Deploy App Control policies by using Microsoft Configuration Manager

Article • 10/01/2024 • 1 contributor •

Applies to: ☑ Windows 11, ☑ Windows 10, ☑ Windows Server 2025, ☑ Windows Server 2022, ☑ Windows Server 2019, ☑ Windows Server 2016

Feedback

In this article

Use Configuration Manager's built-in policies
Deploy custom App Control policies using Packages/Programs or Task Sequences

> **Note**
>
> Some capabilities of App Control for Business are only available on specific Windows versions. Learn more about App Control feature availability.

You can use Microsoft Configuration Manager to configure App Control for Business on client machines.

Use Configuration Manager's built-in policies

Configuration Manager includes native support for App Control, which allows you to configure Windows 10 and Windows 11 client computers with a policy that will only allow:

- Windows components
- Microsoft Store apps
- Apps installed by Configuration Manager (Configuration Manager self-configured as a managed installer)
- (Optional) Reputable apps as defined by the Intelligent Security Graph (ISG)
- (Optional) Apps and executables already installed in admin-definable folder locations that Configuration Manager will allow through a one-time scan during policy creation on managed endpoints.

Configuration Manager doesn't remove policies once deployed. To stop enforcement, you should switch the policy to audit mode, which will produce the same effect. If you want to disable App Control for Business altogether (including audit mode), you can deploy a script to delete the policy file from disk, and either trigger a reboot or wait for the next reboot.

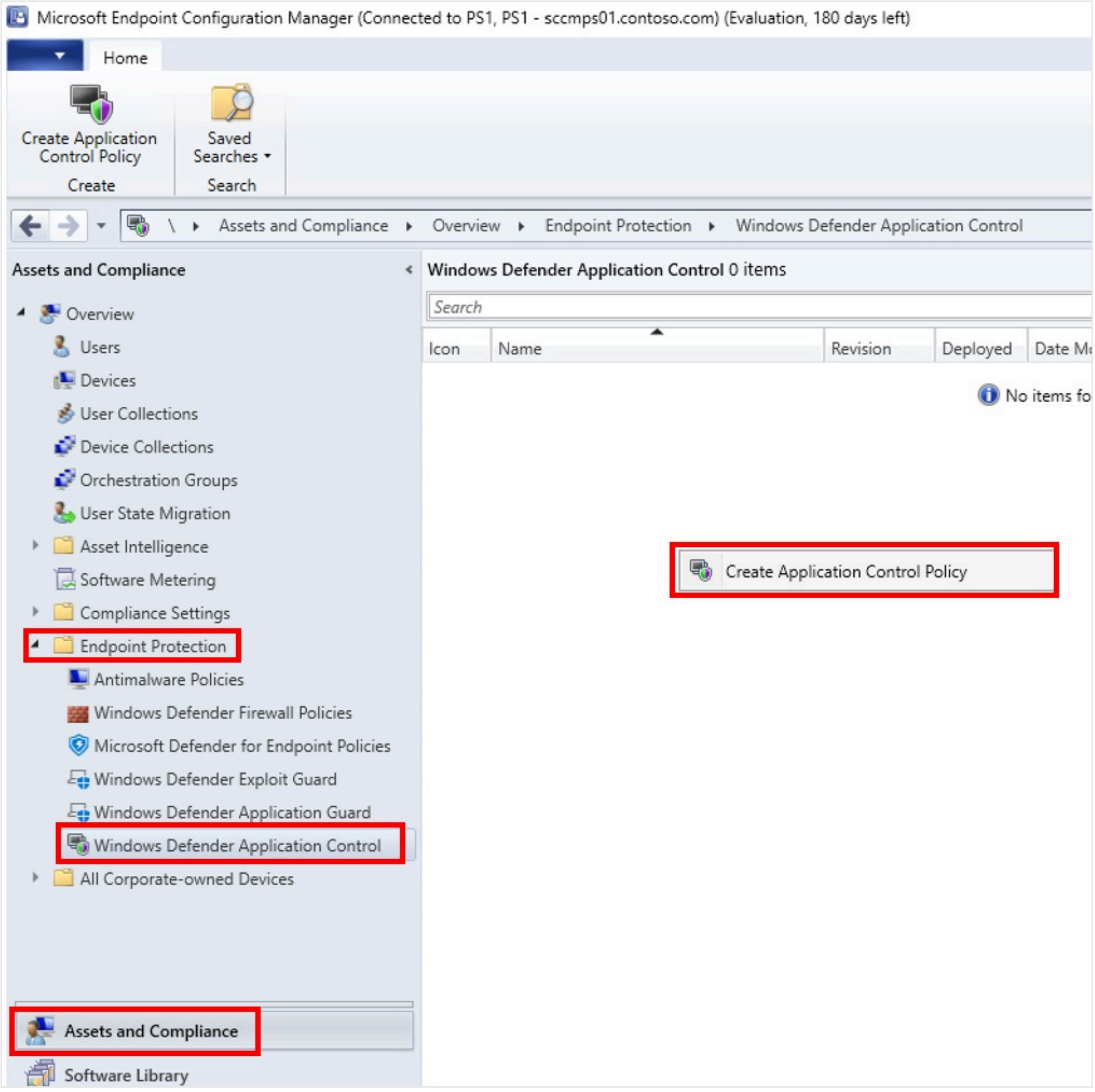
Create an App Control Policy in Configuration Manager

1. Select **Asset and Compliance** > **Endpoint Protection** > **App Control for Business** > **Create Application Control Policy**

Filter by title
Application Control for Windows
About application control for Windows
About application control for Windows
App Control and AppLocker Overview
App Control and AppLocker Feature Availability
Virtualization-based protection of code integrity
Design guide
Deployment guide
Deployment guide
Deploy App Control policies with MDM
Deploy App Control policies with Configuration Manager
Deploy App Control policies with script
Deploy App Control policies with group policy
Audit App Control policies
Merge App Control policies
Enforce App Control policies
Use code signing for added control and protection with App Control
Disable App Control policies
Operational guide

› AppId Tagging guide

› AppLocker


Microsoft Endpoint Configuration Manager (Connected to PS1, PS1 - sccmps01.contoso.com) (Evaluation, 180 days left)
Home
Create Application Control Policy
Create
Saved Searches
Search
\ ▸ Assets and Compliance ▸ Overview ▸ Endpoint Protection ▸ Windows Defender Application Control
Assets and Compliance
Overview
Users
Devices
User Collections
Device Collections
Orchestration Groups
User State Migration
Asset Intelligence
Software Metering
Compliance Settings
Endpoint Protection
Antimalware Policies
Windows Defender Firewall Policies
Microsoft Defender for Endpoint Policies
Windows Defender Exploit Guard
Windows Defender Application Guard
Windows Defender Application Control
All Corporate-owned Devices
Assets and Compliance
Software Library
Windows Defender Application Control 0 items
Search
Icon
Name
Revision
Deployed
Date M
No items fo
Create Application Control Policy

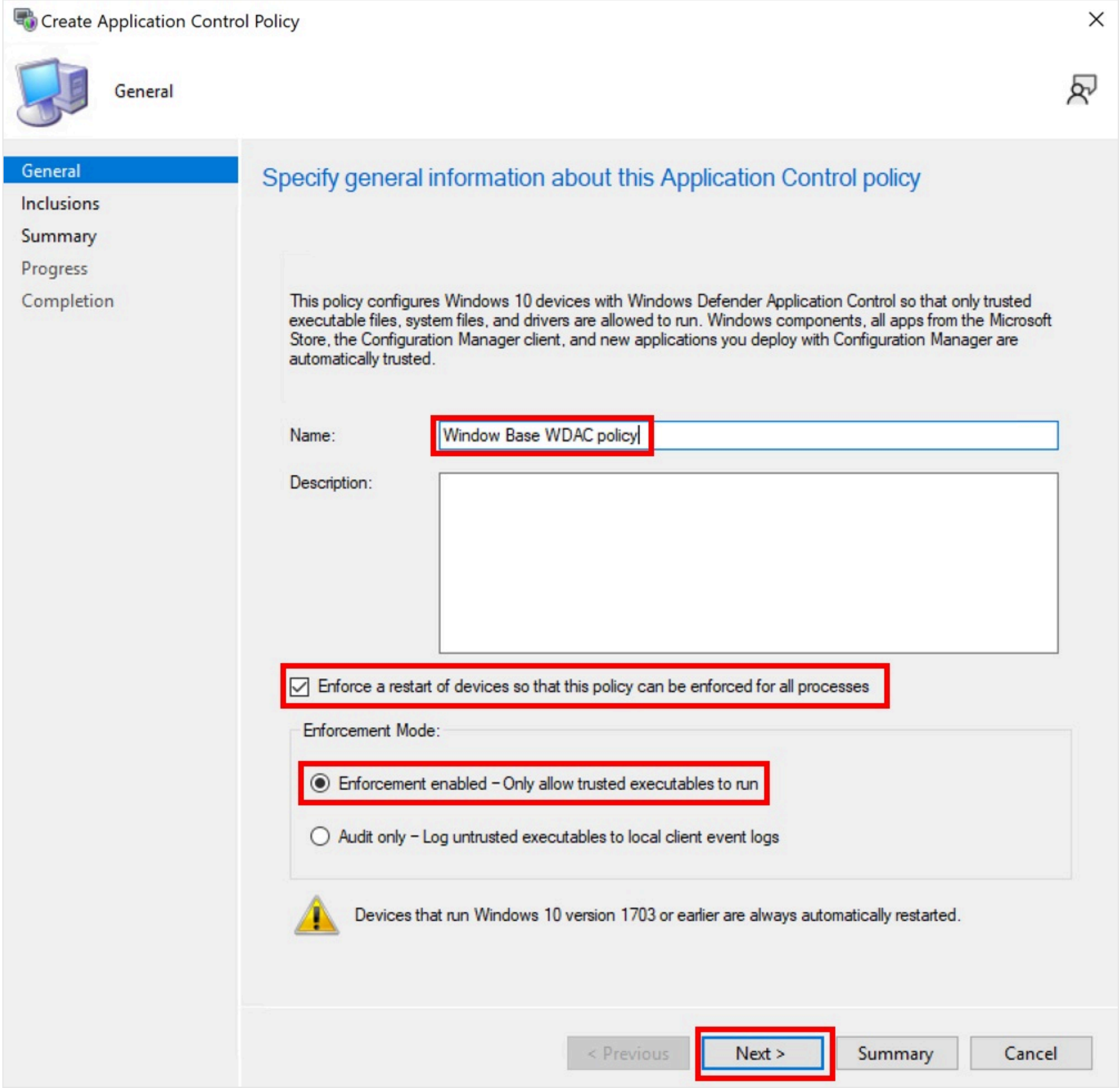
2. Enter the name of the policy > **Next**

3. Enable **Enforce a restart of devices so that this policy can be enforced for all processes**

4. Select the mode that you want the policy to run (Enforcement enabled / Audit Only)

5. Select **Next**

Download PDF



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: Window Base WDAC policy

Description:

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

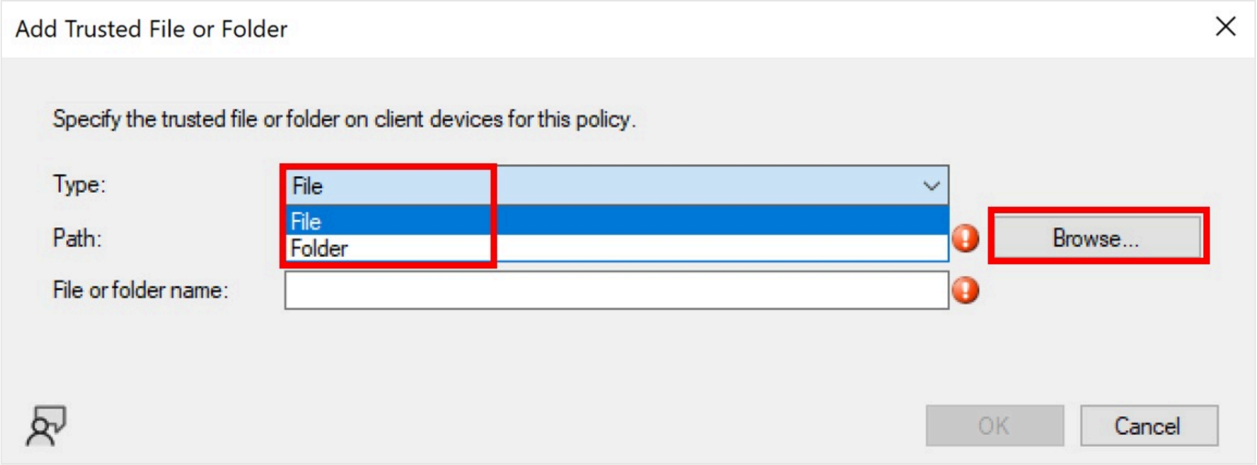
Enforcement Mode:

● 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.

6. Select **Add** to begin creating rules for trusted software



Add Trusted File or Folder

Specify the trusted file or folder on client devices for this policy.

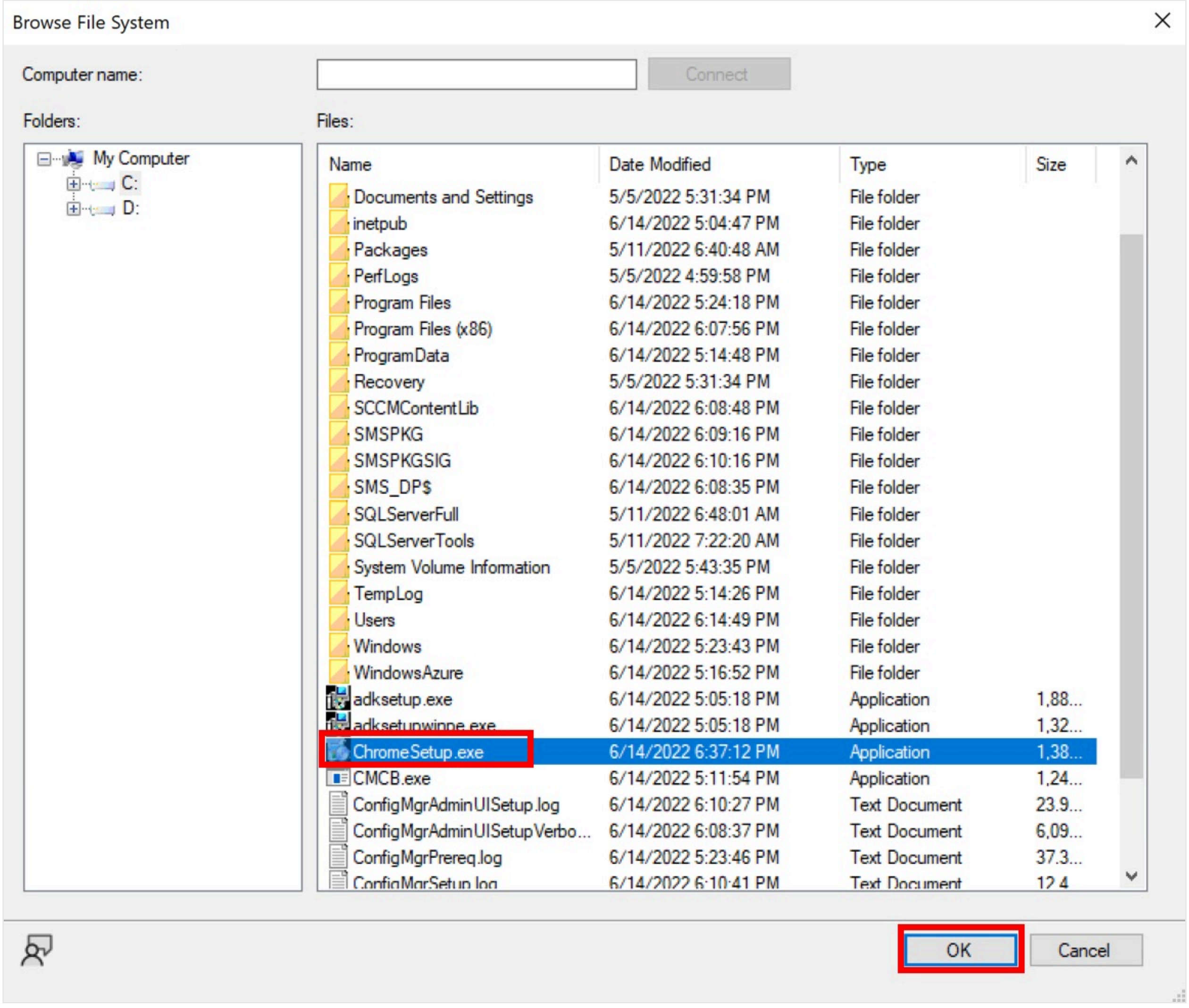
Type: File

File
Folder

Path:

File or folder name:

7. Select **File** or **Folder** to create a path rule > **Browse**



Browse File System

Computer name:

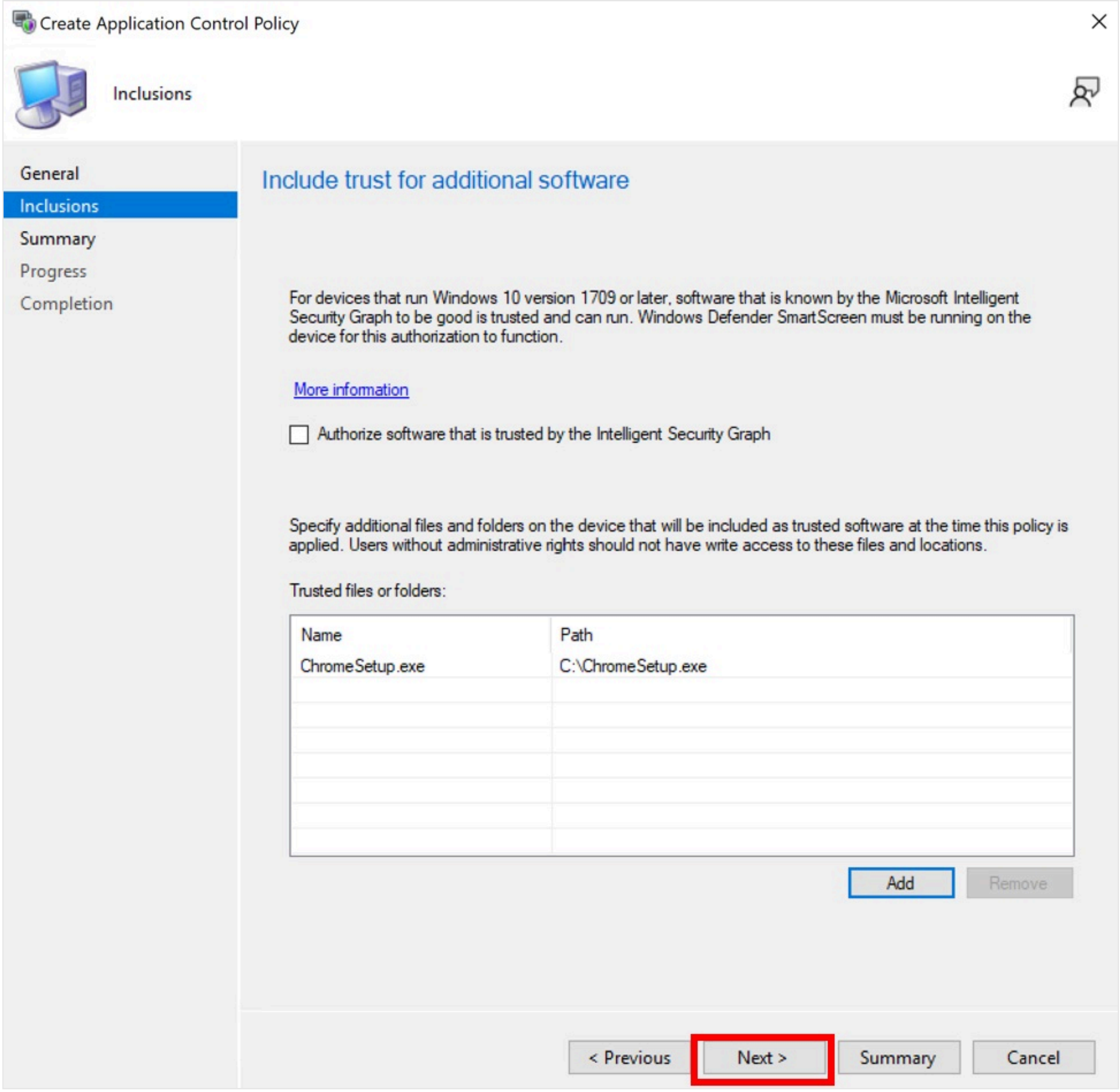
Folders:

My Computer
C:
D:

Files:

Name	Date Modified	Type	Size
Documents and Settings	5/5/2022 5:31:34 PM	File folder	
inetpub	6/14/2022 5:04:47 PM	File folder	
Packages	5/11/2022 6:40:48 AM	File folder	
PerfLogs	5/5/2022 4:59:58 PM	File folder	
Program Files	6/14/2022 5:24:18 PM	File folder	
Program Files (x86)	6/14/2022 6:07:56 PM	File folder	
ProgramData	6/14/2022 5:14:48 PM	File folder	
Recovery	5/5/2022 5:31:34 PM	File folder	
SCCMContentLib	6/14/2022 6:08:48 PM	File folder	
SMSPKG	6/14/2022 6:09:16 PM	File folder	
SMSPKGSIG	6/14/2022 6:10:16 PM	File folder	
SMS_DP$	6/14/2022 6:08:35 PM	File folder	
SQLServerFull	5/11/2022 6:48:01 AM	File folder	
SQLServerTools	5/11/2022 7:22:20 AM	File folder	
System Volume Information	5/5/2022 5:43:35 PM	File folder	
TempLog	6/14/2022 5:14:26 PM	File folder	
Users	6/14/2022 6:14:49 PM	File folder	
Windows	6/14/2022 5:23:43 PM	File folder	
WindowsAzure	6/14/2022 5:16:52 PM	File folder	
adksetup.exe	6/14/2022 5:05:18 PM	Application	1,88...
adksetupwinpe.exe	6/14/2022 5:05:18 PM	Application	1,32...
ChromeSetup.exe	6/14/2022 6:37:12 PM	Application	1,38...
CMCB.exe	6/14/2022 5:11:54 PM	Application	1,24...
ConfigMgrAdminUISetup.log	6/14/2022 6:10:27 PM	Text Document	23.9...
ConfigMgrAdminUISetupVerbo...	6/14/2022 6:08:37 PM	Text Document	6,09...
ConfigMgrPrereq.log	6/14/2022 5:23:46 PM	Text Document	37.3...
ConfigMgrSetup.log	6/14/2022 6:10:41 PM	Text Document	12.4

8. Select the executable or folder for your path rule > **OK**



Create Application Control Policy

Inclusions

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

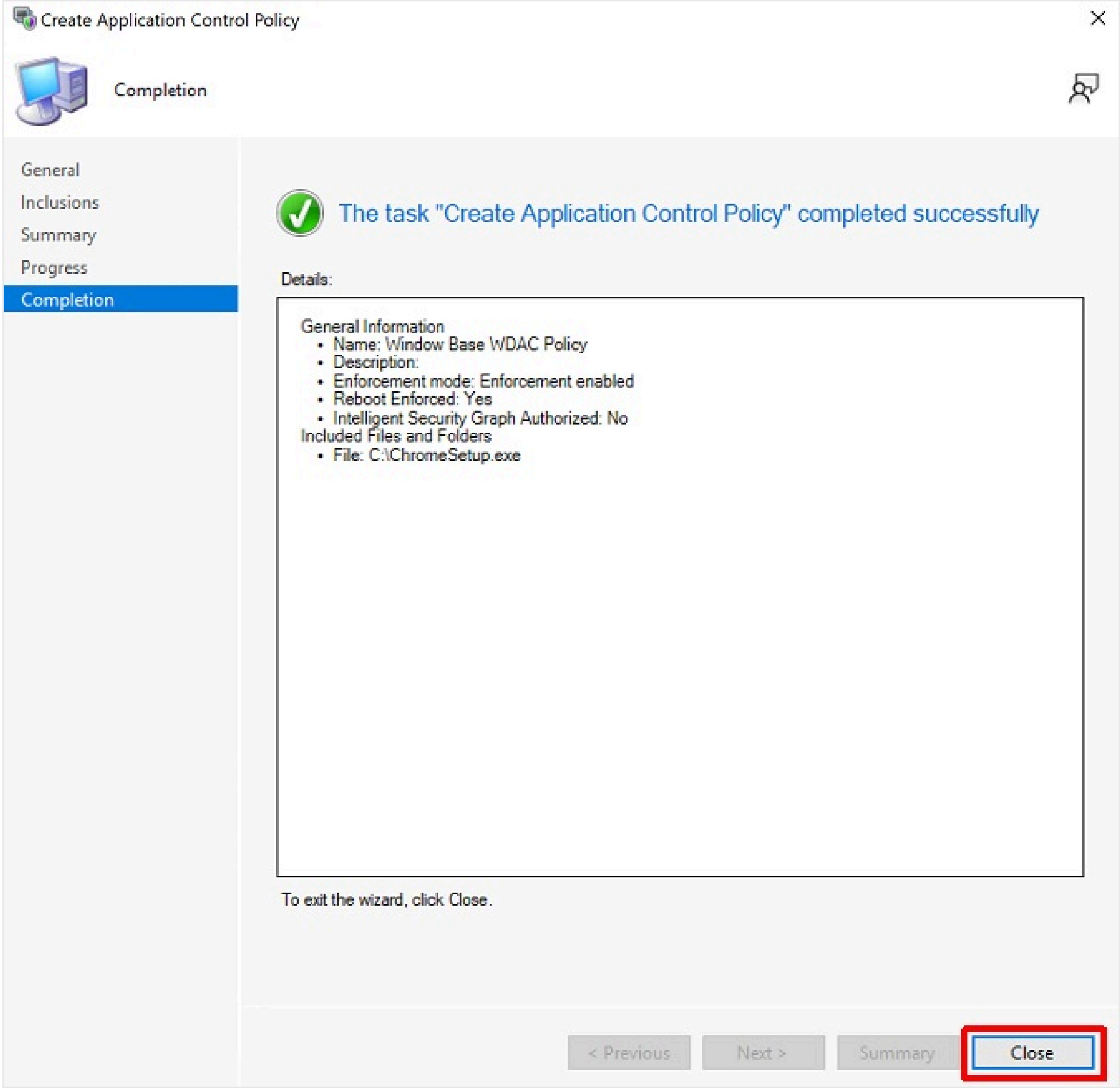
Specify additional files and folders on the device that will be included as trusted software at the time this policy is applied. Users without administrative rights should not have write access to these files and locations.

Trusted files or folders:

Name	Path
ChromeSetup.exe	C:\ChromeSetup.exe

9. Select **OK** to add the rule to the table of trusted files or folder

10. Select **Next** to navigate to the summary page > **Close**



Create Application Control Policy

Completion

The task "Create Application Control Policy" completed successfully

Details:

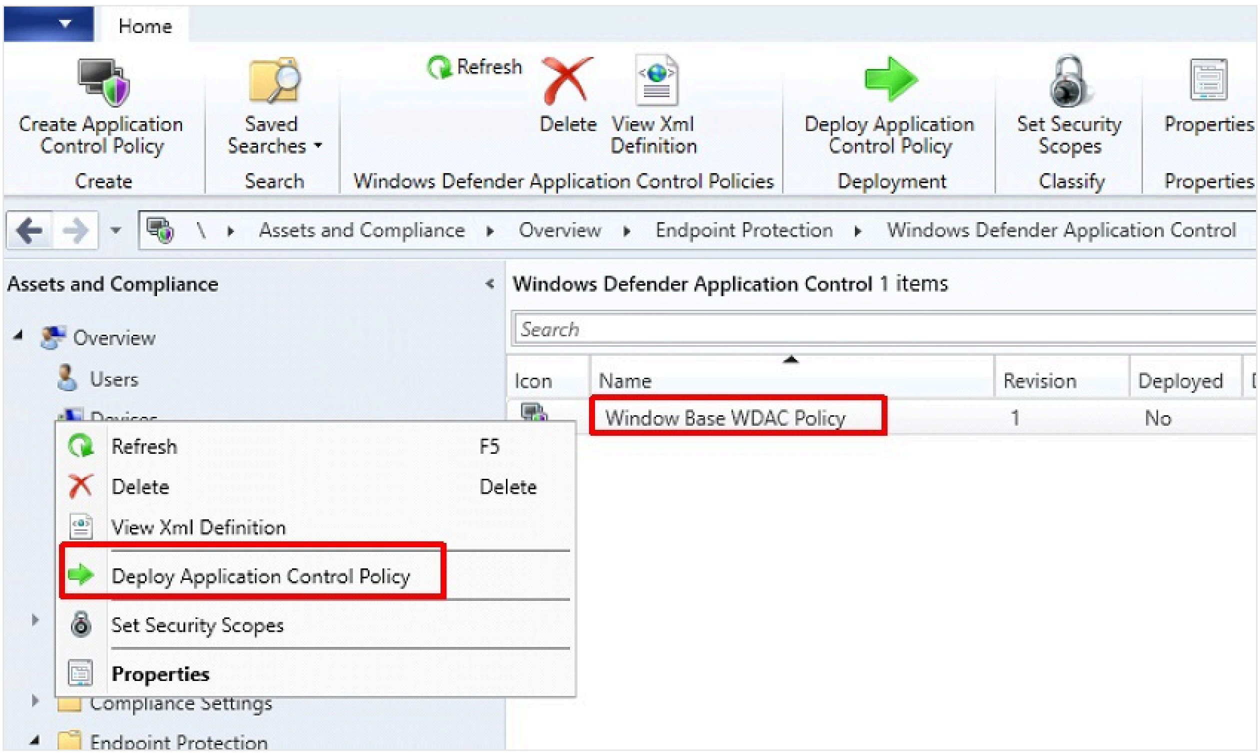
General Information
- Name: Window Base WDAC Policy
- Description:
- Enforcement mode: Enforcement enabled
- Reboot Enforced: Yes
- Intelligent Security Graph Authorized: No

Included Files and Folders
- File: C:\ChromeSetup.exe

To exit the wizard, click Close.

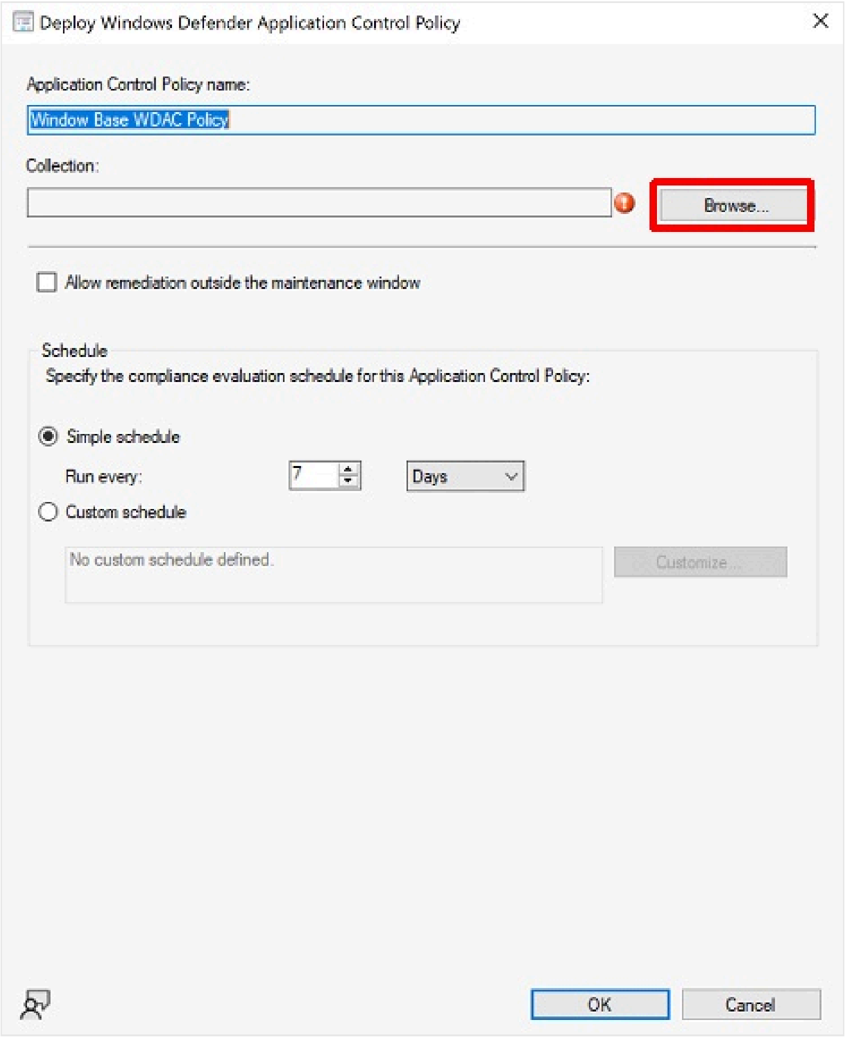
Deploy the App Control policy in Configuration Manager

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


Home
Create Application Control Policy
Create
Saved Searches
Search
Refresh
Delete
View Xml Definition
Windows Defender Application Control Policies
Deploy Application Control Policy
Deployment
Set Security Scopes
Classify
Properties
Properties
\ ▸ Assets and Compliance ▸ Overview ▸ Endpoint Protection ▸ Windows Defender Application Control
Assets and Compliance
Overview
Users
Devices
Compliance Settings
Endpoint Protection
Refresh F5
Delete Delete
View Xml Definition
Deploy Application Control Policy
Set Security Scopes
Properties
Windows Defender Application Control 1 items
Search

Icon	Name	Revision	Deployed
	Window Base WDAC Policy	1	No

2. Select **Browse**



Application Control Policy name: Window Base WDAC Policy

Collection:

□ Allow remediation outside the maintenance window

Schedule

Specify the compliance evaluation schedule for this Application Control Policy:

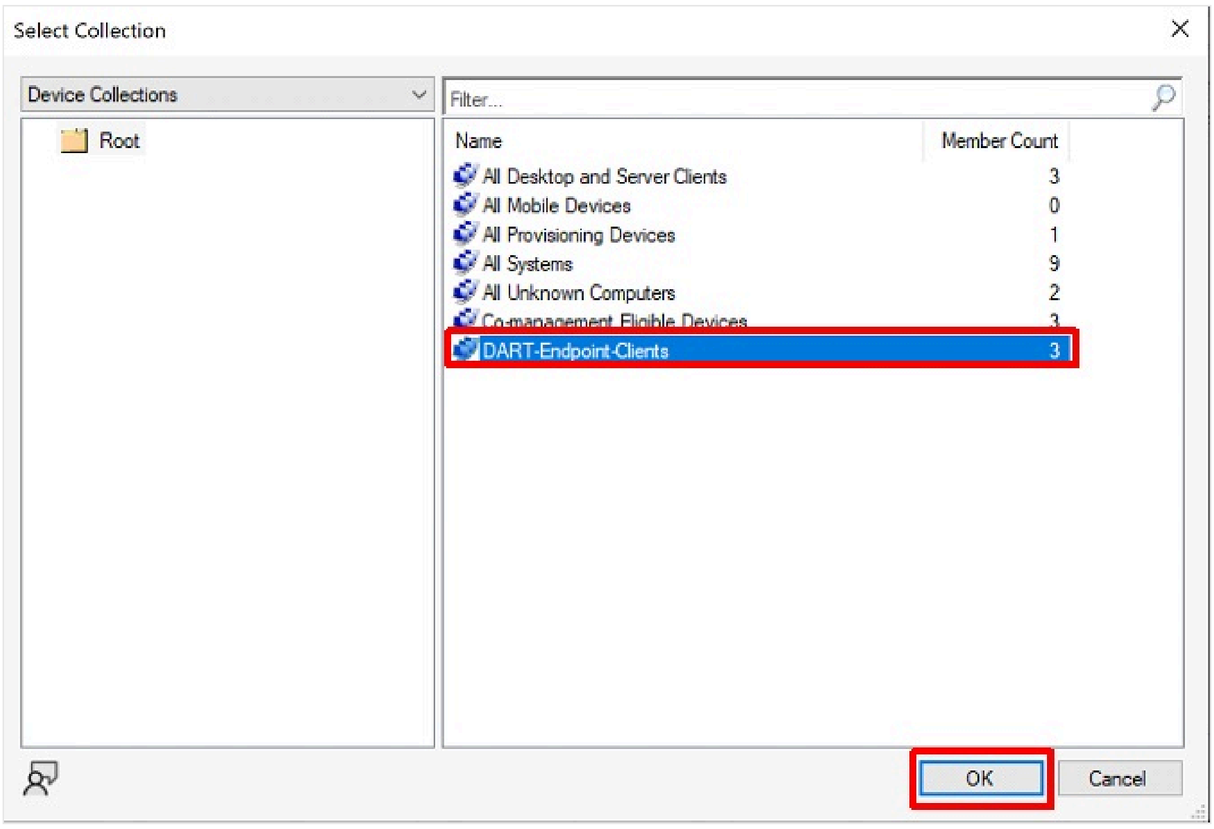
● Simple schedule

Run every: 7 Days

○ Custom schedule

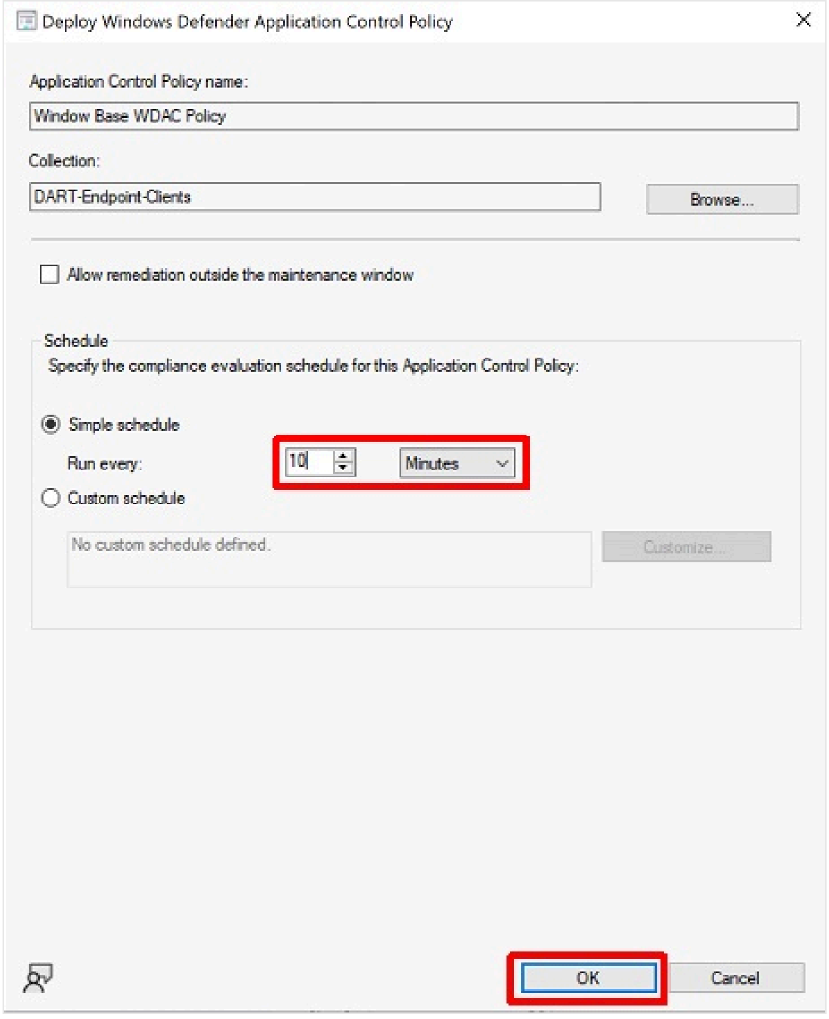
No custom schedule defined.

3. Select the Device Collection you created earlier > **OK**



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

□ 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.

For more information on using Configuration Manager's native App Control policies, see App Control for Business management with Configuration Manager.

Download the entire App Control in Configuration Manager lab paper.

Deploy custom App Control policies using Packages/Programs or Task Sequences

Using Configuration Manager's built-in policies can be a helpful starting point, but customers may find the circle-of-trust options available in Configuration Manager too limiting. To define your own circle-of-trust, you can use Configuration Manager to deploy custom App Control policies using script-based deployment via Software Distribution Packages and Programs or Operating System Deployment Task Sequences.

Feedback

Was this page helpful? Yes No

Provide product feedback

Additional resources

Training

Module
MD-102 3-Deploy using Endpoint Configuration Manager - Training

This module explains the common day to day tasks that Administrators would use Configuration Manager to perform.

Certification
Microsoft 365 Certified: Endpoint Administrator Associate - Certifications

Plan and execute an endpoint deployment strategy, using essential elements of modern management, co-management approaches, and Microsoft Intune integration.