Bereitstellung von Cisco Secure Endpoint/Secure Client mit Microsoft Intune

Inhalt

Einleitung

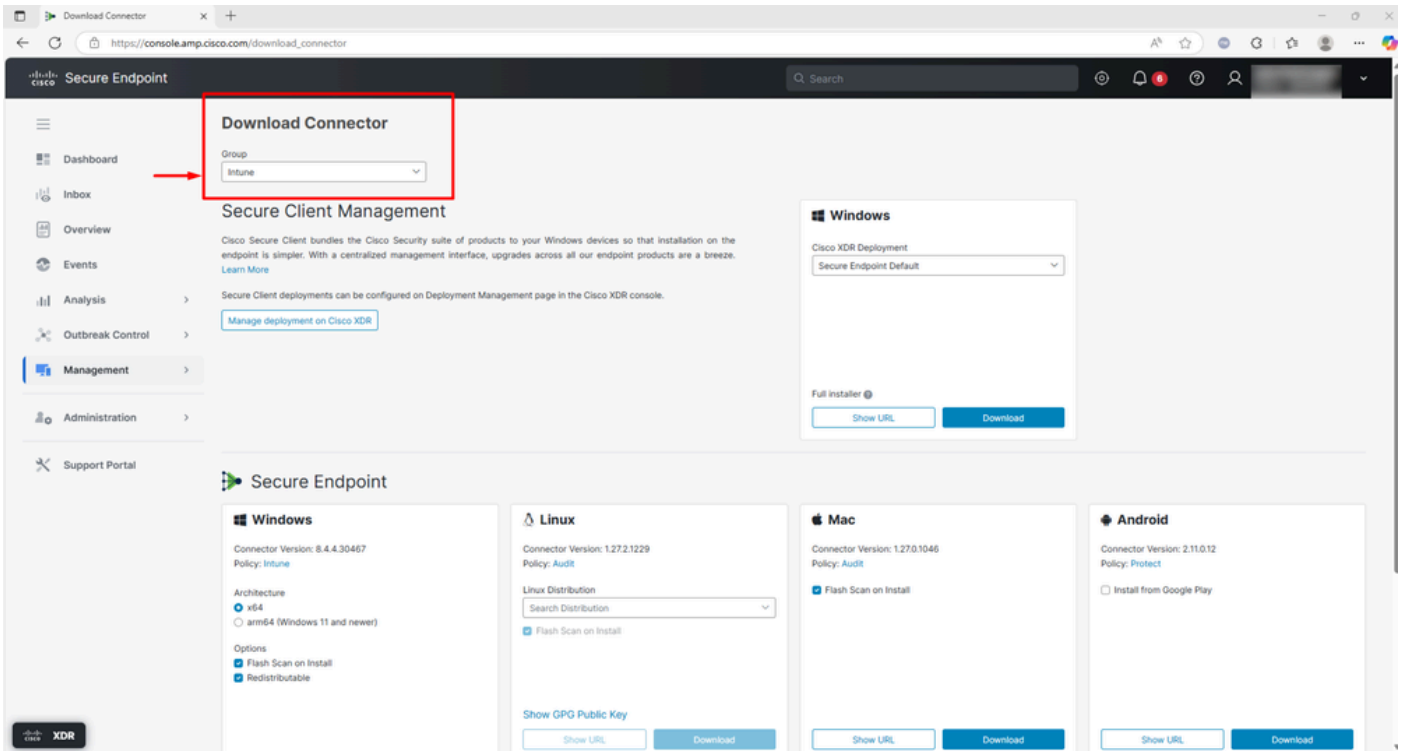
In diesem Dokument wird der Prozess für die Bereitstellung von Cisco Secure Endpoint oder Secure Client mit Microsoft Intune beschrieben. In diesem Dokument werden die Schritte zum Erstellen einer von Microsoft Intune unterstützten Anwendung mithilfe der Secure Endpoint/Secure Client-Installationsprogramme und zum anschließenden Verwenden dieser Anwendungen für die Bereitstellung mit dem Microsoft Intune-Admin-Center erläutert. Dabei wird der Cisco Secure Endpoint-Installer mithilfe des Intune Win32 Content Prep Tools als Win32-Anwendung verpackt und anschließend über Intune konfiguriert und bereitgestellt. Wir haben das offizielle Microsoft Prep Tool für die Erstellung der App verwendet.

Konfiguration

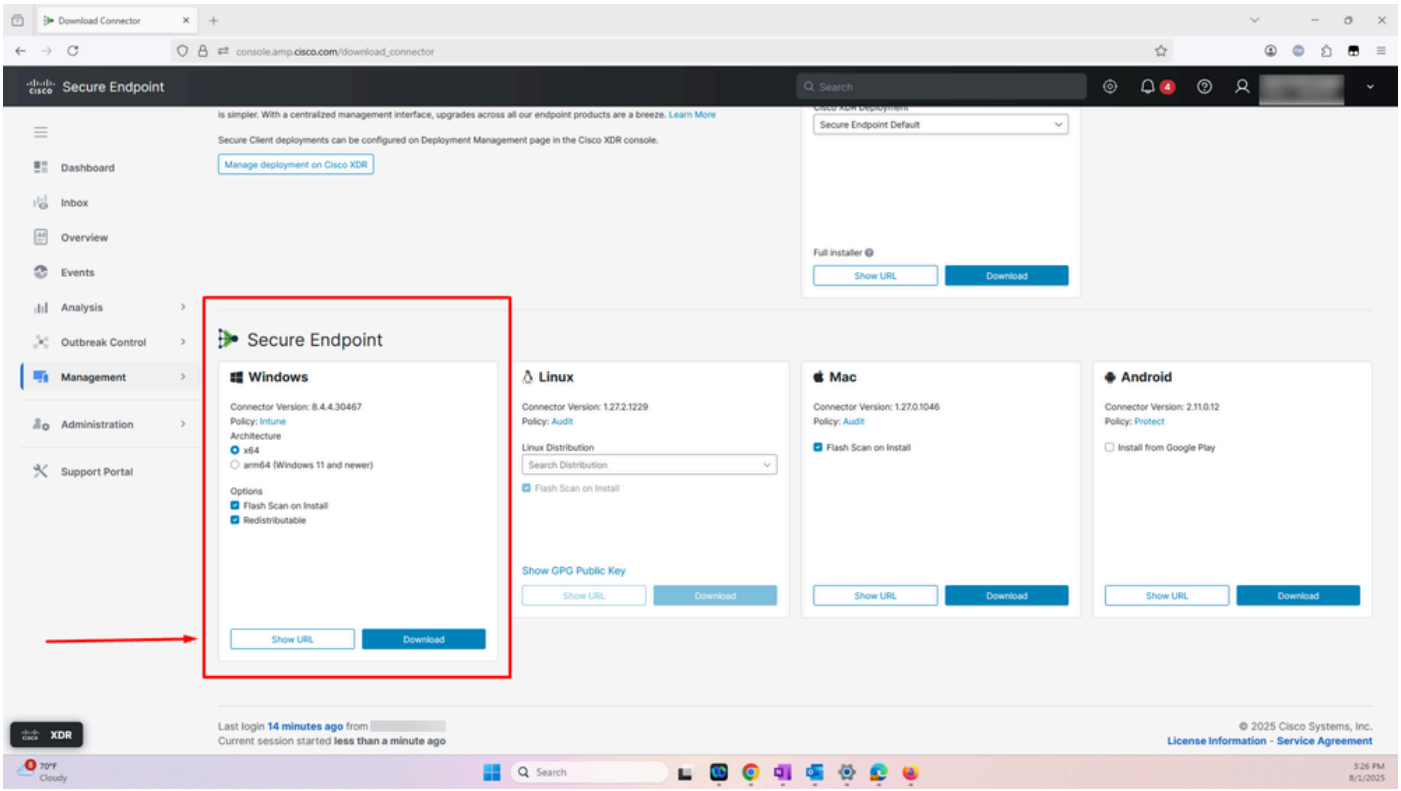
Sichere Endgerätebereitstellung

Schritt 1: Laden Sie den Cisco Secure Endpoint Installer herunter.

- Melden Sie sich je nach Region bei Ihrem Secure Endpoint Portal an: https://apps.security.cisco.com/overview
- Navigieren Sie zur Registerkarte Management, und wählen Sie Download Connector aus.
- Wählen Sie die Gruppe für sichere Endpunkte aus, für die der Connector registriert werden soll.



- Wählen Sie Download aus, und der EXE-Installer wird lokal heruntergeladen, wie im Screenshot gezeigt.



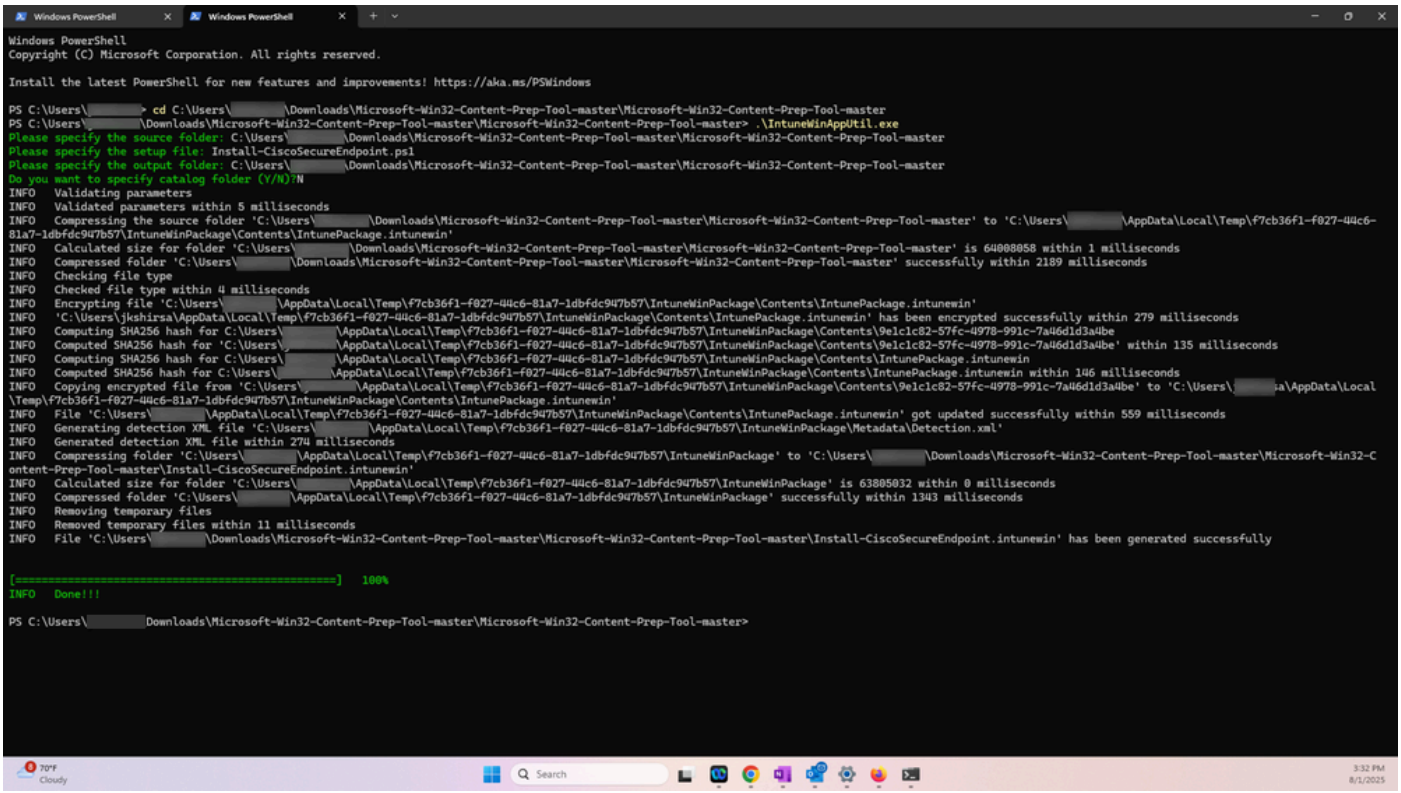
Schritt 2: Bereiten Sie die Intune-Datei mit dem Win32 Content Prep Tool vor.

Das Win32-Tool zur Inhaltsvorbereitung ist ein von Microsoft Intune bereitgestelltes Dienstprogramm, das IT-Administratoren bei der Vorbereitung von Win32-Anwendungen (d. h. herkömmlichen Windows-Desktop-Anwendungen) für die Bereitstellung über Microsoft Intune

unterstützt. Das Tool konvertiert Win32-Anwendungsinstallationsprogramme (wie EXE-, MSI- und verwandte Dateien) in ein .intunewin-Dateiformat, das für die Bereitstellung dieser Apps über Intune erforderlich ist.

Um die Intune-Datei vorzubereiten, gehen Sie folgendermaßen vor:

- Laden Sie das Win32 Content Prep Tool von Github herunter. Download: https://github.com/microsoft/Microsoft-Win32-Content-Prep-Tool
- Ausführen von IntuneWinAppUtil.exe
- Wechseln Sie im nächsten Schritt zum Ordner mit der ausführbaren Datei für Cisco Secure Endpoint, die in Schritt 1 heruntergeladen wurde, und dem Skript für die Powershell-Installation (Install-CiscoSecureEndpoint.ps1).
- Geben Sie dann den Skriptdateinamen für die Setup-Datei an: Installation - CiscoSecureEndpoint.ps1
- Geben Sie im nächsten Schritt den Ordner an, in dem die Intunewin-Datei generiert werden soll.
- Geben Sie N ein, wenn Sie zur Angabe des Katalogs aufgefordert werden.
- Die Intunewin-Datei wird wie im Screenshot gezeigt generiert:

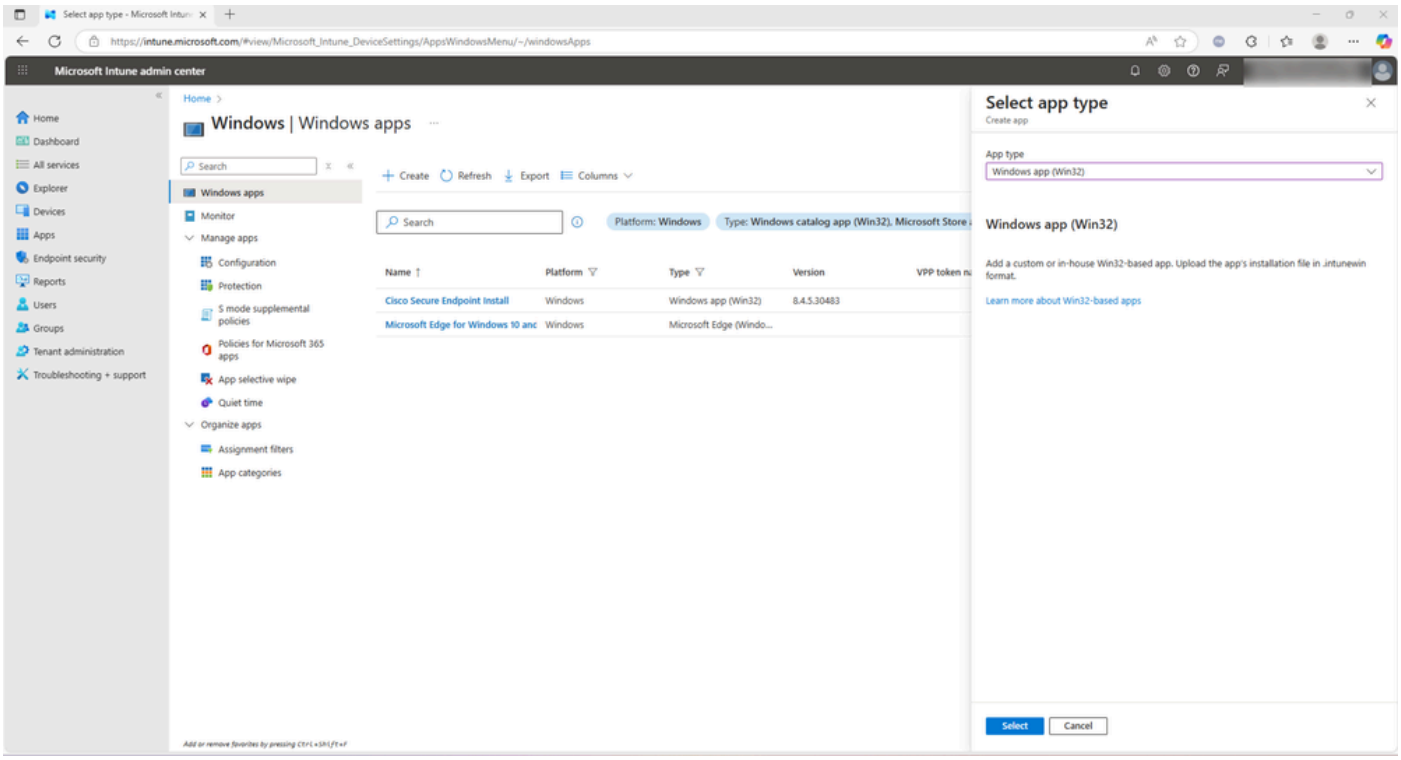


Schritt 3: Laden Sie die Datei Secure Endpoint IntuneWin in das Microsoft Intune Admin Center hoch.

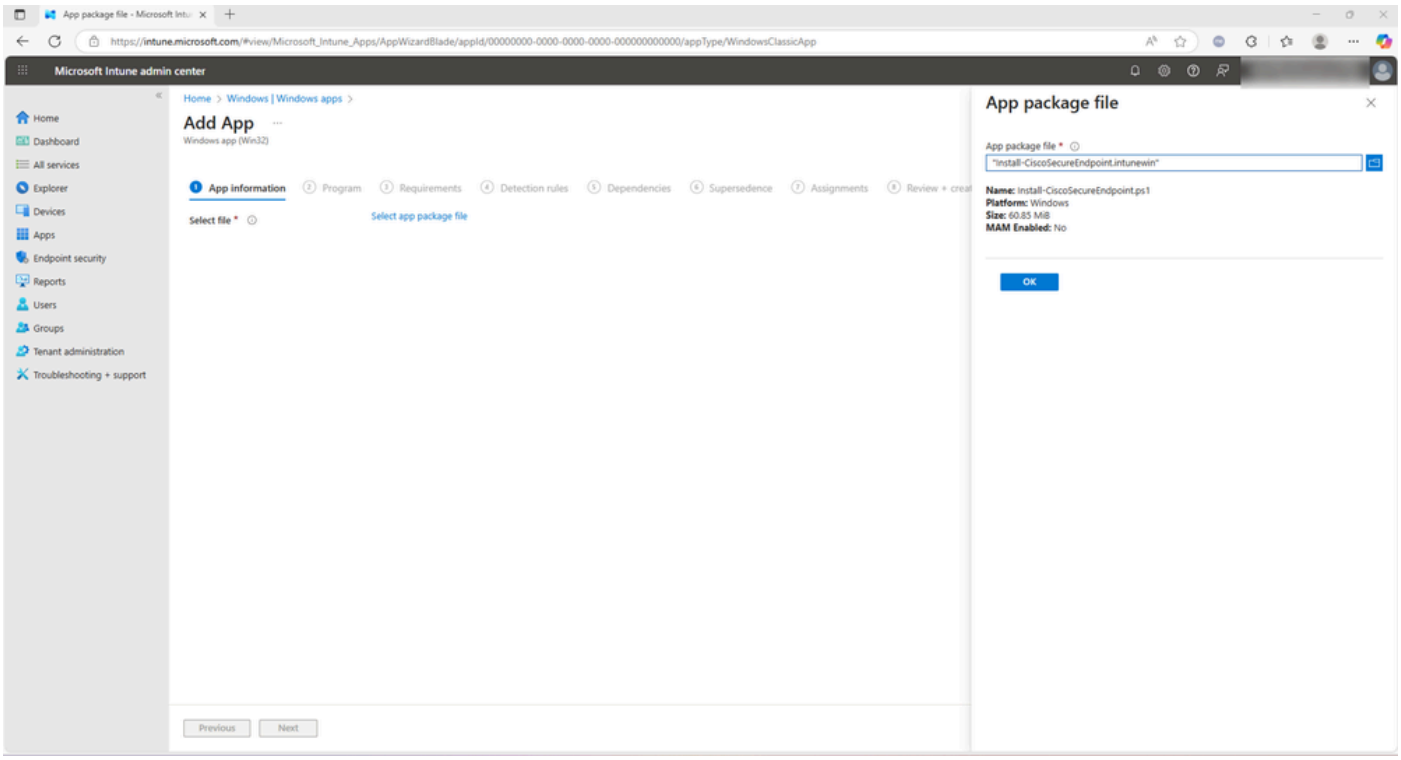
Führen Sie die folgenden Schritte aus:

- Melden Sie sich beim Microsoft Intune Admin Center an.
- Navigieren Sie zu den Windows-Apps im Microsoft Intune Admin Center, und wählen Sie Anwendungstyp - Win32 aus, und wählen Sie

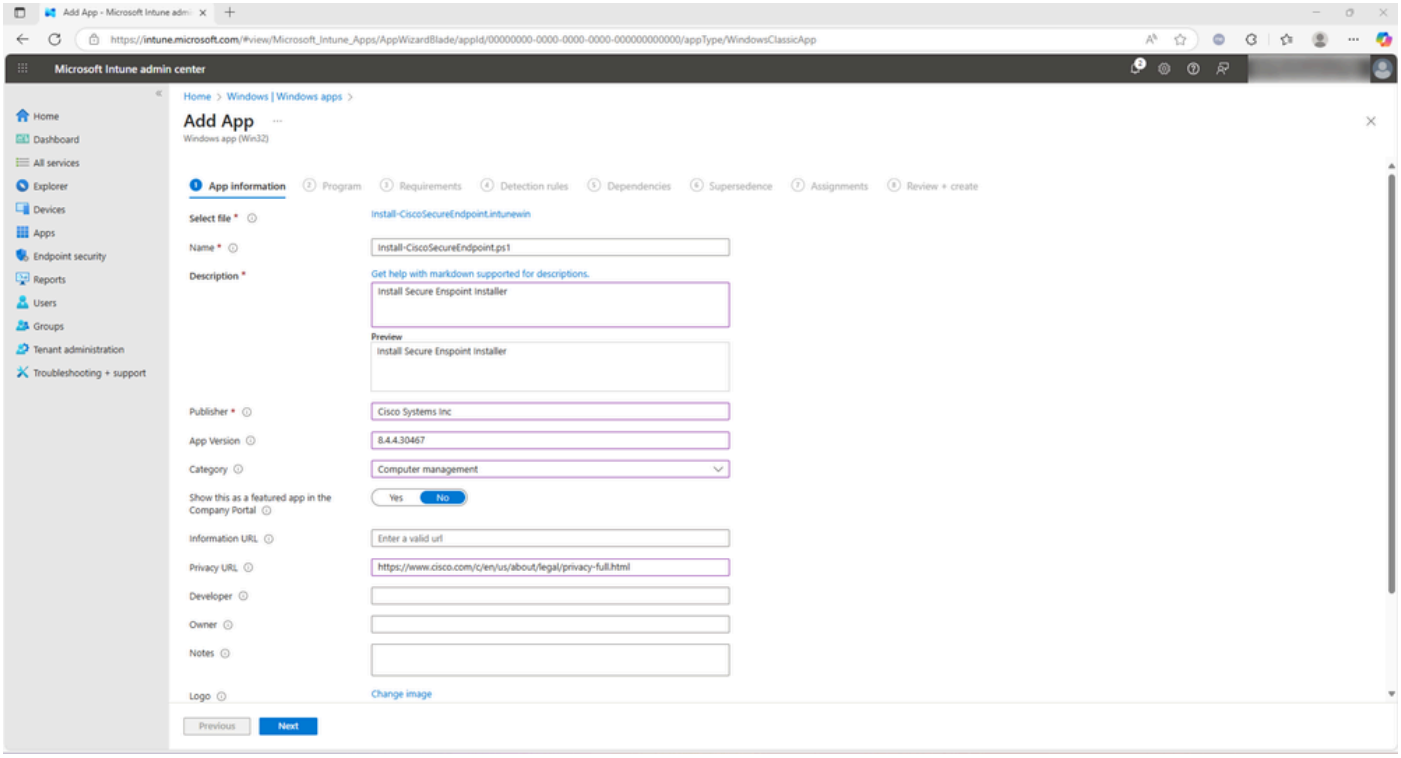
Diese beiden Aktionen werden im Screenshot veranschaulicht:



- Laden Sie im nächsten Schritt die Secure Endpoint Intunewin-Datei hoch, die Sie in Schritt 2 erstellt haben, und wählen Sie OK.



- Nachdem Sie OK ausgewählt haben, geben Sie die Informationen wie im Screenshot dargestellt ein. Die optionalen Felder können auf jeder Registerkarte leer gelassen werden. Fahren Sie mit dem nächsten Schritt fort, indem Sie Weiter auswählen.

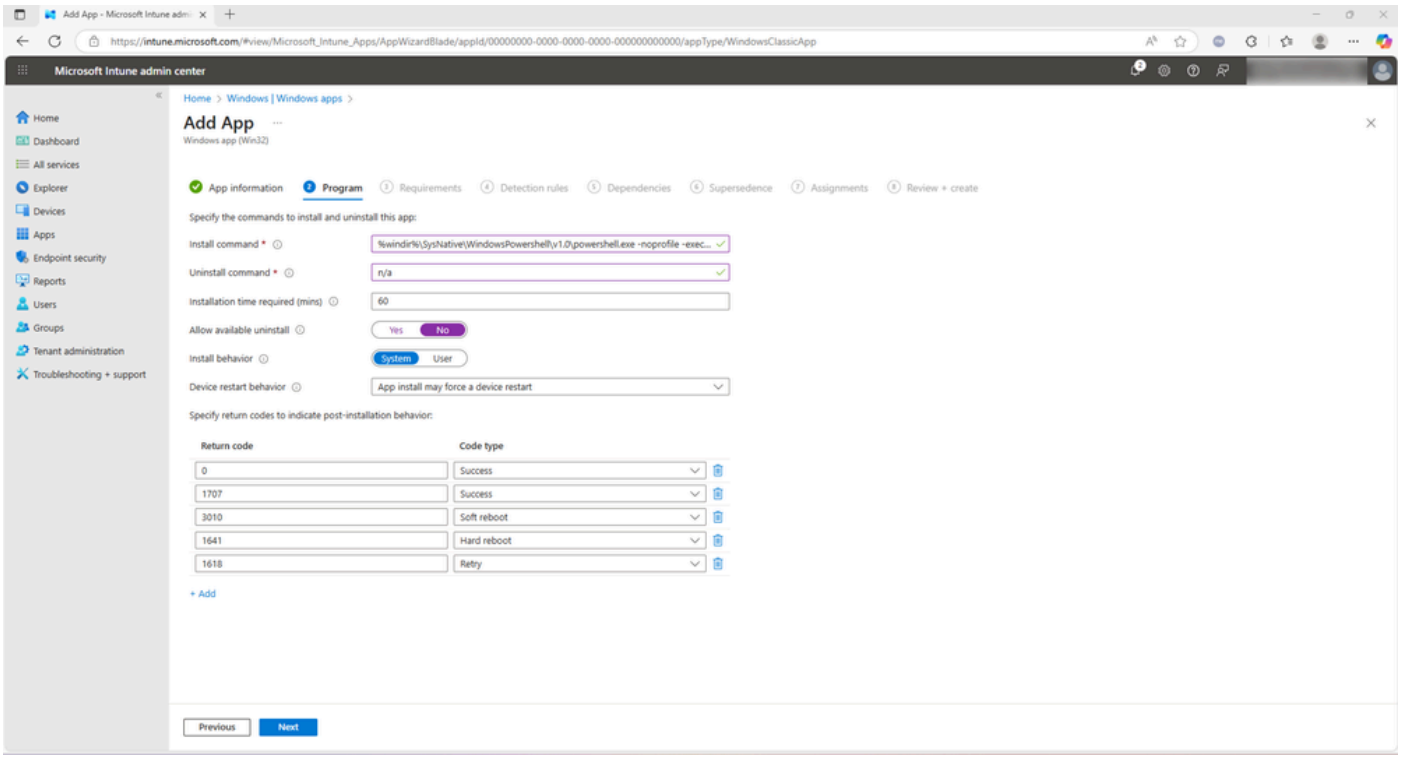


- Geben Sie den Installationsbefehl wie folgt ein:

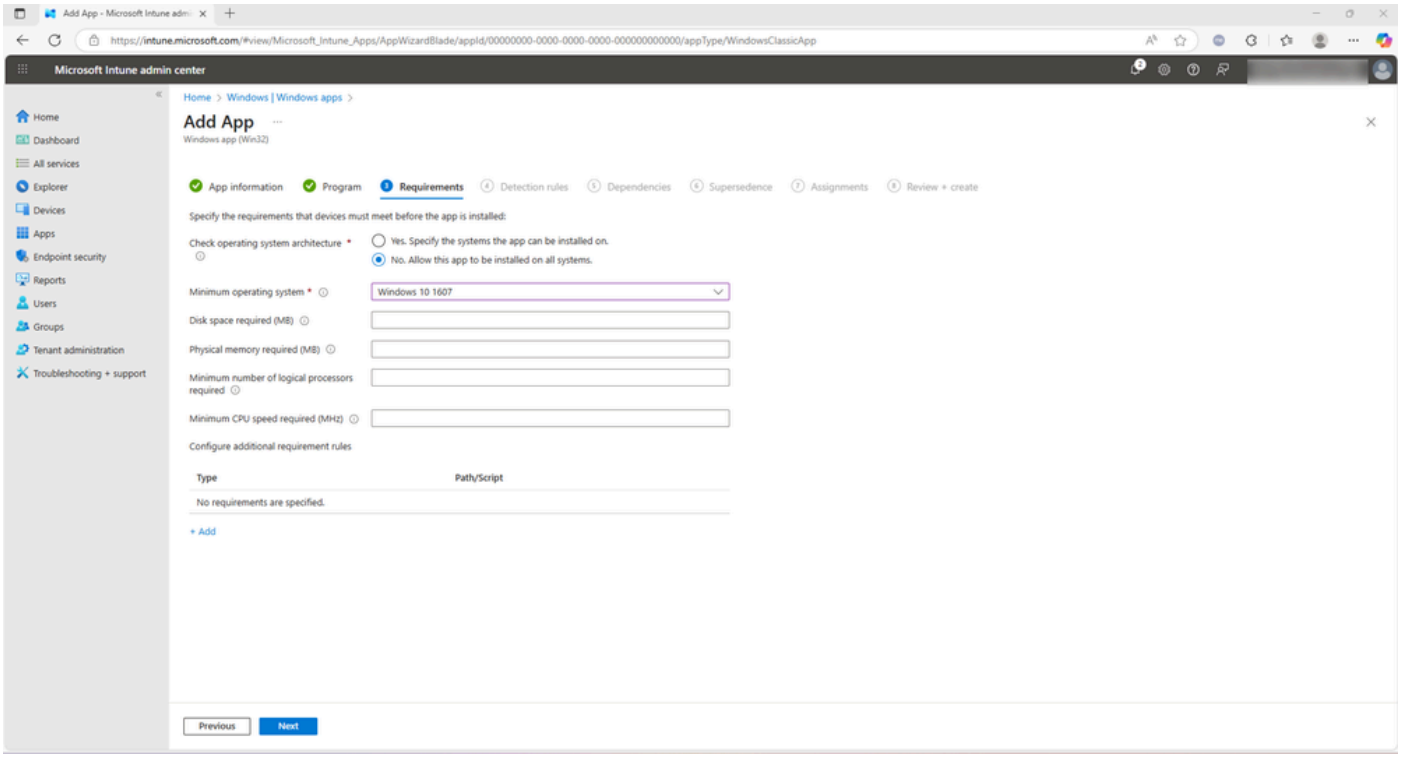
```
%windir%\SysNative\WindowsPowershell\v1.0\powershell.exe -noprofile -executionpolicy Bypass -file
```

Beachten Sie, dass der hier gezeigte Code als Beispiel dient und jeder Code als Installationsbefehl für dieses Installationsprogramm verwendet werden kann.

- Geben Sie Uninstall als n/a und die erforderliche Installationszeit als 60 (optional) ein. Legen Sie die Option Verfügbare Deinstallation zulassen als Nein fest, wählen Sie Installationsverhalten als System aus, und geben Sie optionale Details ein, bevor Sie Weiter auswählen.



- Aktivieren Sie auf der Registerkarte "Anforderungen" das Kontrollkästchen "Nein". Diese App darf auf allen Systemen installiert sein, und wählen Sie das Mindestbetriebssystem aus. Füllen Sie ggf. Felder aus, und wählen Sie Weiter aus.

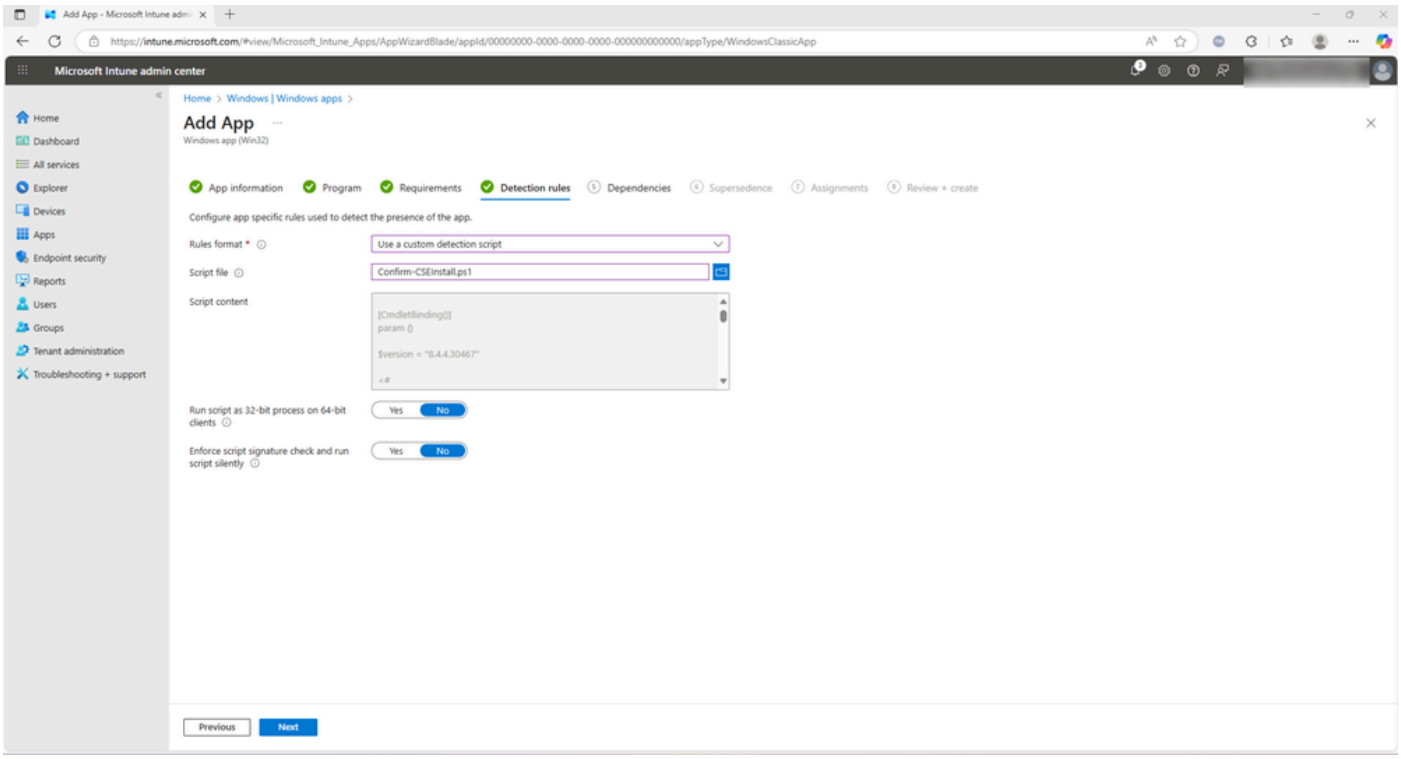


- Auf der Registerkarte Erkennungsregeln bietet das Dropdown-Menü Regelformat zwei Optionen: Erkennungsregeln manuell konfigurieren und ein benutzerdefiniertes Erkennungsskript verwenden. Beide Optionen können je nach Bereitstellungsanforderungen ausgewählt werden.

- Wenn Sie die Option Erkennungsregeln manuell konfigurieren auswählen, können Sie einen

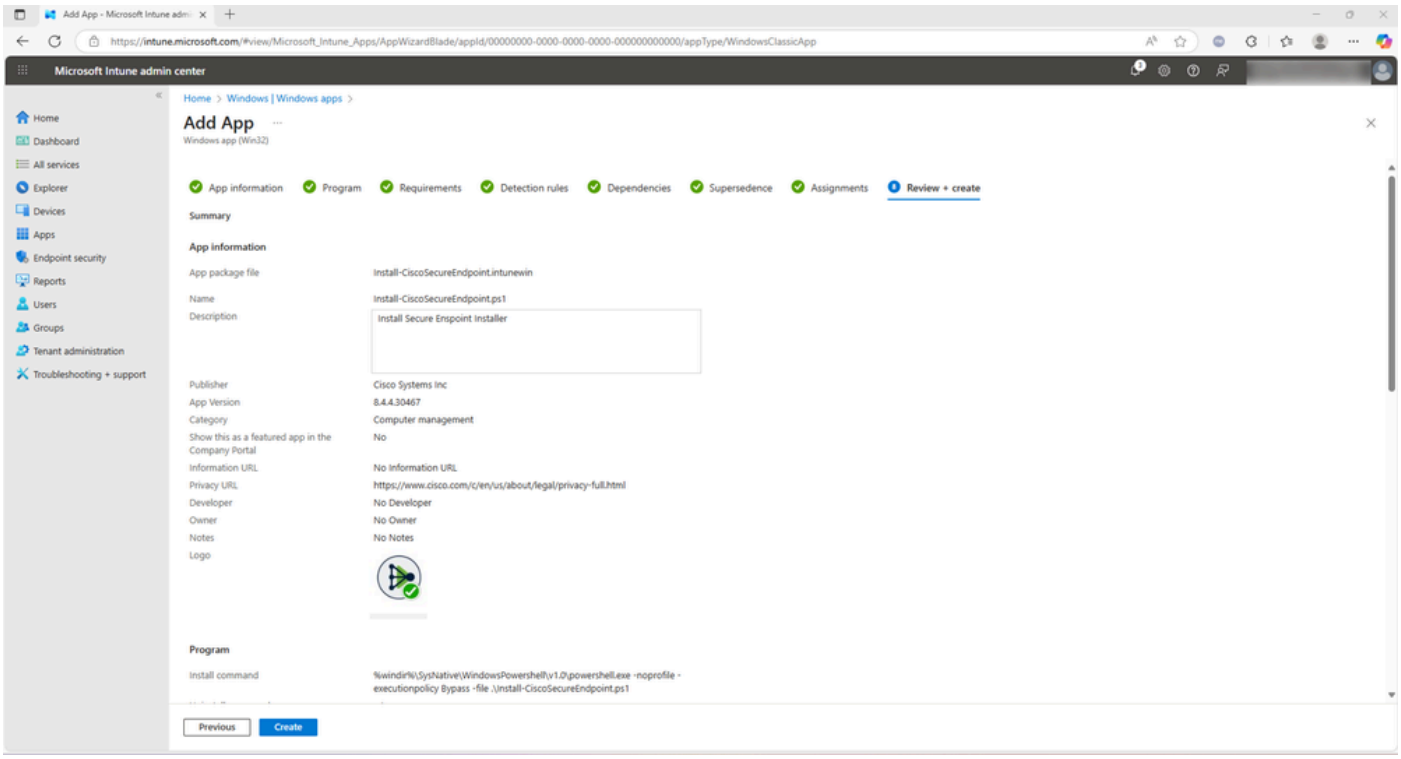
Regeltyp wie MSI, Datei oder Registrierung definieren, um das Vorhandensein der Anwendung zu erkennen. In diesem Dokument wurde die alternative Option Benutzerdefiniertes Erkennungsskript verwenden ausgewählt.

- Ein PowerShell-Skript mit dem Namen Confirm-CSEInstall.ps1 wird verwendet, um die erfolgreiche Installation von Cisco Secure Endpoint zu überprüfen. Diese finden Sie am Ende dieses Dokuments.



- Wählen Sie Weiter, um fortzufahren. Anmerkung: Speziell für diesen Bereitstellungsprozess kann ein benutzerdefiniertes Erkennungsskript erstellt werden, das den Anforderungen Ihrer Umgebung und den Erkennungskriterien entspricht.

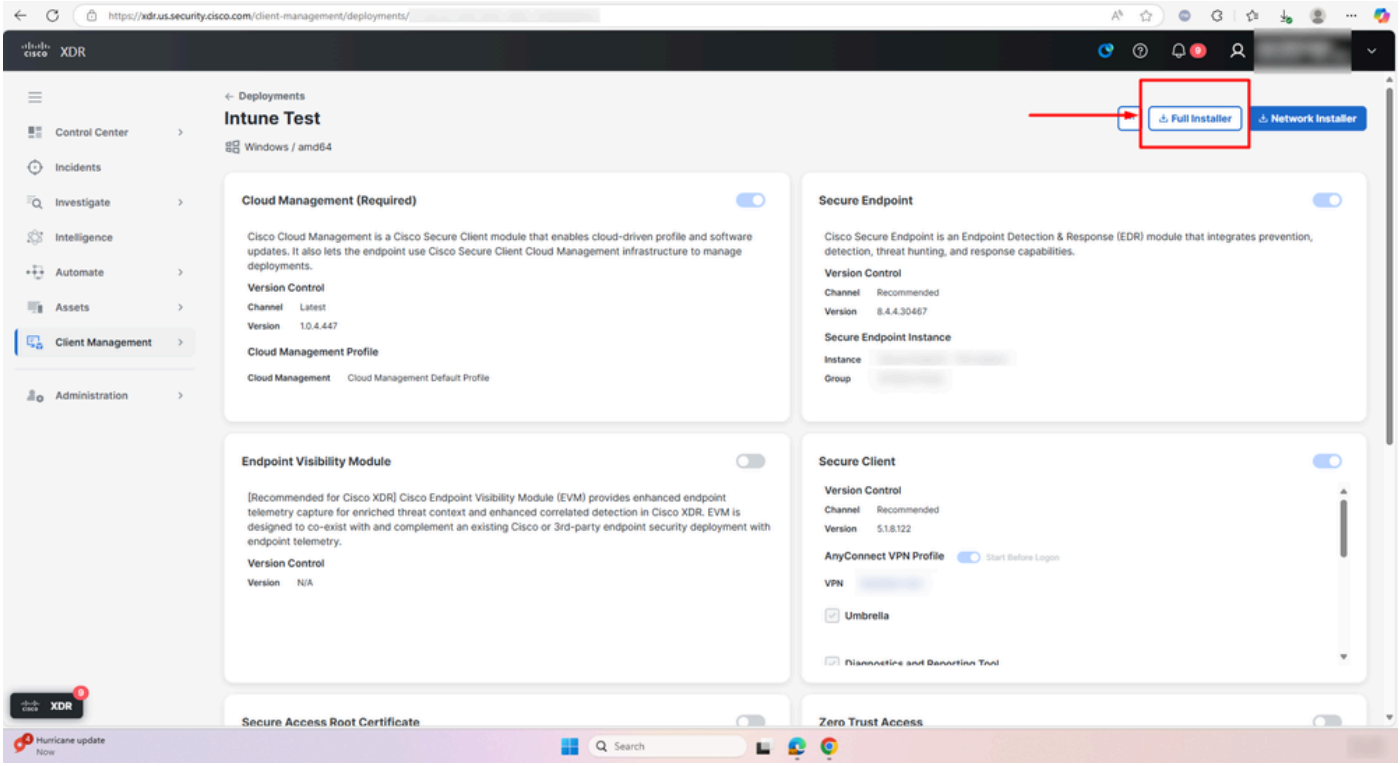
- Die nächsten Registerkarten sind optional. Es müssen keine Abhängigkeiten konfiguriert werden. Weisen Sie die Anwendung der erforderlichen Gruppe zu, und wählen Sie Prüfen + Erstellen.



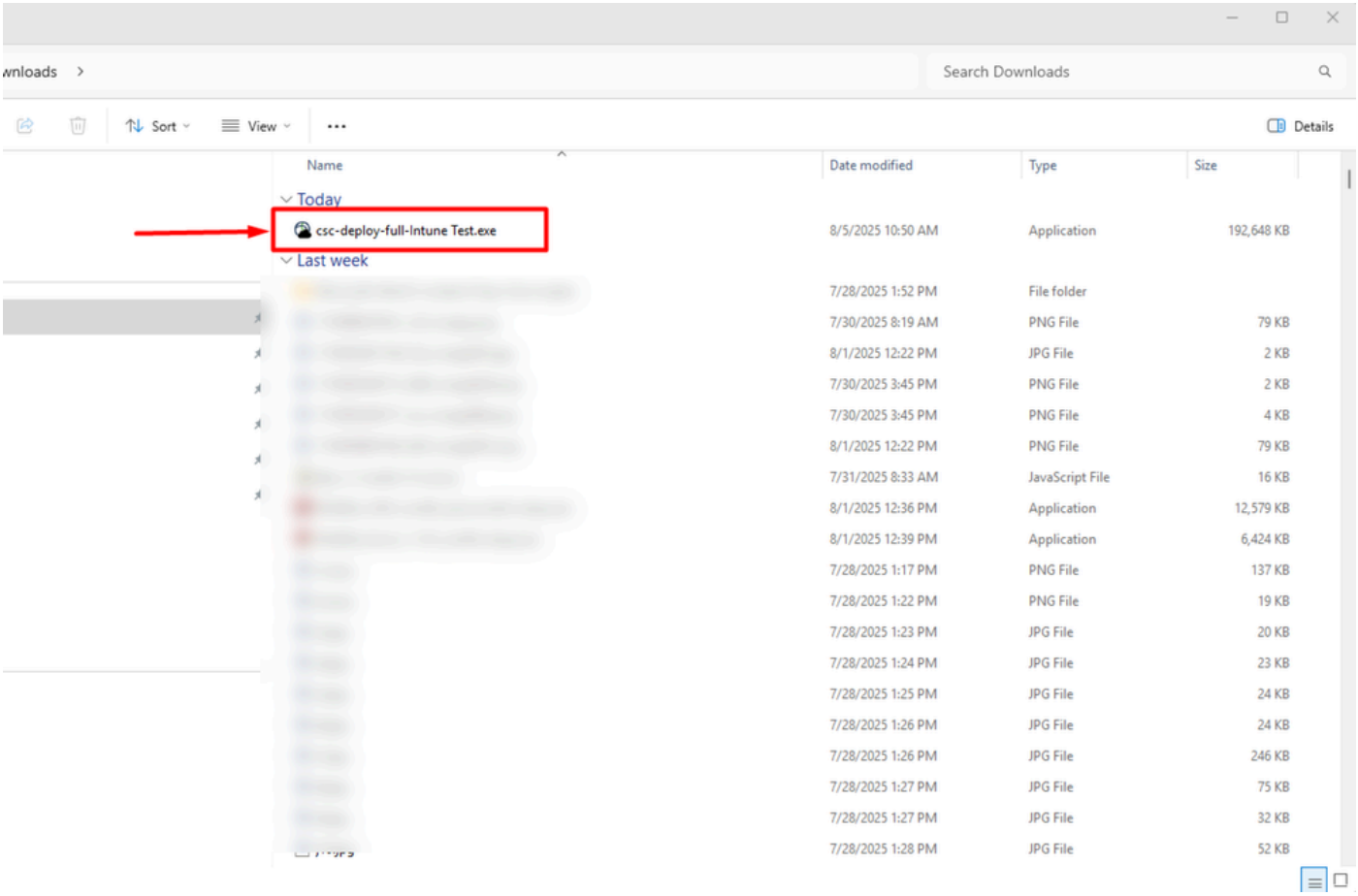
Sichere Client-Bereitstellung

Schritt 1: Laden Sie die vollständige Cisco Secure Client-Bereitstellung herunter.

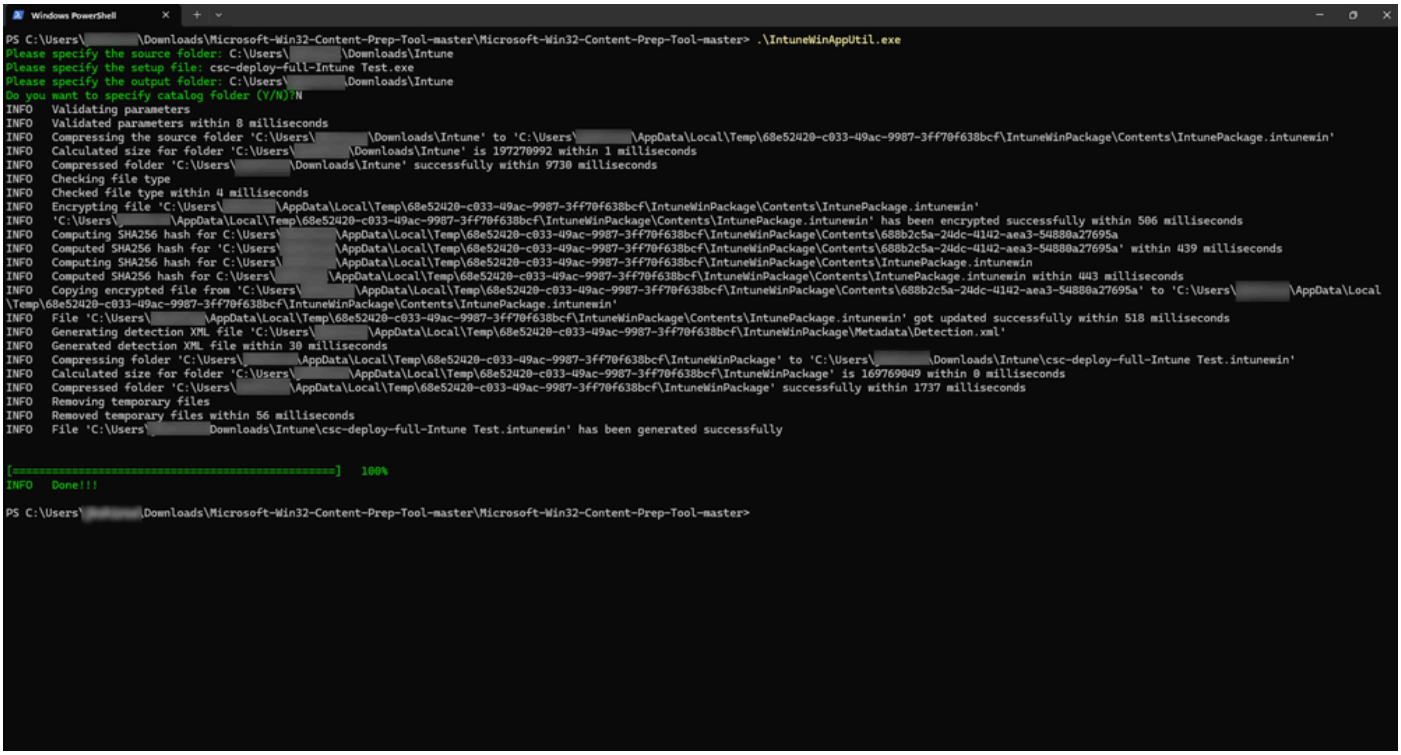
- Melden Sie sich je nach Region bei der XDR- oder Secure Client Cloud Management-Konsole an: https://apps.security.cisco.com/overview
- Erstellen Sie eine neue Bereitstellung, und wählen Sie je nach Bereitstellungstyp den Vollinstallateur oder Netzwerkinstallateur aus.



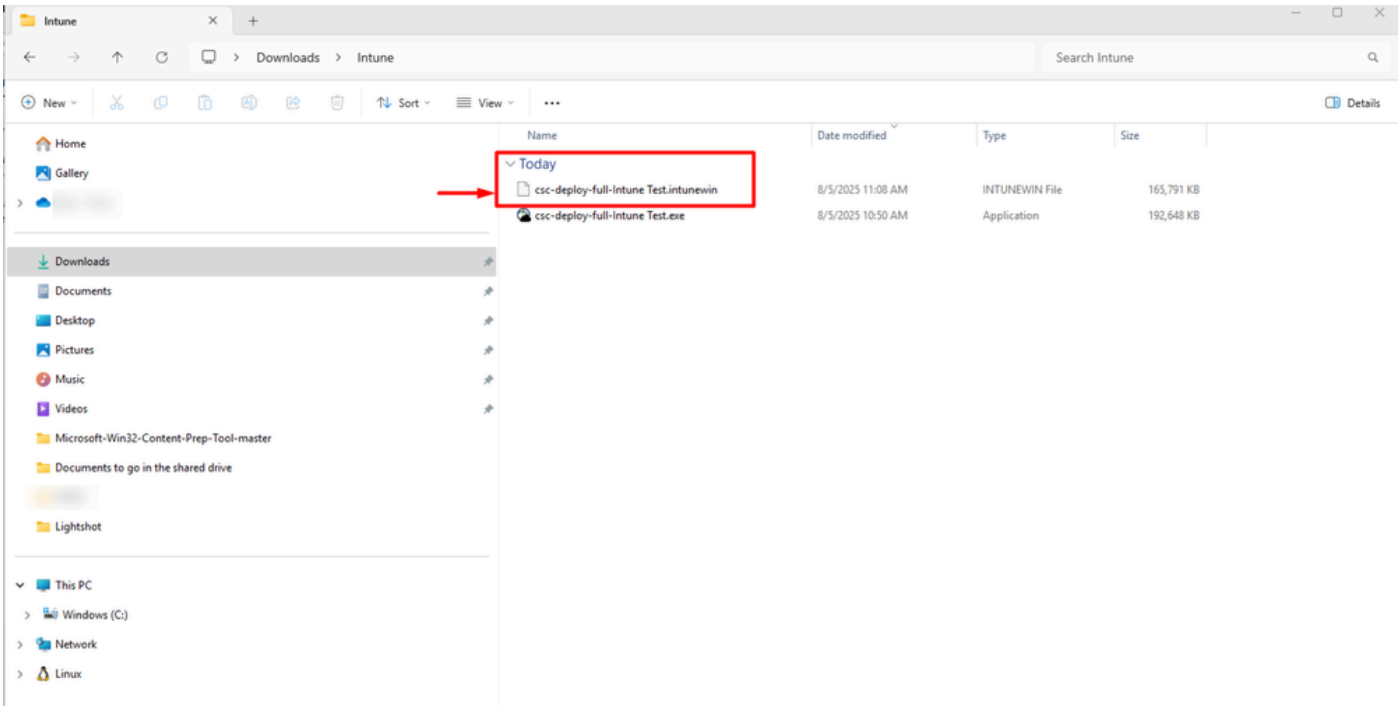
- Eine Datei csc-deploy-Intune Test.exe wird wie im Screenshot gezeigt heruntergeladen.



Schritt 2: Bereiten Sie die Intune-Datei wie in Schritt 2 vor. Dadurch wird die Datei "csc-deploy-full-Intune Test.intunewin" erstellt.



- Die obigen Schritte führen zum Erstellen einer Datei "csc-deploy-full-Intune Test.intunewin", wie im Screenshot gezeigt.



Schritt 3: Laden Sie die Datei csc-deploy-full-intune Test.intunewin aus Teil 1 in das Microsoft Intune Admin Center wie oben beschrieben hoch.

Damit ist der Prozess zur Bereitstellung von Cisco Secure Endpoint mithilfe von Intune abgeschlossen.

Install-CiscoSecureEndpoint.ps1-Skript

```
[CmdletBinding()]
param ()

$cse_exe =



$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-Skript

```
[CmdletBinding()]
param ()

$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
```

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.