

Deploy WDAC USING SCCM

Contents

Supported WDAC Policies	2
WDAC limitations with managed installer	2
Deploy WDAC policy using SCCM.....	3
Create Device Collection	3
Create WDAC Policy	21
Deploy WDAC Policy to Device Collection.....	28

Windows Defender Application Control is designed to protect devices against malware and other untrusted software. It prevents malicious code from running by ensuring that only approved code, that you know, can be run.

Application Control is a software-based security layer that enforces an explicit list of software that is allowed to run on a PC. On its own, Application Control doesn't have any hardware or firmware prerequisites. Application Control policies deployed with Configuration Manager enable a policy on devices in targeted collections that meet the minimum Windows version and SKU requirements outlined in this article. Optionally, hypervisor-based protection of Application Control policies deployed through Configuration Manager can be enabled through group policy on capable hardware.

You can use Configuration Manager to deploy an Application Control policy. This policy lets you configure the mode in which Application Control runs on devices in a collection.

You can configure one of the following modes:

- **Enforcement enabled** - Only trusted executables are allowed to run.
- **Audit only** - Allow all executables to run, but log untrusted executables that run in the local client event log.

Supported WDAC Policies in SCCM

Deploying WDAC policy using SCCM only supports the following rule types:

- **Managed Installer** – When a policy is created using SCCM, SCCM will be registered as a “Managed Installer”. This means any application deployed using SCCM will be allowed to run
- **File** – Any executable selected during the policy creation will be allowed to run
- **Folder** – Any executable running in the selected folder will be allowed to run

Since managed installer is a heuristic-based mechanism, it doesn't provide the same security guarantees that explicit allow or deny rules do. The managed installer is best suited for use where each user operates as a standard non-administrative user and where all software is deployed and installed by a software distribution solution, such as SCCM.

Users with administrator privileges, or malware running as an administrator user on the system, may be able to circumvent the intent of Windows Defender Application Control when the managed installer option is allowed.

If a managed installer process runs in the context of a user with standard privileges, then it's possible that standard users or malware running as standard user may be able to circumvent the intent of Windows Defender Application Control.

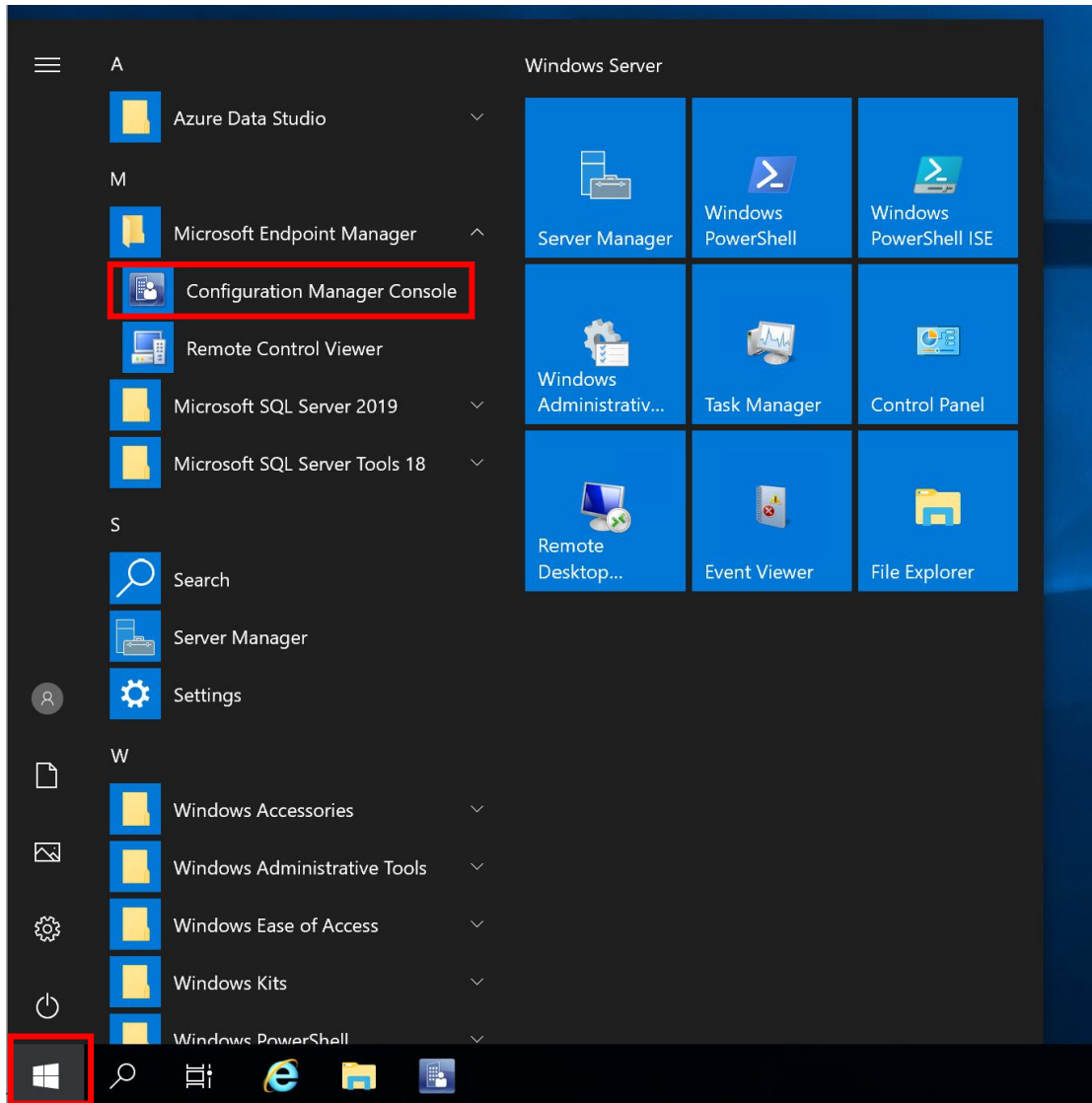
WDAC limitations with managed installer

- WDAC policies, based on managed installer, doesn't support applications that self-update. An application that self-updates is an application that updates its self outside of the managed installer process such as an update pushed through SCCM. If an application that was deployed by a managed installer later updates itself, the updated application files won't include the origin information from the managed installer, and they might not be able to run. When you rely on managed installers, you must deploy and install all application updates by using a managed installer, or update the WDAC policy rules to authorize the newly updated app to run.
- Packaged apps (MSIX) deployed through a managed installer aren't tracked by the managed installer and will need to be separately authorized in your WDAC policy.
- Some applications or installers may extract, download, or generate binaries and immediately attempt to run them. Files run by such a process may not be allowed by the managed installer. In some cases, it may be possible to also designate an application binary that performs such an operation as a managed installer.
- The managed installer heuristic doesn't authorize kernel drivers. The WDAC policy must be updated to have rules that allow the necessary drivers to run or a supplemental policy must be created

Deploy WDAC policy using SCCM

Create Device Collection

1. Log into the Primary Site system
2. Open the



3. In the bottom left select **Assets and Compliance** → **Device Collections** → **Right click** → **Create Device Collection**

Home Folder

Create Device Collection Import Collections Manage Device Categories Saved Searches

Create Categories Search

Assets and Compliance Overview Device Collections

Assets and Compliance

- Overview
- Users
- Devices
- User Collections
- Device Collections**
- User State Migration
- Asset Intelligence
- Software Metering
- Compliance Settings
- Endpoint Protection
- All Corporate-owned Devices

Device Collections 6 items

Icon	Name	Limiting Collection	Member Cou
	All Desktop and Server Clients	All Systems	1
	All Mobile Devices	All Systems	0
	All Provisioning Devices	All Systems	1
	All Systems		7
	All Unknown Computers	All Systems	2
	Co-management Eligible Devices	All Systems	1

Create Device Collection Import Collections Manage Device Categories Folder

Assets and Compliance Software Library Monitoring Administration

4. Enter a **Name** → **Browse**

Create Device Collection Wizard

General

General

Membership Rules

Summary

Progress

Completion

Specify details for this collection

Name: DART-EP-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.

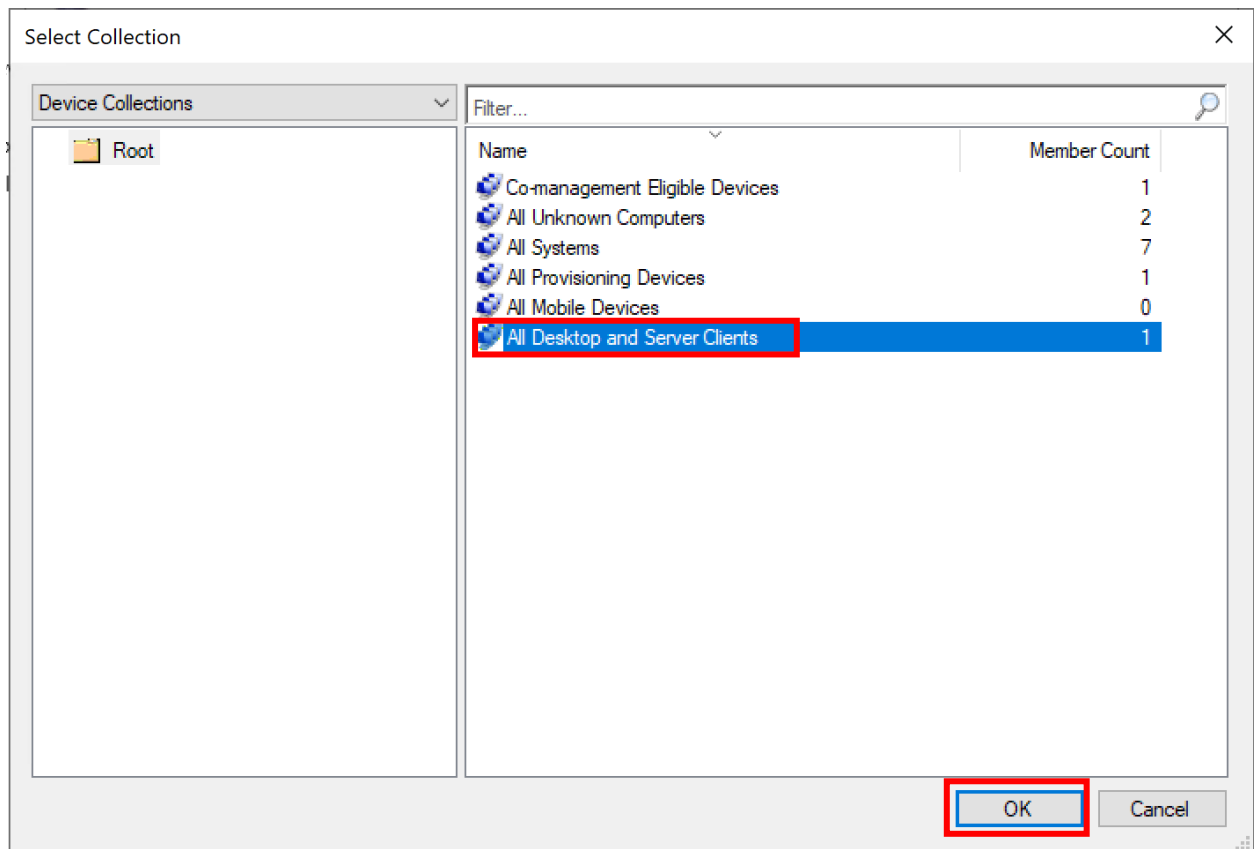
Limiting collection: Browse...

Last update
The collection has not been updated yet.

Last membership change
The collection has not been updated yet.

< Previous Next > Summary Cancel

5. Select **All Desktop and Server Clients** →



6. Select **Next**



General



General

Membership Rules

Summary

Progress

Completion

Specify details for this collection

Name:

DART-EP-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 Desktop and Server Clients

Browse...

Last update

The collection has not been updated yet.

Last membership change

The collection has not been updated yet.

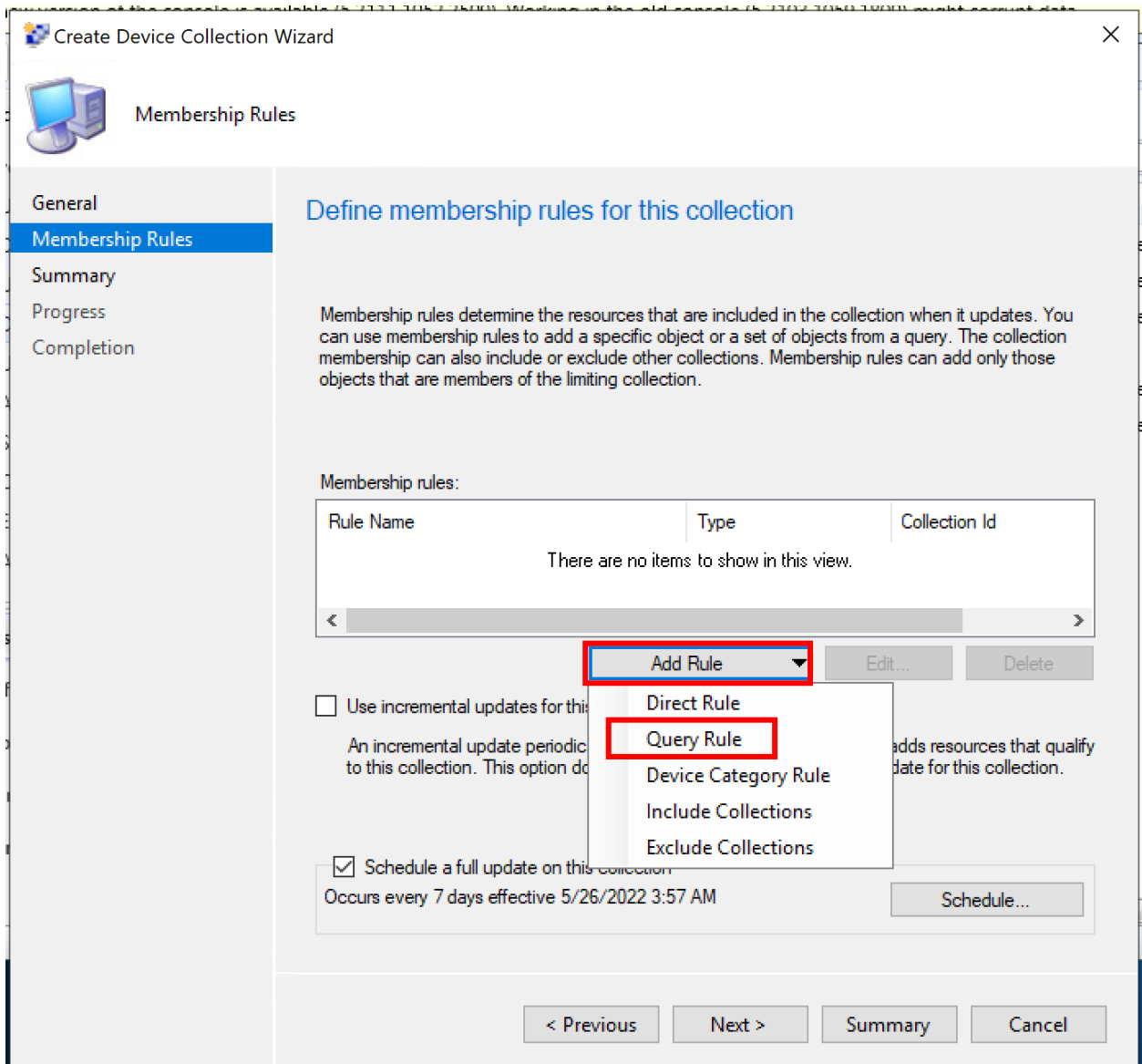
< Previous

Next >

Summary

Cancel

7. Select **Add Rule** → **Query Rule**



8. Enter a query name
9. Select **Edit Query Statement**

Query Rule Properties

General

Name: DART-Endpoint-Clients

Import Query Statement...

Resource class: System Resource

Edit Query Statement...

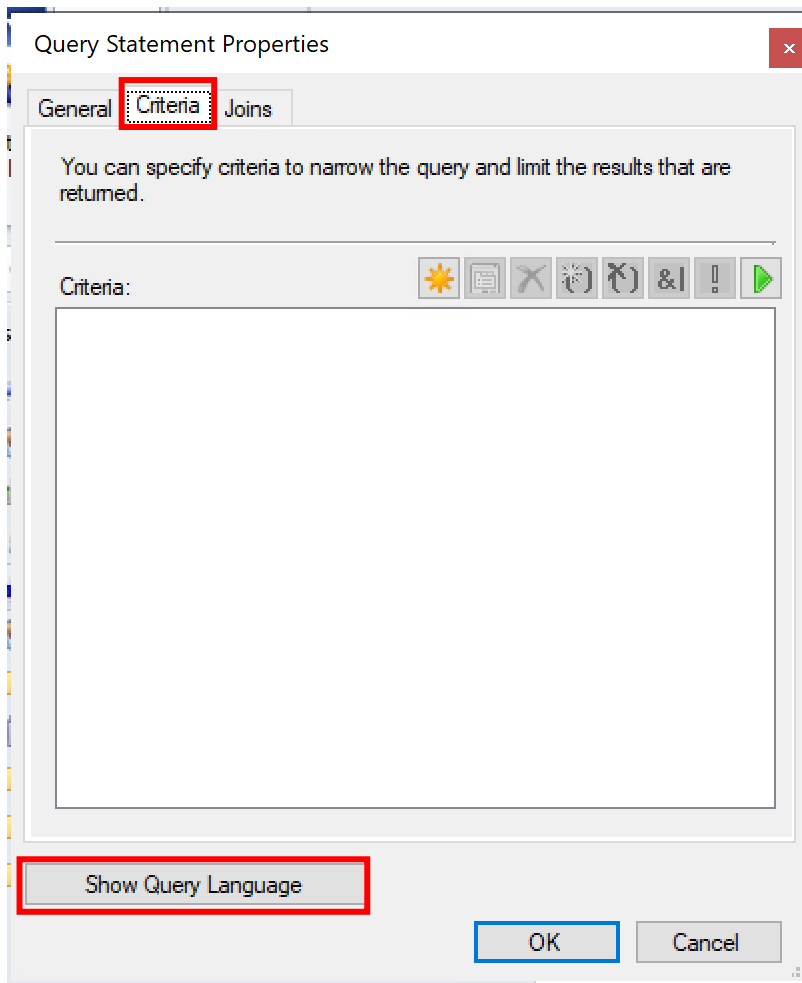
Query Statement:

```
Select * from  
SMS_R_System
```

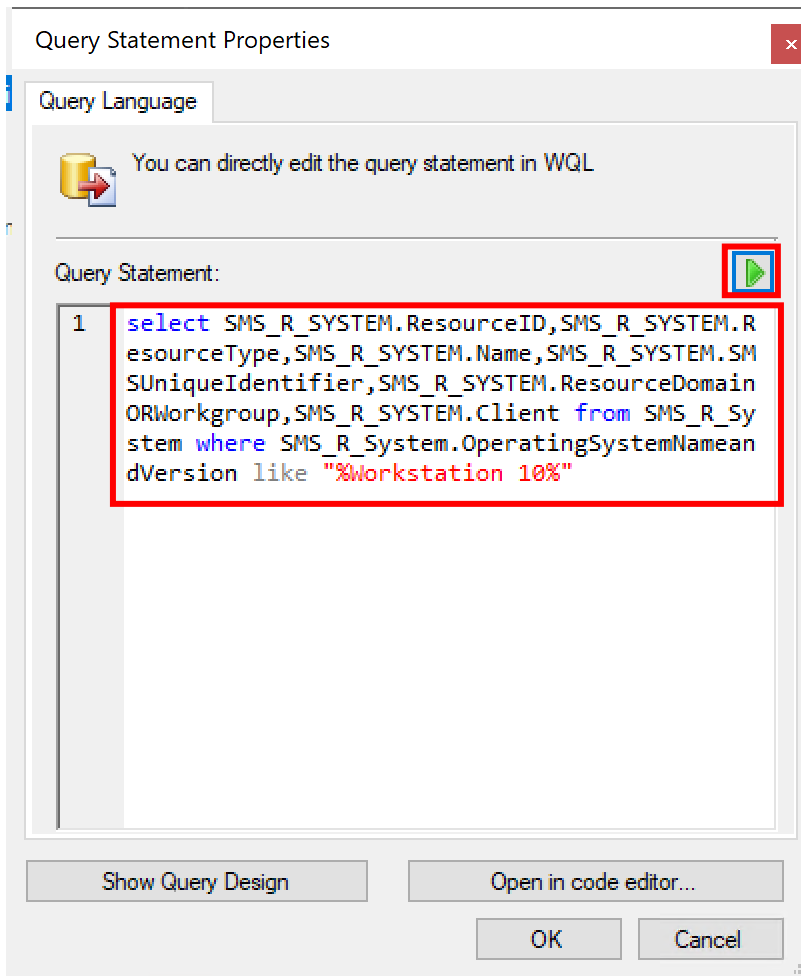
Configuration Manager uses the Windows Management Instrumentation (WMI) Query Language (WQL) to query the site database.

OK Cancel

10. Select **Criteria** → **Show Query Language**



11. Cut and paste the following queries depending on the Operating system using the examples below. Use the ledger below to determine which query is best for you.
12. Select the **Green** triangle. Clicking the **Green** triangle will cause the query to run and return results



Example query 1 - Windows 11 ONLY

```
select
SMS_R_SYSTEM.ResourceID,SMS_R_SYSTEM.ResourceType,SMS_R_SYSTEM.Name,SMS_R_SYSTEM.
SMSUniqueIdentifier,SMS_R_SYSTEM.ResourceDomainORWorkgroup,SMS_R_SYSTEM.Client from
SMS_R_System inner join SMS_G_System_OPERATING_SYSTEM on
SMS_G_System_OPERATING_SYSTEM.ResourceID = SMS_R_System.ResourceId where
SMS_G_System_OPERATING_SYSTEM.Name like "%Microsoft Windows 11 Enterprise%"
```

Example query 2 - Windows 10 ONLY

```
select
SMS_R_SYSTEM.ResourceID,SMS_R_SYSTEM.ResourceType,SMS_R_SYSTEM.Name,SMS_R_SYSTEM.
SMSUniqueIdentifier,SMS_R_SYSTEM.ResourceDomainORWorkgroup,SMS_R_SYSTEM.Client from
SMS_R_System where SMS_R_System.OperatingSystemNameandVersion like "%Workstation 10%"
```

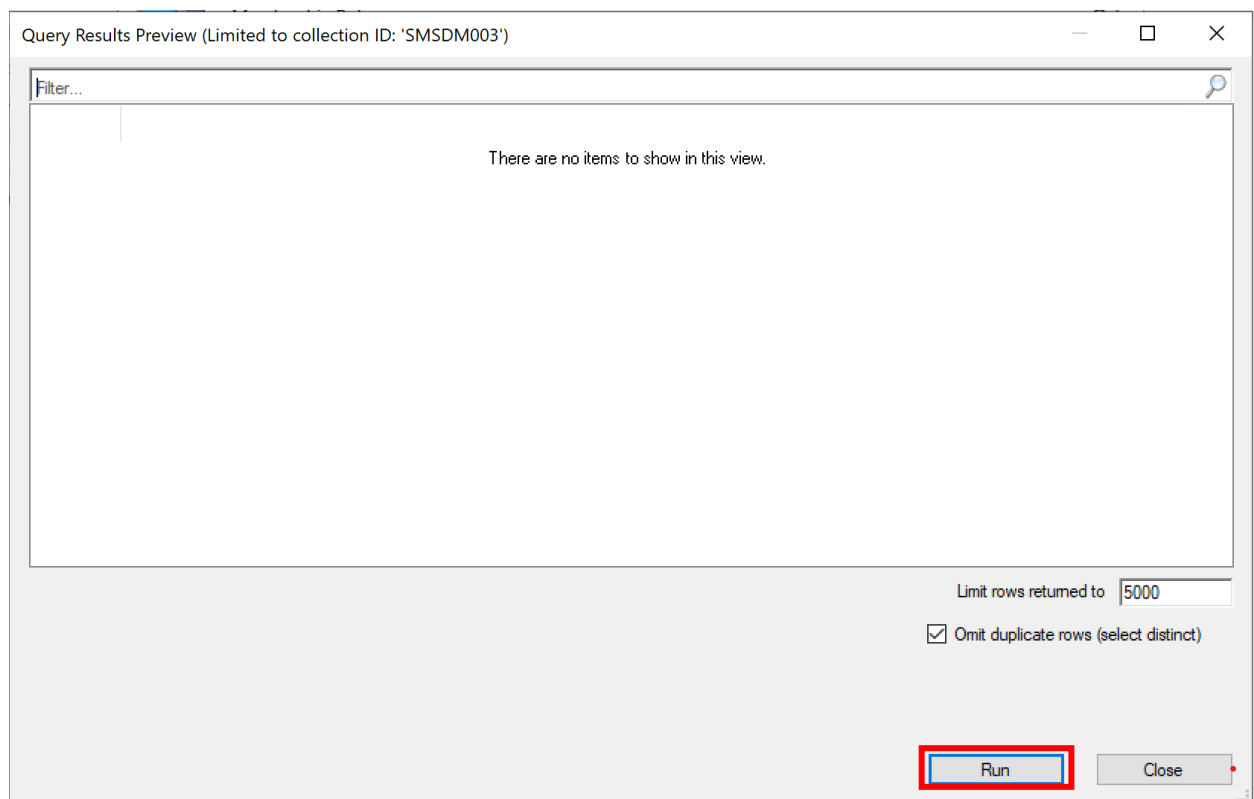
Example query 3 - All Windows Server (2012, 2016, 2019 and 2022)

```
select  
SMS_R_SYSTEM.ResourceID,SMS_R_SYSTEM.ResourceType,SMS_R_SYSTEM.Name,SMS_R_SYSTEM.  
SMSUniqueIdentifier,SMS_R_SYSTEM.ResourceDomainORWorkgroup,SMS_R_SYSTEM.Client from  
SMS_R_System where SMS_R_System.OperatingSystemNameandVersion like "%Server%"
```

Example query 4 - All Desktops (Windows 10, Windows 11)

```
select  
SMS_R_SYSTEM.ResourceID,SMS_R_SYSTEM.ResourceType,SMS_R_SYSTEM.Name,SMS_R_SYSTEM.  
SMSUniqueIdentifier,SMS_R_SYSTEM.ResourceDomainORWorkgroup,SMS_R_SYSTEM.Client from  
SMS_R_System where SMS_R_System.OperatingSystemNameandVersion like "%Workstation%"
```

13. Select Run



14. Confirm all the correct systems are present for the Operating system you want to onboard →
Close

Query Results Preview (Limited to collection ID: 'SMSDM003')

Filter...

Client	Name	ResourceDomainORWorkgroup	ResourceId	ResourceType	SMSUniqueIdentifier
1	sccmlabcl03	contoso	16777219	5	GUID:47064F91-D42C-45C4-942E-2768CCE1653
1	sccmlabcl01	contoso	16777220	5	GUID:F8418177-31E9-4B68-A002-3B81499F9EC1
1	sccmlabcl02	contoso	16777221	5	GUID:FB6AE4CF-F823-4F91-B68E-7C943C6E8E4

Query run complete.

Limit rows returned to 5000

☒ Omit duplicate rows (select distinct)

Statistics

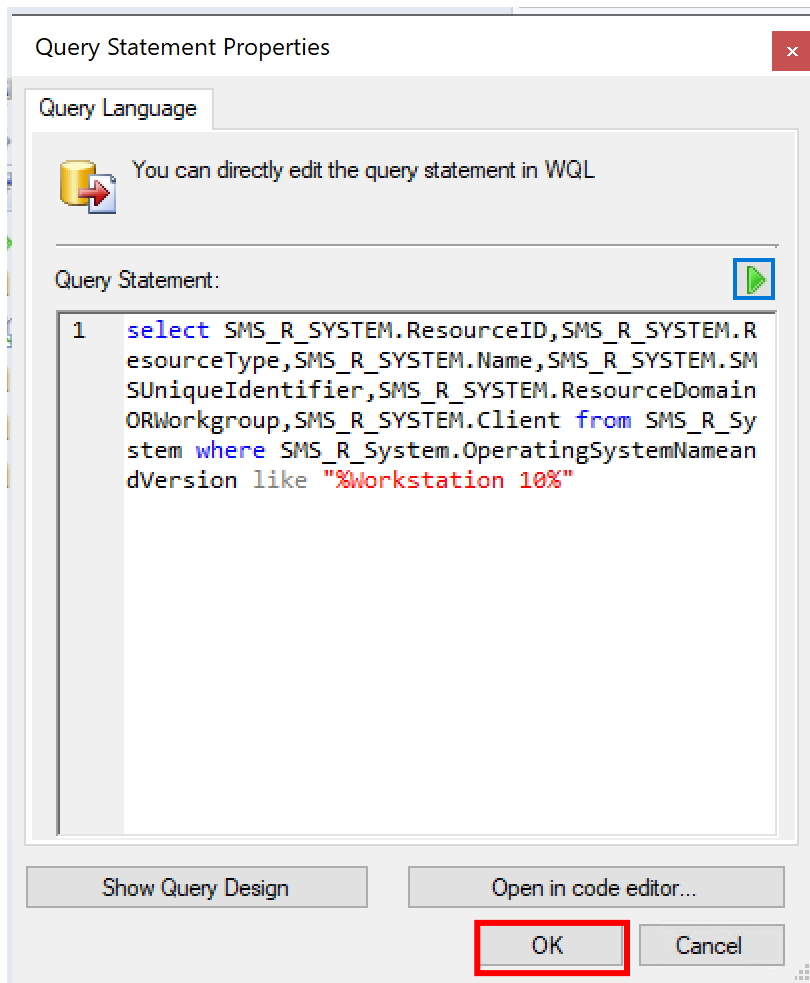
Rows returned 3

Query execution elapsed time 00:00:00.264

Displaying results elapsed time 00:00:01.164

Run Close


15. Select **OK**



16. Select **OK**

Query Rule Properties


General

 Name:

Resource class:

Query Statement:

```
select
SMS_R_SYSTEM.ResourceID,
SMS_R_SYSTEM.ResourceTyp
e,SMS_R_SYSTEM.Name,SMS_
R_SYSTEM.SMSUniqueIdenti
```

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

17. Select **Next**

Create Device Collection Wizard

Membership Rules

General
Membership Rules
Summary
Progress
Completion

Define membership rules for this collection

Membership rules determine the resources that are included in the collection when it updates. You can use membership rules to add a specific object or a set of objects from a query. The collection membership can also include or exclude other collections. Membership rules can add only those objects that are members of the limiting collection.

Membership rules:

Rule Name	Type	Collection Id
Windows 10	Query	Not Applicable

< >

Add Rule Edit... Delete

☐ Use incremental updates for this collection

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

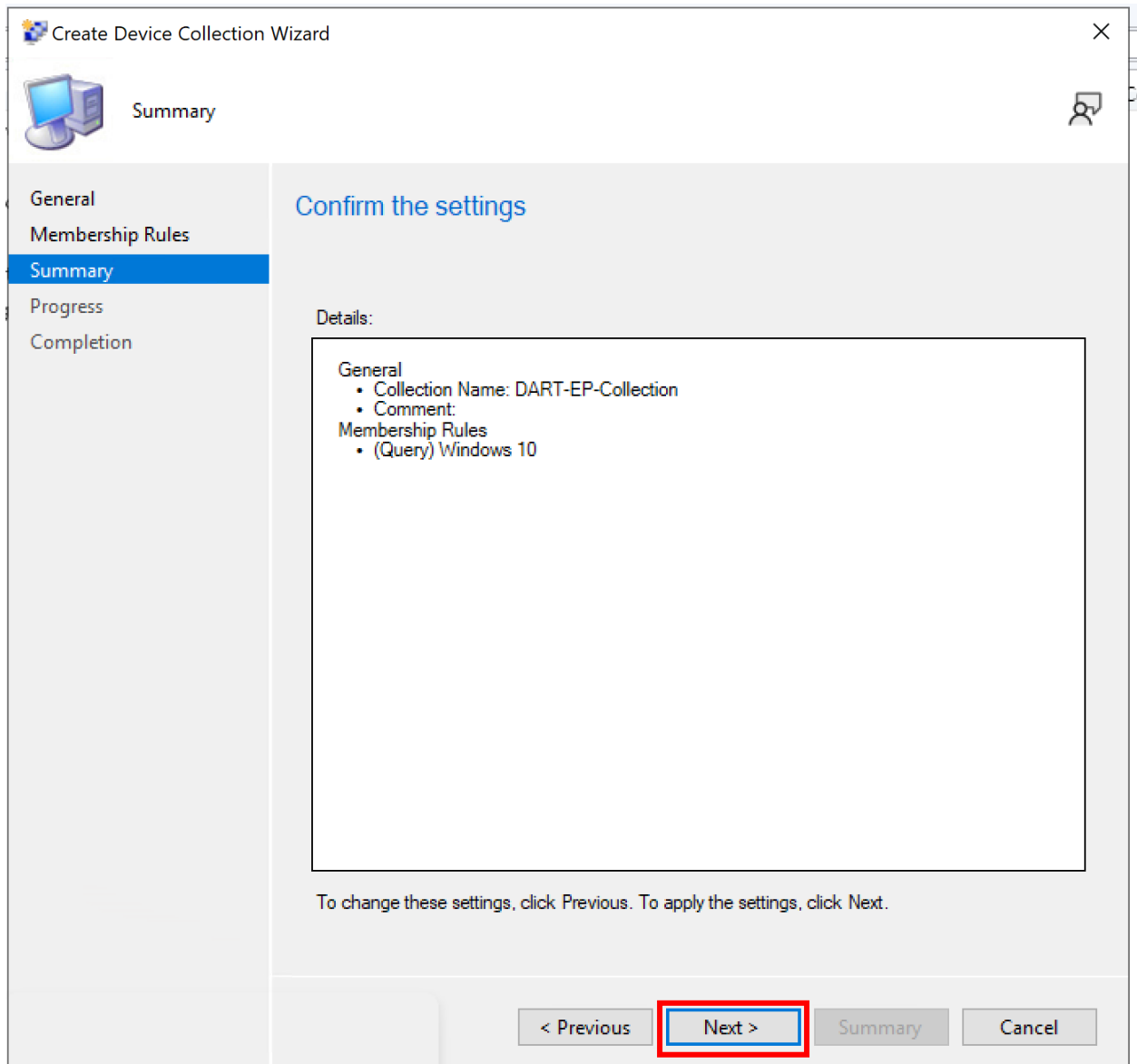
☒ Schedule a full update on this collection

Occurs every 7 days effective 2/18/2022 10:17 PM

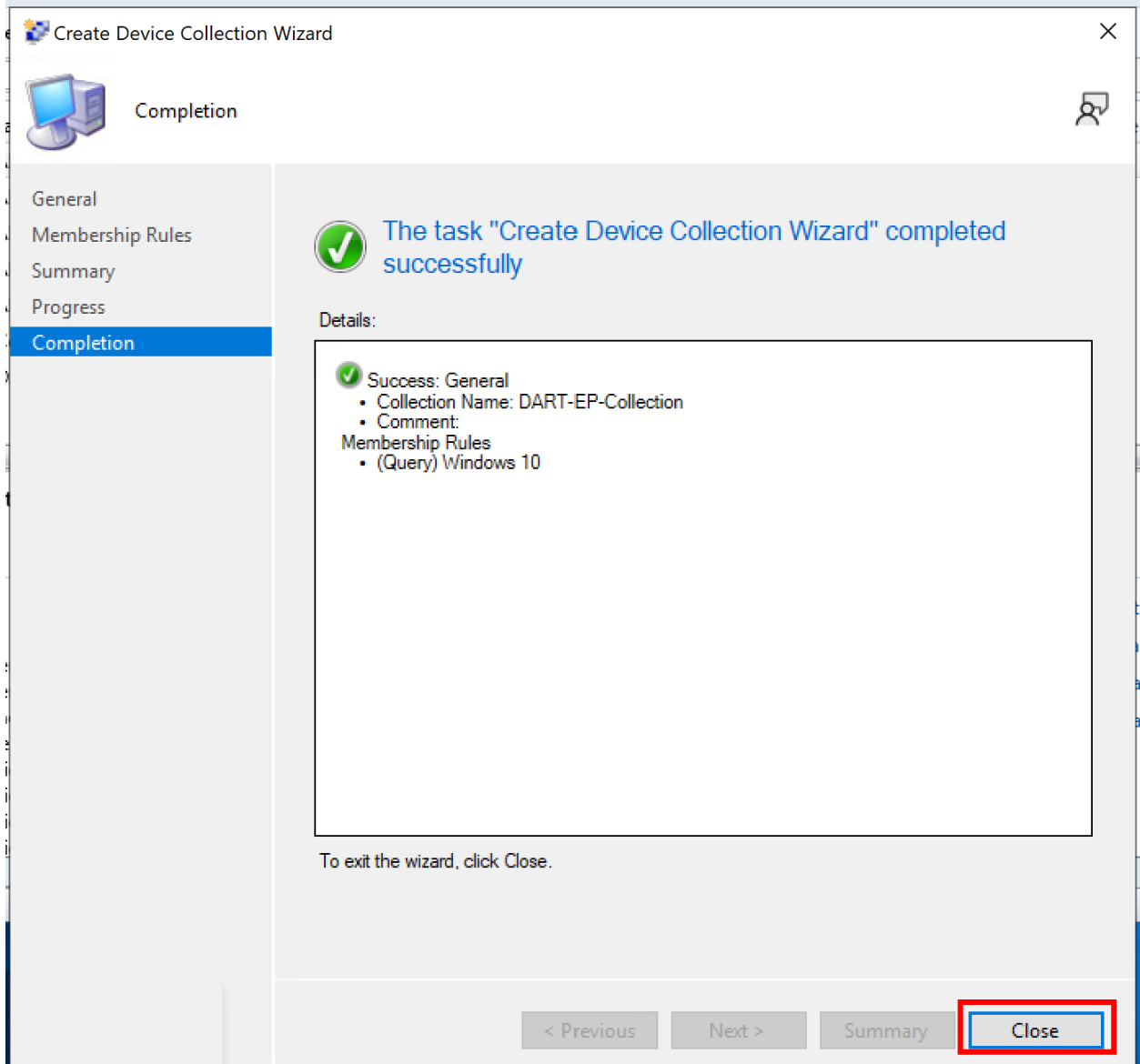
Schedule...

< Previous Next > Summary Cancel

18. Select **Next**



19. Select **Close**



20. Now you should have the newly created SCCM collection

Microsoft Endpoint Configuration Manager (Connected to PS1, PS1 - sccmps01.contoso.com) (Evaluation, 180 days left)

Home Folder

Create Manage Device Categories Saved Searches Collection Deployment View Relationships Move Properties

Assets and Compliance Overview Device Collections

Device Collections 7 items

Icon	Name	Limiting Collection	Member Count	Members Visible on Site	Reference
	All Desktop and Server Clients	All Systems	1	1	0
	All Mobile Devices	All Systems	0	0	0
	All Provisioning Devices	All Systems	1	1	0
	All Systems		7	7	0
	All Unknown Computers	All Systems	2	2	0
	Co-management Eligible Devices	All Systems	1	1	0
	DART-EP-Collection	All Desktop and Se...	0	0	0

All Desktop and Server Clients

Summary

Name: All Desktop and Server Clients
Update Time: 2/18/2022 4:00 AM
Member Count: 1
Members Visible on Site: 1
Referenced Collections: 0
Comment: All Desktop and Server Clients
Evaluation (Full) Run Time (ms): 1,062
Evaluation (Full) Member Changes: 0
Evaluation (Full) Last Member Change Time: 2/17/2022 11:01 PM
Evaluation (Full) Last Completion Time: 2/18/2022 4:00 AM

Related Objects

- Full Evaluation Queue
- Incremental Evaluation Queue
- Manual Evaluation Queue
- New Evaluation Queue

Ready

21. Right click Collection → **Update membership**

Microsoft Endpoint Configuration Manager (Connected to PS1, PS1 - sccmps01.contoso.com) (Evaluation, 180 days)

Folder Tools

Home Folder

Create Manage Device Categories Saved Searches Collection Deployment View Relationships Move Properties

Assets and Compliance Overview Device Collections

Device Collections 7 items

Icon	Name	Limiting Collection
	All Desktop and Server Clients	All Systems
	All Mobile Devices	All Systems
	All Provisioning Devices	All Systems
	All Systems	
	All Unknown Computers	All Systems
	Co-management Eligible Devices	All Systems
	DART-EP-Collection	All Desktop and S

Update Membership

DART-EP-Collection

Summary

Name: DART-EP-Collection

Update Time: 1/1/1980 12:00 AM

Member Count: 0

Members Visible on Site: 0

Referenced Collections: 0

Deployment (Full) Run Time (ms): 0

Deployment (Full) Member Changes: 0

Deployment (Full) Last Member Change Time: 1/1/1970 12:00 AM

Deployment (Full) Last Completion Time: 1/1/1970 12:00 AM

Deployments Custom Client Settings

22. Select Yes

Co-management Eligible Devices	All Systems	1	1
DART-EP-Collection	All Desktop and Se...	0	0

DART-EP-Collection

Summary

Name: DART-EP-Collection

Update Time: 1/1/1980 12:00 AM

Member Count: 0

Members Visible on Site: 0

Referenced Collections: 0

Configuration Manager

This action will re-evaluate the membership rules for the selected collections and might take some time to finish.

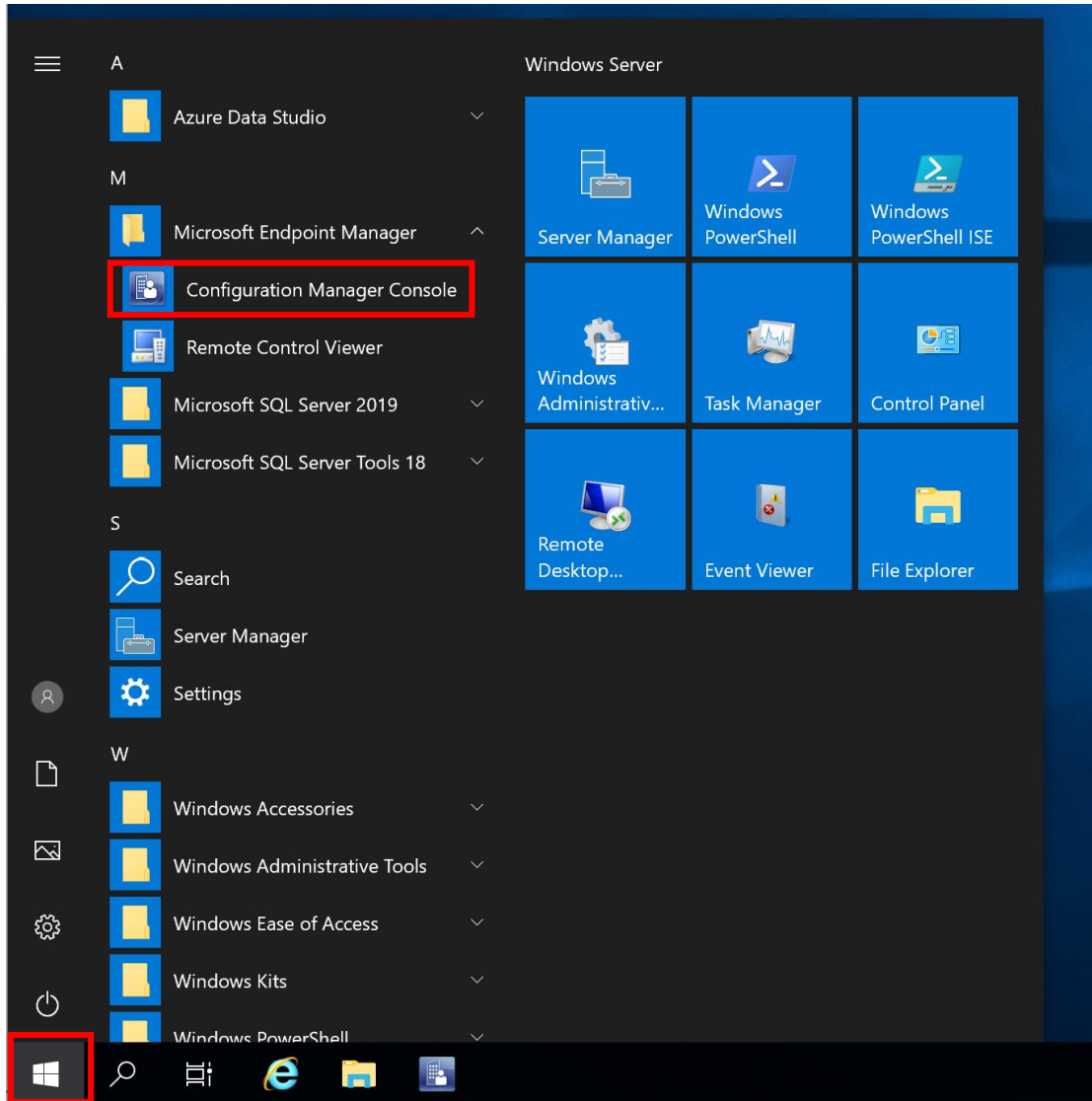
Are you sure that you want to continue?

Yes No

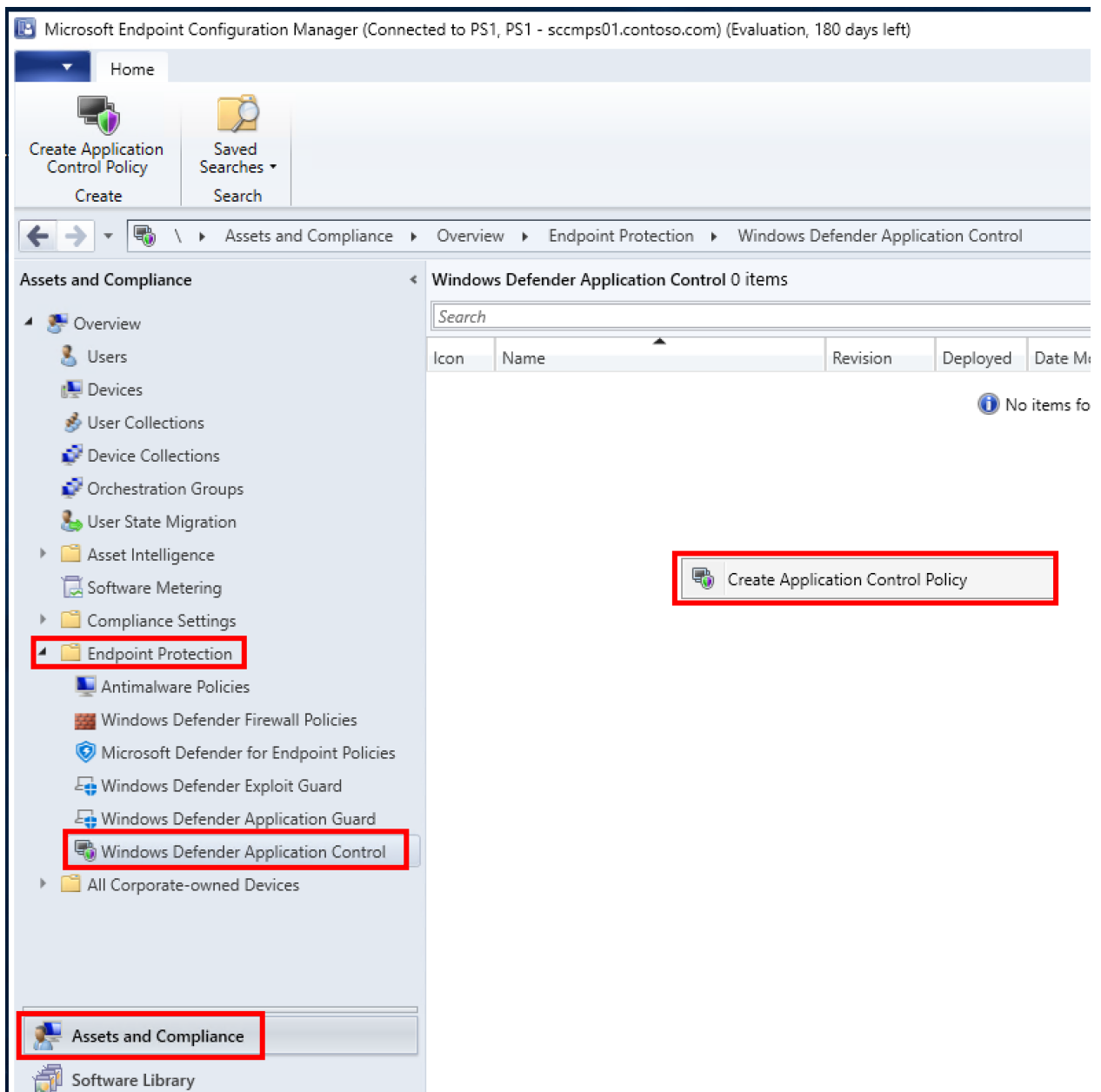
Create WDAC Policy

23. Log into the Primary Site system

24. Open the



25. Select **Asset and Compliance** → **Endpoint Protection** → **Windows Defender Application Control** → **Create Application Control Policy**



26. Enter the name of the policy → **Next**
27. Enable **Enforce a restart of devices so that this policy can be enforced for all processes**
28. Select the mode which you want the policy to run (Enforce enabled / Audit Only)
29. Click **Next**

Create Application Control Policy

General

General

Inclusions

Summary

Progress

Completion

Specify general information about this Application Control policy

This policy configures Windows 10 devices with Windows Defender Application Control so that only trusted executable files, system files, and drivers are allowed to run. Windows components, all apps from the Microsoft Store, the Configuration Manager client, and new applications you deploy with Configuration Manager are automatically trusted.

Name:


Description:

☒ Enforce a restart of devices so that this policy can be enforced for all processes

Enforcement Mode:

☒ Enforcement enabled - Only allow trusted executables to run


☐ Audit only - Log untrusted executables to local client event logs

 Devices that run Windows 10 version 1703 or earlier are always automatically restarted.

< Previous **Next >** Summary Cancel

30. Click **Add**

Create Application Control Policy



Inclusions

General

Inclusions

Summary

Progress

Completion

Include trust for additional software

For devices that run Windows 10 version 1709 or later, software that is known by the Microsoft Intelligent Security Graph to be good is trusted and can run. Windows Defender SmartScreen must be running on the device for this authorization to function.

[More information](#)

☐ Authorize software that is trusted by the Intelligent Security Graph

Specify additional files and folders on the device that will be included as trusted software at the time this policy is applied. Users without administrative rights should not have write access to these files and locations.

Trusted files or folders:

Name	Path
There are no items to show in this view.	

Add

Remove

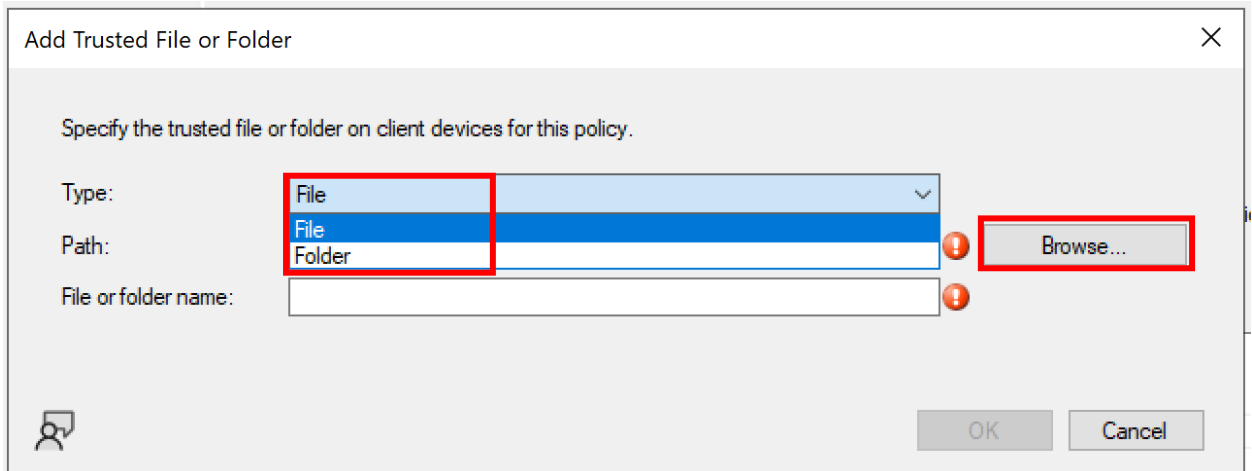
< Previous

Next >

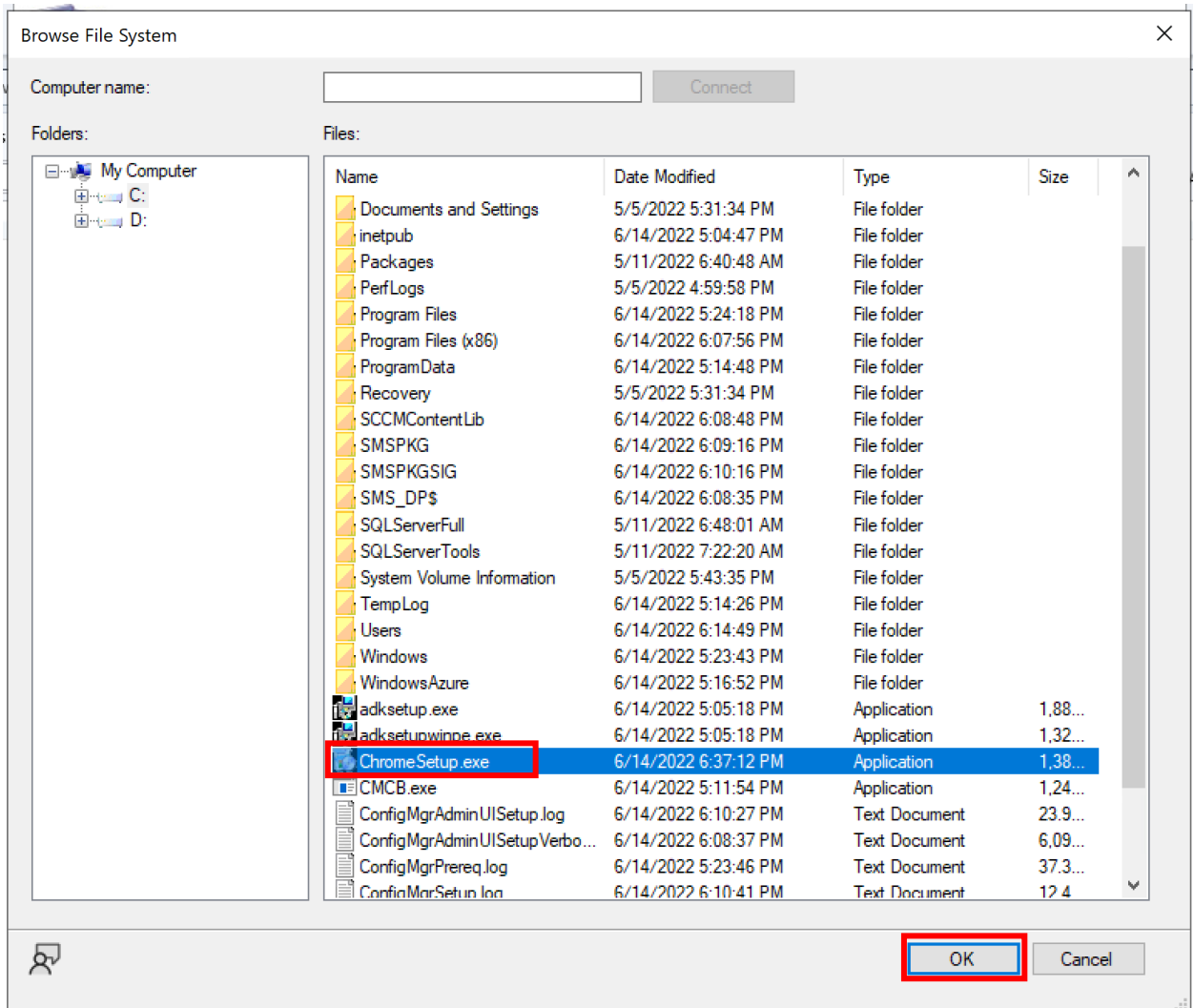
Summary

Cancel

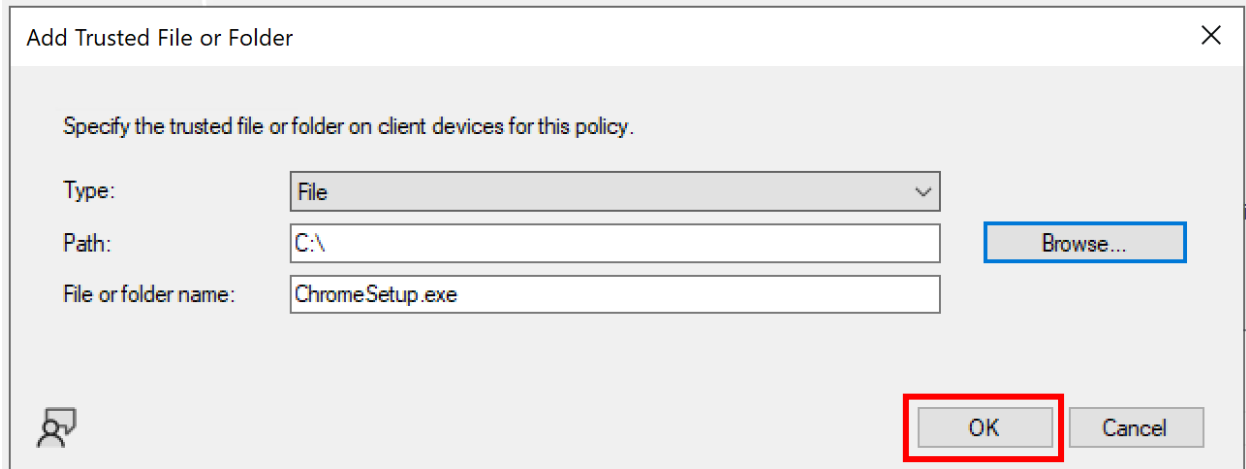
31. Select **File** or **Folder** → **Browse**



32. Select the executable for your policy → **OK**



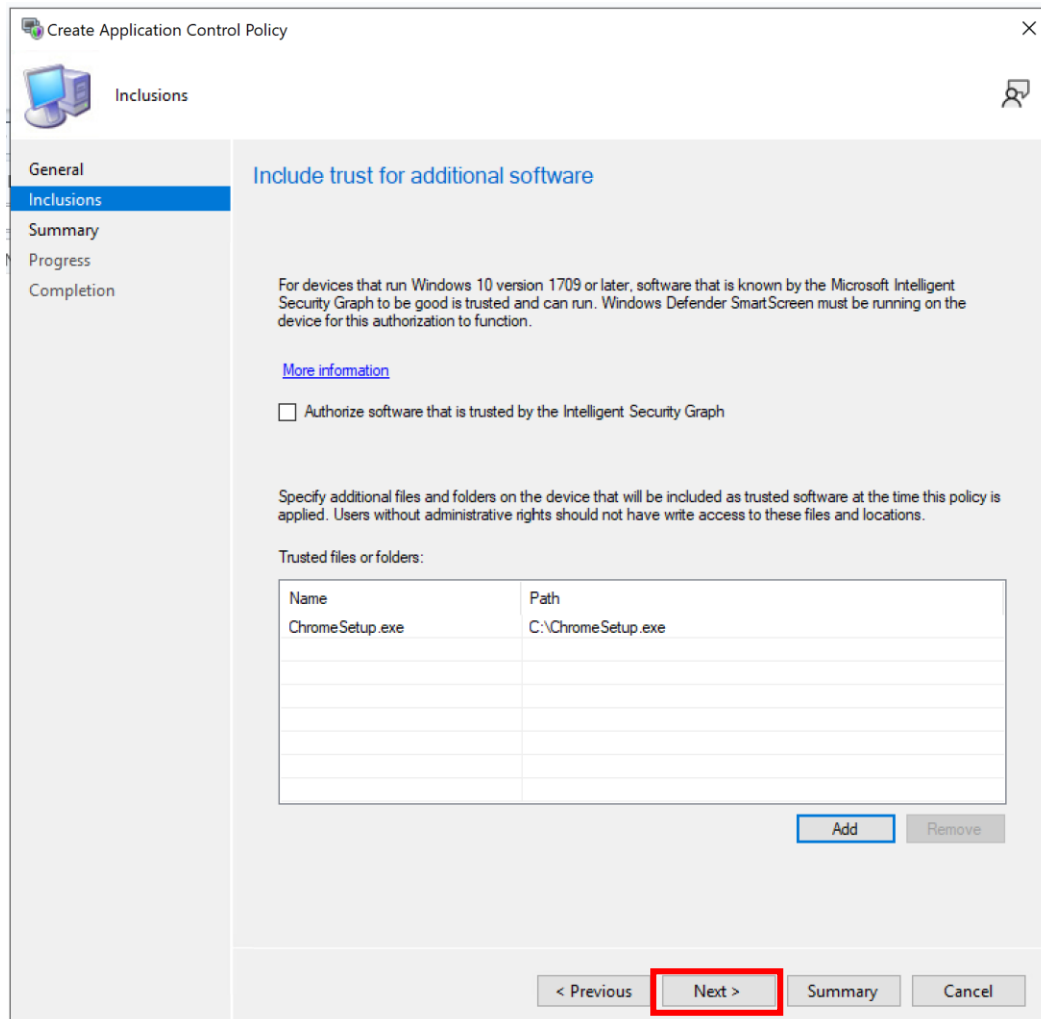
33. Select **OK**



The dialog box is titled "Add Trusted File or Folder" and contains the following fields and buttons:

- Type:** A dropdown menu with "File" selected.
- Path:** A text box containing "C:\".
- File or folder name:** A text box containing "ChromeSetup.exe".
- Browse...** A button to the right of the Path field.
- OK** and **Cancel** buttons at the bottom right. The **OK** button is highlighted with a red rectangle.

34. Select **Next**



The "Create Application Control Policy" window is shown with the "Inclusions" tab selected. The left sidebar contains the following tabs: General, Inclusions, Summary, Progress, and Completion. The main content area is titled "Include trust for additional software" and contains the following text and controls:

For devices that run Windows 10 version 1709 or later, software that is known by the Microsoft Intelligent Security Graph to be good is trusted and can run. Windows Defender SmartScreen must be running on the device for this authorization to function.

[More information](#)

☐ Authorize software that is trusted by the Intelligent Security Graph

Specify additional files and folders on the device that will be included as trusted software at the time this policy is applied. Users without administrative rights should not have write access to these files and locations.

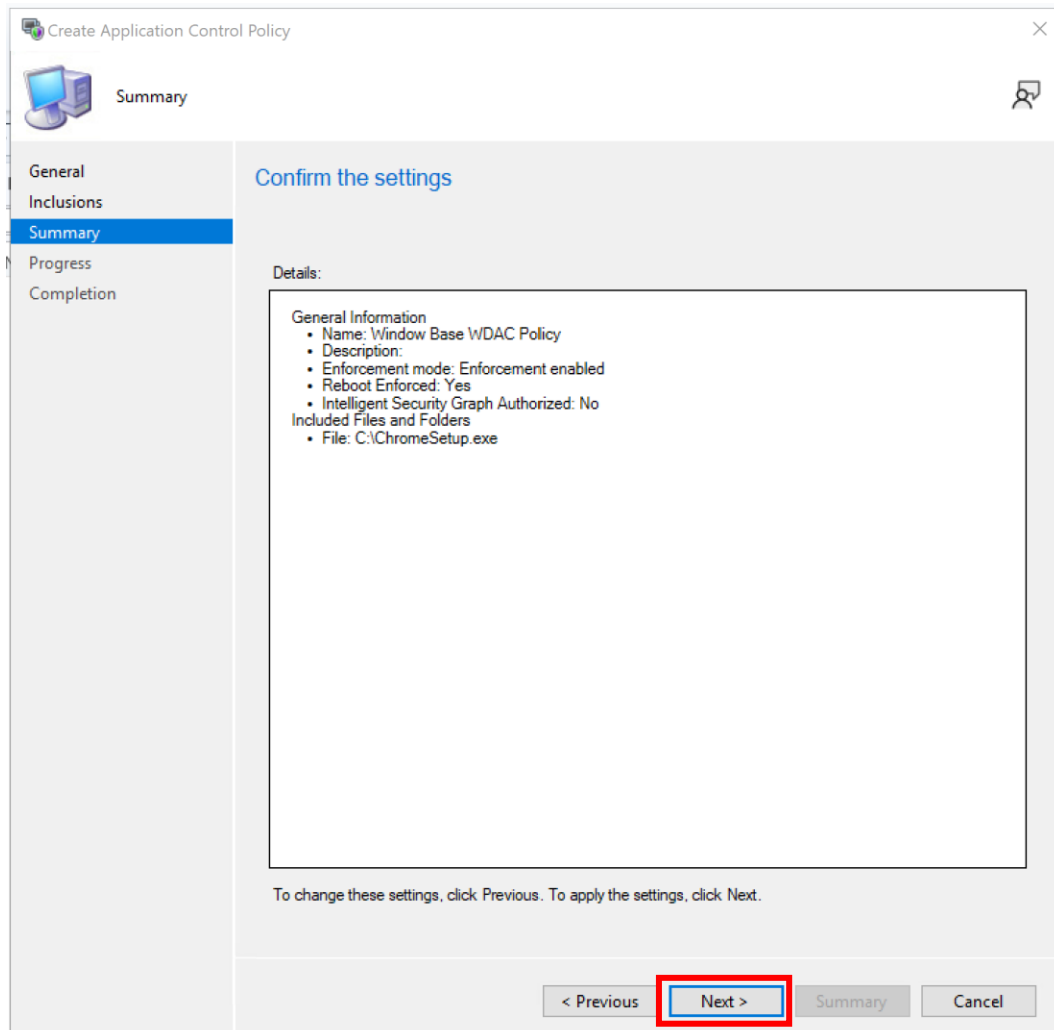
Trusted files or folders:

Name	Path
ChromeSetup.exe	C:\ChromeSetup.exe

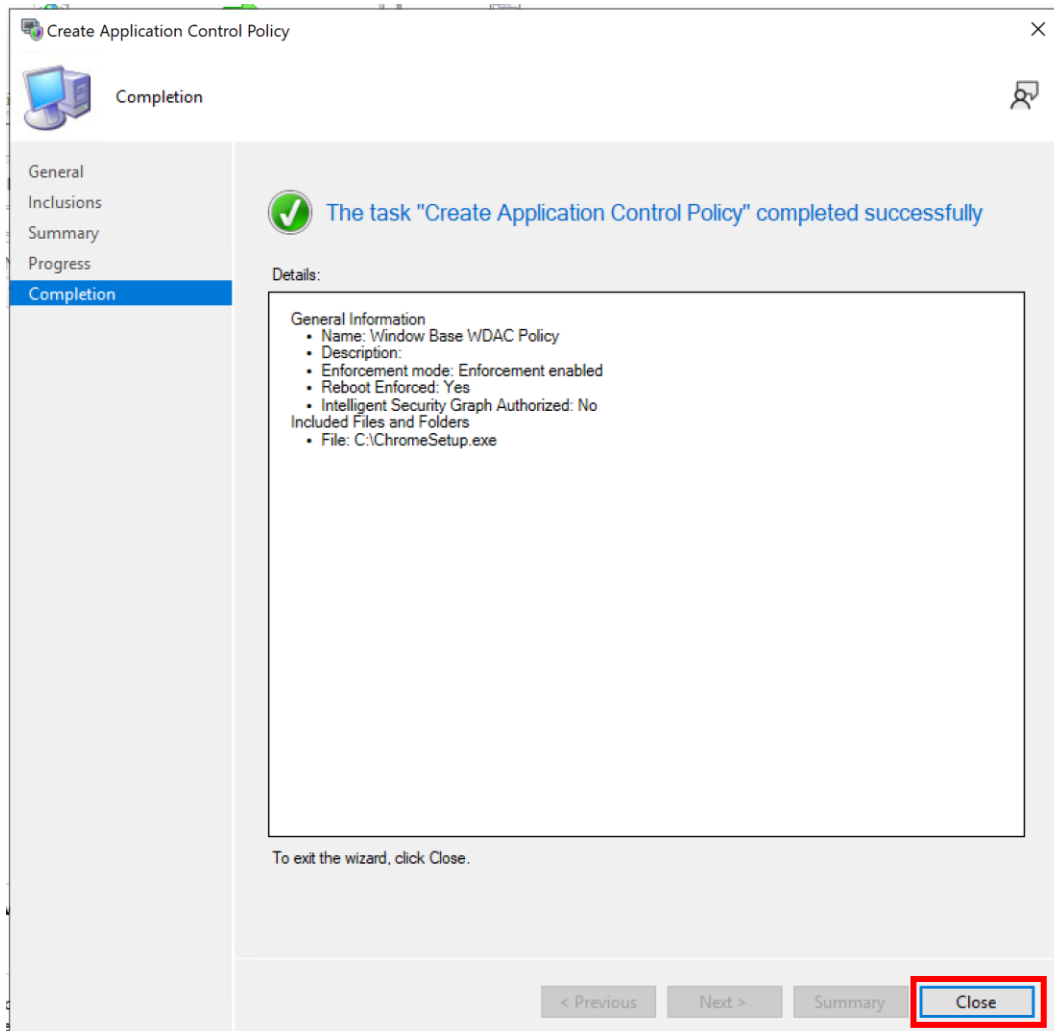
Add **Remove**

At the bottom of the window, the **Next >** button is highlighted with a red rectangle.

35. Select **Next**

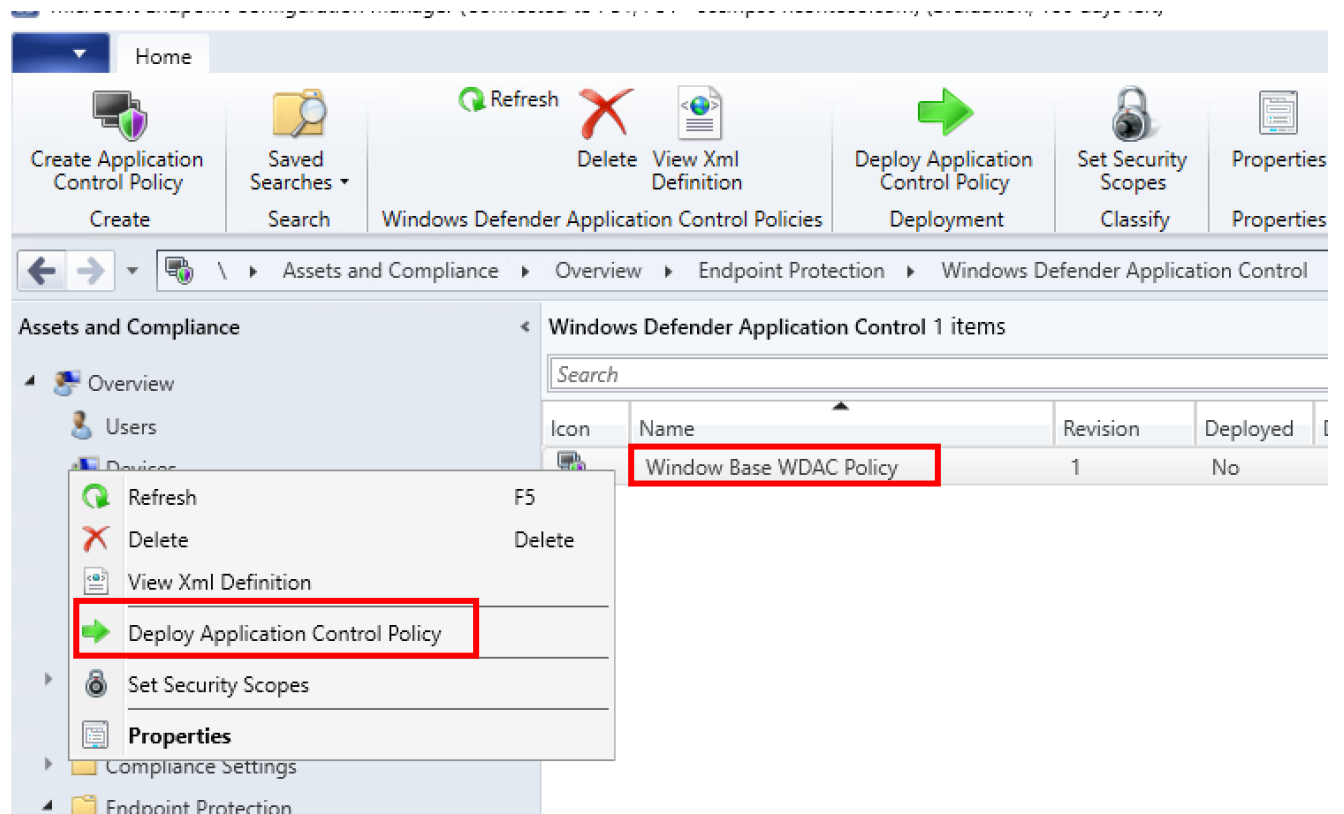


36. Select **Close**



Deploy WDAC Policy to Device Collection

1. Right-click the newly created policy → **Deploy Application Control Policy**



2. Select **Browse**

Deploy Windows Defender Application Control Policy

Application Control Policy name:

Collection:

☐ Allow remediation outside the maintenance window

Schedule
Specify the compliance evaluation schedule for this Application Control Policy:

☒ Simple schedule
Run every: Days

☐ Custom schedule

3. Select the Device Collection you created earlier → OK

Select Collection

Device Collections
Filter...

Name	Member Count
All Desktop and Server Clients	3
All Mobile Devices	0
All Provisioning Devices	1
All Systems	9
All Unknown Computers	2
Co-management Eligible Devices	3
DART-Endpoint-Clients	3

4. Change the Schedule → OK

Deploy Windows Defender Application Control Policy

Application Control Policy name:
Window Base WDAC Policy

Collection:
DART-Endpoint-Clients Browse...

☐ Allow remediation outside the maintenance window

Schedule
Specify the compliance evaluation schedule for this Application Control Policy:

☒ Simple schedule
Run every: 10 Minutes

☐ Custom schedule
No custom schedule defined. Customize...

OK Cancel