Deploy Cisco Secure Endpoint/Secure Client using Microsoft Intune

Contents

Introduction

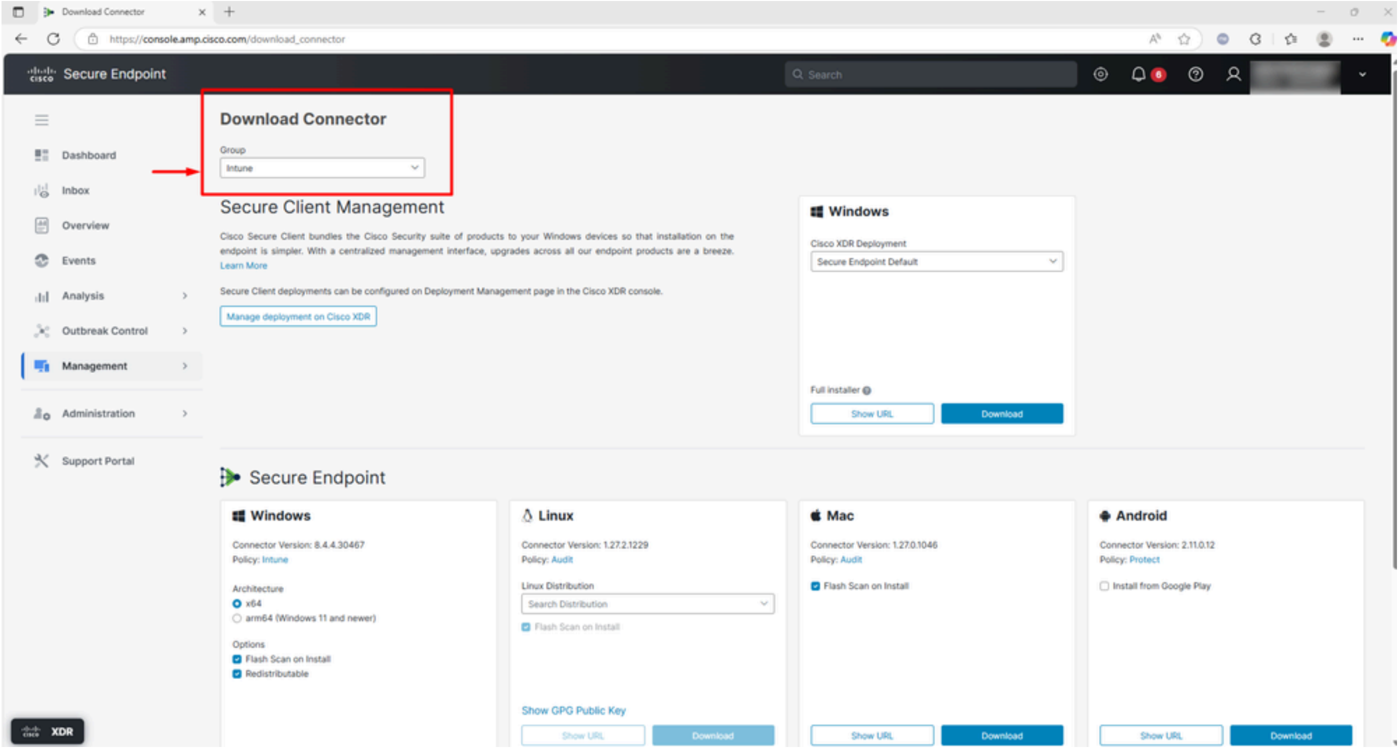
This document outlines the process for deploying Cisco Secure Endpoint or Secure Client using Microsoft Intune. The document walks through the steps on how to create a Microsoft Intune supported apps from the Secure Endpoint/Secure Client installers and then use that for deployment using the Microsoft Intune admin center. Specifically, the process includes packaging the Cisco Secure Endpoint installer as a Win32 application using the Intune Win32 Content Prep Tool, followed by configuring and deploying the app through Intune. We have utilized the official Microsoft Prep Tool for creating the app.

Configuration

Secure Endpoint Deployment

Step 1. Download the Cisco Secure Endpoint Installer.

- Login to your respective Secure Endpoint Portal, depending on the region: https://apps.security.cisco.com/overview
- Navigate to the **Management** tab and select **Download Connector**
- Select the Secure Endpoint **group** you want the connector to register to



Download Connector

Group: Intune

Secure Client Management

Cisco Secure Client bundles the Cisco Security suite of products to your Windows devices so that installation on the endpoint is simpler. With a centralized management interface, upgrades across all our endpoint products are a breeze. Learn More

Secure Client deployments can be configured on Deployment Management page in the Cisco XDR console.

Windows

Cisco XDR Deployment: Secure Endpoint Default

Secure Endpoint

Windows

Connector Version: 8.4.4.30467
Policy: Intune

Architecture
● x64
○ arm64 (Windows 11 and newer)

Options
☑ Flash Scan on Install
☑ Redistributable

Linux

Connector Version: 1.27.2.1229
Policy: Audit

Linux Distribution: Search Distribution
☑ Flash Scan on Install

Mac

Connector Version: 1.27.0.1046
Policy: Audit

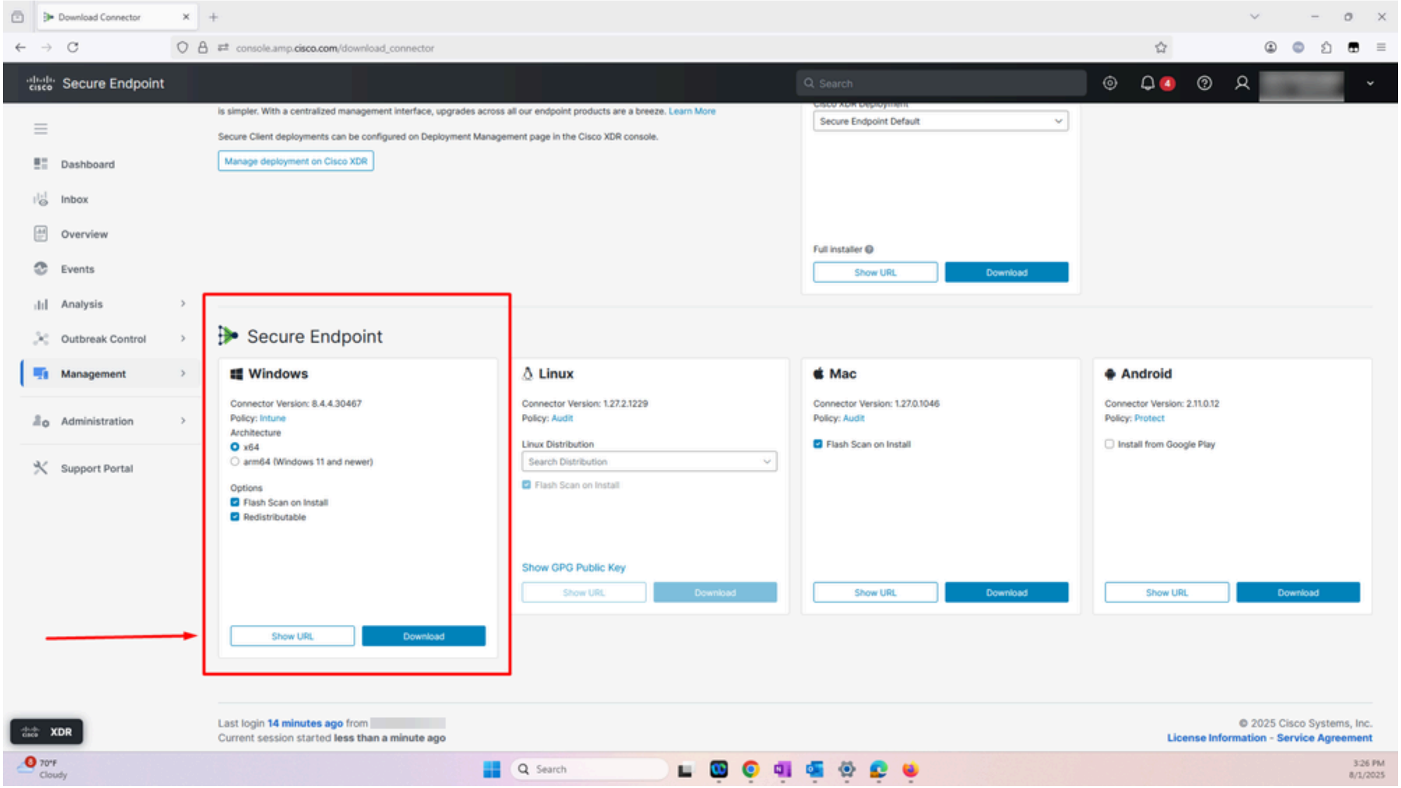
☑ Flash Scan on Install

Android

Connector Version: 2.11.0.12
Policy: Protect

□ Install from Google Play

- Select **download** and the EXE installer gets downloaded locally as shown in the screenshot



is simpler. With a centralized management interface, upgrades across all our endpoint products are a breeze. Learn More

Secure Client deployments can be configured on Deployment Management page in the Cisco XDR console.

Cisco XDR Deployment: Secure Endpoint Default

Secure Endpoint

Windows

Connector Version: 8.4.4.30467
Policy: Intune
Architecture
● x64
○ arm64 (Windows 11 and newer)

Options
☑ Flash Scan on Install
☑ Redistributable

Linux

Connector Version: 1.27.2.1229
Policy: Audit

Linux Distribution: Search Distribution
☑ Flash Scan on Install

Mac

Connector Version: 1.27.0.1046
Policy: Audit

☑ Flash Scan on Install

Android

Connector Version: 2.11.0.12
Policy: Protect

□ Install from Google Play

Last login 14 minutes ago from [redacted]
Current session started less than a minute ago

© 2025 Cisco Systems, Inc.
License Information - Service Agreement

Step 2. Prepare the Intune file using Win32 Content Prep Tool.

The Win32 Content Prep Tool is a utility provided by Microsoft Intune to help IT administrators prepare Win32 applications (i.e., traditional Windows desktop apps) for deployment through Microsoft Intune. The tool converts Win32 application installers (like .exe, .msi, and related files) into a .intunewin file format, which is required for deploying these apps via Intune.

To prepare the Intune file, follow these step:

- Download the Win32 Content Prep Tool from Github.
  Download: https://github.com/microsoft/Microsoft-Win32-Content-Prep-Tool

- Execute **IntuneWinAppUtil.exe**

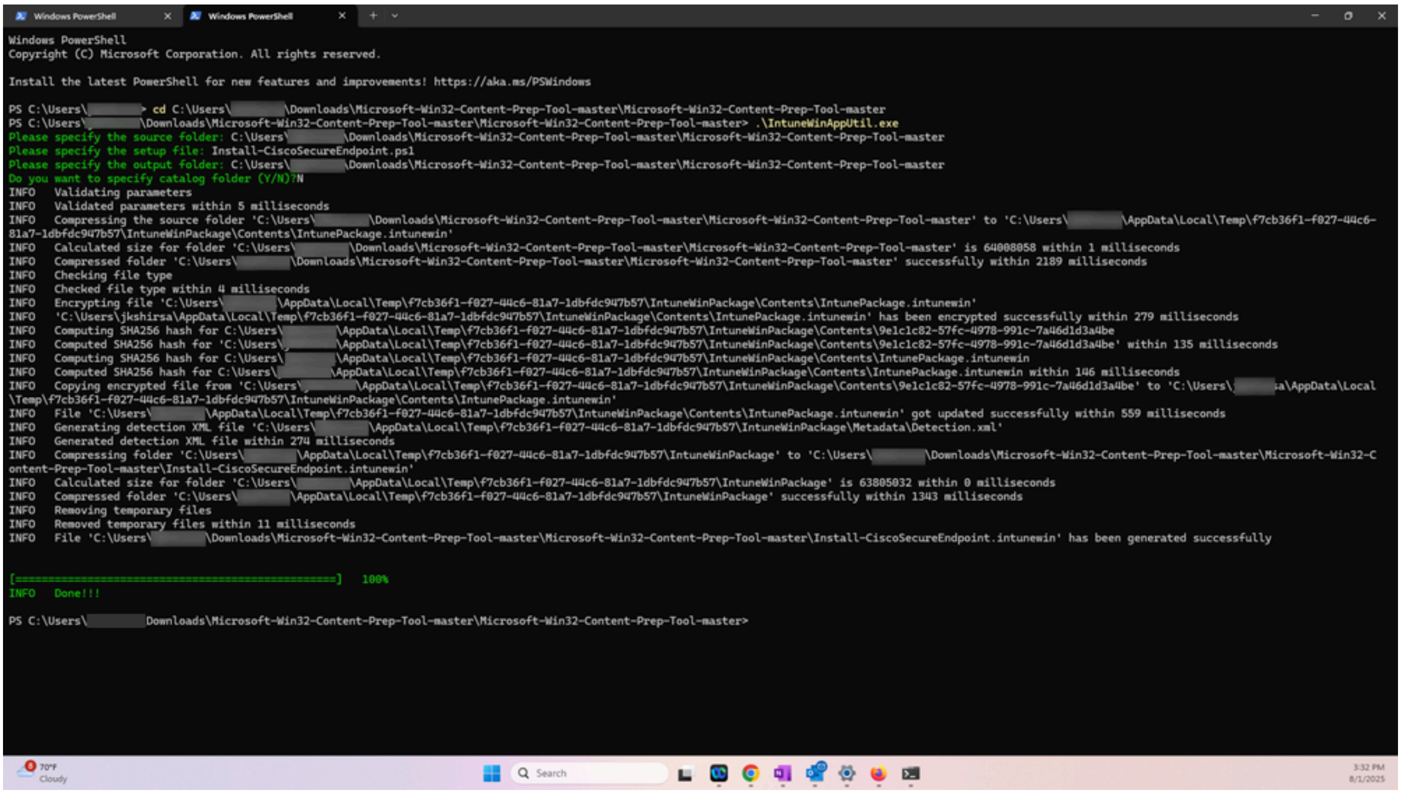
- In the next step, change directory to the folder that contains the Cisco Secure Endpoint executable file that was downloaded in step 1 and the install powershell script **(Install-CiscoSecureEndpoint.ps1**)

- Then specify the script filename for the setup file: **Install-CiscoSecureEndpoint.ps1**

- In the next step, specify the folder where the **Intunewin** file must be generated

- Enter **N**, when prompted to specify catalog

- **Intunewin** File is generated as shown in the screenshot:



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\[redacted]> cd C:\Users\[redacted]\Downloads\Microsoft-Win32-Content-Prep-Tool-master\Microsoft-Win32-Content-Prep-Tool-master
PS C:\Users\[redacted]\Downloads\Microsoft-Win32-Content-Prep-Tool-master\Microsoft-Win32-Content-Prep-Tool-master> .\IntuneWinAppUtil.exe
Please specify the source folder: C:\Users\[redacted]\Downloads\Microsoft-Win32-Content-Prep-Tool-master\Microsoft-Win32-Content-Prep-Tool-master
Please specify the setup file: Install-CiscoSecureEndpoint.ps1
Please specify the output folder: C:\Users\[redacted]\Downloads\Microsoft-Win32-Content-Prep-Tool-master\Microsoft-Win32-Content-Prep-Tool-master
Do you want to specify catalog folder (Y/N)?N
INFO   Validating parameters
INFO   Validated parameters within 5 milliseconds
INFO   Compressing the source folder 'C:\Users\[redacted]\Downloads\Microsoft-Win32-Content-Prep-Tool-master\Microsoft-Win32-Content-Prep-Tool-master' to 'C:\Users\[redacted]\AppData\Local\Temp\f7cb36f1-f027-44c6-
81a7-1dbfdc947b57\IntuneWinPackage\Contents\IntunePackage.intunewin'
INFO   Calculated size for folder 'C:\Users\[redacted]\Downloads\Microsoft-Win32-Content-Prep-Tool-master\Microsoft-Win32-Content-Prep-Tool-master' is 64008058 within 1 milliseconds
INFO   Compressed folder 'C:\Users\[redacted]\Downloads\Microsoft-Win32-Content-Prep-Tool-master\Microsoft-Win32-Content-Prep-Tool-master' successfully within 2189 milliseconds
INFO   Checking file type
INFO   Checked file type within 4 milliseconds
INFO   Encrypting file 'C:\Users\[redacted]\AppData\Local\Temp\f7cb36f1-f027-44c6-81a7-1dbfdc947b57\IntuneWinPackage\Contents\IntunePackage.intunewin'
INFO   'C:\Users\jkshirsa\AppData\Local\Temp\f7cb36f1-f027-44c6-81a7-1dbfdc947b57\IntuneWinPackage\Contents\IntunePackage.intunewin' has been encrypted successfully within 279 milliseconds
INFO   Computing SHA256 hash for C:\Users\[redacted]\AppData\Local\Temp\f7cb36f1-f027-44c6-81a7-1dbfdc947b57\IntuneWinPackage\Contents\9e1c1c82-57fc-4978-991c-7a46d1d3a4be
INFO   Computed SHA256 hash for 'C:\Users\[redacted]\AppData\Local\Temp\f7cb36f1-f027-44c6-81a7-1dbfdc947b57\IntuneWinPackage\Contents\9e1c1c82-57fc-4978-991c-7a46d1d3a4be' within 135 milliseconds
INFO   Computing SHA256 hash for C:\Users\[redacted]\AppData\Local\Temp\f7cb36f1-f027-44c6-81a7-1dbfdc947b57\IntuneWinPackage\Contents\IntunePackage.intunewin
INFO   Computed SHA256 hash for C:\Users\[redacted]\AppData\Local\Temp\f7cb36f1-f027-44c6-81a7-1dbfdc947b57\IntuneWinPackage\Contents\IntunePackage.intunewin within 146 milliseconds
INFO   Copying encrypted file from 'C:\Users\[redacted]\AppData\Local\Temp\f7cb36f1-f027-44c6-81a7-1dbfdc947b57\IntuneWinPackage\Contents\9e1c1c82-57fc-4978-991c-7a46d1d3a4be' to 'C:\Users\[redacted]\AppData\Local
\Temp\f7cb36f1-f027-44c6-81a7-1dbfdc947b57\IntuneWinPackage\Contents\IntunePackage.intunewin'
INFO   File 'C:\Users\[redacted]\AppData\Local\Temp\f7cb36f1-f027-44c6-81a7-1dbfdc947b57\IntuneWinPackage\Contents\IntunePackage.intunewin' got updated successfully within 559 milliseconds
INFO   Generating detection XML file 'C:\Users\[redacted]\AppData\Local\Temp\f7cb36f1-f027-44c6-81a7-1dbfdc947b57\IntuneWinPackage\Metadata\Detection.xml'
INFO   Generated detection XML file within 274 milliseconds
INFO   Compressing folder 'C:\Users\[redacted]\AppData\Local\Temp\f7cb36f1-f027-44c6-81a7-1dbfdc947b57\IntuneWinPackage' to 'C:\Users\[redacted]\Downloads\Microsoft-Win32-Content-Prep-Tool-master\Microsoft-Win32-C
ontent-Prep-Tool-master\Install-CiscoSecureEndpoint.intunewin'
INFO   Calculated size for folder 'C:\Users\[redacted]\AppData\Local\Temp\f7cb36f1-f027-44c6-81a7-1dbfdc947b57\IntuneWinPackage' is 63805032 within 0 milliseconds
INFO   Compressed folder 'C:\Users\[redacted]\AppData\Local\Temp\f7cb36f1-f027-44c6-81a7-1dbfdc947b57\IntuneWinPackage' successfully within 1343 milliseconds
INFO   Removing temporary files
INFO   Removed temporary files within 11 milliseconds
INFO   File 'C:\Users\[redacted]\Downloads\Microsoft-Win32-Content-Prep-Tool-master\Microsoft-Win32-Content-Prep-Tool-master\Install-CiscoSecureEndpoint.intunewin' has been generated successfully


[=================================================]   100%
INFO   Done!!!

PS C:\Users\[redacted]Downloads\Microsoft-Win32-Content-Prep-Tool-master\Microsoft-Win32-Content-Prep-Tool-master>
```

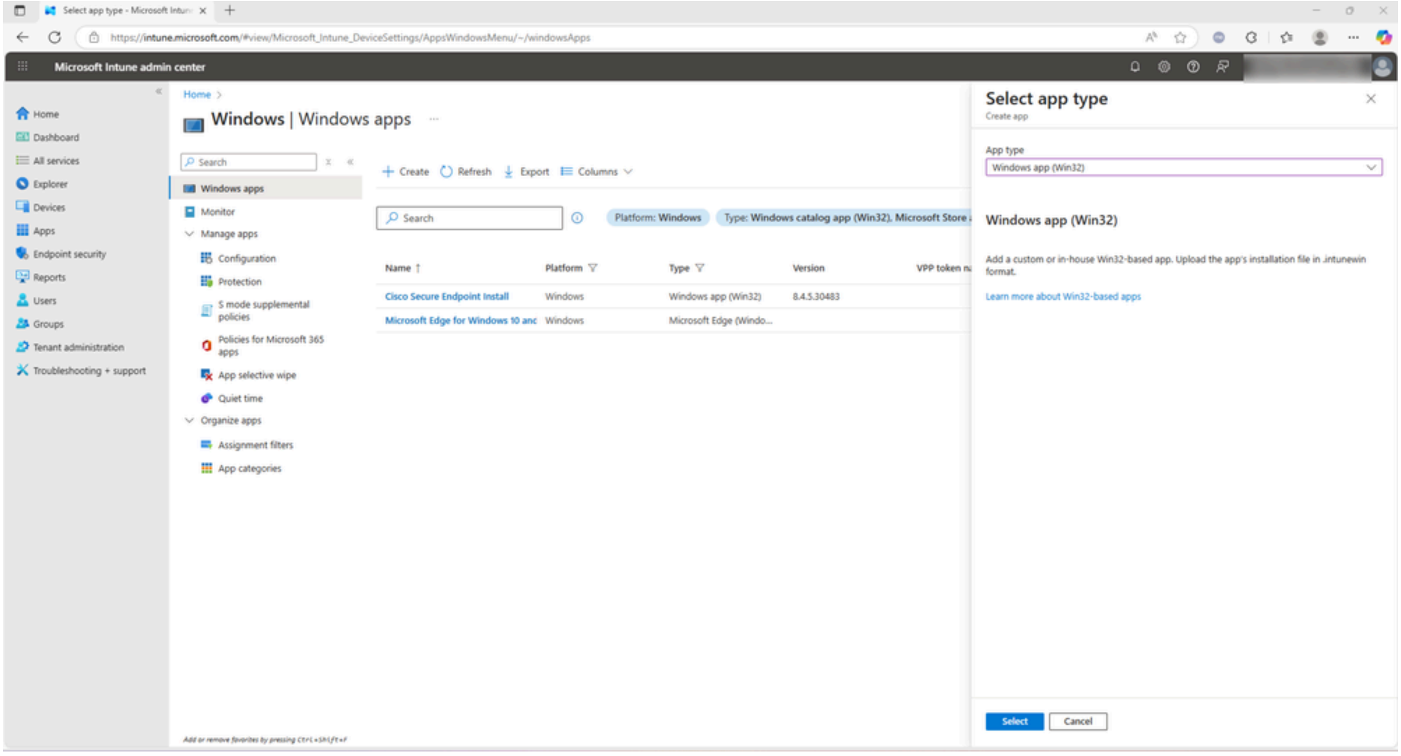
Step 3. Upload the Secure Endpoint IntuneWin File to Microsoft Intune Admin Center.

Perform the following steps:

- Log in to **Microsoft Intune Admin Center**

- Navigate to the **Windows Apps** in the Microsoft Intune Admin Center and Select **App Type – Win32** and **select**

These two actions are demonstrated in the screenshot:



Name	Platform	Type	Version	VPP token na
Cisco Secure Endpoint Install	Windows	Windows app (Win32)	8.4.5.30483	
Microsoft Edge for Windows 10 anc	Windows	Microsoft Edge (Windo...		

Select app type

Create app

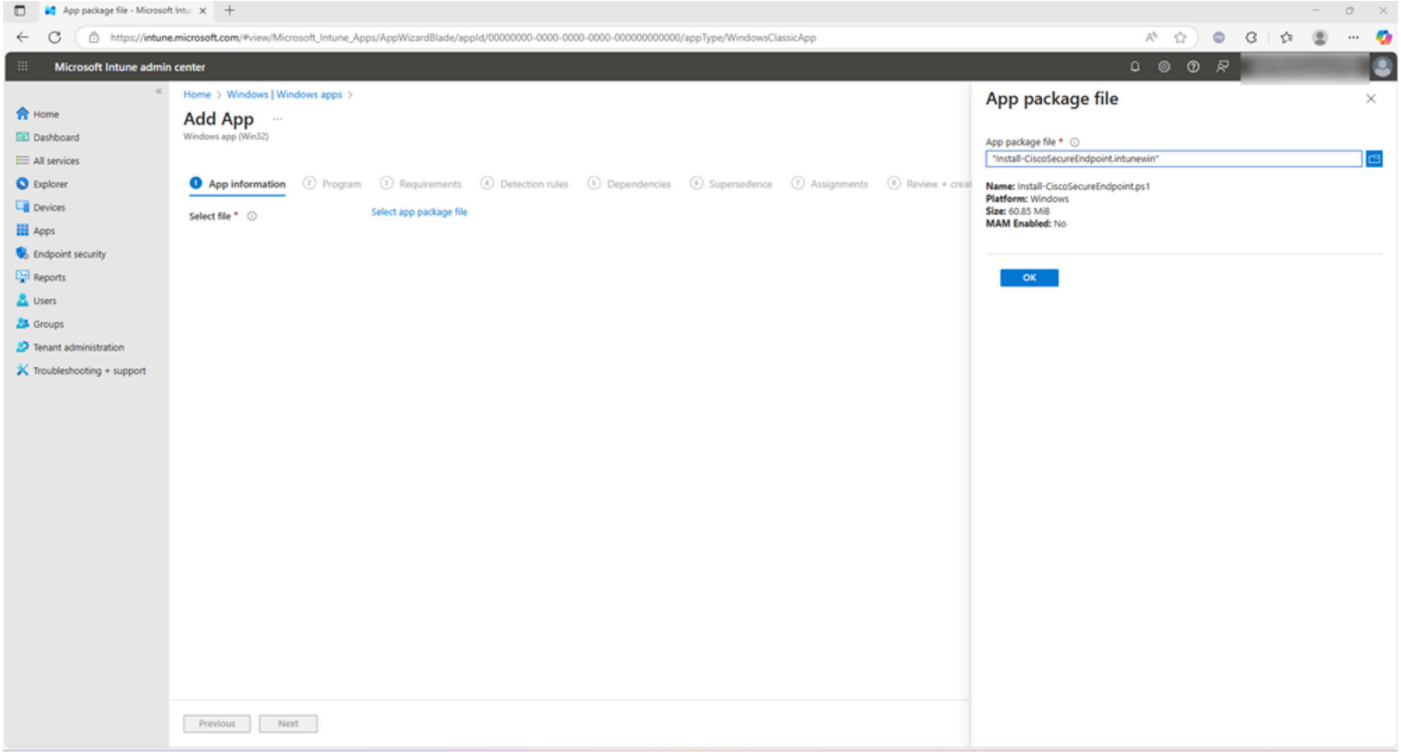
App type: Windows app (Win32)

Windows app (Win32)

Add a custom or in-house Win32-based app. Upload the app's installation file in .intunewin format.

Learn more about Win32-based apps

- In the next step, upload the Secure Endpoint Intunewin file created in step 2 and select **OK**



Add App

Windows app (Win32)

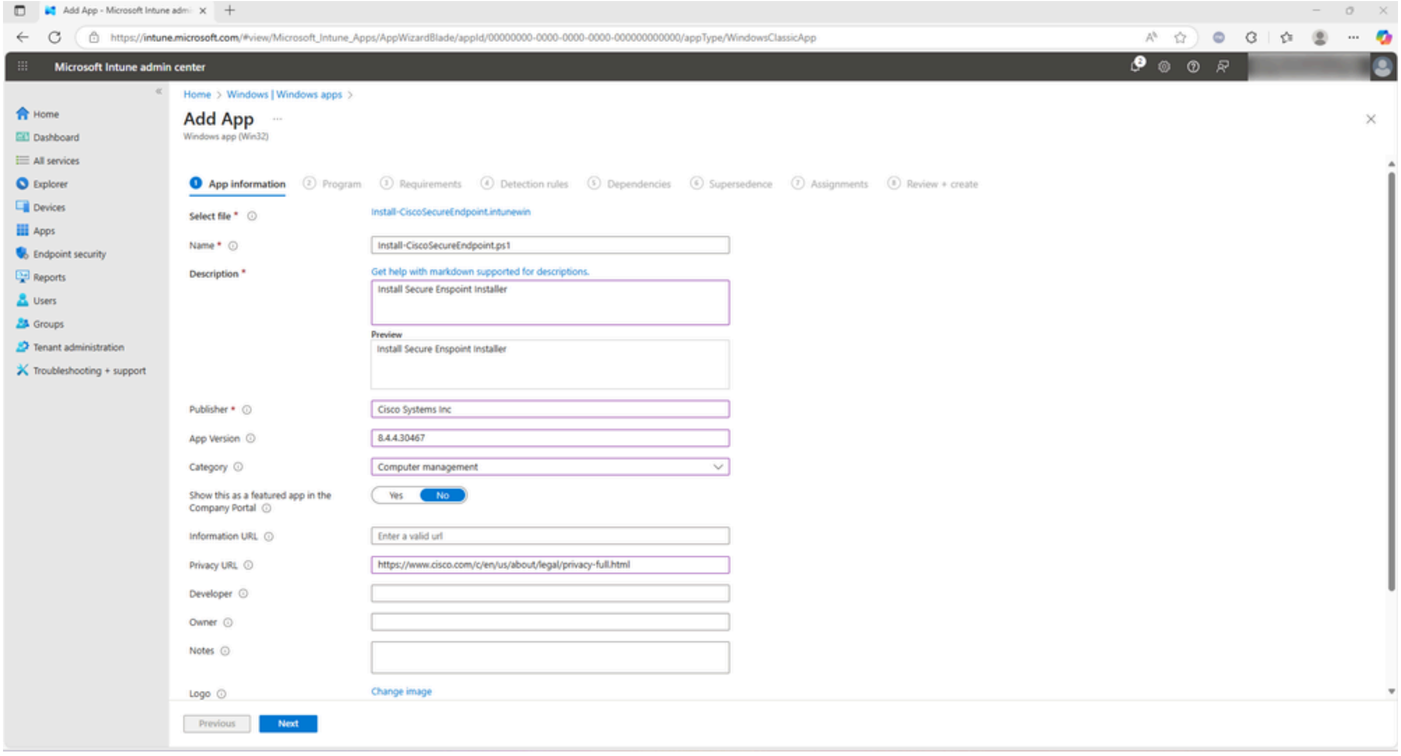
Select file * Select app package file

App package file

App package file * "Install-CiscoSecureEndpoint.intunewin"

Name: Install-CiscoSecureEndpoint.ps1
Platform: Windows
Size: 60.85 MiB
MAM Enabled: No

- After selecting **OK**, enter the information as presented in the screenshot. The optional fields can be left blank on each tab. Proceed to the next step by selecting **Next**


Add App - Microsoft Intune admin
https://intune.microsoft.com/#view/Microsoft_Intune_Apps/AppWizardBlade/appId/00000000-0000-0000-0000-000000000000/appType/WindowsClassicApp
Microsoft Intune admin center
Home
Dashboard
All services
Explorer
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Windows | Windows apps >
①App information
② Program
③ Requirements
④ Detection rules
⑤ Dependencies
⑥ Supersedence
⑦ Assignments
⑧ Review + create
Previous
Next

Add App

Windows app (Win32)

Select file *: Install-CiscoSecureEndpoint.intunewin

Name *: Install-CiscoSecureEndpoint.ps1

Description *: Install Secure Enspoint Installer

Get help with markdown supported for descriptions.

Preview: Install Secure Enspoint Installer

Publisher *: Cisco Systems Inc

App Version: 8.4.4.30467

Category: Computer management

Show this as a featured app in the Company Portal: Yes [✓ No]

Information URL: Enter a valid url

Privacy URL: https://www.cisco.com/c/en/us/about/legal/privacy-full.html

Developer:

Owner:

Notes:

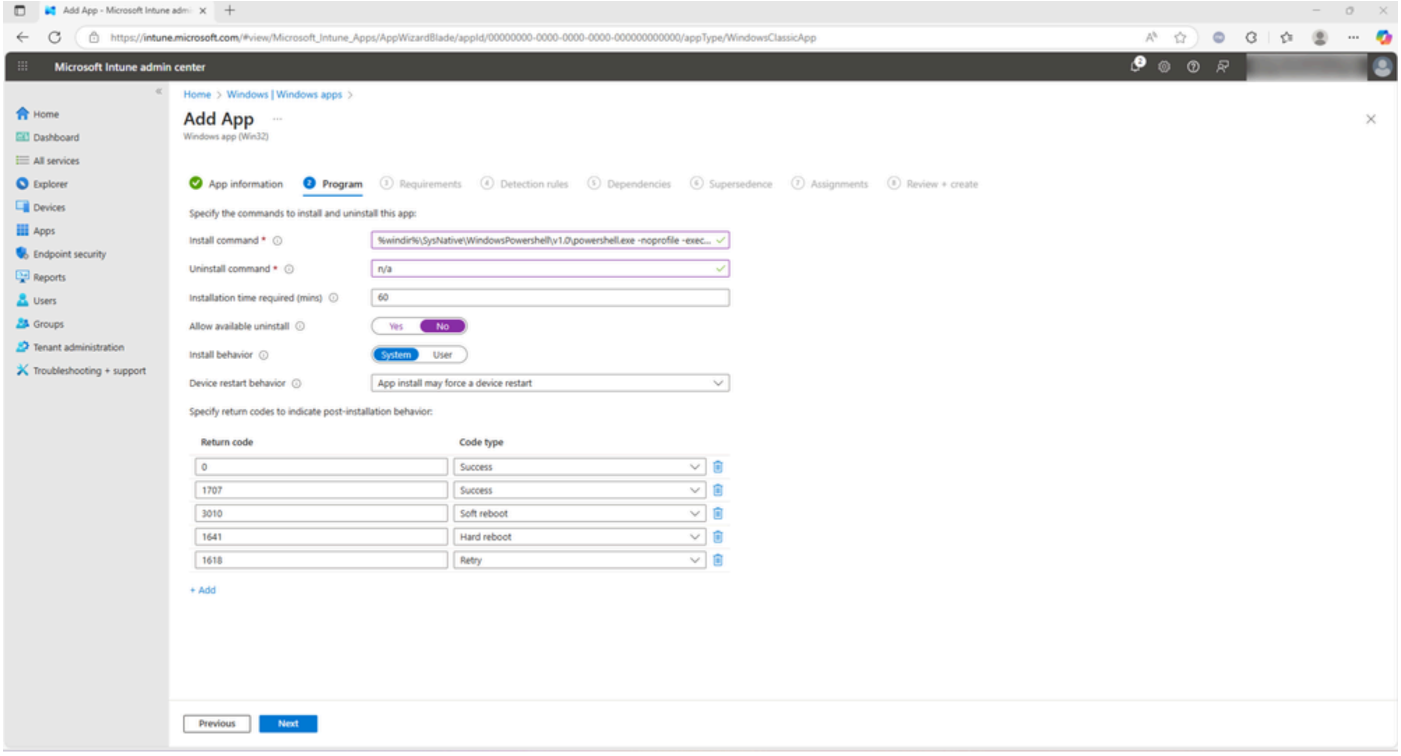
Logo: Change image

- Enter the **Install** Command as shown:

```
%windir%\SysNative\WindowsPowershell\v1.0\powershell.exe -noprofile -executionpolicy Bypass -file
```

Please note that the code presented here serves as an example and any code can be used as an install command for this installer

- Enter **Uninstall** as n/a and installation time required as 60 (optional). Set Allow available uninstall as **No**, select Install behavior as **System,**and enter any optional details before you select **Next**


Add App - Microsoft Intune admin
https://intune.microsoft.com/#view/Microsoft_Intune_Apps/AppWizardBlade/appId/00000000-0000-0000-0000-000000000000/appType/WindowsClassicApp
Microsoft Intune admin center
Home
Dashboard
All services
Explorer
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Windows | Windows apps >
App information
② Program
③ Requirements
④ Detection rules
⑤ Dependencies
⑥ Supersedence
⑦ Assignments
⑧ Review + create
+ Add
Previous
Next

Add App

Windows app (Win32)

Specify the commands to install and uninstall this app:

Install command *: %windir%\SysNative\WindowsPowershell\v1.0\powershell.exe -noprofile -exec...

Uninstall command *: n/a

Installation time required (mins): 60

Allow available uninstall: Yes [✓ No]

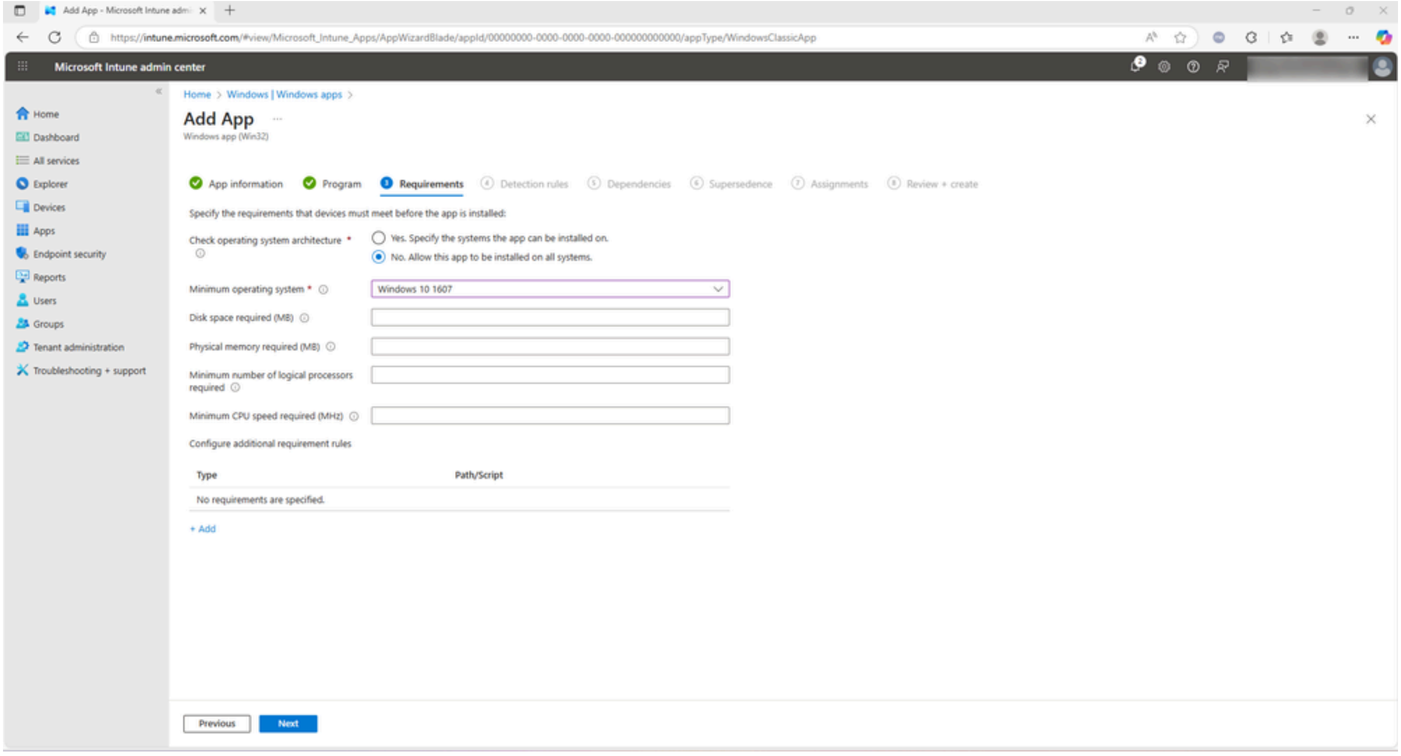
Install behavior: [✓ System] User

Device restart behavior: App install may force a device restart

Specify return codes to indicate post-installation behavior:

Return code	Code type
0	Success
1707	Success
3010	Soft reboot
1641	Hard reboot
1618	Retry

- On the requirements tab, check **No. Allow this app to be installed on all systems** and select the minimum operating system. Fill and optional fields if desired and select **Next**



Add App - Microsoft Intune adm
https://intune.microsoft.com/#view/Microsoft_Intune_Apps/AppWizardBlade/appId/00000000-0000-0000-0000-000000000000/appType/WindowsClassicApp
Microsoft Intune admin center
Home
Dashboard
All services
Explorer
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Home > Windows | Windows apps >
App information
Program
Requirements
4 Detection rules
5 Dependencies
6 Supersedence
7 Assignments
8 Review + create
Previous
Next

Add App ...

Windows app (Win32)

Specify the requirements that devices must meet before the app is installed:

Check operating system architecture *
○ Yes. Specify the systems the app can be installed on.
● No. Allow this app to be installed on all systems.

Minimum operating system * : Windows 10 1607

Disk space required (MB):

Physical memory required (MB):

Minimum number of logical processors required:

Minimum CPU speed required (MHz):

Configure additional requirement rules

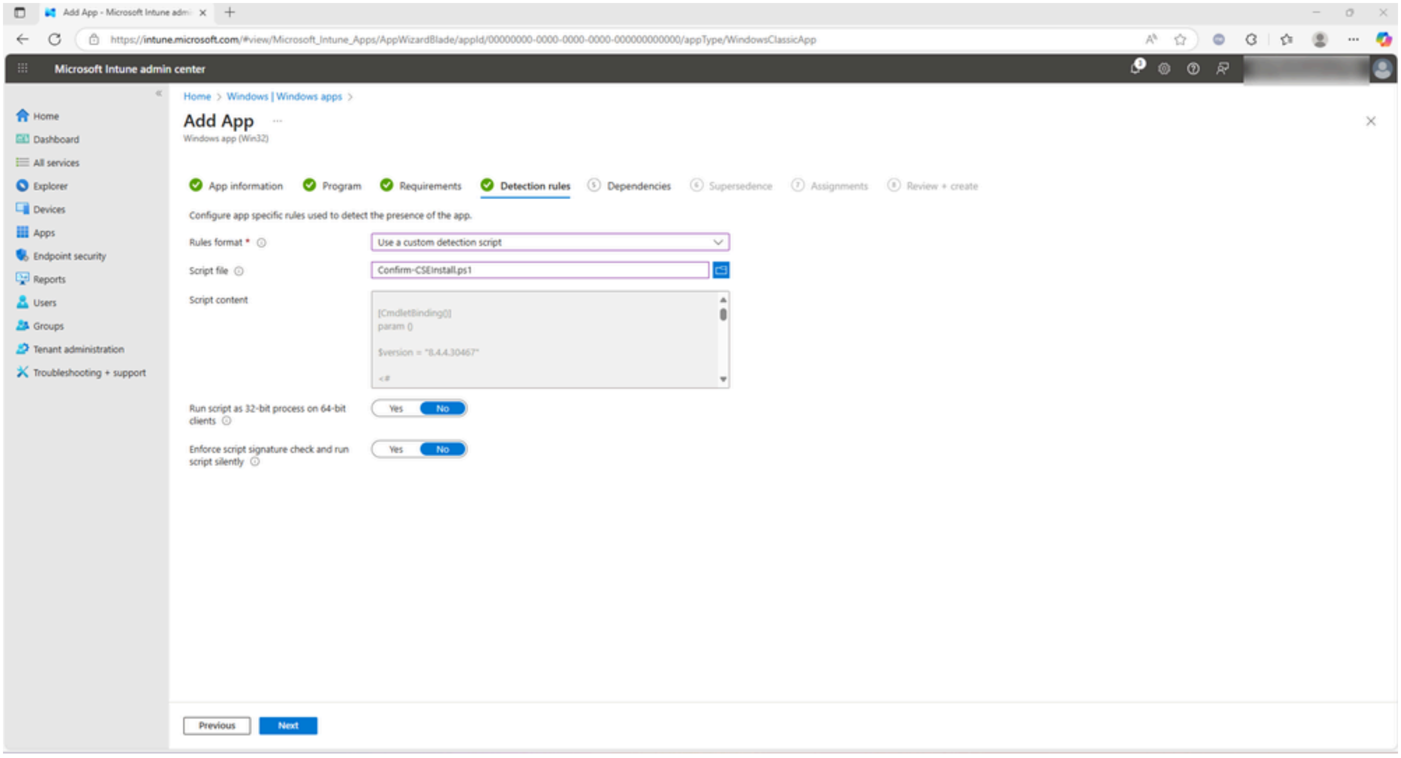
Type	Path/Script
No requirements are specified.	

+ Add

- On the **Detection Rules** tab, the Rules format drop-down menu provides two options: **Manually configure detection rules** and **Use a custom detection script**. Either option can be selected based on the deployment requirements.

- When choosing Manually configure detection rules, you can define a rule type such as MSI, File, or Registry to detect the presence of the application. In this document, the alternative option, **Use a custom detection script**, has been selected.

- A PowerShell script named **Confirm-CSEInstall.ps1** is used to verify successful installation of Cisco Secure Endpoint. It is listed at the bottom of this document.



Configure app specific rules used to detect the presence of the app.

Rules format *: Use a custom detection script

Script file: Confirm-CSEInstall.ps1

Script content:

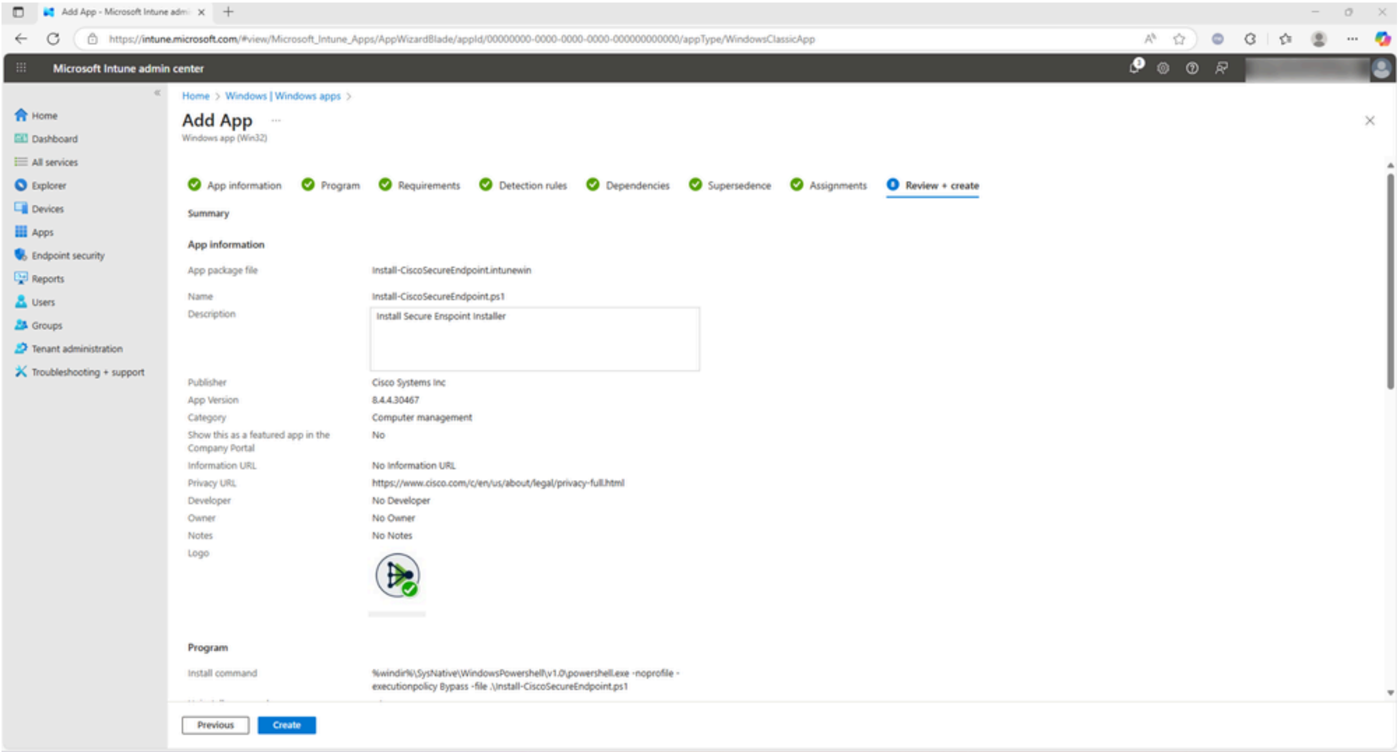
```
[CmdletBinding()]
param ()

$version = "8.4.4.30467"

<#
```

Run script as 32-bit process on 64-bit clients: Yes [✓ No]

Enforce script signature check and run script silently: Yes [✓ No]

- Select **Next** to proceed. Note: A custom detection script can be created specifically for this deployment process to suit your environment and detection criteria.

- The next few tabs are optional. No dependencies need to be configured, assign the application to the required group and select **Review + create**



Summary

App information

App package file: Install-CiscoSecureEndpoint.intunewin

Name: Install-CiscoSecureEndpoint.ps1

Description: Install Secure Enspoint Installer

Publisher: Cisco Systems Inc

App Version: 8.4.4.30467

Category: Computer management

Show this as a featured app in the Company Portal: No

Information URL: No Information URL

Privacy URL: https://www.cisco.com/c/en/us/about/legal/privacy-full.html

Developer: No Developer

Owner: No Owner

Notes: No Notes

Logo

Program

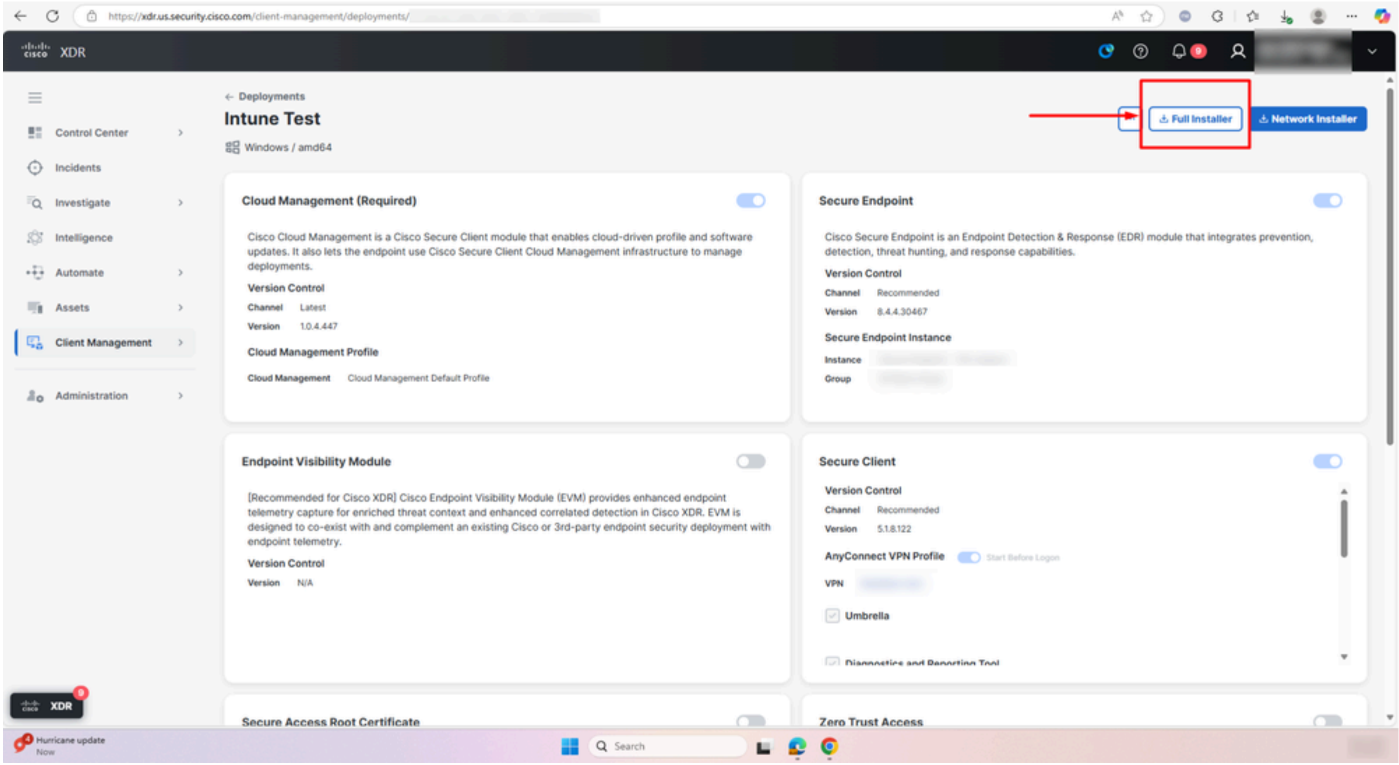
Install command: %windir%\SysNative\WindowsPowershell\v1.0\powershell.exe -noprofile -executionpolicy Bypass -file .\Install-CiscoSecureEndpoint.ps1

Secure Client Deployment

Step 1. Download the Cisco Secure Client Full Deployment

- Log in to the XDR or Secure Client Cloud Management console, depending on the region: https://apps.security.cisco.com/overview

- Create a new deployment and select **Full Installer** or **Network Installer** depending on your deployment type



← Deployments

Intune Test

Windows / amd64

Cloud Management (Required)

Cisco Cloud Management is a Cisco Secure Client module that enables cloud-driven profile and software updates. It also lets the endpoint use Cisco Secure Client Cloud Management infrastructure to manage deployments.

Version Control

Channel Latest

Version 1.0.4.447

Cloud Management Profile

Cloud Management Cloud Management Default Profile

Secure Endpoint

Cisco Secure Endpoint is an Endpoint Detection & Response (EDR) module that integrates prevention, detection, threat hunting, and response capabilities.

Version Control

Channel Recommended

Version 8.4.4.30467

Secure Endpoint Instance

Instance [redacted]

Group [redacted]

Endpoint Visibility Module

[Recommended for Cisco XDR] Cisco Endpoint Visibility Module (EVM) provides enhanced endpoint telemetry capture for enriched threat context and enhanced correlated detection in Cisco XDR. EVM is designed to co-exist with and complement an existing Cisco or 3rd-party endpoint security deployment with endpoint telemetry.

Version Control

Version N/A

Secure Client

Version Control

Channel Recommended

Version 5.1.8.122

AnyConnect VPN Profile Start Before Logon

VPN [redacted]

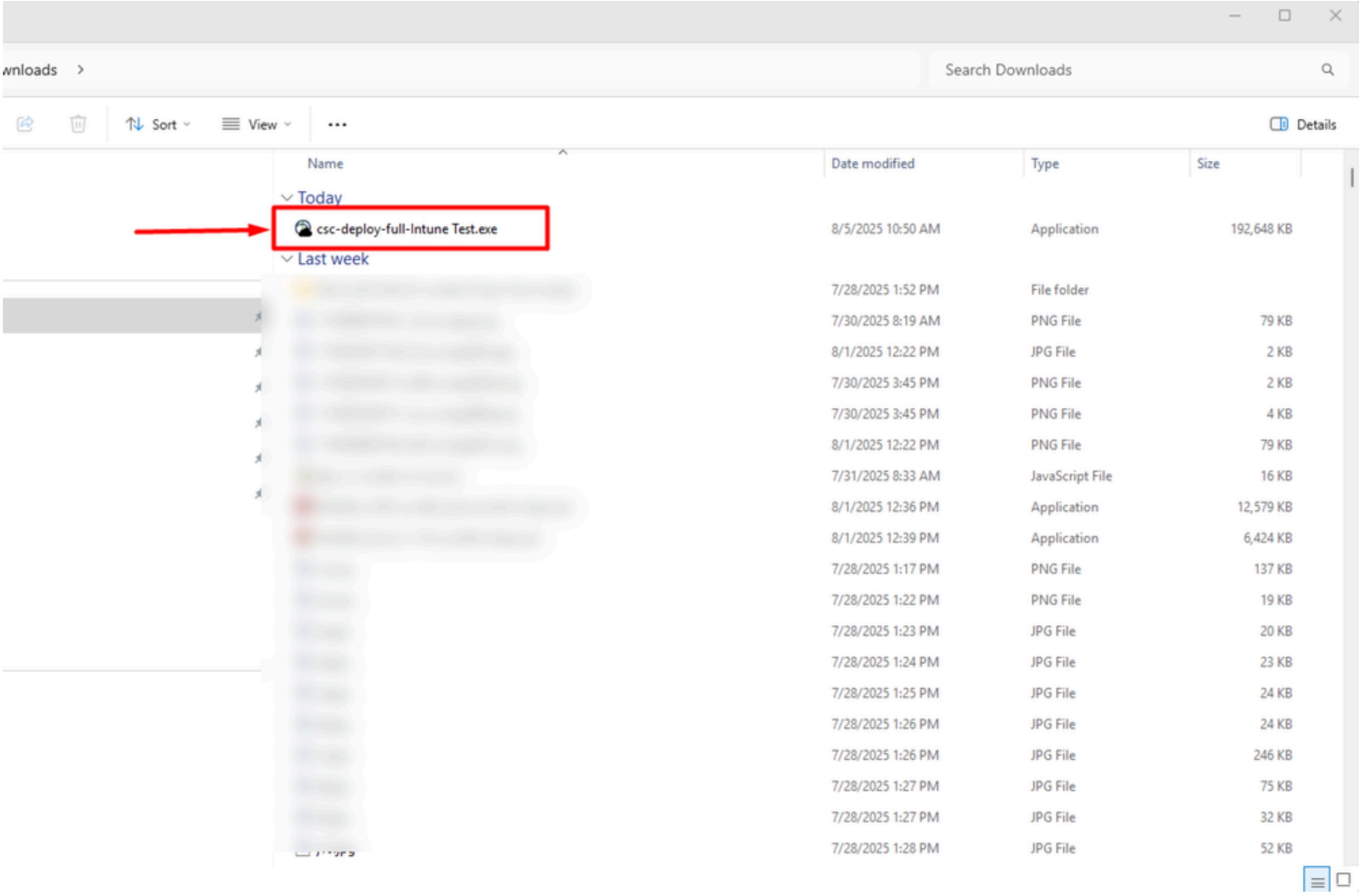
☑ Umbrella

☑ Diagnostics and Reporting Tool

Secure Access Root Certificate

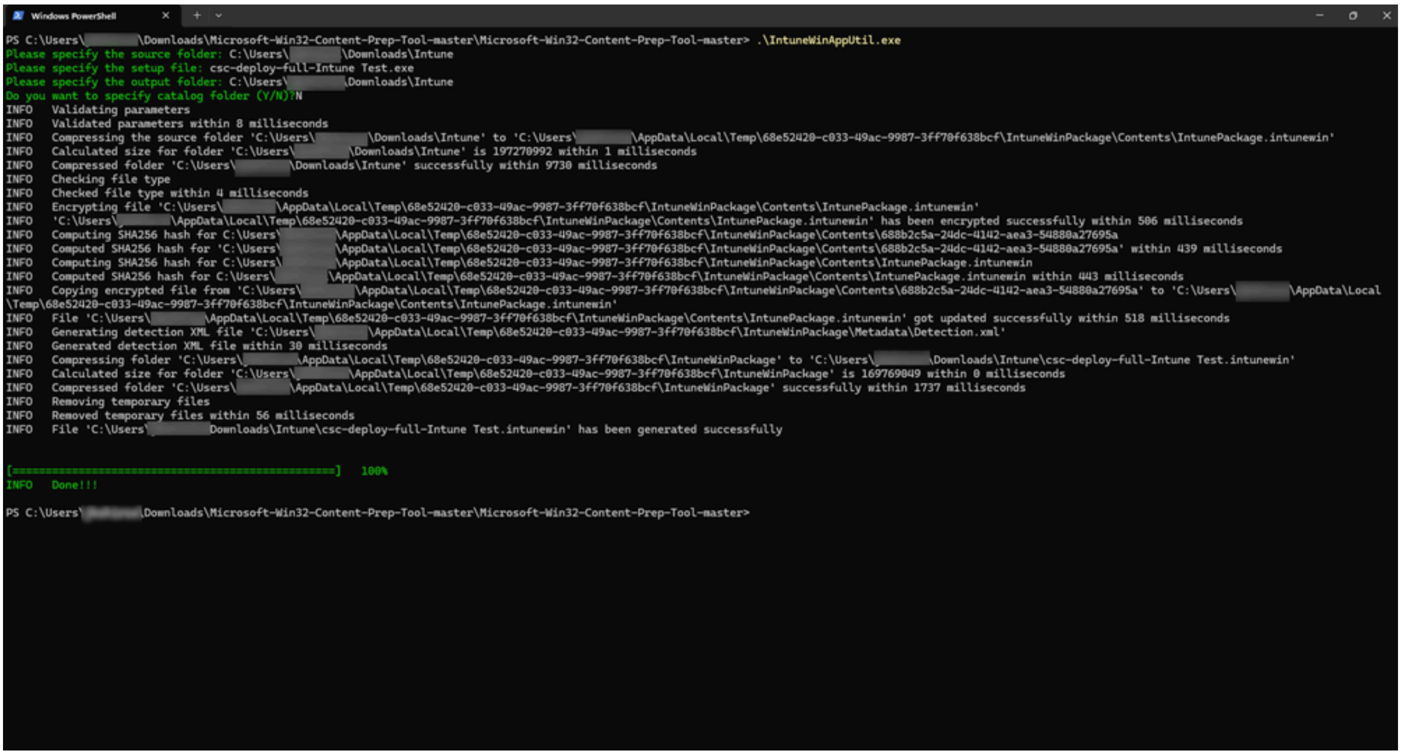
Zero Trust Access

- A **csc-deploy-full-Intune Test.exe** gets downloaded as shown in the screenshot.



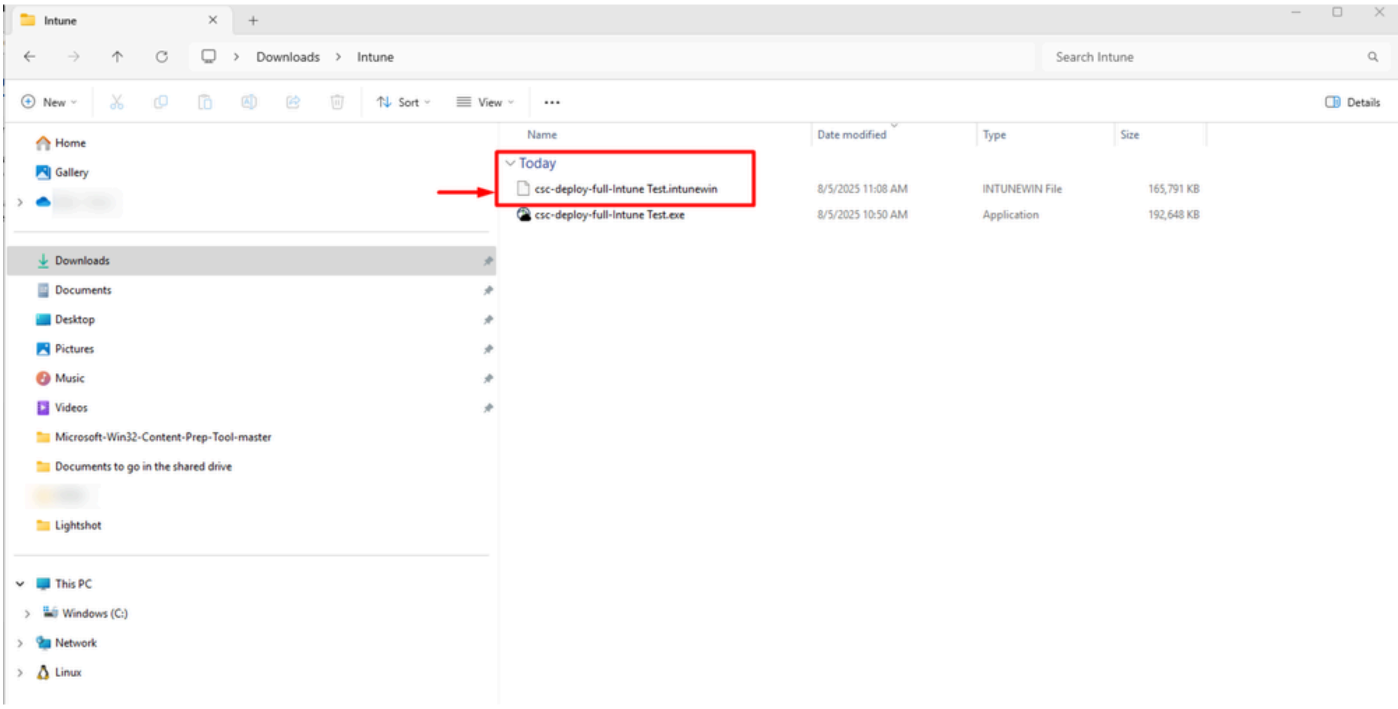
Name	Date modified	Type	Size
Today			
csc-deploy-full-Intune Test.exe	8/5/2025 10:50 AM	Application	192,648 KB
Last week			
[redacted]	7/28/2025 1:52 PM	File folder	
[redacted]	7/30/2025 8:19 AM	PNG File	79 KB
[redacted]	8/1/2025 12:22 PM	JPG File	2 KB
[redacted]	7/30/2025 3:45 PM	PNG File	2 KB
[redacted]	7/30/2025 3:45 PM	PNG File	4 KB
[redacted]	8/1/2025 12:22 PM	PNG File	79 KB
[redacted]	7/31/2025 8:33 AM	JavaScript File	16 KB
[redacted]	8/1/2025 12:36 PM	Application	12,579 KB
[redacted]	8/1/2025 12:39 PM	Application	6,424 KB
[redacted]	7/28/2025 1:17 PM	PNG File	137 KB
[redacted]	7/28/2025 1:22 PM	PNG File	19 KB
[redacted]	7/28/2025 1:23 PM	JPG File	20 KB
[redacted]	7/28/2025 1:24 PM	JPG File	23 KB
[redacted]	7/28/2025 1:25 PM	JPG File	24 KB
[redacted]	7/28/2025 1:26 PM	JPG File	24 KB
[redacted]	7/28/2025 1:26 PM	JPG File	246 KB
[redacted]	7/28/2025 1:27 PM	JPG File	75 KB
[redacted]	7/28/2025 1:27 PM	JPG File	32 KB
[redacted]	7/28/2025 1:28 PM	JPG File	52 KB

Step 2. Prepare the Intune file by following the same procedure in step 2. This creates csc-deploy-full-Intune Test.intunewin file.



```
PS C:\Users\[redacted]\Downloads\Microsoft-Win32-Content-Prep-Tool-master\Microsoft-Win32-Content-Prep-Tool-master> .\IntuneWinAppUtil.exe
Please specify the source folder: C:\Users\[redacted]\Downloads\Intune
Please specify the setup file: csc-deploy-full-Intune Test.exe
Please specify the output folder: C:\Users\[redacted]\Downloads\Intune
Do you want to specify catalog folder (Y/N)?N
INFO   Validating parameters
INFO   Validated parameters within 8 milliseconds
INFO   Compressing the source folder 'C:\Users\[redacted]\Downloads\Intune' to 'C:\Users\[redacted]\AppData\Local\Temp\68e52420-c033-49ac-9987-3ff70f638bcf\IntuneWinPackage\Contents\IntunePackage.intunewin'
INFO   Calculated size for folder 'C:\Users\[redacted]\Downloads\Intune' is 197270992 within 1 milliseconds
INFO   Compressed folder 'C:\Users\[redacted]\Downloads\Intune' successfully within 9730 milliseconds
INFO   Checking file type
INFO   Checked file type within 4 milliseconds
INFO   Encrypting file 'C:\Users\[redacted]\AppData\Local\Temp\68e52420-c033-49ac-9987-3ff70f638bcf\IntuneWinPackage\Contents\IntunePackage.intunewin'
INFO   'C:\Users\[redacted]\AppData\Local\Temp\68e52420-c033-49ac-9987-3ff70f638bcf\IntuneWinPackage\Contents\IntunePackage.intunewin' has been encrypted successfully within 506 milliseconds
INFO   Computing SHA256 hash for C:\Users\[redacted]\AppData\Local\Temp\68e52420-c033-49ac-9987-3ff70f638bcf\IntuneWinPackage\Contents\688b2c5a-24dc-4142-aea3-54880a27695a
INFO   Computed SHA256 hash for 'C:\Users\[redacted]\AppData\Local\Temp\68e52420-c033-49ac-9987-3ff70f638bcf\IntuneWinPackage\Contents\688b2c5a-24dc-4142-aea3-54880a27695a' within 439 milliseconds
INFO   Computing SHA256 hash for C:\Users\[redacted]\AppData\Local\Temp\68e52420-c033-49ac-9987-3ff70f638bcf\IntuneWinPackage\Contents\IntunePackage.intunewin
INFO   Computed SHA256 hash for C:\Users\[redacted]\AppData\Local\Temp\68e52420-c033-49ac-9987-3ff70f638bcf\IntuneWinPackage\Contents\IntunePackage.intunewin within 443 milliseconds
INFO   Copying encrypted file from 'C:\Users\[redacted]\AppData\Local\Temp\68e52420-c033-49ac-9987-3ff70f638bcf\IntuneWinPackage\Contents\688b2c5a-24dc-4142-aea3-54880a27695a' to 'C:\Users\[redacted]\AppData\Local
\Temp\68e52420-c033-49ac-9987-3ff70f638bcf\IntuneWinPackage\Contents\IntunePackage.intunewin'
INFO   File 'C:\Users\[redacted]\AppData\Local\Temp\68e52420-c033-49ac-9987-3ff70f638bcf\IntuneWinPackage\Contents\IntunePackage.intunewin' got updated successfully within 518 milliseconds
INFO   Generating detection XML file 'C:\Users\[redacted]\AppData\Local\Temp\68e52420-c033-49ac-9987-3ff70f638bcf\IntuneWinPackage\Metadata\Detection.xml'
INFO   Generated detection XML file within 30 milliseconds
INFO   Compressing folder 'C:\Users\[redacted]\AppData\Local\Temp\68e52420-c033-49ac-9987-3ff70f638bcf\IntuneWinPackage' to 'C:\Users\[redacted]\Downloads\Intune\csc-deploy-full-Intune Test.intunewin'
INFO   Calculated size for folder 'C:\Users\[redacted]\AppData\Local\Temp\68e52420-c033-49ac-9987-3ff70f638bcf\IntuneWinPackage' is 169769049 within 0 milliseconds
INFO   Compressed folder 'C:\Users\[redacted]\AppData\Local\Temp\68e52420-c033-49ac-9987-3ff70f638bcf\IntuneWinPackage' successfully within 1737 milliseconds
INFO   Removing temporary files
INFO   Removed temporary files within 56 milliseconds
INFO   File 'C:\Users\[redacted]Downloads\Intune\csc-deploy-full-Intune Test.intunewin' has been generated successfully


[=================================================]   100%
INFO   Done!!!

PS C:\Users\[redacted]Downloads\Microsoft-Win32-Content-Prep-Tool-master\Microsoft-Win32-Content-Prep-Tool-master>
```

- The above steps results in creating a csc-deploy-full-Intune Test.intunewin file as shown in the screenshot.



Name	Date modified	Type	Size
csc-deploy-full-Intune Test.intunewin	8/5/2025 11:08 AM	INTUNEWIN File	165,791 KB
csc-deploy-full-Intune Test.exe	8/5/2025 10:50 AM	Application	192,648 KB

Step 3. Upload the csc-deploy-full-intune Test.intunewin file from part 1 to Microsoft Intune Admin Center as per the steps shown above.

This completes the process to deploy Cisco Secure Endpoint using Intune.

Install-CiscoSecureEndpoint.ps1 script

```
[CmdletBinding()]
param ()

$cse_exe = <Secure Endpoint Installer>
$version = <Secure Endpoint Version>

if ($PSCommandPath -eq $null) {
    function GetPSCommandPath() {
        return $MyInvocation.PSCommandPath;
    }
    $PSCommandPath = GetPSCommandPath
}

$script = [pscustomobject]@{
    "Path" = Split-Path $PSCommandPath -Parent
    "Name" = Split-Path $PSCommandPath -Leaf
}

Set-Location -Path $script.Path

$cse_installer = [IO.Path]::Combine($script.Path, $cse_exe)
$csc_installer_args = "/R /S"

<#
    Cannot use -wait for 'Cisco Secure Endpoint' and therefore cannot get the exit code to return.
    Using -wait, returns varied results, instead use Get-Process and while loop to wait for installatio
#>
$install = Start-Process -WorkingDirectory "$($script.Path)" -FilePath "${cse_installer}" -ArgumentList

while (Get-Process "$($cse_exe -replace '.exe', '')" -ErrorAction SilentlyContinue)
{
    Start-Sleep -Seconds 10
}
```

Confirm-CSEInstall.ps1 script

```
[CmdletBinding()]
param ()

$version = <Secure Endpoint Version>

<#
    https://learn.microsoft.com/en-us/intune/intune-service/apps/apps-win32-add#step-4-detection-rules
    The app gets detected when the script both returns a 0 value exit code and writes a string value to

    The Intune agent checks the results from the script. It reads the values written by the script to t
    the standard error (STDERR) stream, and the exit code. If the script exits with a nonzero value, th
    the application detection status isn't installed. If the exit code is zero and STDOUT has data, the
    detection status is installed.
#>

$cse = Get-ItemProperty HKLM:\Software\Microsoft\Windows\CurrentVersion\Uninstall\*, HKLM:\SOFTWARE\Wow
if ($cse | Where-Object { [System.Version] $_.DisplayVersion -ge [System.Version] "${version}" })
{
    Write-Host "Installed"
    exit 0
}

exit 1
```