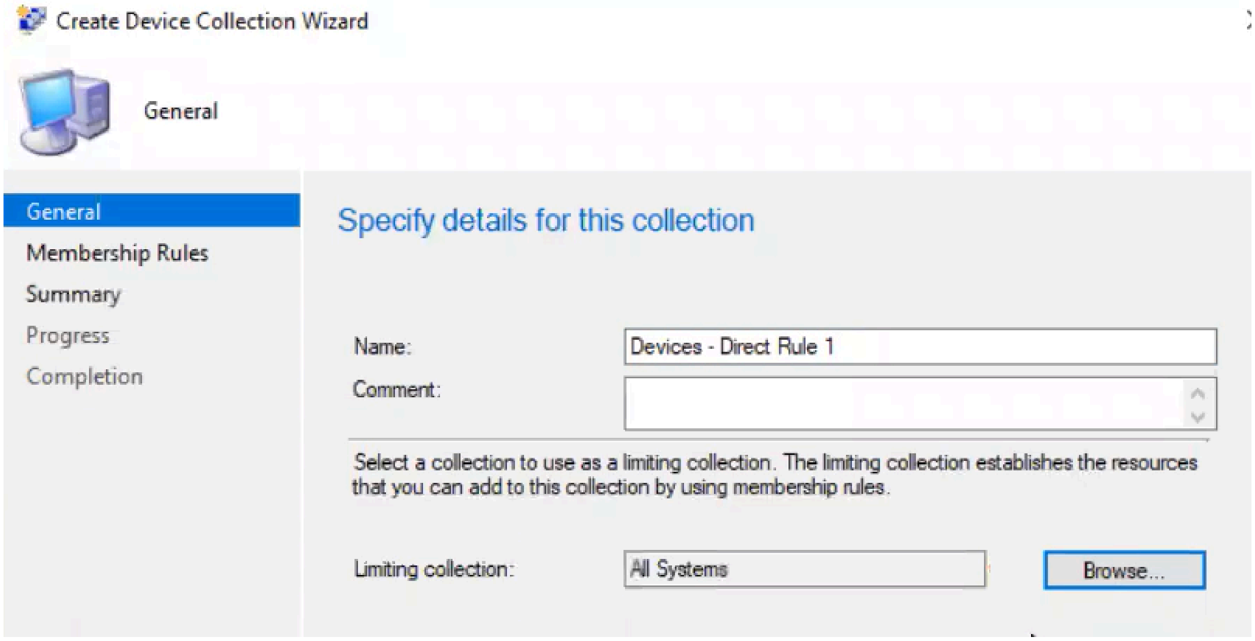
Resources:

☑ SERVERACADEMY\Administrator (Administrator)
☑ SERVERACADEMY\paul.hill (Paul Hill)
☑ SERVERACADEMY\SCCM-admin (SCCM Admin)
☑ SERVERACADEMY\SQLService (SQL Service)
☑ SERVERACADEMY\tanner.jones-admin (Tanner Jones (Admin))
☑ SERVERACADEMY\tanner.jones (Tanner Jones)
☑ SERVERACADEMY\test.user (Test User)
☑ SERVERACADEMY\troy.taysom-admin (Troy Taysom (Admin))
☑ SERVERACADEMY\troy.taysom (Troy Taysom)



User Collections 4 items

Icon	Name	Limiting Collection	Member Count	Members Visible on Site
	All User Groups	All Users and User...	24	24
	All Users	All Users and User...	9	9
	All Users and User Groups		33	33
	User Collection Direct Rule	All Users	9	9



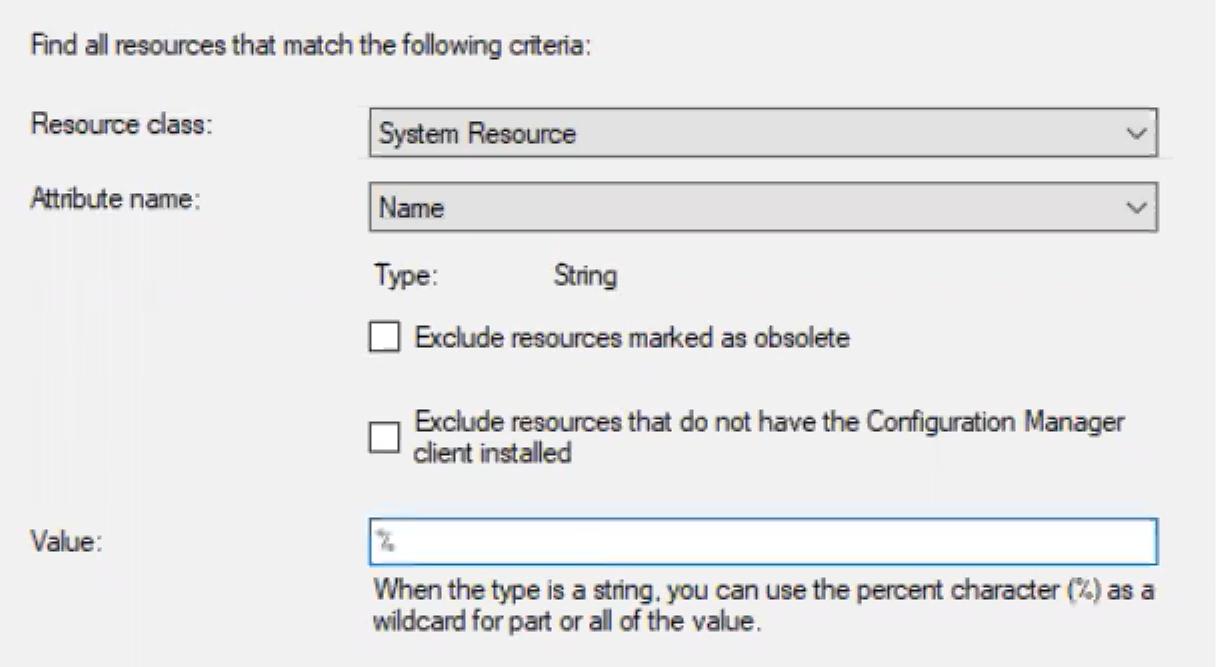
Specify details for this collection

Name: Devices - Direct Rule 1

Comment:

Select a collection to use as a limiting collection. The limiting collection establishes the resources that you can add to this collection by using membership rules.

Limiting collection: All Systems



Find all resources that match the following criteria:

Resource class: System Resource

Attribute name: Name

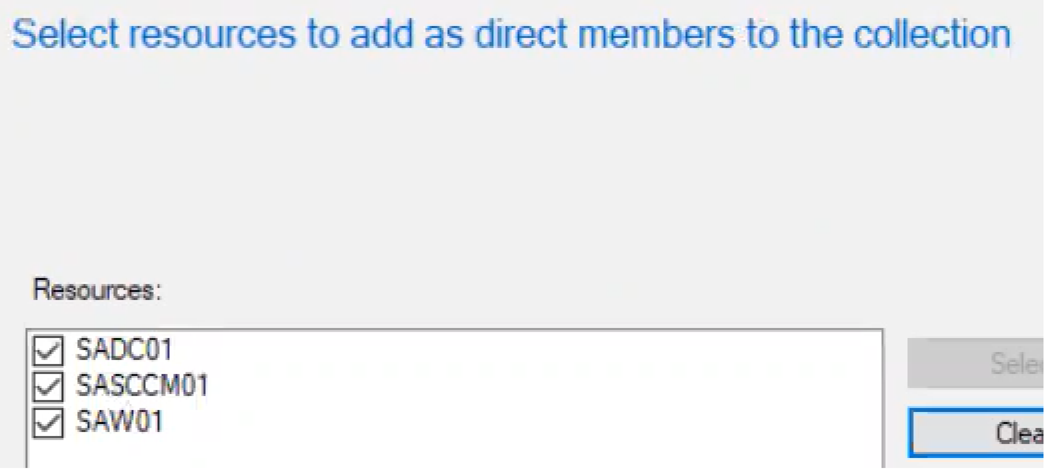
Type: String

□ Exclude resources marked as obsolete

□ Exclude resources that do not have the Configuration Manager client installed

Value: %

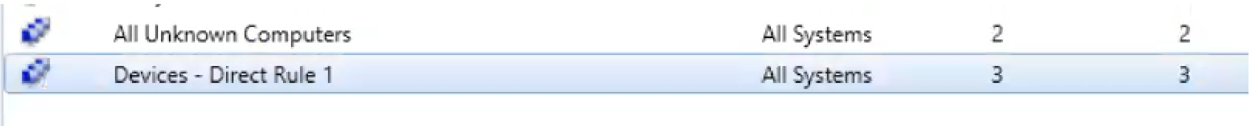
When the type is a string, you can use the percent character (%) as a wildcard for part or all of the value.



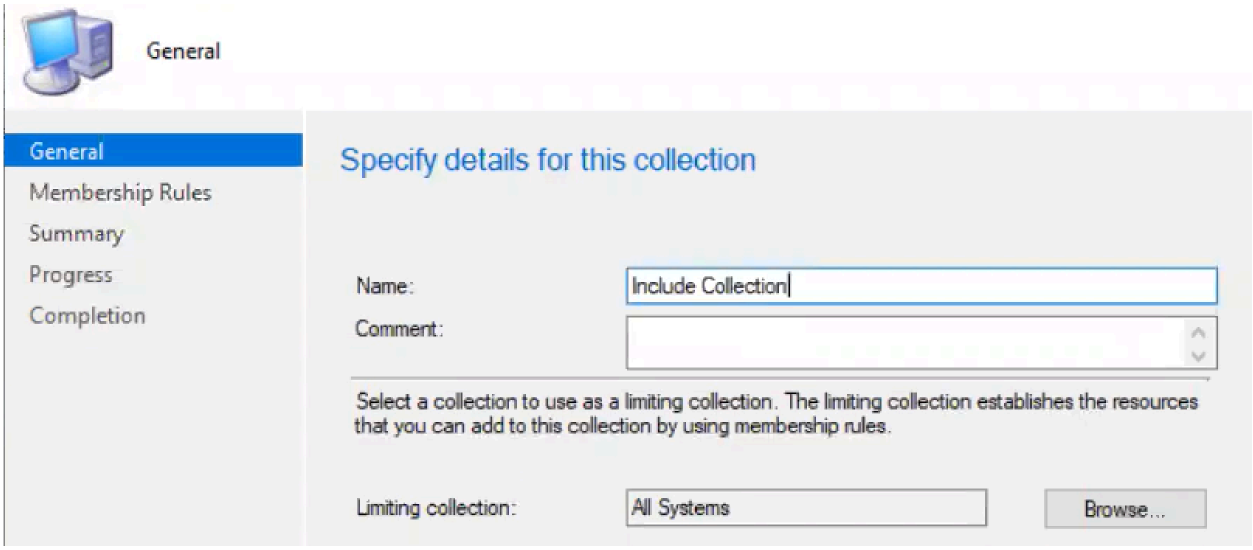
Select resources to add as direct members to the collection

Resources:

☑ SADC01
☑ SASCCM01
☑ SAW01



All Unknown Computers	All Systems	2	2
Devices - Direct Rule 1	All Systems	3	3



General

- General
- Membership Rules
- Summary
- Progress
- Completion

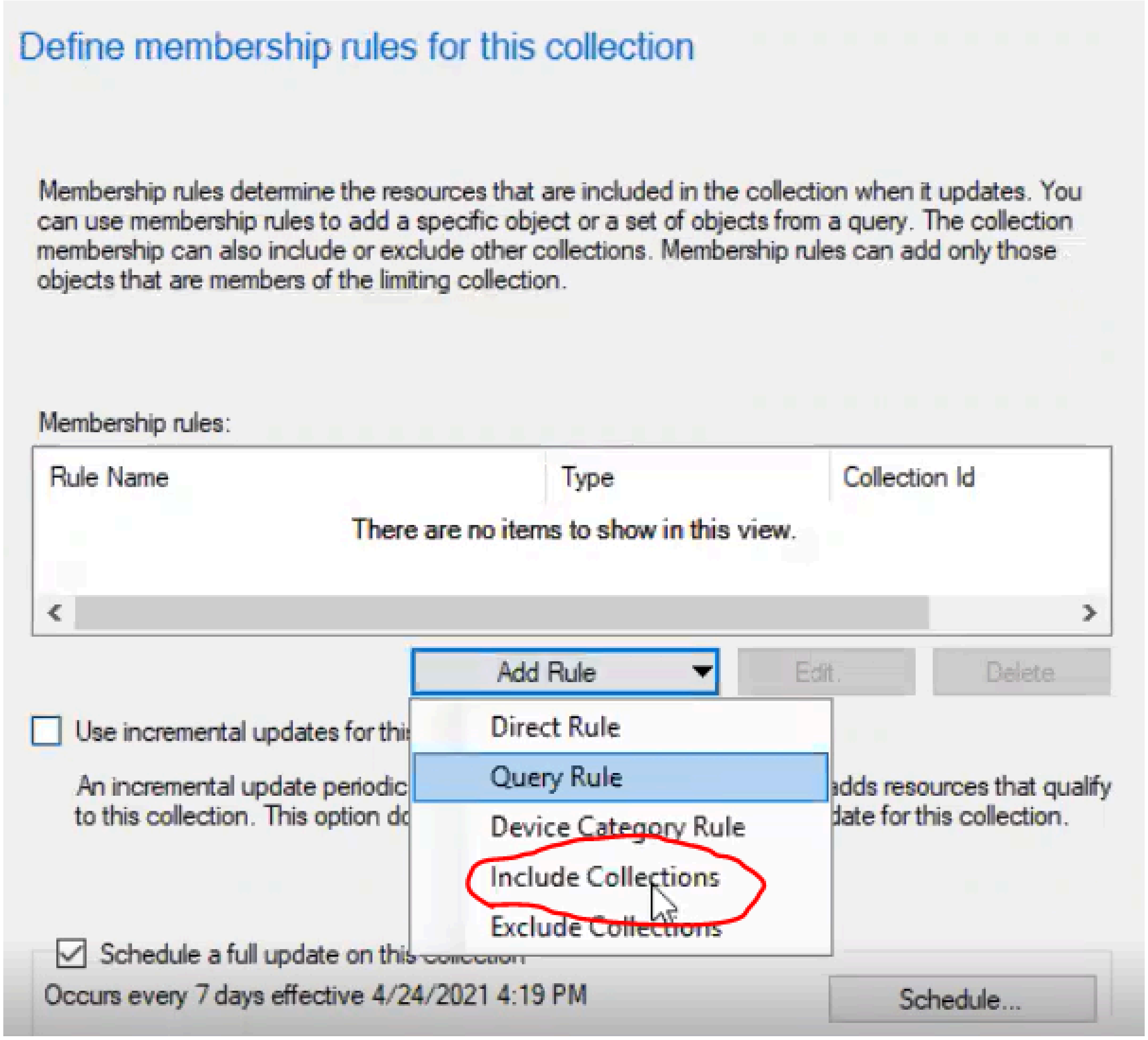
Specify details for this collection

Name: Include Collection

Comment:

Select a collection to use as a limiting collection. The limiting collection establishes the resources that you can add to this collection by using membership rules.

Limiting collection: All Systems



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:

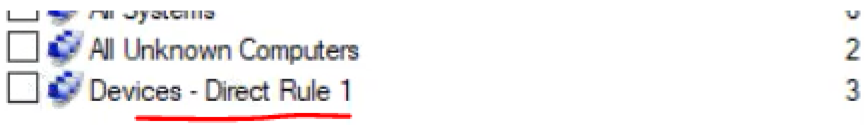
Rule Name	Type	Collection Id
There are no items to show in this view.		

□ Use incremental updates for thi

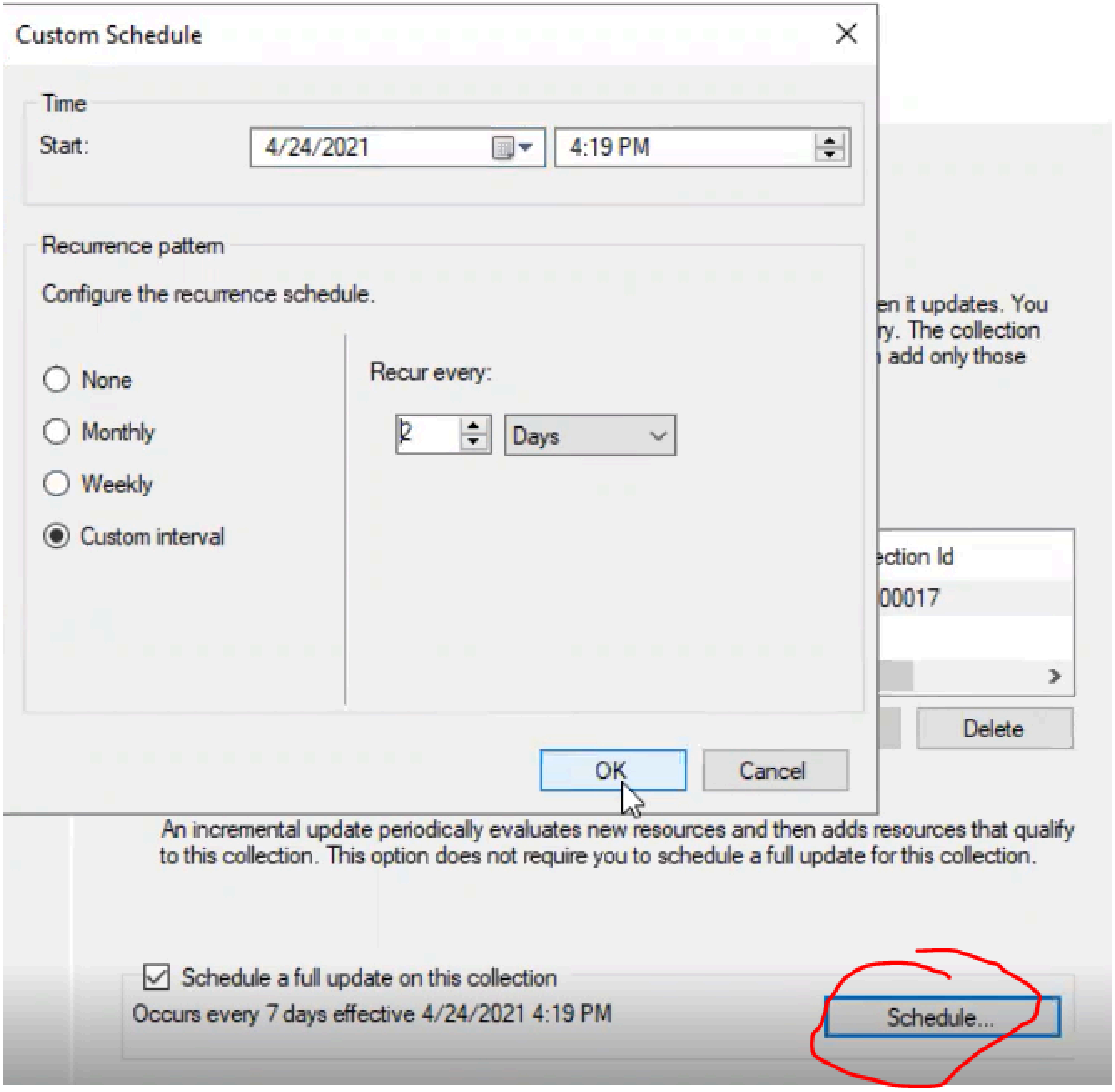
An incremental update periodic adds resources that qualify to this collection. This option d date for this collection.

☑ Schedule a full update on this collection

Occurs every 7 days effective 4/24/2021 4:19 PM



□ All Systems	0
□ All Unknown Computers	2
□ Devices - Direct Rule 1	3



Custom Schedule

Time

Start: 4/24/2021 4:19 PM

Recurrence pattern

Configure the recurrence schedule.

○ None

○ Monthly

○ Weekly

● Custom interval

Recur every: 2 Days

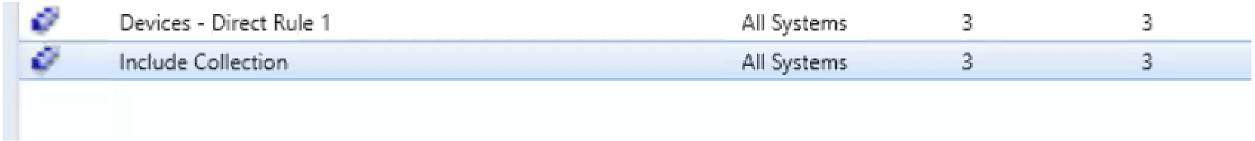
en it updates. You
ry. The collection
add only those

ction Id
00017

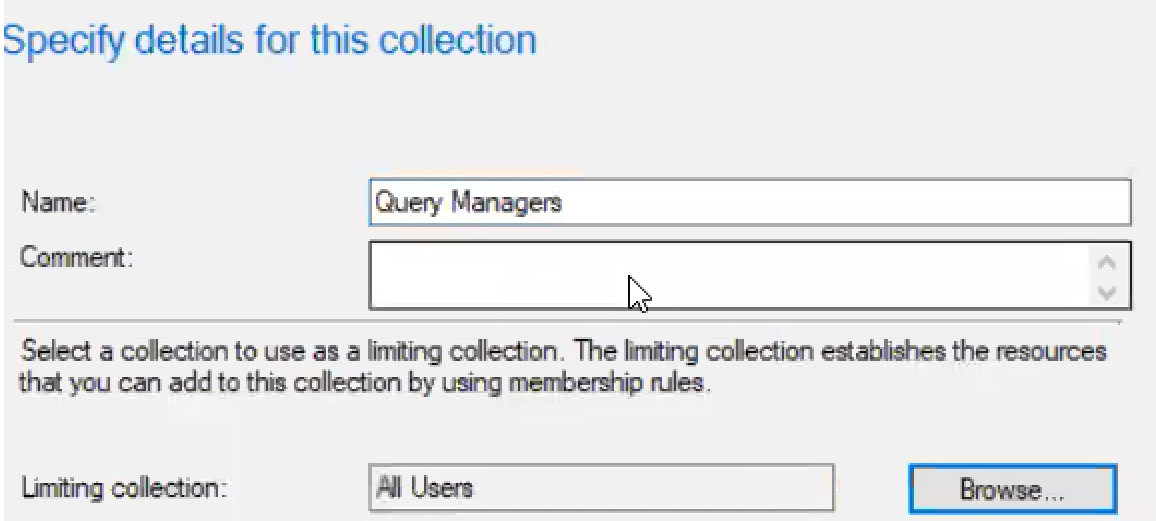
An incremental update periodically evaluates new resources and then adds resources that qualify to this collection. This option does not require you to schedule a full update for this collection.

☑ Schedule a full update on this collection

Occurs every 7 days effective 4/24/2021 4:19 PM



Devices - Direct Rule 1	All Systems	3	3
Include Collection	All Systems	3	3



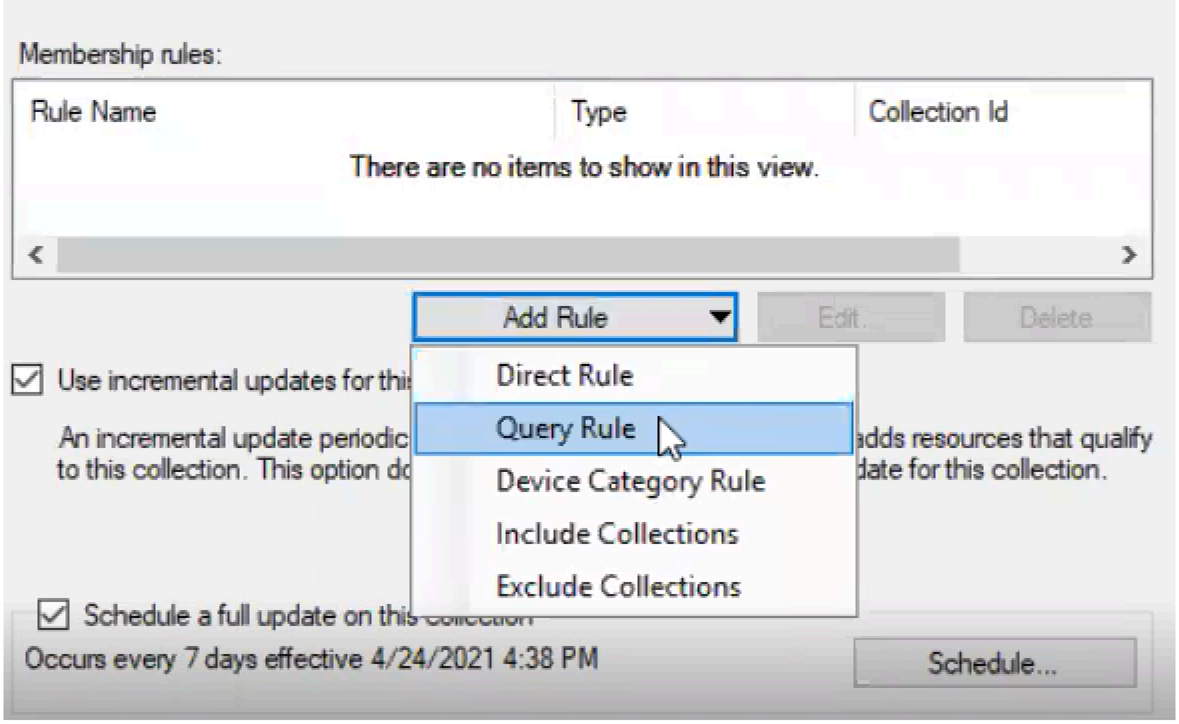
Specify details for this collection

Name: Query Managers

Comment:

Select a collection to use as a limiting collection. The limiting collection establishes the resources that you can add to this collection by using membership rules.

Limiting collection: All Users



Membership rules:

Rule Name	Type	Collection Id

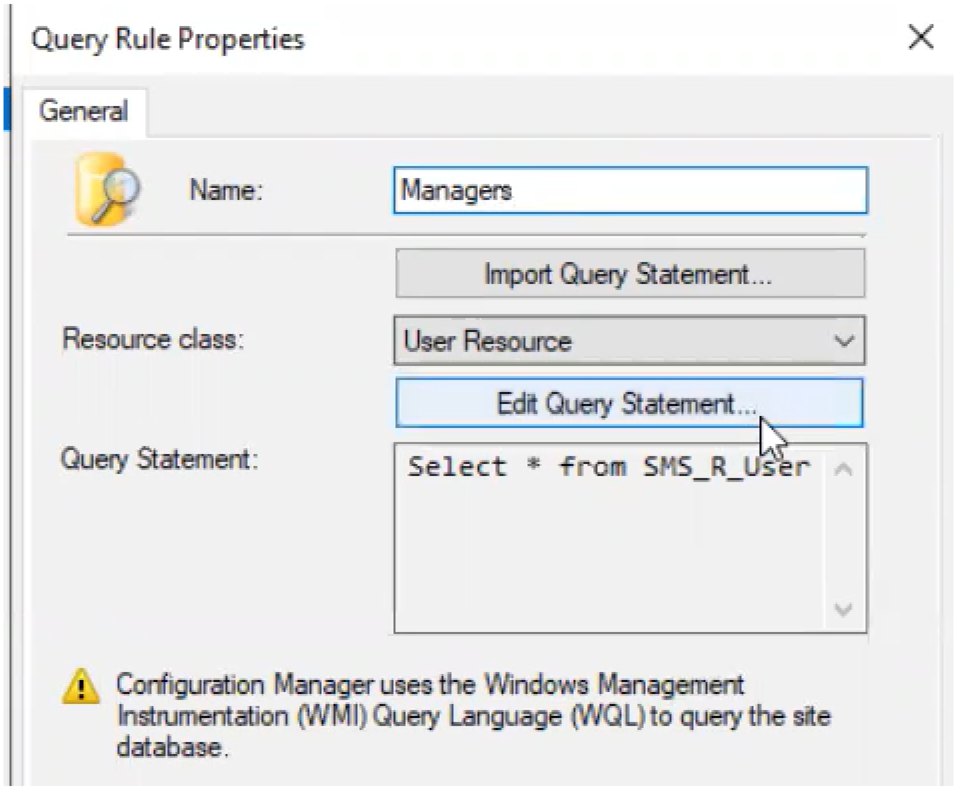
There are no items to show in this view.

☑ Use incremental updates for thi

An incremental update periodic adds resources that qualify to this collection. This option do date for this collection.

☑ Schedule a full update on this collection

Occurs every 7 days effective 4/24/2021 4:38 PM



Query Rule Properties

General

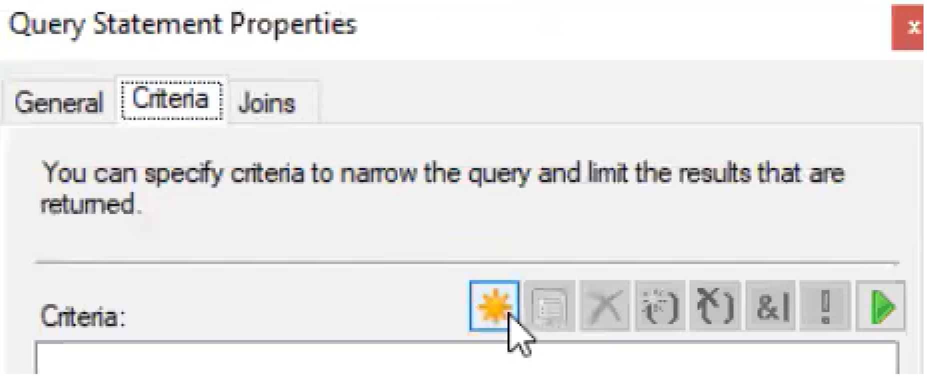
Name: Managers

Resource class: User Resource

Query Statement:

```
Select * from SMS_R_User
```

Configuration Manager uses the Windows Management Instrumentation (WMI) Query Language (WQL) to query the site database.

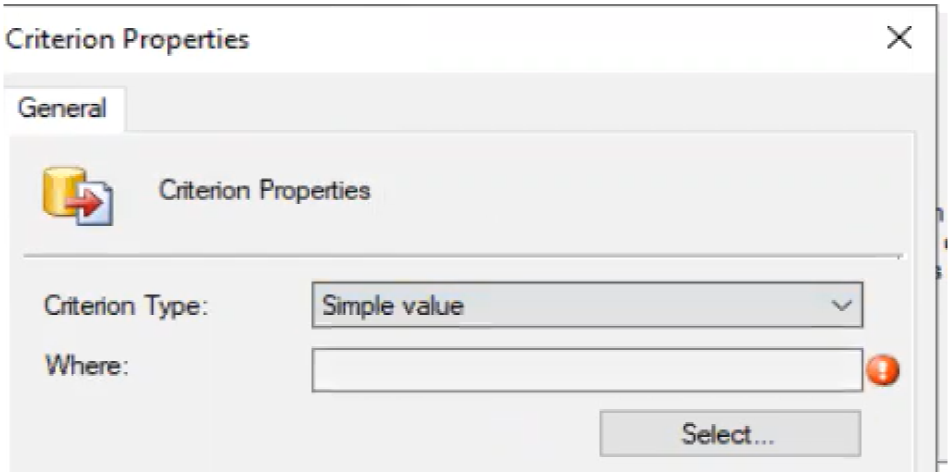


Query Statement Properties

General | Criteria | Joins

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

Criteria:



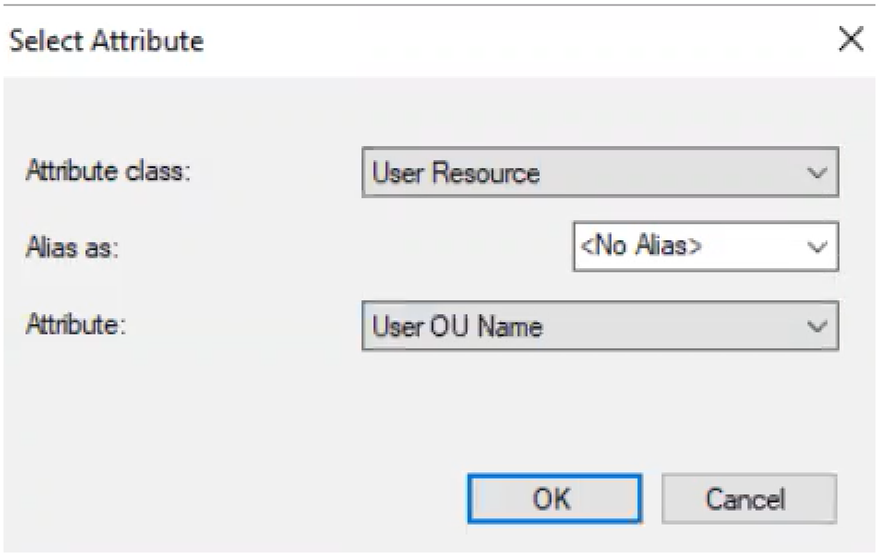
Criterion Properties

General

Criterion Properties

Criterion Type: Simple value

Where:

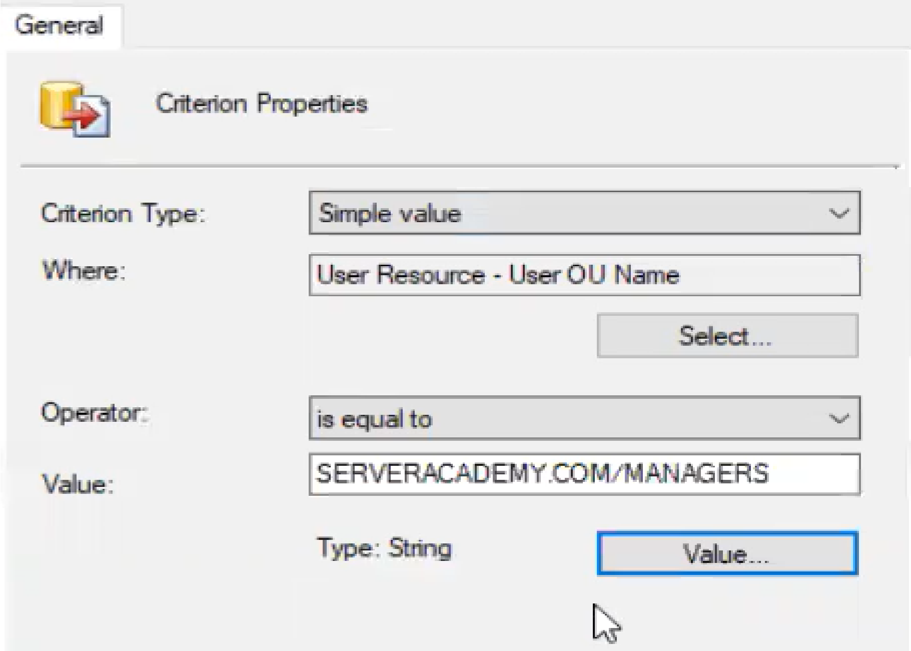


Select Attribute

Attribute class: User Resource

Alias as: <No Alias>

Attribute: User OU Name



General

Criterion Properties

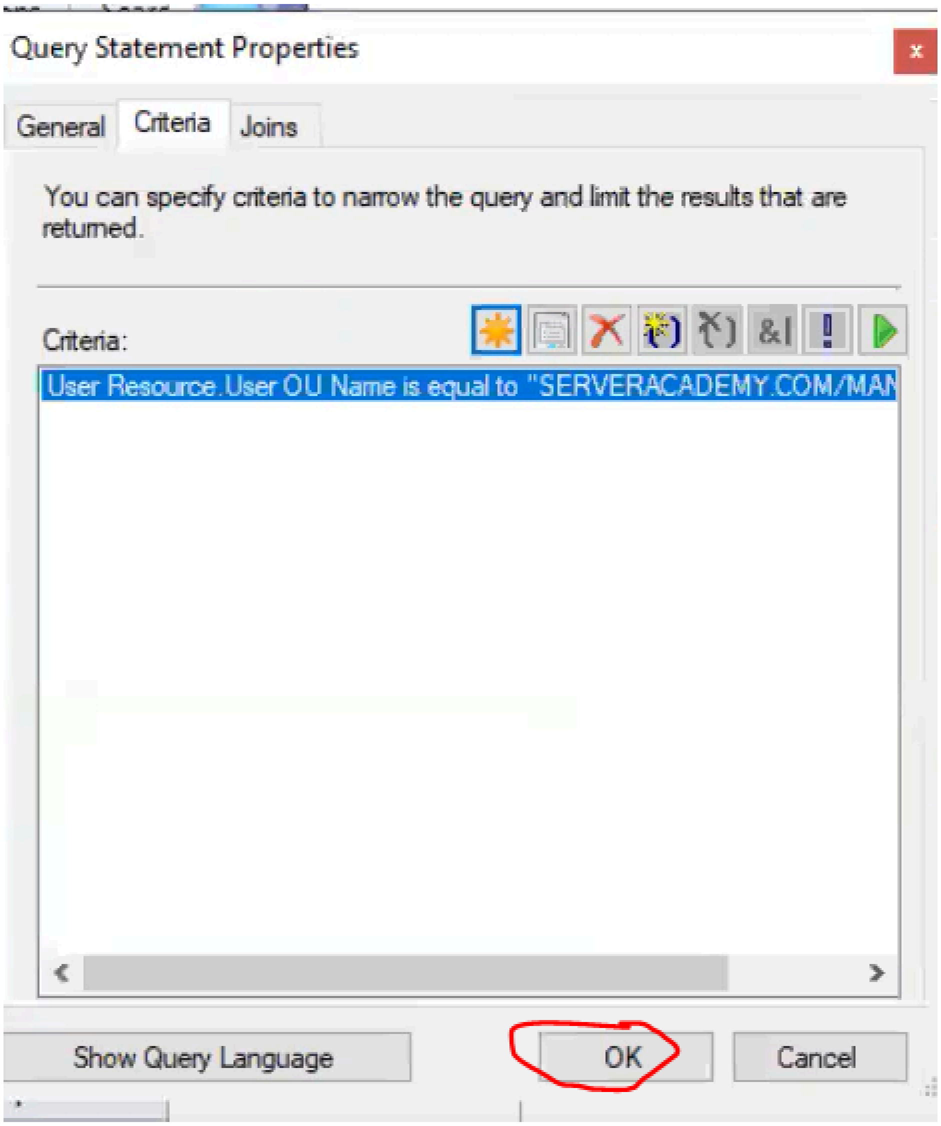
Criterion Type: Simple value

Where: User Resource - User OU Name

Operator: is equal to

Value: SERVERACADEMY.COM/MANAGERS

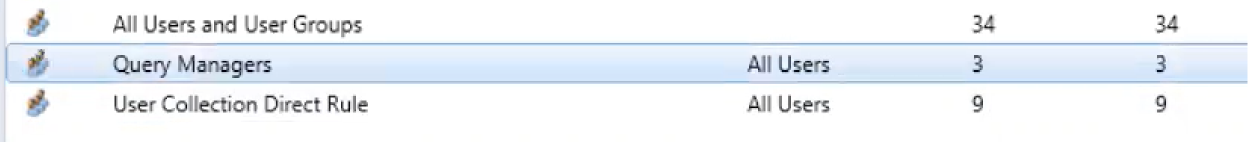
Type: String



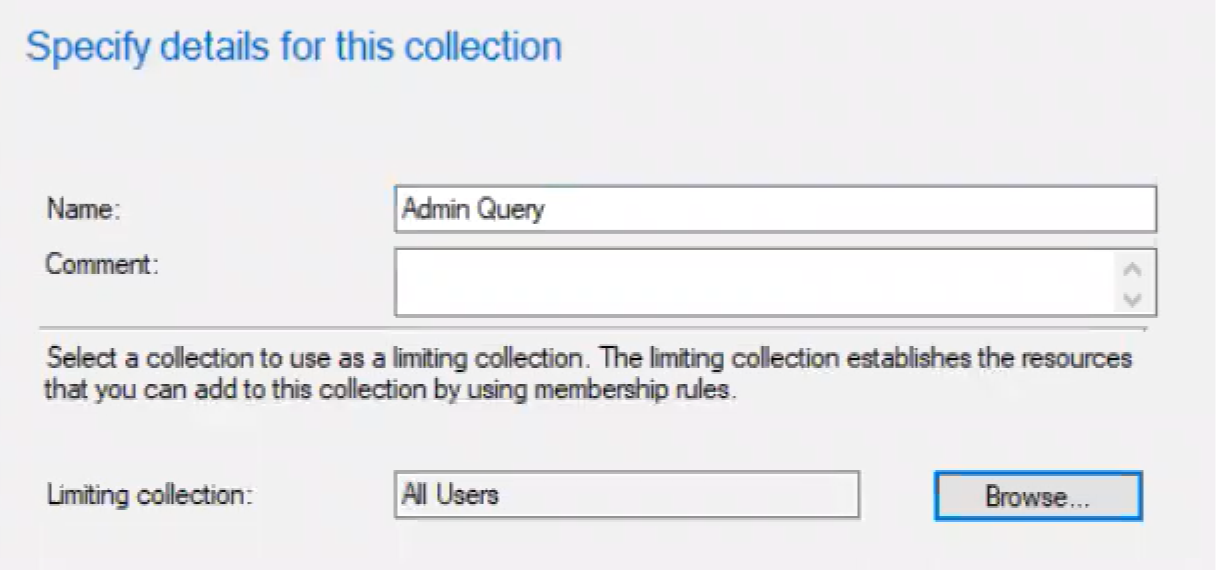
You can specify criteria to narrow the query and limit the results that are returned.

Criteria:

User Resource.User OU Name is equal to "SERVERACADEMY.COM/MAN



All Users and User Groups		34	34
Query Managers	All Users	3	3
User Collection Direct Rule	All Users	9	9



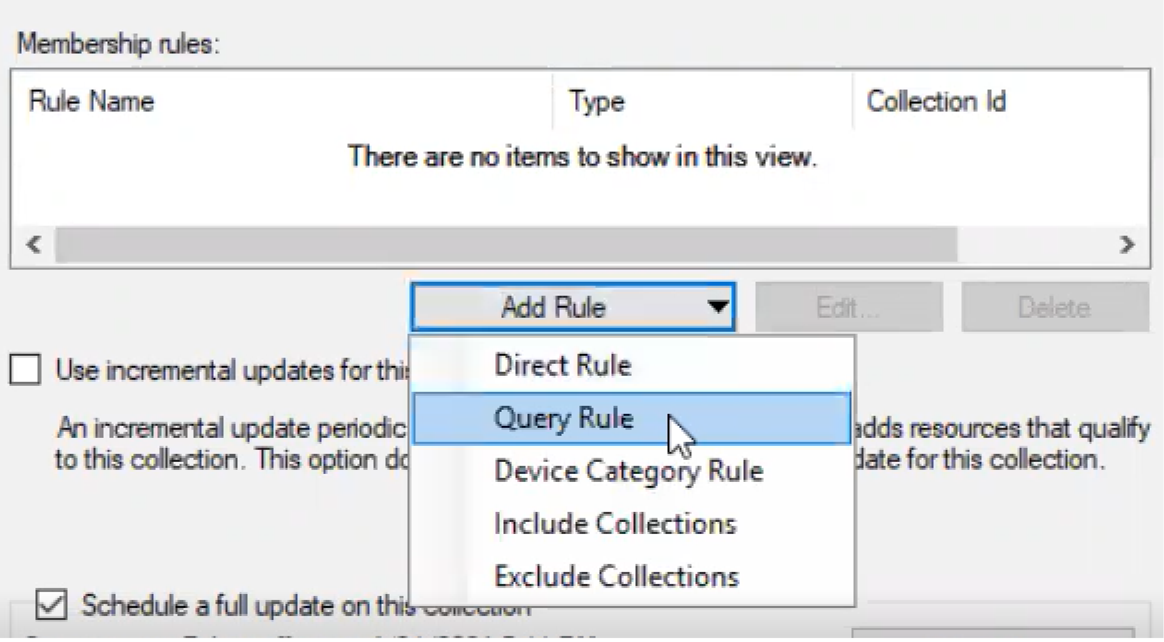
Specify details for this collection

Name: Admin Query

Comment:

Select a collection to use as a limiting collection. The limiting collection establishes the resources that you can add to this collection by using membership rules.

Limiting collection: All Users



Membership rules:

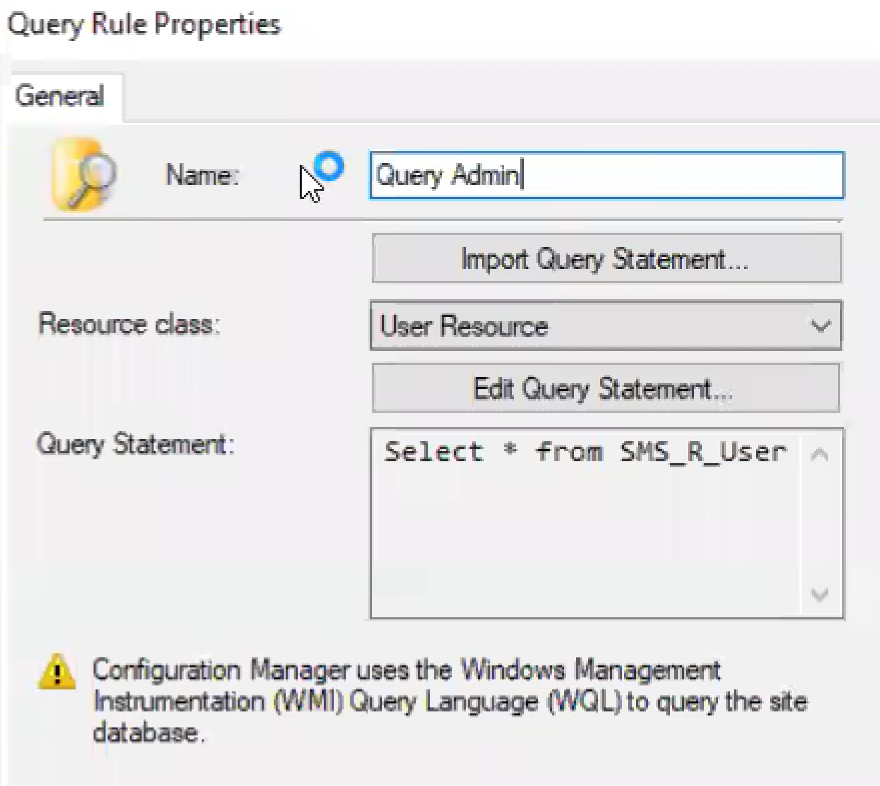
Rule Name	Type	Collection Id

There are no items to show in this view.

□ Use incremental updates for thi

An incremental update periodic adds resources that qualify to this collection. This option do date for this collection.

☑ Schedule a full update on this collection



Query Rule Properties

General

Name: Query Admin

Import Query Statement...

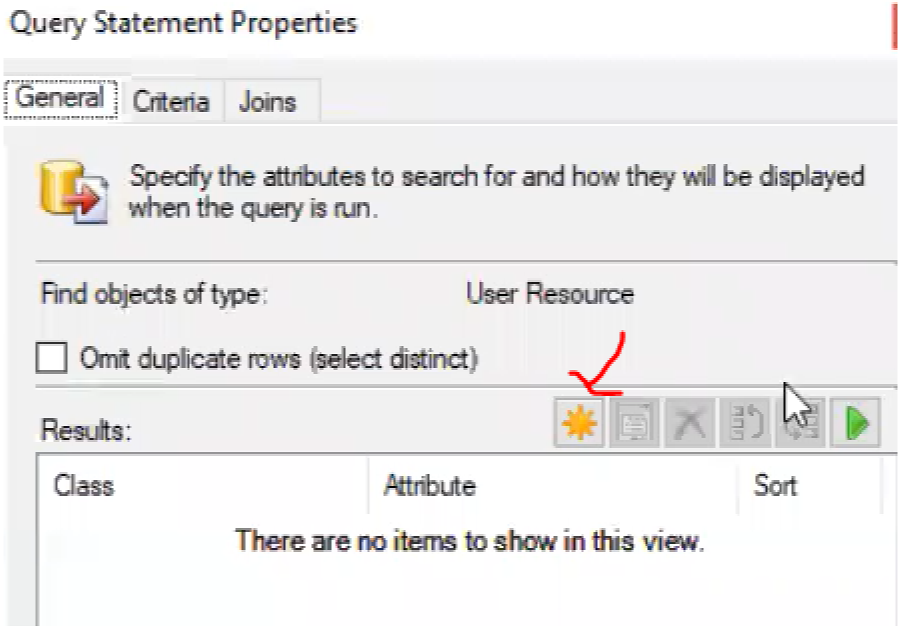
Resource class: User Resource

Edit Query Statement...

Query Statement:

```
Select * from SMS_R_User
```

Configuration Manager uses the Windows Management Instrumentation (WMI) Query Language (WQL) to query the site database.



Query Statement Properties

Specify the attributes to search for and how they will be displayed when the query is run.

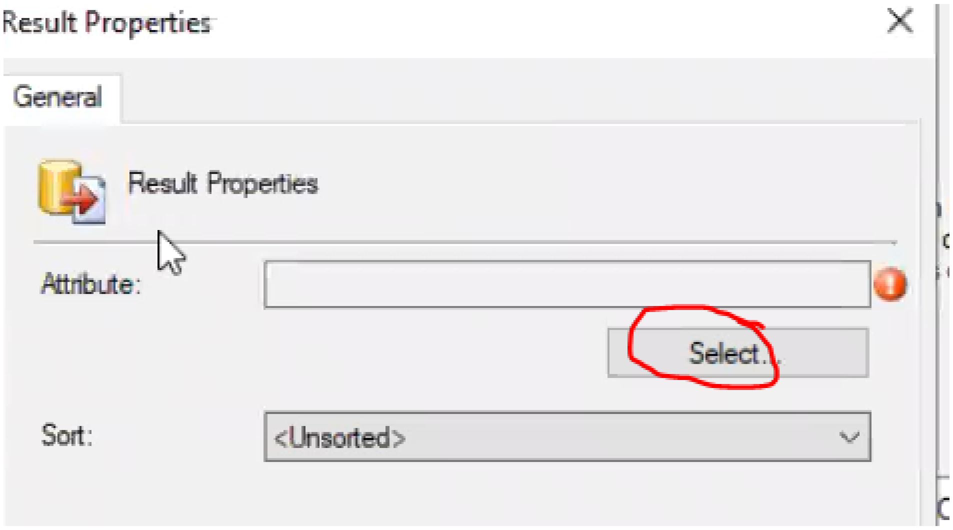
Find objects of type: User Resource

□ Omit duplicate rows (select distinct)

Results:

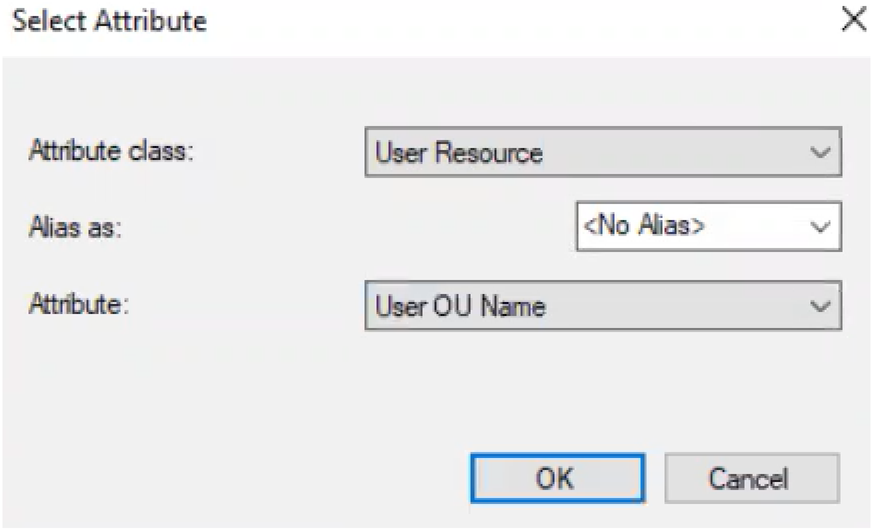
Class	Attribute	Sort

There are no items to show in this view.



Attribute:

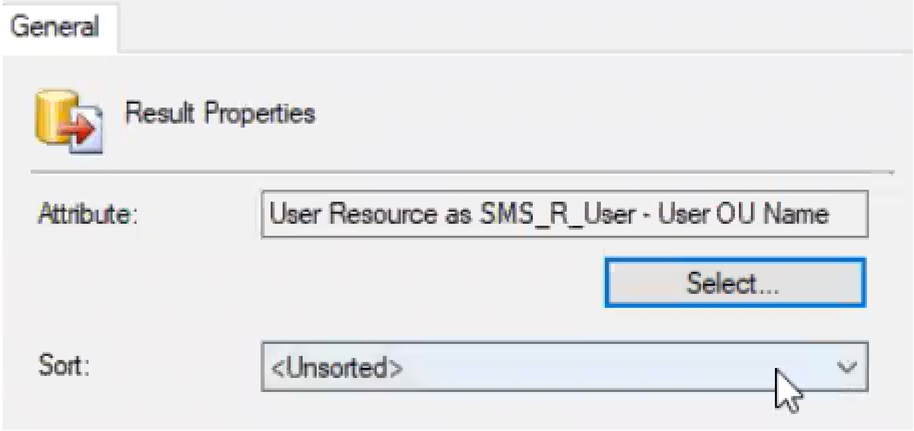
Sort: <Unsorted>



Attribute class: User Resource

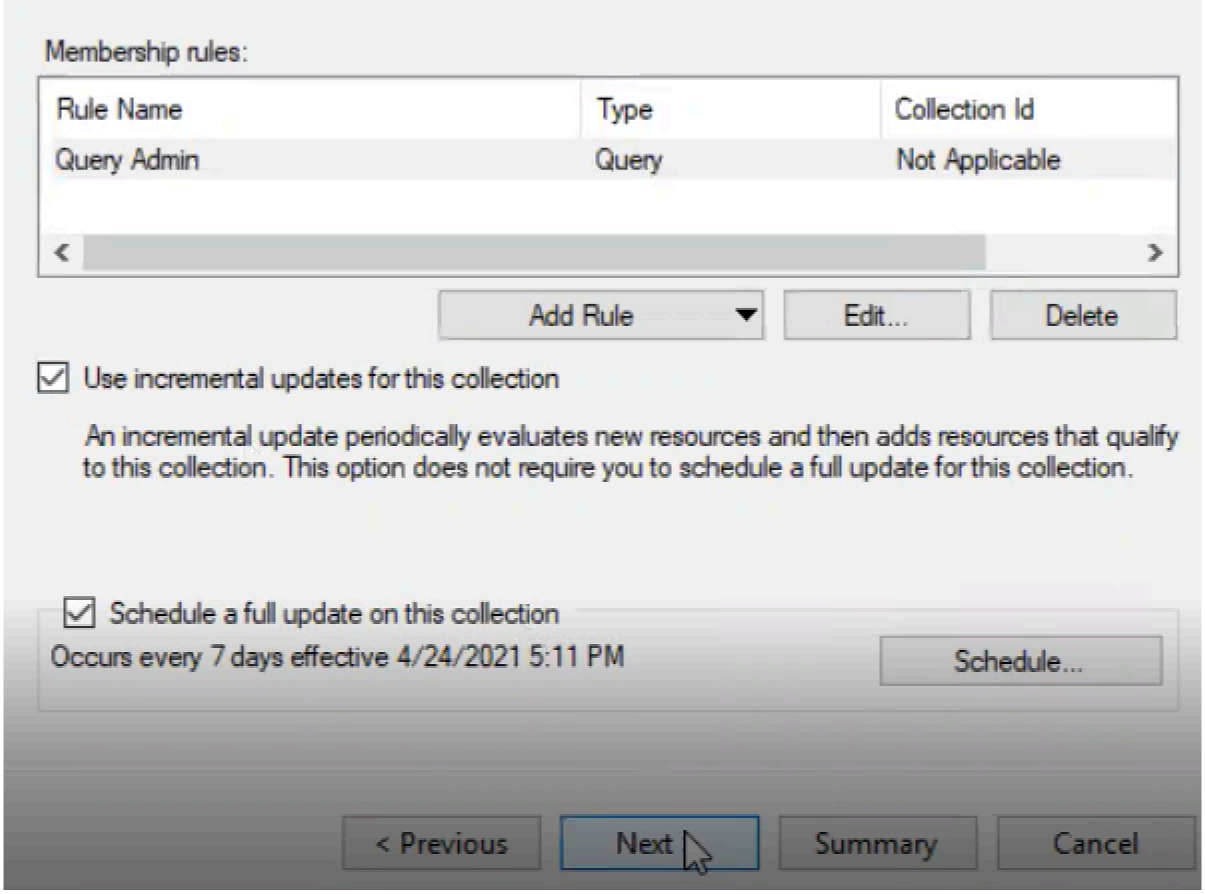
Alias as: <No Alias>

Attribute: User OU Name



Attribute: User Resource as SMS_R_User - User OU Name

Sort: <Unsorted>



Membership rules:

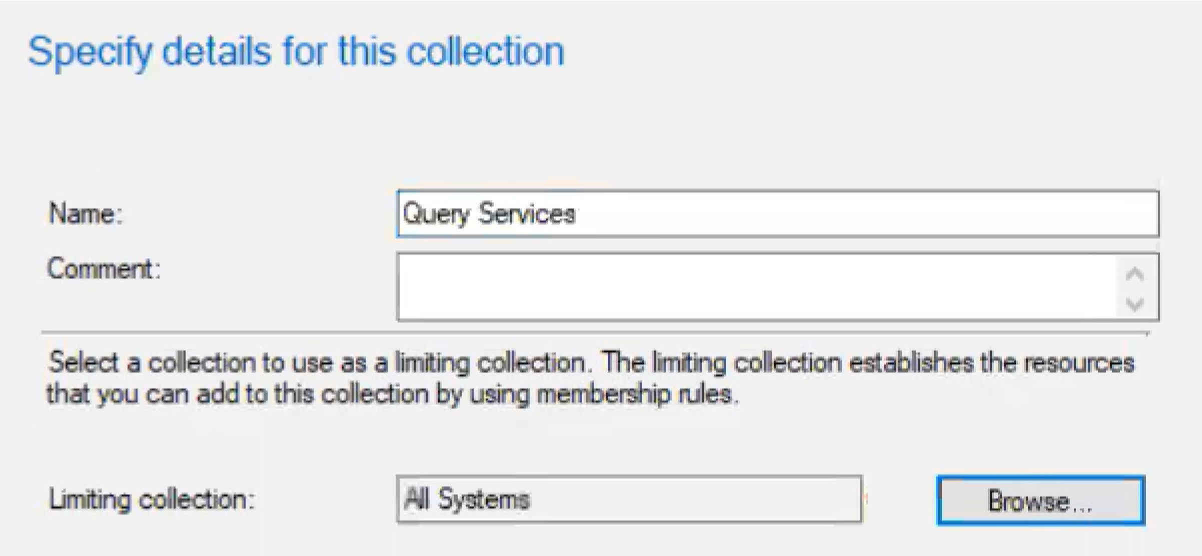
Rule Name	Type	Collection Id
Query Admin	Query	Not Applicable

☑ 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 4/24/2021 5:11 PM



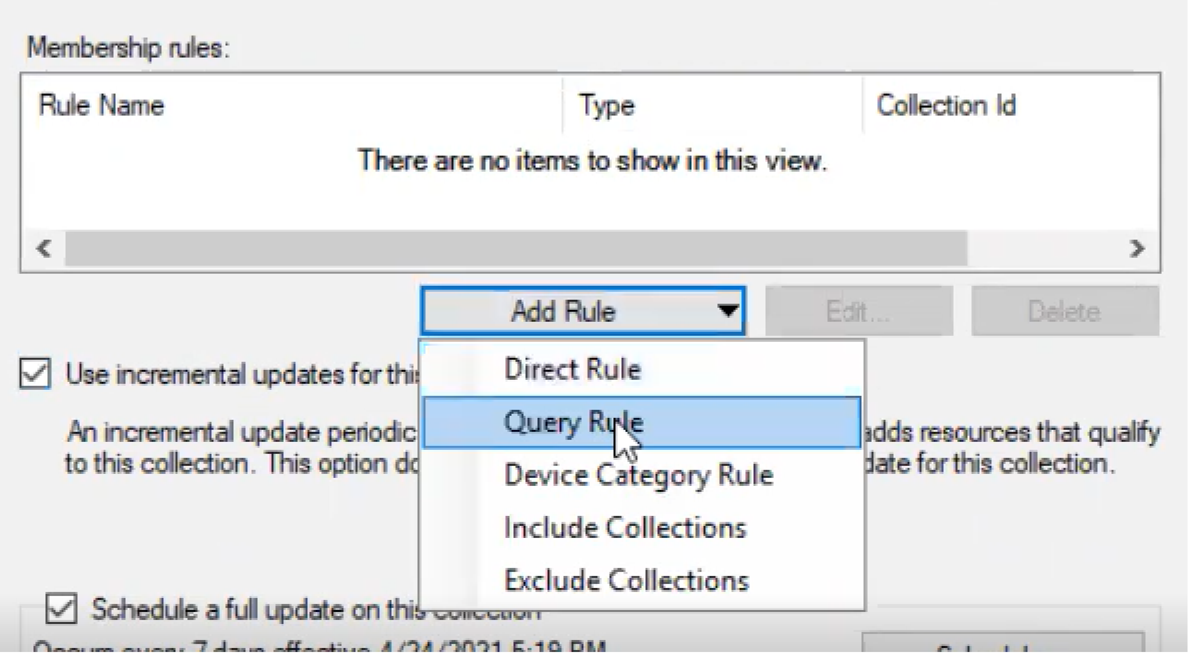
Specify details for this collection

Name: Query Services

Comment:

Select a collection to use as a limiting collection. The limiting collection establishes the resources that you can add to this collection by using membership rules.

Limiting collection: All Systems



Membership rules:

Rule Name	Type	Collection Id

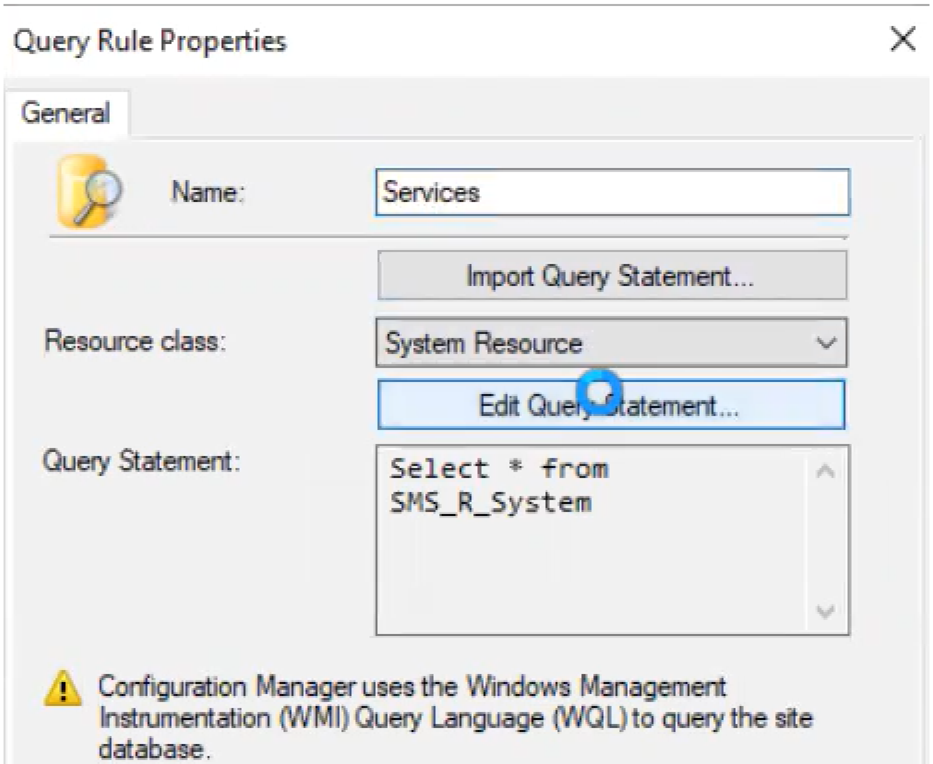
There are no items to show in this view.

☑ Use incremental updates for thi

An incremental update periodic adds resources that qualify to this collection. This option do date for this collection.

☑ Schedule a full update on this collection

Occurs every 7 days effective 4/24/2021 5:19 PM



Query Rule Properties

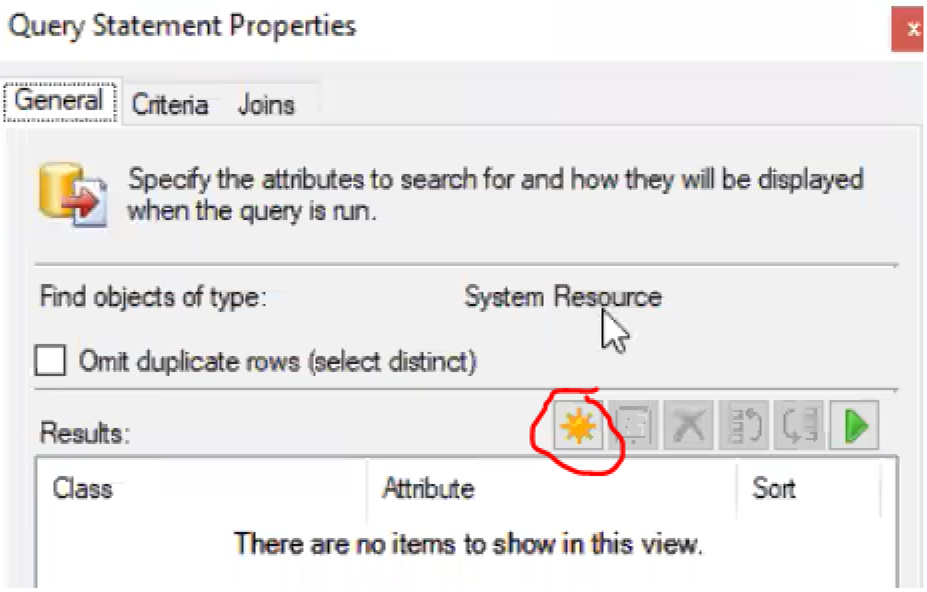
Name: Services

Resource class: System Resource

Query Statement:

```
Select * from
SMS_R_System
```

⚠ Configuration Manager uses the Windows Management Instrumentation (WMI) Query Language (WQL) to query the site database.



Specify the attributes to search for and how they will be displayed when the query is run.

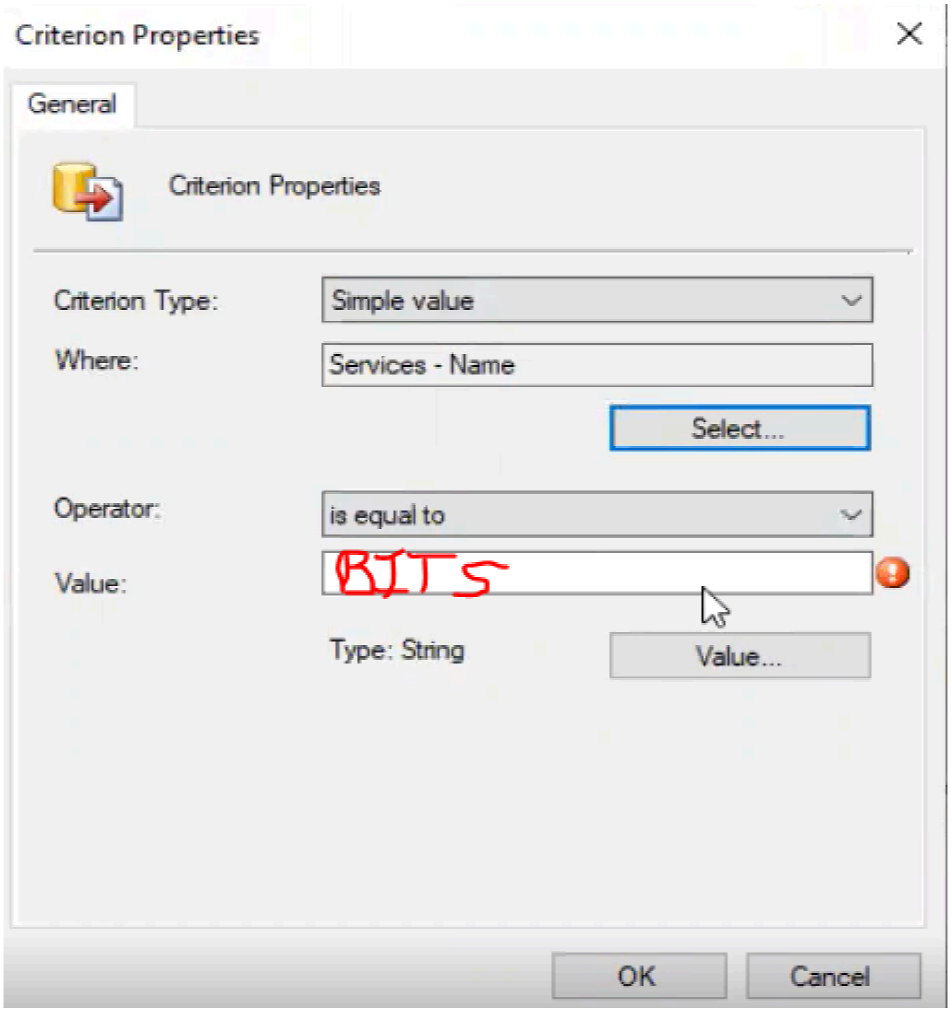
Find objects of type: System Resource

□ Omit duplicate rows (select distinct)

Results:

Class	Attribute	Sort

There are no items to show in this view.



Criterion Properties

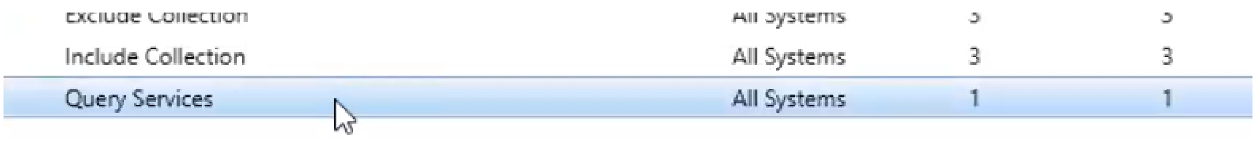
Criterion Type: Simple value

Where: Services - Name

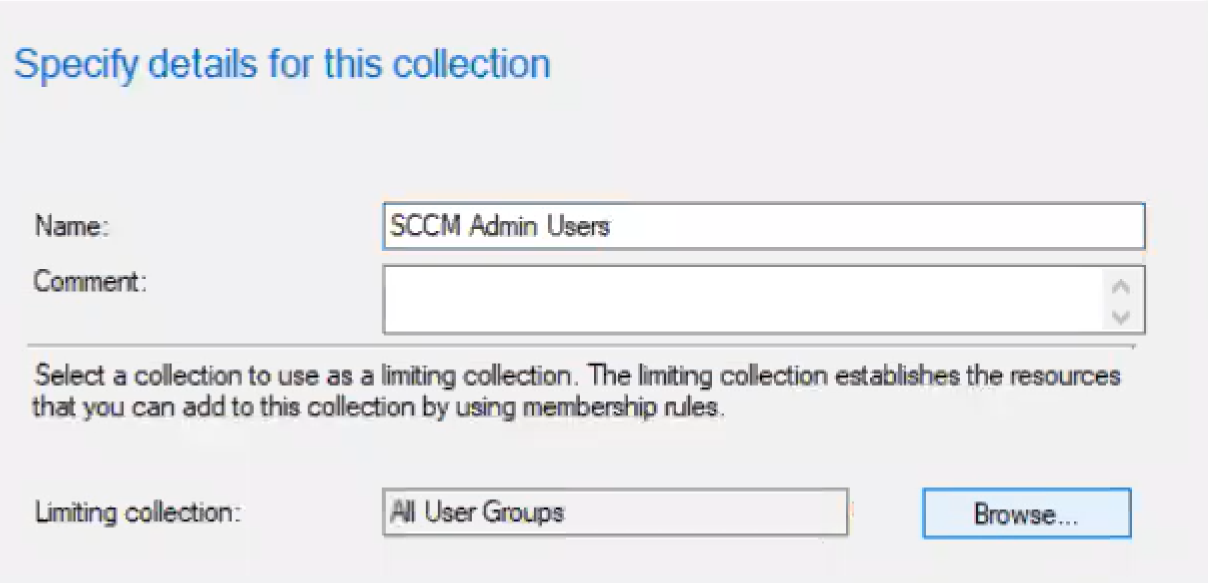
Operator: is equal to

Value: BITS

Type: String



Exclude Collection	All Systems	3	3
Include Collection	All Systems	3	3
Query Services	All Systems	1	1



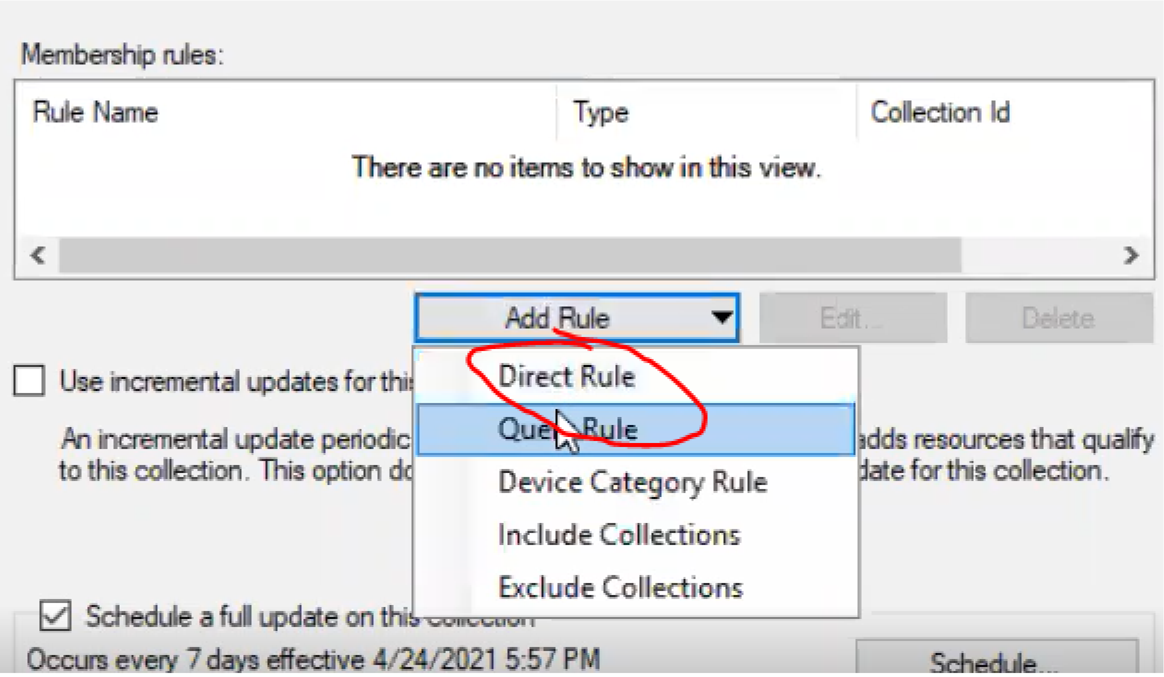
Specify details for this collection

Name: SCCM Admin Users

Comment:

Select a collection to use as a limiting collection. The limiting collection establishes the resources that you can add to this collection by using membership rules.

Limiting collection: All User Groups



Membership rules:

Rule Name	Type	Collection Id

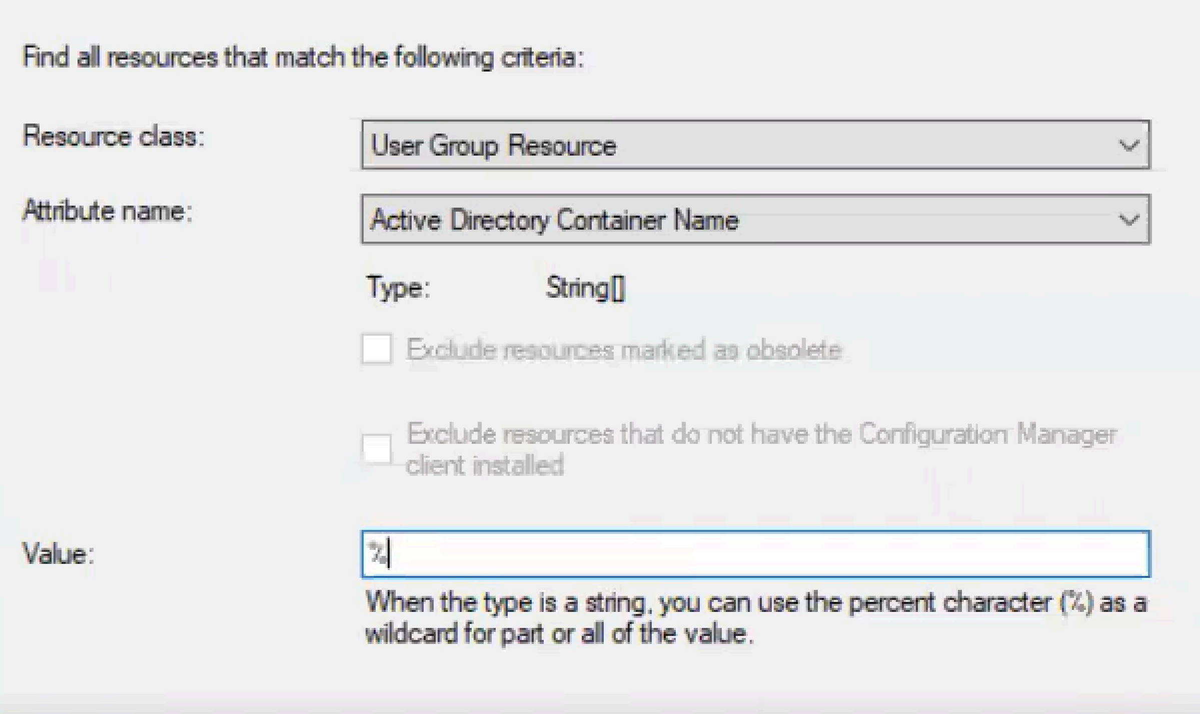
There are no items to show in this view.

□ Use incremental updates for thi

An incremental update periodic adds resources that qualify to this collection. This option do date for this collection.

☑ Schedule a full update on this collection

Occurs every 7 days effective 4/24/2021 5:57 PM



Find all resources that match the following criteria:

Resource class: User Group Resource

Attribute name: Active Directory Container Name

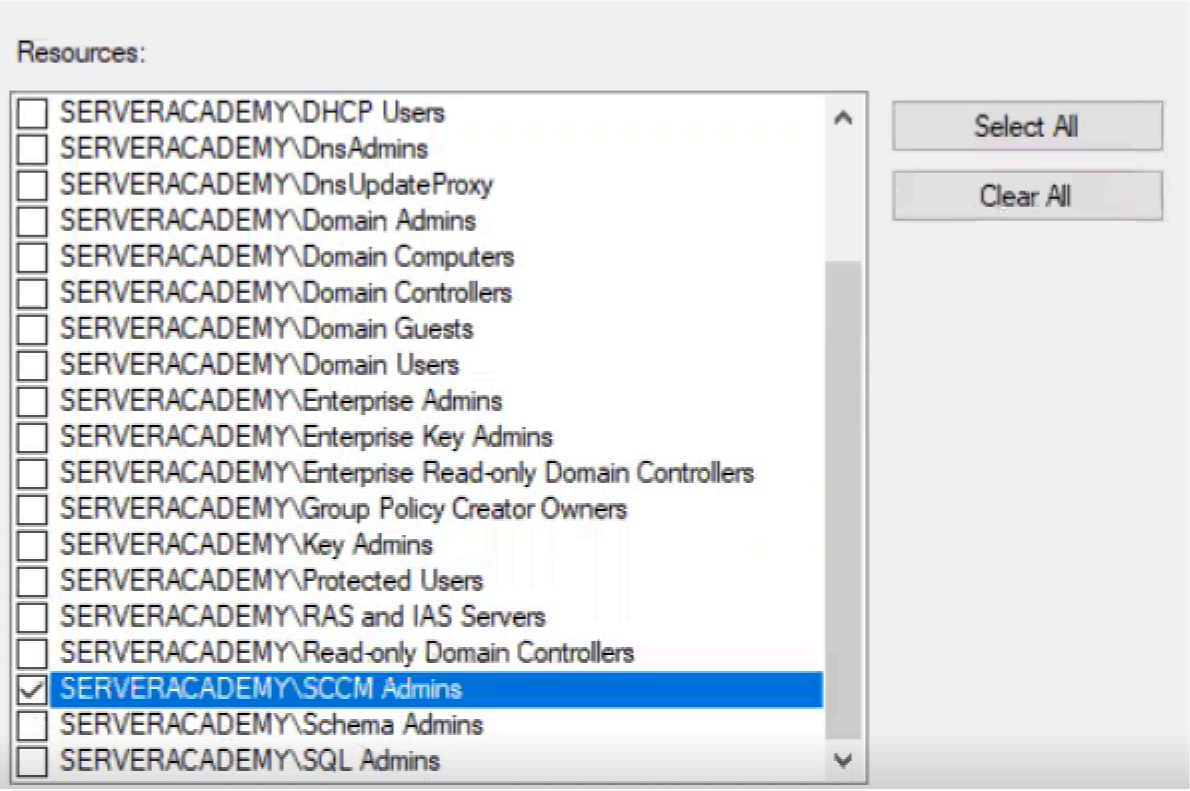
Type: String[]

□ Exclude resources marked as obsolete

□ Exclude resources that do not have the Configuration Manager client installed

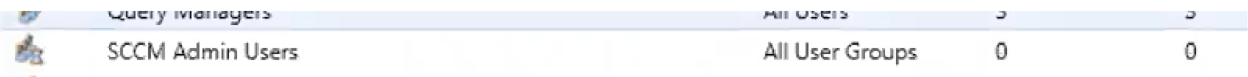
Value: %

When the type is a string, you can use the percent character (%) as a wildcard for part or all of the value.

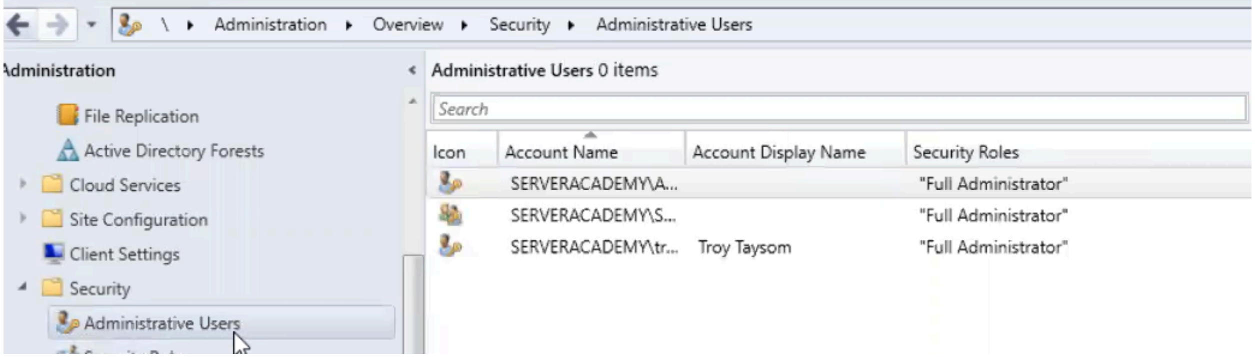


Resources:

- □ SERVERACADEMY\DHCP Users
- □ SERVERACADEMY\DnsAdmins
- □ SERVERACADEMY\DnsUpdateProxy
- □ SERVERACADEMY\Domain Admins
- □ SERVERACADEMY\Domain Computers
- □ SERVERACADEMY\Domain Controllers
- □ SERVERACADEMY\Domain Guests
- □ SERVERACADEMY\Domain Users
- □ SERVERACADEMY\Enterprise Admins
- □ SERVERACADEMY\Enterprise Key Admins
- □ SERVERACADEMY\Enterprise Read-only Domain Controllers
- □ SERVERACADEMY\Group Policy Creator Owners
- □ SERVERACADEMY\Key Admins
- □ SERVERACADEMY\Protected Users
- □ SERVERACADEMY\RAS and IAS Servers
- □ SERVERACADEMY\Read-only Domain Controllers
- ☑ SERVERACADEMY\SCCM Admins
- □ SERVERACADEMY\Schema Admins
- □ SERVERACADEMY\SQL Admins



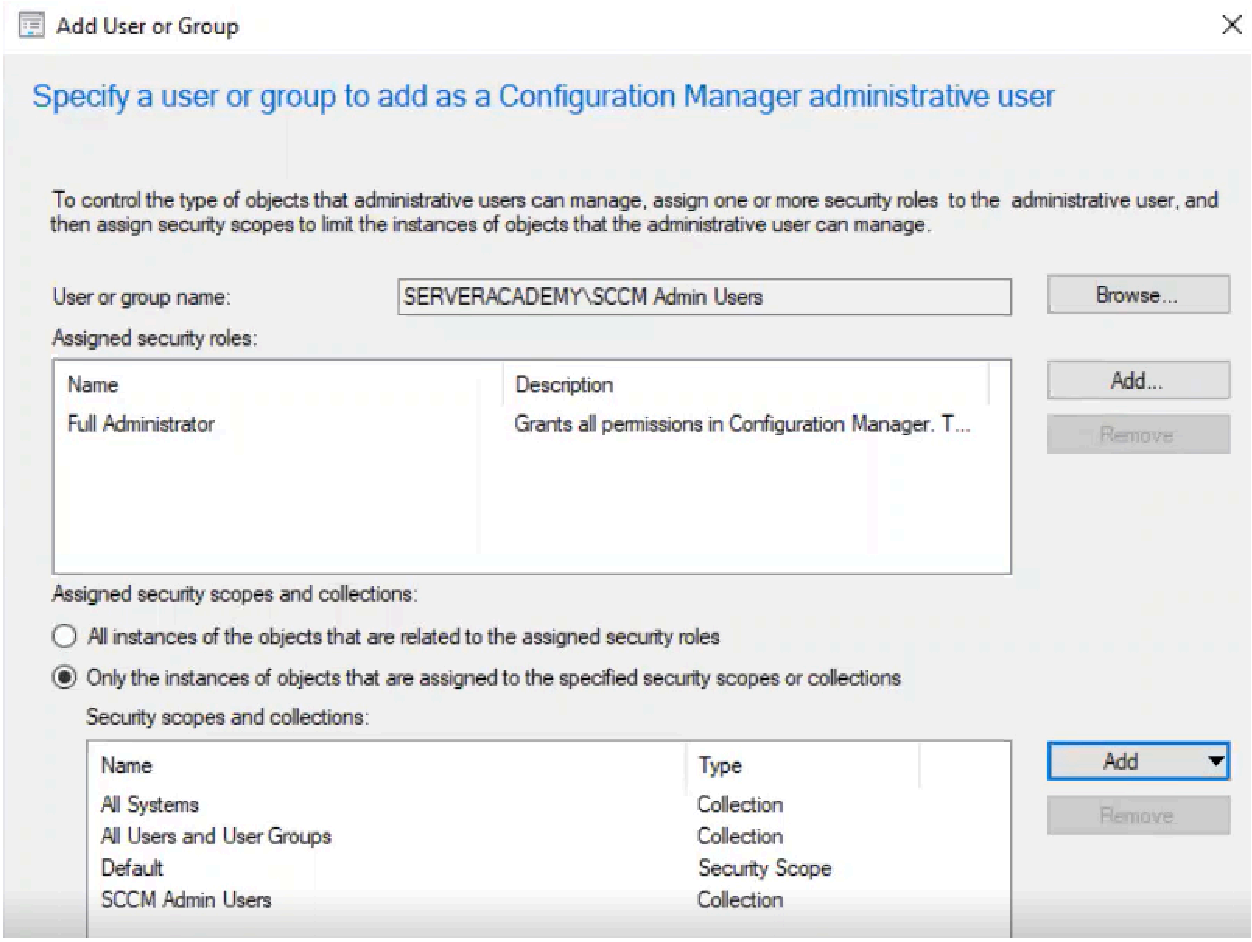
Query Managers	All Users	5	5
SCCM Admin Users	All User Groups	0	0



Administrative Users 0 items

Search

Icon	Account Name	Account Display Name	Security Roles
	SERVERACADEMY\A...		"Full Administrator"
	SERVERACADEMY\S...		"Full Administrator"
	SERVERACADEMY\tr...	Troy Taysom	"Full Administrator"


Add User or Group

Specify a user or group to add as a Configuration Manager administrative user

To control the type of objects that administrative users can manage, assign one or more security roles to the administrative user, and then assign security scopes to limit the instances of objects that the administrative user can manage.

User or group name: SERVERACADEMY\SCCM Admin Users

Assigned security roles:

Name	Description
Full Administrator	Grants all permissions in Configuration Manager. T...

Assigned security scopes and collections:

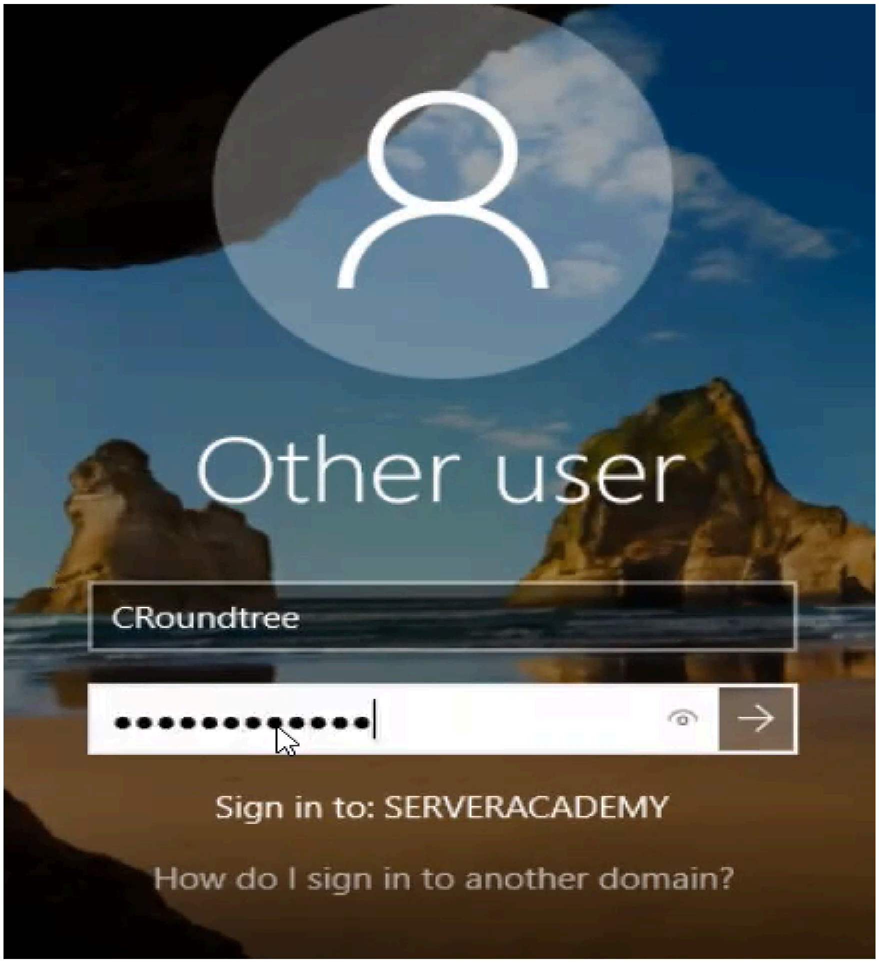
○ All instances of the objects that are related to the assigned security roles

● Only the instances of objects that are assigned to the specified security scopes or collections

Security scopes and collections:

Name	Type
All Systems	Collection
All Users and User Groups	Collection
Default	Security Scope
SCCM Admin Users	Collection

SCCM Admin Group User Clay Roundtree Logging in to Verify Admin Privileges for SCCM



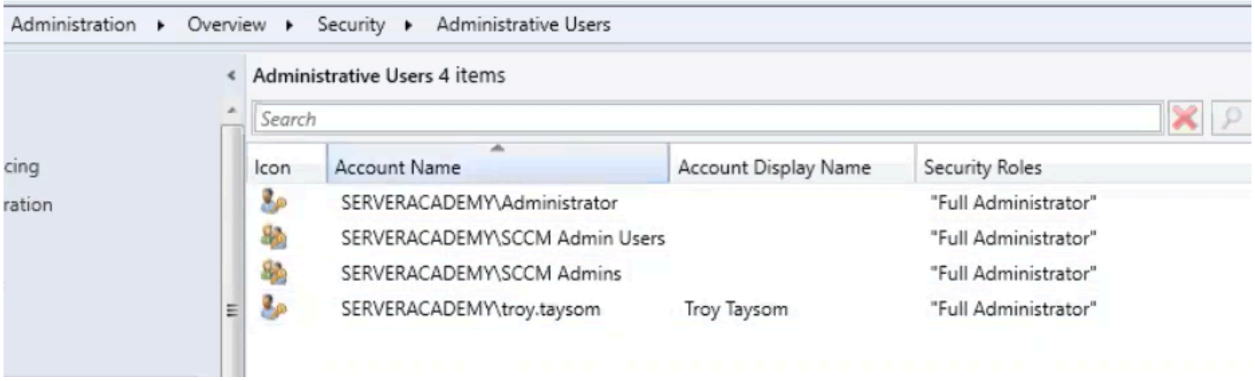
Other user

CRoundtree

●●●●●●●●●●●●●

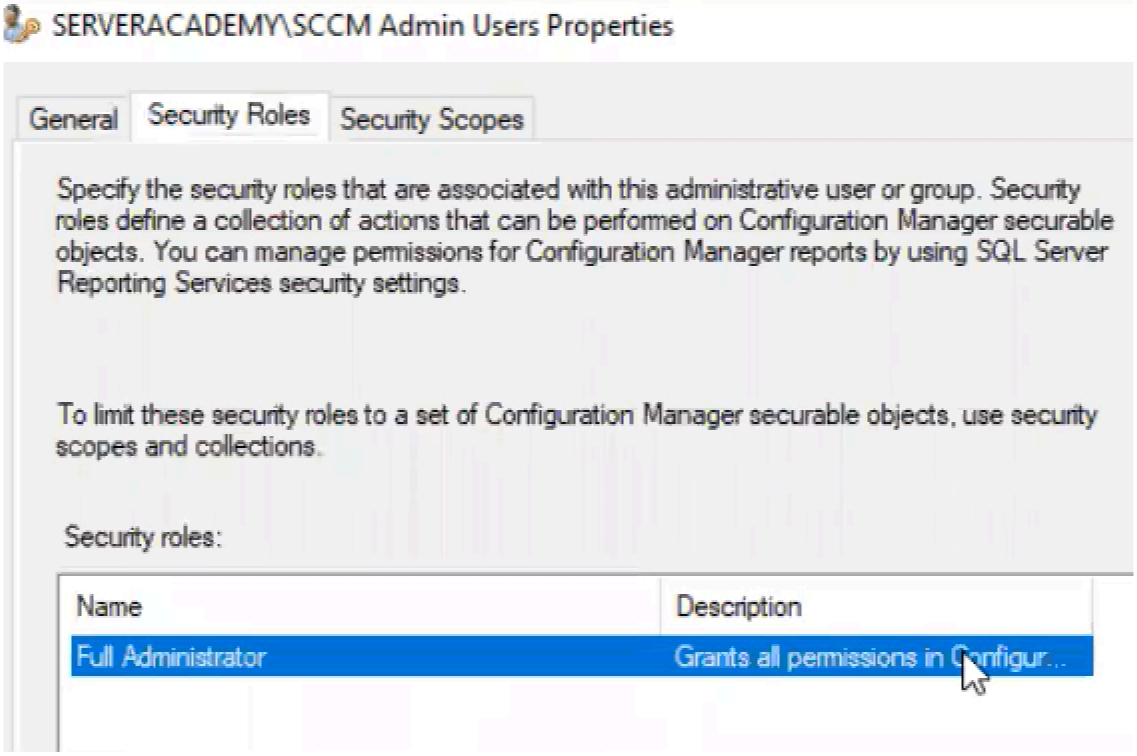
Sign in to: SERVERACADEMY

How do I sign in to another domain?



Administrative Users 4 items

Icon	Account Name	Account Display Name	Security Roles
	SERVERACADEMY\Administrator		"Full Administrator"
	SERVERACADEMY\SCCM Admin Users		"Full Administrator"
	SERVERACADEMY\SCCM Admins		"Full Administrator"
	SERVERACADEMY\troy.taysom	Troy Taysom	"Full Administrator"



SERVERACADEMY\SCCM Admin Users Properties

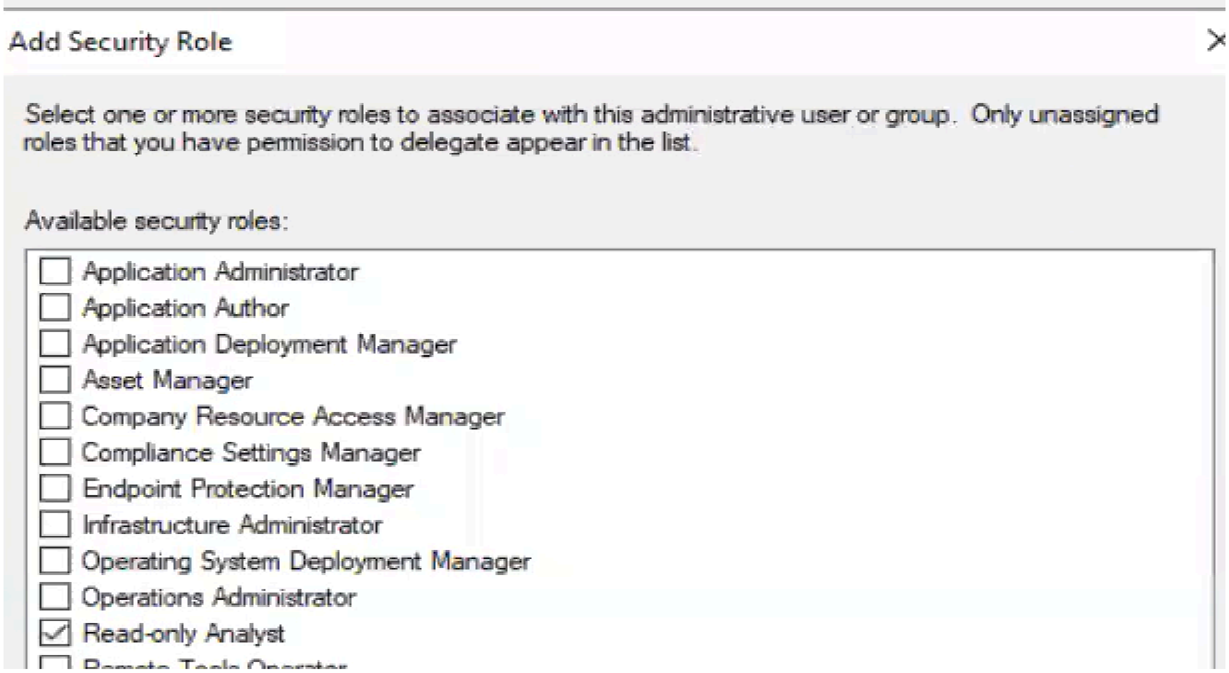
Specify the security roles that are associated with this administrative user or group. Security roles define a collection of actions that can be performed on Configuration Manager securable objects. You can manage permissions for Configuration Manager reports by using SQL Server Reporting Services security settings.

To limit these security roles to a set of Configuration Manager securable objects, use security scopes and collections.

Security roles:

Name	Description
Full Administrator	Grants all permissions in Configur...

Downgrading Permissions to Read Only for SCCM Admins

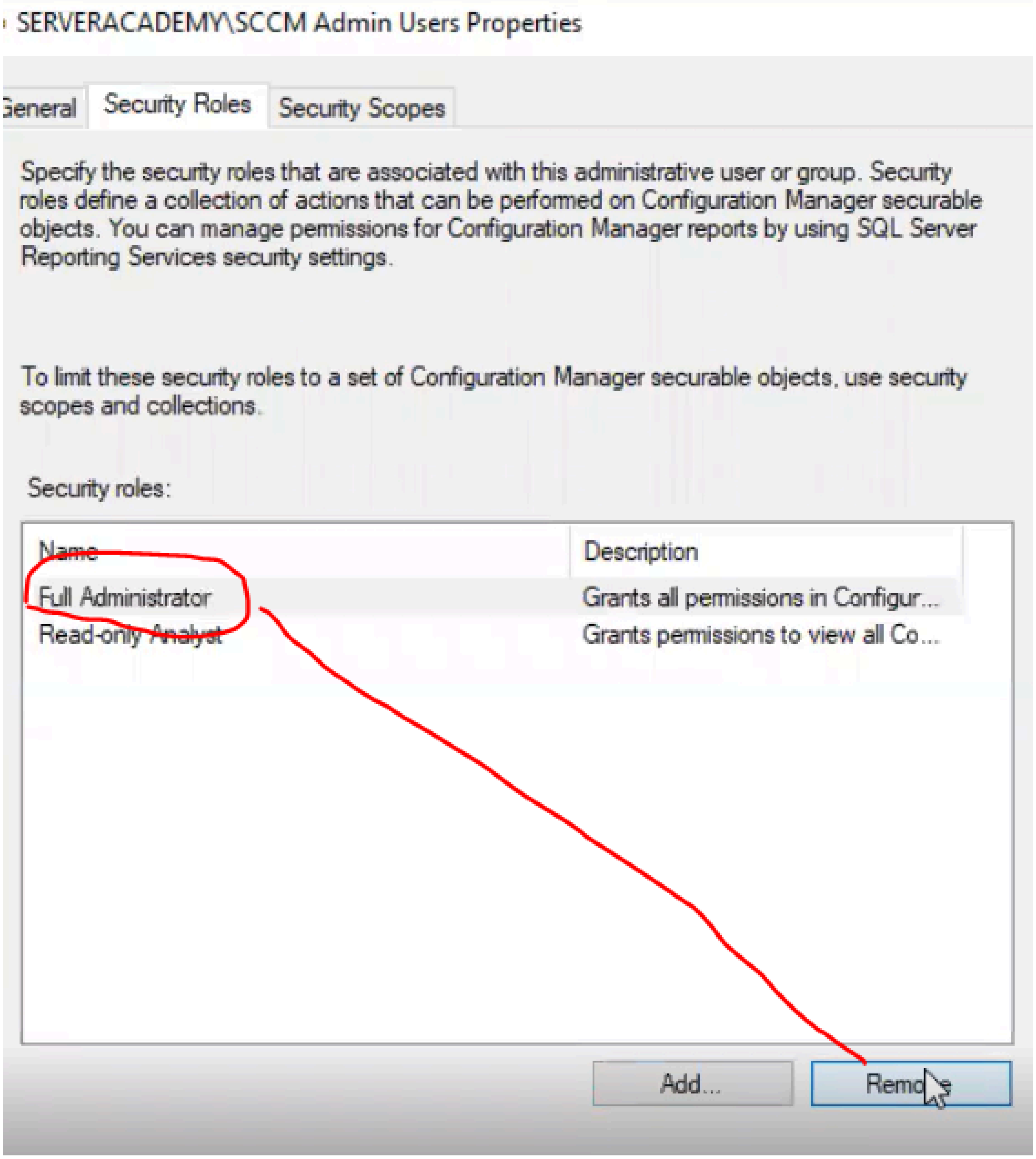


Add Security Role

Select one or more security roles to associate with this administrative user or group. Only unassigned roles that you have permission to delegate appear in the list.

Available security roles:

- ☐ Application Administrator
- ☐ Application Author
- ☐ Application Deployment Manager
- ☐ Asset Manager
- ☐ Company Resource Access Manager
- ☐ Compliance Settings Manager
- ☐ Endpoint Protection Manager
- ☐ Infrastructure Administrator
- ☐ Operating System Deployment Manager
- ☐ Operations Administrator
- ☑ Read-only Analyst
- ☐ Remote Tools Operator



SERVERACADEMY\SCCM Admin Users Properties

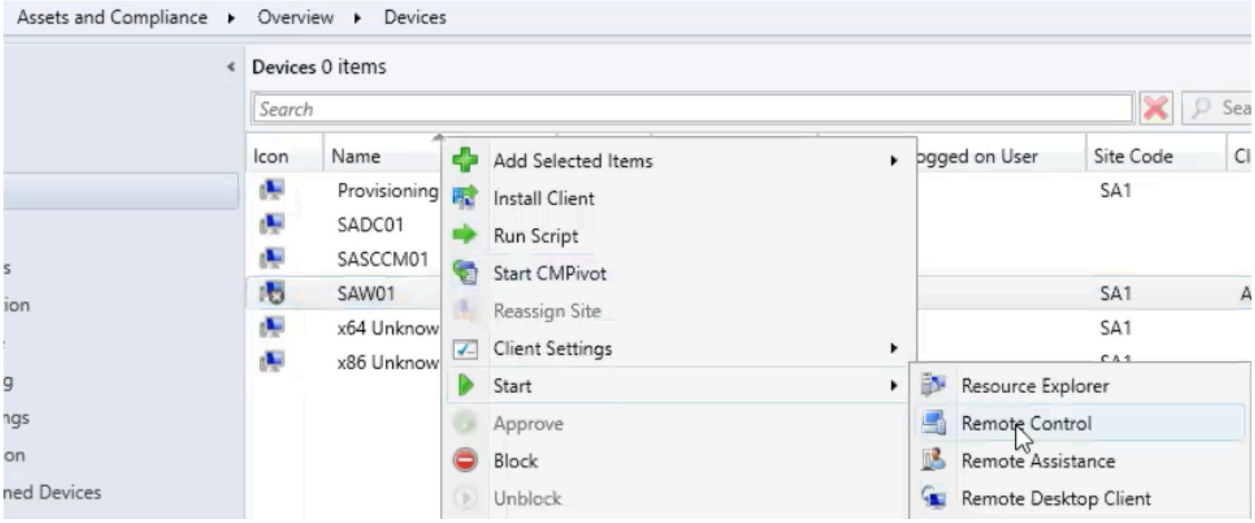
Specify the security roles that are associated with this administrative user or group. Security roles define a collection of actions that can be performed on Configuration Manager securable objects. You can manage permissions for Configuration Manager reports by using SQL Server Reporting Services security settings.

To limit these security roles to a set of Configuration Manager securable objects, use security scopes and collections.

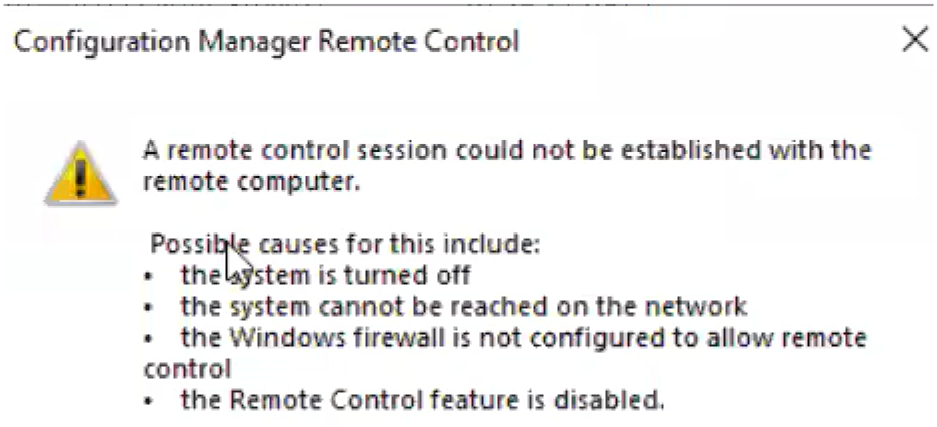
Security roles:

Name	Description
Full Administrator	Grants all permissions in Configur...
Read-only Analyst	Grants permissions to view all Co...

Establishing a Remote Session with Client Machine



Connection Refused

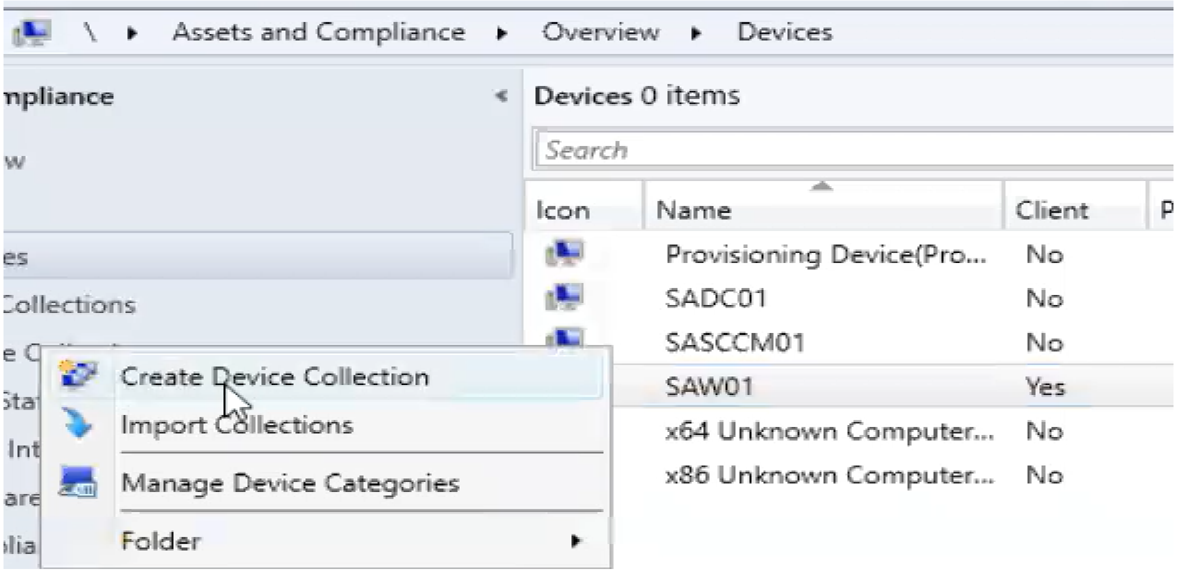


A remote control session could not be established with the remote computer.

Possible causes for this include:

- the system is turned off
- the system cannot be reached on the network
- the Windows firewall is not configured to allow remote control
- the Remote Control feature is disabled.

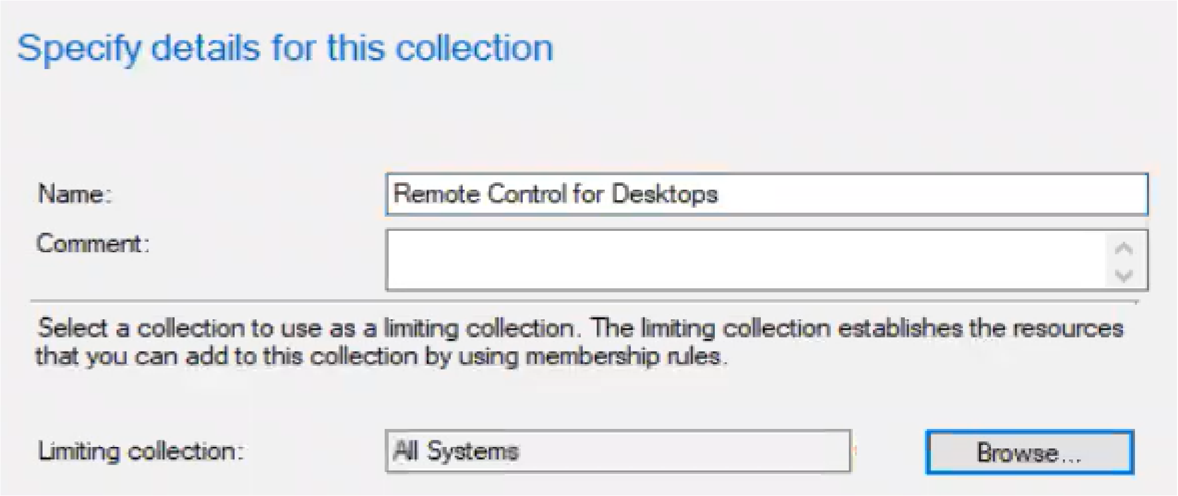
Enabling Connection with SCCM with a Direct Rule



Devices 0 items

Search

Icon	Name	Client	P
	Provisioning Device(Pro...	No	
	SADC01	No	
	SASCCM01	No	
	SAW01	Yes	
	x64 Unknown Computer...	No	
	x86 Unknown Computer...	No	



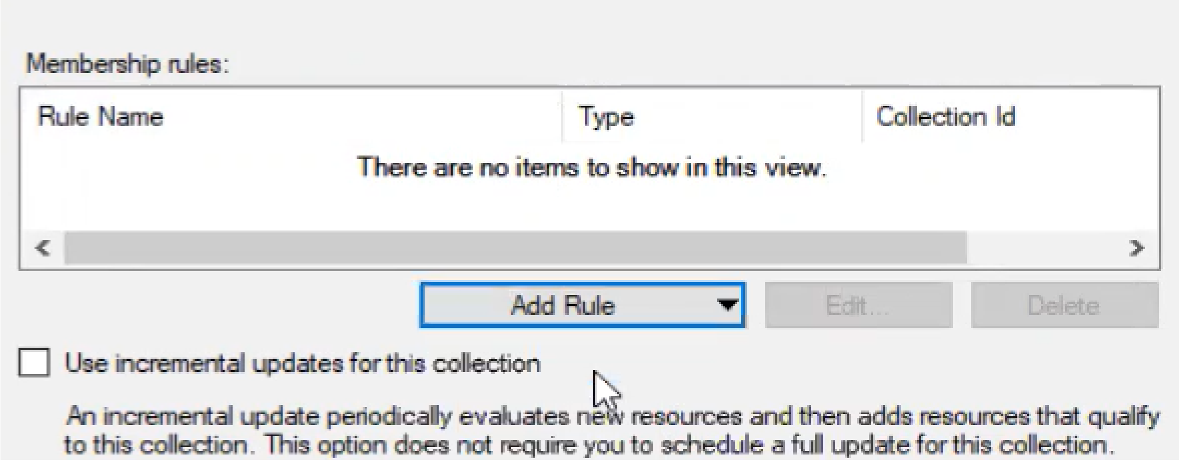
Specify details for this collection

Name: Remote Control for Desktops

Comment:

Select a collection to use as a limiting collection. The limiting collection establishes the resources that you can add to this collection by using membership rules.

Limiting collection: All Systems



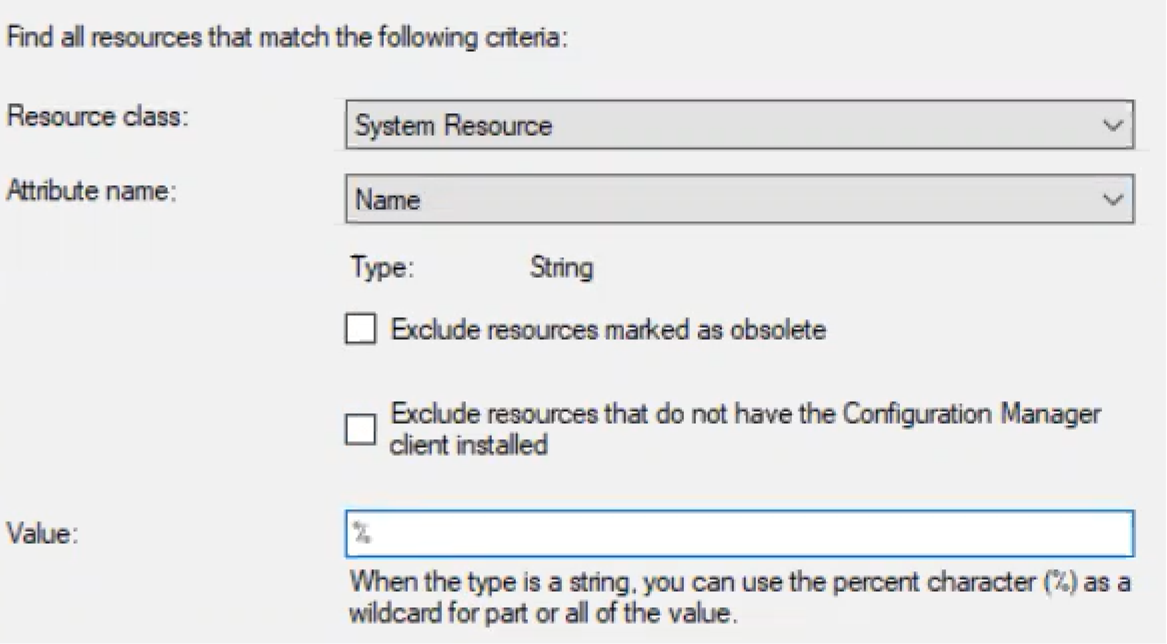
Membership rules:

Rule Name	Type	Collection Id

There are no items to show in this view.

□ 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.



Find all resources that match the following criteria:

Resource class: System Resource

Attribute name: Name

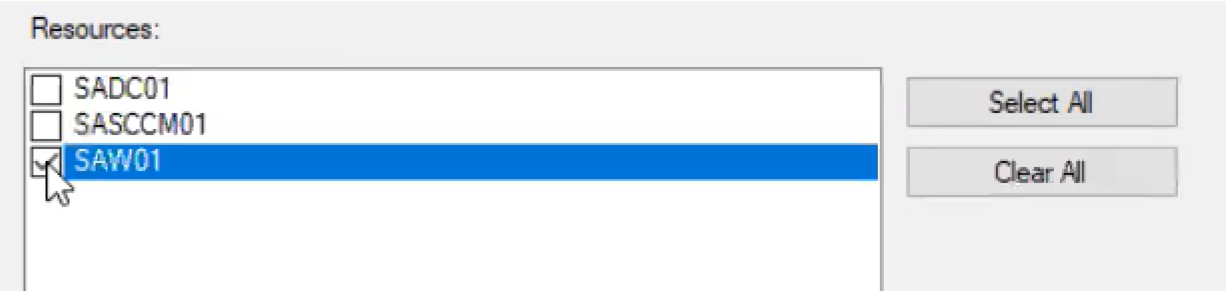
Type: String

□ Exclude resources marked as obsolete

□ Exclude resources that do not have the Configuration Manager client installed

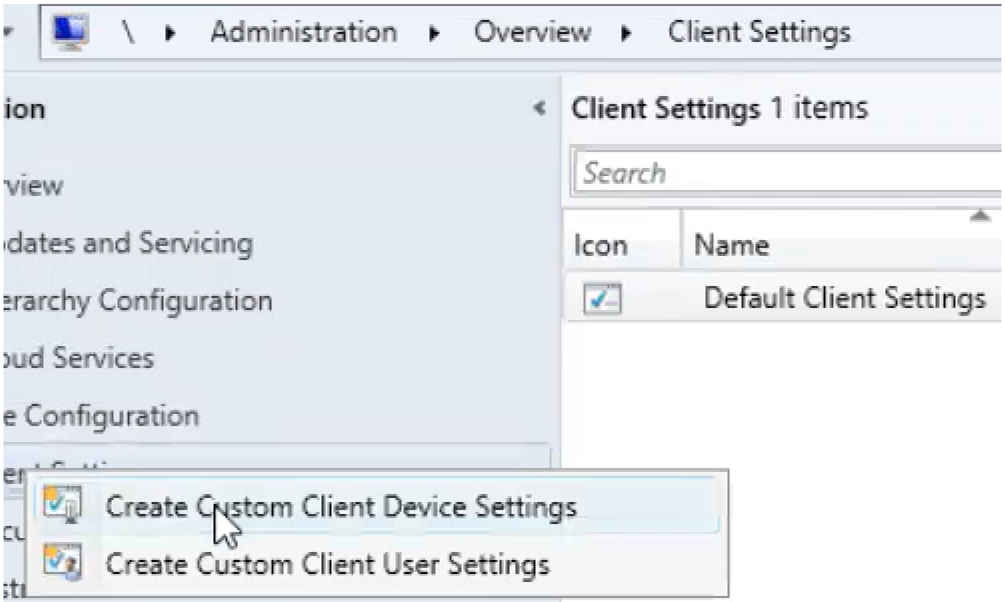
Value: %

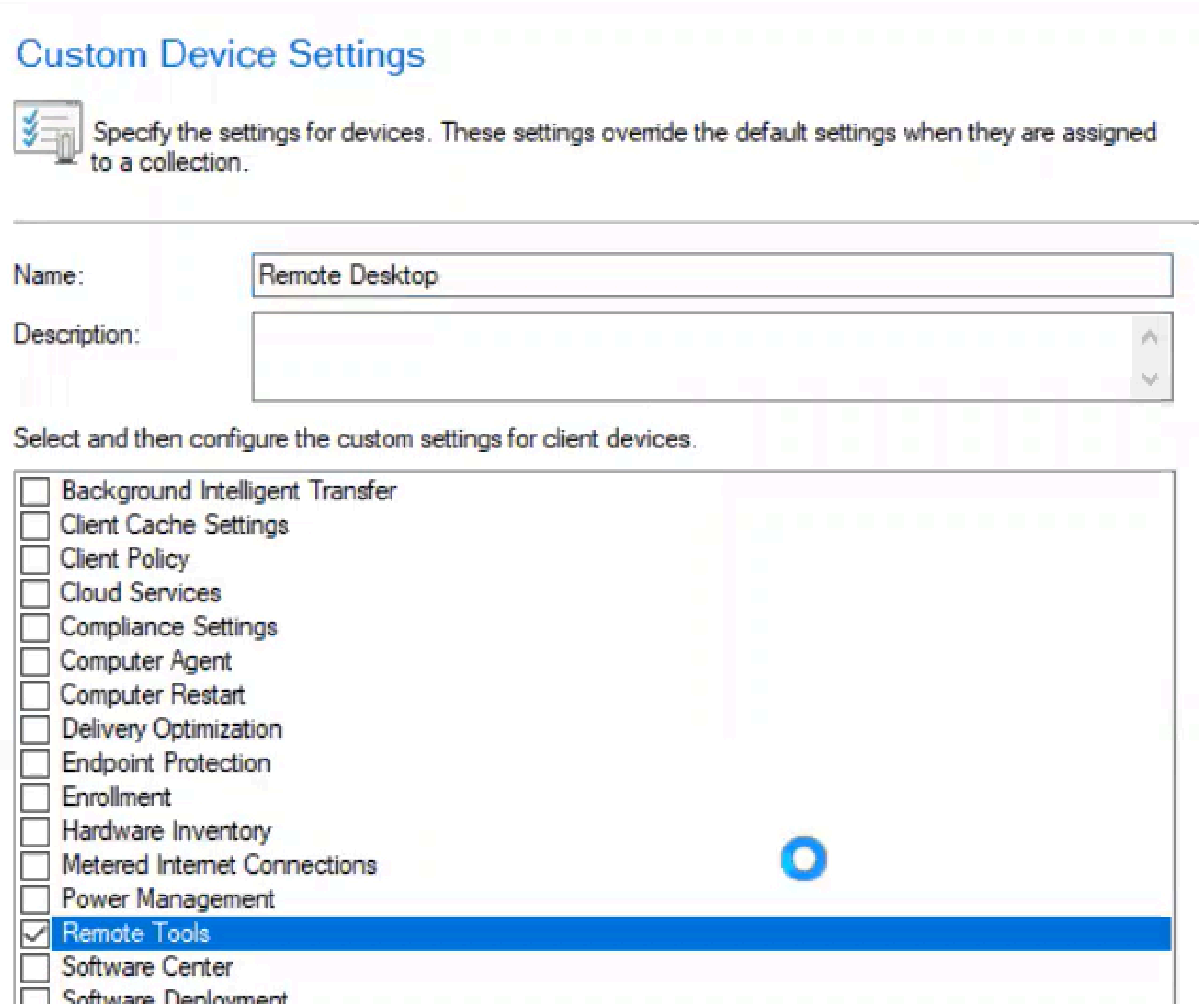
When the type is a string, you can use the percent character (%) as a wildcard for part or all of the value.



Resources:

□ SADC01
□ SASCCM01
☑ SAW01





Custom Device Settings

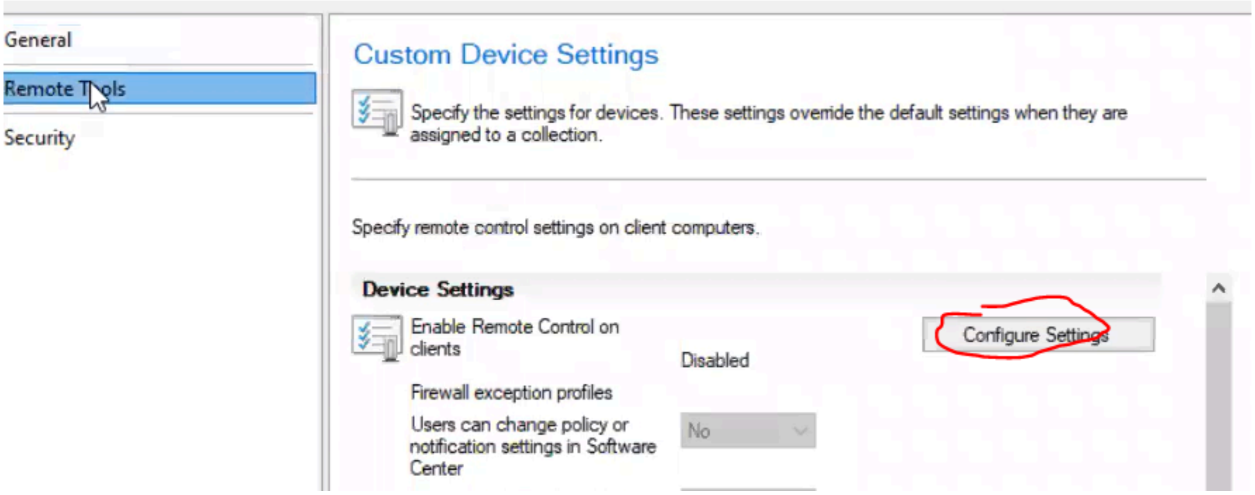
Specify the settings for devices. These settings override the default settings when they are assigned to a collection.

Name: Remote Desktop

Description:

Select and then configure the custom settings for client devices.

- □ 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



Custom Device Settings

Specify the settings for devices. These settings override the default settings when they are assigned to a collection.

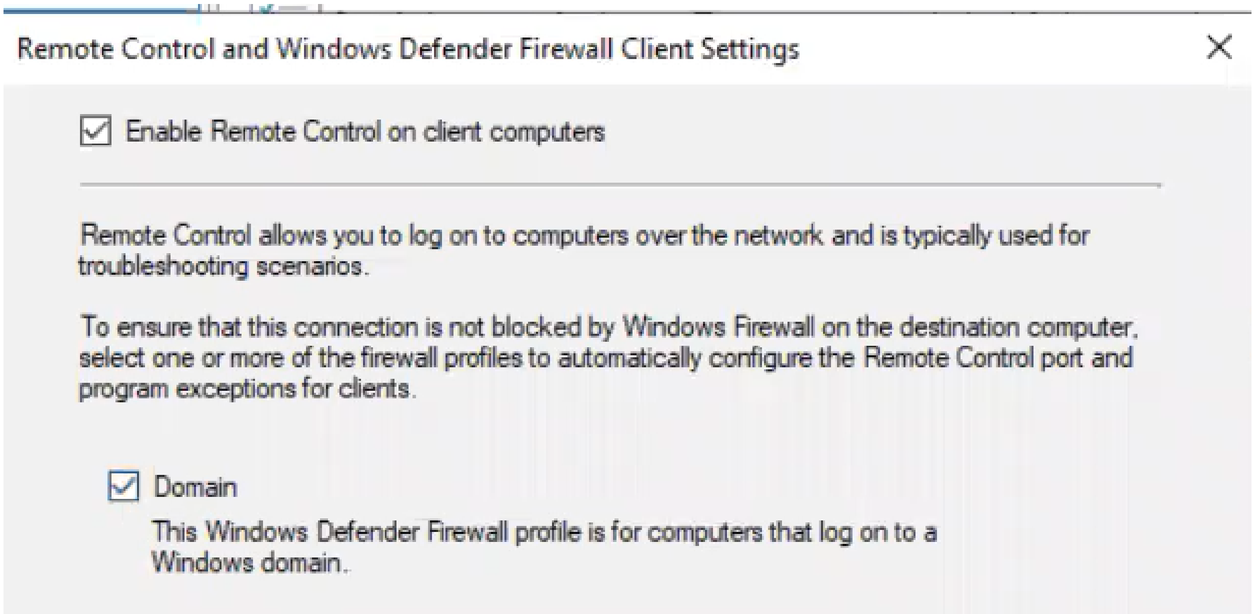
Specify remote control settings on client computers.

Device Settings

Enable Remote Control on clients: Disabled

Firewall exception profiles

Users can change policy or notification settings in Software Center: No



Remote Control and Windows Defender Firewall Client Settings

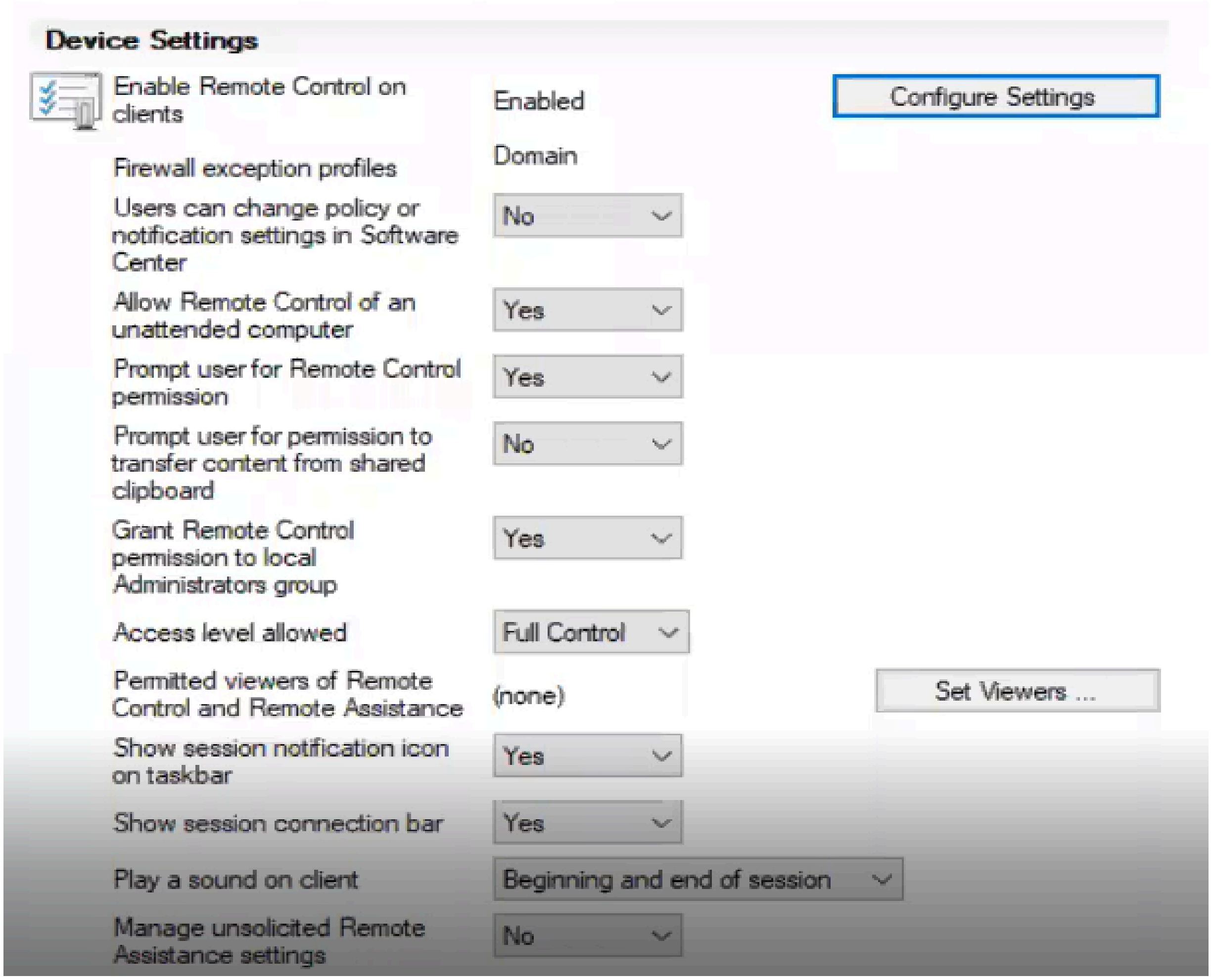
☑ Enable Remote Control on client computers

Remote Control allows you to log on to computers over the network and is typically used for troubleshooting scenarios.

To ensure that this connection is not blocked by Windows Firewall on the destination computer, select one or more of the firewall profiles to automatically configure the Remote Control port and program exceptions for clients.

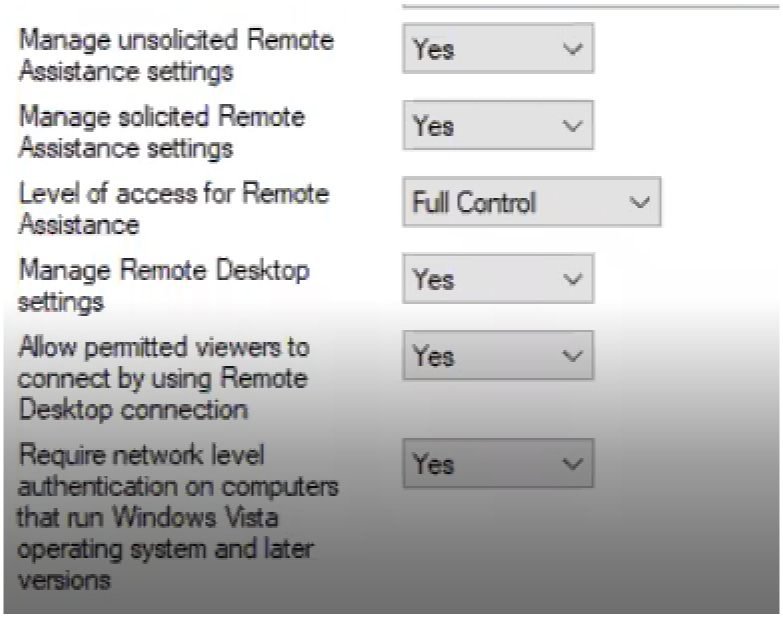
☑ Domain

This Windows Defender Firewall profile is for computers that log on to a Windows domain.

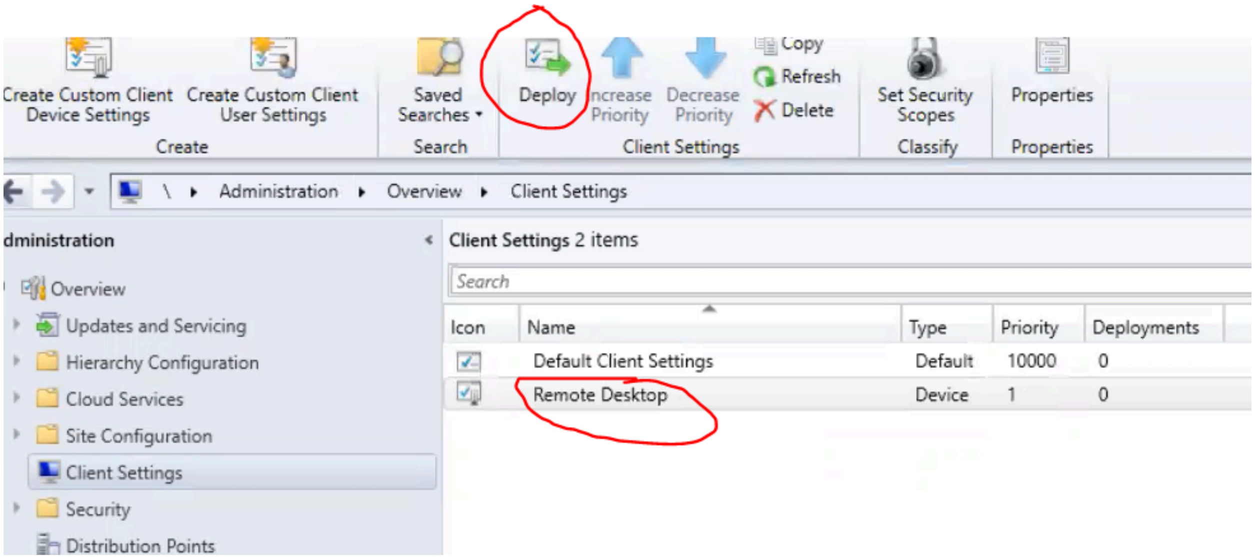


Device Settings

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

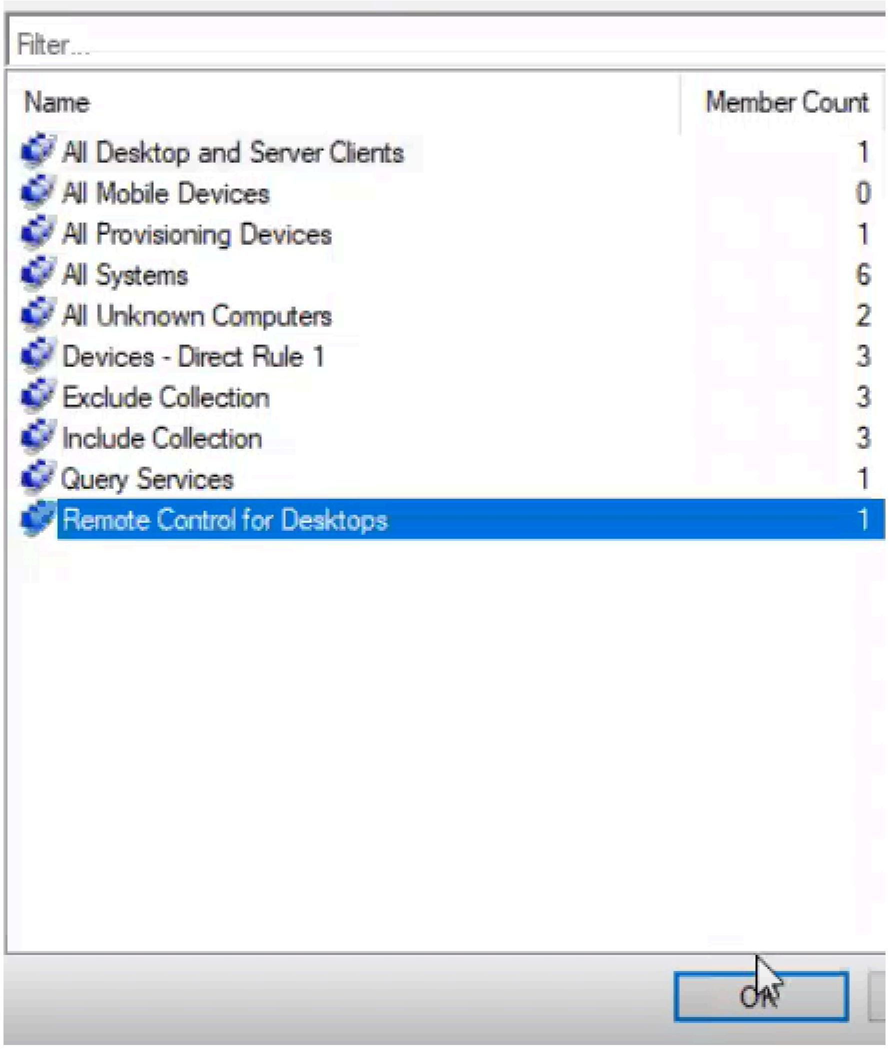


Manage unsolicited Remote Assistance settings	Yes
Manage solicited Remote Assistance settings	Yes
Level of access for Remote Assistance	Full Control
Manage Remote Desktop settings	Yes
Allow permitted viewers to connect by using Remote Desktop connection	Yes
Require network level authentication on computers that run Windows Vista operating system and later versions	Yes



Client Settings 2 items

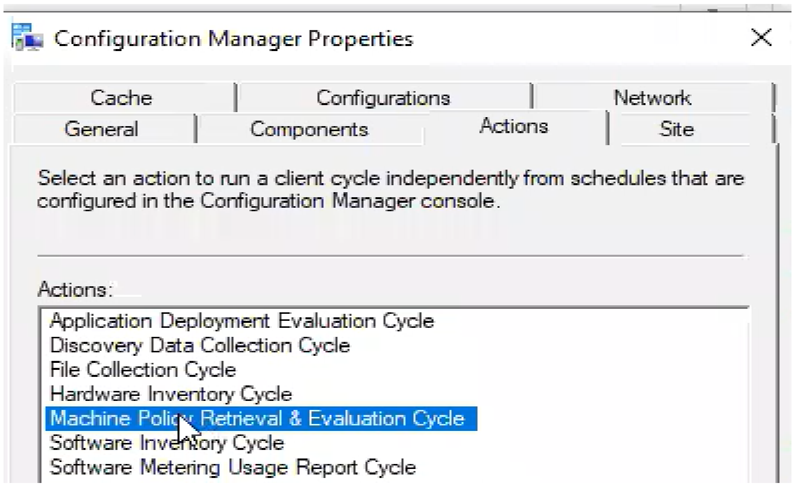
Icon	Name	Type	Priority	Deployments
✓	Default Client Settings	Default	10000	0
✓	Remote Desktop	Device	1	0



Filter...

Name	Member Count
All Desktop and Server Clients	1
All Mobile Devices	0
All Provisioning Devices	1
All Systems	6
All Unknown Computers	2
Devices - Direct Rule 1	3
Exclude Collection	3
Include Collection	3
Query Services	1
Remote Control for Desktops	1

Running Policy Retrieval on Client Machine



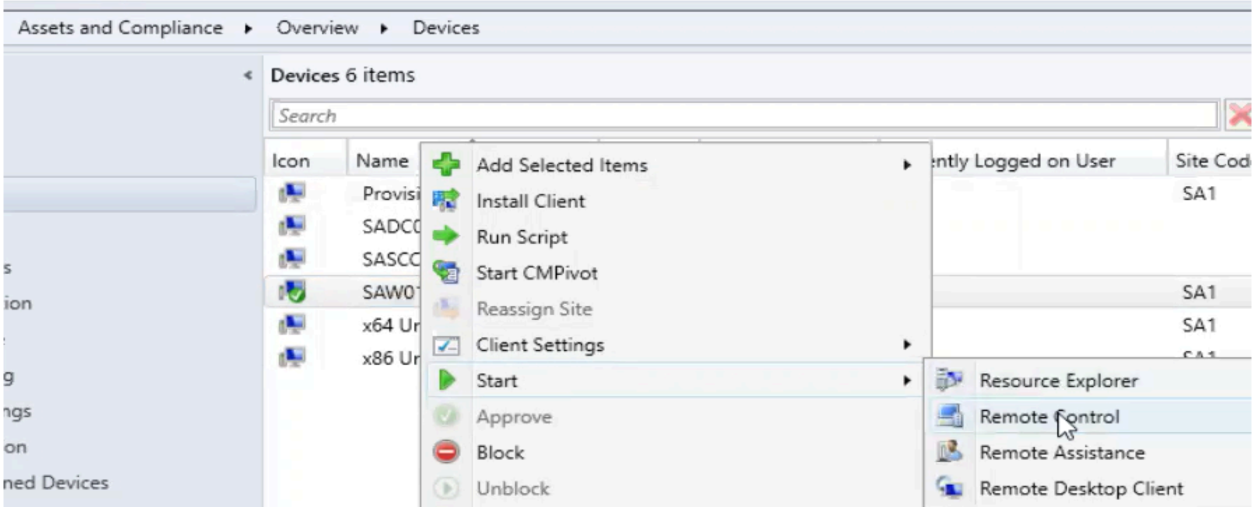
Configuration Manager Properties

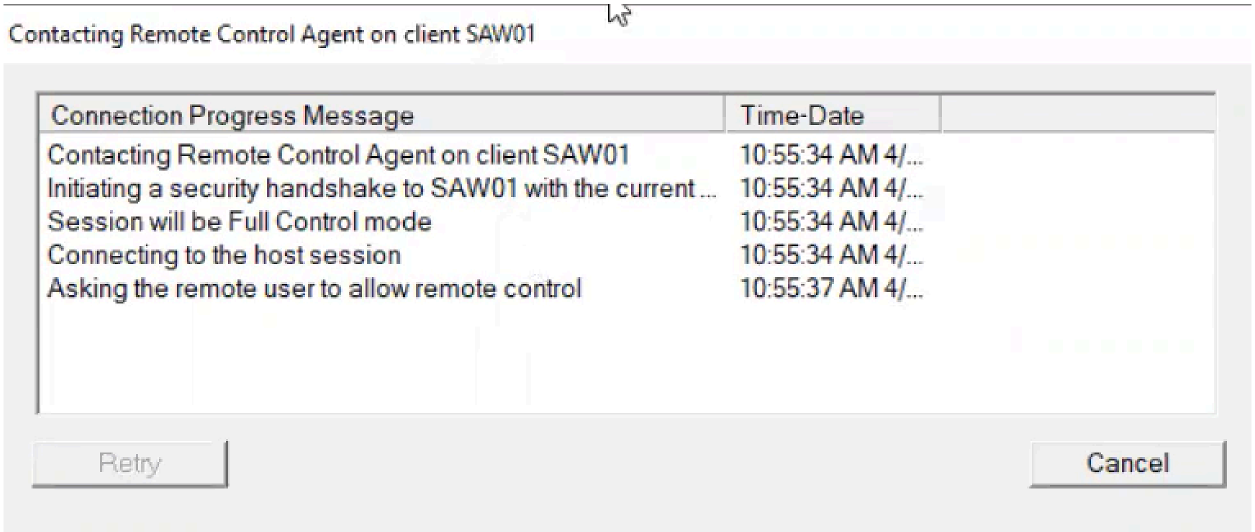
Select an action to run a client cycle independently from schedules that are configured in the Configuration Manager console.

Actions:

Application Deployment Evaluation Cycle
Discovery Data Collection Cycle
File Collection Cycle
Hardware Inventory Cycle
Machine Policy Retrieval & Evaluation Cycle
Software Inventory Cycle
Software Metering Usage Report Cycle

Reinitiating Remote Control with Client

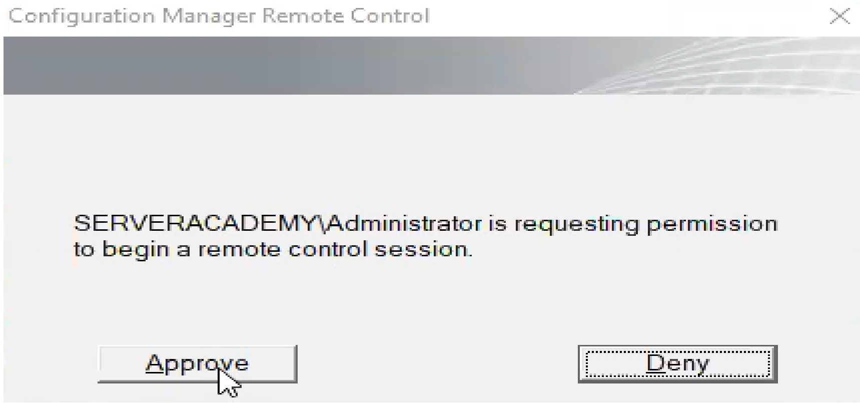




Contacting Remote Control Agent on client SAW01

Connection Progress Message	Time-Date
Contacting Remote Control Agent on client SAW01	10:55:34 AM 4/...
Initiating a security handshake to SAW01 with the current ...	10:55:34 AM 4/...
Session will be Full Control mode	10:55:34 AM 4/...
Connecting to the host session	10:55:34 AM 4/...
Asking the remote user to allow remote control	10:55:37 AM 4/...

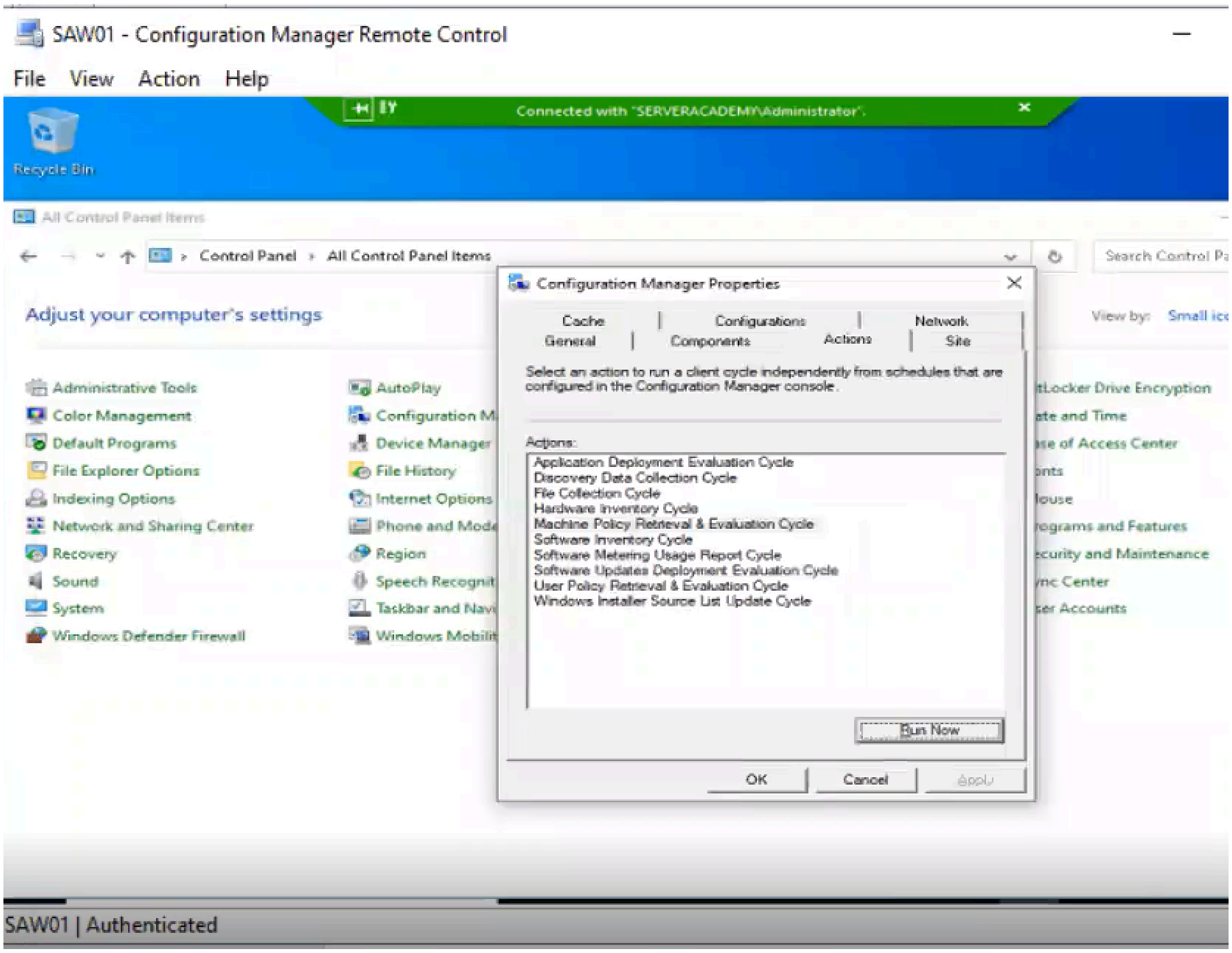
Client Grants Permission to Remote In



Configuration Manager Remote Control

SERVERACADEMY\Administrator is requesting permission to begin a remote control session.

View of Remote Session

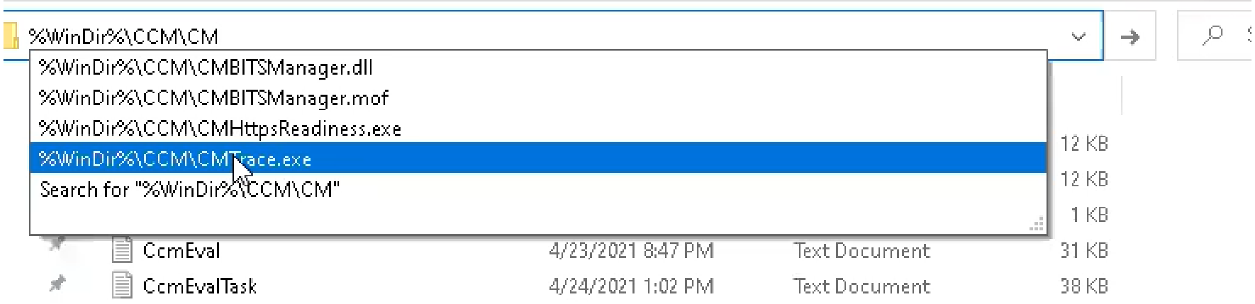


Select an action to run a client cycle independently from schedules that are configured in the Configuration Manager console.

Actions:

Application Deployment Evaluation Cycle
Discovery Data Collection Cycle
File Collection Cycle
Hardware Inventory Cycle
Machine Policy Retrieval & Evaluation Cycle
Software Inventory Cycle
Software Metering Usage Report Cycle
Software Updates Deployment Evaluation Cycle
User Policy Retrieval & Evaluation Cycle
Windows Installer Source List Update Cycle

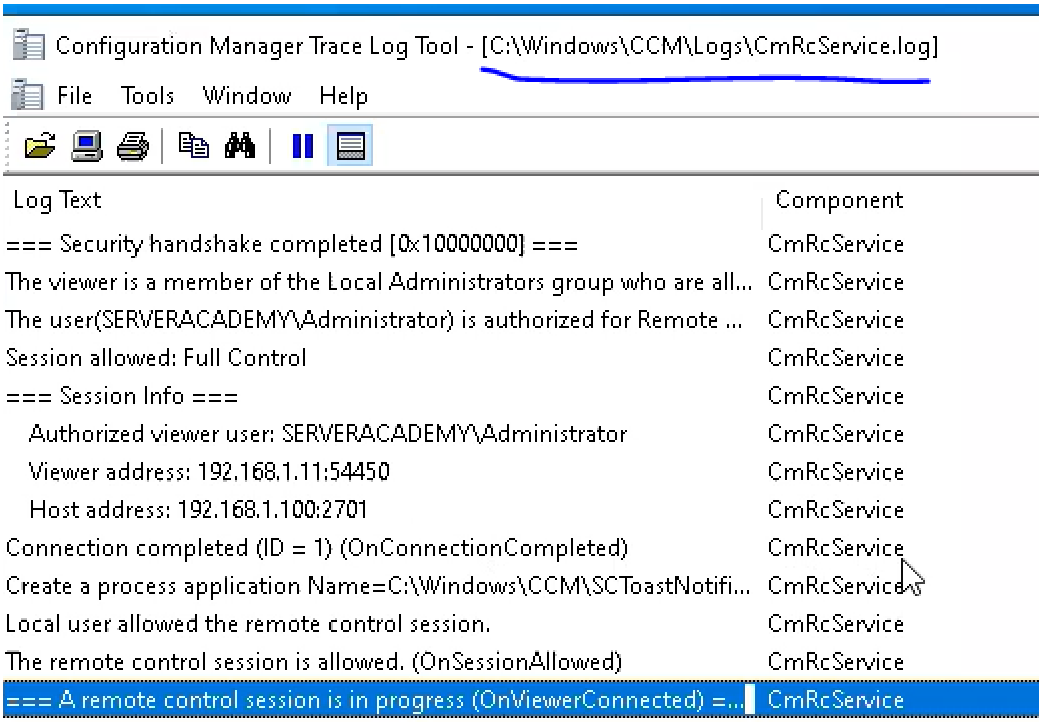
Running CMTrace on Client to View Log of Remote Session



%WinDir%\CCM\CM

%WinDir%\CCM\CMBITSManager.dll
%WinDir%\CCM\CMBITSManager.mof
%WinDir%\CCM\CMHttpsReadiness.exe
%WinDir%\CCM\CMTrace.exe
Search for "%WinDir%\CCM\CM"

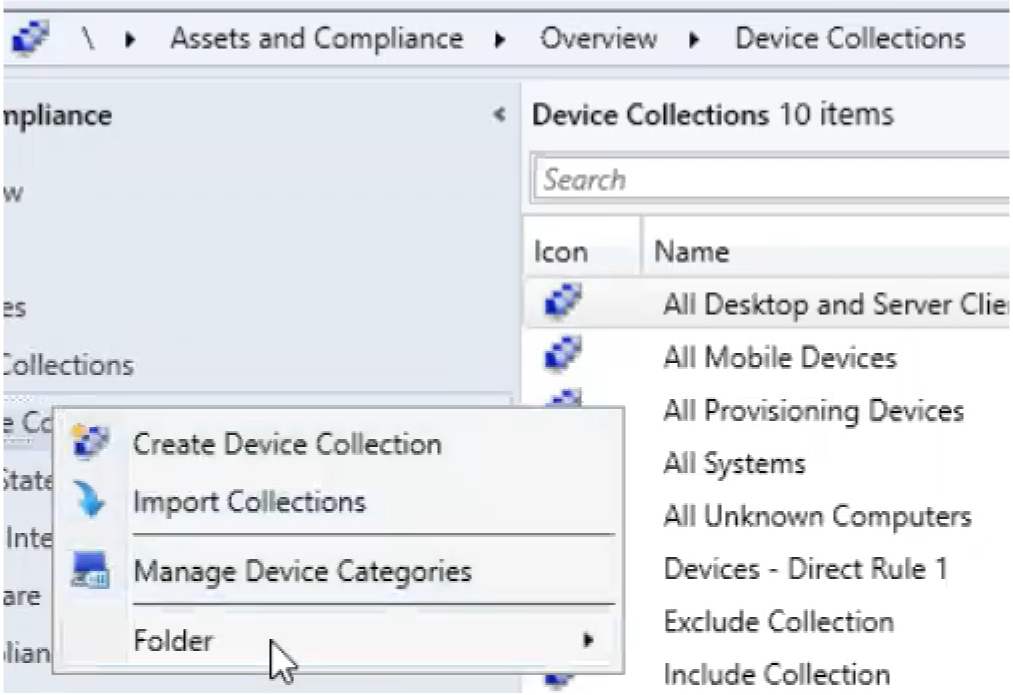
			12 KB
			12 KB
			1 KB
CcmEval	4/23/2021 8:47 PM	Text Document	31 KB
CcmEvalTask	4/24/2021 1:02 PM	Text Document	38 KB



Configuration Manager Trace Log Tool - [C:\Windows\CCM\Logs\CmRcService.log]
File Tools Window Help

```
Log Text                                                               Component
=== Security handshake completed [0x10000000] ===                      CmRcService
The viewer is a member of the Local Administrators group who are all... CmRcService
The user(SERVERACADEMY\Administrator) is authorized for Remote ...     CmRcService
Session allowed: Full Control                                          CmRcService
=== Session Info ===                                                   CmRcService
   Authorized viewer user: SERVERACADEMY\Administrator                 CmRcService
   Viewer address: 192.168.1.11:54450                                  CmRcService
   Host address: 192.168.1.100:2701                                    CmRcService
Connection completed (ID = 1) (OnConnectionCompleted)                  CmRcService
Create a process application Name=C:\Windows\CCM\SCToastNotifi...      CmRcService
Local user allowed the remote control session.                         CmRcService
The remote control session is allowed. (OnSessionAllowed)              CmRcService
=== A remote control session is in progress (OnViewerConnected) =...   CmRcService
```

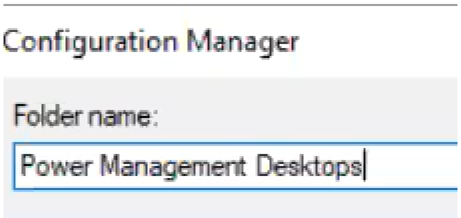
Deploying Power Management with Collections



Device Collections 10 items

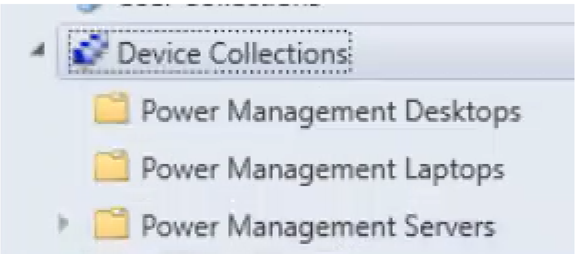
Search

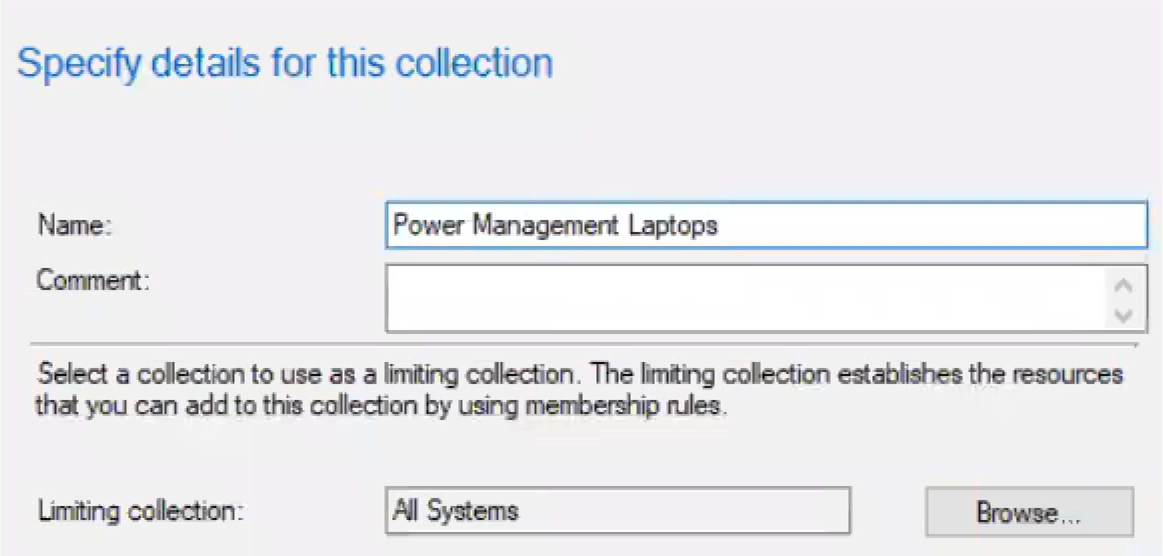
Icon	Name
	All Desktop and Server Clie
	All Mobile Devices
	All Provisioning Devices
	All Systems
	All Unknown Computers
	Devices - Direct Rule 1
	Exclude Collection
	Include Collection



Configuration Manager

Folder name: Power Management Desktops





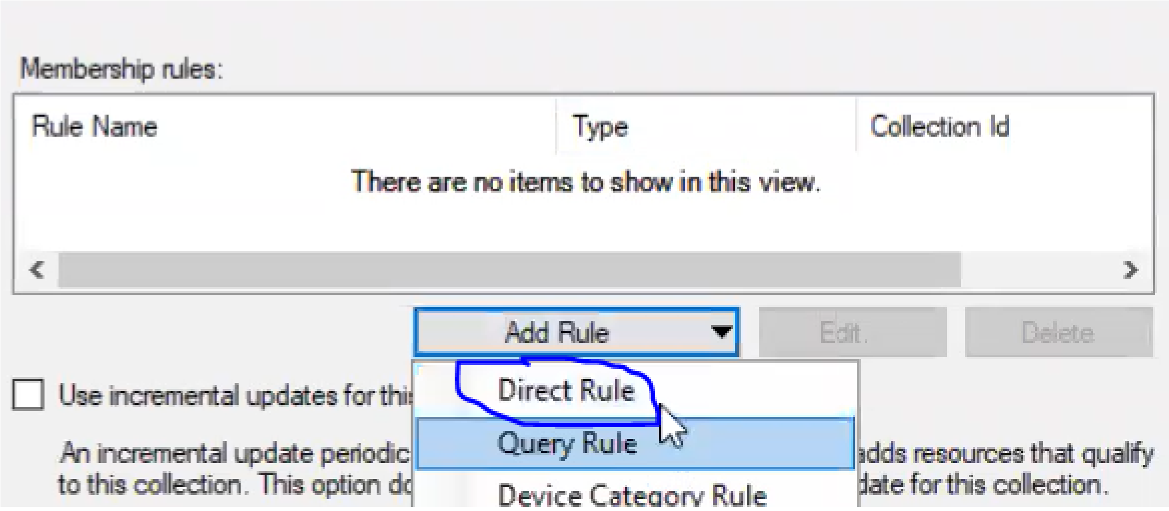
Specify details for this collection

Name: Power Management Laptops

Comment:

Select a collection to use as a limiting collection. The limiting collection establishes the resources that you can add to this collection by using membership rules.

Limiting collection: All Systems



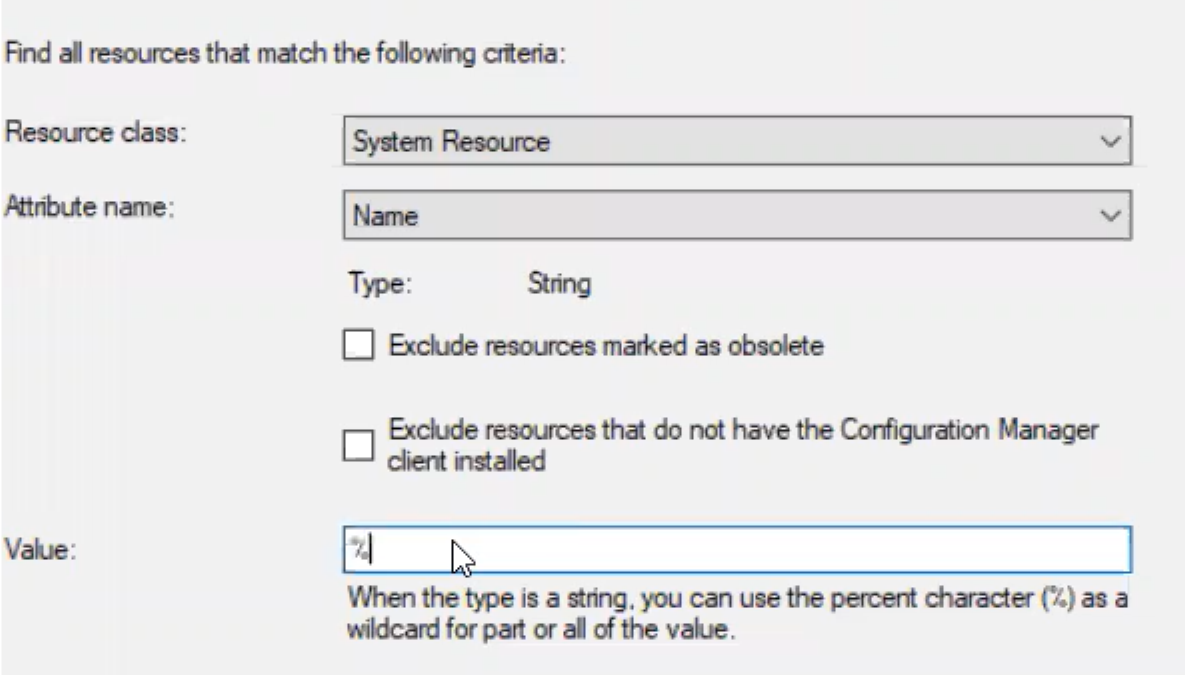
Membership rules:

Rule Name	Type	Collection Id

There are no items to show in this view.

□ Use incremental updates for thi

An incremental update periodic adds resources that qualify to this collection. This option d date for this collection.



Find all resources that match the following criteria:

Resource class: System Resource

Attribute name: Name

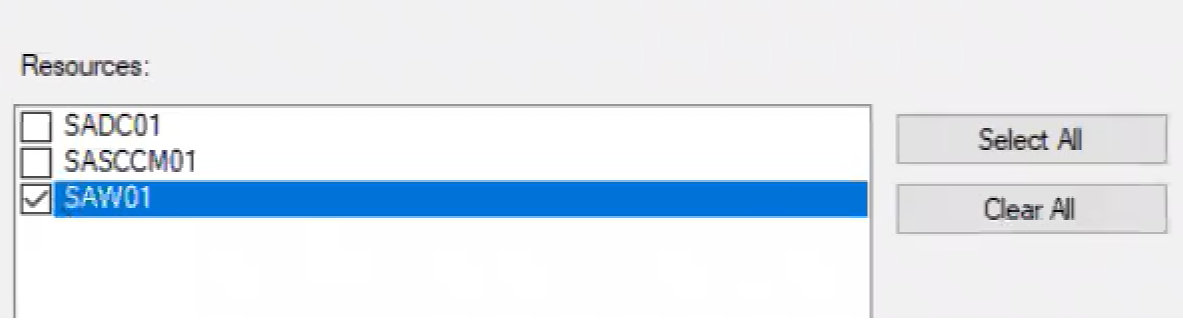
Type: String

□ Exclude resources marked as obsolete

□ Exclude resources that do not have the Configuration Manager client installed

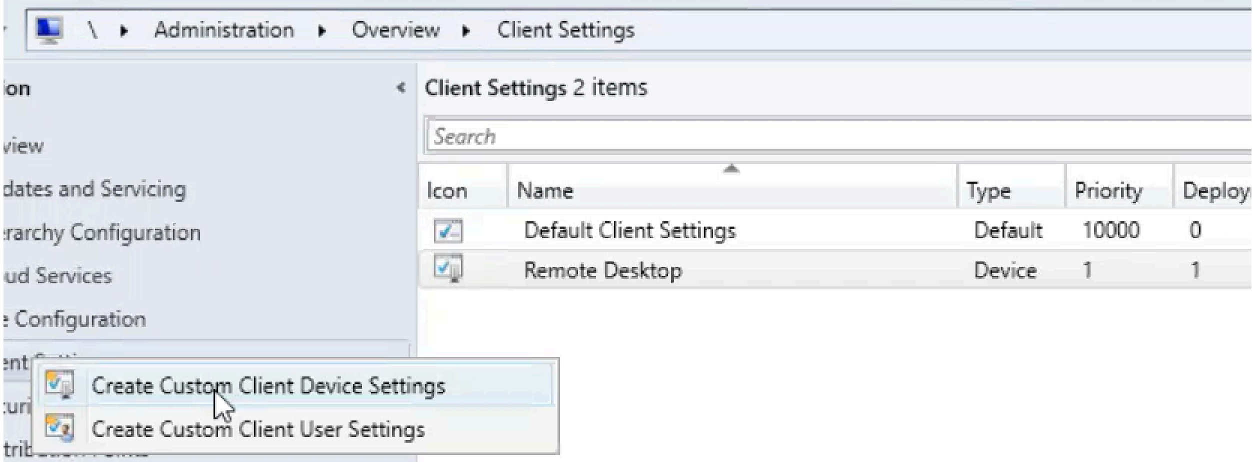
Value: %

When the type is a string, you can use the percent character (%) as a wildcard for part or all of the value.



Resources:

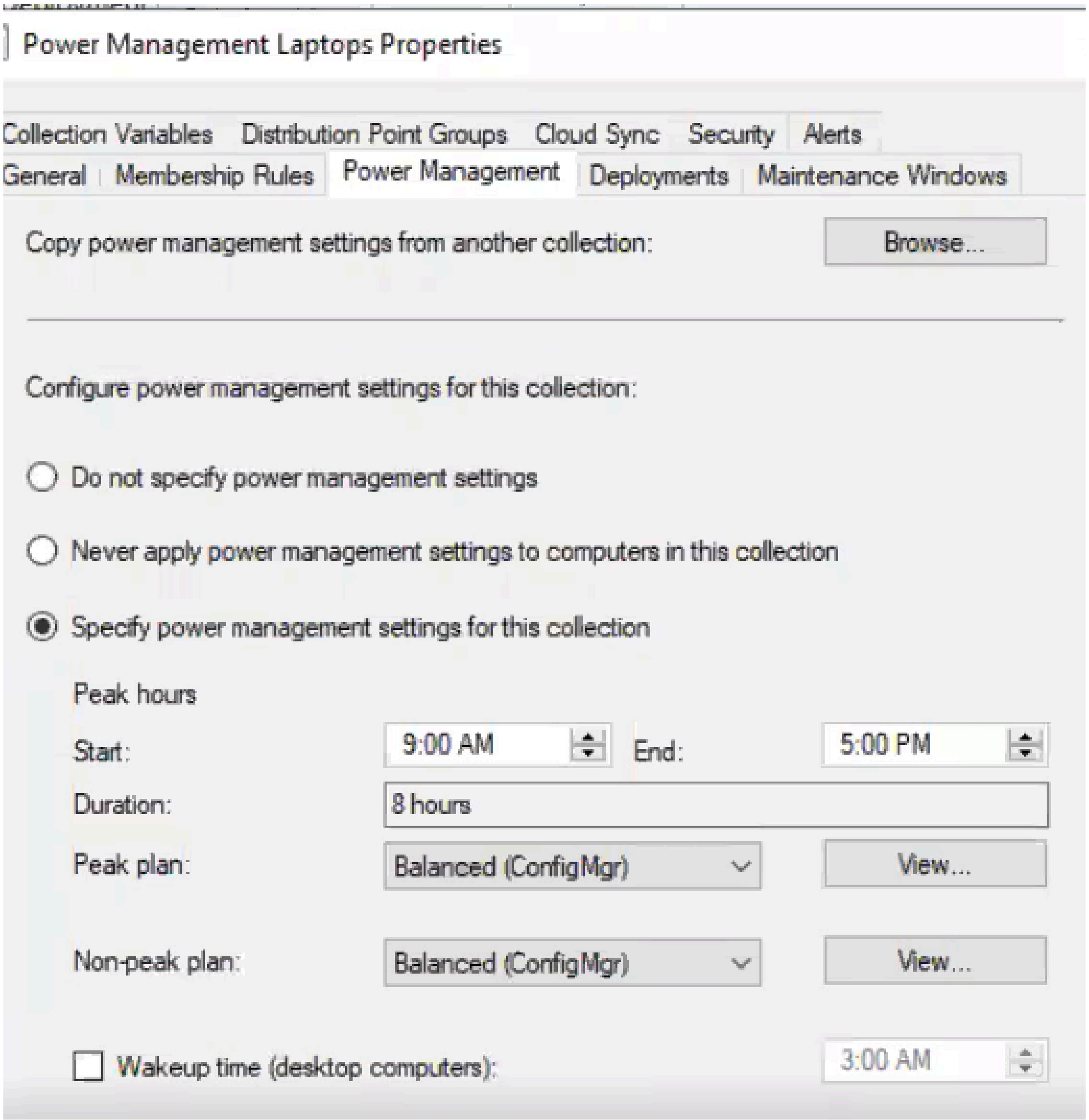
□ SADC01
□ SASCCM01
☑ SAW01



\ ▸ Administration ▸ Overview ▸ Client Settings

Client Settings 2 items

Icon	Name	Type	Priority	Deploy
✓	Default Client Settings	Default	10000	0
✓	Remote Desktop	Device	1	1



Power Management Laptops Properties

Copy power management settings from another collection:

Configure power management settings for this collection:

○ Do not specify power management settings

○ Never apply power management settings to computers in this collection

● Specify power management settings for this collection

Peak hours

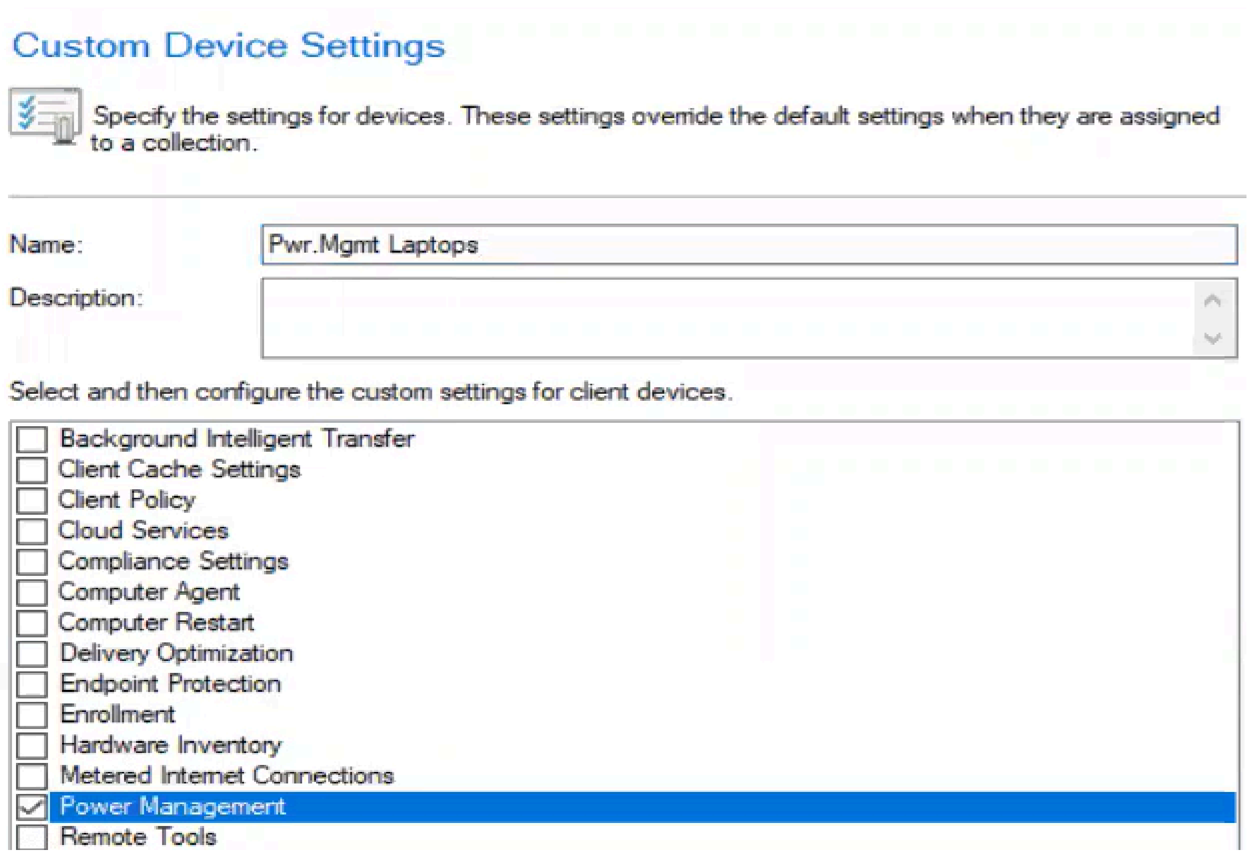
Start: 9:00 AM End: 5:00 PM

Duration: 8 hours

Peak plan: Balanced (ConfigMgr)

Non-peak plan: Balanced (ConfigMgr)

□ Wakeup time (desktop computers): 3:00 AM



Custom Device Settings

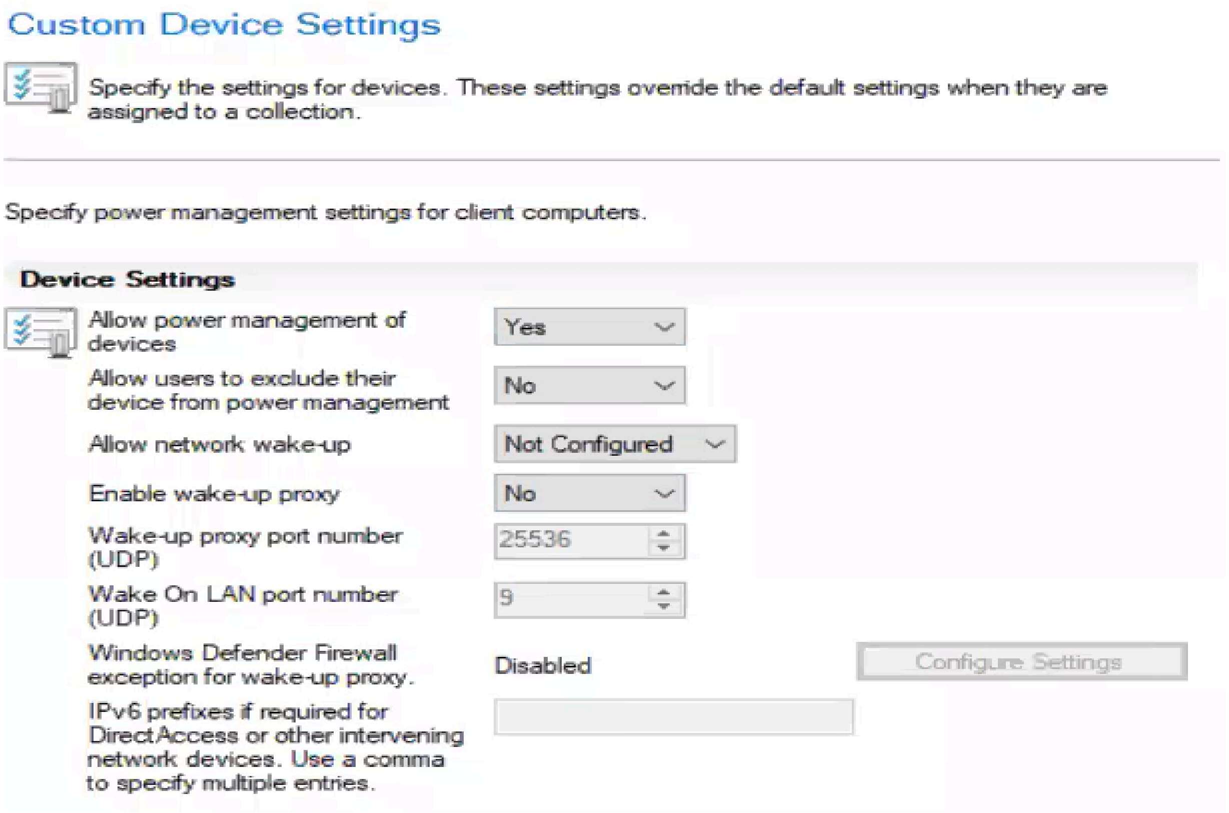
Specify the settings for devices. These settings ovenide the default settings when they are assigned to a collection.

Name: Pwr.Mgmt Laptops

Description:

Select and then configure the custom settings for client devices.

- ☐ Background Intelligent Transfer
- ☐ Client Cache Settings
- ☐ Client Policy
- ☐ Cloud Services
- ☐ Compliance Settings
- ☐ Computer Agent
- ☐ Computer Restart
- ☐ Delivery Optimization
- ☐ Endpoint Protection
- ☐ Enrollment
- ☐ Hardware Inventory
- ☐ Metered Intemet Connections
- ☑ Power Management
- ☐ Remote Tools



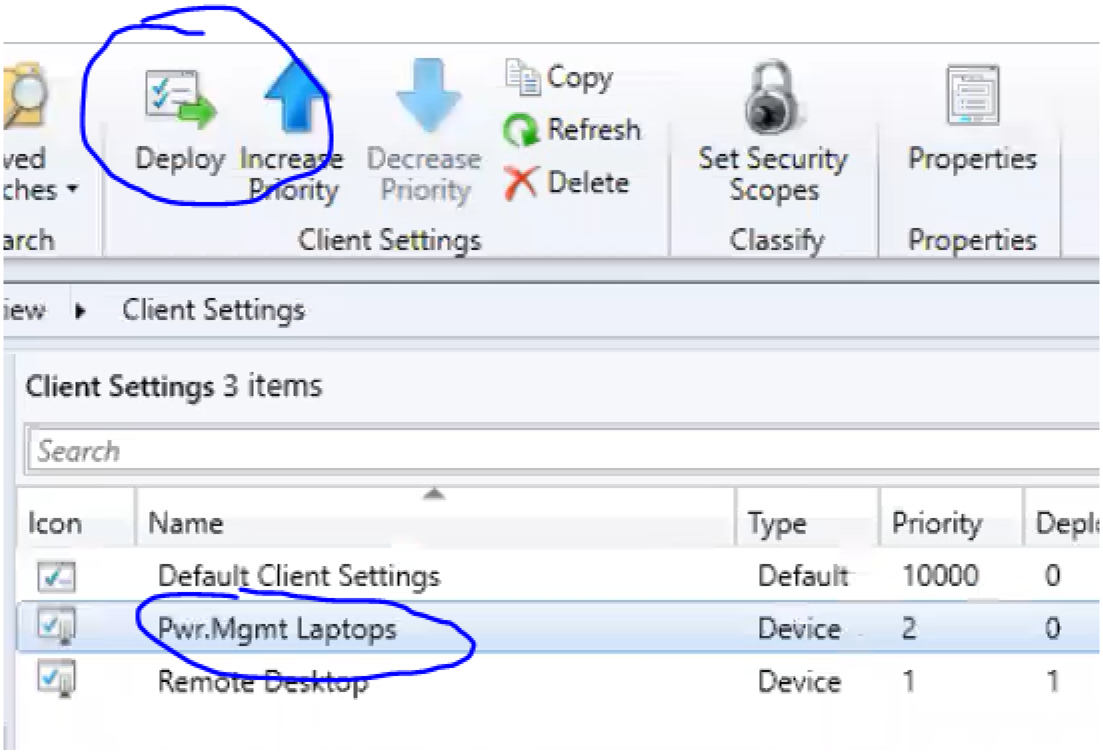
Custom Device Settings

Specify the settings for devices. These settings ovenide the default settings when they are assigned to a collection.

Specify power management settings for client computers.

Device Settings

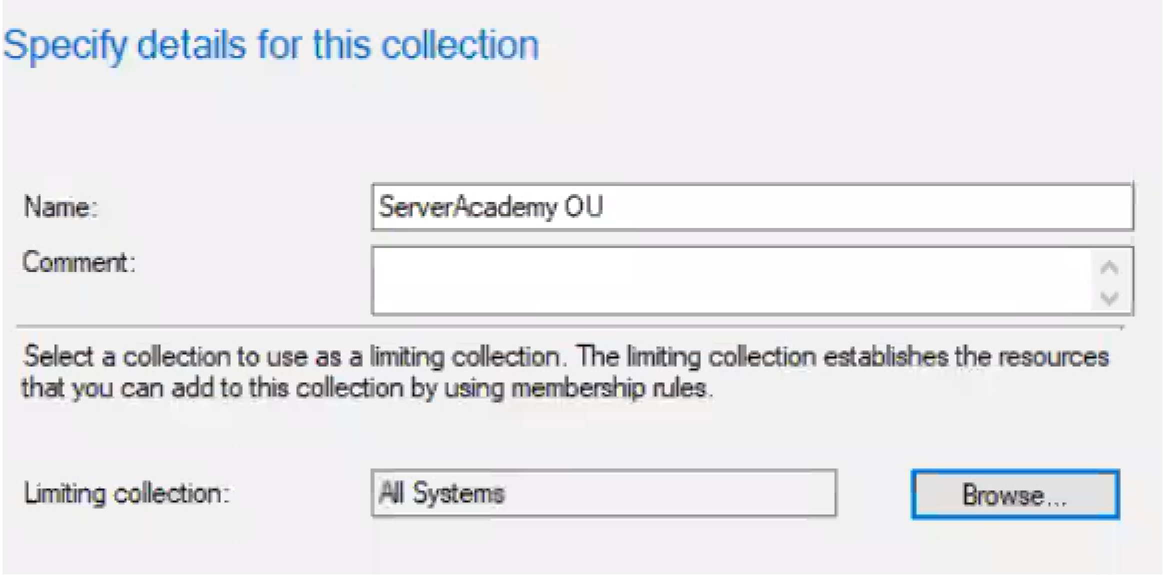
Allow power management of devices	Yes
Allow users to exclude their device from power management	No
Allow network wake-up	Not Configured
Enable wake-up proxy	No
Wake-up proxy port number (UDP)	25536
Wake On LAN port number (UDP)	9
Windows Defender Firewall exception for wake-up proxy.	Disabled
IPv6 prefixes if required for DirectAccess or other intervening network devices. Use a comma to specify multiple entries.	



Client Settings 3 items

Icon	Name	Type	Priority	Depl
✓	Default Client Settings	Default	10000	0
✓	Pwr.Mgmt Laptops	Device	2	0
✓	Remote Desktop	Device	1	1

Creating a Maintenance Window with Collections



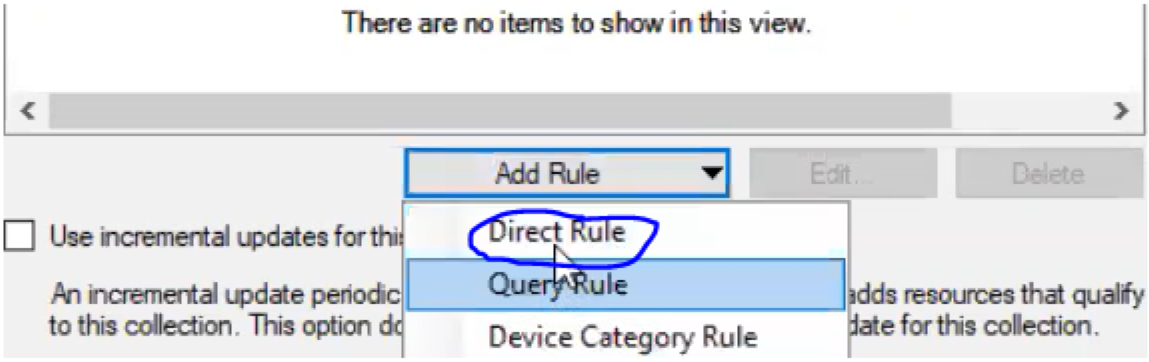
Specify details for this collection

Name: ServerAcademy OU

Comment:

Select a collection to use as a limiting collection. The limiting collection establishes the resources that you can add to this collection by using membership rules.

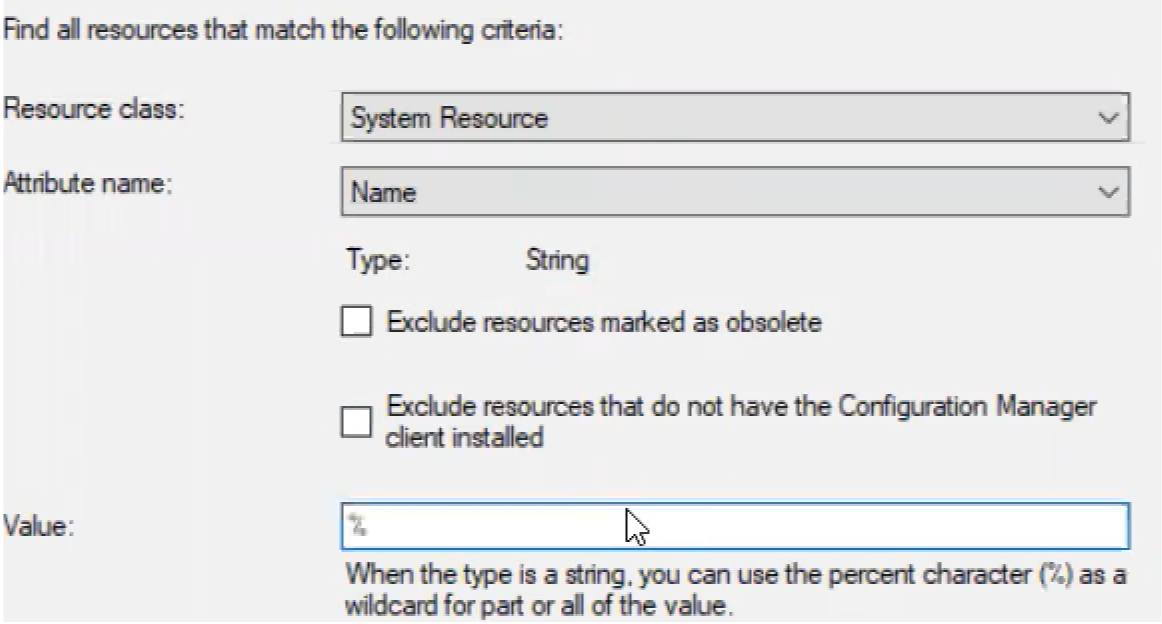
Limiting collection: All Systems



There are no items to show in this view.

□ Use incremental updates for thi

An incremental update periodic adds resources that qualify to this collection. This option do date for this collection.



Find all resources that match the following criteria:

Resource class: System Resource

Attribute name: Name

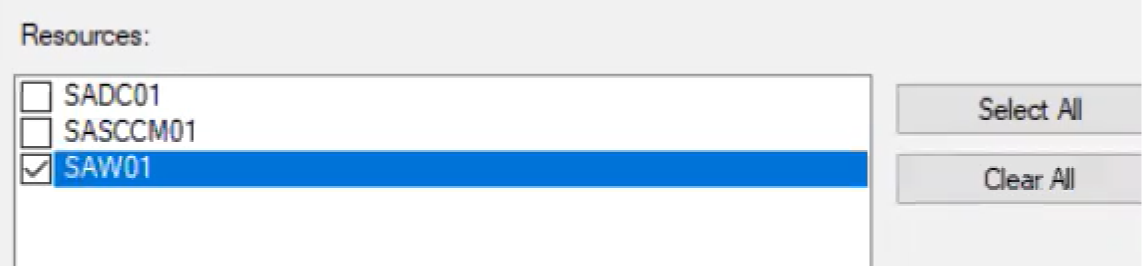
Type: String

□ Exclude resources marked as obsolete

□ Exclude resources that do not have the Configuration Manager client installed

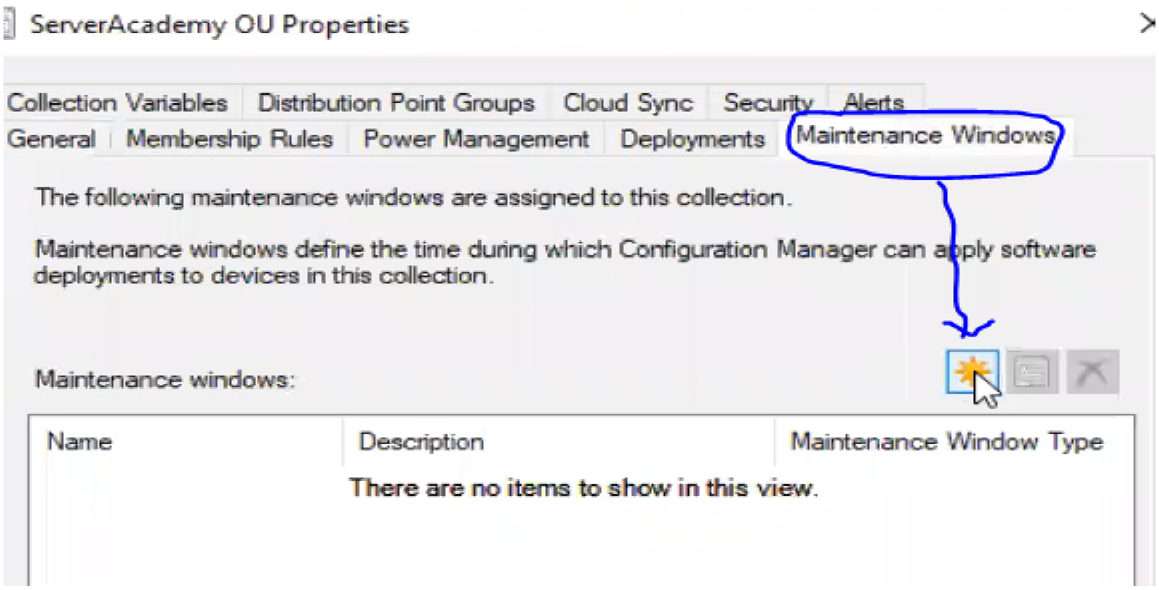
Value: %

When the type is a string, you can use the percent character (%) as a wildcard for part or all of the value.



Resources:

□ SADC01
□ SASCCM01
☑ SAW01

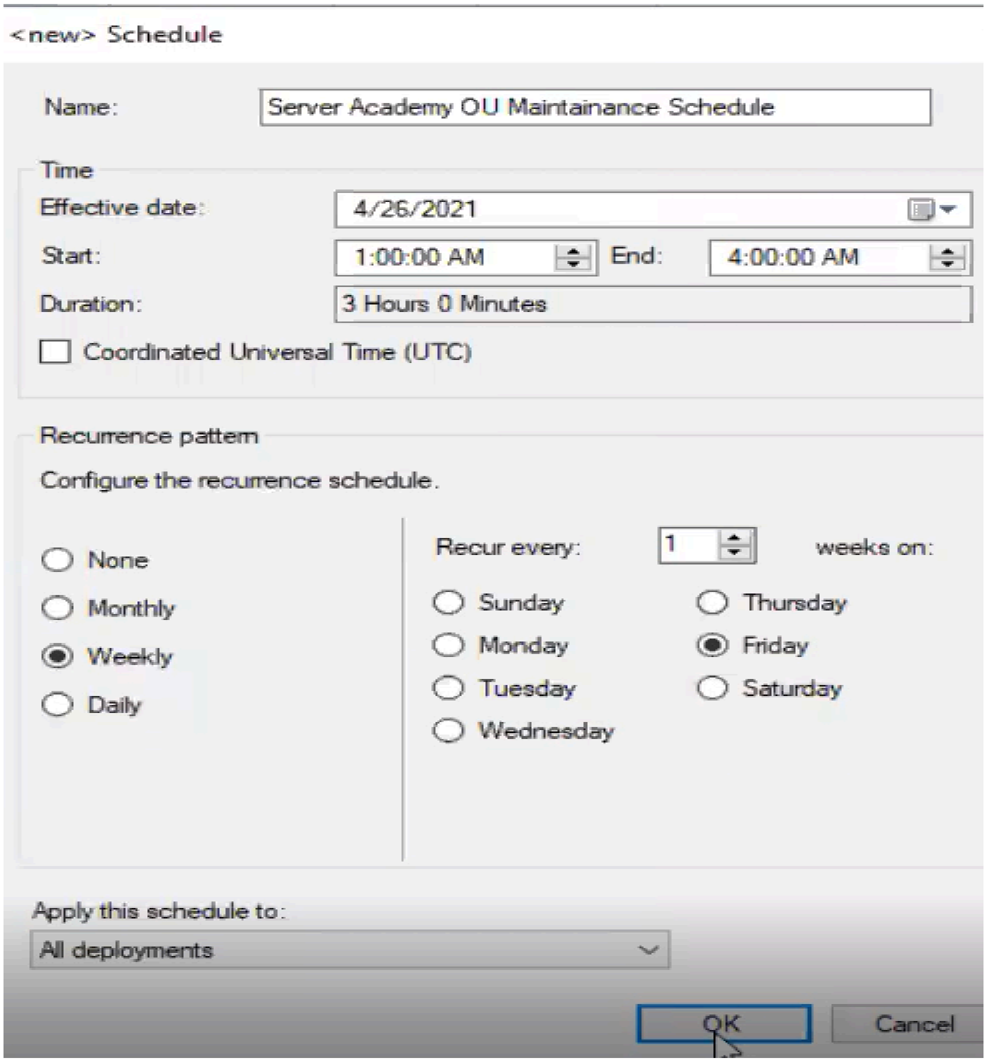


The following maintenance windows are assigned to this collection.

Maintenance windows define the time during which Configuration Manager can apply software deployments to devices in this collection.

Maintenance windows:

Name	Description	Maintenance Window Type
	There are no items to show in this view.	



Name: Server Academy OU Maintainance Schedule

Time

Effective date: 4/26/2021

Start: 1:00:00 AM End: 4:00:00 AM

Duration: 3 Hours 0 Minutes

□ Coordinated Universal Time (UTC)

Recurrence pattern

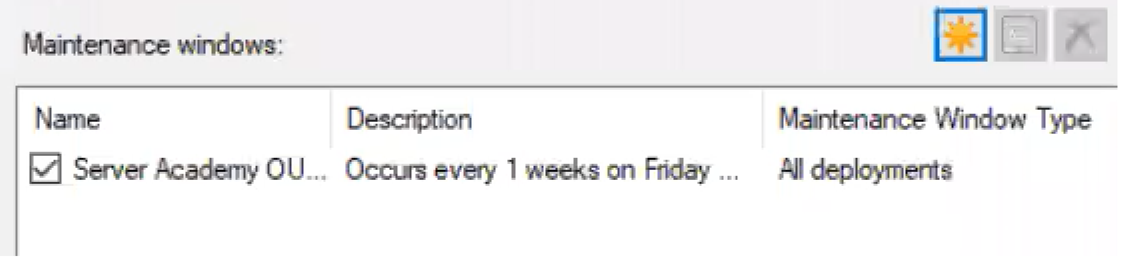
Configure the recurrence schedule.

○ None
○ Monthly
● Weekly
○ Daily

Recur every: 1 weeks on:

○ Sunday
○ Monday
○ Tuesday
○ Wednesday
○ Thursday
● Friday
○ Saturday

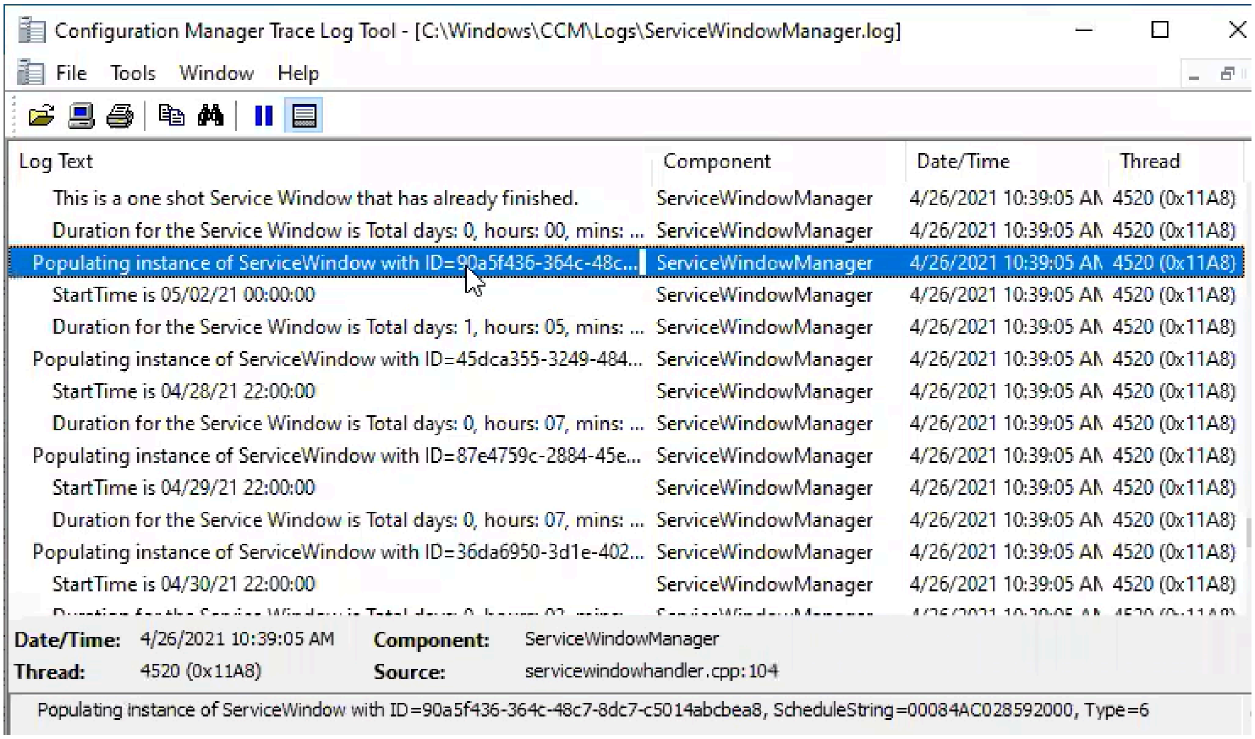
Apply this schedule to: All deployments



Maintenance windows:

Name	Description	Maintenance Window Type
☑ Server Academy OU...	Occurs every 1 weeks on Friday ...	All deployments

Running CMTrace.exe on Client to Verify Window



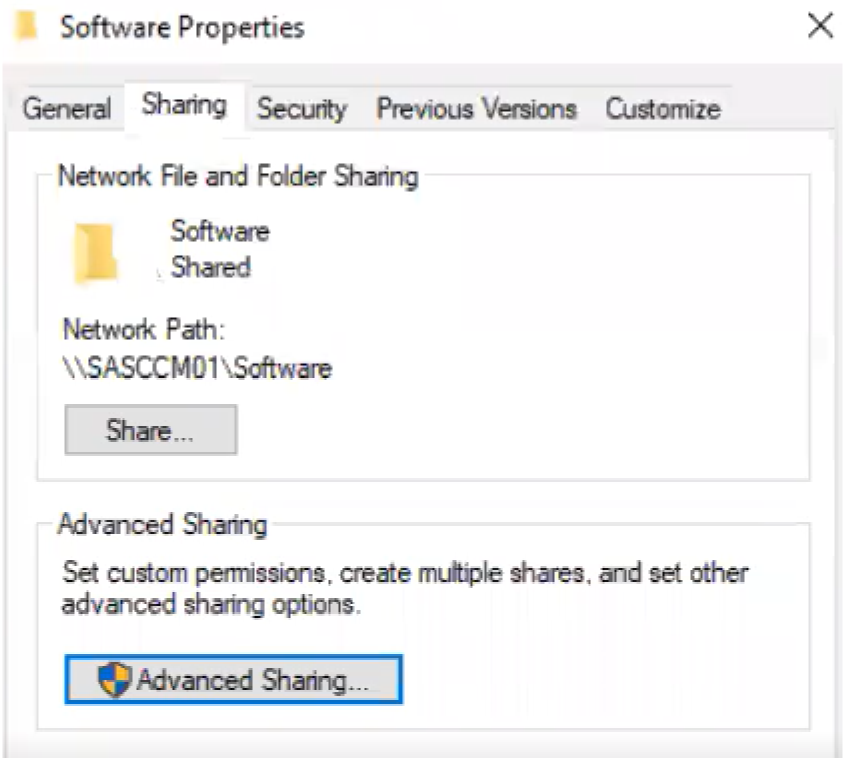
Configuration Manager Trace Log Tool - [C:\Windows\CCM\Logs\ServiceWindowManager.log]
File
Tools
Window
Help

```
Log Text                                                              Component             Date/Time              Thread
   This is a one shot Service Window that has already finished.       ServiceWindowManager  4/26/2021 10:39:05 AN  4520 (0x11A8)
   Duration for the Service Window is Total days: 0, hours: 00, mins: ...  ServiceWindowManager  4/26/2021 10:39:05 AN  4520 (0x11A8)
Populating instance of ServiceWindow with ID=90a5f436-364c-48c...     ServiceWindowManager  4/26/2021 10:39:05 AN  4520 (0x11A8)
   StartTime is 05/02/21 00:00:00                                     ServiceWindowManager  4/26/2021 10:39:05 AN  4520 (0x11A8)
   Duration for the Service Window is Total days: 1, hours: 05, mins: ...  ServiceWindowManager  4/26/2021 10:39:05 AN  4520 (0x11A8)
Populating instance of ServiceWindow with ID=45dca355-3249-484...     ServiceWindowManager  4/26/2021 10:39:05 AN  4520 (0x11A8)
   StartTime is 04/28/21 22:00:00                                     ServiceWindowManager  4/26/2021 10:39:05 AN  4520 (0x11A8)
   Duration for the Service Window is Total days: 0, hours: 07, mins: ...  ServiceWindowManager  4/26/2021 10:39:05 AN  4520 (0x11A8)
Populating instance of ServiceWindow with ID=87e4759c-2884-45e...     ServiceWindowManager  4/26/2021 10:39:05 AN  4520 (0x11A8)
   StartTime is 04/29/21 22:00:00                                     ServiceWindowManager  4/26/2021 10:39:05 AN  4520 (0x11A8)
   Duration for the Service Window is Total days: 0, hours: 07, mins: ...  ServiceWindowManager  4/26/2021 10:39:05 AN  4520 (0x11A8)
Populating instance of ServiceWindow with ID=36da6950-3d1e-402...     ServiceWindowManager  4/26/2021 10:39:05 AN  4520 (0x11A8)
   StartTime is 04/30/21 22:00:00                                     ServiceWindowManager  4/26/2021 10:39:05 AN  4520 (0x11A8)
```

Date/Time: 4/26/2021 10:39:05 AM **Component:** ServiceWindowManager
Thread: 4520 (0x11A8) **Source:** servicewindowhandler.cpp:104

```
Populating instance of ServiceWindow with ID=90a5f436-364c-48c7-8dc7-c5014abcbea8, ScheduleString=00084AC028592000, Type=6
```

Deploying 7-Zip Application to Software Center on Client



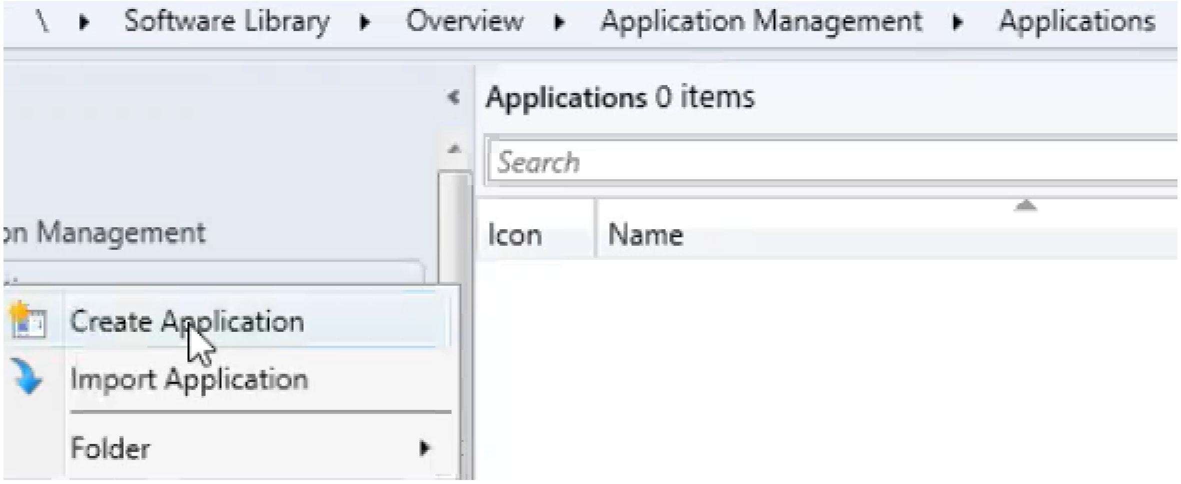
Network File and Folder Sharing

Software
Shared

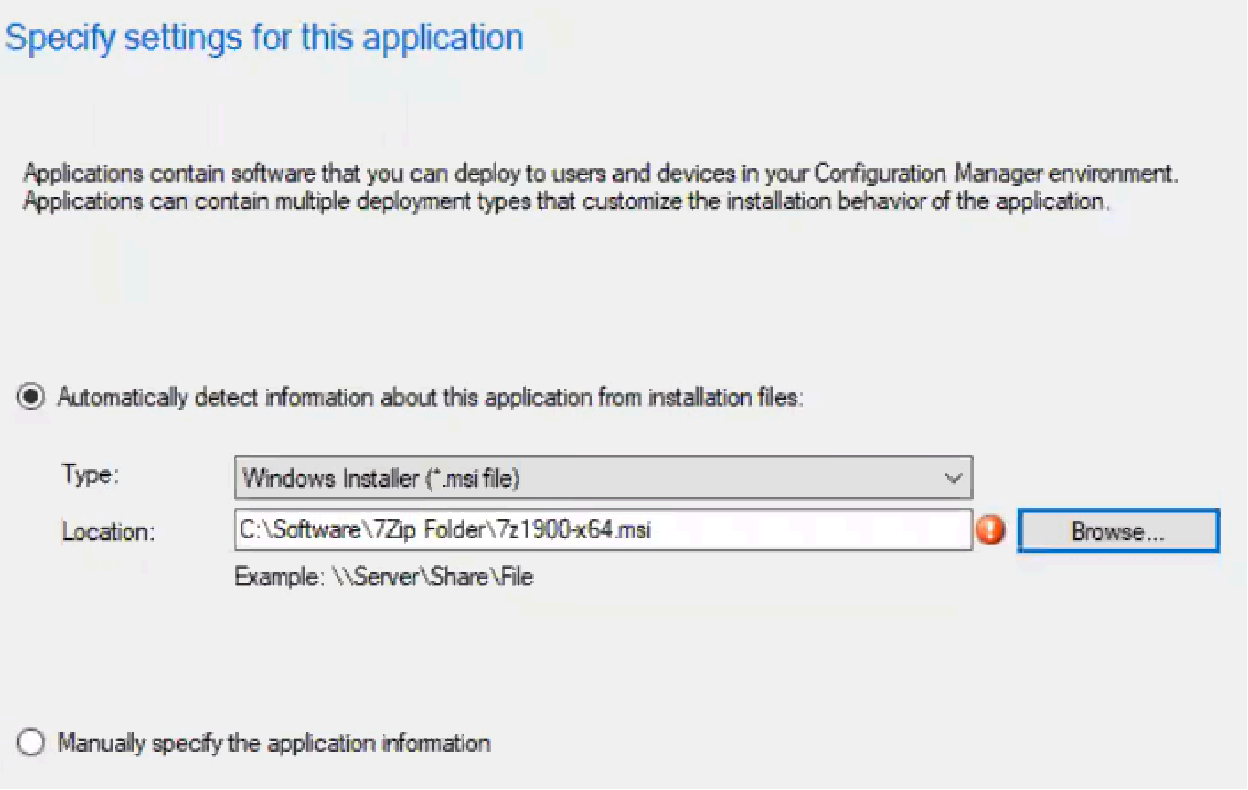
Network Path:
\\SASCCM01\Software

Advanced Sharing

Set custom permissions, create multiple shares, and set other advanced sharing options.



Downloaded .MSI version of 7-Zip on a shared folder on Hypervisor for Creation



Specify settings for this application

Applications contain software that you can deploy to users and devices in your Configuration Manager environment. Applications can contain multiple deployment types that customize the installation behavior of the application.

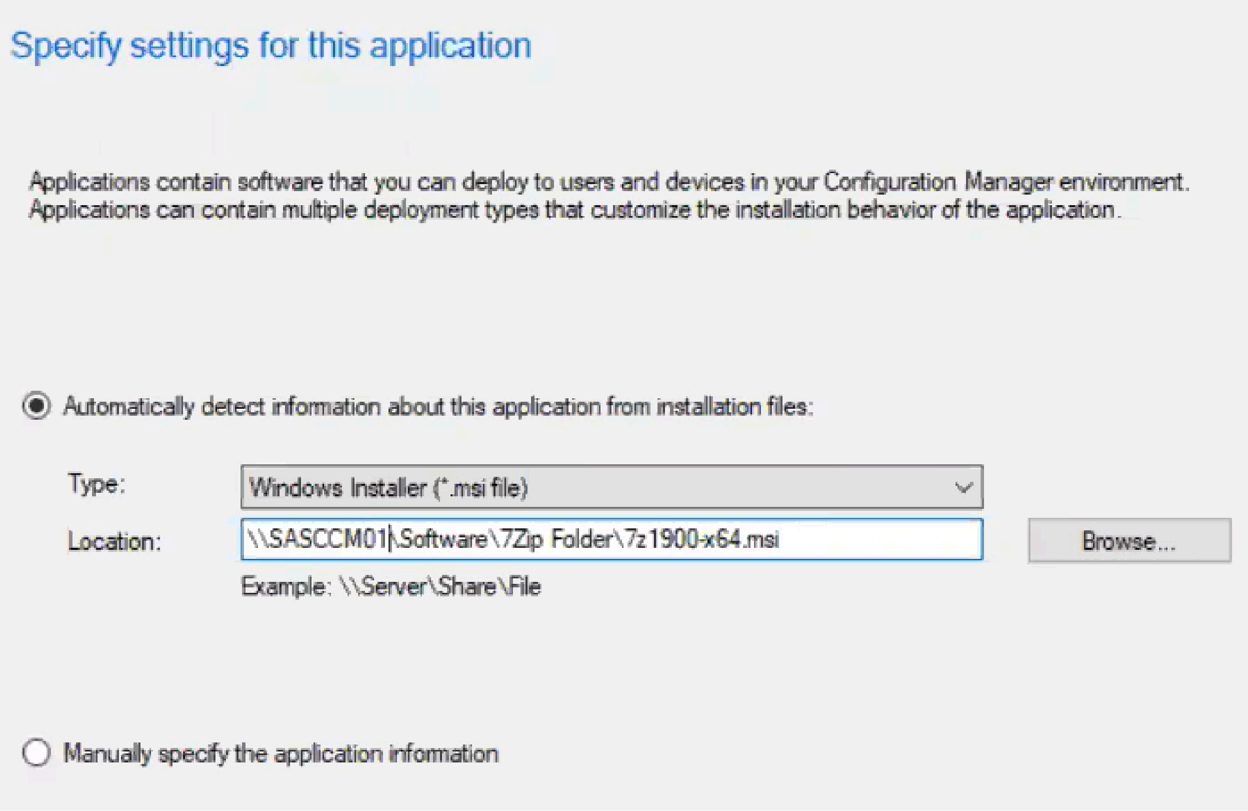
● Automatically detect information about this application from installation files:

Type: Windows Installer (*.msi file)

Location: C:\Software\7Zip Folder\7z1900-x64.msi

Example: \\Server\Share\File

○ Manually specify the application information



Specify settings for this application

Applications contain software that you can deploy to users and devices in your Configuration Manager environment. Applications can contain multiple deployment types that customize the installation behavior of the application.

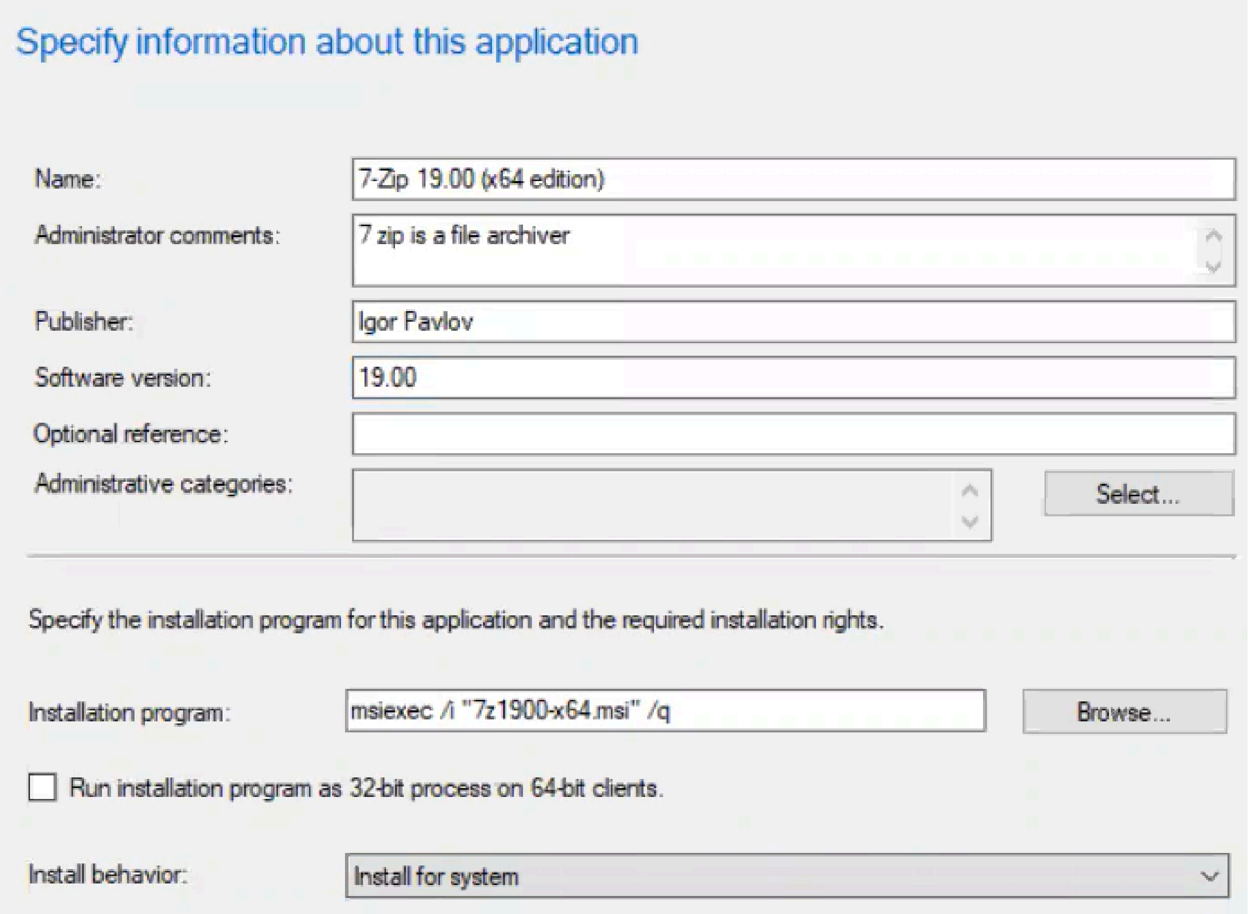
● Automatically detect information about this application from installation files:

Type: Windows Installer (*.msi file)

Location: \\SASCCM01\Software\7Zip Folder\7z1900-x64.msi

Example: \\Server\Share\File

○ Manually specify the application information



Specify information about this application

Name: 7-Zip 19.00 (x64 edition)

Administrator comments: 7 zip is a file archiver

Publisher: Igor Pavlov

Software version: 19.00

Optional reference:

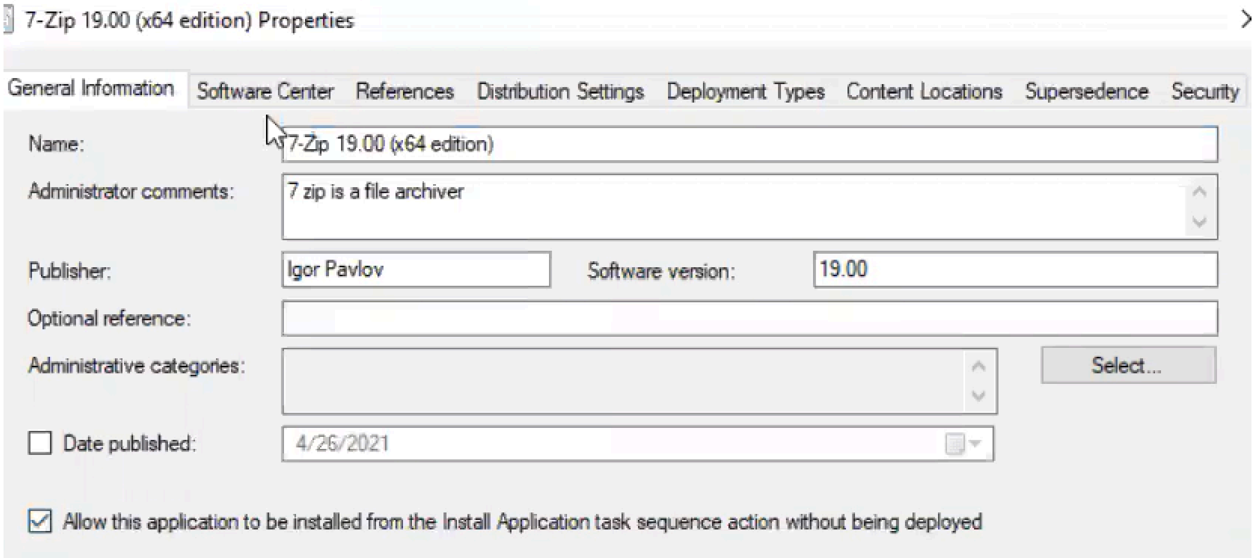
Administrative categories:

Specify the installation program for this application and the required installation rights.

Installation program: msiexec /i "7z1900-x64.msi" /q

□ Run installation program as 32-bit process on 64-bit clients.

Install behavior: Install for system



7-Zip 19.00 (x64 edition) Properties

Name: 7-Zip 19.00 (x64 edition)

Administrator comments: 7 zip is a file archiver

Publisher: Igor Pavlov

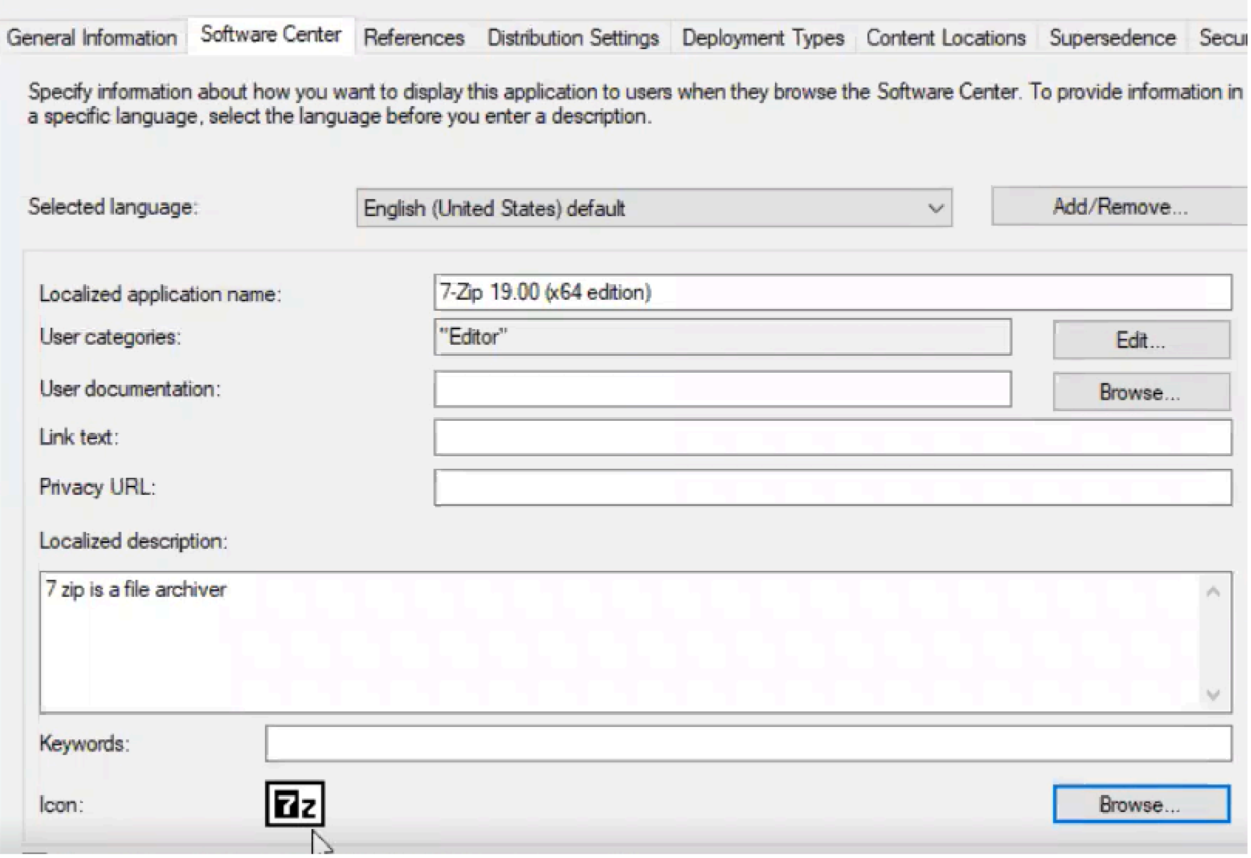
Software version: 19.00

Optional reference:

Administrative categories:

□ Date published: 4/26/2021

☑ Allow this application to be installed from the Install Application task sequence action without being deployed



Specify information about how you want to display this application to users when they browse the Software Center. To provide information in a specific language, select the language before you enter a description.

Selected language: English (United States) default

Localized application name: 7-Zip 19.00 (x64 edition)

User categories: "Editor"

User documentation:

Link text:

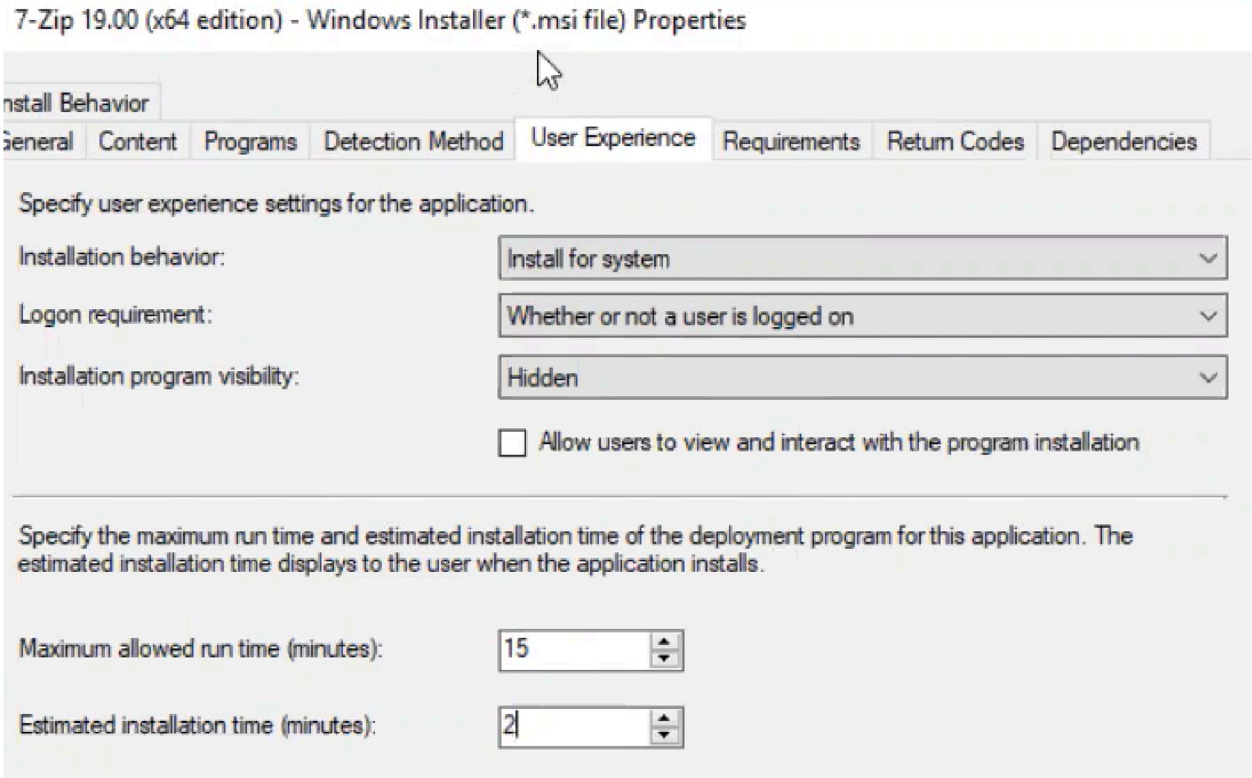
Privacy URL:

Localized description:

7 zip is a file archiver

Keywords:

Icon: 7z


7-Zip 19.00 (x64 edition) - Windows Installer (*.msi file) Properties

Specify user experience settings for the application.

Installation behavior: Install for system

Logon requirement: Whether or not a user is logged on

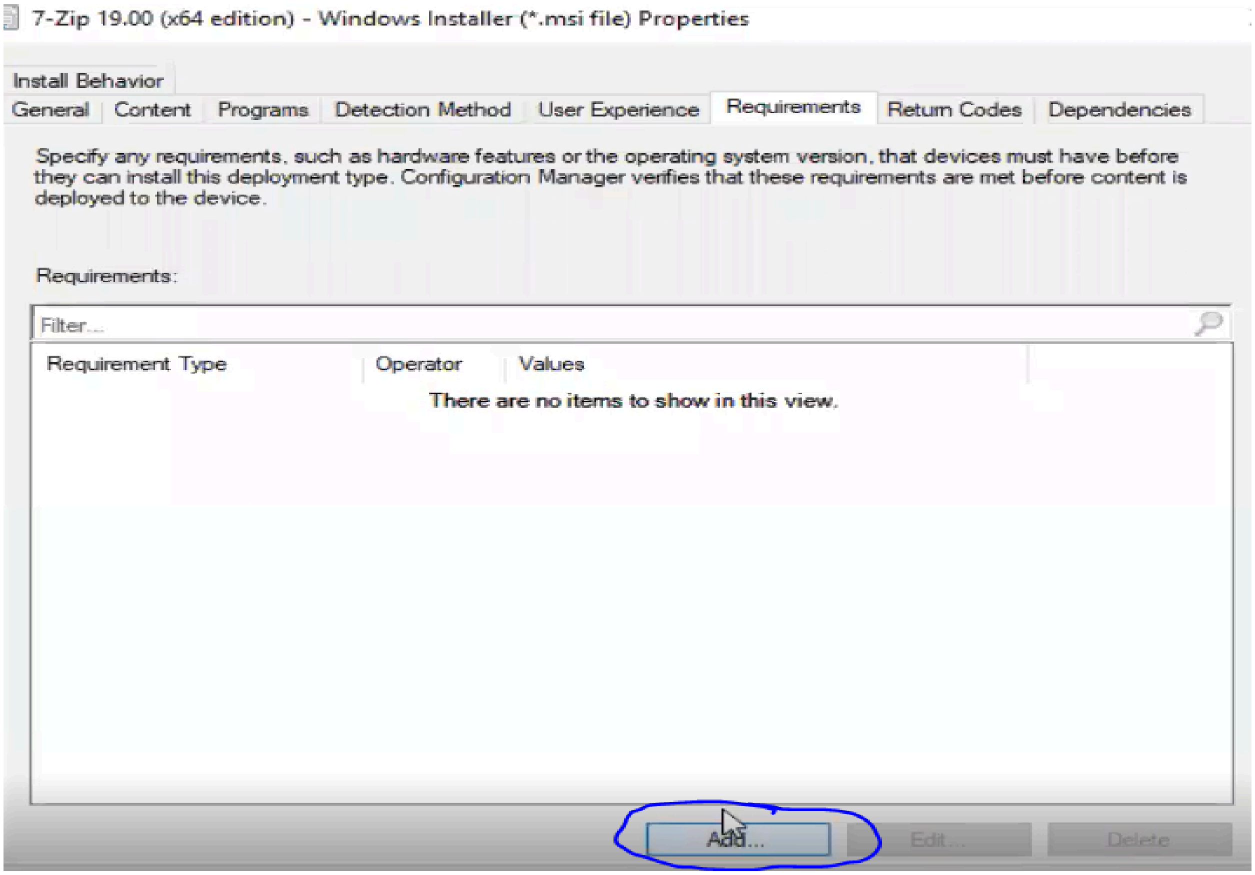
Installation program visibility: Hidden

□ Allow users to view and interact with the program installation

Specify the maximum run time and estimated installation time of the deployment program for this application. The estimated installation time displays to the user when the application installs.

Maximum allowed run time (minutes): 15

Estimated installation time (minutes): 2



7-Zip 19.00 (x64 edition) - Windows Installer (*.msi file) Properties

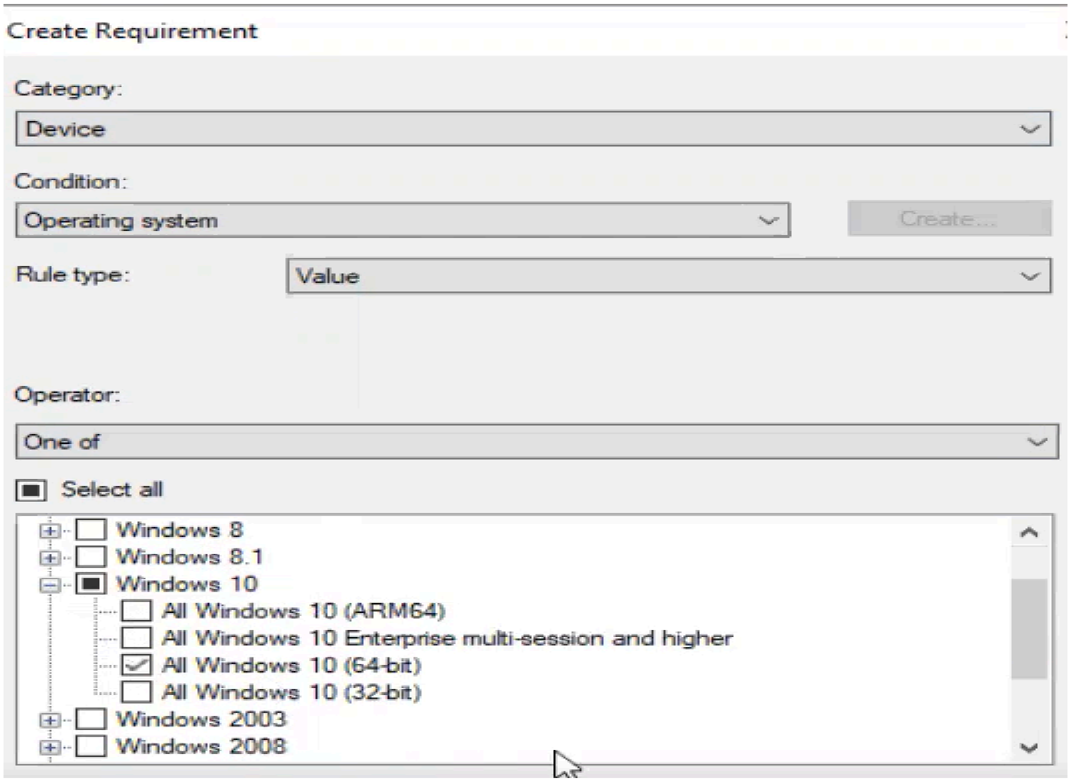
Specify any requirements, such as hardware features or the operating system version, that devices must have before they can install this deployment type. Configuration Manager verifies that these requirements are met before content is deployed to the device.

Requirements:

Filter...

Requirement Type	Operator	Values

There are no items to show in this view.



Create Requirement

Category: Device

Condition: Operating system

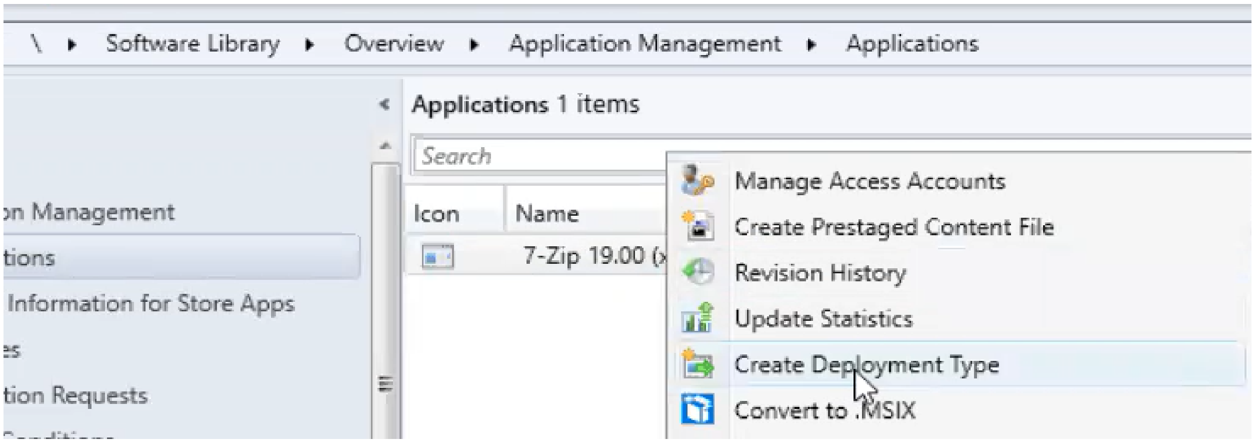
Rule type: Value

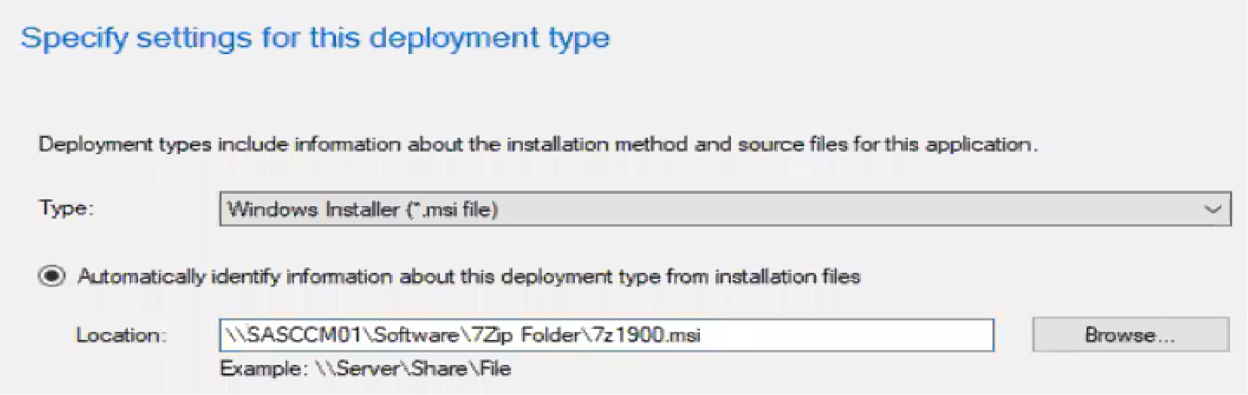
Operator: One of

■ Select all

- □ Windows 8
- □ Windows 8.1
- ■ Windows 10
  - □ All Windows 10 (ARM64)
  - □ All Windows 10 Enterprise multi-session and higher
  - ☑ All Windows 10 (64-bit)
  - □ All Windows 10 (32-bit)
- □ Windows 2003
- □ Windows 2008

Creating a Deployment for 32bit Version of 7-Zip





Specify settings for this deployment type

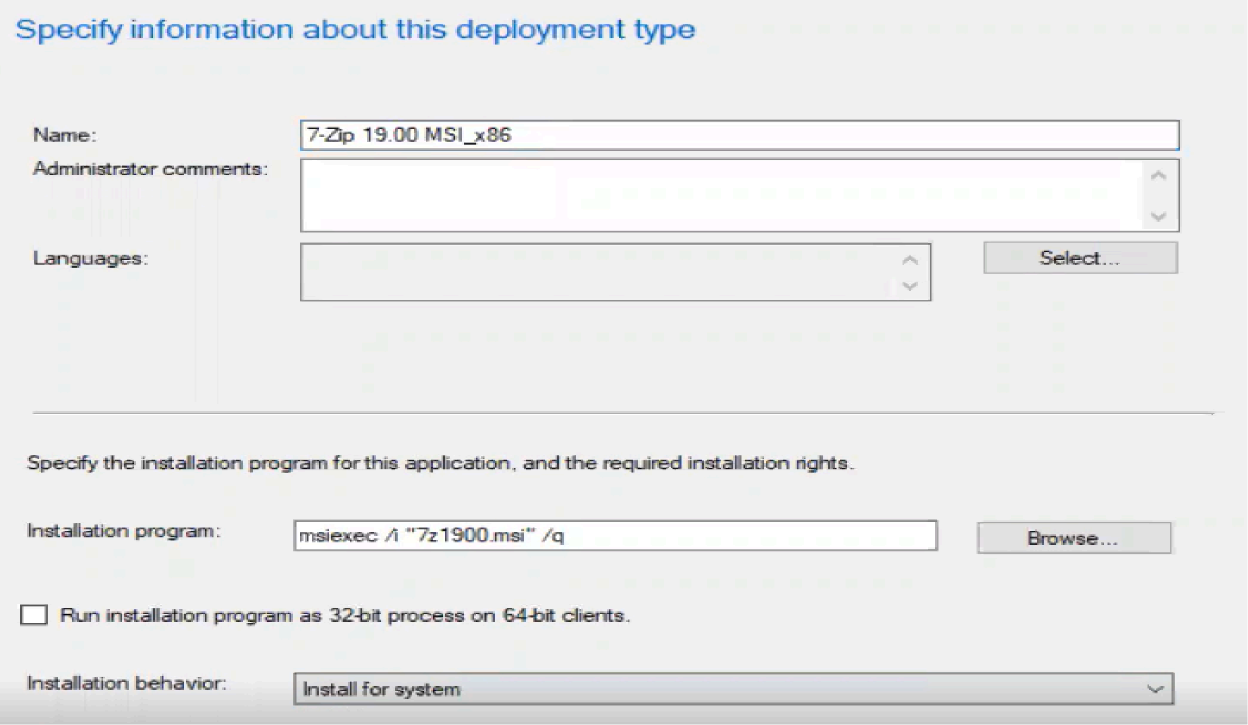
Deployment types include information about the installation method and source files for this application.

Type: Windows Installer (*.msi file)

● Automatically identify information about this deployment type from installation files

Location: \\SASCCM01\Software\7Zip Folder\7z1900.msi

Example: \\Server\Share\File



Specify information about this deployment type

Name: 7-Zip 19.00 MSI_x86

Administrator comments:

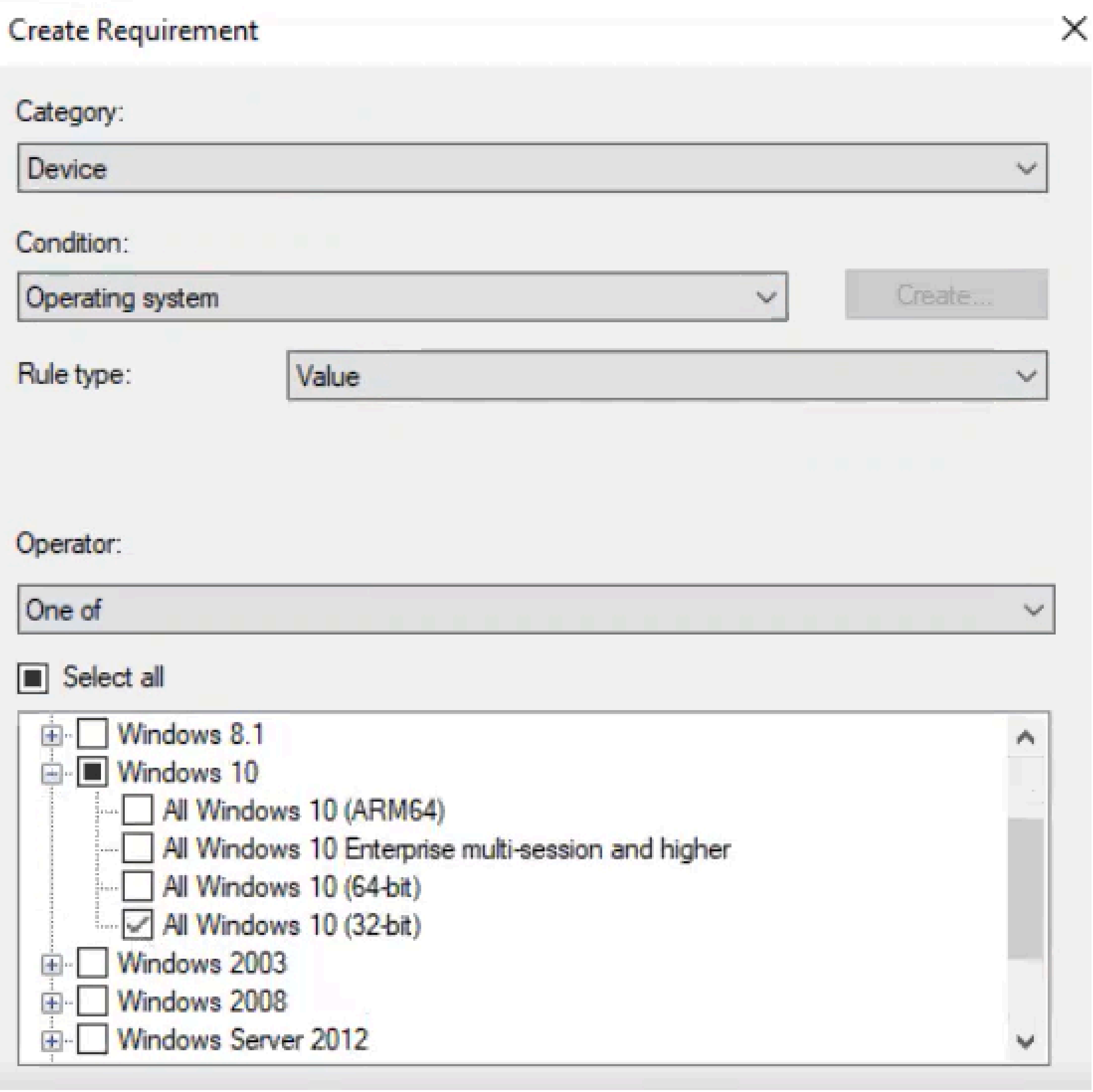
Languages:

Specify the installation program for this application, and the required installation rights.

Installation program: msiexec /i "7z1900.msi" /q

□ Run installation program as 32-bit process on 64-bit clients.

Installation behavior: Install for system



Create Requirement

Category: Device

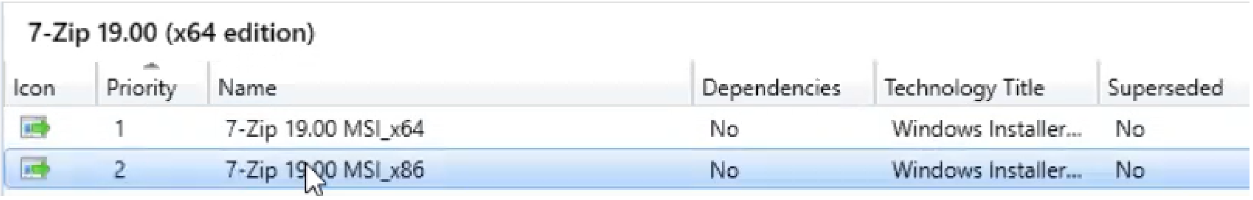
Condition: Operating system

Rule type: Value

Operator: One of

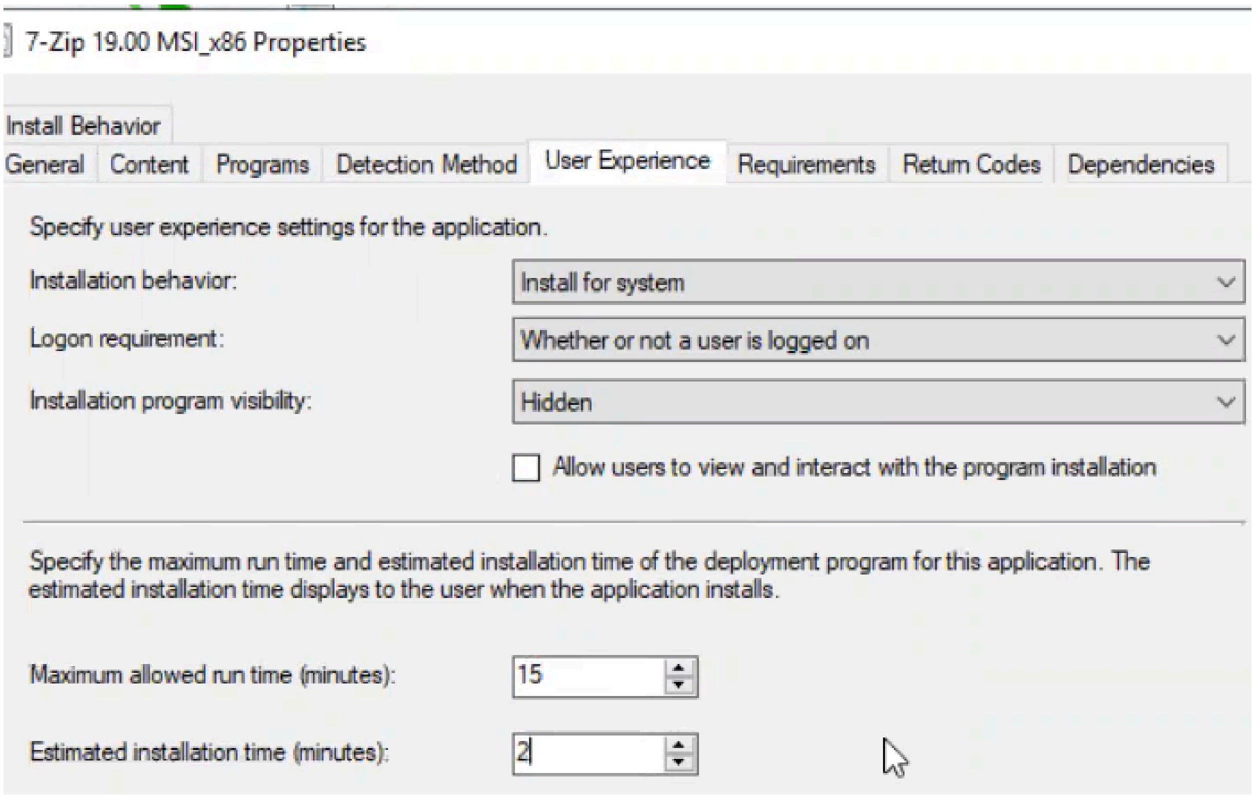
■ Select all

- □ Windows 8.1
- ■ Windows 10
  - □ All Windows 10 (ARM64)
  - □ All Windows 10 Enterprise multi-session and higher
  - □ All Windows 10 (64-bit)
  - ☑ All Windows 10 (32-bit)
- □ Windows 2003
- □ Windows 2008
- □ Windows Server 2012



7-Zip 19.00 (x64 edition)

Icon	Priority	Name	Dependencies	Technology Title	Superseded
	1	7-Zip 19.00 MSI_x64	No	Windows Installer...	No
	2	7-Zip 19.00 MSI_x86	No	Windows Installer...	No



7-Zip 19.00 MSI_x86 Properties

Specify user experience settings for the application.

Installation behavior: Install for system

Logon requirement: Whether or not a user is logged on

Installation program visibility: Hidden

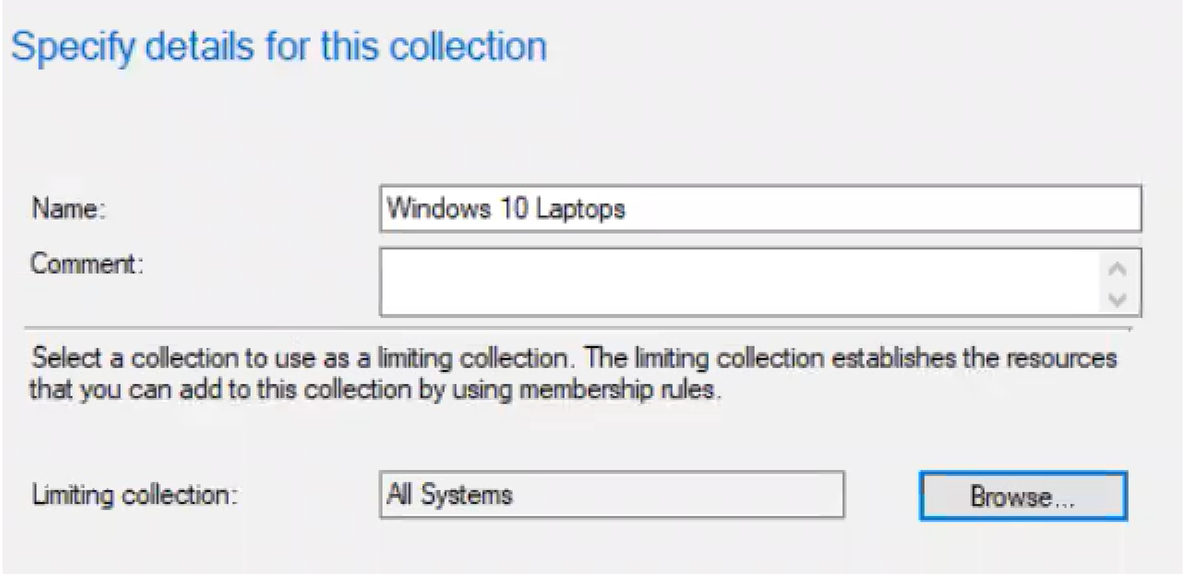
☐ Allow users to view and interact with the program installation

Specify the maximum run time and estimated installation time of the deployment program for this application. The estimated installation time displays to the user when the application installs.

Maximum allowed run time (minutes): 15

Estimated installation time (minutes): 2

Creating Windows 10 Laptops Collection for 7 Zip Deployment



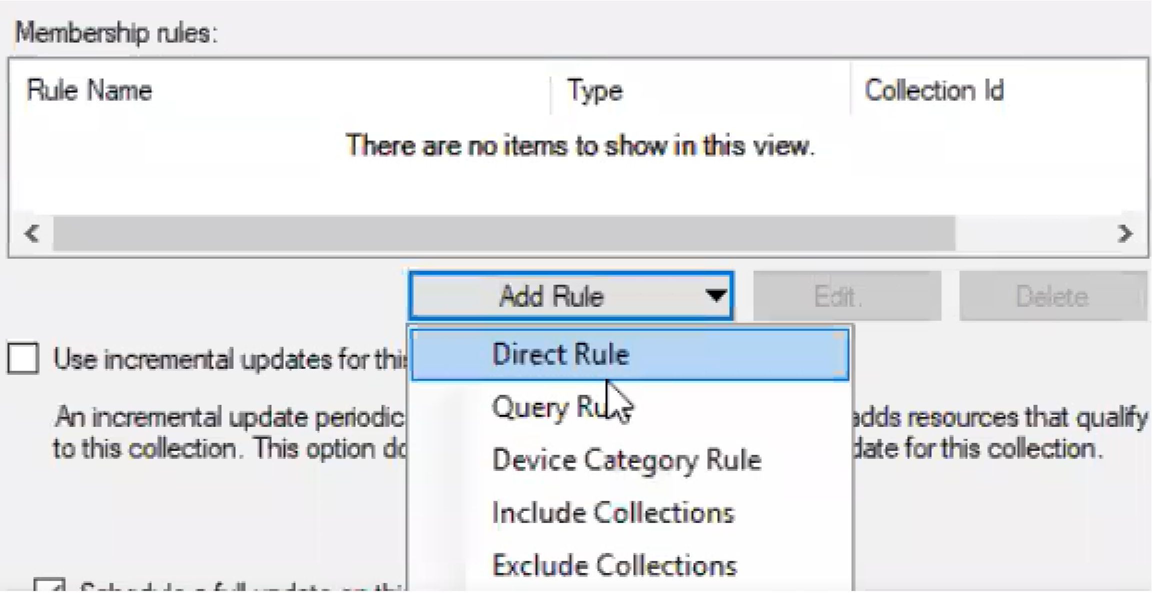
Specify details for this collection

Name: Windows 10 Laptops

Comment:

Select a collection to use as a limiting collection. The limiting collection establishes the resources that you can add to this collection by using membership rules.

Limiting collection: All Systems



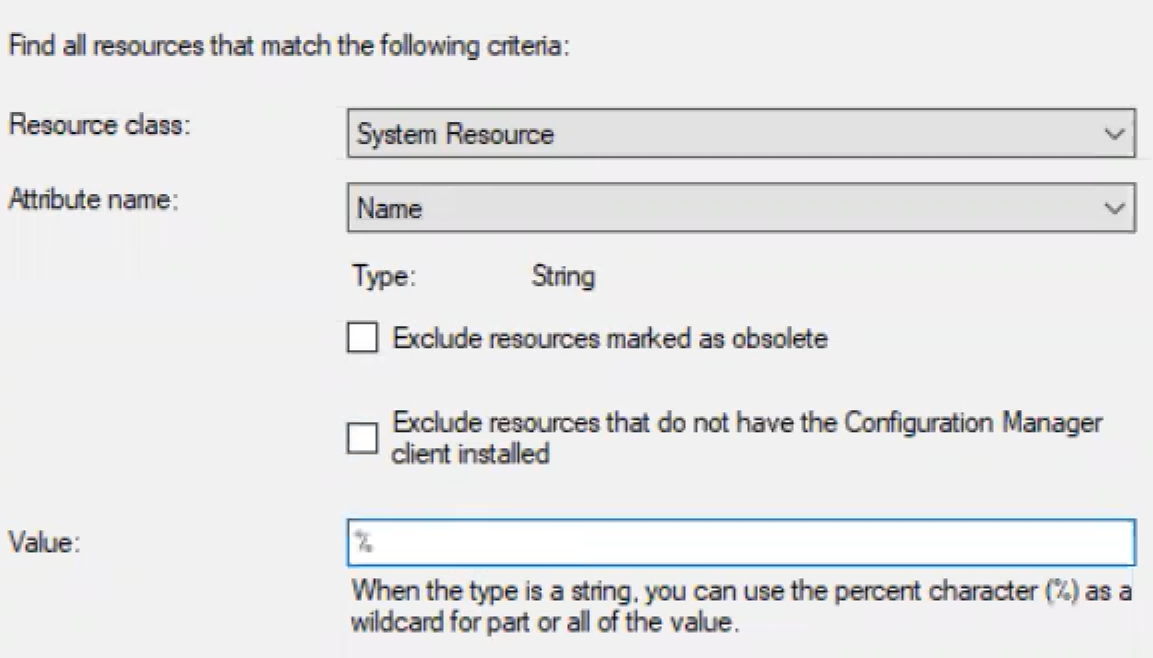
Membership rules:

Rule Name	Type	Collection Id

There are no items to show in this view.

□ Use incremental updates for thi

An incremental update periodic adds resources that qualify to this collection. This option do date for this collection.



Find all resources that match the following criteria:

Resource class: System Resource

Attribute name: Name

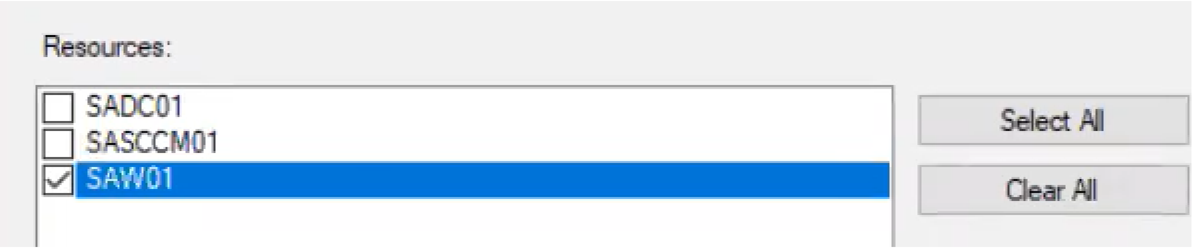
Type: String

□ Exclude resources marked as obsolete

□ Exclude resources that do not have the Configuration Manager client installed

Value: %

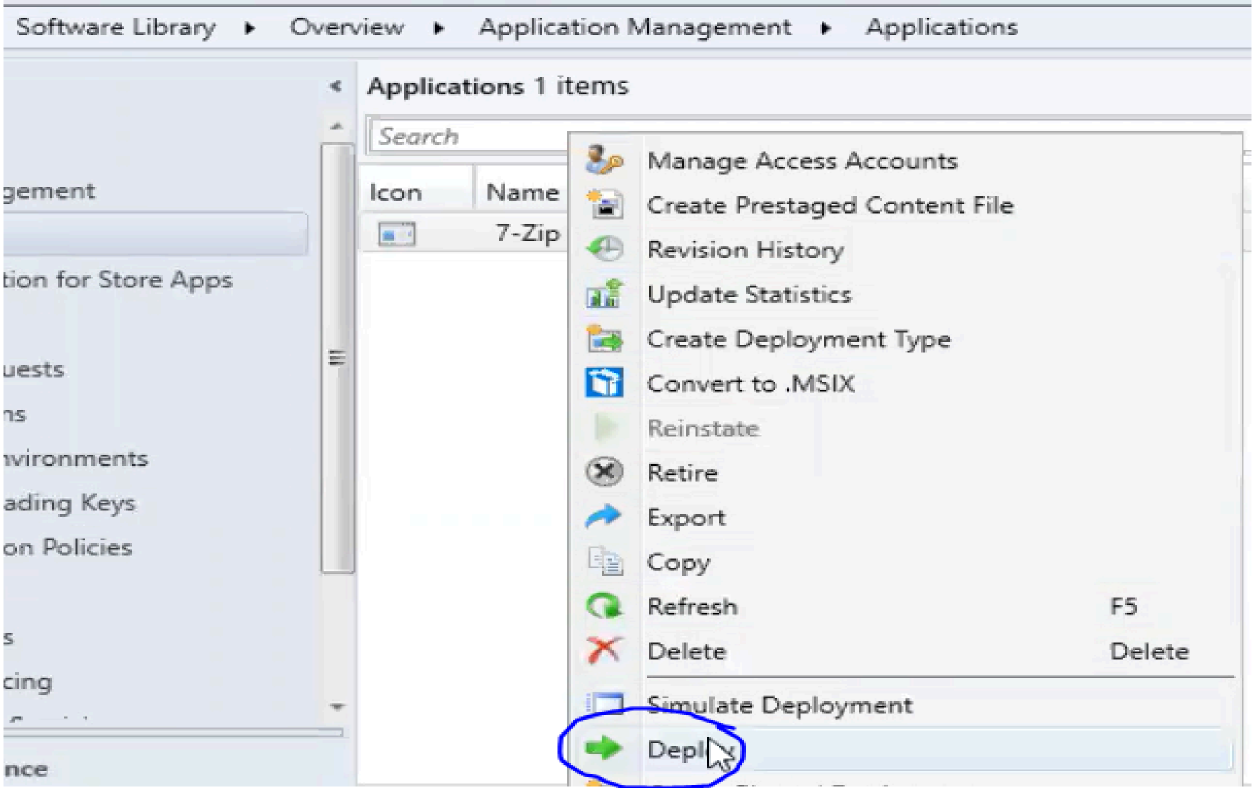
When the type is a string, you can use the percent character (%) as a wildcard for part or all of the value.

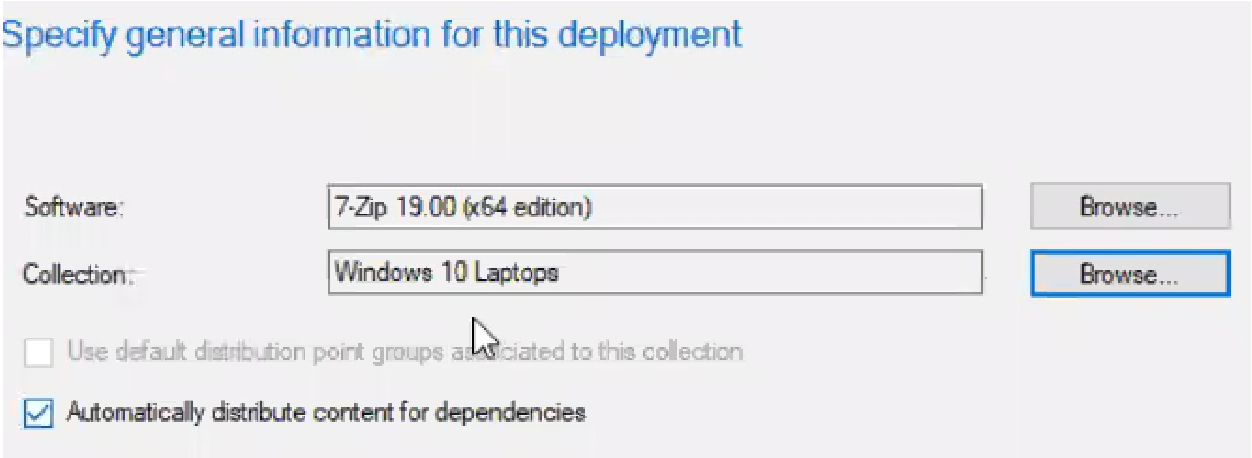


Resources:

□ SADC01
□ SASCCM01
☑ SAW01

Deploying 7 - Zip



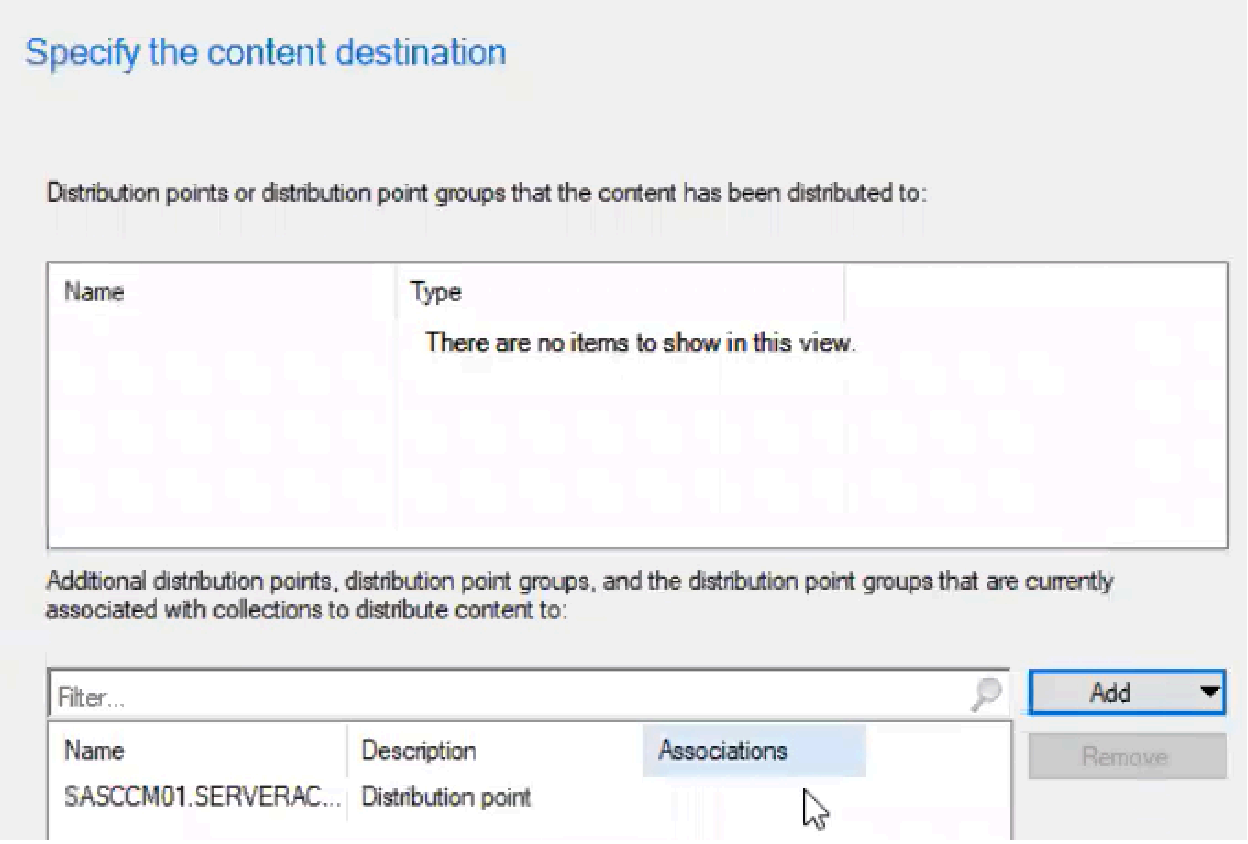

Specify general information for this deployment

Software: 7-Zip 19.00 (x64 edition) Browse...

Collection: Windows 10 Laptops Browse...

□ Use default distribution point groups associated to this collection

☑ Automatically distribute content for dependencies



Specify the content destination

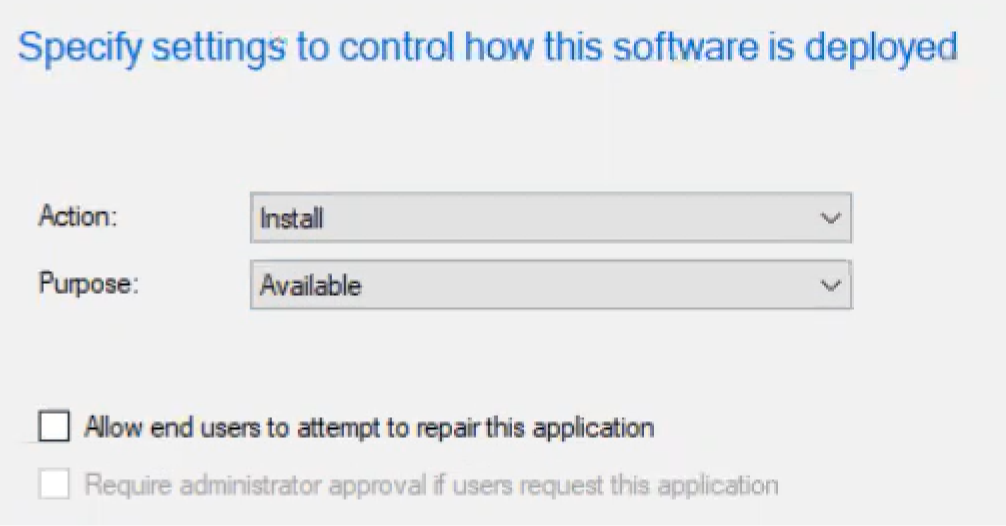
Distribution points or distribution point groups that the content has been distributed to:

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...

Name	Description	Associations
SASCCM01.SERVERAC...	Distribution point	



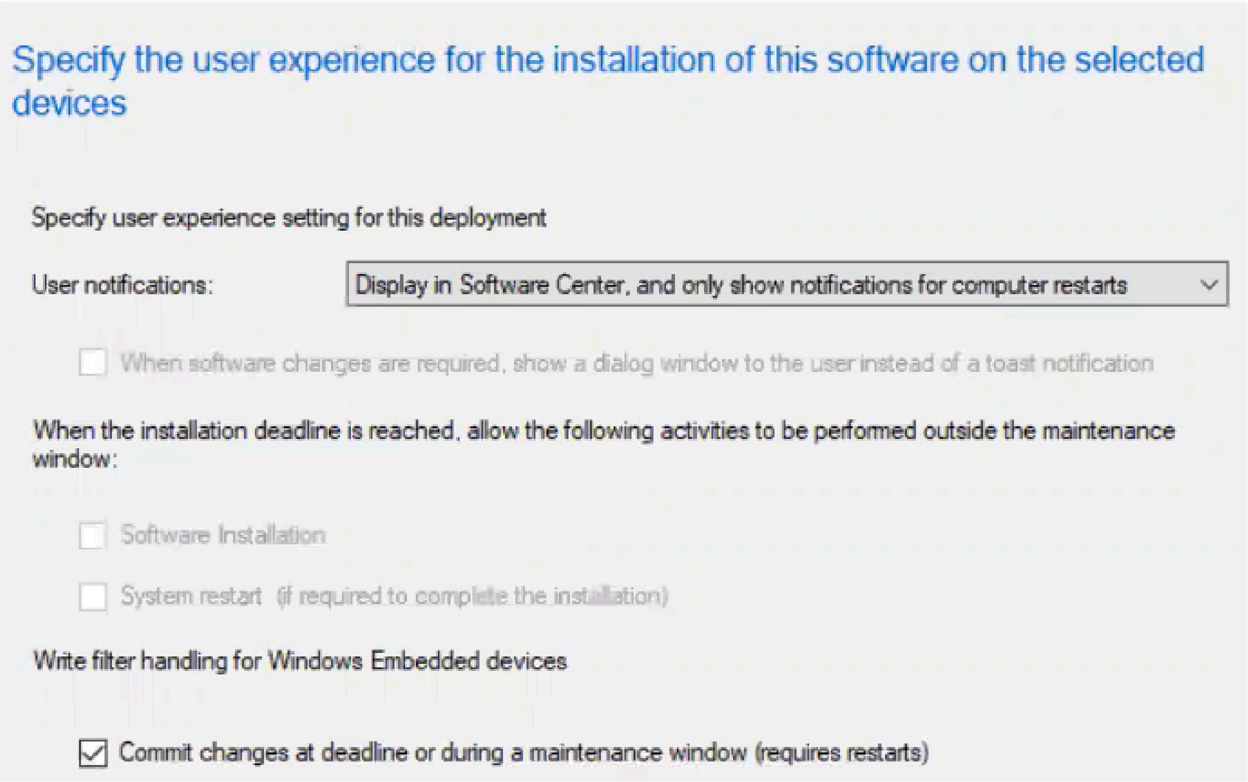
Specify settings to control how this software is deployed

Action: Install

Purpose: Available

☐ Allow end users to attempt to repair this application

☐ Require administrator approval if users request this application



Specify the user experience for the installation of this software on the selected devices

Specify user experience setting for this deployment

User notifications: Display in Software Center, and only show notifications for computer restarts

□ When software changes are required, show a dialog window to the user instead of a toast notification

When the installation deadline is reached, allow the following activities to be performed outside the maintenance window:

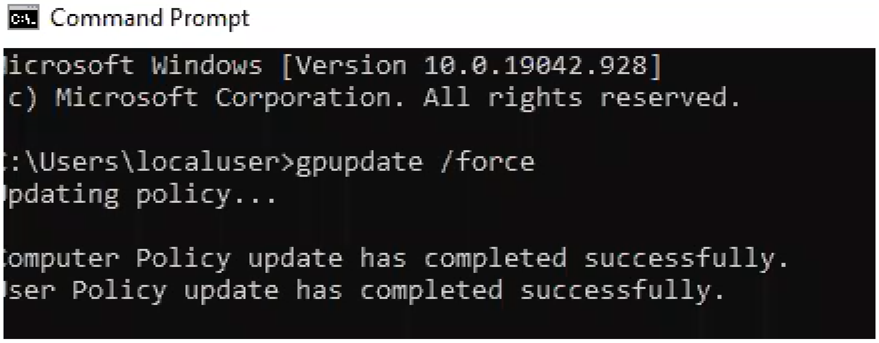
□ Software Installation

□ System restart (if required to complete the installation)

Write filter handling for Windows Embedded devices

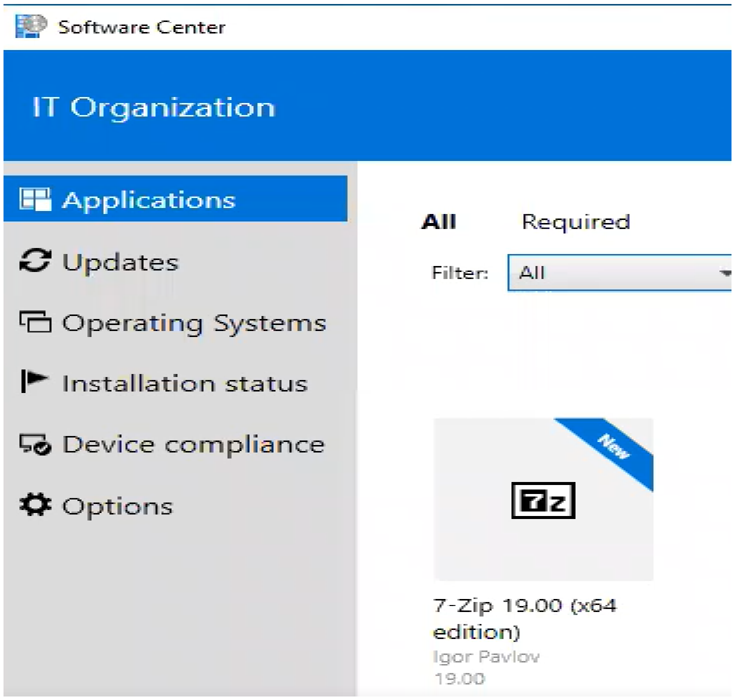
☑ Commit changes at deadline or during a maintenance window (requires restarts)

Running gpupdate in client

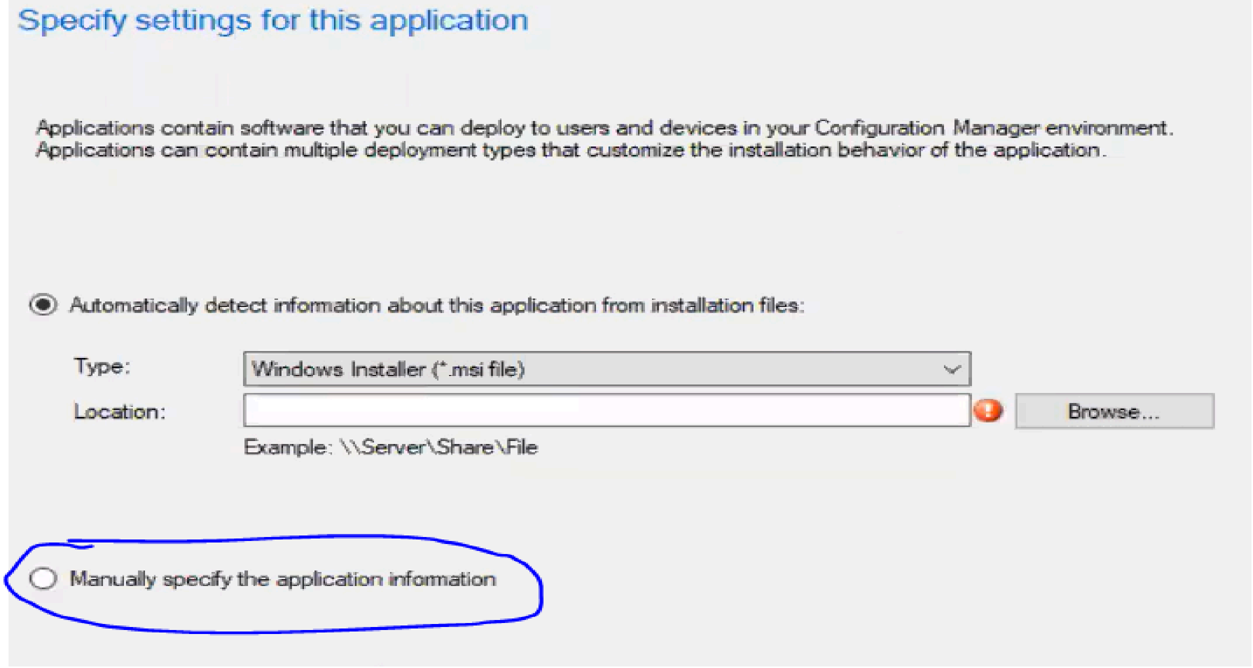


```
icrosoft Windows [Version 10.0.19042.928]
c) Microsoft Corporation. All rights reserved.

:\Users\localuser>gpupdate /force
pdating policy...

omputer Policy update has completed successfully.
ser Policy update has completed successfully.
```

7-Zip Successfully Installed in Software Center on Client



Deploying Google Chrome to Software Center



Specify settings for this application

Applications contain software that you can deploy to users and devices in your Configuration Manager environment. Applications can contain multiple deployment types that customize the installation behavior of the application.

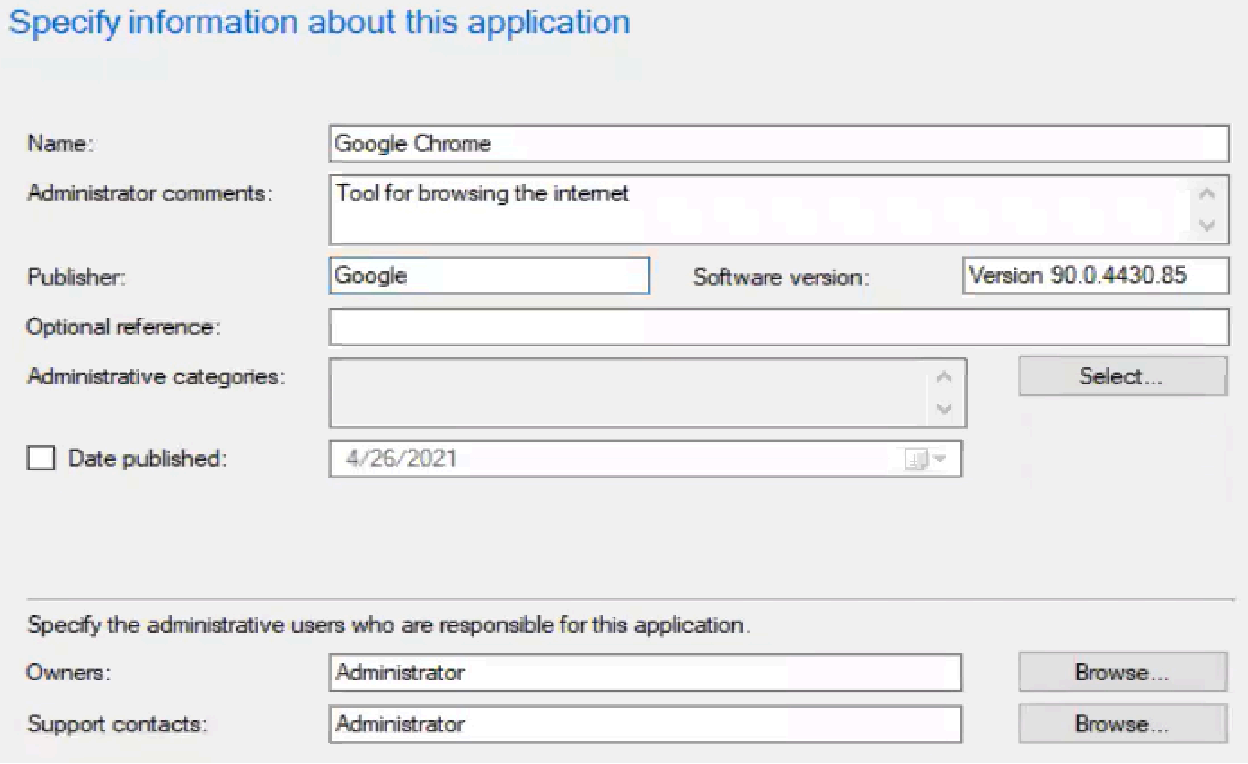
● Automatically detect information about this application from installation files:

Type: Windows Installer (*.msi file)

Location:

Example: \\Server\Share\File

○ Manually specify the application information



Specify information about this application

Name: Google Chrome

Administrator comments: Tool for browsing the internet

Publisher: Google

Software version: Version 90.0.4430.85

Optional reference:

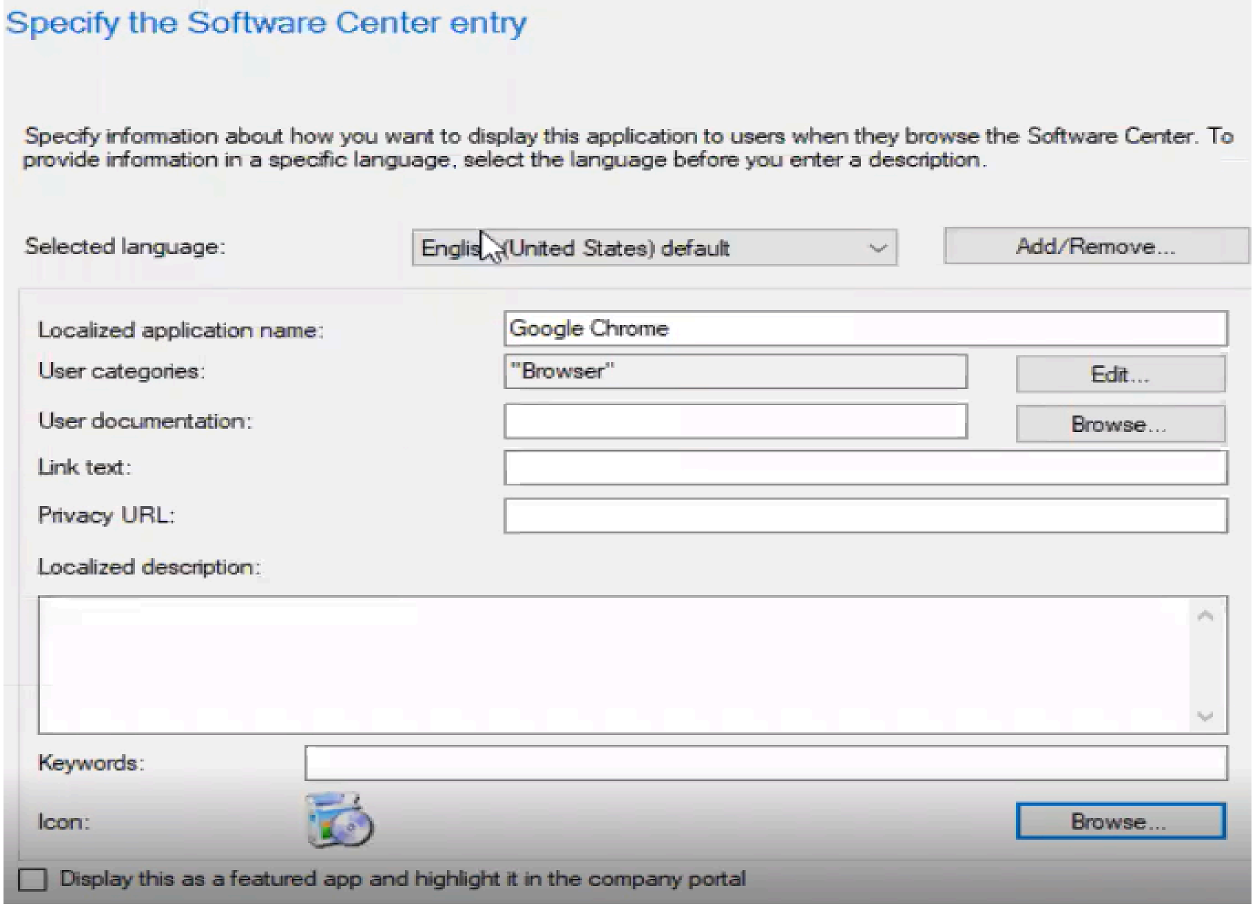
Administrative categories:

□ Date published: 4/26/2021

Specify the administrative users who are responsible for this application.

Owners: Administrator

Support contacts: Administrator



Specify the Software Center entry

Specify information about how you want to display this application to users when they browse the Software Center. To provide information in a specific language, select the language before you enter a description.

Selected language: English (United States) default

Localized application name: Google Chrome

User categories: "Browser"

User documentation:

Link text:

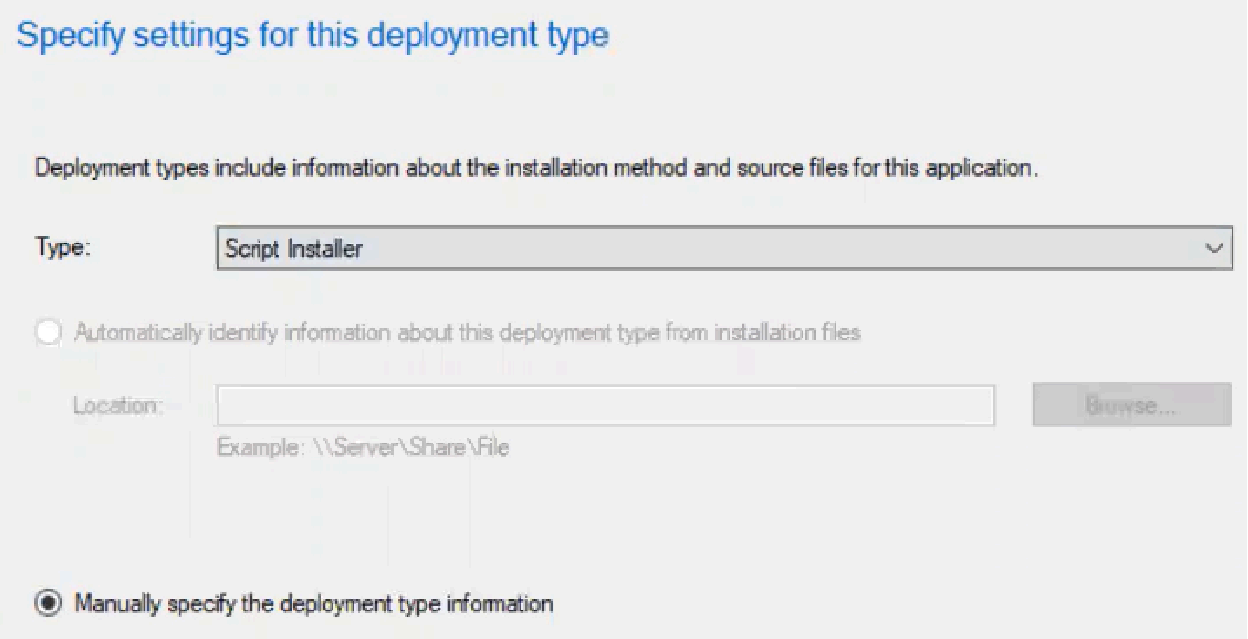
Privacy URL:

Localized description:

Keywords:

Icon:

□ Display this as a featured app and highlight it in the company portal



Specify settings for this deployment type

Deployment types include information about the installation method and source files for this application.

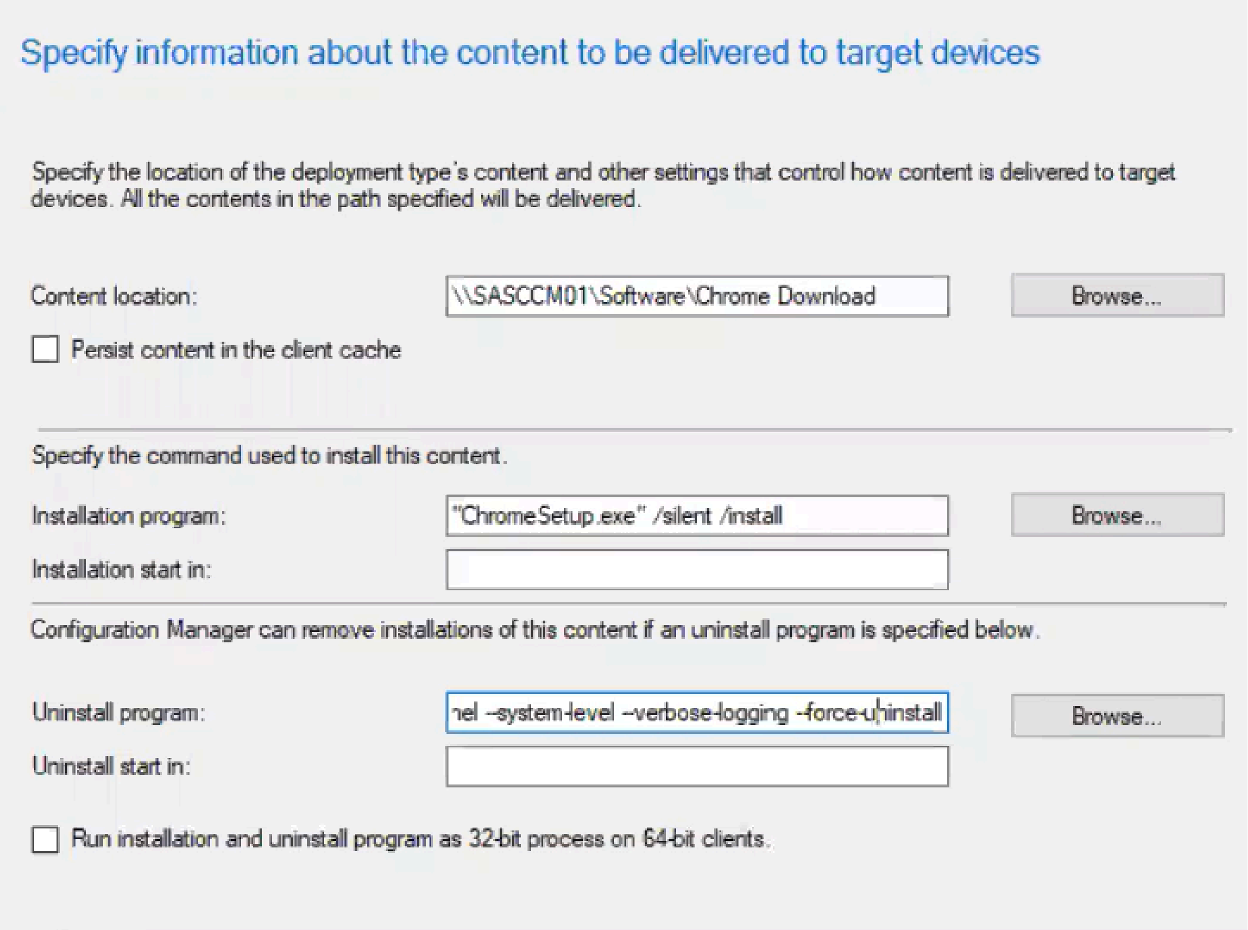
Type: Script Installer

○ Automatically identify information about this deployment type from installation files

Location:

Example: \\Server\Share\File

● Manually specify the deployment type information



Specify information about the content to be delivered to target devices

Specify the location of the deployment type's content and other settings that control how content is delivered to target devices. All the contents in the path specified will be delivered.

Content location: \\SASCCM01\Software\Chrome Download

□ Persist content in the client cache

Specify the command used to install this content.

Installation program: "ChromeSetup.exe" /silent /install

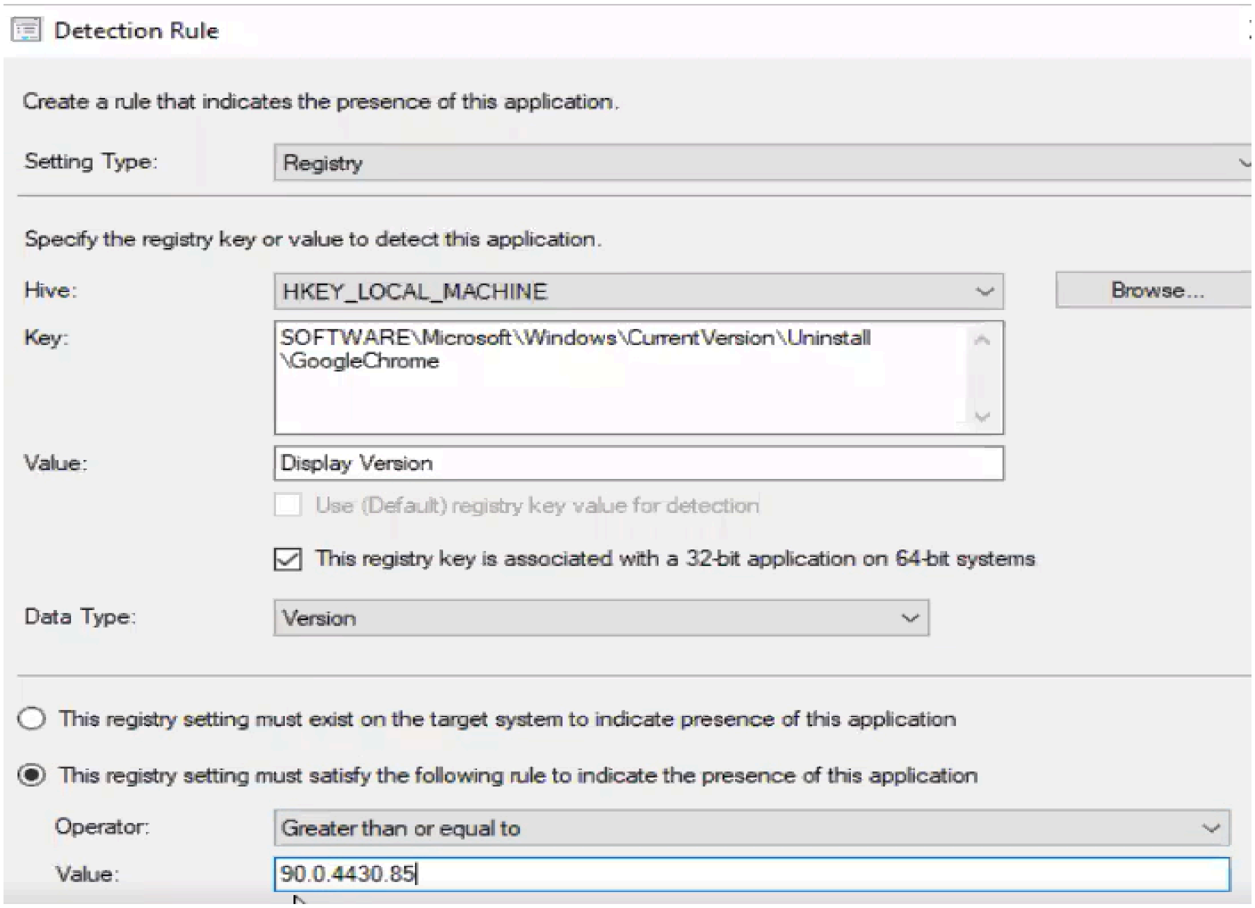
Installation start in:

Configuration Manager can remove installations of this content if an uninstall program is specified below.

Uninstall program: nel --system-level --verbose-logging --force-uninstall

Uninstall start in:

□ Run installation and uninstall program as 32-bit process on 64-bit clients.



Detection Rule

Create a rule that indicates the presence of this application.

Setting Type: Registry

Specify the registry key or value to detect this application.

Hive: HKEY_LOCAL_MACHINE

Key: SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
\GoogleChrome

Value: Display Version

□ Use (Default) registry key value for detection

☑ This registry key is associated with a 32-bit application on 64-bit systems

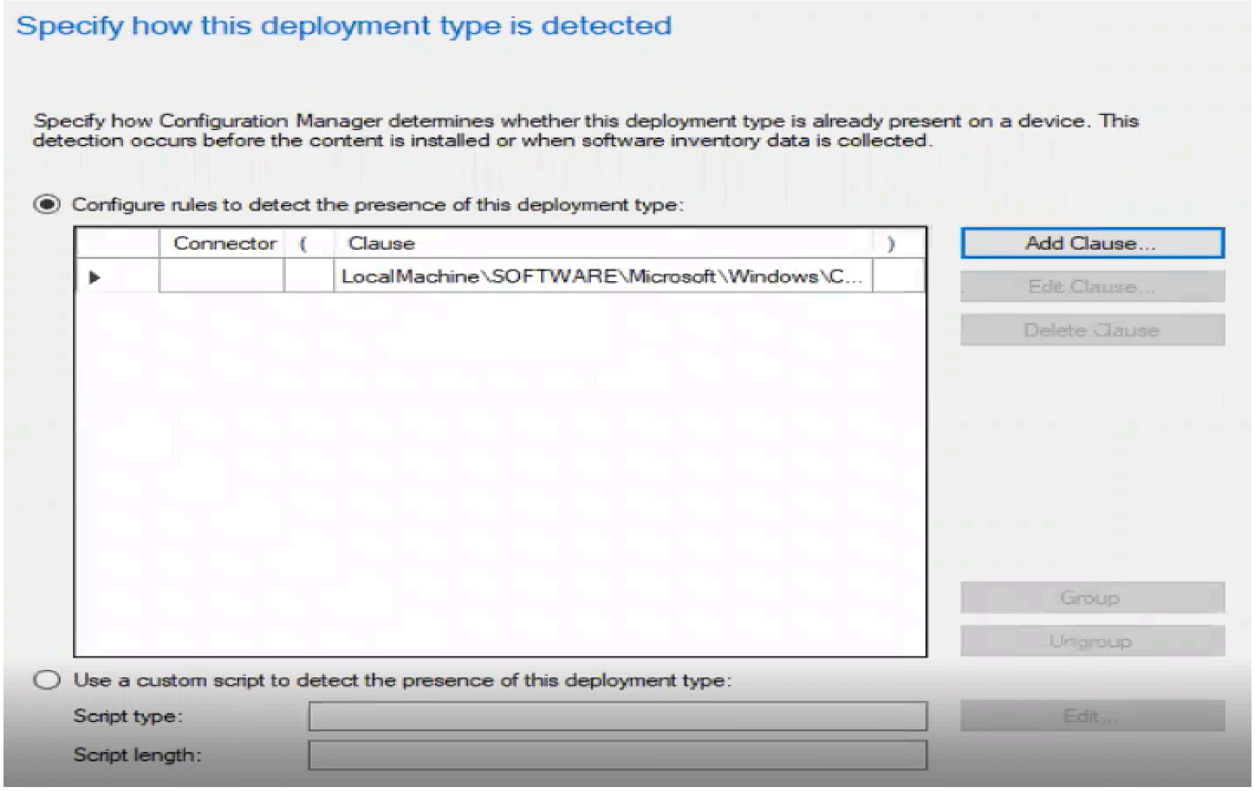
Data Type: Version

○ This registry setting must exist on the target system to indicate presence of this application

● This registry setting must satisfy the following rule to indicate the presence of this application

Operator: Greater than or equal to

Value: 90.0.4430.85



Specify how this deployment type is detected

Specify how Configuration Manager determines whether this deployment type is already present on a device. This detection occurs before the content is installed or when software inventory data is collected.

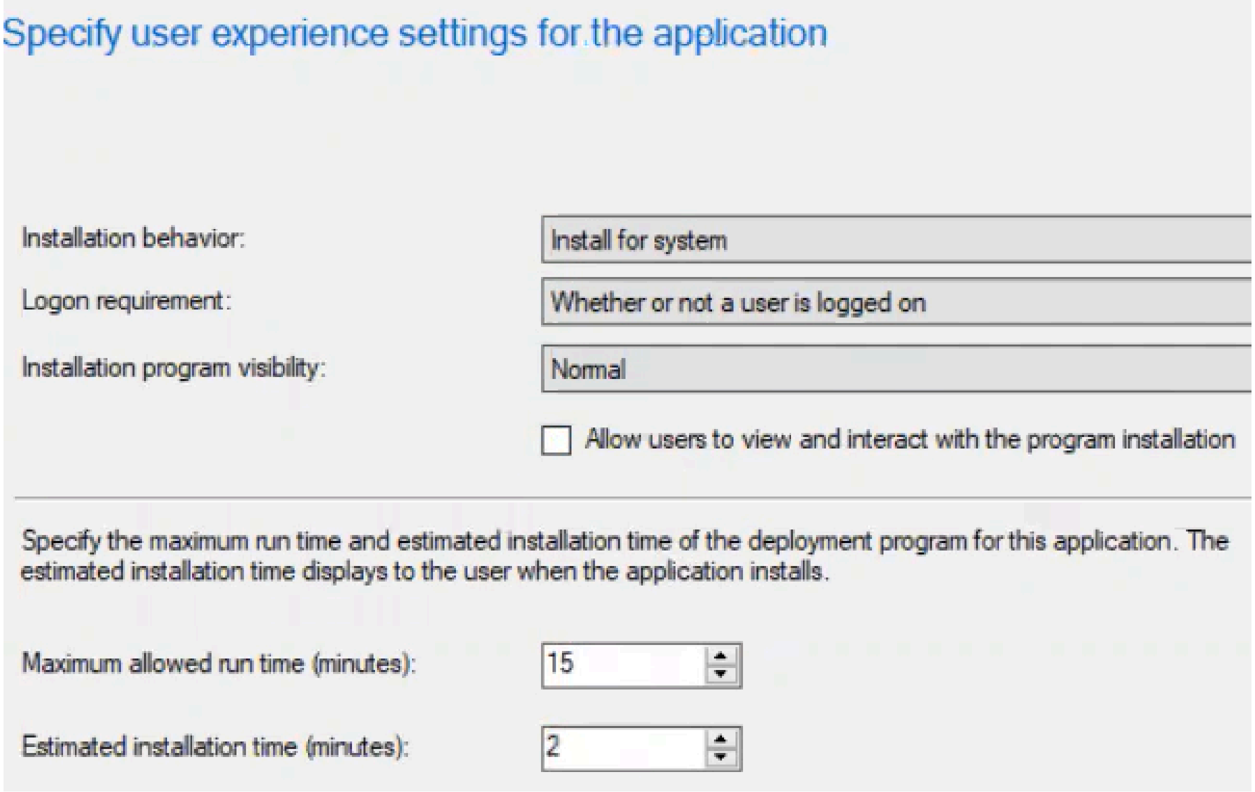
● Configure rules to detect the presence of this deployment type:

	Connector	(	Clause	)
▶			LocalMachine\SOFTWARE\Microsoft\Windows\C...	

○ Use a custom script to detect the presence of this deployment type:

Script type:

Script length:



Specify user experience settings for the application

Installation behavior: Install for system

Logon requirement: Whether or not a user is logged on

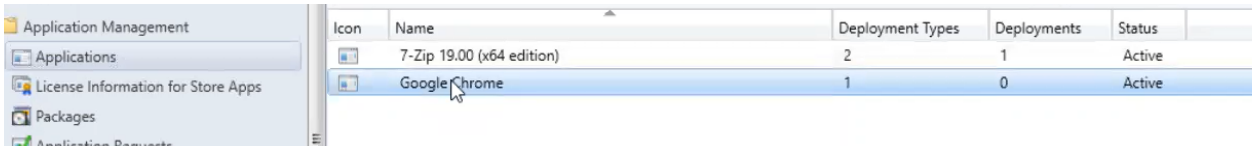
Installation program visibility: Normal

□ Allow users to view and interact with the program installation

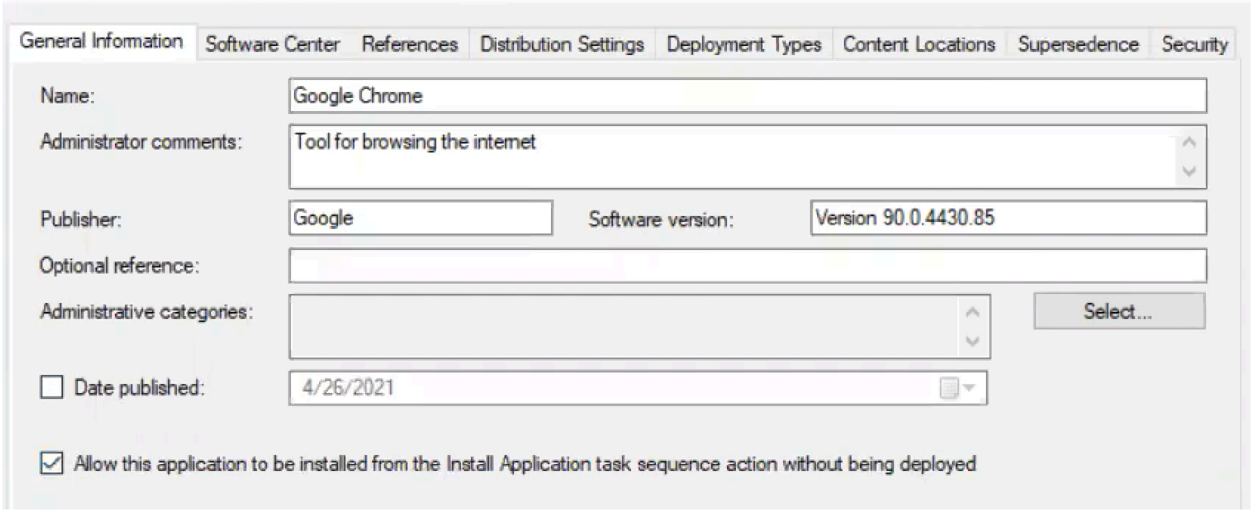
Specify the maximum run time and estimated installation time of the deployment program for this application. The estimated installation time displays to the user when the application installs.

Maximum allowed run time (minutes): 15

Estimated installation time (minutes): 2



Icon	Name	Deployment Types	Deployments	Status
	7-Zip 19.00 (x64 edition)	2	1	Active
	Google Chrome	1	0	Active



Name: Google Chrome

Administrator comments: Tool for browsing the internet

Publisher: Google

Software version: Version 90.0.4430.85

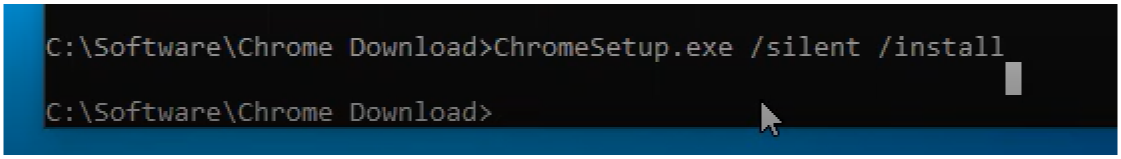
Optional reference:

Administrative categories:

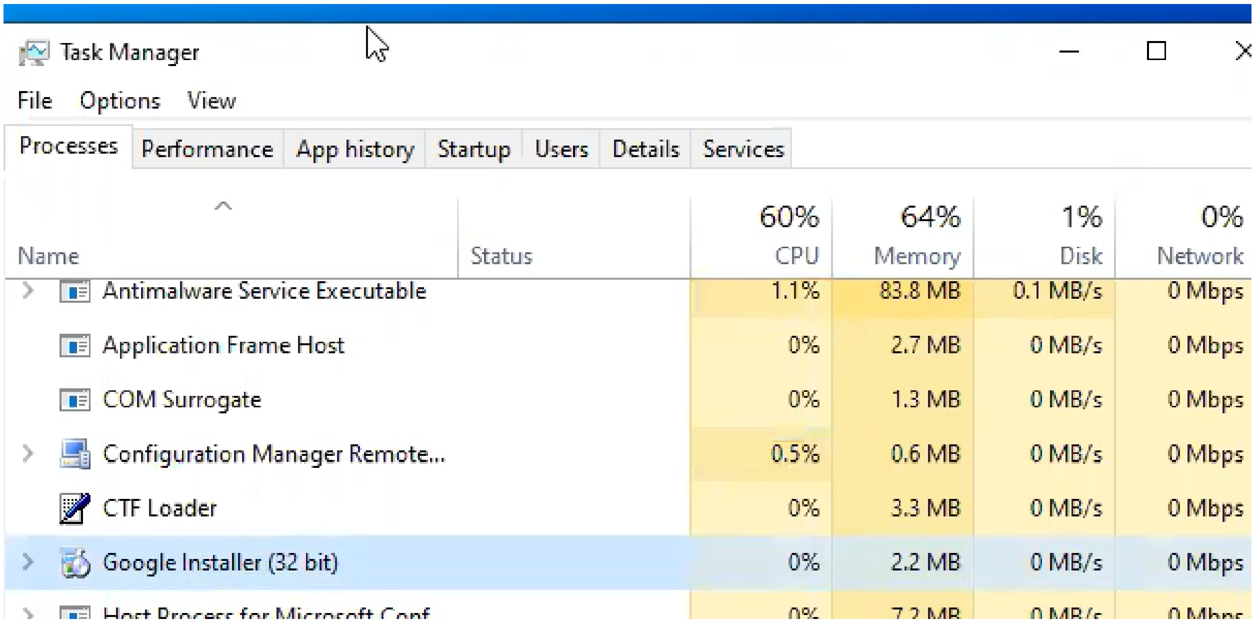
□ Date published: 4/26/2021

☑ Allow this application to be installed from the Install Application task sequence action without being deployed

Preparing Client for Chrome in Software Center



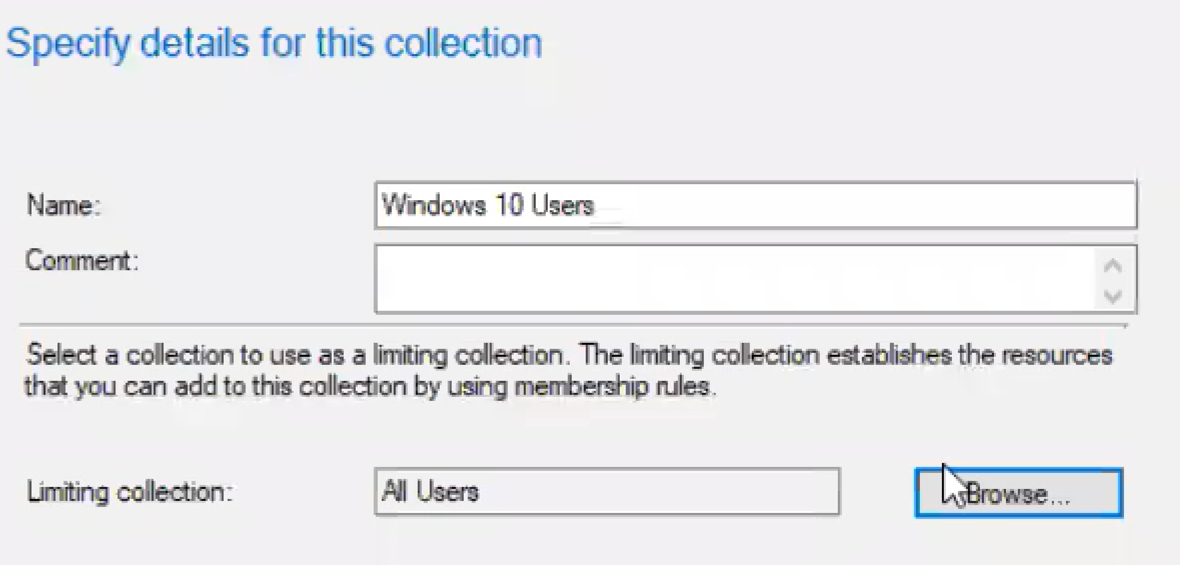
```
C:\Software\Chrome Download>ChromeSetup.exe /silent /install

C:\Software\Chrome Download>
```



Task Manager
File Options View
Processes Performance App history Startup Users Details Services

Name	Status	60% CPU	64% Memory	1% Disk	0% Network
Antimalware Service Executable		1.1%	83.8 MB	0.1 MB/s	0 Mbps
Application Frame Host		0%	2.7 MB	0 MB/s	0 Mbps
COM Surrogate		0%	1.3 MB	0 MB/s	0 Mbps
Configuration Manager Remote...		0.5%	0.6 MB	0 MB/s	0 Mbps
CTF Loader		0%	3.3 MB	0 MB/s	0 Mbps
Google Installer (32 bit)		0%	2.2 MB	0 MB/s	0 Mbps
Host Process for Microsoft Conf...		0%	7.2 MB	0 MB/s	0 Mbps

Creating a Windows 10 User Collection



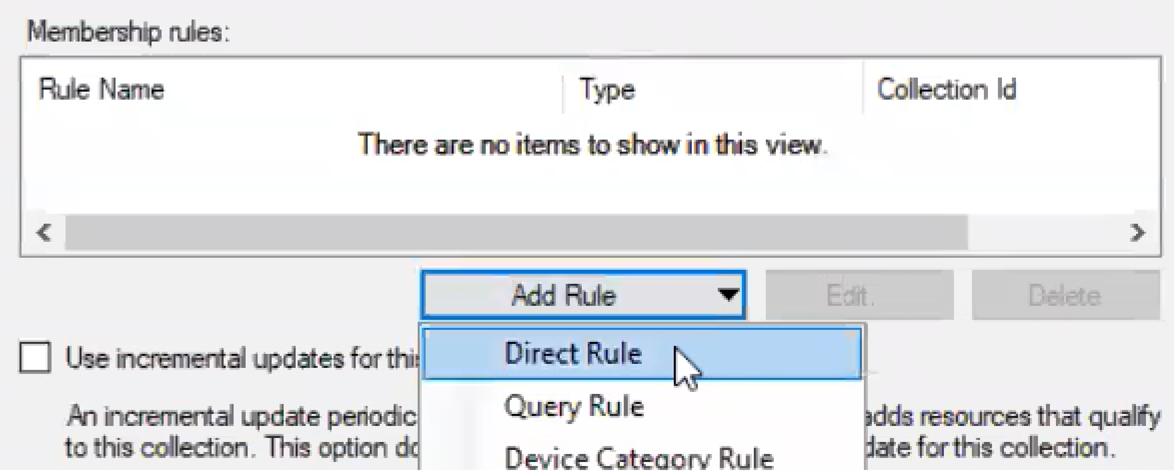
Specify details for this collection

Name: Windows 10 Users

Comment:

Select a collection to use as a limiting collection. The limiting collection establishes the resources that you can add to this collection by using membership rules.

Limiting collection: All Users

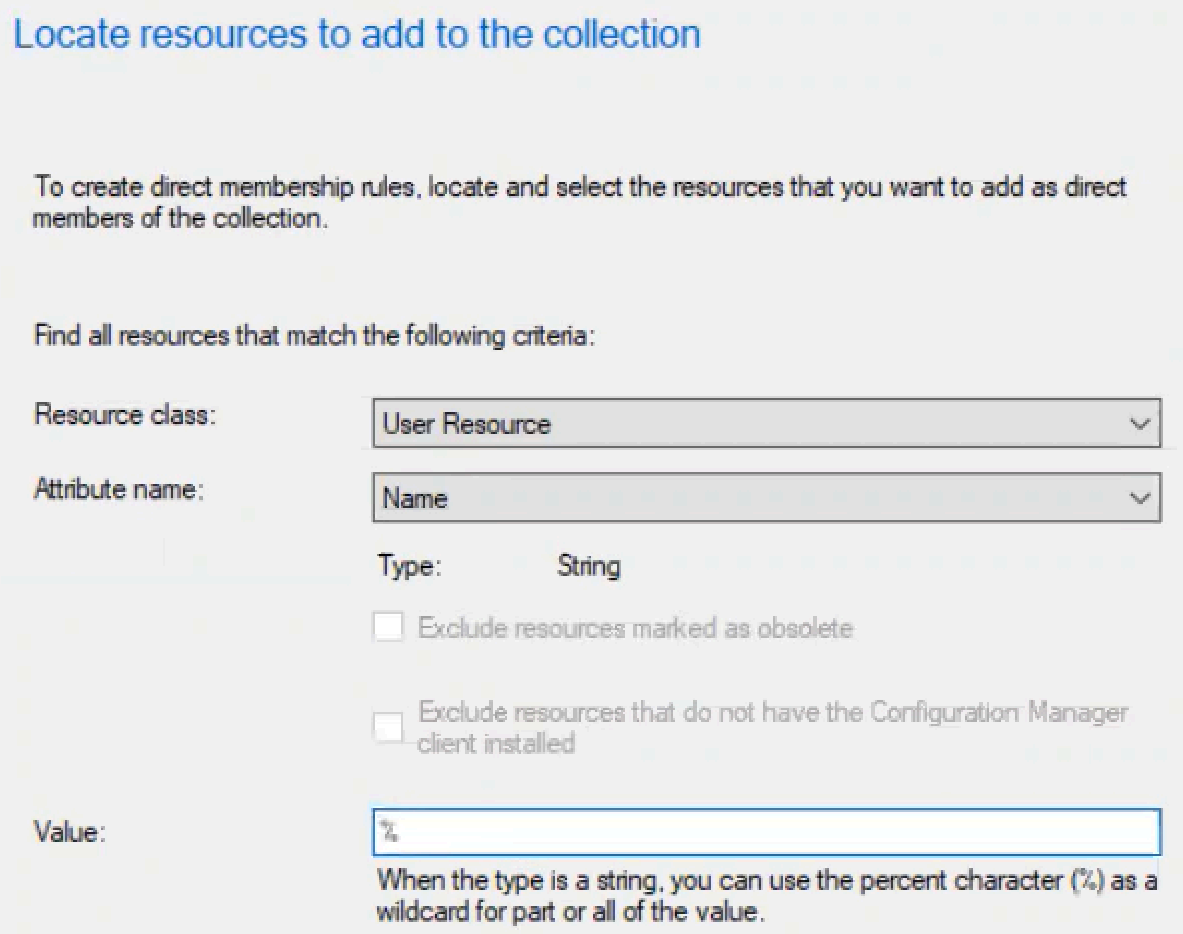


Membership rules:

Rule Name	Type	Collection Id
There are no items to show in this view.		

☐ Use incremental updates for thi

An incremental update periodic adds resources that qualify to this collection. This option do date for this collection.



Locate resources to add to the collection

To create direct membership rules, locate and select the resources that you want to add as direct members of the collection.

Find all resources that match the following criteria:

Resource class: User Resource

Attribute name: Name

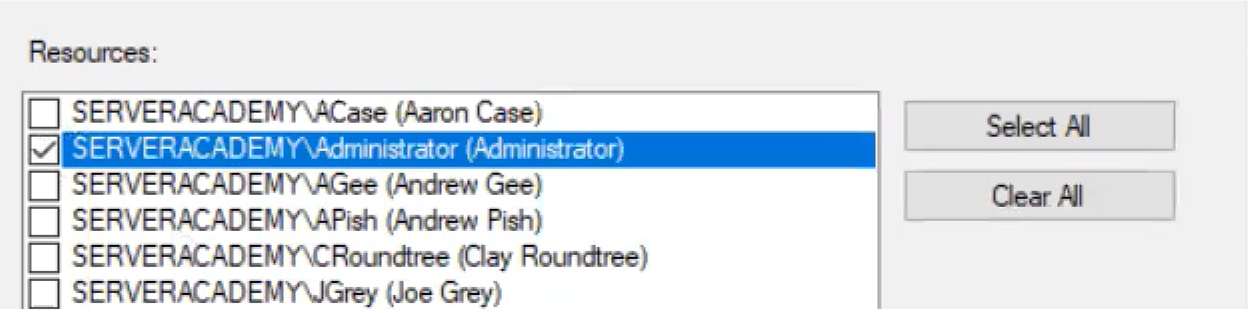
Type: String

☐ Exclude resources marked as obsolete

☐ Exclude resources that do not have the Configuration Manager client installed

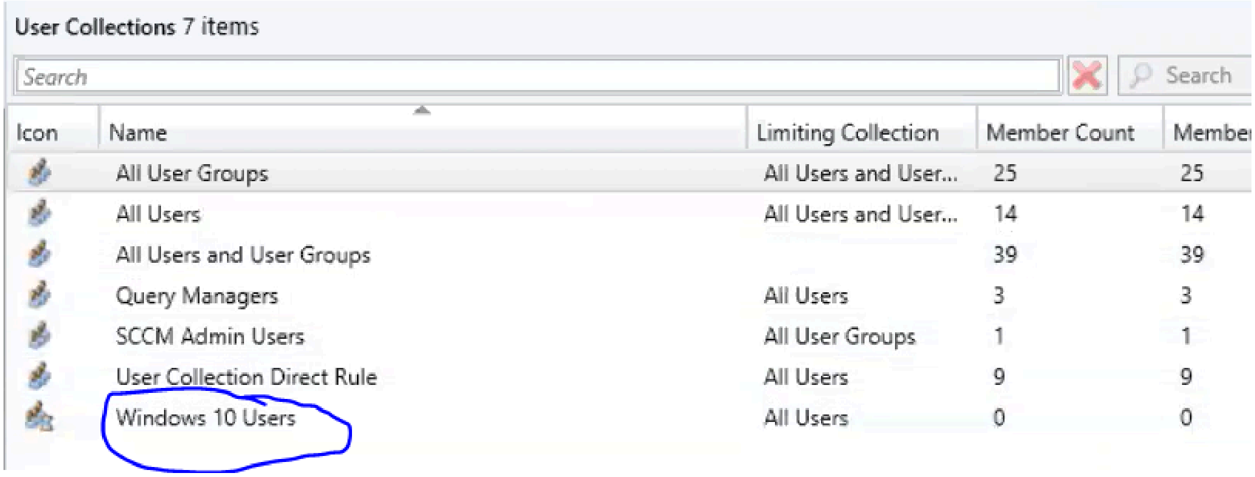
Value: %

When the type is a string, you can use the percent character (%) as a wildcard for part or all of the value.



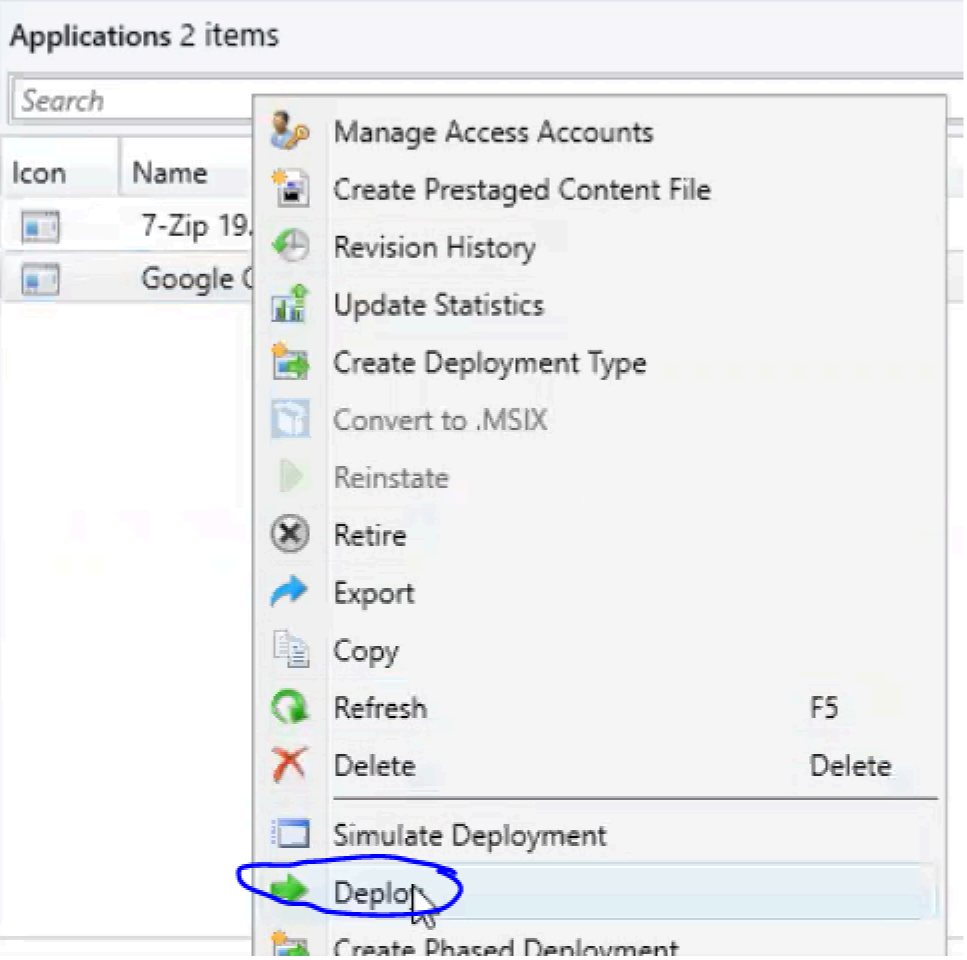
Resources:

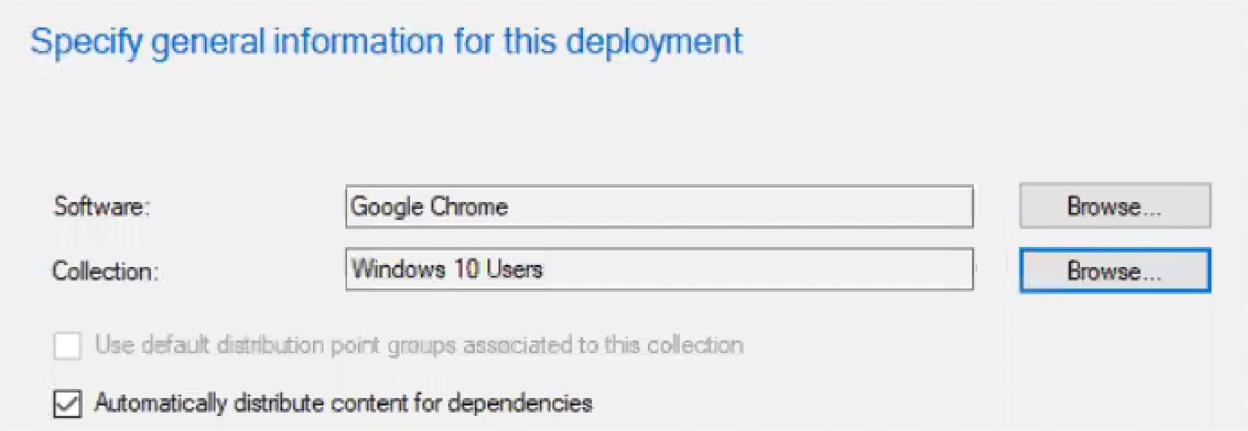
- □ SERVERACADEMY\ACase (Aaron Case)
- ☑ SERVERACADEMY\Administrator (Administrator)
- □ SERVERACADEMY\AGee (Andrew Gee)
- □ SERVERACADEMY\APish (Andrew Pish)
- □ SERVERACADEMY\CRoundtree (Clay Roundtree)
- □ SERVERACADEMY\JGrey (Joe Grey)



User Collections 7 items

Icon	Name	Limiting Collection	Member Count	Membe
	All User Groups	All Users and User...	25	25
	All Users	All Users and User...	14	14
	All Users and User Groups		39	39
	Query Managers	All Users	3	3
	SCCM Admin Users	All User Groups	1	1
	User Collection Direct Rule	All Users	9	9
	Windows 10 Users	All Users	0	0



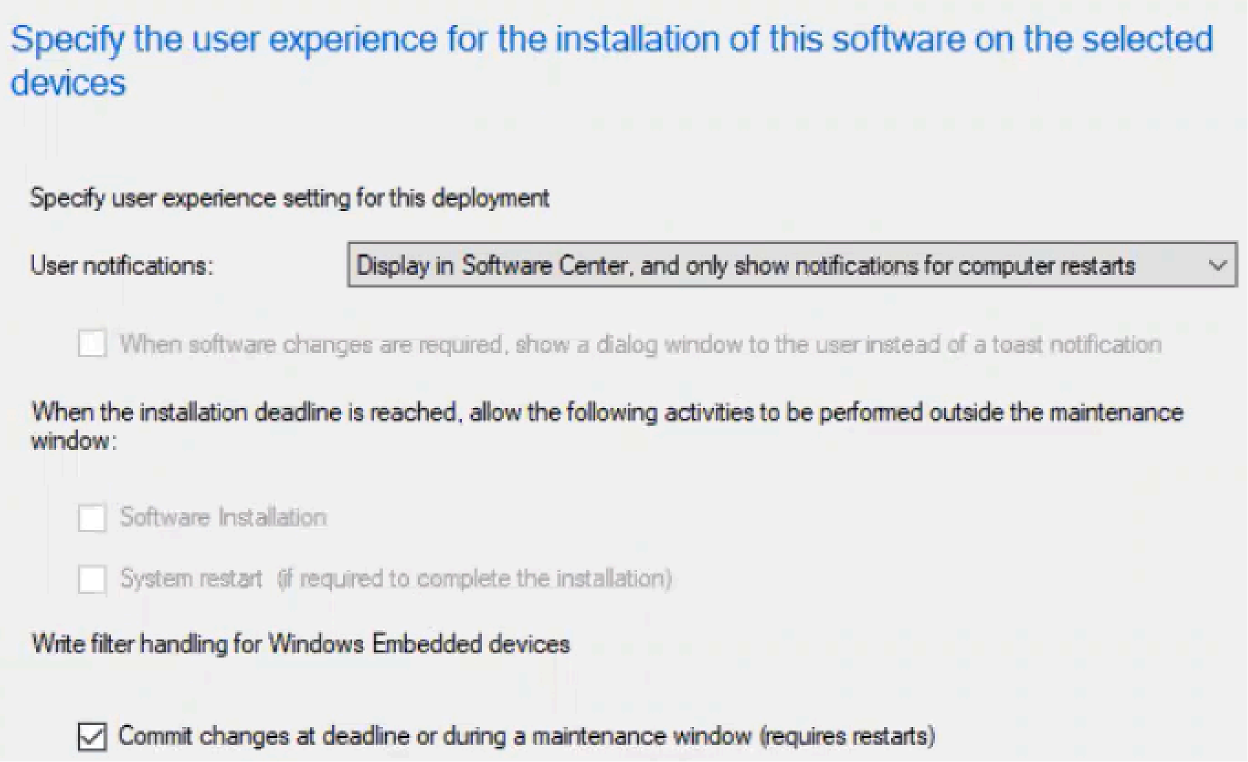

Specify general information for this deployment

Software: Google Chrome

Collection: Windows 10 Users

□ Use default distribution point groups associated to this collection

☑ Automatically distribute content for dependencies



Specify the user experience for the installation of this software on the selected devices

Specify user experience setting for this deployment

User notifications: Display in Software Center, and only show notifications for computer restarts

□ When software changes are required, show a dialog window to the user instead of a toast notification

When the installation deadline is reached, allow the following activities to be performed outside the maintenance window:

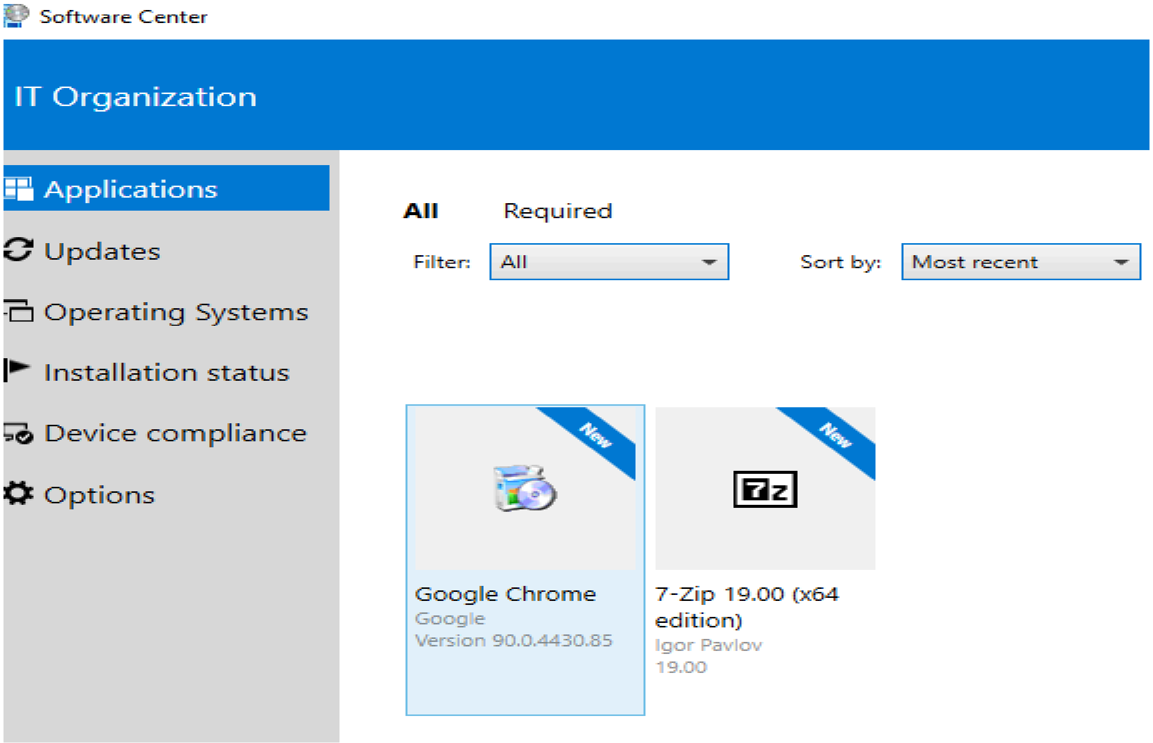
□ Software Installation

□ 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)

Chrome successfully added in Software Center



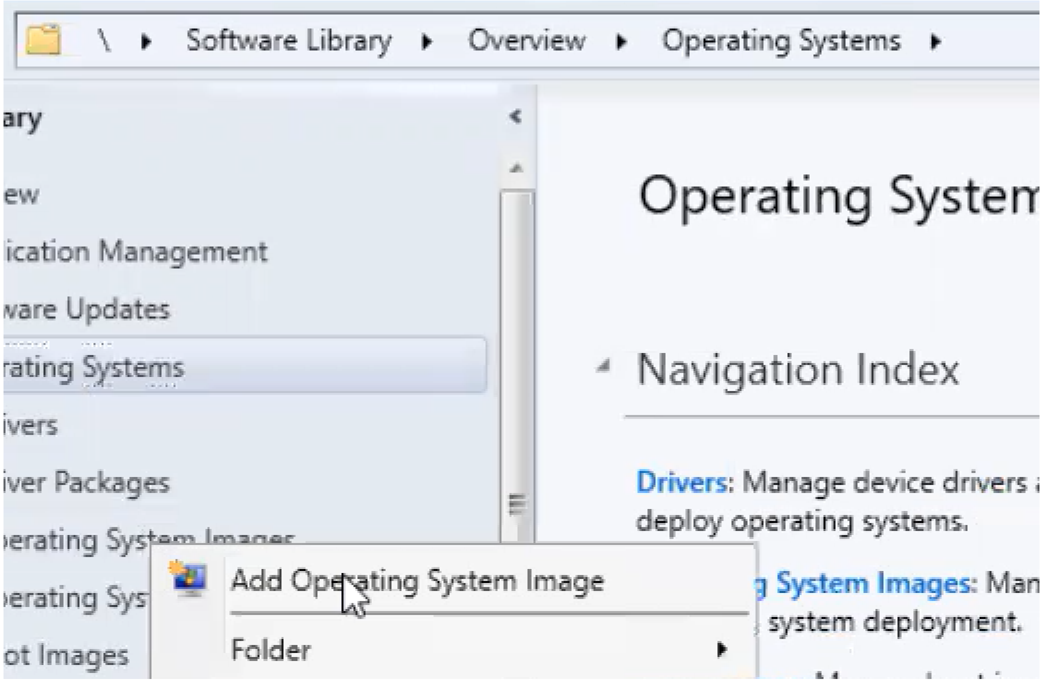
Filter: All

Sort by: Most recent

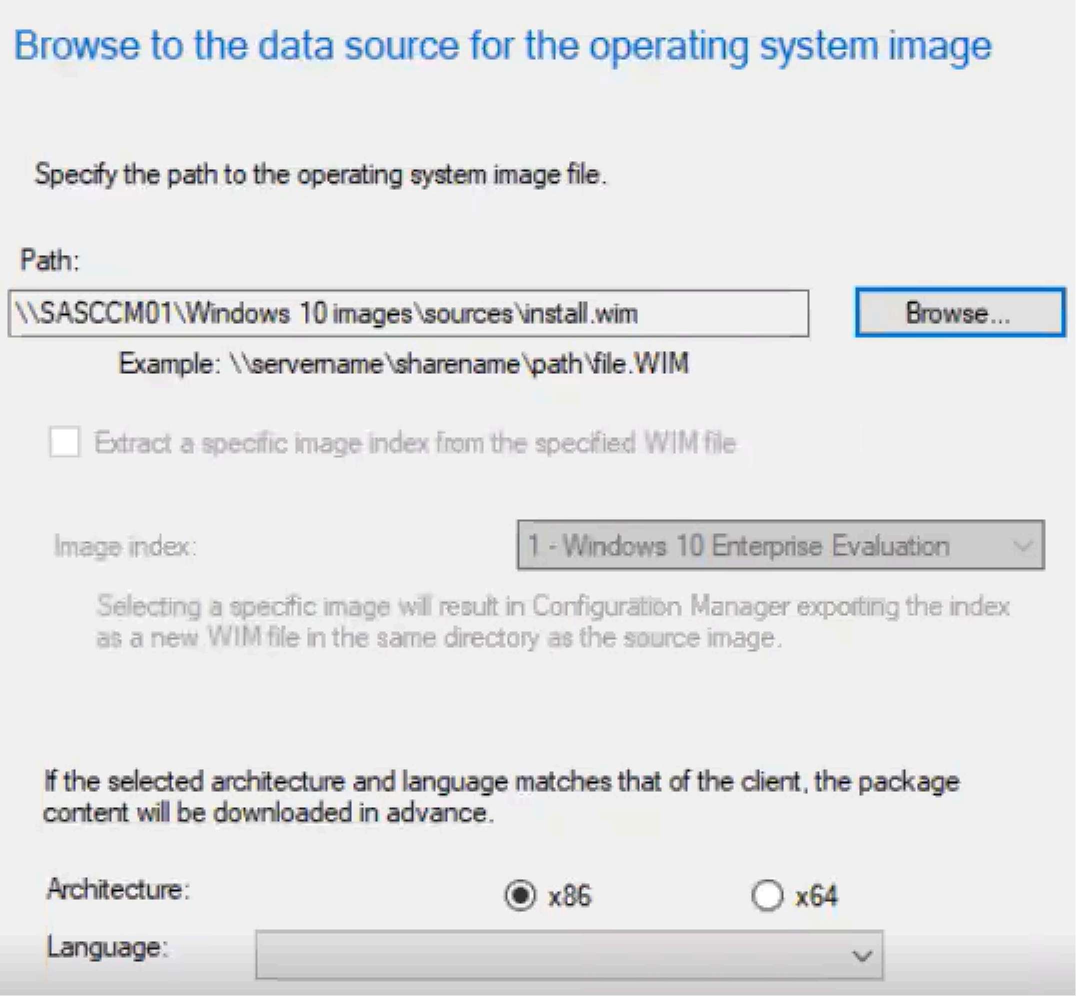
Google Chrome
Google
Version 90.0.4430.85

7-Zip 19.00 (x64 edition)
Igor Pavlov
19.00

Adding Windows 10 Deployable ISO to SCCM



Installed Windows ISO in the shared folder in Hypervisor to transfer ISO to a folder titled “Software” in SCCM server.



Browse to the data source for the operating system image

Specify the path to the operating system image file.

Path: \\SASCCM01\Windows 10 images\sources\install.wim

Example: \\servername\sharename\path\file.WIM

□ Extract a specific image index from the specified WIM file

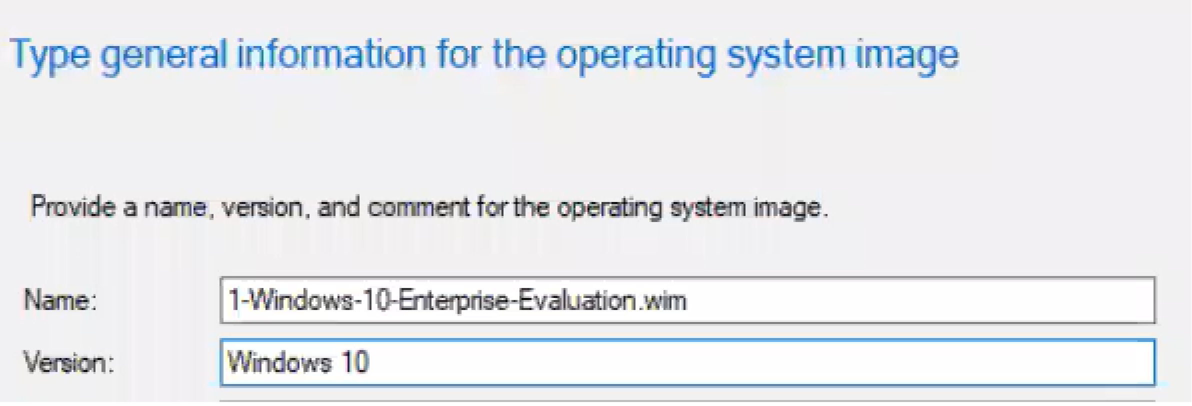
Image index: 1 - Windows 10 Enterprise Evaluation

Selecting a specific image will result in Configuration Manager exporting the index as a new WIM file in the same directory as the source image.

If the selected architecture and language matches that of the client, the package content will be downloaded in advance.

Architecture: ● x86 ○ x64

Language:

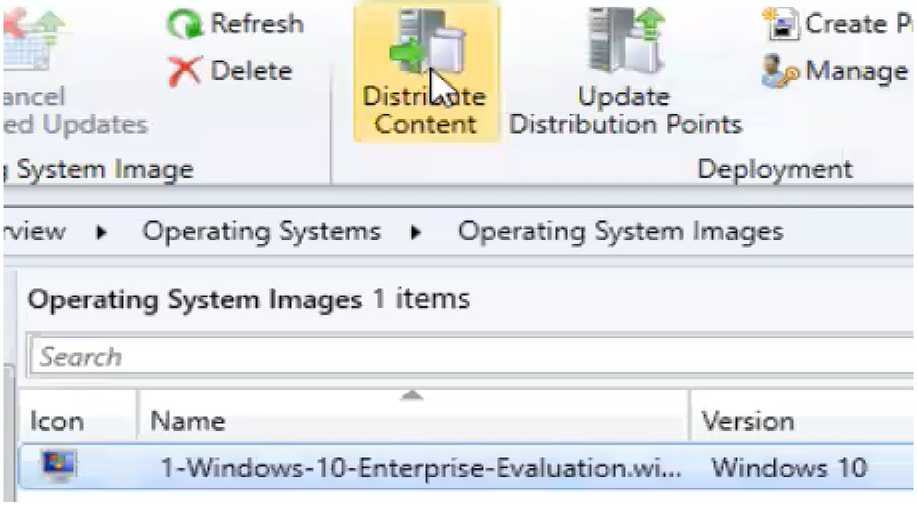


Type general information for the operating system image

Provide a name, version, and comment for the operating system image.

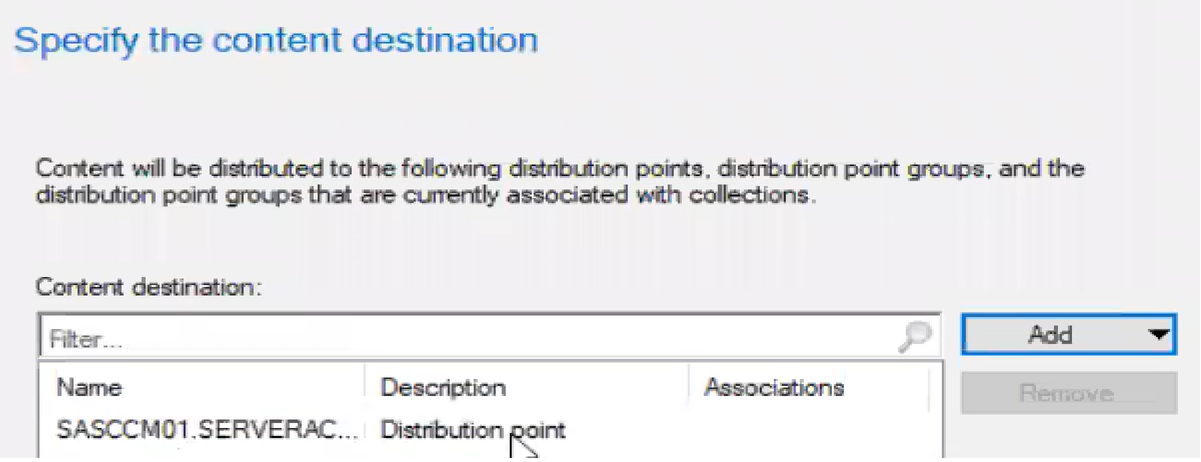
Name: 1-Windows-10-Enterprise-Evaluation.wim

Version: Windows 10



Operating System Images 1 items

Icon	Name	Version
	1-Windows-10-Enterprise-Evaluation.wi...	Windows 10

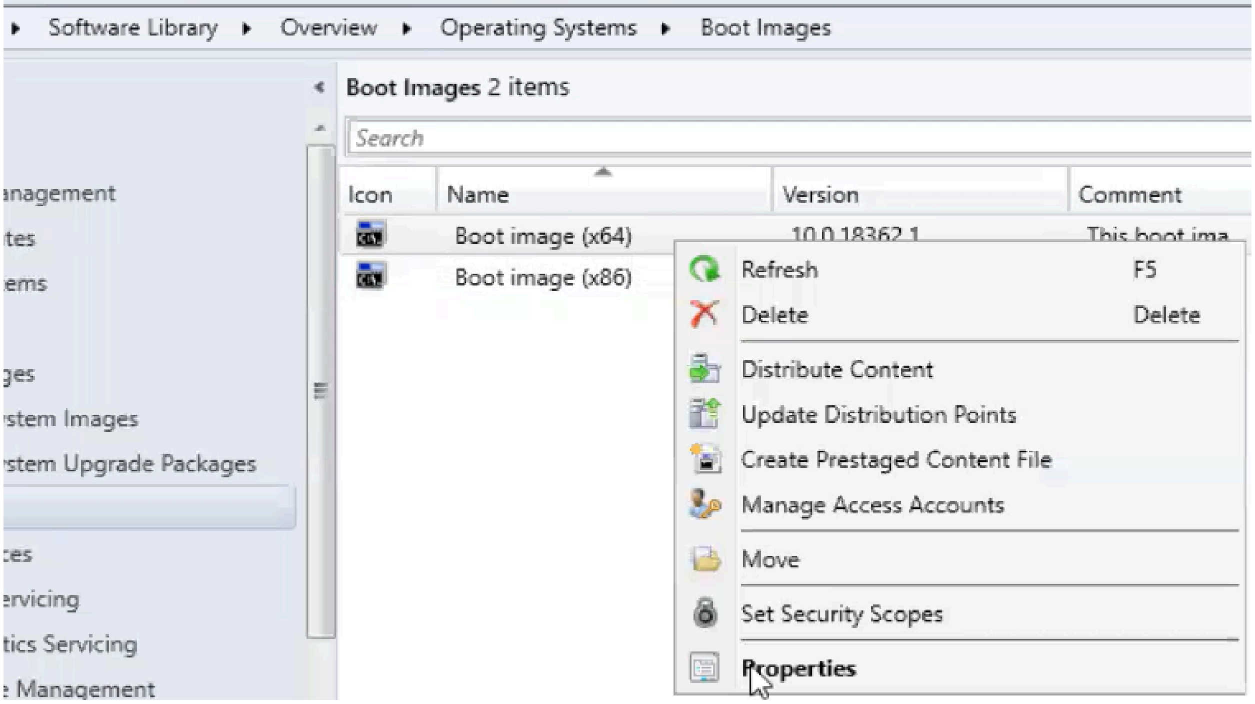


Specify the content destination

Content will be distributed to the following distribution points, distribution point groups, and the distribution point groups that are currently associated with collections.

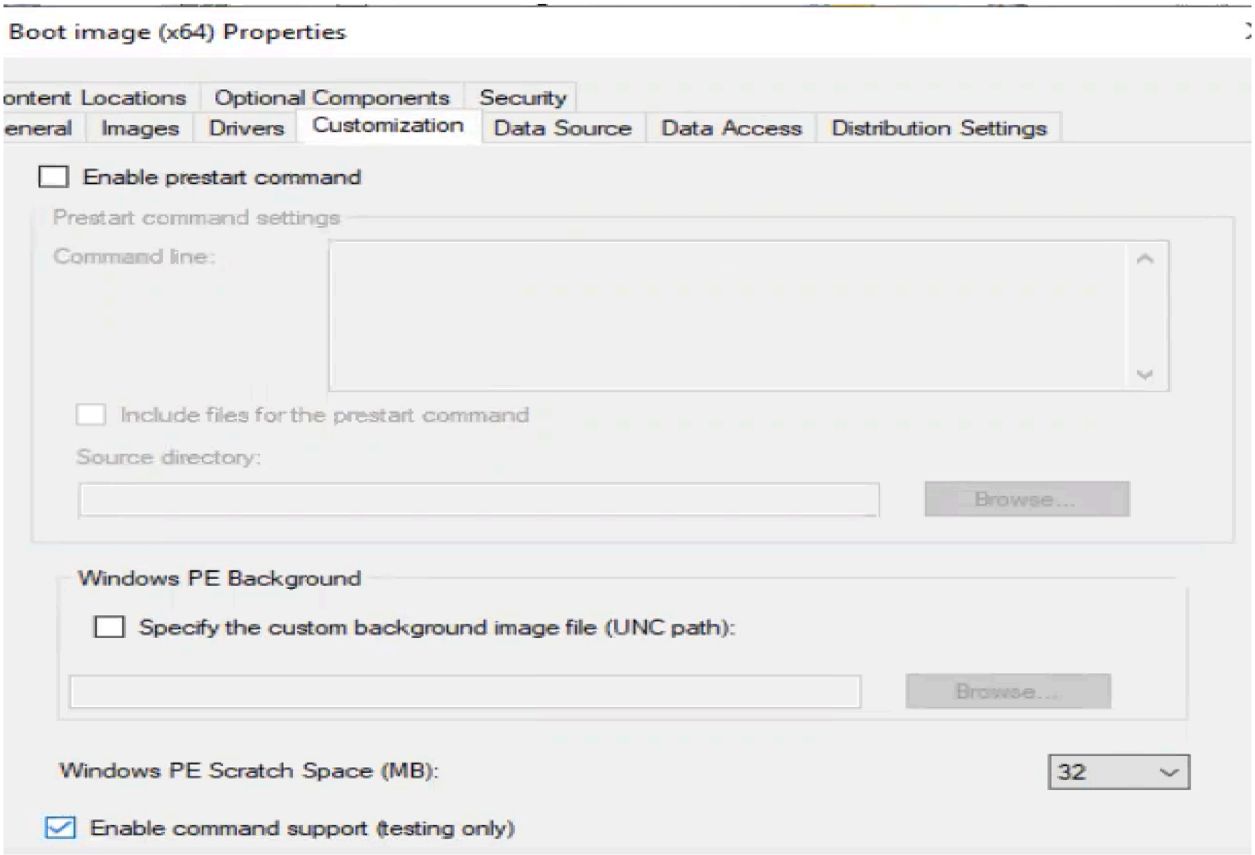
Content destination:

Name	Description	Associations
SASCCM01.SERVERAC...	Distribution point	



Boot Images 2 items

Icon	Name	Version	Comment
	Boot image (x64)	10.0.18362.1	This boot ima...
	Boot image (x86)		



☐ Enable prestart command

Prestart command settings

Command line:

☐ Include files for the prestart command

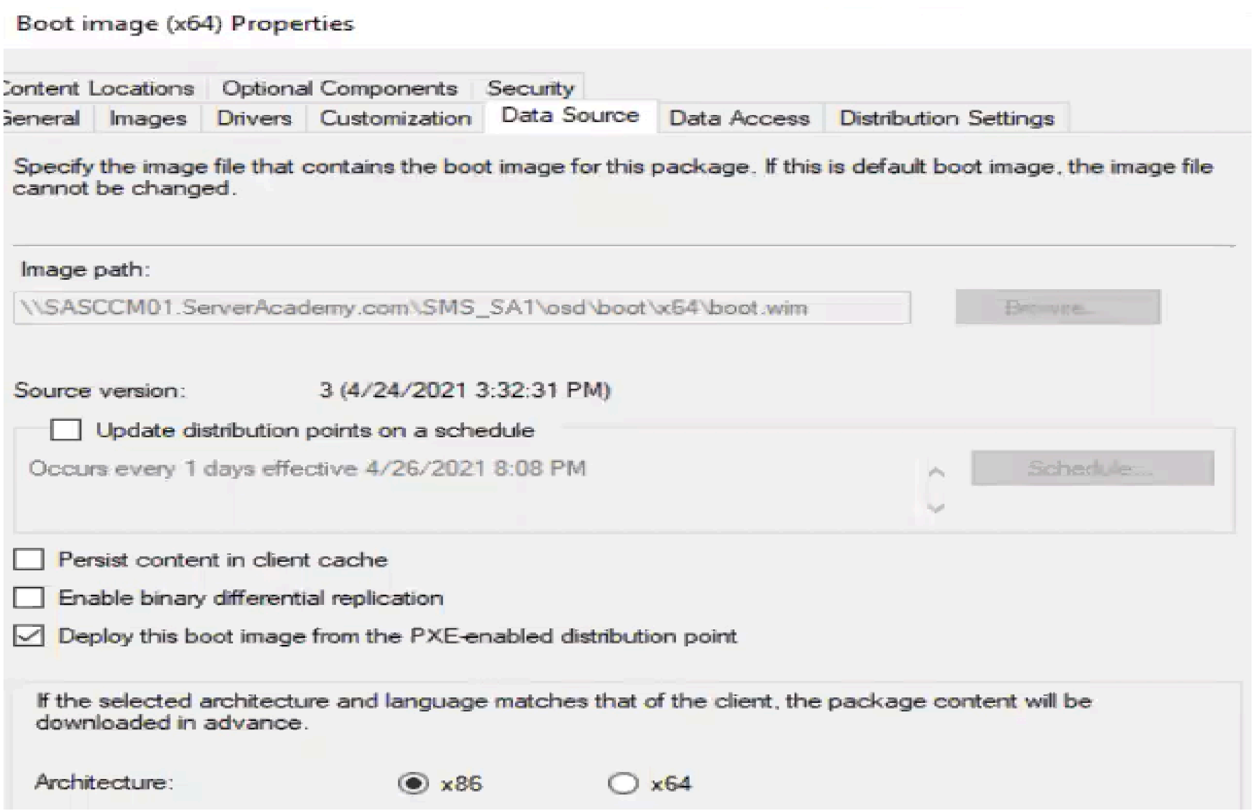
Source directory:

Windows PE Background

☐ Specify the custom background image file (UNC path):

Windows PE Scratch Space (MB): 32

☑ Enable command support (testing only)



Specify the image file that contains the boot image for this package. If this is default boot image, the image file cannot be changed.

Image path: \\SASCCM01.ServerAcademy.com\SMS_SA1\osd\boot\x64\boot.wim

Source version: 3 (4/24/2021 3:32:31 PM)

☐ Update distribution points on a schedule

Occurs every 1 days effective 4/26/2021 8:08 PM

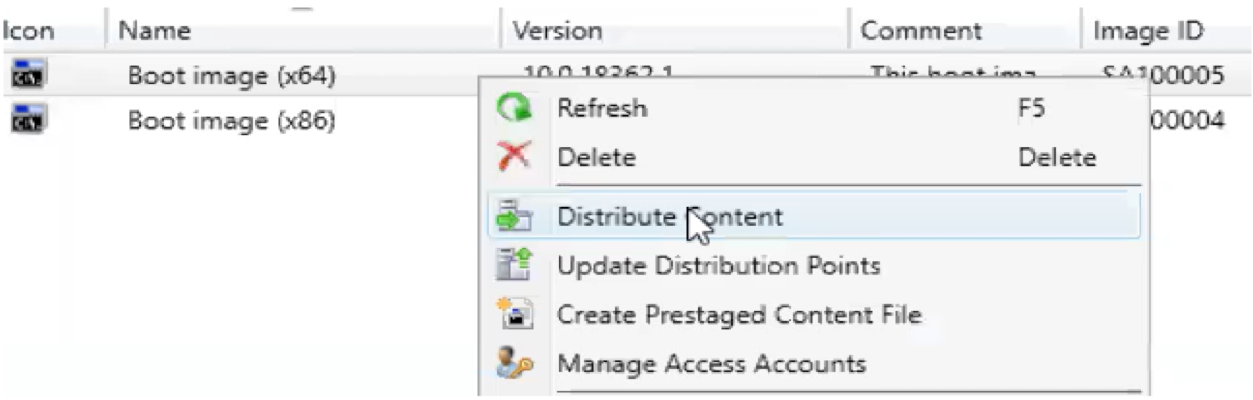
☐ Persist content in client cache

☐ Enable binary differential replication

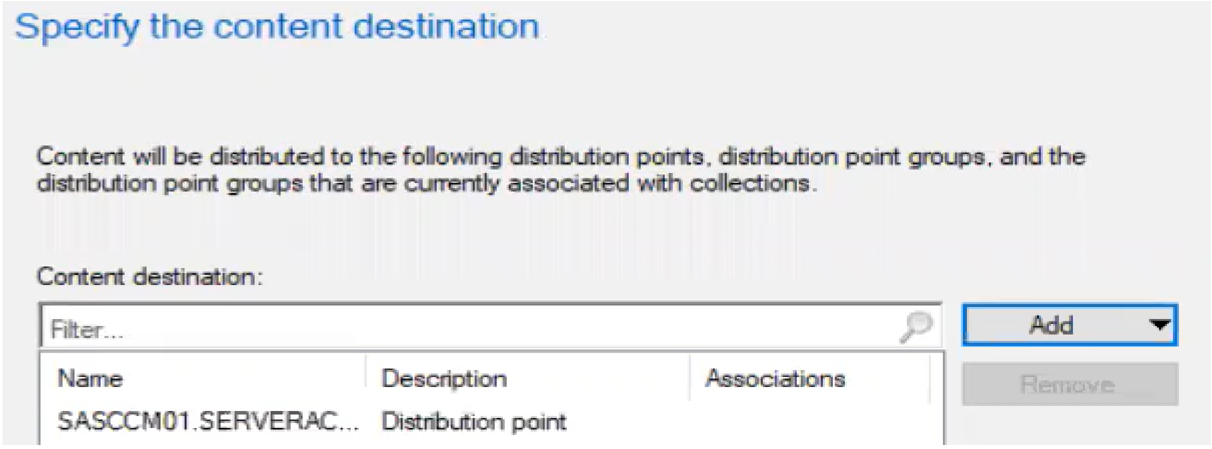
☑ Deploy this boot image from the PXE-enabled distribution point

If the selected architecture and language matches that of the client, the package content will be downloaded in advance.

Architecture: ● x86 ○ x64



Icon	Name	Version	Comment	Image ID
	Boot image (x64)	10.0.18362.1	This boot ima	SA100005
	Boot image (x86)			00004

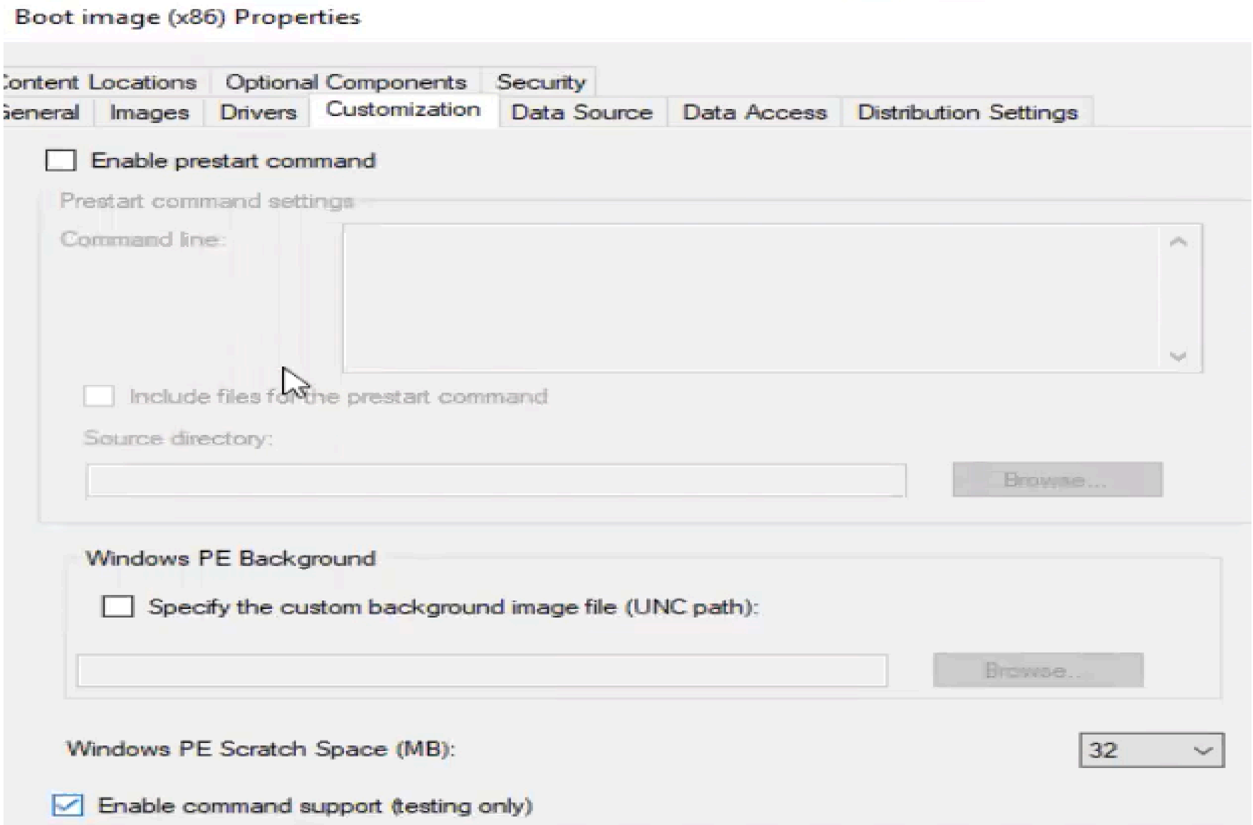


Specify the content destination

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:

Name	Description	Associations
SASCCM01.SERVERAC...	Distribution point	



Boot image (x86) Properties

□ Enable prestart command

Prestart command settings

Command line:

□ Include files for the prestart command

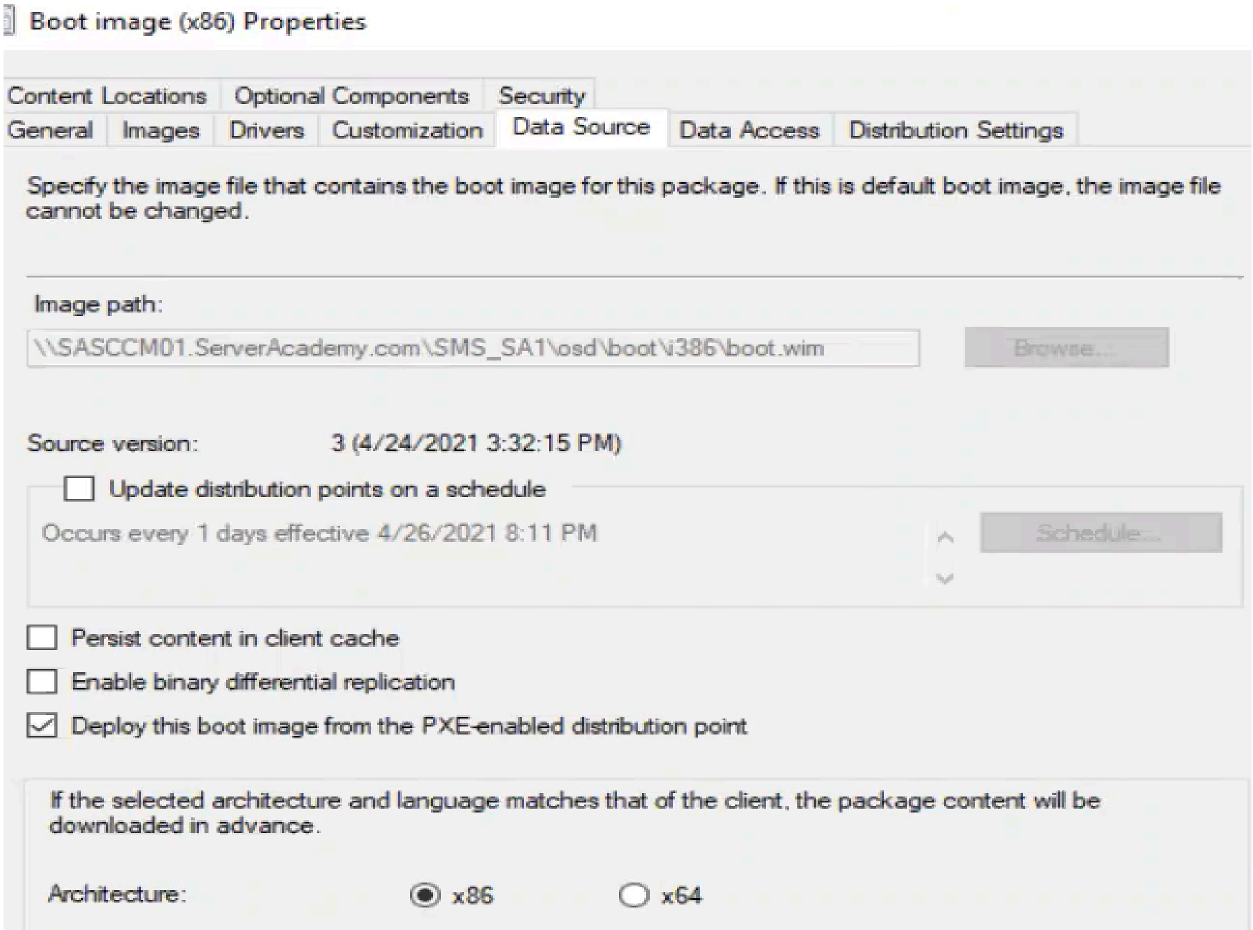
Source directory:

Windows PE Background

□ Specify the custom background image file (UNC path):

Windows PE Scratch Space (MB): 32

☑ Enable command support (testing only)



Boot image (x86) Properties

Specify the image file that contains the boot image for this package. If this is default boot image, the image file cannot be changed.

Image path: \\SASCCM01.ServerAcademy.com\SMS_SA1\osd\boot\i386\boot.wim

Source version: 3 (4/24/2021 3:32:15 PM)

□ Update distribution points on a schedule

Occurs every 1 days effective 4/26/2021 8:11 PM

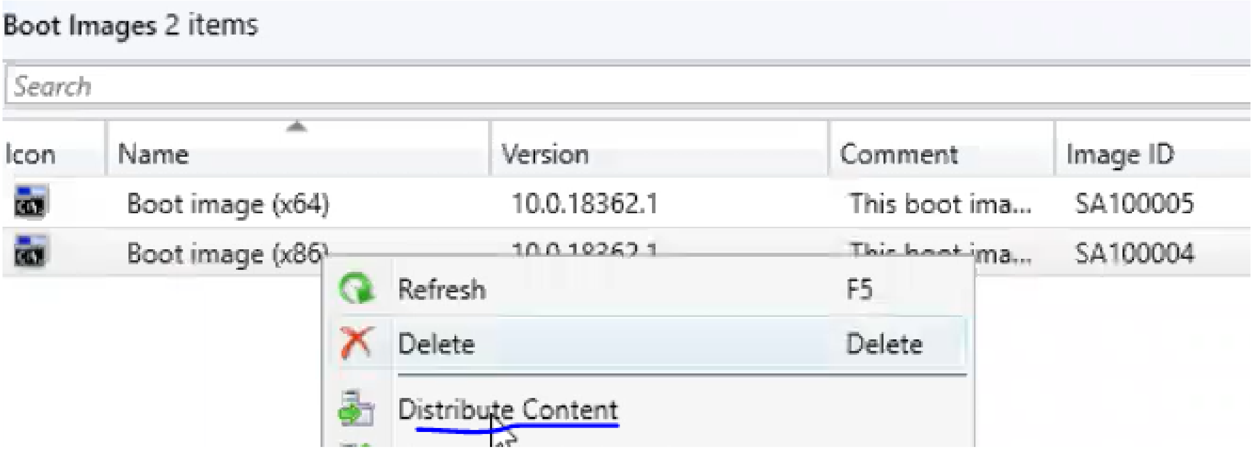
□ Persist content in client cache

□ Enable binary differential replication

☑ Deploy this boot image from the PXE-enabled distribution point

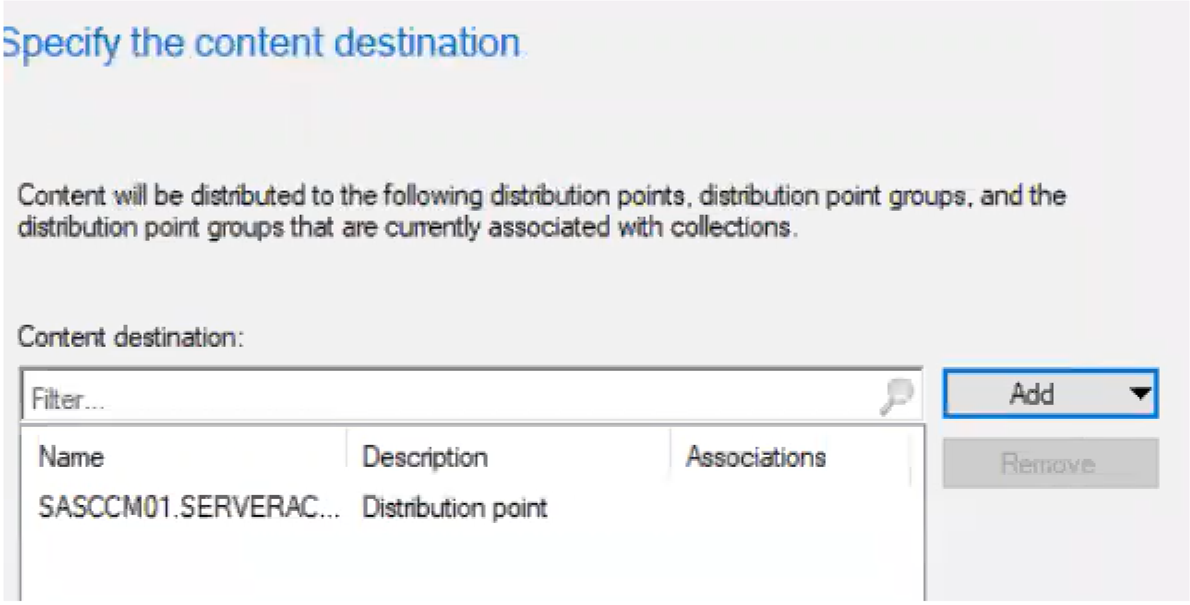
If the selected architecture and language matches that of the client, the package content will be downloaded in advance.

Architecture: ● x86 ○ x64



Boot Images 2 items

Icon	Name	Version	Comment	Image ID
	Boot image (x64)	10.0.18362.1	This boot ima...	SA100005
	Boot image (x86)	10.0.18362.1	This boot ima...	SA100004

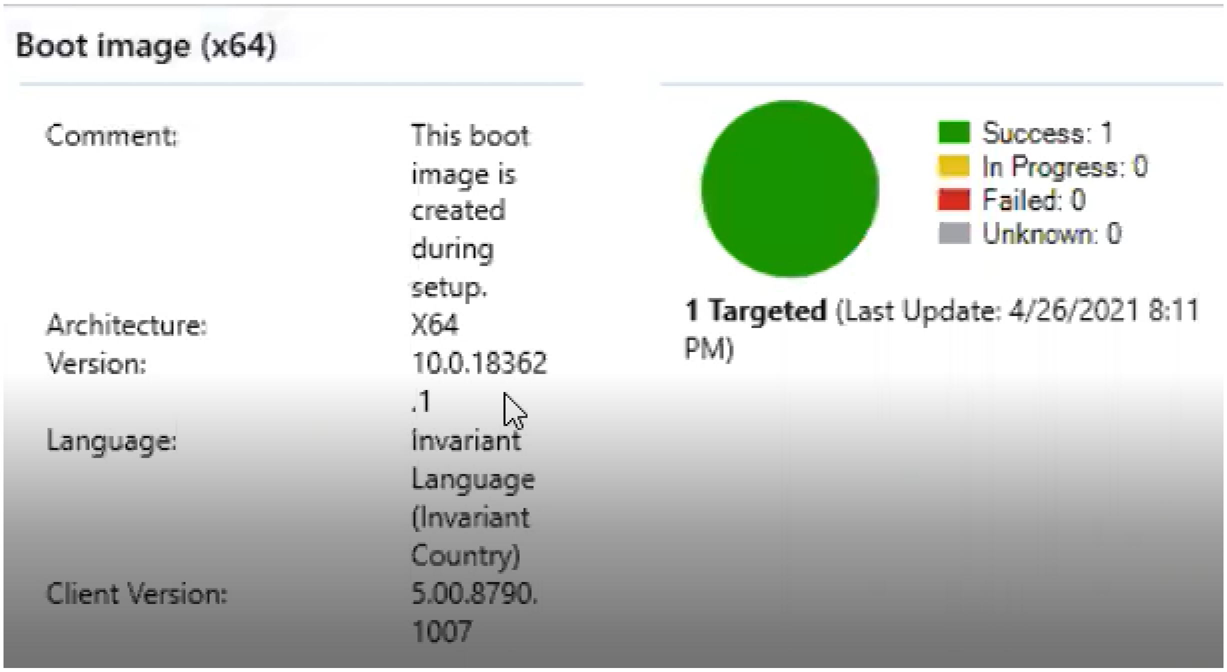


Specify the content destination

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:

Name	Description	Associations
SASCCM01.SERVERAC...	Distribution point	

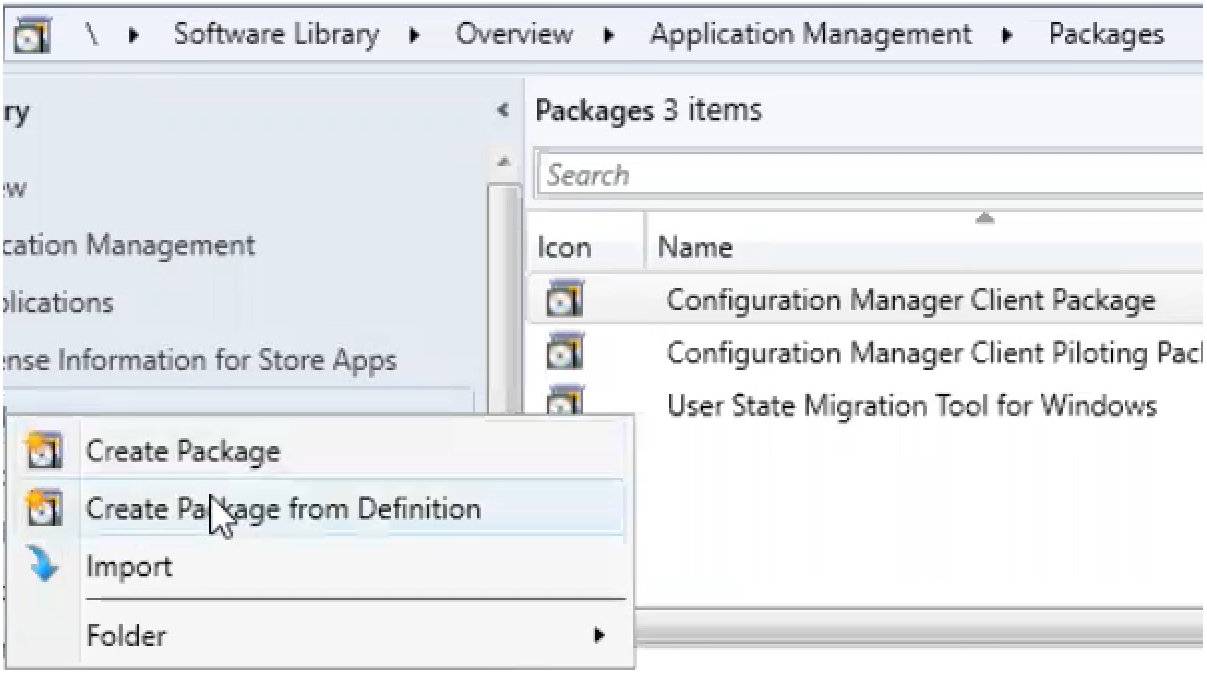


Boot image (x64)

Comment:	This boot image is created during setup.
Architecture:	X64
Version:	10.0.18362.1
Language:	Invariant Language (Invariant Country)
Client Version:	5.00.8790.1007

🟩 Success: 1
🟨 In Progress: 0
🟥 Failed: 0
▨ Unknown: 0

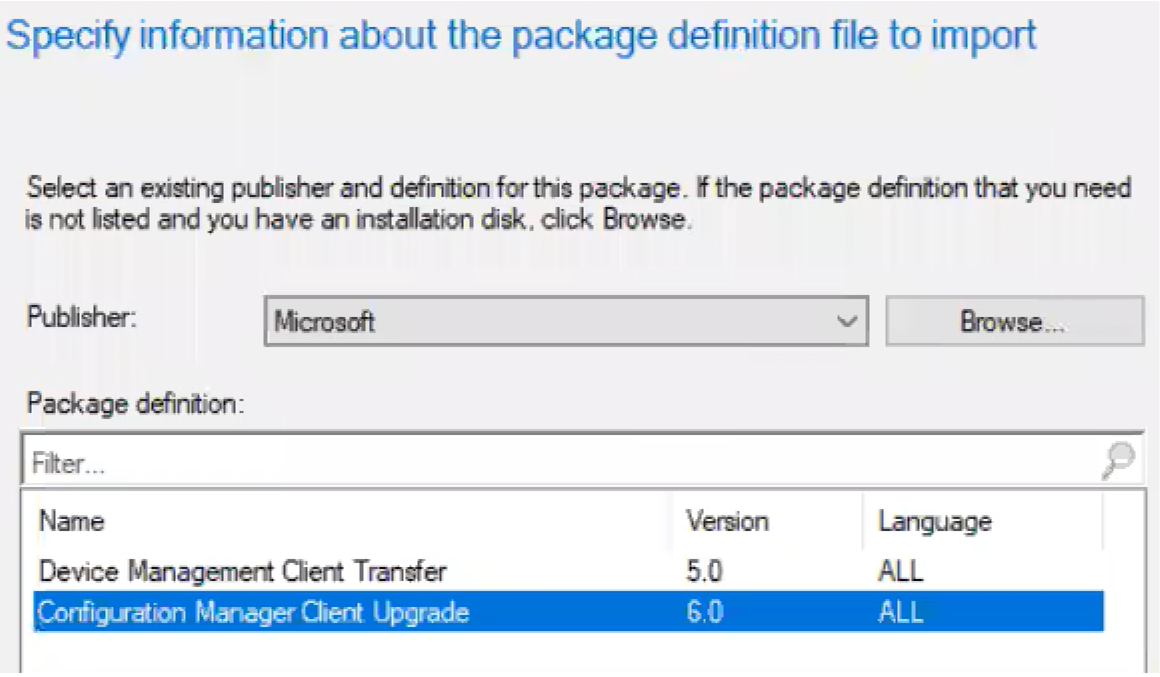
1 Targeted (Last Update: 4/26/2021 8:11 PM)



\ ▸ Software Library ▸ Overview ▸ Application Management ▸ Packages

Packages 3 items

Icon	Name
	Configuration Manager Client Package
	Configuration Manager Client Piloting Pacl
	User State Migration Tool for Windows



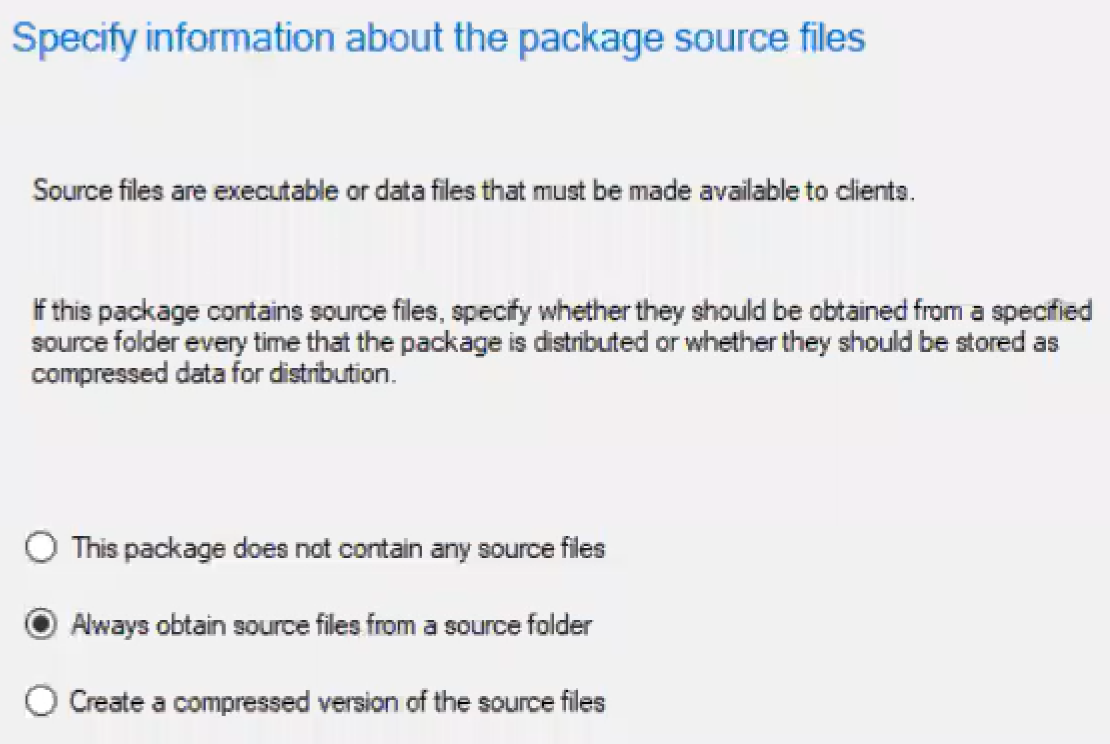
Specify information about the package definition file to import

Select an existing publisher and definition for this package. If the package definition that you need is not listed and you have an installation disk, click Browse.

Publisher: Microsoft

Package definition:

Name	Version	Language
Device Management Client Transfer	5.0	ALL
Configuration Manager Client Upgrade	6.0	ALL



Specify information about the package source files

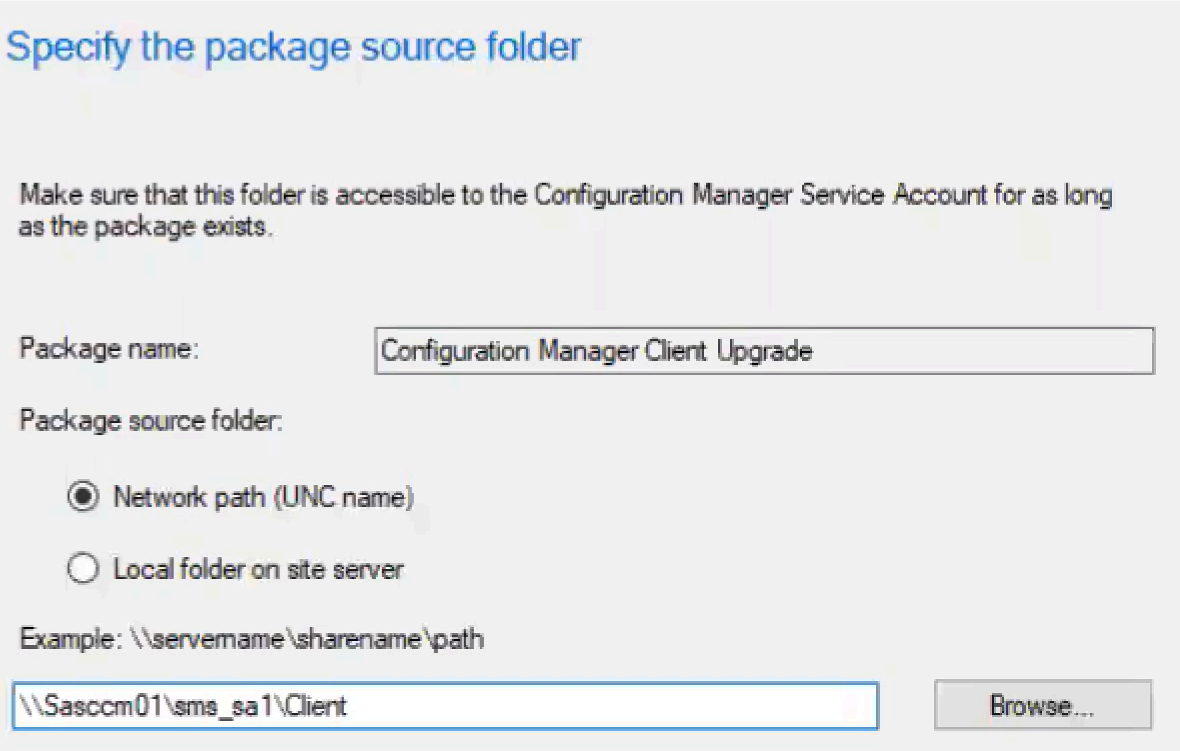
Source files are executable or data files that must be made available to clients.

If this package contains source files, specify whether they should be obtained from a specified source folder every time that the package is distributed or whether they should be stored as compressed data for distribution.

○ This package does not contain any source files

● Always obtain source files from a source folder

○ Create a compressed version of the source files



Specify the package source folder

Make sure that this folder is accessible to the Configuration Manager Service Account for as long as the package exists.

Package name: Configuration Manager Client Upgrade

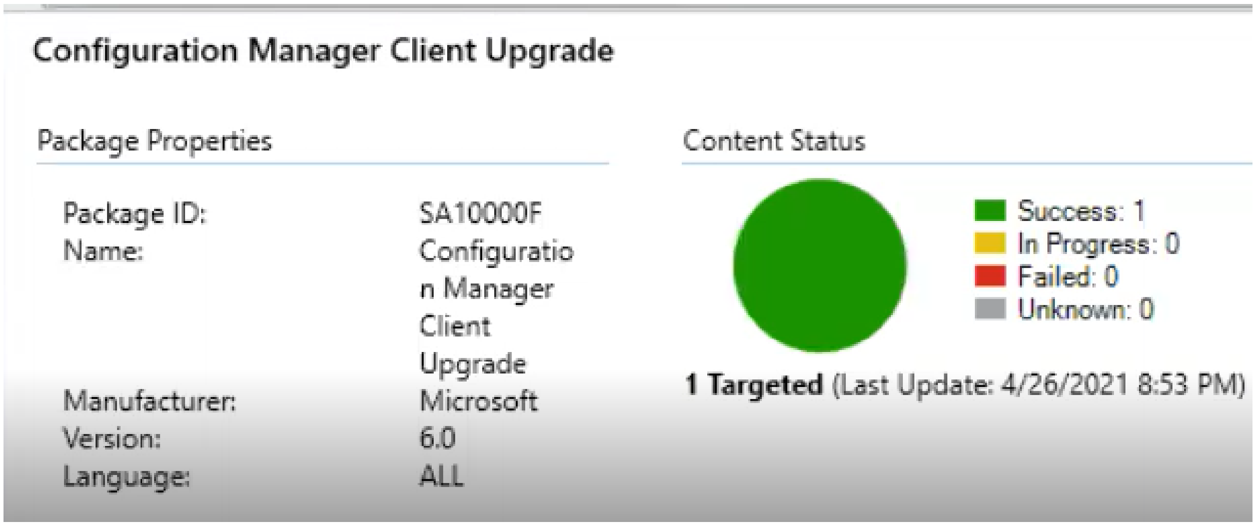
Package source folder:

● Network path (UNC name)

○ Local folder on site server

Example: \\servername\sharename\path

\\Sasccm01\sms_sa1\Client



Configuration Manager Client Upgrade

Package Properties

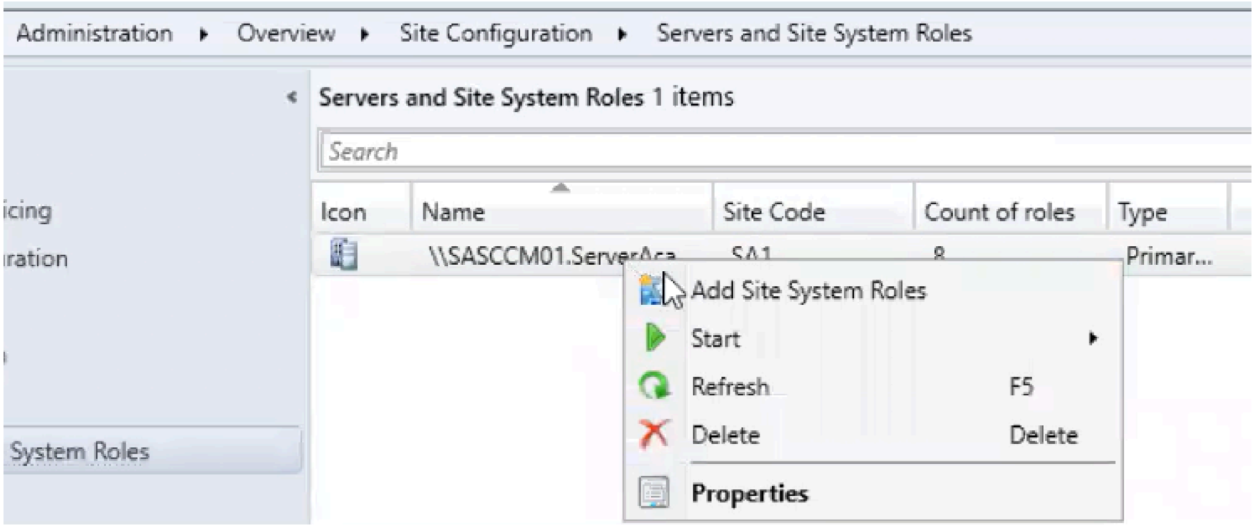
Package ID:	SA10000F
Name:	Configuration Manager Client Upgrade
Manufacturer:	Microsoft
Version:	6.0
Language:	ALL

Content Status

🟩 Success: 1
🟨 In Progress: 0
🟥 Failed: 0
⬜ Unknown: 0

1 Targeted (Last Update: 4/26/2021 8:53 PM)

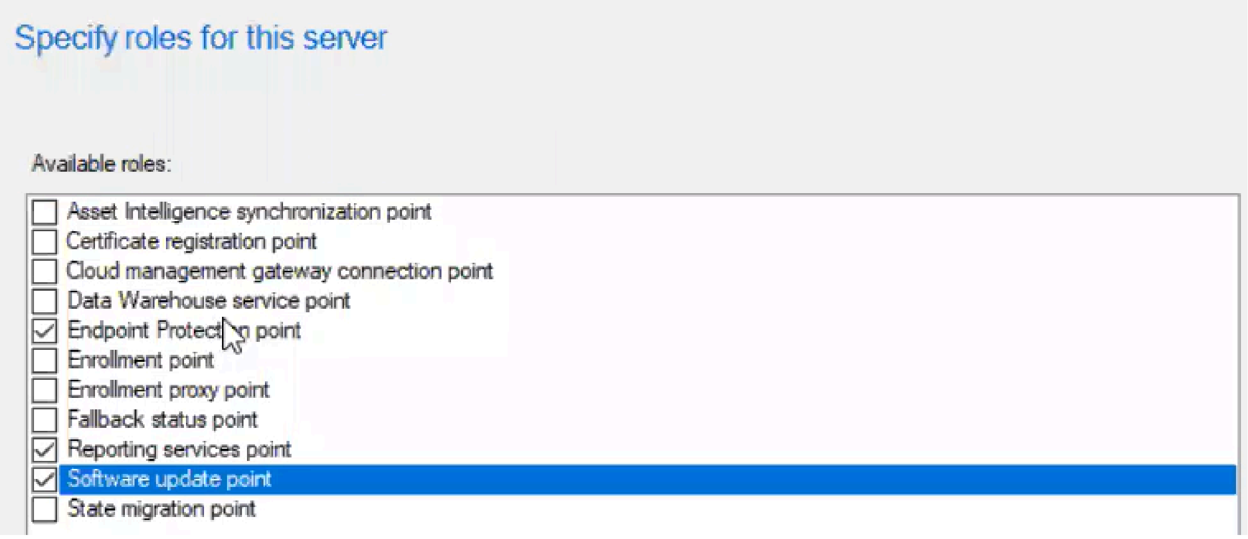
Installing Endpoint Protection Server Roles



Administration ▸ Overview ▸ Site Configuration ▸ Servers and Site System Roles

Servers and Site System Roles 1 items

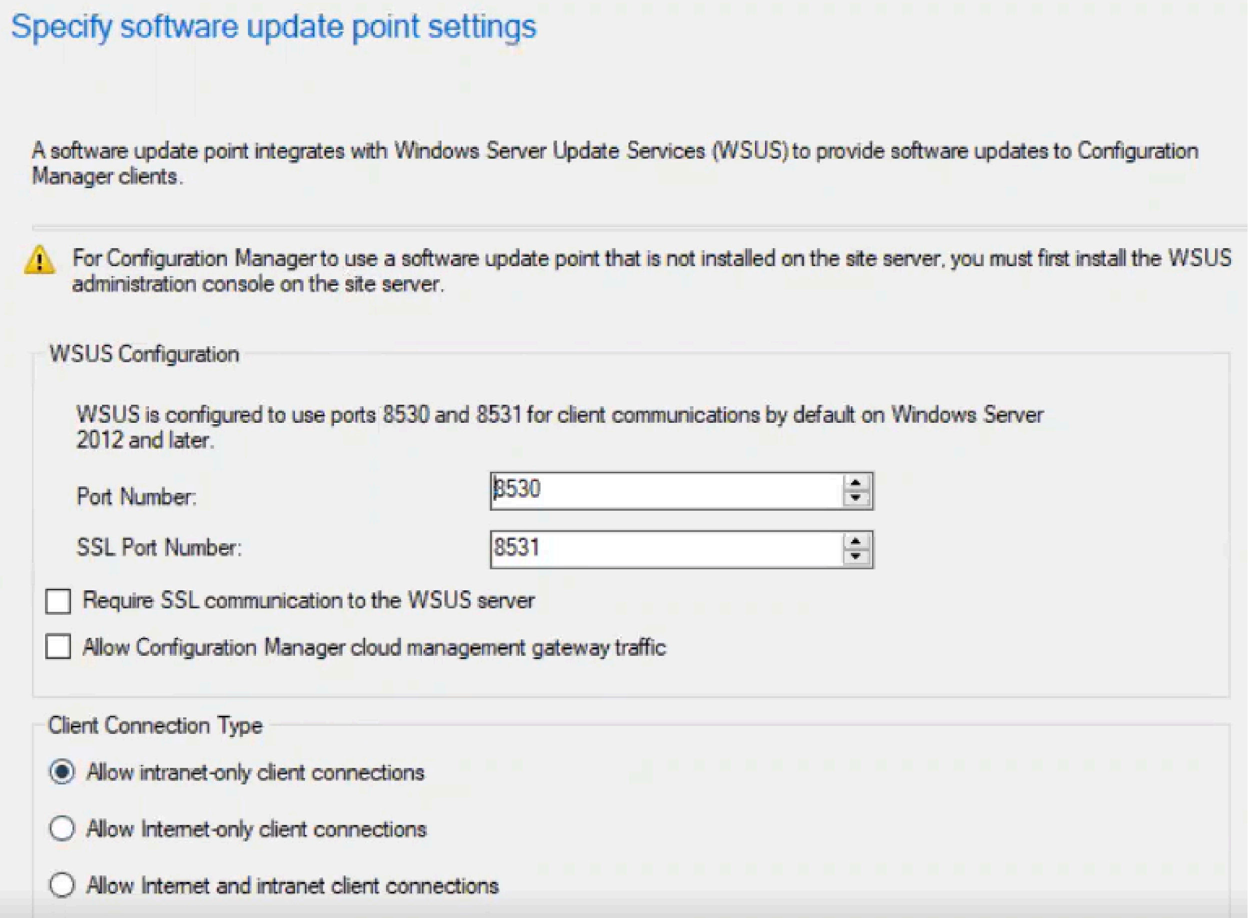
Icon	Name	Site Code	Count of roles	Type
	\\SASCCM01.ServerAca...	SA1	8	Primar...



Specify roles for this server

Available roles:

☐ 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
☑ Reporting services point
☑ Software update point
☐ State migration point



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 8530 and 8531 for client communications by default on Windows Server 2012 and later.

Port Number: 8530

SSL Port Number: 8531

□ Require SSL communication to the WSUS server

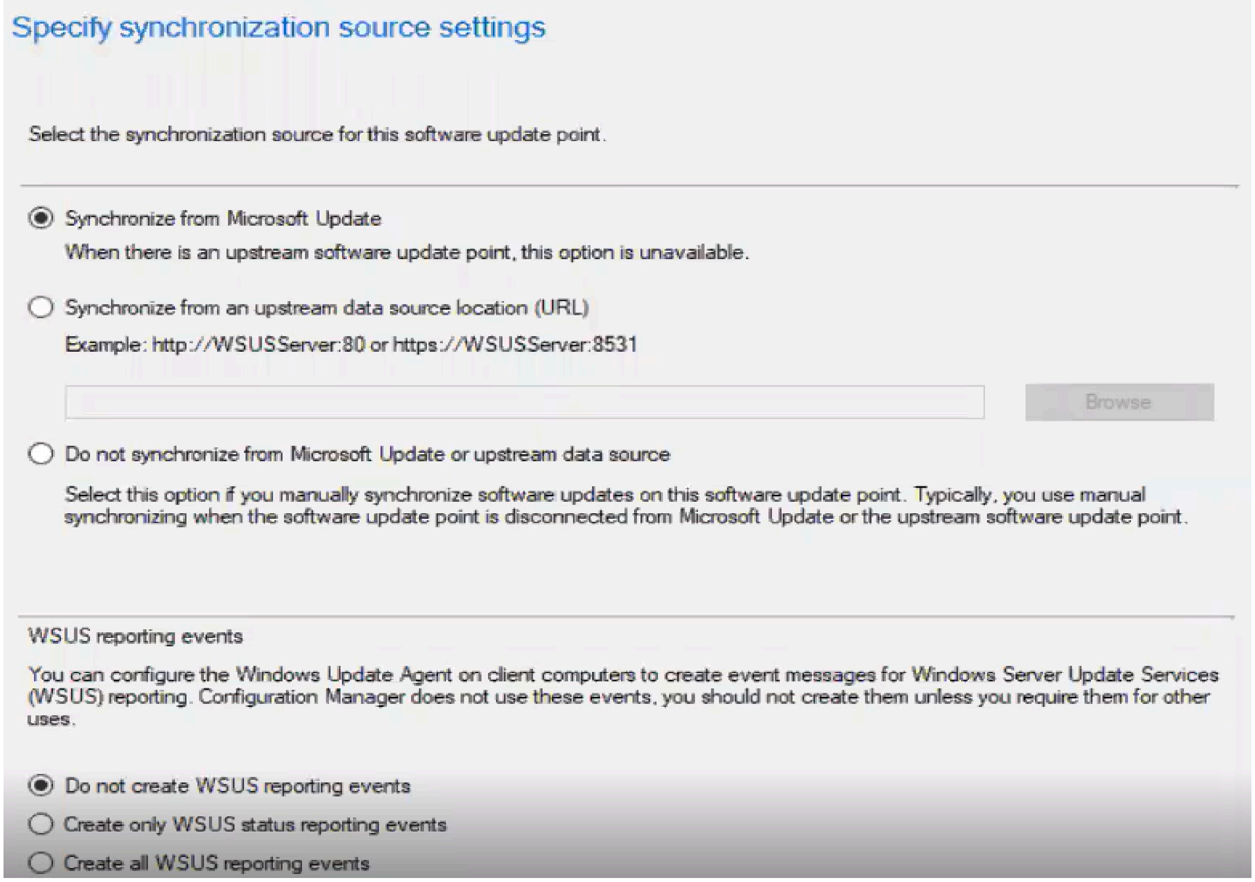
□ Allow Configuration Manager cloud management gateway traffic

Client Connection Type

● Allow intranet-only client connections

○ Allow Internet-only client connections

○ Allow Internet and intranet client connections



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

○ 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.

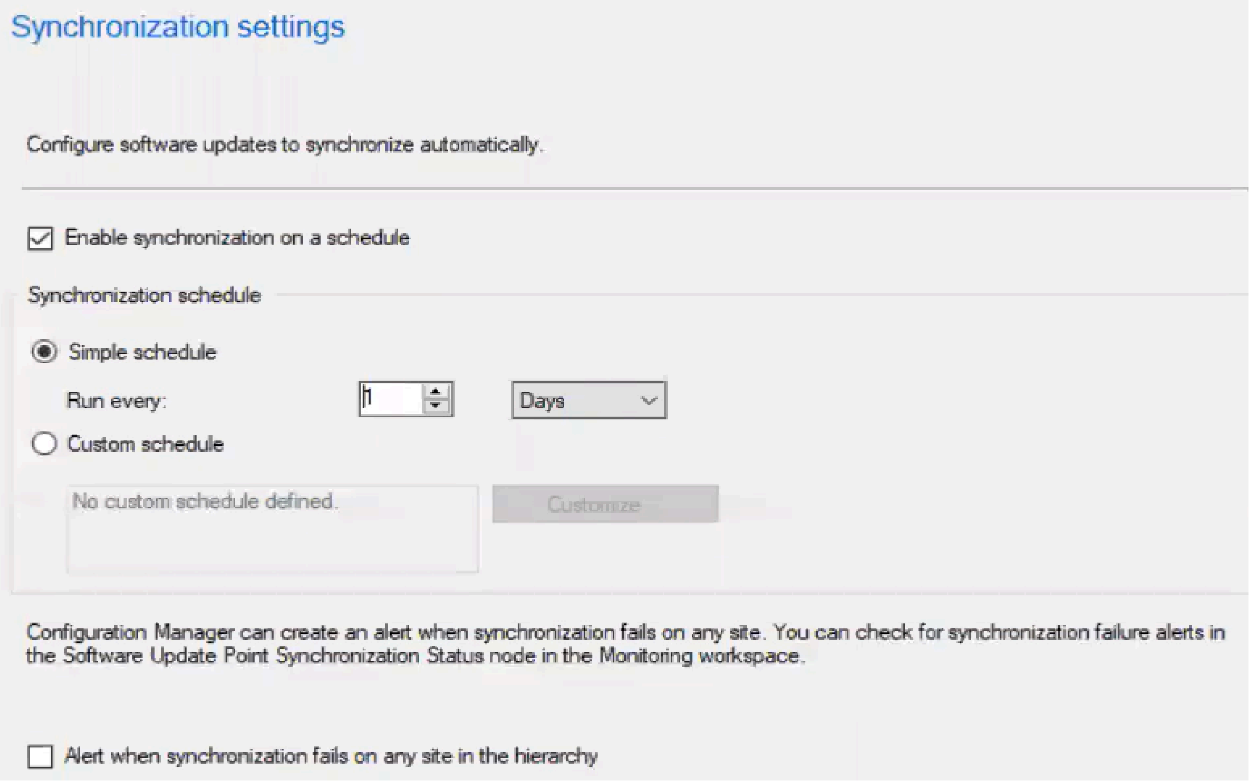
WSUS reporting events

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



Synchronization settings

Configure software updates to synchronize automatically.

☑ Enable synchronization on a schedule

Synchronization schedule

● Simple schedule

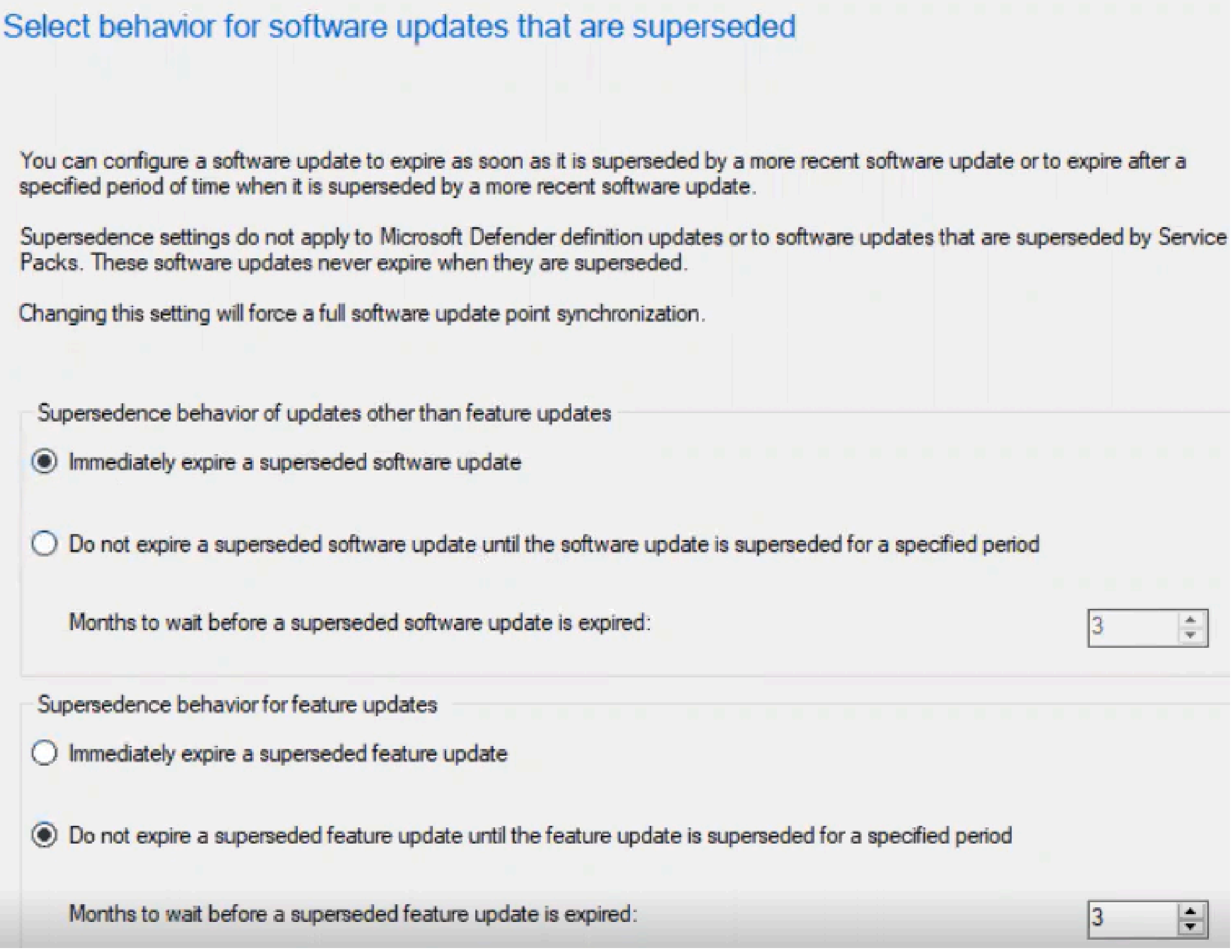
Run every: 1 Days

○ Custom schedule

No custom schedule defined.

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



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 Microsoft Defender 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 of updates other than feature updates

● Immediately expire a superseded software update

○ Do not expire a superseded software update until the software update is superseded for a specified period

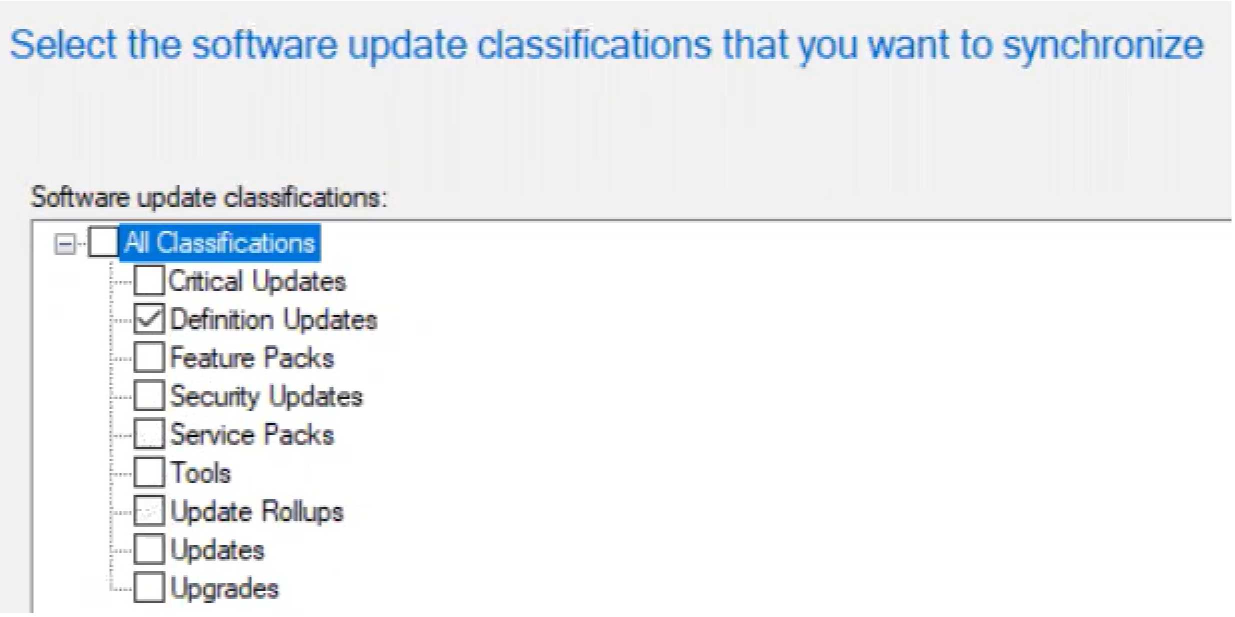
Months to wait before a superseded software update is expired: 3

Supersedence behavior for feature updates

○ Immediately expire a superseded feature update

● Do not expire a superseded feature update until the feature update is superseded for a specified period

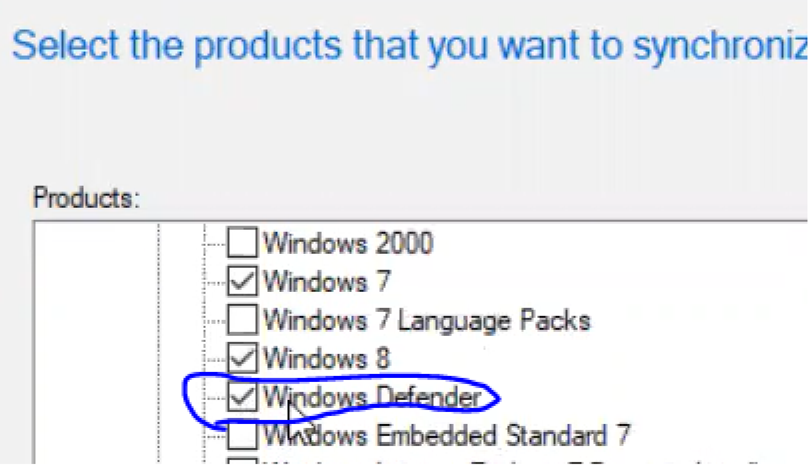
Months to wait before a superseded feature update is expired: 3



Select the software update classifications that you want to synchronize

Software update classifications:

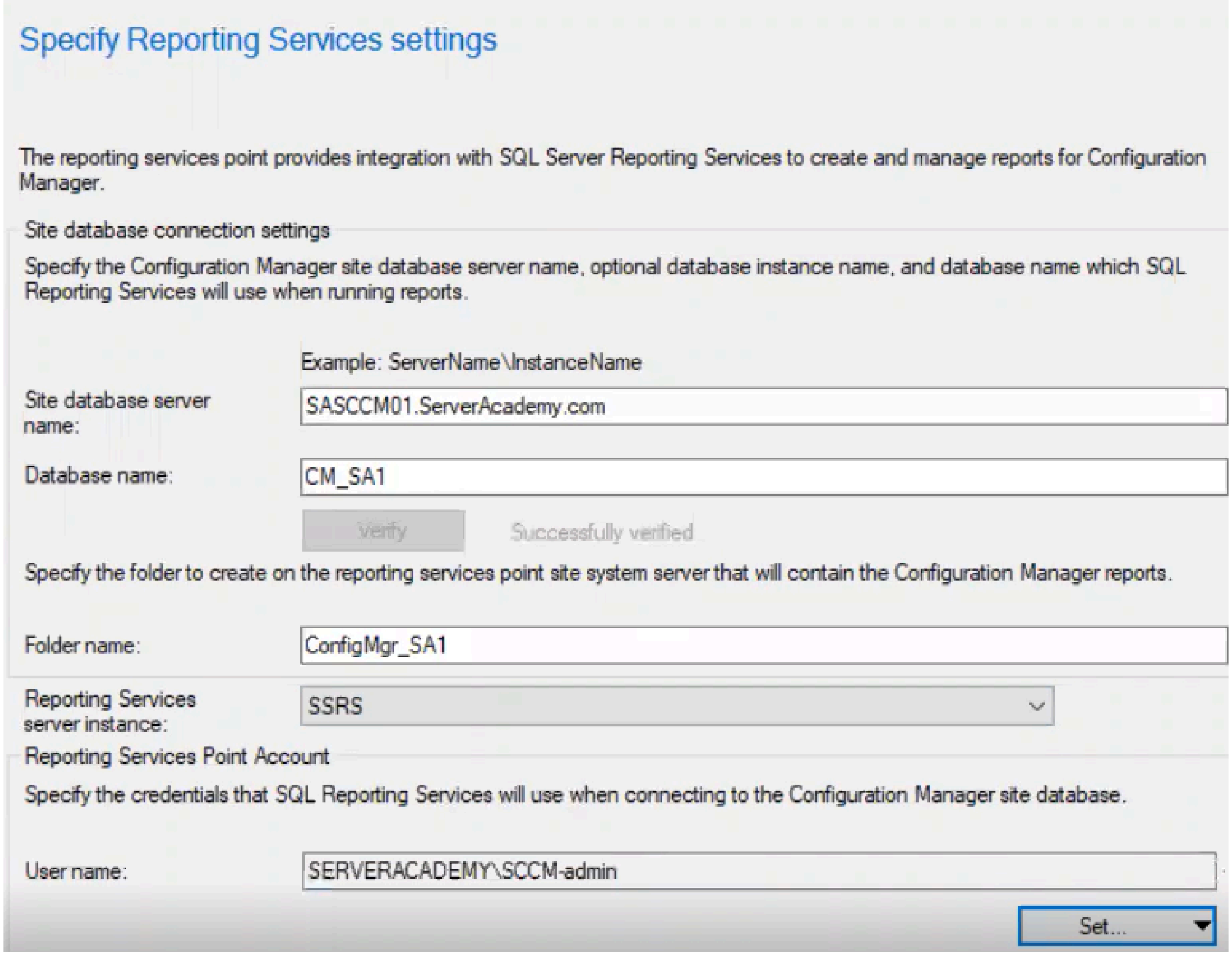
- □ All Classifications
  - □ Critical Updates
  - ☑ Definition Updates
  - □ Feature Packs
  - □ Security Updates
  - □ Service Packs
  - □ Tools
  - □ Update Rollups
  - □ Updates
  - □ Upgrades



Select the products that you want to synchroniz

Products:

- ☐ Windows 2000
- ☑ Windows 7
- ☐ Windows 7 Language Packs
- ☑ Windows 8
- ☑ Windows Defender
- ☐ Windows Embedded Standard 7



Specify Reporting Services settings

The reporting services point provides integration with SQL Server Reporting Services to create and manage reports for Configuration Manager.

Site database connection settings

Specify the Configuration Manager site database server name, optional database instance name, and database name which SQL Reporting Services will use when running reports.

Example: ServerName\InstanceName

Site database server name: SASCCM01.ServerAcademy.com

Database name: CM_SA1

Successfully verified

Specify the folder to create on the reporting services point site system server that will contain the Configuration Manager reports.

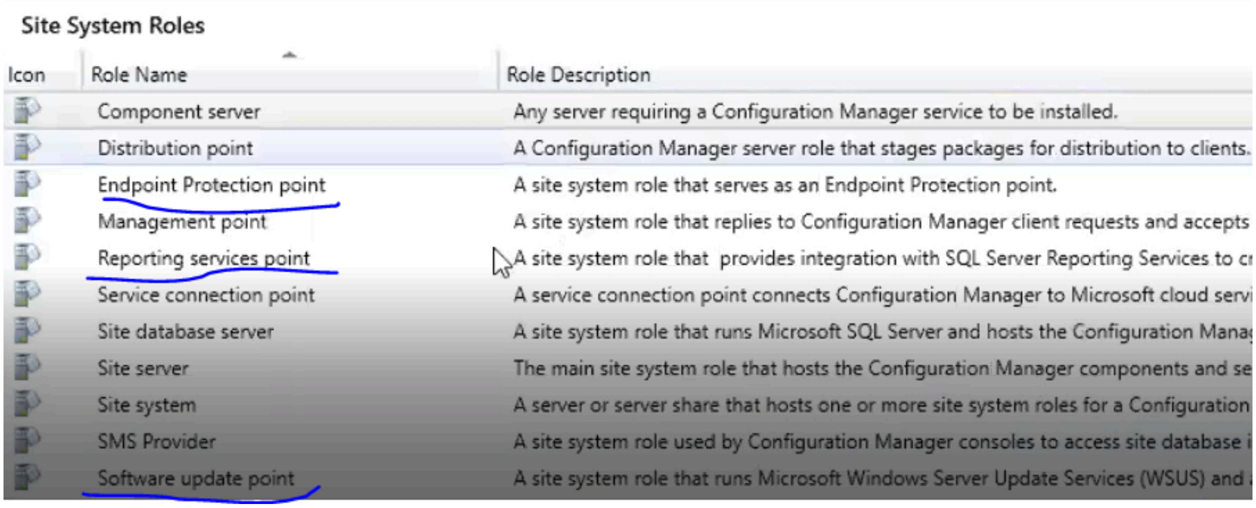
Folder name: ConfigMgr_SA1

Reporting Services server instance: SSRS

Reporting Services Point Account

Specify the credentials that SQL Reporting Services will use when connecting to the Configuration Manager site database.

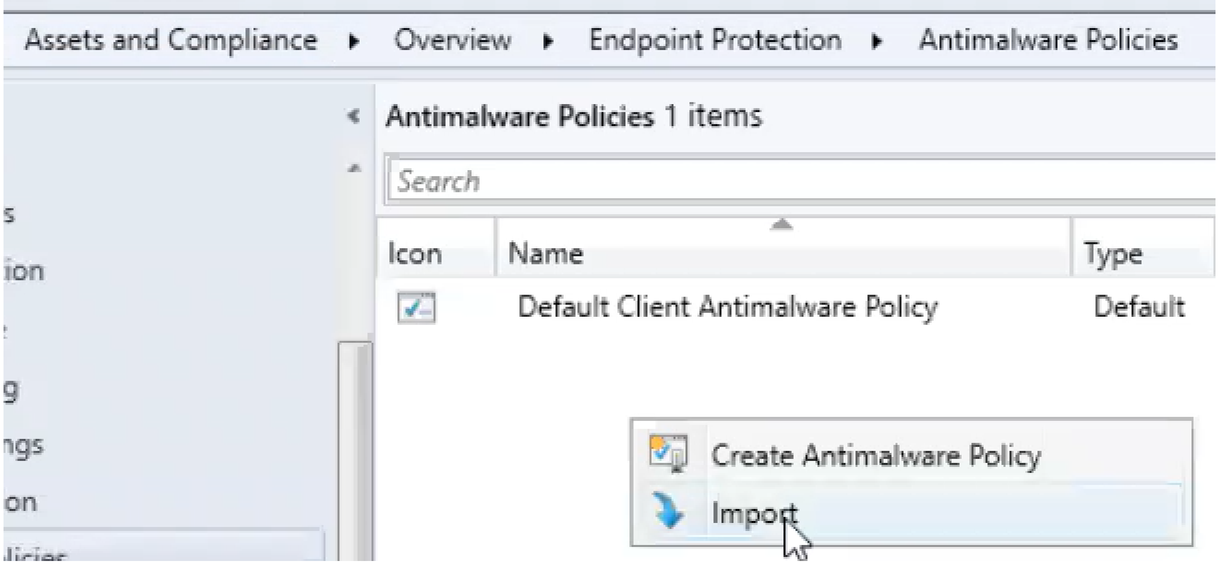
User name: SERVERACADEMY\SCCM-admin



Site System Roles

Icon	Role Name	Role Description
	Component server	Any server requiring a Configuration Manager service to be installed.
	Distribution point	A Configuration Manager server role that stages packages for distribution to clients.
	Endpoint Protection point	A site system role that serves as an Endpoint Protection point.
	Management point	A site system role that replies to Configuration Manager client requests and accepts
	Reporting services point	A site system role that provides integration with SQL Server Reporting Services to cr
	Service connection point	A service connection point connects Configuration Manager to Microsoft cloud servi
	Site database server	A site system role that runs Microsoft SQL Server and hosts the Configuration Manag
	Site server	The main site system role that hosts the Configuration Manager components and se
	Site system	A server or server share that hosts one or more site system roles for a Configuration
	SMS Provider	A site system role used by Configuration Manager consoles to access site database i
	Software update point	A site system role that runs Microsoft Windows Server Update Services (WSUS) and

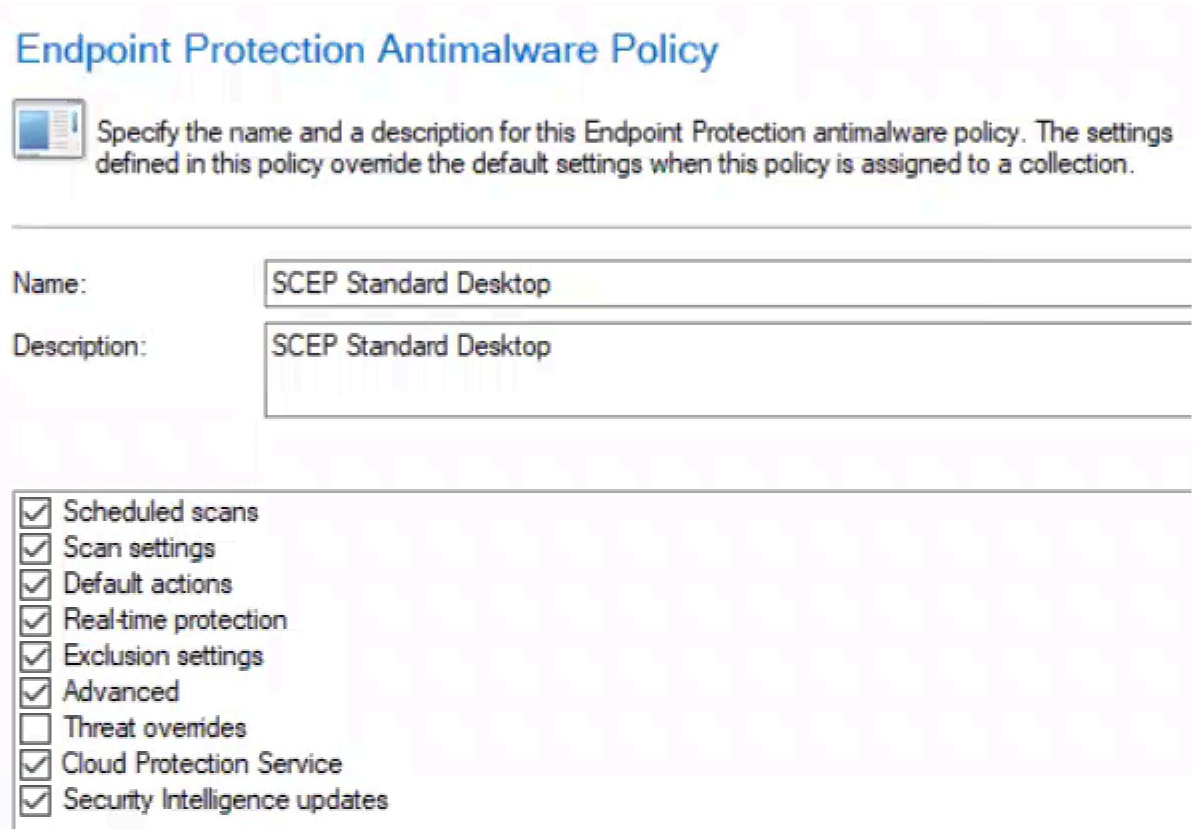
Endpoint Protection Policies



Assets and Compliance ▸ Overview ▸ Endpoint Protection ▸ Antimalware Policies
Search
Create Antimalware Policy
Import

Antimalware Policies 1 items

Icon	Name	Type
✓	Default Client Antimalware Policy	Default



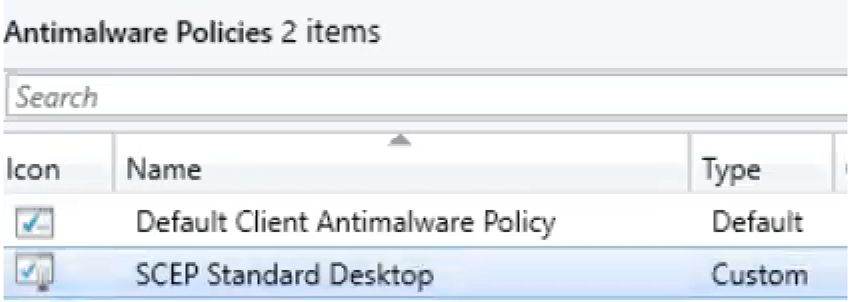
Endpoint Protection Antimalware Policy

Specify the name and a description for this Endpoint Protection antimalware policy. The settings defined in this policy override the default settings when this policy is assigned to a collection.

Name: SCEP Standard Desktop

Description: SCEP Standard Desktop

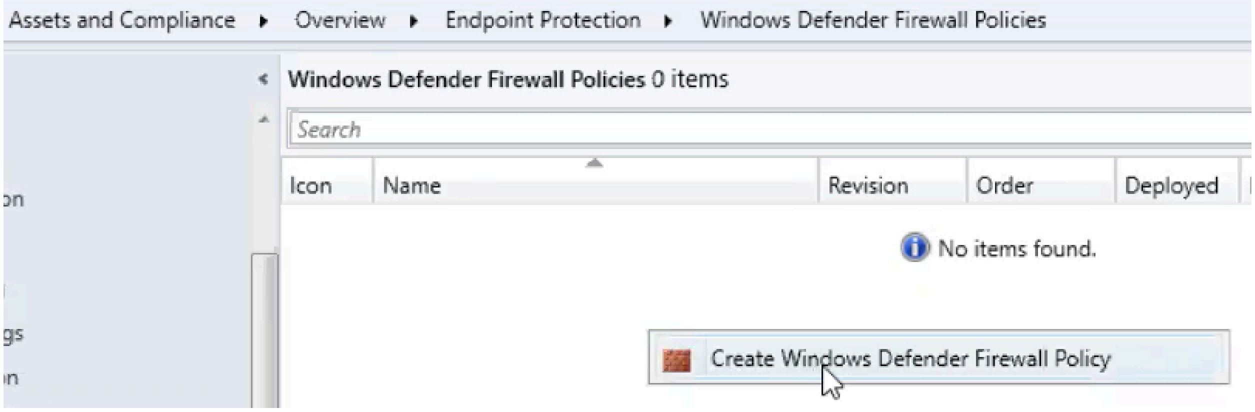
- ☑ Scheduled scans
- ☑ Scan settings
- ☑ Default actions
- ☑ Real-time protection
- ☑ Exclusion settings
- ☑ Advanced
- □ Threat overrides
- ☑ Cloud Protection Service
- ☑ Security Intelligence updates



Antimalware Policies 2 items

Search

Icon	Name	Type
✓	Default Client Antimalware Policy	Default
✓	SCEP Standard Desktop	Custom



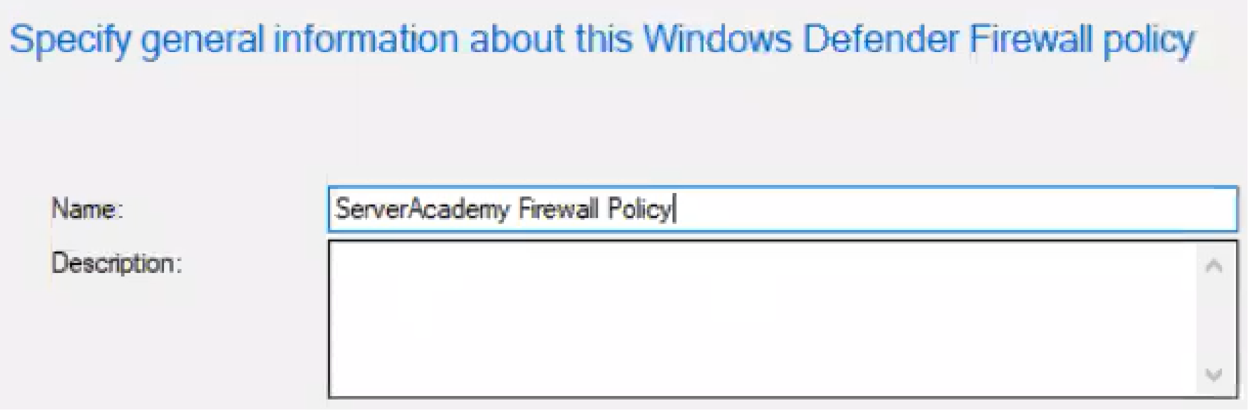
Assets and Compliance ▸ Overview ▸ Endpoint Protection ▸ Windows Defender Firewall Policies

Windows Defender Firewall Policies 0 items

Search

Icon	Name	Revision	Order	Deployed

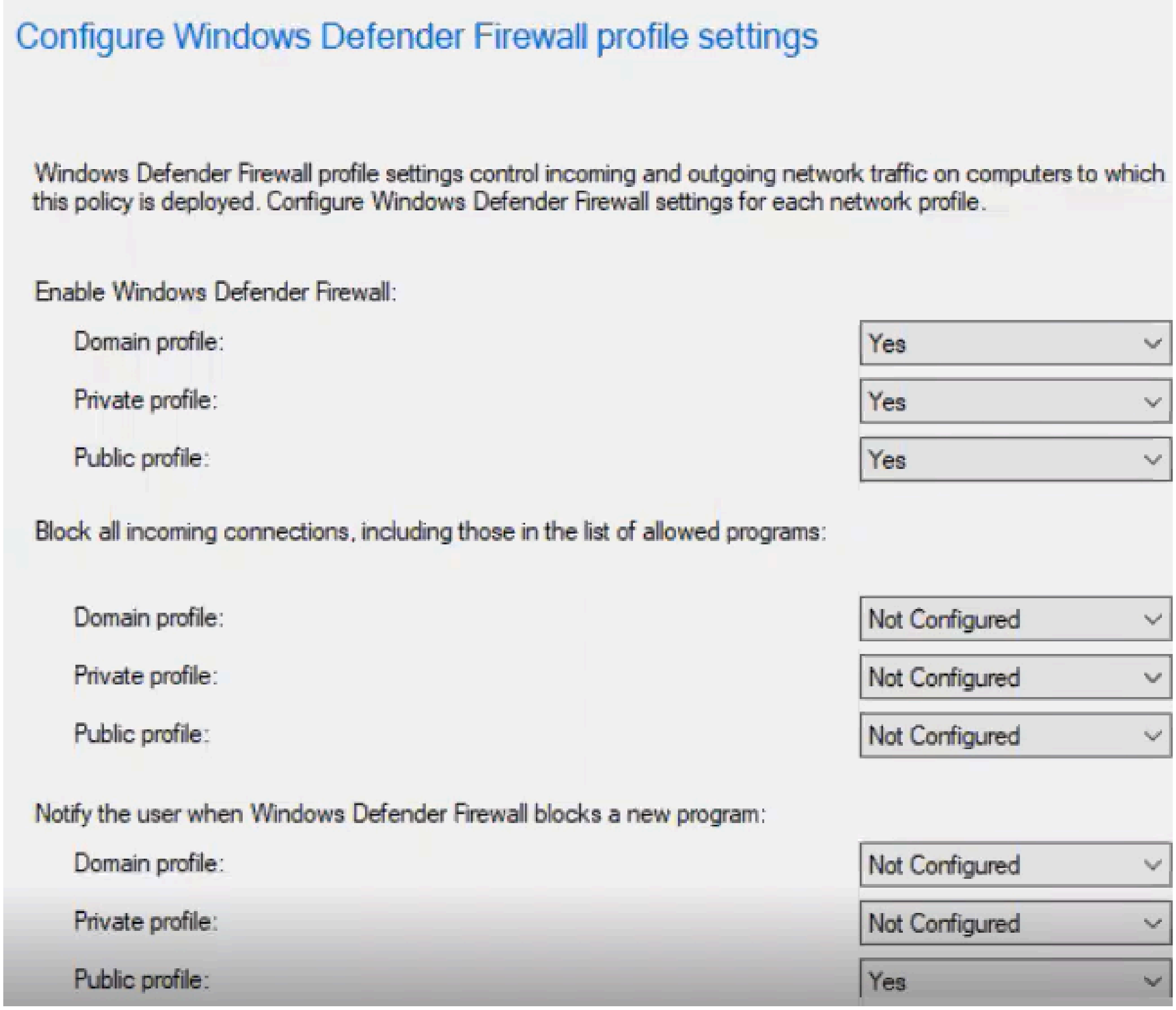
No items found.



Specify general information about this Windows Defender Firewall policy

Name: ServerAcademy Firewall Policy

Description:



Configure Windows Defender Firewall profile settings

Windows Defender Firewall profile settings control incoming and outgoing network traffic on computers to which this policy is deployed. Configure Windows Defender Firewall settings for each network profile.

Enable Windows Defender Firewall:

Domain profile: Yes

Private profile: Yes

Public profile: Yes

Block all incoming connections, including those in the list of allowed programs:

Domain profile: Not Configured

Private profile: Not Configured

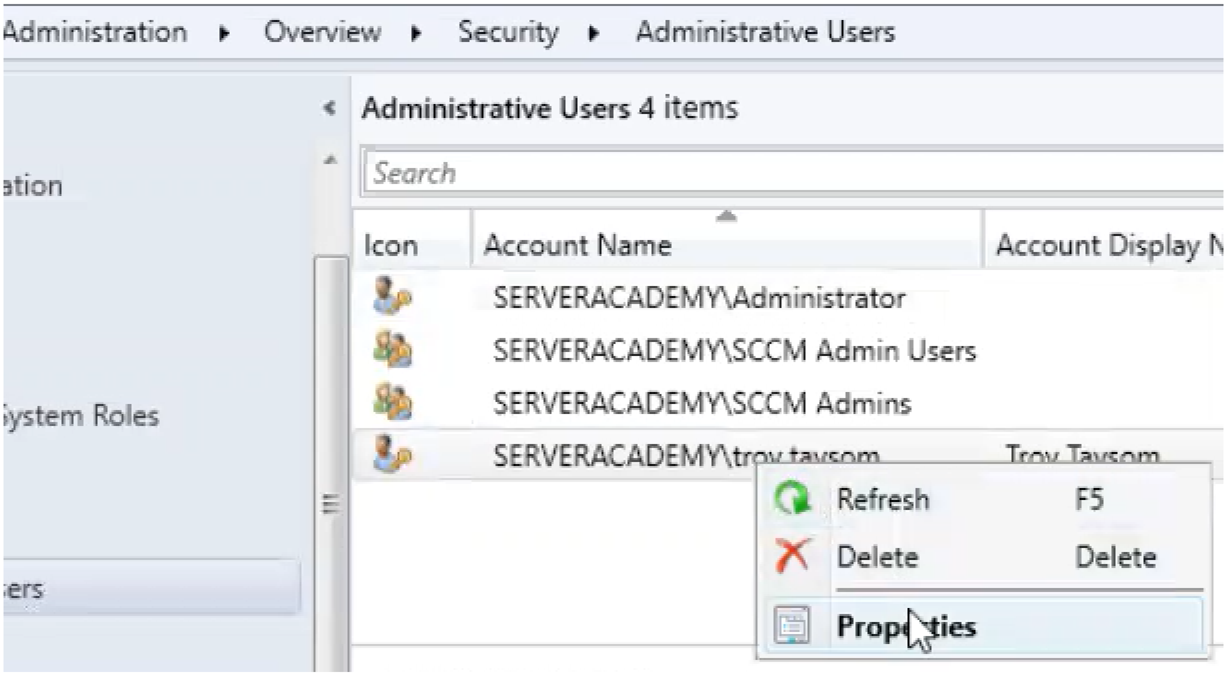
Public profile: Not Configured

Notify the user when Windows Defender Firewall blocks a new program:

Domain profile: Not Configured

Private profile: Not Configured

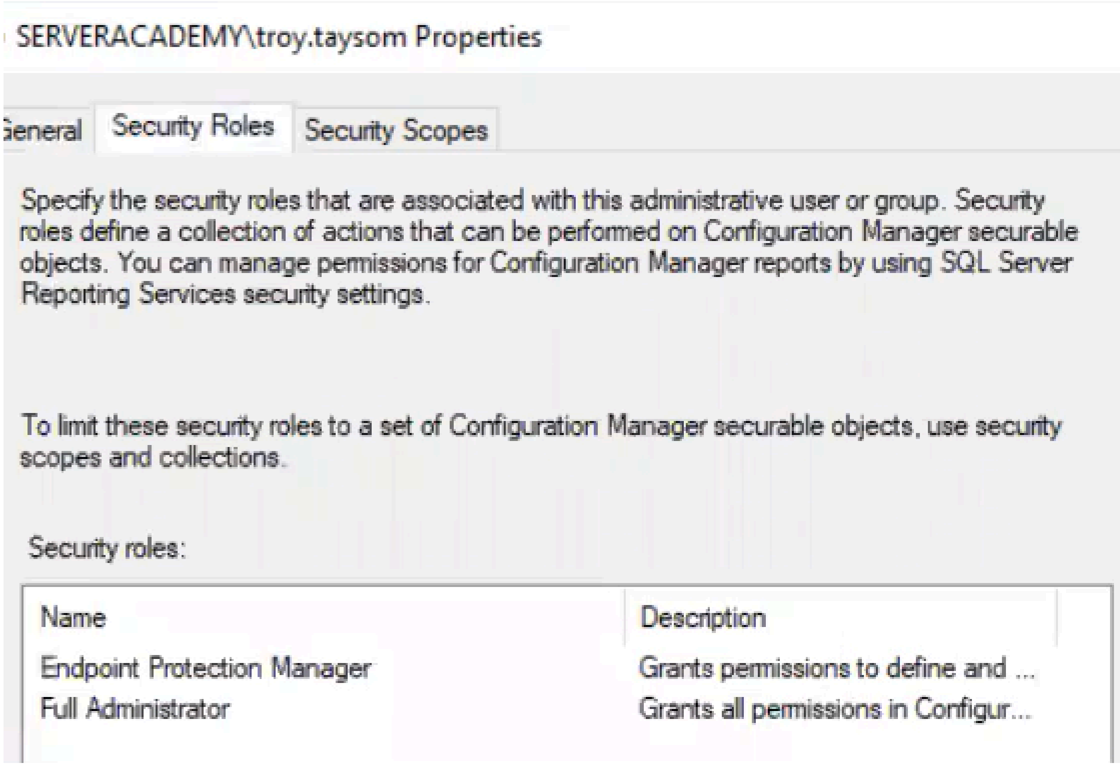
Public profile: Yes



Administration ▸ Overview ▸ Security ▸ Administrative Users

Administrative Users 4 items

Icon	Account Name	Account Display N
	SERVERACADEMY\Administrator	
	SERVERACADEMY\SCCM Admin Users	
	SERVERACADEMY\SCCM Admins	
	SERVERACADEMY\troy.taysom	Troy Taysom



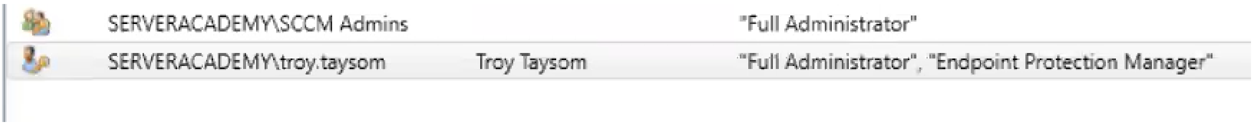
SERVERACADEMY\troy.taysom Properties

Specify the security roles that are associated with this administrative user or group. Security roles define a collection of actions that can be performed on Configuration Manager securable objects. You can manage permissions for Configuration Manager reports by using SQL Server Reporting Services security settings.

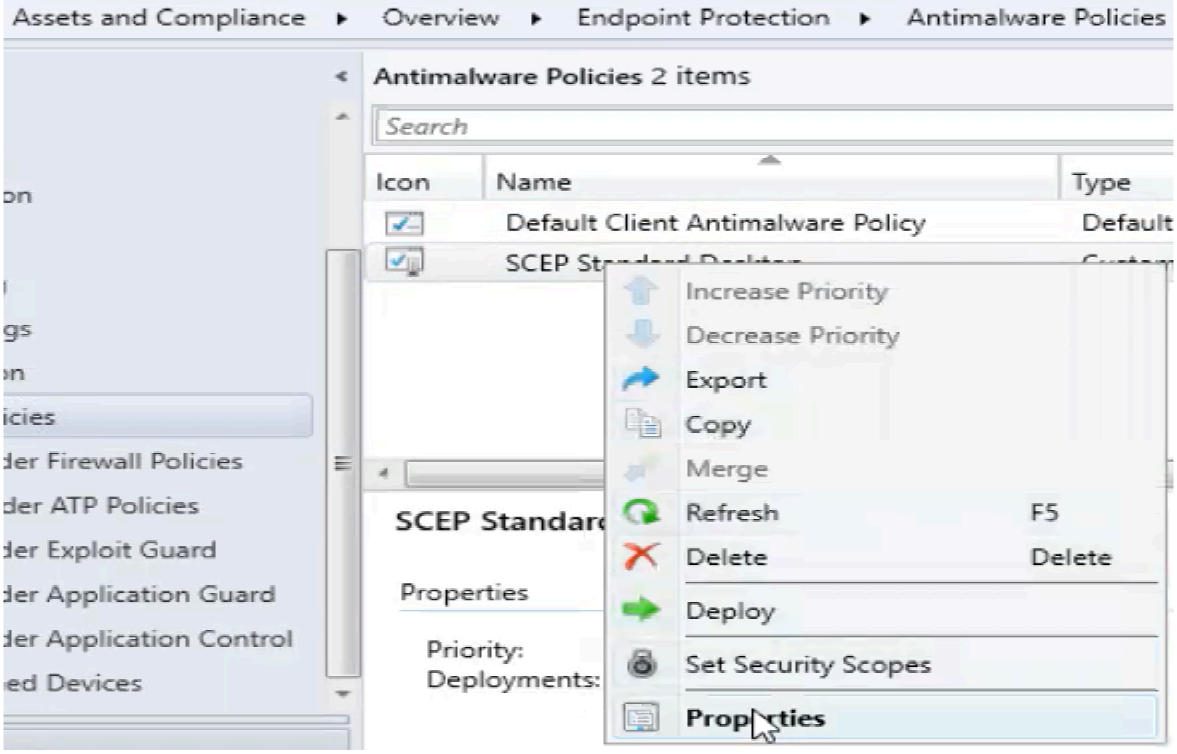
To limit these security roles to a set of Configuration Manager securable objects, use security scopes and collections.

Security roles:

Name	Description
Endpoint Protection Manager	Grants permissions to define and ...
Full Administrator	Grants all permissions in Configur...



SERVERACADEMY\SCCM Admins		"Full Administrator"
SERVERACADEMY\troy.taysom	Troy Taysom	"Full Administrator", "Endpoint Protection Manager"

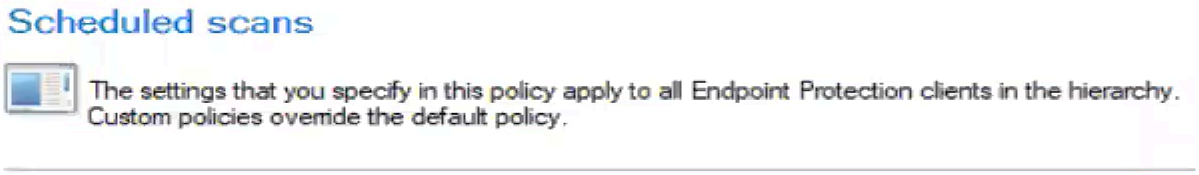


Assets and Compliance ▸ Overview ▸ Endpoint Protection ▸ Antimalware Policies

Antimalware Policies 2 items

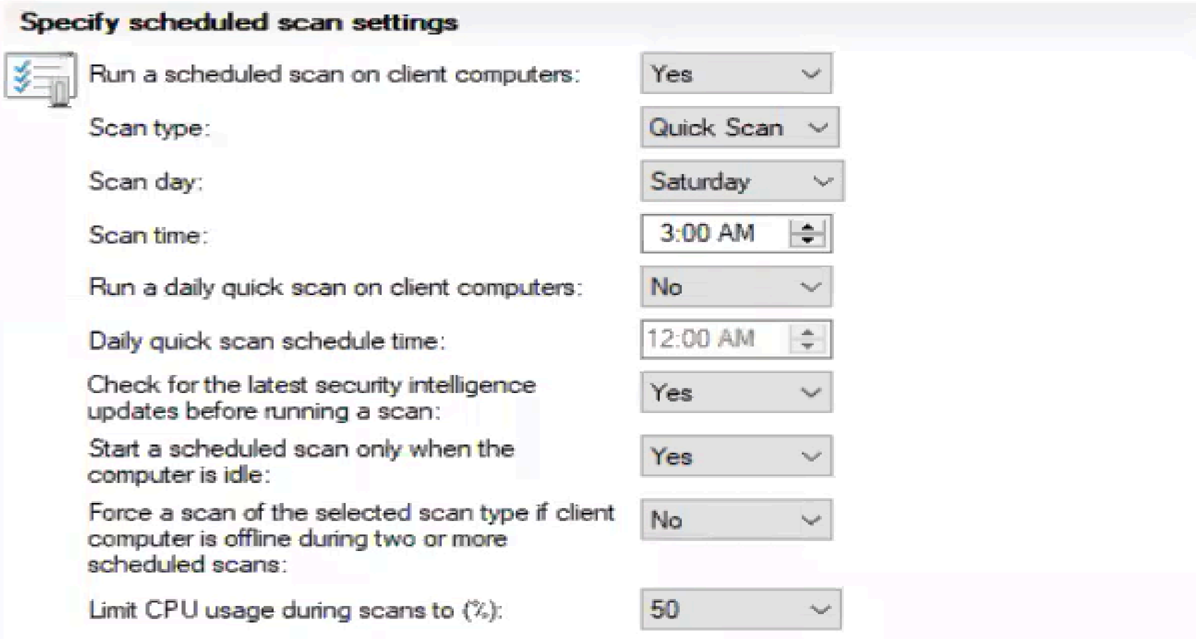
Icon	Name	Type
☑	Default Client Antimalware Policy	Default
☑	SCEP St	

SCEP Standar



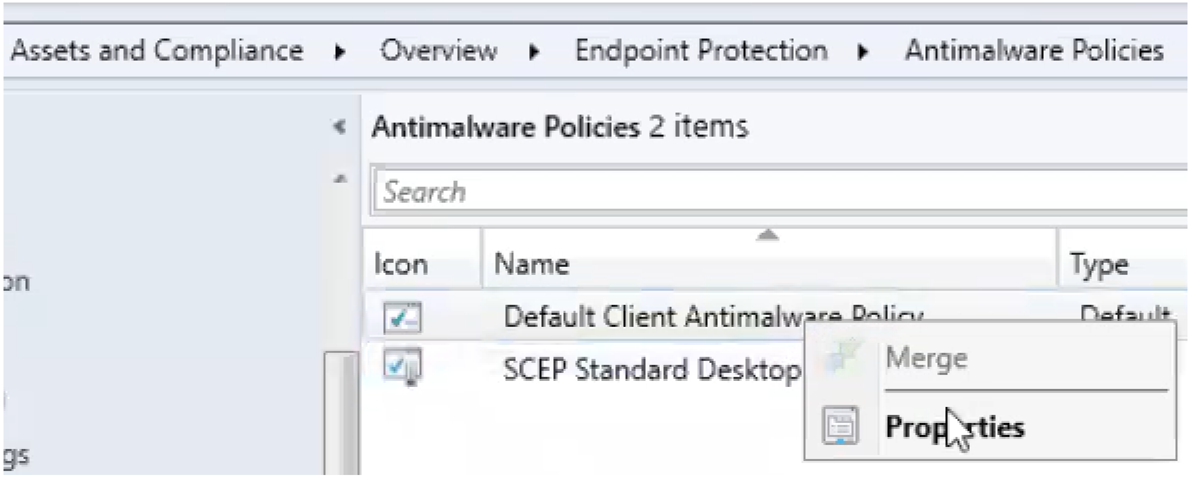
Scheduled scans

The settings that you specify in this policy apply to all Endpoint Protection clients in the hierarchy. Custom policies override the default policy.



Specify scheduled scan settings

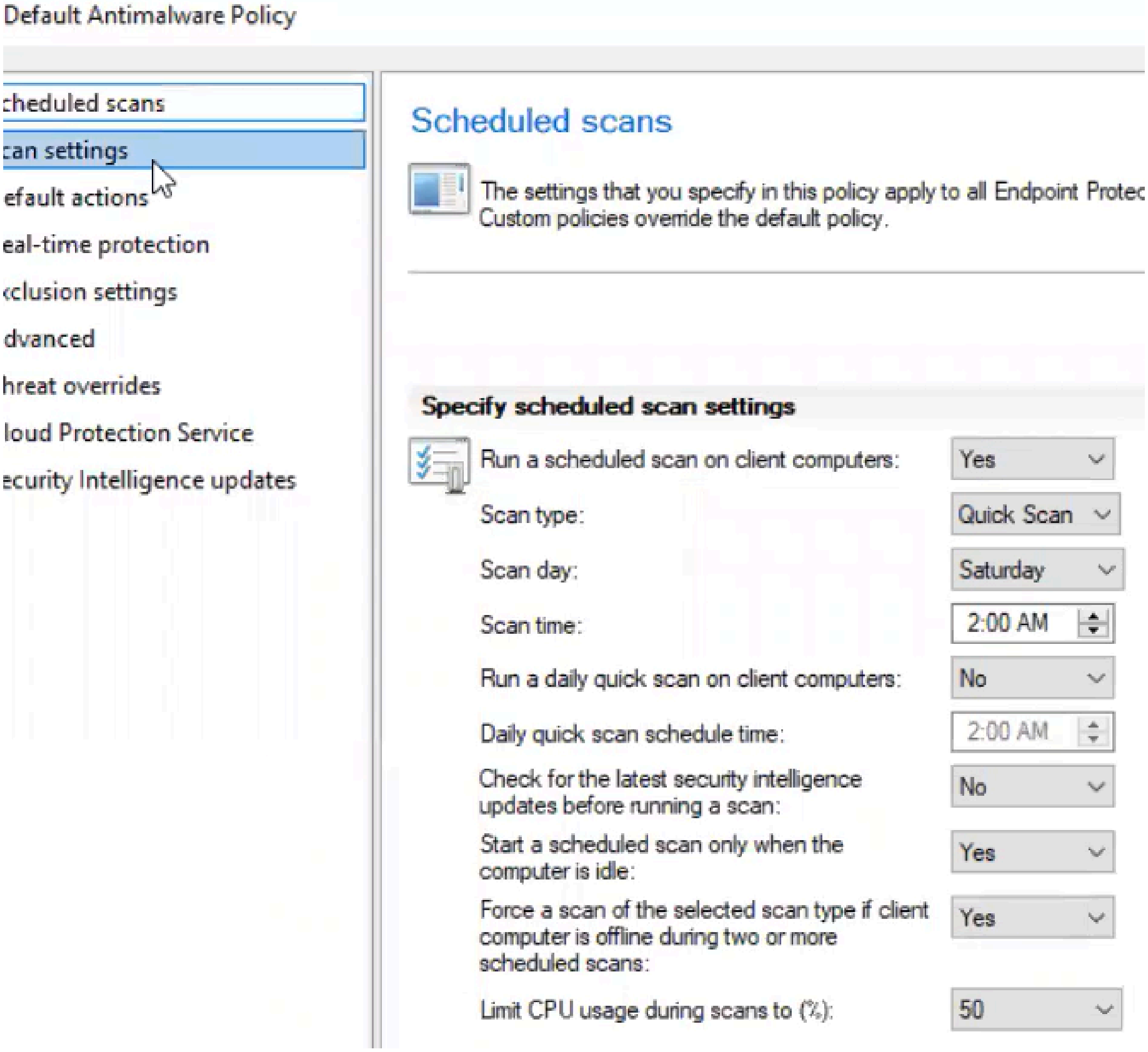
Run a scheduled scan on client computers:	Yes
Scan type:	Quick Scan
Scan day:	Saturday
Scan time:	3:00 AM
Run a daily quick scan on client computers:	No
Daily quick scan schedule time:	12:00 AM
Check for the latest security intelligence updates before running a scan:	Yes
Start a scheduled scan only when the computer is idle:	Yes
Force a scan of the selected scan type if client computer is offline during two or more scheduled scans:	No
Limit CPU usage during scans to (%):	50


Assets and Compliance ▸ Overview ▸ Endpoint Protection ▸ Antimalware Policies
on
gs
Merge
Properties

Antimalware Policies 2 items

Search

Icon	Name	Type
✓	Default Client Antimalware Policy	Default
✓	SCEP Standard Desktop	

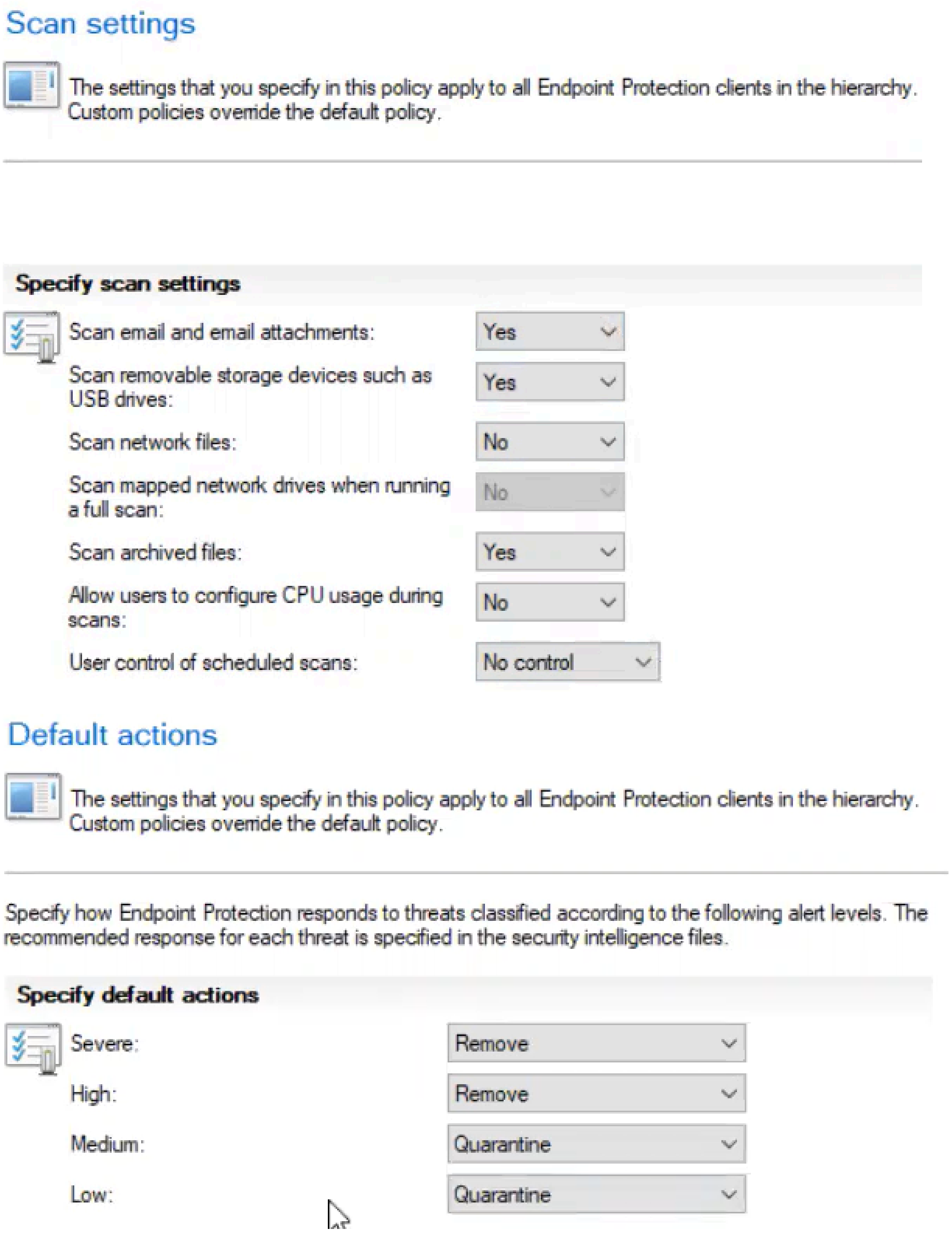


Scheduled scans

The settings that you specify in this policy apply to all Endpoint Protec
Custom policies override the default policy.

Specify scheduled scan settings

Run a scheduled scan on client computers:	Yes
Scan type:	Quick Scan
Scan day:	Saturday
Scan time:	2:00 AM
Run a daily quick scan on client computers:	No
Daily quick scan schedule time:	2:00 AM
Check for the latest security intelligence updates before running a scan:	No
Start a scheduled scan only when the computer is idle:	Yes
Force a scan of the selected scan type if client computer is offline during two or more scheduled scans:	Yes
Limit CPU usage during scans to (%):	50



Scan settings

The settings that you specify in this policy apply to all Endpoint Protection clients in the hierarchy. Custom policies override the default policy.

Specify scan settings

Scan email and email attachments: Yes

Scan removable storage devices such as USB drives: Yes

Scan network files: No

Scan mapped network drives when running a full scan: No

Scan archived files: Yes

Allow users to configure CPU usage during scans: No

User control of scheduled scans: No control

Default actions

The settings that you specify in this policy apply to all Endpoint Protection clients in the hierarchy. Custom policies override the default policy.

Specify how Endpoint Protection responds to threats classified according to the following alert levels. The recommended response for each threat is specified in the security intelligence files.

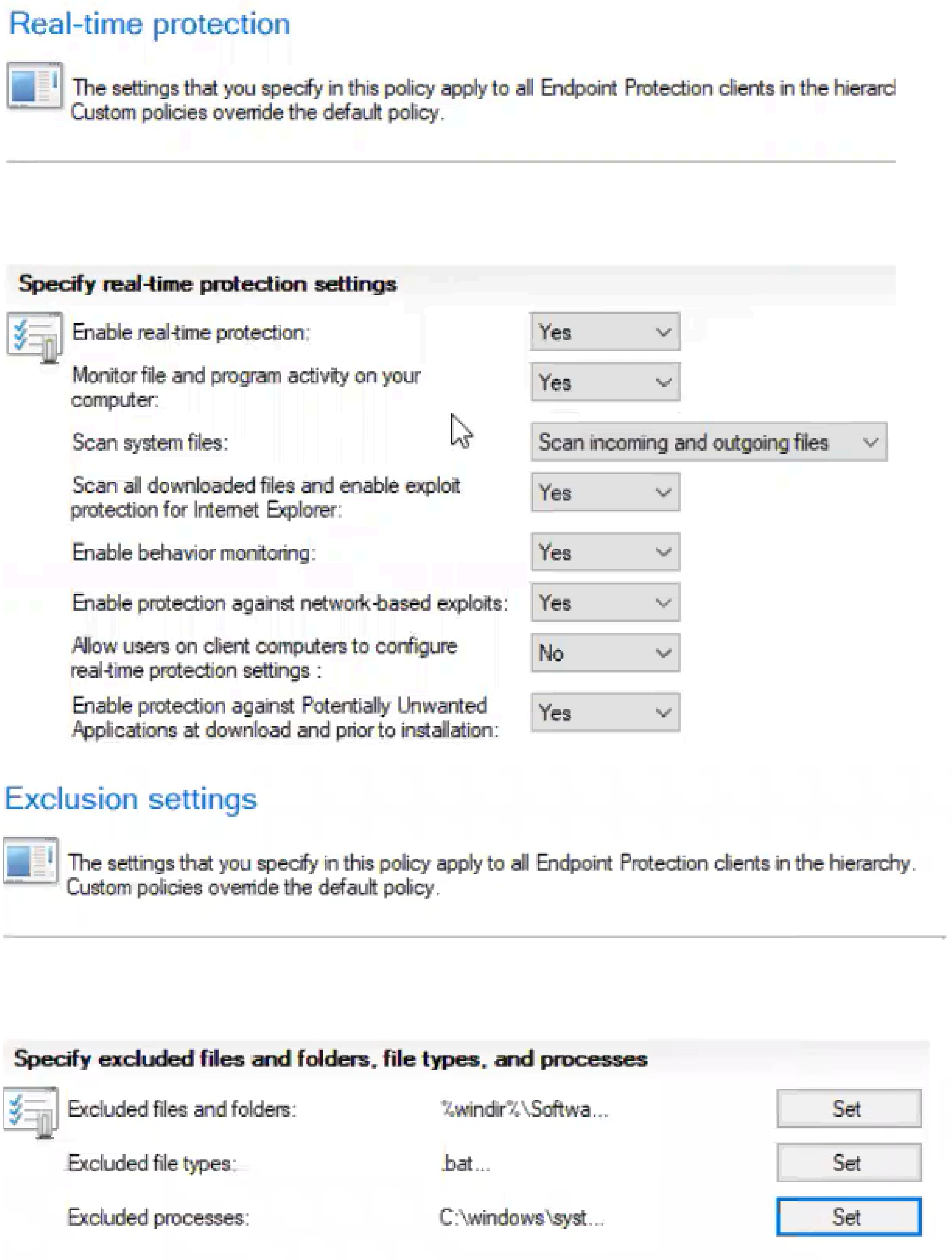
Specify default actions

Severe: Remove

High: Remove

Medium: Quarantine

Low: Quarantine



Real-time protection

The settings that you specify in this policy apply to all Endpoint Protection clients in the hierarc
Custom policies override the default policy.

Specify real-time protection settings

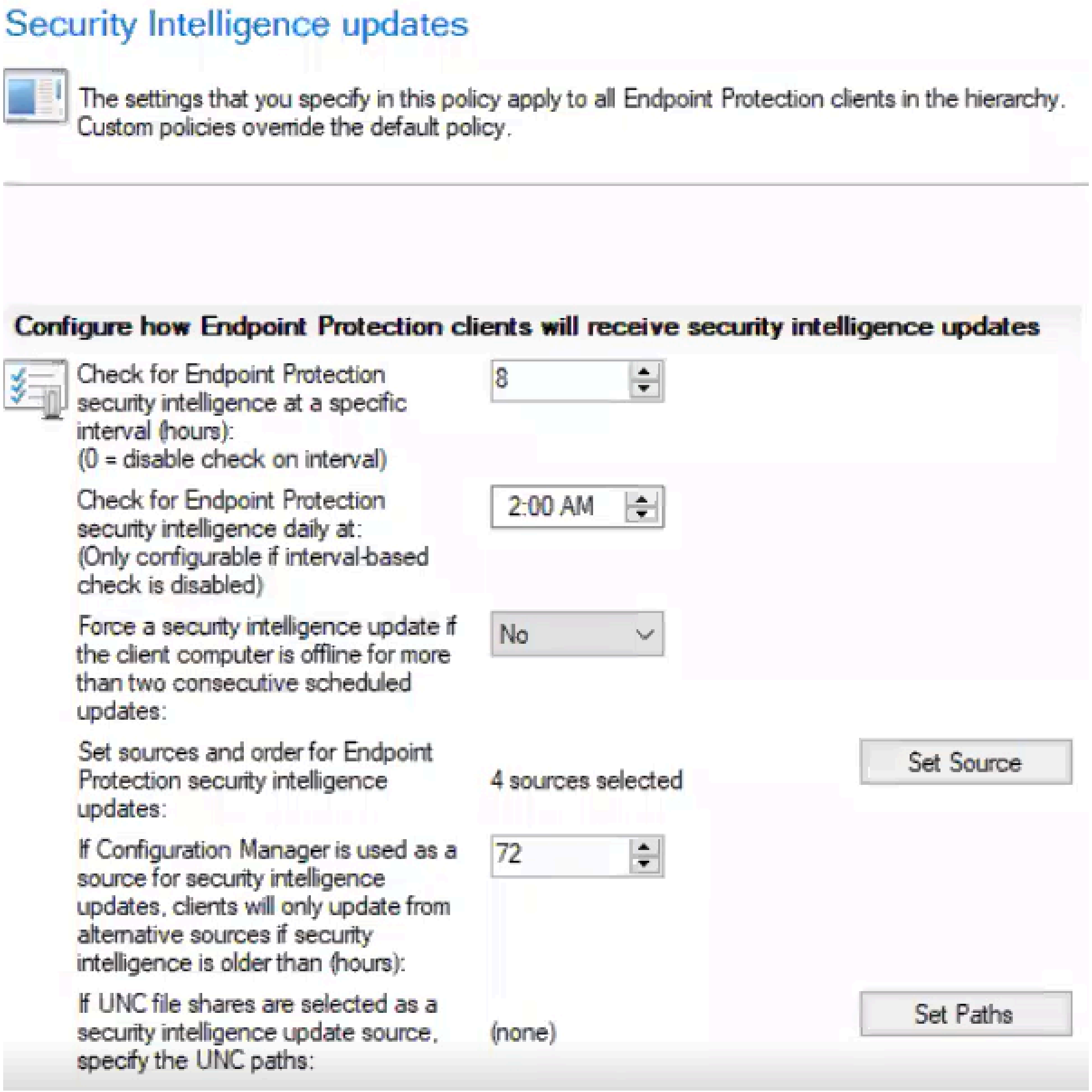
Enable real-time protection:	Yes
Monitor file and program activity on your computer:	Yes
Scan system files:	Scan incoming and outgoing files
Scan all downloaded files and enable exploit protection for Internet Explorer:	Yes
Enable behavior monitoring:	Yes
Enable protection against network-based exploits:	Yes
Allow users on client computers to configure real-time protection settings :	No
Enable protection against Potentially Unwanted Applications at download and prior to installation:	Yes

Exclusion settings

The settings that you specify in this policy apply to all Endpoint Protection clients in the hierarchy.
Custom policies override the default policy.

Specify excluded files and folders, file types, and processes

Excluded files and folders:	%windir%\Softwa...	Set
Excluded file types:	.bat...	Set
Excluded processes:	C:\windows\syst...	Set



Security Intelligence updates

The settings that you specify in this policy apply to all Endpoint Protection clients in the hierarchy. Custom policies override the default policy.

Configure how Endpoint Protection clients will receive security intelligence updates

Check for Endpoint Protection security intelligence at a specific interval (hours):
(0 = disable check on interval): 8

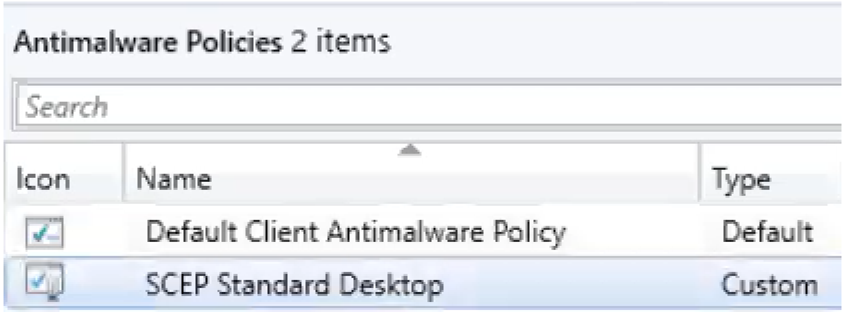
Check for Endpoint Protection security intelligence daily at:
(Only configurable if interval-based check is disabled): 2:00 AM

Force a security intelligence update if the client computer is offline for more than two consecutive scheduled updates: No

Set sources and order for Endpoint Protection security intelligence updates: 4 sources selected

If Configuration Manager is used as a source for security intelligence updates, clients will only update from alternative sources if security intelligence is older than (hours): 72

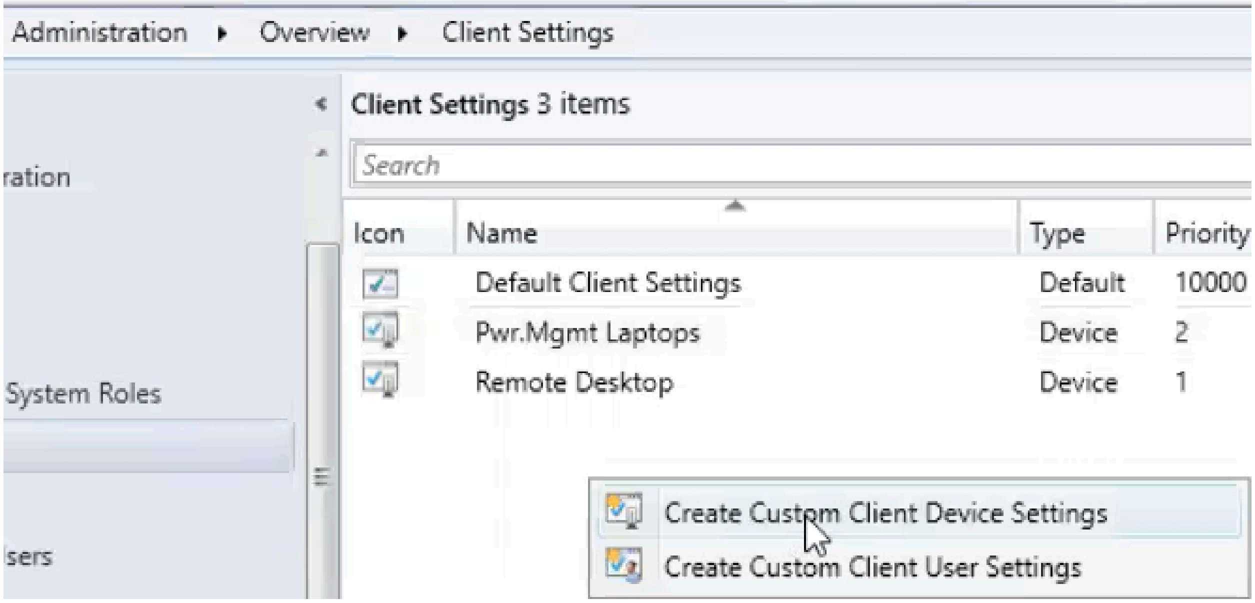
If UNC file shares are selected as a security intelligence update source, specify the UNC paths: (none)



Antimalware Policies 2 items

Icon	Name	Type
✓	Default Client Antimalware Policy	Default
✓	SCEP Standard Desktop	Custom

Endpoint Protection Client Installation



Administration ▸ Overview ▸ Client Settings

ration

System Roles

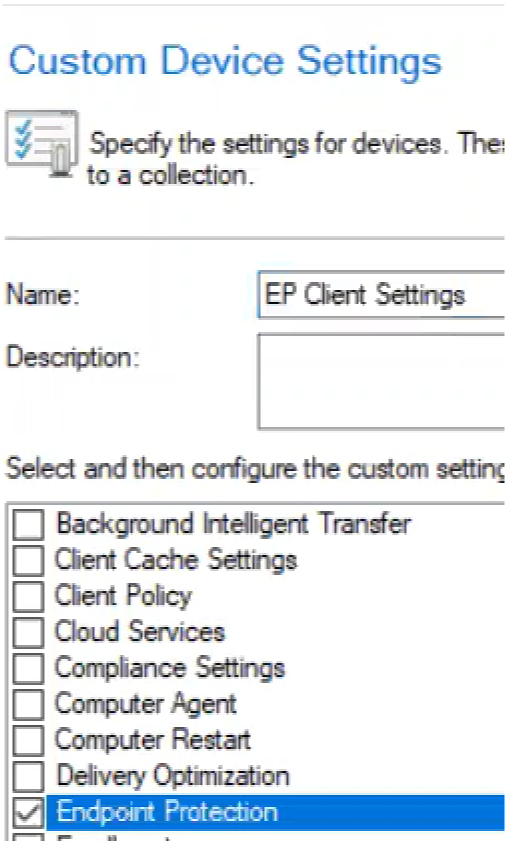
sers

Client Settings 3 items

Search

Icon	Name	Type	Priority
✓	Default Client Settings	Default	10000
✓	Pwr.Mgmt Laptops	Device	2
✓	Remote Desktop	Device	1

Create Custom Client Device Settings
Create Custom Client User Settings



Custom Device Settings

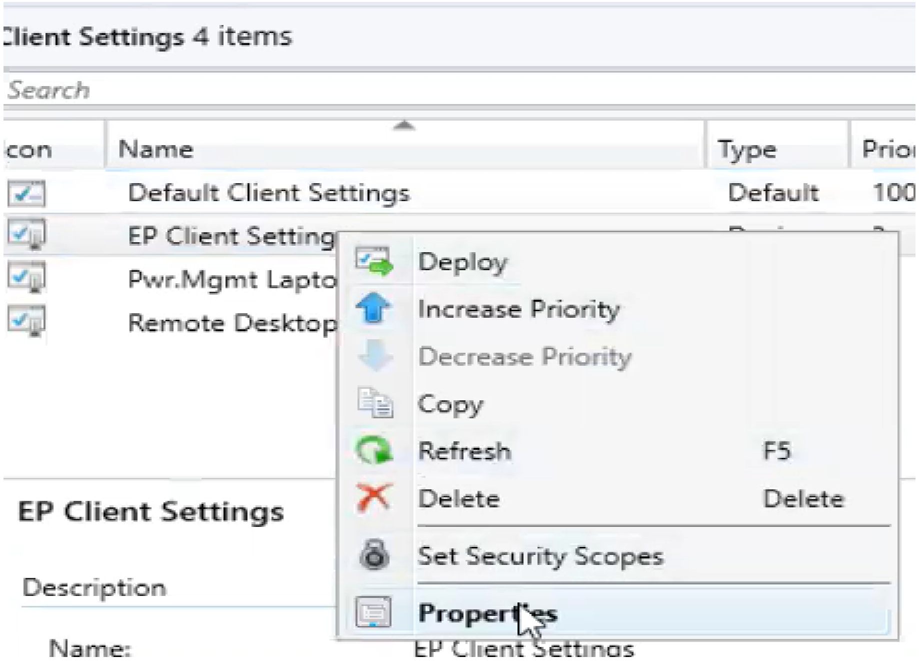
Specify the settings for devices. The:
to a collection.

Name: EP Client Settings

Description:

Select and then configure the custom settinc

- □ Background Intelligent Transfer
- □ Client Cache Settings
- □ Client Policy
- □ Cloud Services
- □ Compliance Settings
- □ Computer Agent
- □ Computer Restart
- □ Delivery Optimization
- ☑ Endpoint Protection



Client Settings 4 items

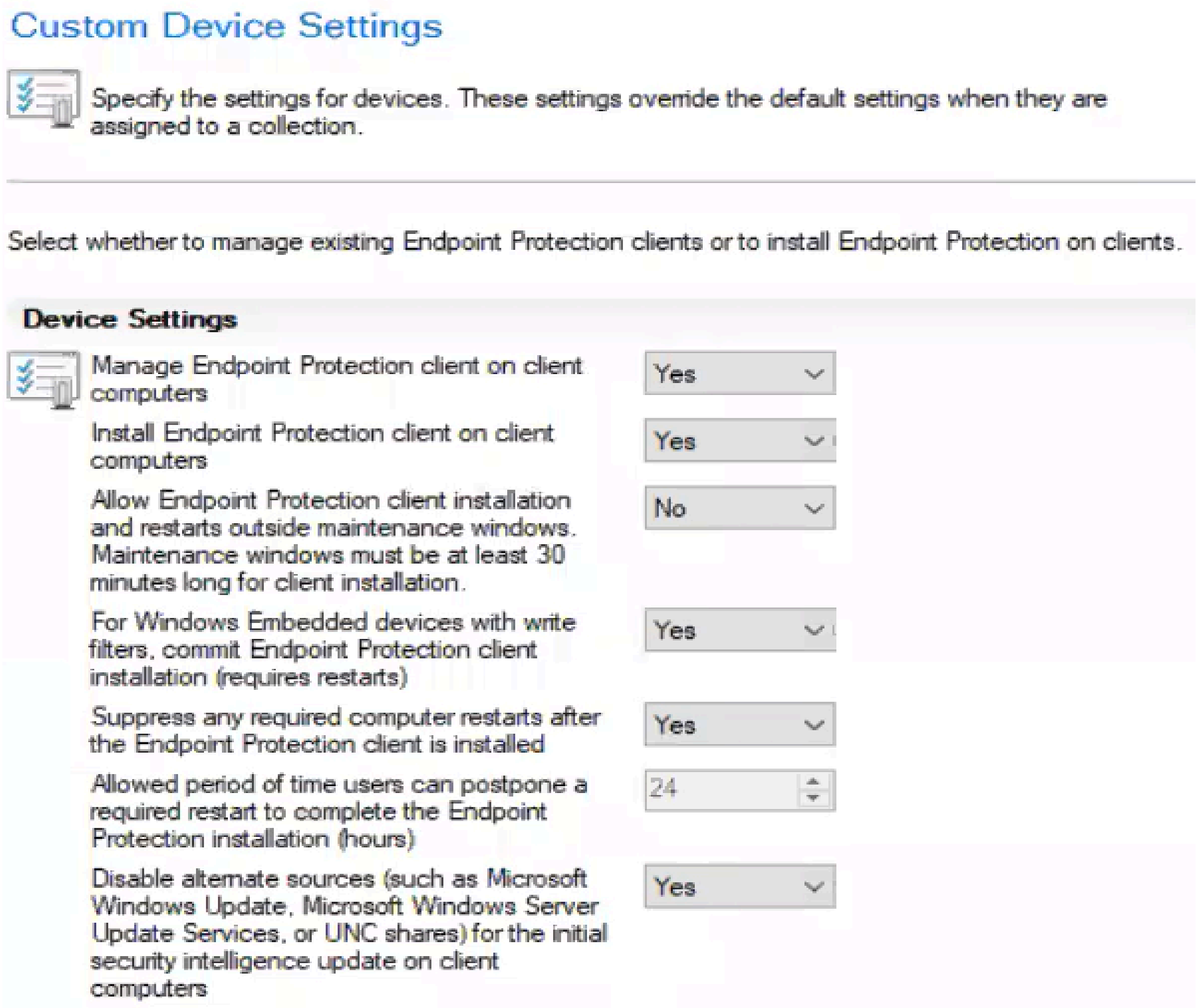
Search

Icon	Name	Type	Prio
☑	Default Client Settings	Default	100
☑	EP Client Setting		
☑	Pwr.Mgmt Lapto		
☑	Remote Desktop		

EP Client Settings

Description

Name: EP Client Settings



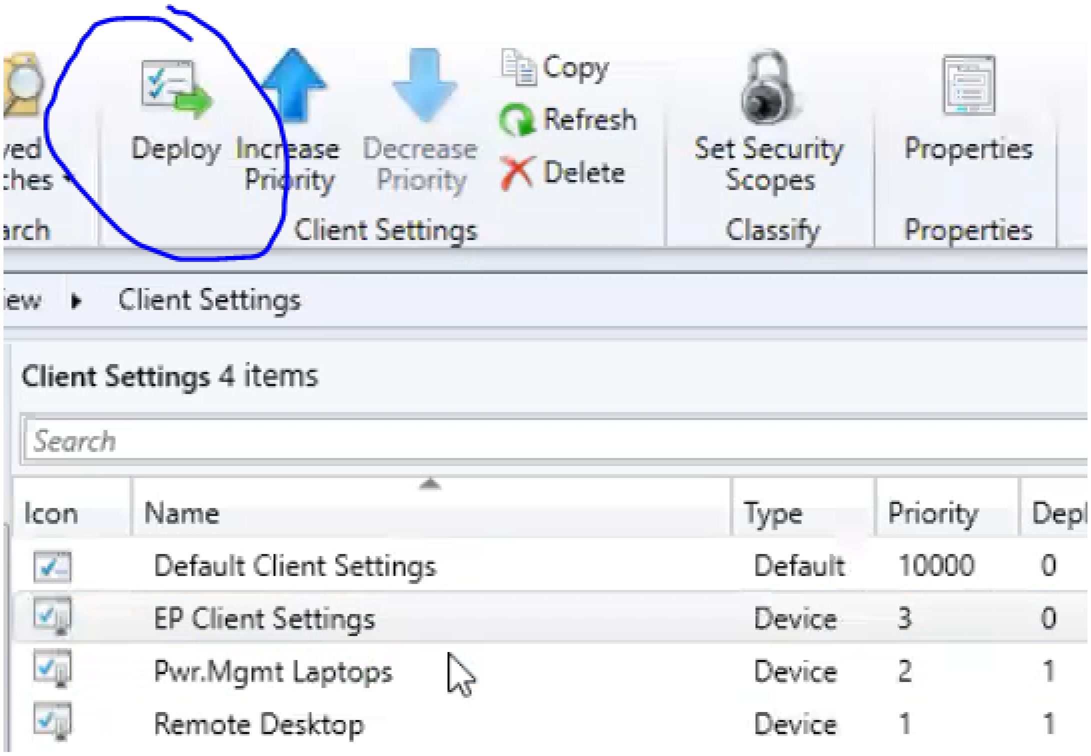
Custom Device Settings

Specify the settings for devices. These settings override the default settings when they are assigned to a collection.

Select whether to manage existing Endpoint Protection clients or to install Endpoint Protection on clients.

Device Settings

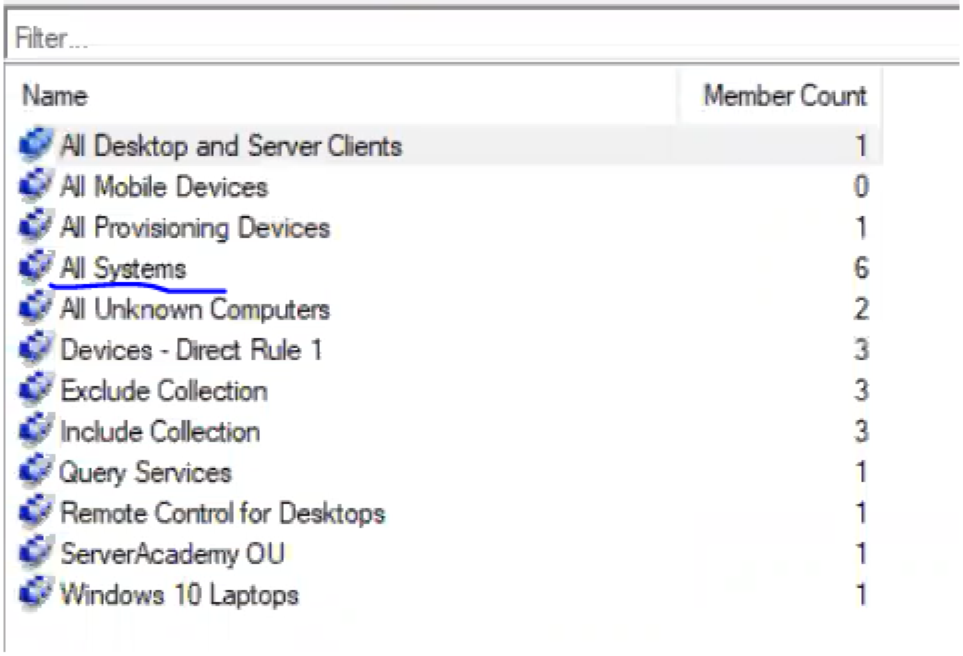
Manage Endpoint Protection client on client computers	Yes
Install Endpoint Protection client on client computers	Yes
Allow Endpoint Protection client installation and restarts outside maintenance windows. Maintenance windows must be at least 30 minutes long for client installation.	No
For Windows Embedded devices with write filters, commit Endpoint Protection client installation (requires restarts)	Yes
Suppress any required computer restarts after the Endpoint Protection client is installed	Yes
Allowed period of time users can postpone a required restart to complete the Endpoint Protection installation (hours)	24
Disable alternate sources (such as Microsoft Windows Update, Microsoft Windows Server Update Services, or UNC shares) for the initial security intelligence update on client computers	Yes



Client Settings 4 items

Search

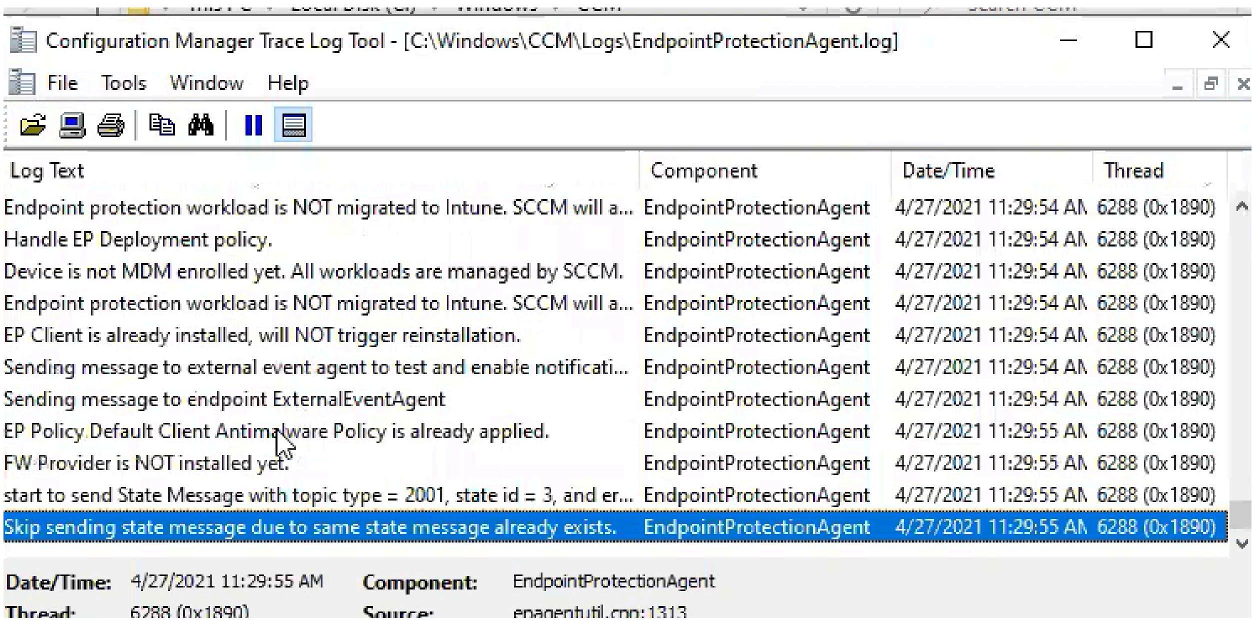
Icon	Name	Type	Priority	Depl
✓	Default Client Settings	Default	10000	0
✓	EP Client Settings	Device	3	0
✓	Pwr.Mgmt Laptops	Device	2	1
✓	Remote Desktop	Device	1	1



Filter...

Name	Member Count
All Desktop and Server Clients	1
All Mobile Devices	0
All Provisioning Devices	1
All Systems	6
All Unknown Computers	2
Devices - Direct Rule 1	3
Exclude Collection	3
Include Collection	3
Query Services	1
Remote Control for Desktops	1
ServerAcademy OU	1
Windows 10 Laptops	1

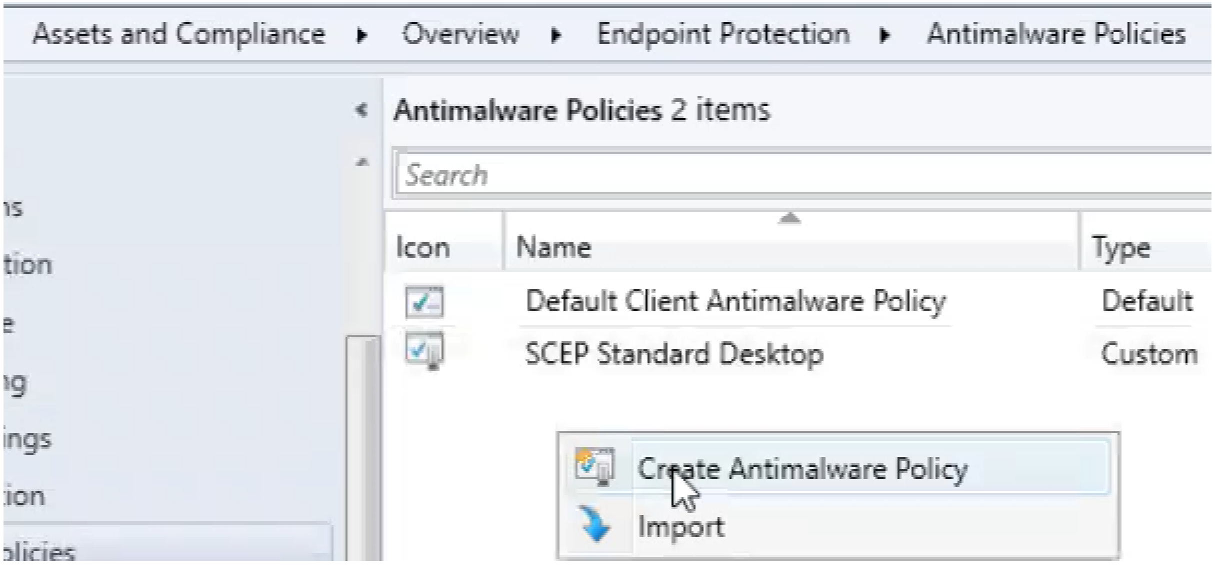
Running CMTrace on Client to Verify Policy Update


Configuration Manager Trace Log Tool - [C:\Windows\CCM\Logs\EndpointProtectionAgent.log]
File
Tools
Window
Help

Log Text	Component	Date/Time	Thread
Endpoint protection workload is NOT migrated to Intune. SCCM will a...	EndpointProtectionAgent	4/27/2021 11:29:54 AM	6288 (0x1890)
Handle EP Deployment policy.	EndpointProtectionAgent	4/27/2021 11:29:54 AM	6288 (0x1890)
Device is not MDM enrolled yet. All workloads are managed by SCCM.	EndpointProtectionAgent	4/27/2021 11:29:54 AM	6288 (0x1890)
Endpoint protection workload is NOT migrated to Intune. SCCM will a...	EndpointProtectionAgent	4/27/2021 11:29:54 AM	6288 (0x1890)
EP Client is already installed, will NOT trigger reinstallation.	EndpointProtectionAgent	4/27/2021 11:29:54 AM	6288 (0x1890)
Sending message to external event agent to test and enable notificati...	EndpointProtectionAgent	4/27/2021 11:29:54 AM	6288 (0x1890)
Sending message to endpoint ExternalEventAgent	EndpointProtectionAgent	4/27/2021 11:29:54 AM	6288 (0x1890)
EP Policy Default Client Antimalware Policy is already applied.	EndpointProtectionAgent	4/27/2021 11:29:55 AM	6288 (0x1890)
FW Provider is NOT installed yet.	EndpointProtectionAgent	4/27/2021 11:29:55 AM	6288 (0x1890)
start to send State Message with topic type = 2001, state id = 3, and er...	EndpointProtectionAgent	4/27/2021 11:29:55 AM	6288 (0x1890)
Skip sending state message due to same state message already exists.	EndpointProtectionAgent	4/27/2021 11:29:55 AM	6288 (0x1890)

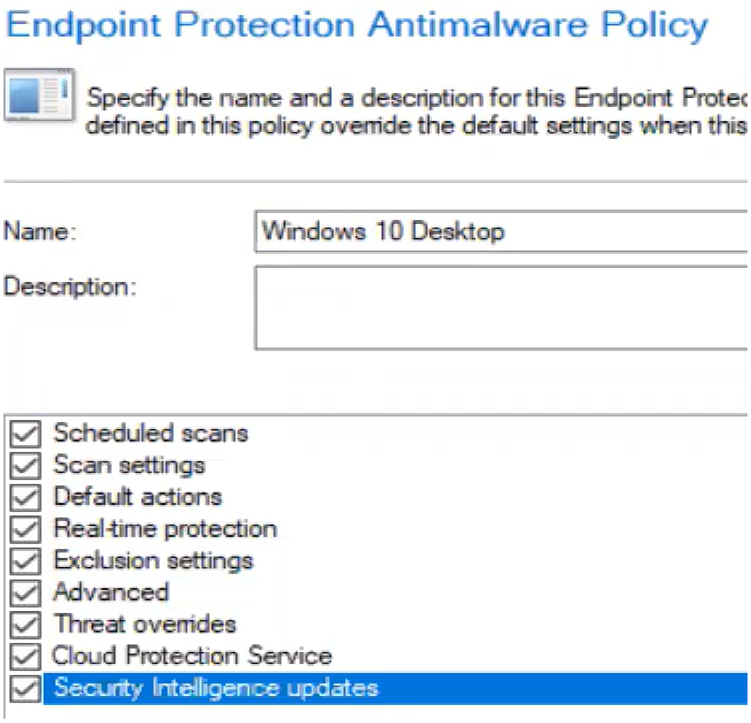
Date/Time: 4/27/2021 11:29:55 AM **Component:** EndpointProtectionAgent
Thread: 6288 (0x1890) **Source:** epagentutil.cpp:1313

Creating Windows 10 Antimalware Policy


Assets and Compliance ▸ Overview ▸ Endpoint Protection ▸ Antimalware Policies
ns
tion
e
ng
ings
ion
olicies
Search
Create Antimalware Policy
Import

Antimalware Policies 2 items

Icon	Name	Type
✓	Default Client Antimalware Policy	Default
✓	SCEP Standard Desktop	Custom



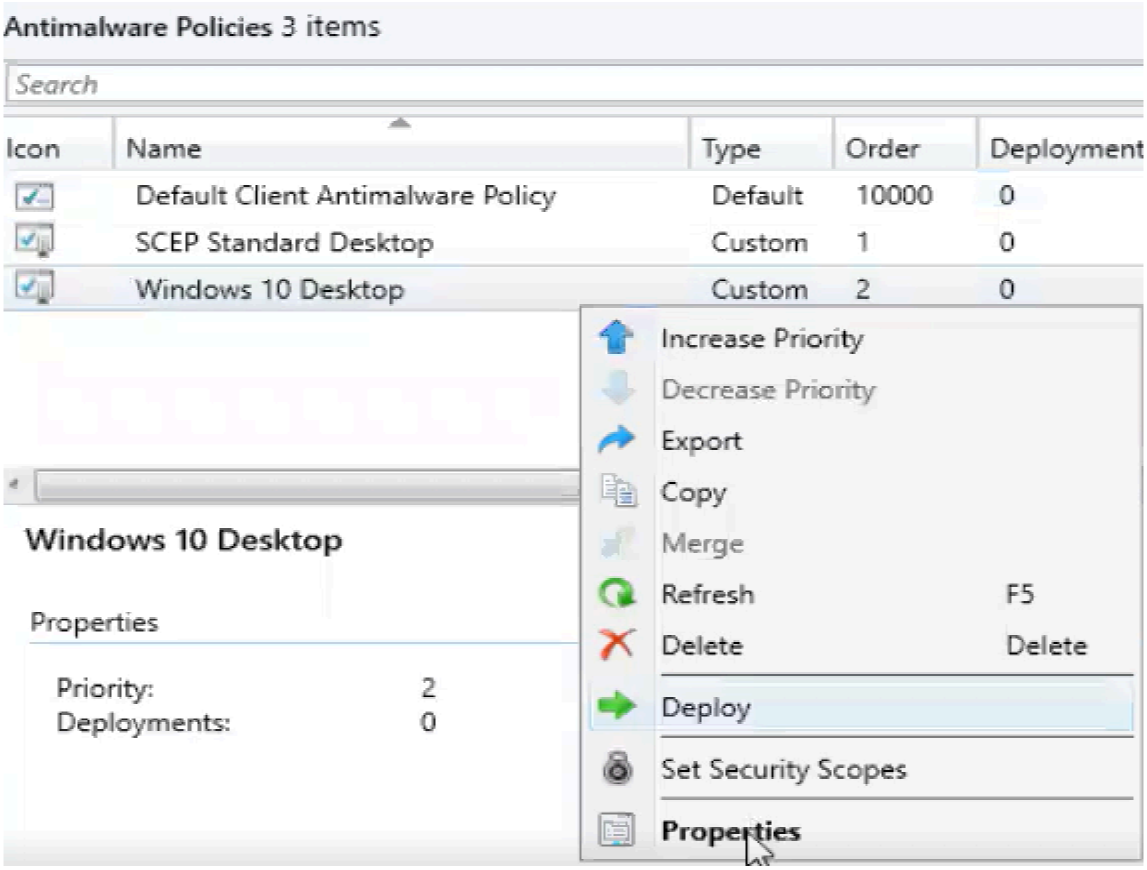
Endpoint Protection Antimalware Policy

Specify the name and a description for this Endpoint Protec
defined in this policy override the default settings when this

Name: Windows 10 Desktop

Description:

- ☑ Scheduled scans
- ☑ Scan settings
- ☑ Default actions
- ☑ Real-time protection
- ☑ Exclusion settings
- ☑ Advanced
- ☑ Threat overrides
- ☑ Cloud Protection Service
- ☑ Security Intelligence updates



Antimalware Policies 3 items

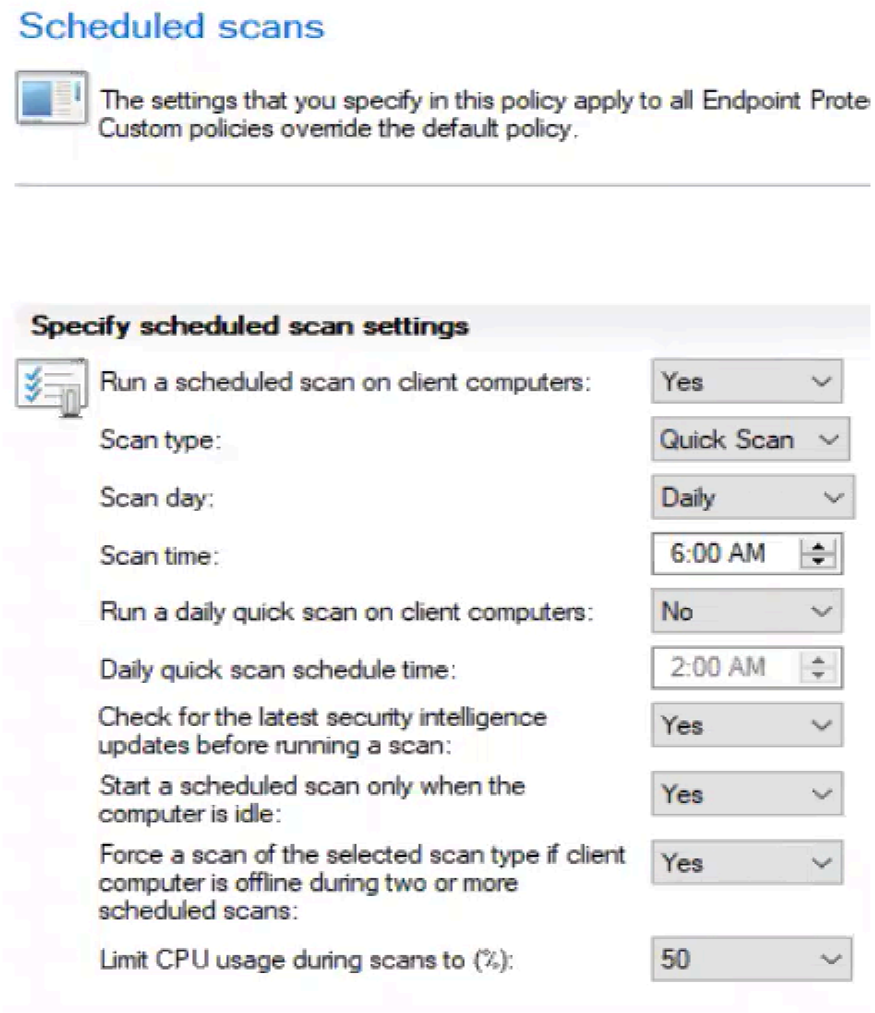
Search

Icon	Name	Type	Order	Deployment
✓	Default Client Antimalware Policy	Default	10000	0
✓	SCEP Standard Desktop	Custom	1	0
✓	Windows 10 Desktop	Custom	2	0

Windows 10 Desktop

Properties

Priority: 2
Deployments: 0

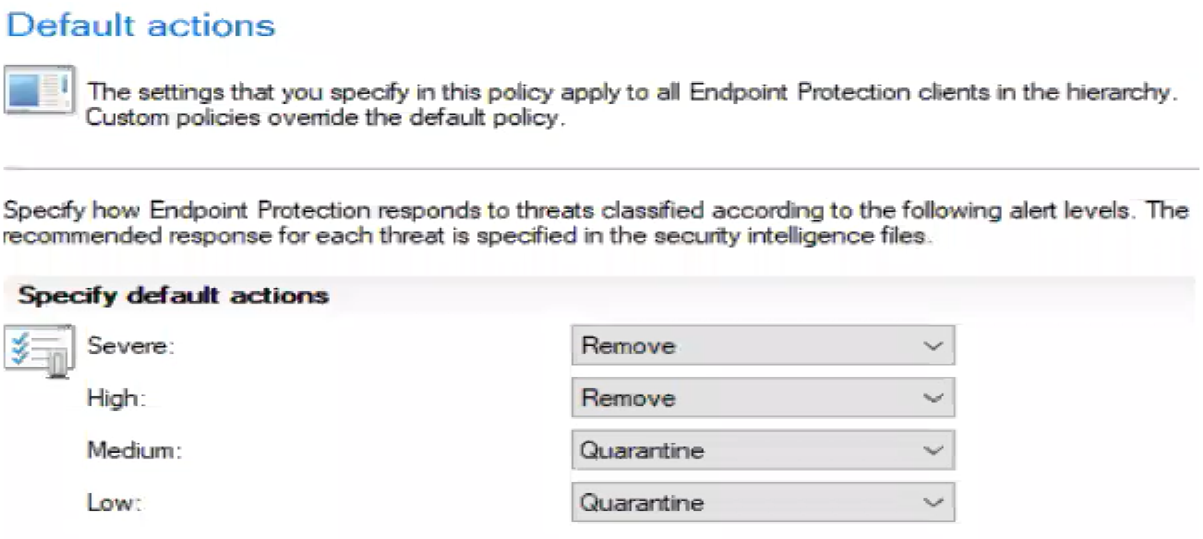


Scheduled scans

The settings that you specify in this policy apply to all Endpoint Prote
Custom policies override the default policy.

Specify scheduled scan settings

Run a scheduled scan on client computers:	Yes
Scan type:	Quick Scan
Scan day:	Daily
Scan time:	6:00 AM
Run a daily quick scan on client computers:	No
Daily quick scan schedule time:	2:00 AM
Check for the latest security intelligence updates before running a scan:	Yes
Start a scheduled scan only when the computer is idle:	Yes
Force a scan of the selected scan type if client computer is offline during two or more scheduled scans:	Yes
Limit CPU usage during scans to (%):	50



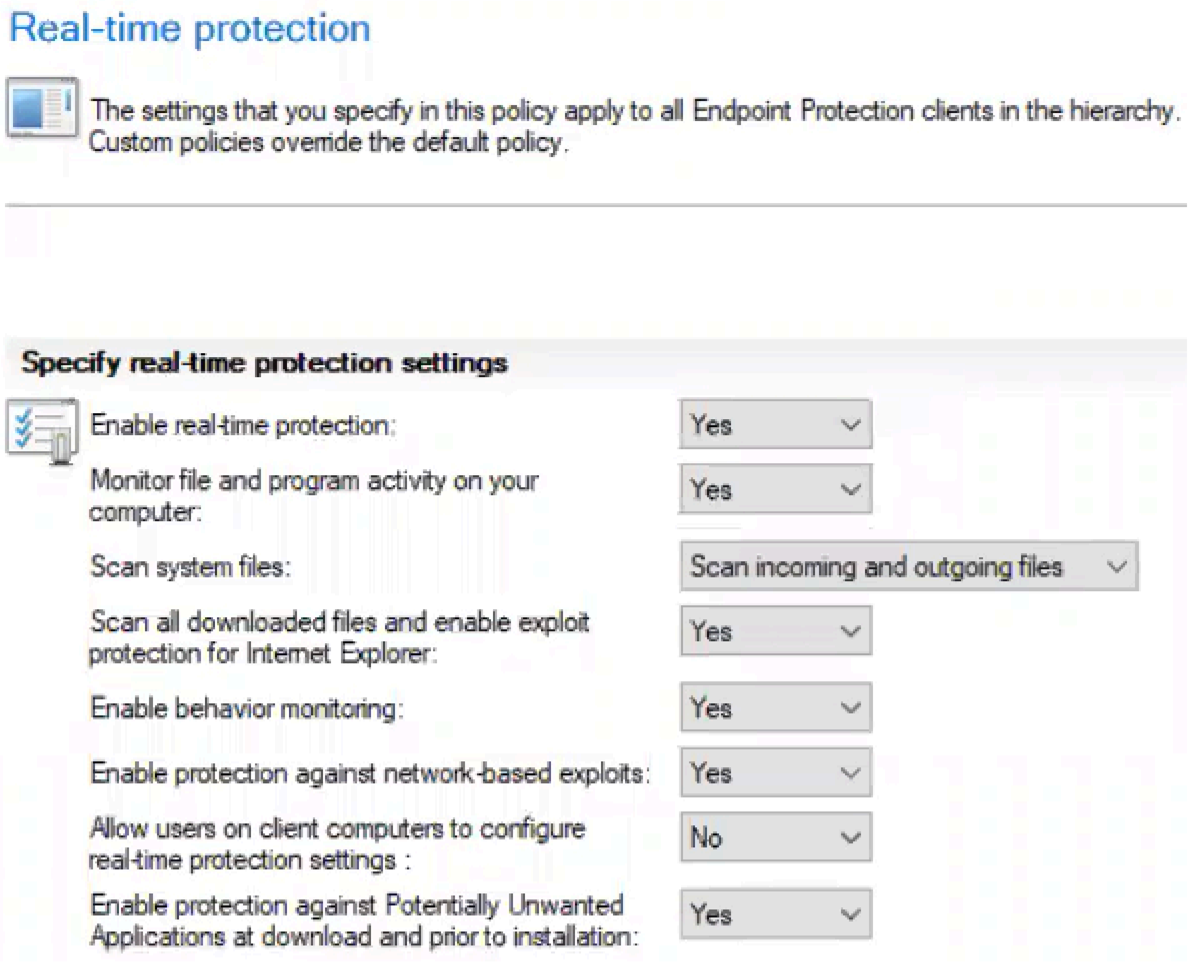
Default actions

The settings that you specify in this policy apply to all Endpoint Protection clients in the hierarchy. Custom policies override the default policy.

Specify how Endpoint Protection responds to threats classified according to the following alert levels. The recommended response for each threat is specified in the security intelligence files.

Specify default actions

Severe:	Remove
High:	Remove
Medium:	Quarantine
Low:	Quarantine

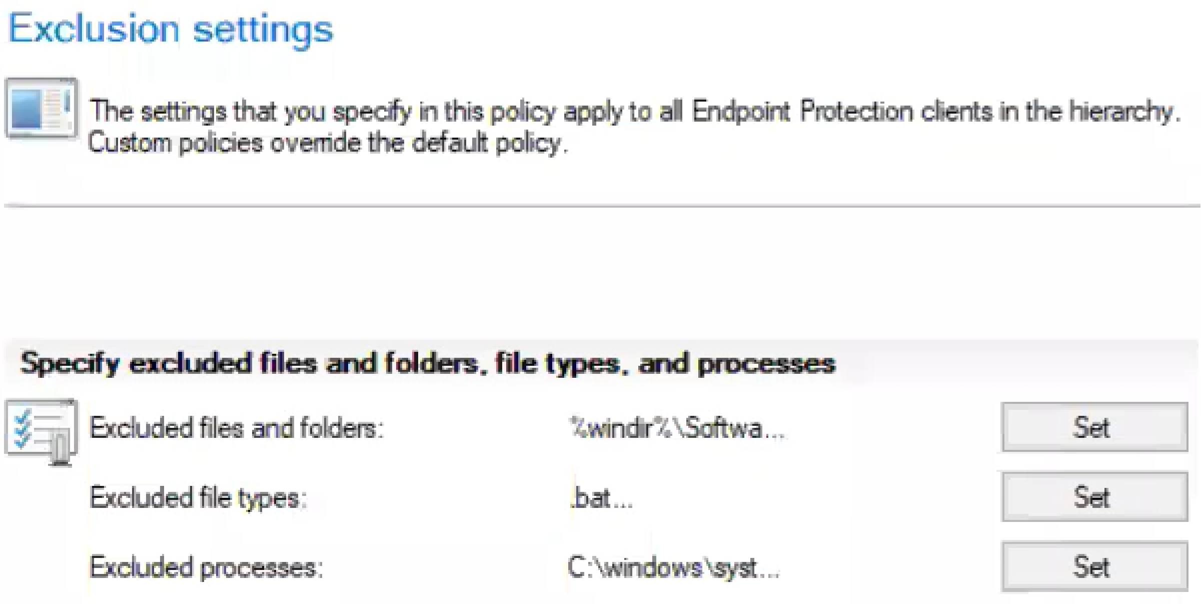


Real-time protection

The settings that you specify in this policy apply to all Endpoint Protection clients in the hierarchy. Custom policies override the default policy.

Specify real-time protection settings

Enable real-time protection:	Yes
Monitor file and program activity on your computer:	Yes
Scan system files:	Scan incoming and outgoing files
Scan all downloaded files and enable exploit protection for Internet Explorer:	Yes
Enable behavior monitoring:	Yes
Enable protection against network-based exploits:	Yes
Allow users on client computers to configure real-time protection settings :	No
Enable protection against Potentially Unwanted Applications at download and prior to installation:	Yes

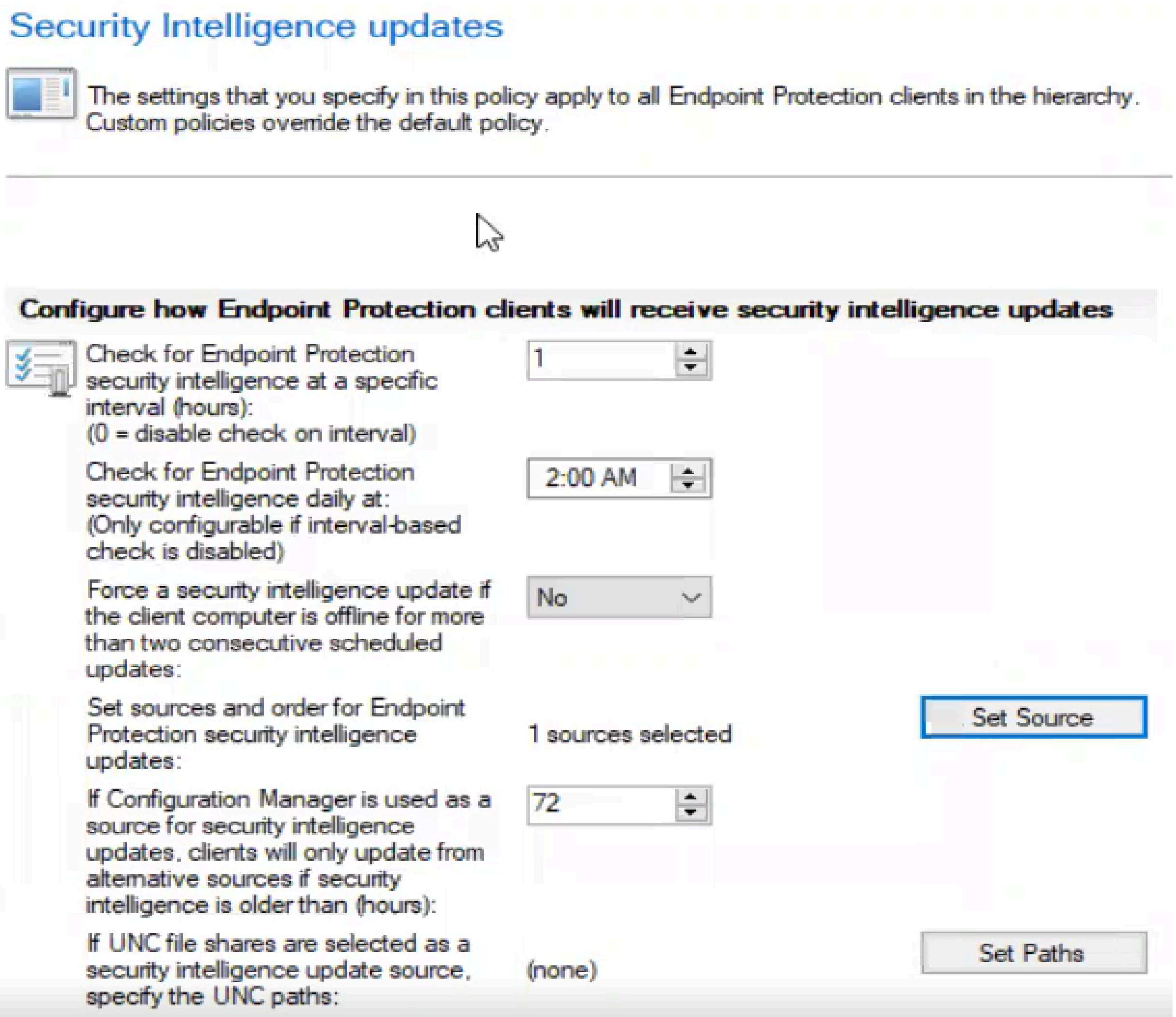


Exclusion settings

The settings that you specify in this policy apply to all Endpoint Protection clients in the hierarchy. Custom policies override the default policy.

Specify excluded files and folders, file types, and processes

Excluded files and folders:	%windir%\Softwa...	Set
Excluded file types:	.bat...	Set
Excluded processes:	C:\windows\syst...	Set

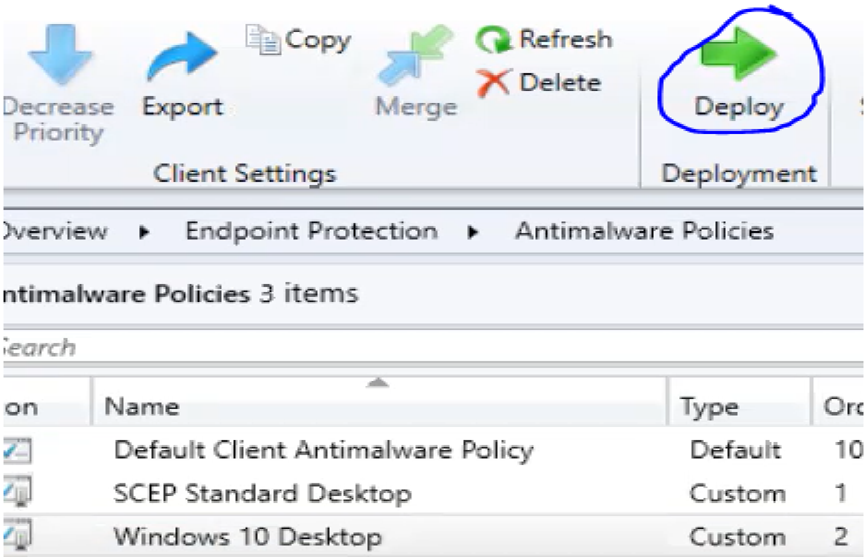


Security Intelligence updates

The settings that you specify in this policy apply to all Endpoint Protection clients in the hierarchy. Custom policies override the default policy.

Configure how Endpoint Protection clients will receive security intelligence updates

Check for Endpoint Protection security intelligence at a specific interval (hours): (0 = disable check on interval)	1	
Check for Endpoint Protection security intelligence daily at: (Only configurable if interval-based check is disabled)	2:00 AM	
Force a security intelligence update if the client computer is offline for more than two consecutive scheduled updates:	No	
Set sources and order for Endpoint Protection security intelligence updates:	1 sources selected	Set Source
If Configuration Manager is used as a source for security intelligence updates, clients will only update from alternative sources if security intelligence is older than (hours):	72	
If UNC file shares are selected as a security intelligence update source, specify the UNC paths:	(none)	Set Paths



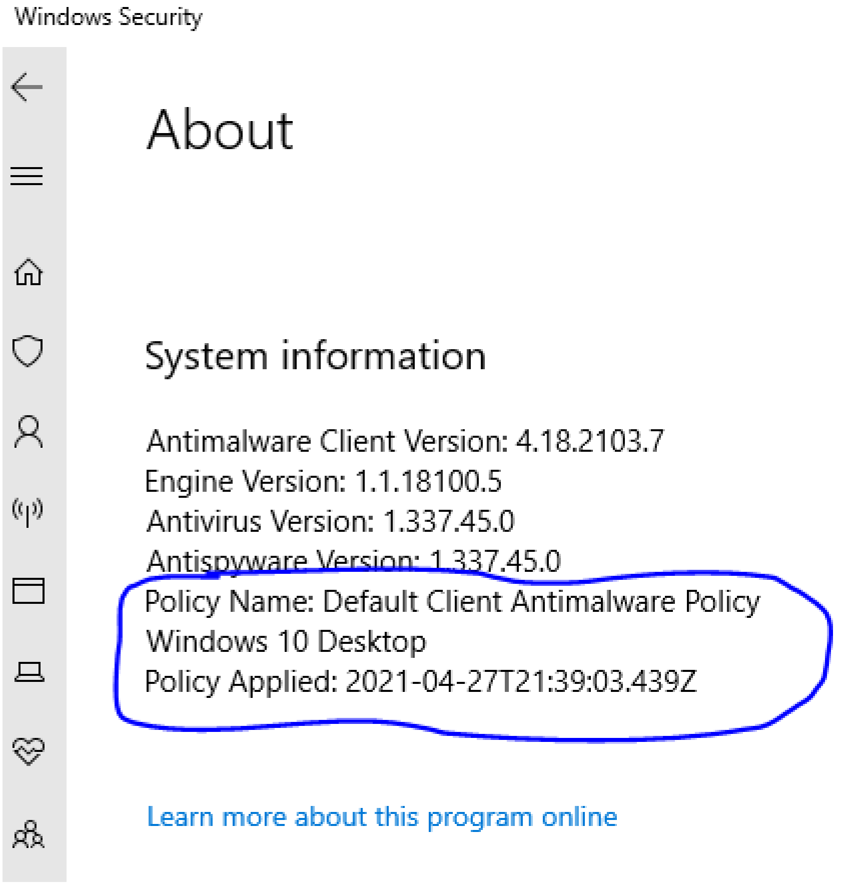
Overview ▸ Endpoint Protection ▸ Antimalware Policies

ntimalware Policies 3 items

earch

on	Name	Type	Orc
	Default Client Antimalware Policy	Default	10
	SCEP Standard Desktop	Custom	1
	Windows 10 Desktop	Custom	2

Verifying Applied Policies on Client

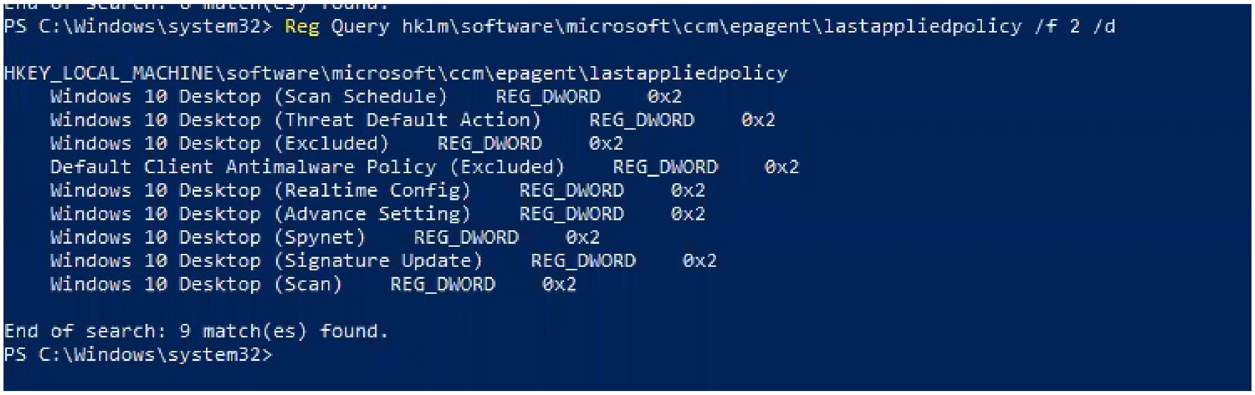


About

System information

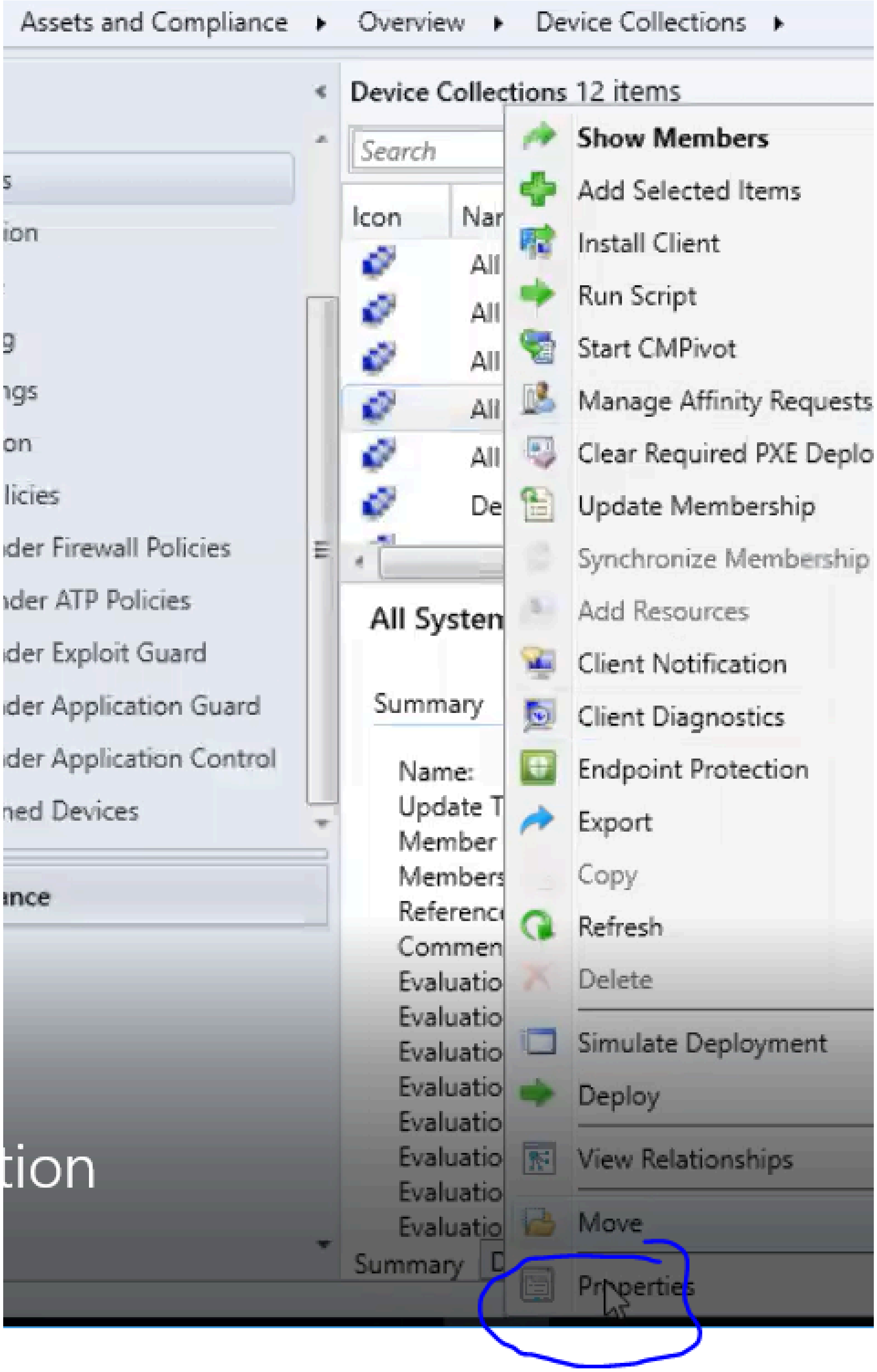
Antimalware Client Version: 4.18.2103.7
Engine Version: 1.1.18100.5
Antivirus Version: 1.337.45.0
Antispyware Version: 1.337.45.0
Policy Name: Default Client Antimalware Policy
Windows 10 Desktop
Policy Applied: 2021-04-27T21:39:03.439Z

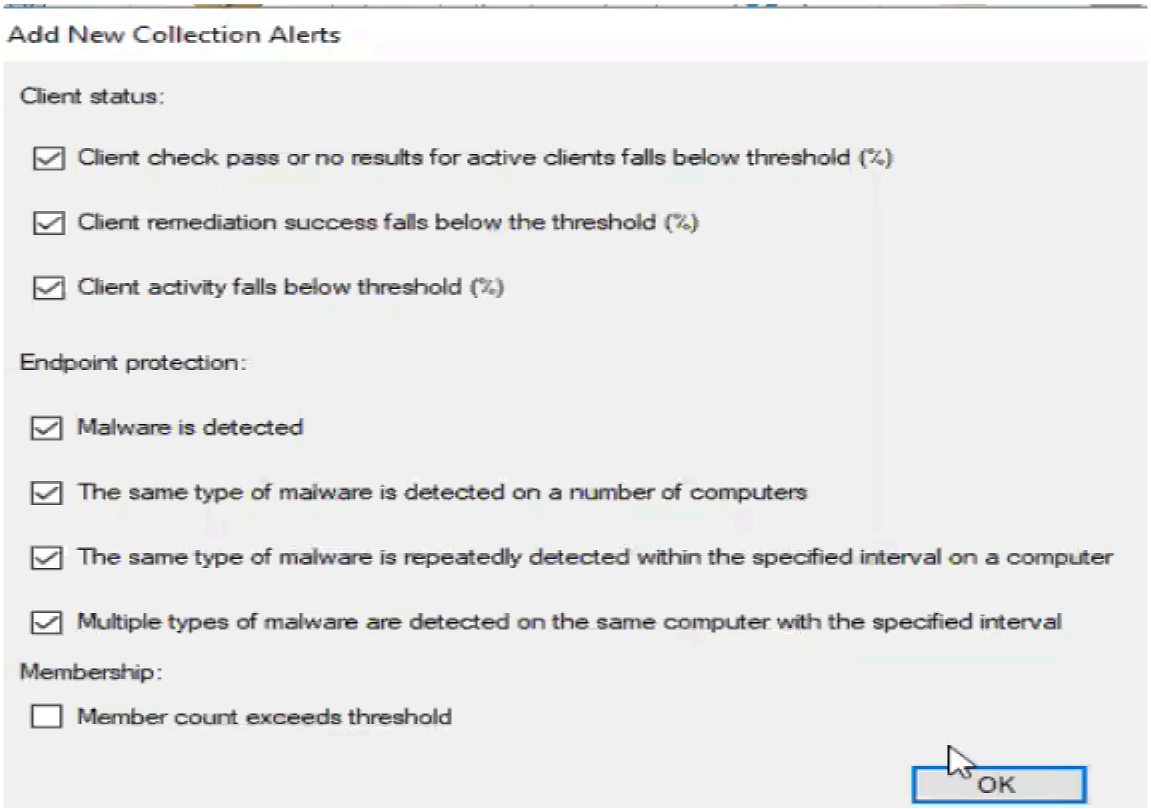
Learn more about this program online



```
End of search: 0 match(es) found.
PS C:\Windows\system32> Reg Query hklm\software\microsoft\ccm\epagent\lastappliedpolicy /f 2 /d

HKEY_LOCAL_MACHINE\software\microsoft\ccm\epagent\lastappliedpolicy
    Windows 10 Desktop (Scan Schedule)    REG_DWORD    0x2
    Windows 10 Desktop (Threat Default Action)    REG_DWORD    0x2
    Windows 10 Desktop (Excluded)    REG_DWORD    0x2
    Default Client Antimalware Policy (Excluded)    REG_DWORD    0x2
    Windows 10 Desktop (Realtime Config)    REG_DWORD    0x2
    Windows 10 Desktop (Advance Setting)    REG_DWORD    0x2
    Windows 10 Desktop (Spynet)    REG_DWORD    0x2
    Windows 10 Desktop (Signature Update)    REG_DWORD    0x2
    Windows 10 Desktop (Scan)    REG_DWORD    0x2

End of search: 9 match(es) found.
PS C:\Windows\system32>
```

Managing Alerts on All Systems





Add New Collection Alerts

Client status:

☑ Client check pass or no results for active clients falls below threshold (%)

☑ Client remediation success falls below the threshold (%)

☑ Client activity falls below threshold (%)

Endpoint protection:

☑ Malware is detected

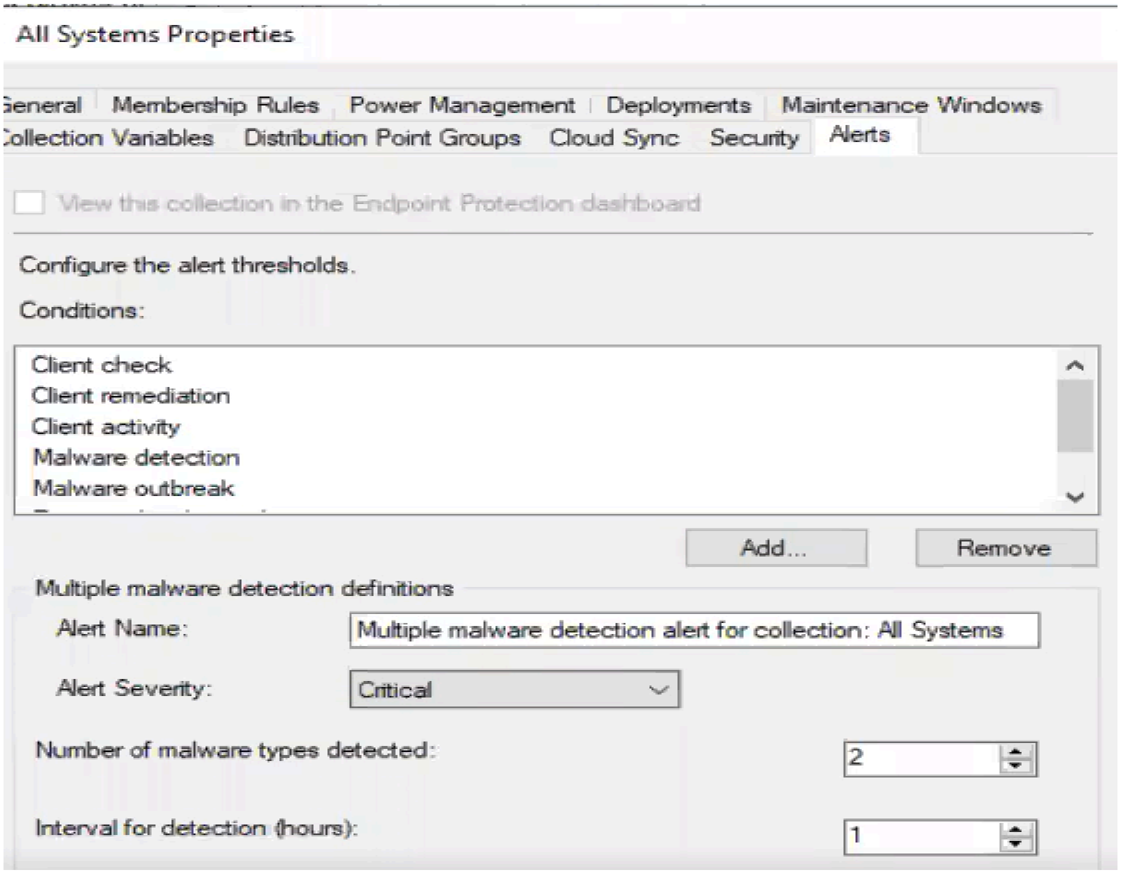
☑ The same type of malware is detected on a number of computers

☑ The same type of malware is repeatedly detected within the specified interval on a computer

☑ Multiple types of malware are detected on the same computer with the specified interval

Membership:

□ Member count exceeds threshold



All Systems Properties

□ View this collection in the Endpoint Protection dashboard

Configure the alert thresholds.

Conditions:

Client check
Client remediation
Client activity
Malware detection
Malware outbreak

Multiple malware detection definitions

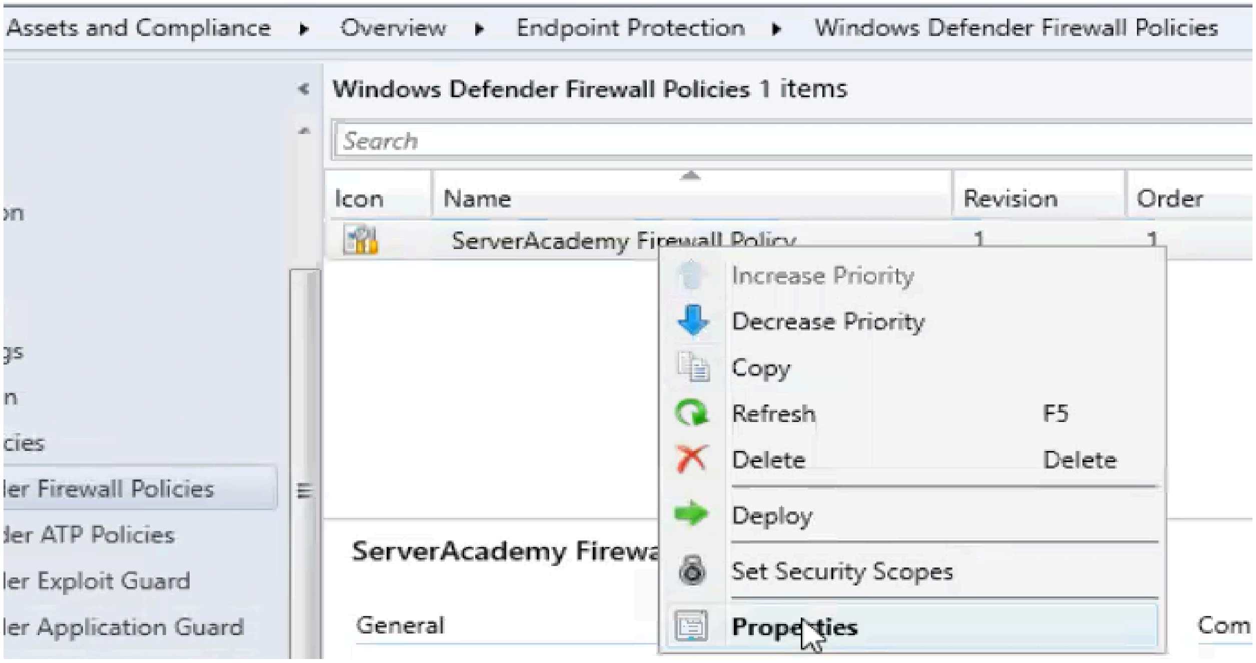
Alert Name: Multiple malware detection alert for collection: All Systems

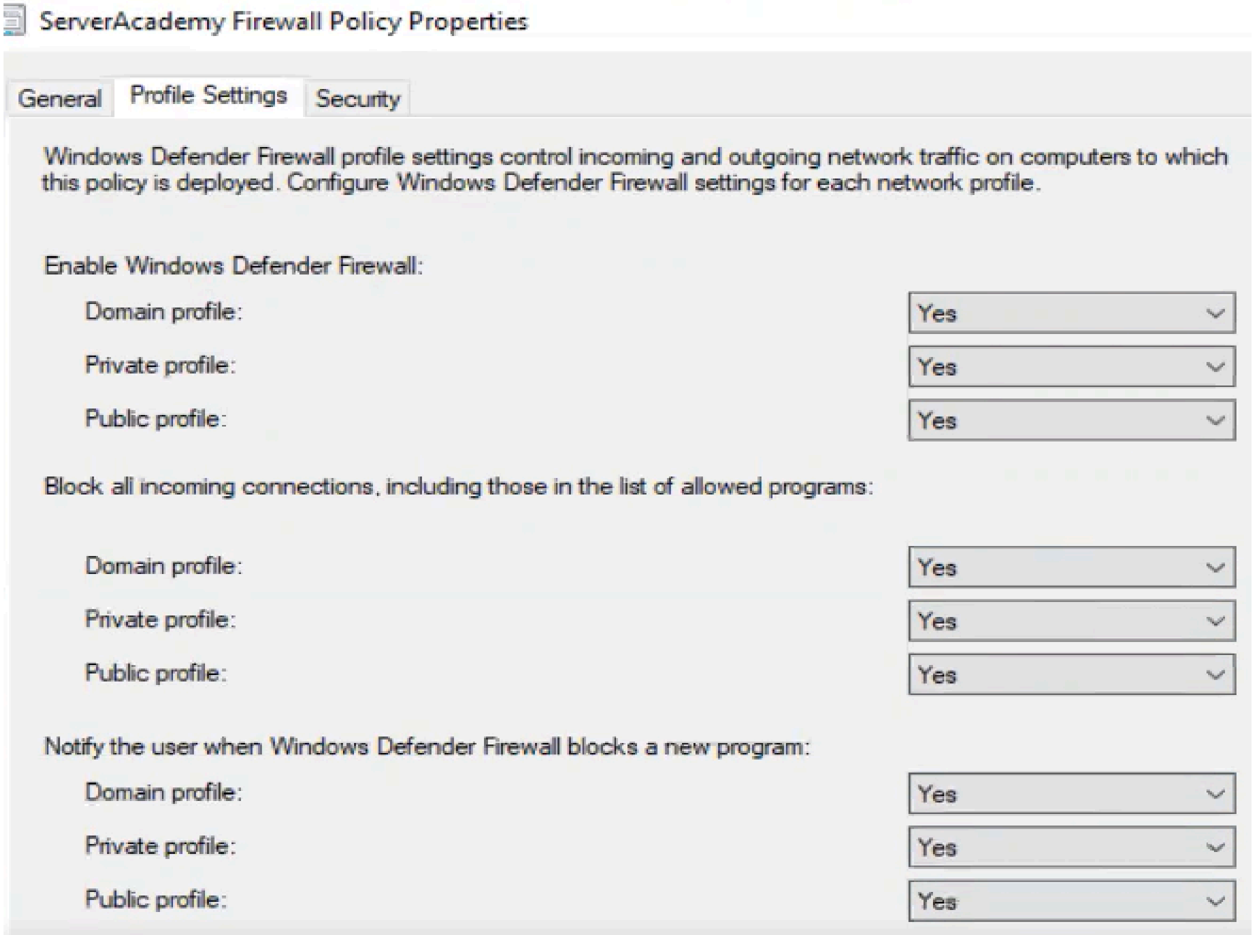
Alert Severity: Critical

Number of malware types detected: 2

Interval for detection (hours): 1

Reconfiguring Firewall Policy




ServerAcademy Firewall Policy Properties

General | Profile Settings | Security

Windows Defender Firewall profile settings control incoming and outgoing network traffic on computers to which this policy is deployed. Configure Windows Defender Firewall settings for each network profile.

Enable Windows Defender Firewall:

Domain profile:	Yes
Private profile:	Yes
Public profile:	Yes

Block all incoming connections, including those in the list of allowed programs:

Domain profile:	Yes
Private profile:	Yes
Public profile:	Yes

Notify the user when Windows Defender Firewall blocks a new program:

Domain profile:	Yes
Private profile:	Yes
Public profile:	Yes

!!

!!

!!SCCM SERVER CONFIGURATION ENDS HERE!!

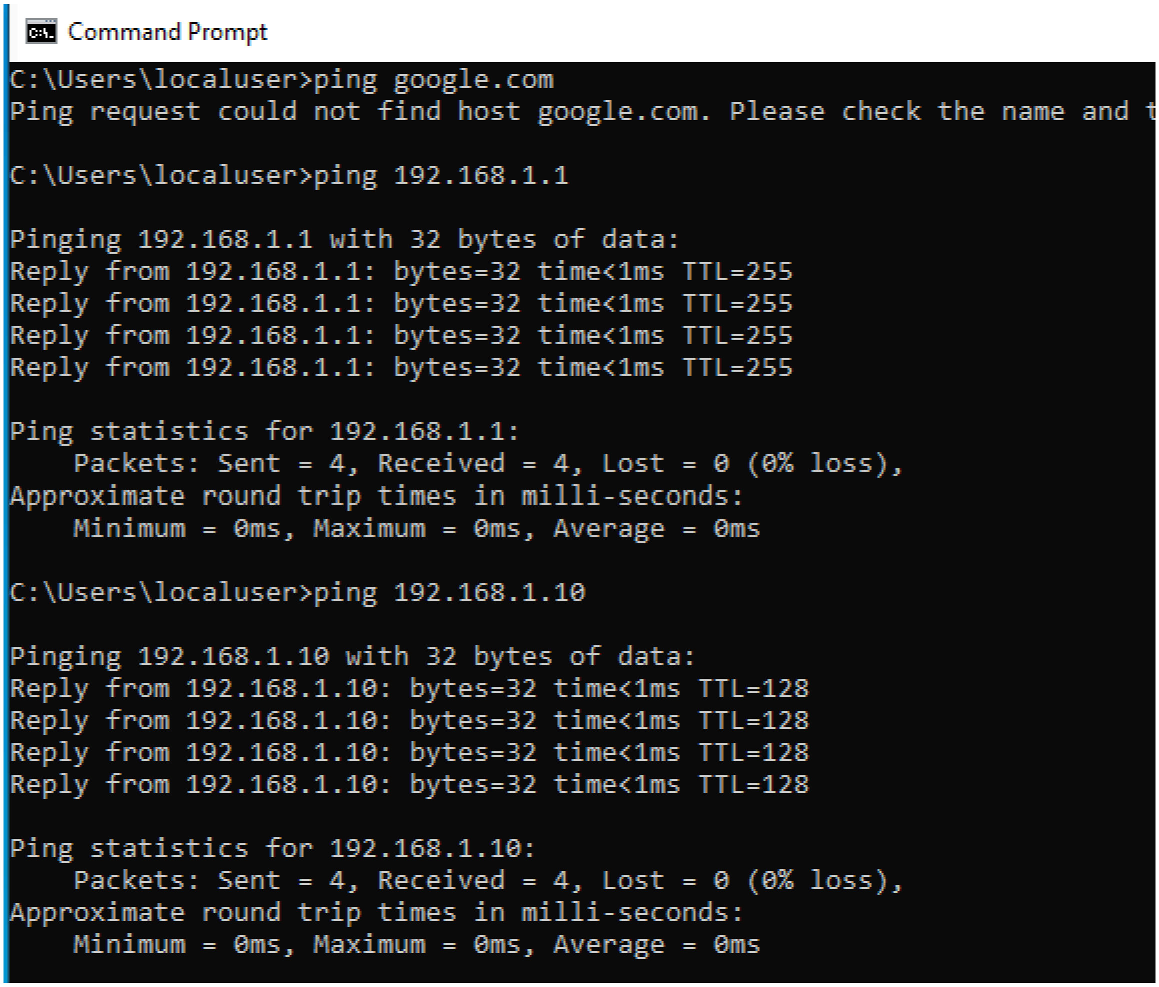
!!

!!

!!

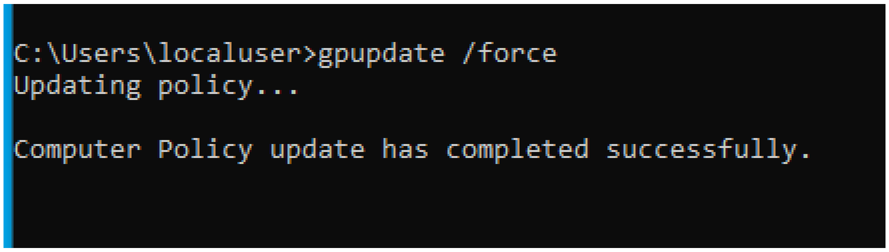
SAW01 Client Machine Configuration

Testing connection to gateway and Domain Controller



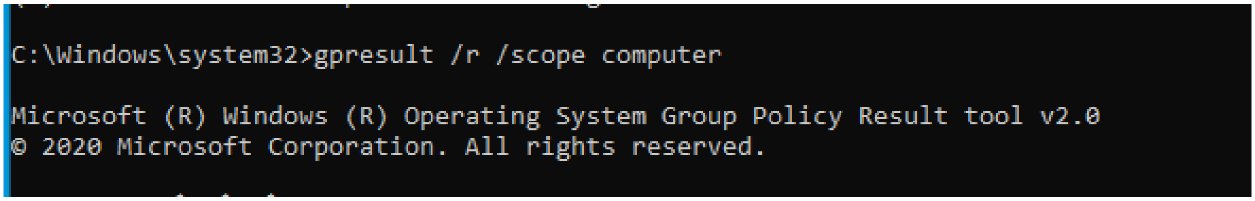
```
C:\Users\localuser>ping google.com
Ping request could not find host google.com. Please check the name and t

C:\Users\localuser>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\localuser>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:
Reply from 192.168.1.10: bytes=32 time<1ms TTL=128
Reply from 192.168.1.10: bytes=32 time<1ms TTL=128
Reply from 192.168.1.10: bytes=32 time<1ms TTL=128
Reply from 192.168.1.10: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Performing a Group Policy Update for any changes made in the group policy

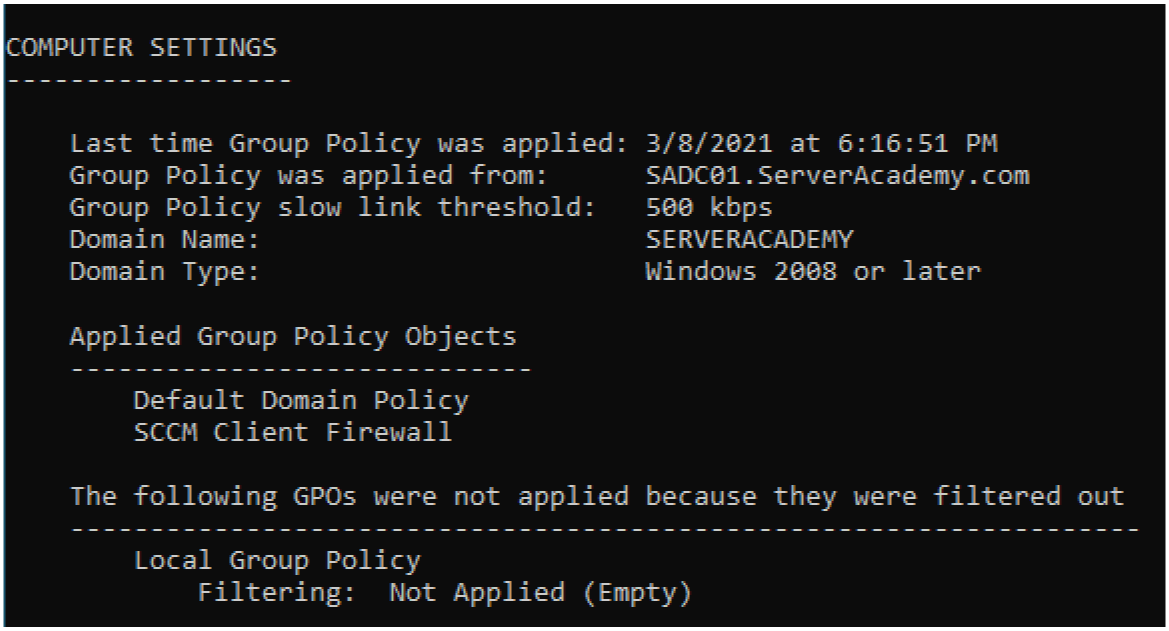


```
C:\Users\localuser>gpupdate /force
Updating policy...

Computer Policy update has completed successfully.
```

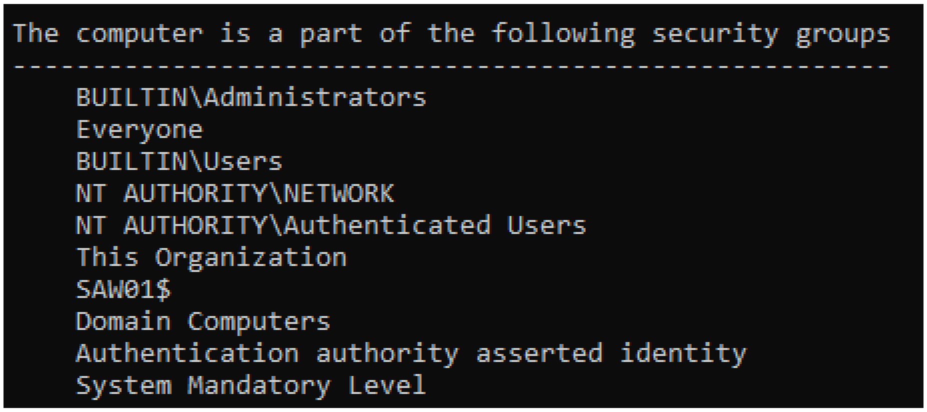
Verifying results of gpupdate



```
C:\Windows\system32>gpresult /r /scope computer

Microsoft (R) Windows (R) Operating System Group Policy Result tool v2.0
© 2020 Microsoft Corporation. All rights reserved.
```



```
COMPUTER SETTINGS
------------------

    Last time Group Policy was applied: 3/8/2021 at 6:16:51 PM
    Group Policy was applied from:      SADC01.ServerAcademy.com
    Group Policy slow link threshold:   500 kbps
    Domain Name:                        SERVERACADEMY
    Domain Type:                        Windows 2008 or later

    Applied Group Policy Objects
    -----------------------------
        Default Domain Policy
        SCCM Client Firewall

    The following GPOs were not applied because they were filtered out
    -------------------------------------------------------------------
        Local Group Policy
            Filtering:  Not Applied (Empty)
```



```
The computer is a part of the following security groups
-------------------------------------------------------
    BUILTIN\Administrators
    Everyone
    BUILTIN\Users
    NT AUTHORITY\NETWORK
    NT AUTHORITY\Authenticated Users
    This Organization
    SAW01$
    Domain Computers
    Authentication authority asserted identity
    System Mandatory Level
```