Deploy App Control policies using script

Article • 10/22/2024 • 2 contributors •

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

Feedback

In this article

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

This article describes how to deploy App Control for Business policies using script. The following instructions use PowerShell but can work with any scripting host.

You should now have one or more App Control policies converted into binary form. If not, follow the steps described in Deploying App Control for Business policies.

> **Important**
>
> Due to a known issue in Windows 11 updates earlier than 2024 (24H2), you should always activate new **signed** App Control Base policies with a reboot on systems with memory integrity enabled. Skip all steps below that use CiTool, RefreshPolicy.exe, or WMI to initiate a policy activation. Instead, copy the policy binary to the correct system32 and EFI locations and then activate the policy with a system restart.
>
> This issue does not affect updates to signed Base policies that are already active on the system, deployment of unsigned policies, or deployment of supplemental policies (signed or unsigned). It also does not affect deployments to systems that are not running memory integrity.

Deploying policies for Windows 11 22H2 and above, and Windows Server 2025 and above

You can use the inbox CiTool to deploy signed and unsigned policies on Windows 11 22H2 and Windows Server 2025 with the following commands. Be sure to replace `<Path to policy binary file to deploy>` in the following example with the actual path to your App Control policy binary file.

PowerShell Copy

```
# Policy binary files should be named as {GUID}.cip for multiple policy format files (wher
$PolicyBinary = "<Path to policy binary file to deploy>"
CiTool --update-policy $PolicyBinary [-json]
```

Deploying policies for Windows 11, Windows 10 version 1903 and above, and Windows Server 2022 and above

To use this procedure, download and distribute the App Control policy refresh tool to all managed endpoints. Ensure your App Control policies allow the App Control policy refresh tool or use a managed installer to distribute the tool.

1. Initialize the variables to be used by the script.

```powershell
# Policy binary files should be named as {GUID}.cip for multiple policy format files
$PolicyBinary = "<Path to policy binary file to deploy>"
$DestinationFolder = $env:windir+"\System32\CodeIntegrity\CIPolicies\Active\"
$RefreshPolicyTool = "<Path where RefreshPolicy.exe can be found from managed endpoint
```

2. Copy App Control for Business policy binary to the destination folder.

```powershell
Copy-Item -Path $PolicyBinary -Destination $DestinationFolder -Force
```

3. Repeat steps 1-2 as appropriate to deploy more App Control policies.

4. Run RefreshPolicy.exe to activate and refresh all App Control policies on the managed endpoint.

```powershell
& $RefreshPolicyTool
```

Deploying policies for all other versions of Windows and Windows Server

Use WMI to deploy policies on all other versions of Windows and Windows Server.

1. Initialize the variables to be used by the script.

```powershell
# Policy binary files should be named as SiPolicy.p7b for Windows 10 versions earlier
$PolicyBinary = "<Path to policy binary file to deploy>"
$DestinationBinary = $env:windir+"\System32\CodeIntegrity\SiPolicy.p7b"
```

2. Copy App Control for Business policy binary to the destination.

```powershell
Copy-Item  -Path $PolicyBinary -Destination $DestinationBinary -Force
```

3. Refresh and activate App Control policy using WMI

```powershell
Invoke-CimMethod -Namespace root\Microsoft\Windows\CI -ClassName PS_UpdateAndCompareCI
```

Deploying signed policies

If you're using signed App Control policies, the policies must be deployed into your device's EFI partition.

1. Mount the EFI volume and make the directory, if it doesn't exist, in an elevated PowerShell prompt:

```powershell
$MountPoint = 'C:\EFIMount'
$EFIDestinationFolder = "$MountPoint\EFI\Microsoft\Boot\CiPolicies\Active"
$EFIPartition = (Get-Partition | Where-Object IsSystem).AccessPaths[0]
if (-Not (Test-Path $MountPoint)) { New-Item -Path $MountPoint -Type Directory -Force
mountvol $MountPoint $EFIPartition
if (-Not (Test-Path $EFIDestinationFolder)) { New-Item -Path $EFIDestinationFolder -Ty
```

2. Copy the signed policy to the created folder:

```powershell
Copy-Item -Path $PolicyBinary -Destination $EFIDestinationFolder -Force
```

3. Restart the system.

Feedback

Was this page helpful? Yes No

Provide product feedback

Additional resources

Training

Module

Deploy and update applications - Training

In this module, you will be introduced to application deployment in Intune and Microsoft Store for Business.

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.