Distribuire Cisco Secure Endpoint/Secure Client con Microsoft Intune

Sommario

Introduzione

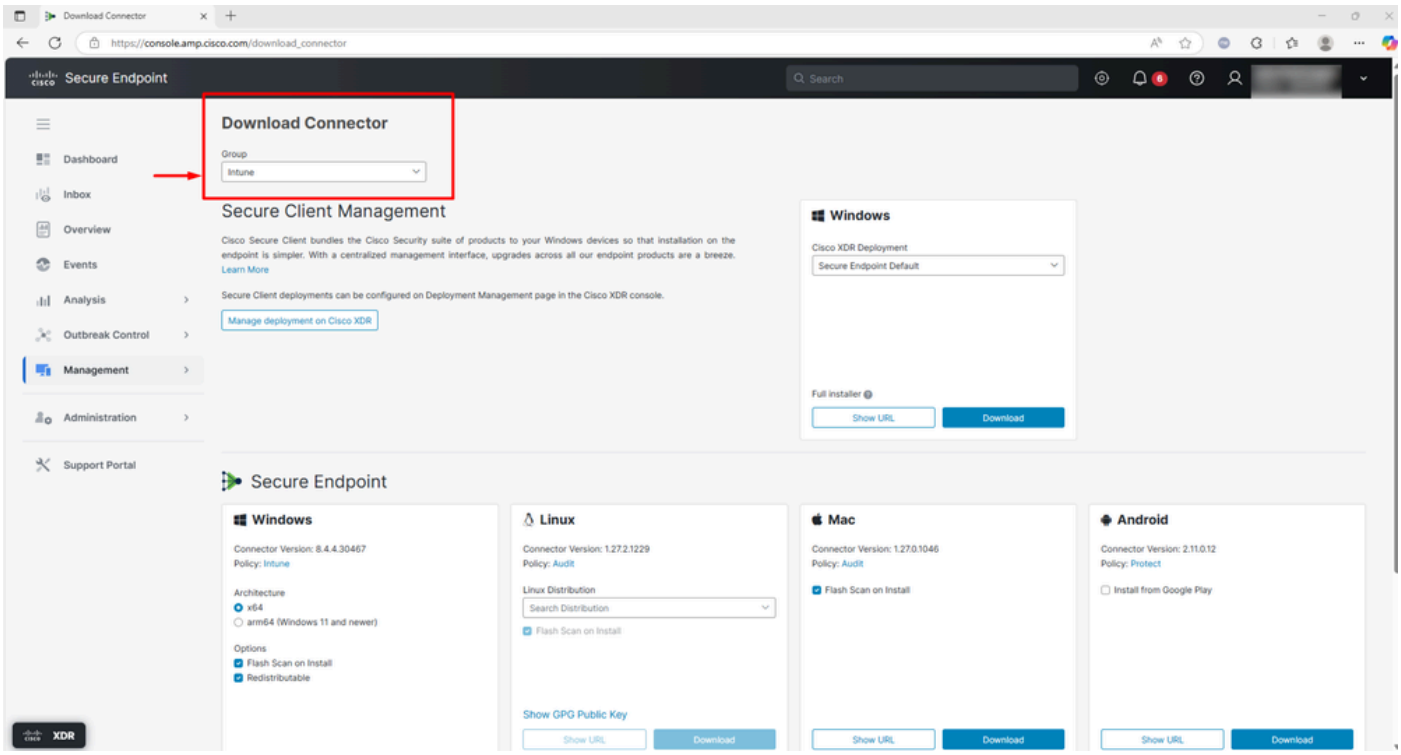
In questo documento viene descritto il processo di distribuzione di Cisco Secure Endpoint o Secure Client con Microsoft Intune. In questo documento viene descritto come creare un'app supportata da Microsoft Intune dai programmi di installazione di Secure Endpoint/Secure Client e come utilizzarla per la distribuzione tramite l'interfaccia di amministrazione di Microsoft Intune. In particolare, il processo include il packaging del programma di installazione di Cisco Secure Endpoint come applicazione Win32 utilizzando lo strumento di preparazione dei contenuti Win32 di Intune, seguito dalla configurazione e dalla distribuzione dell'app tramite Intune. Per la creazione dell'app è stato utilizzato lo strumento ufficiale Microsoft Prep Tool.

Configurazione

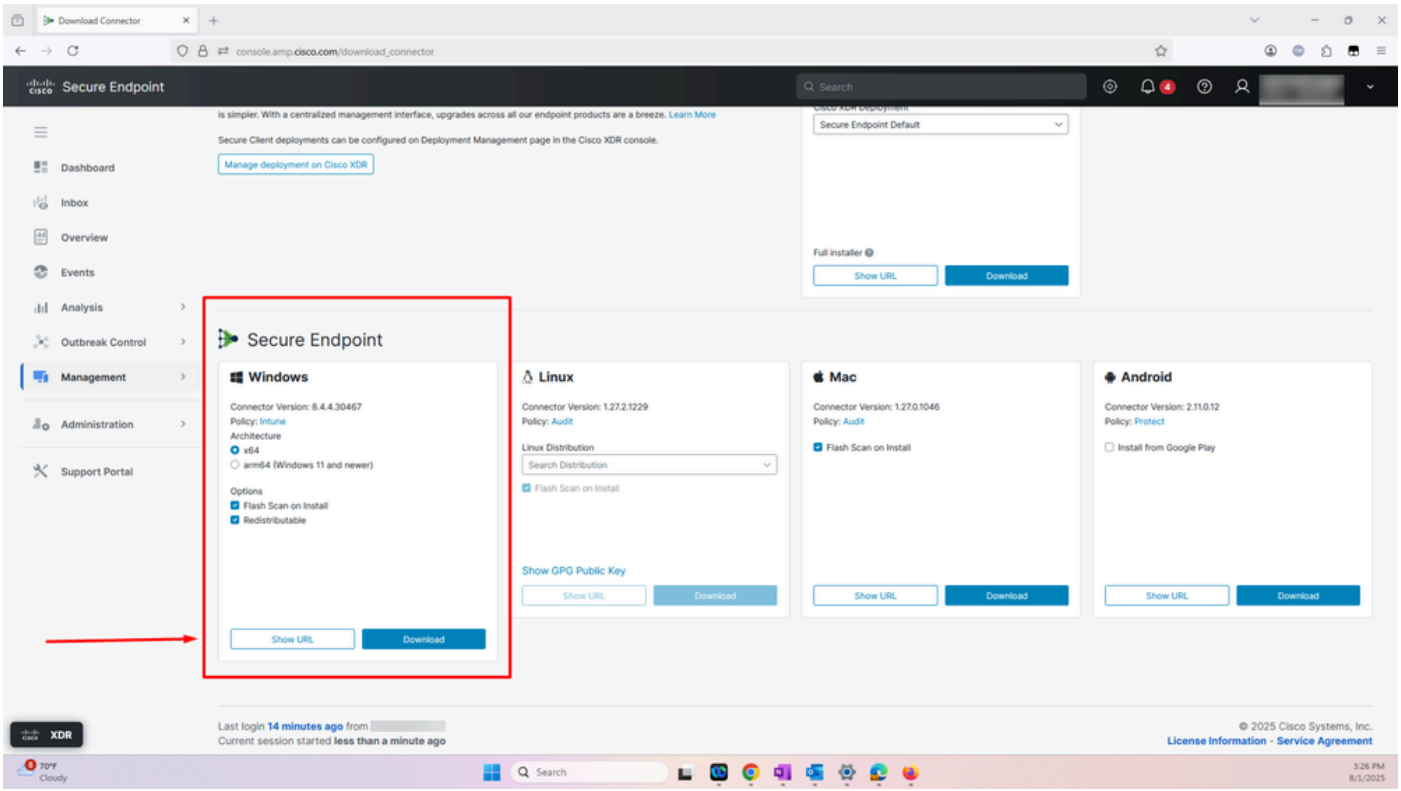
Distribuzione sicura degli endpoint

Passaggio 1. Scaricare Cisco Secure Endpoint Installer.

- Accedere al rispettivo Secure Endpoint Portal, a seconda dell'area geografica: https://apps.security.cisco.com/overview
- Passare alla scheda Gestione e selezionare Scarica connettore
- Selezionare il gruppo di endpoint protetti a cui si desidera registrare il connettore



- Selezionare download e il programma di installazione EXE viene scaricato localmente, come mostrato nello screenshot



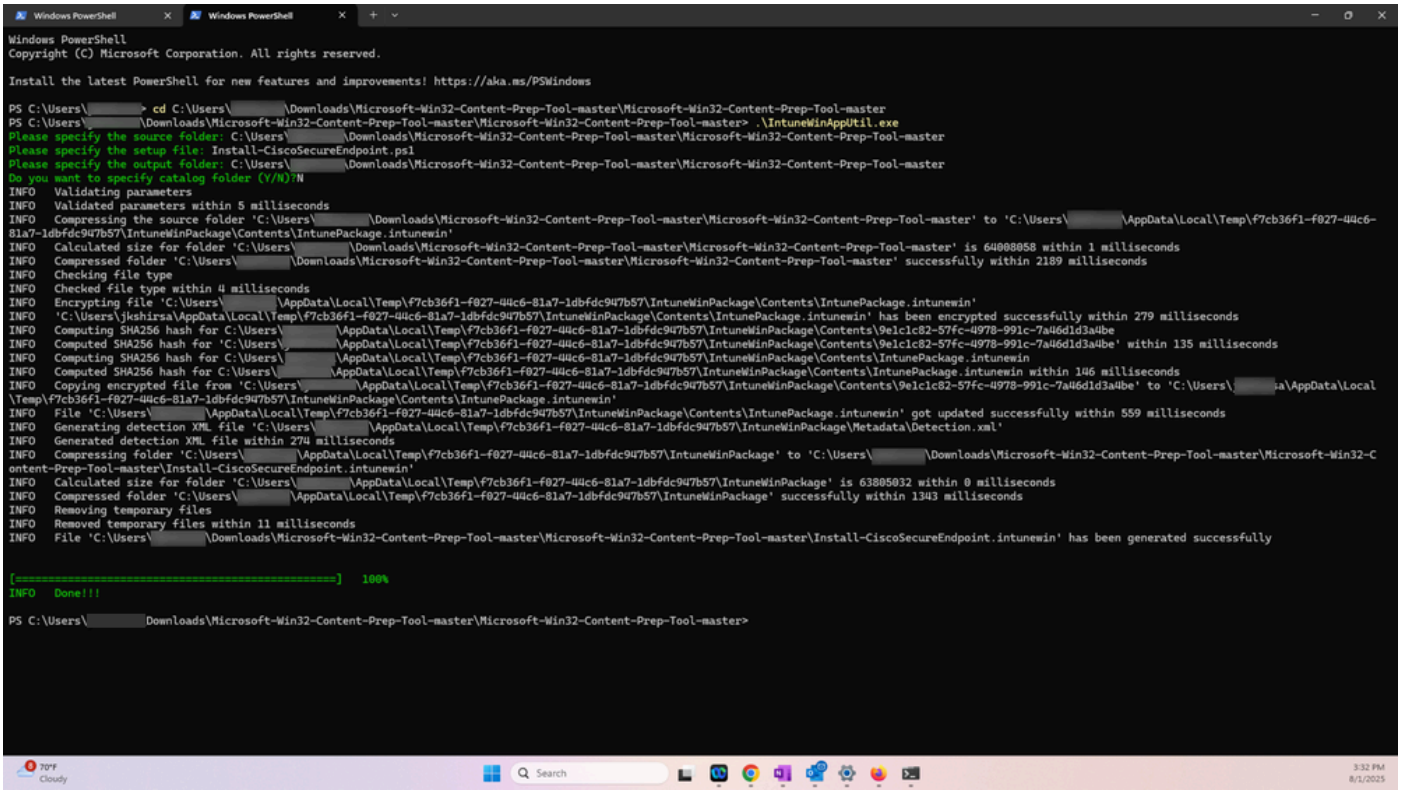
Passaggio 2. Preparare il file Intune utilizzando lo strumento di preparazione del contenuto Win32.

Lo strumento Win32 Content Prep è un'utilità fornita da Microsoft Intune per aiutare gli amministratori IT a preparare le applicazioni Win32 (ad esempio le tradizionali applicazioni

desktop di Windows) per la distribuzione tramite Microsoft Intune. Lo strumento converte i programmi di installazione delle applicazioni Win32 (ad esempio file con estensione exe, msi e file correlati) in un formato di file con estensione intunewin, necessario per la distribuzione di queste app tramite Intune.

Per preparare il file di Intune, eseguire la procedura seguente:

- Scaricare lo strumento Win32 Content Prep da Github. Download: https://github.com/microsoft/Microsoft-Win32-Content-Prep-Tool
- Eseguire IntuneWinAppUtil.exe
- Nel passaggio successivo, passare alla cartella contenente il file eseguibile di Cisco Secure Endpoint scaricato nel passaggio 1 e lo script di installazione di PowerShell (Install-CiscoSecureEndpoint.ps1)
- Specificare quindi il nome del file di script per il file di installazione: Install-CiscoSecureEndpoint.ps1
- Nel passaggio successivo specificare la cartella in cui deve essere generato il file Intunewin
- Immettere N, quando richiesto per specificare il catalogo
- Il file Intunewin viene generato come mostrato nello screenshot:

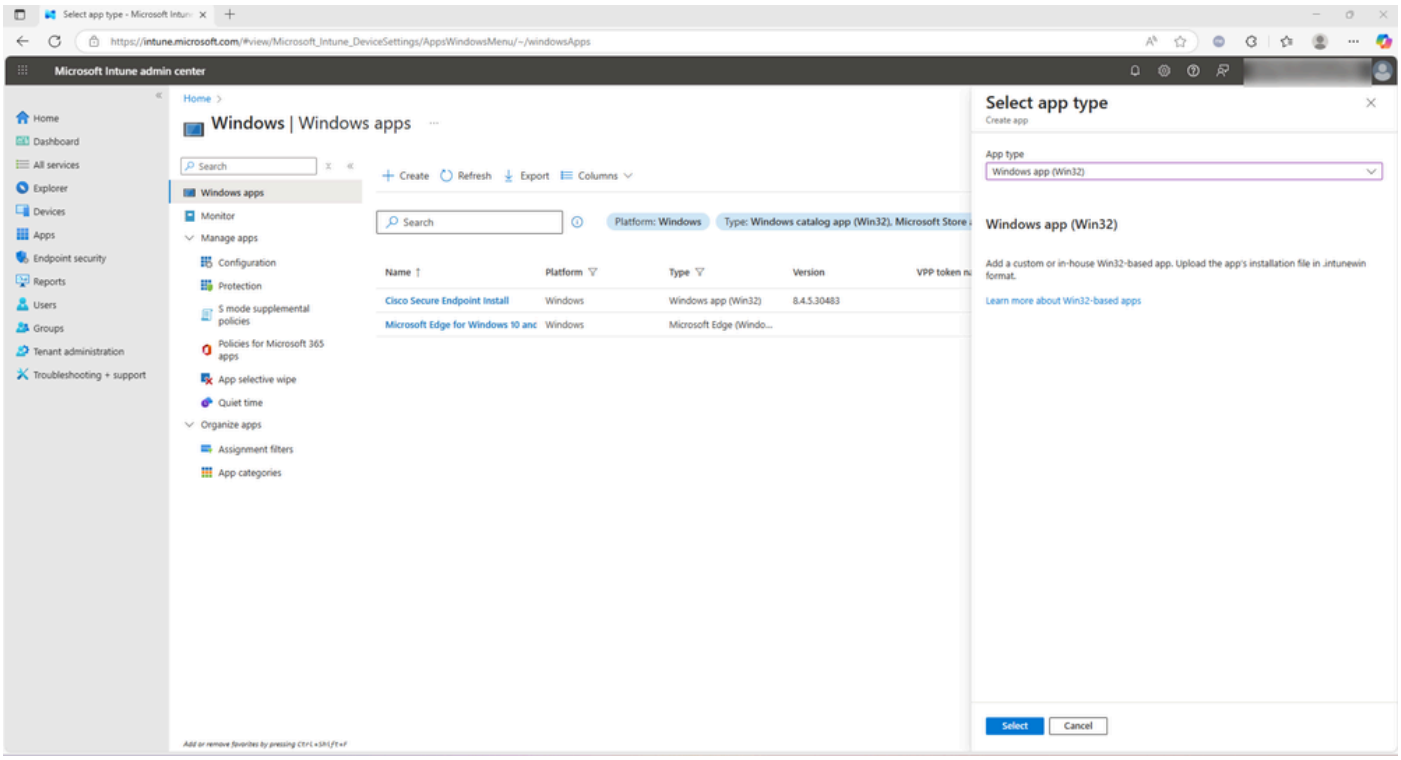


Passaggio 3. Caricare il file IntuneWin di Secure Endpoint in Microsoft Intune Admin Center.

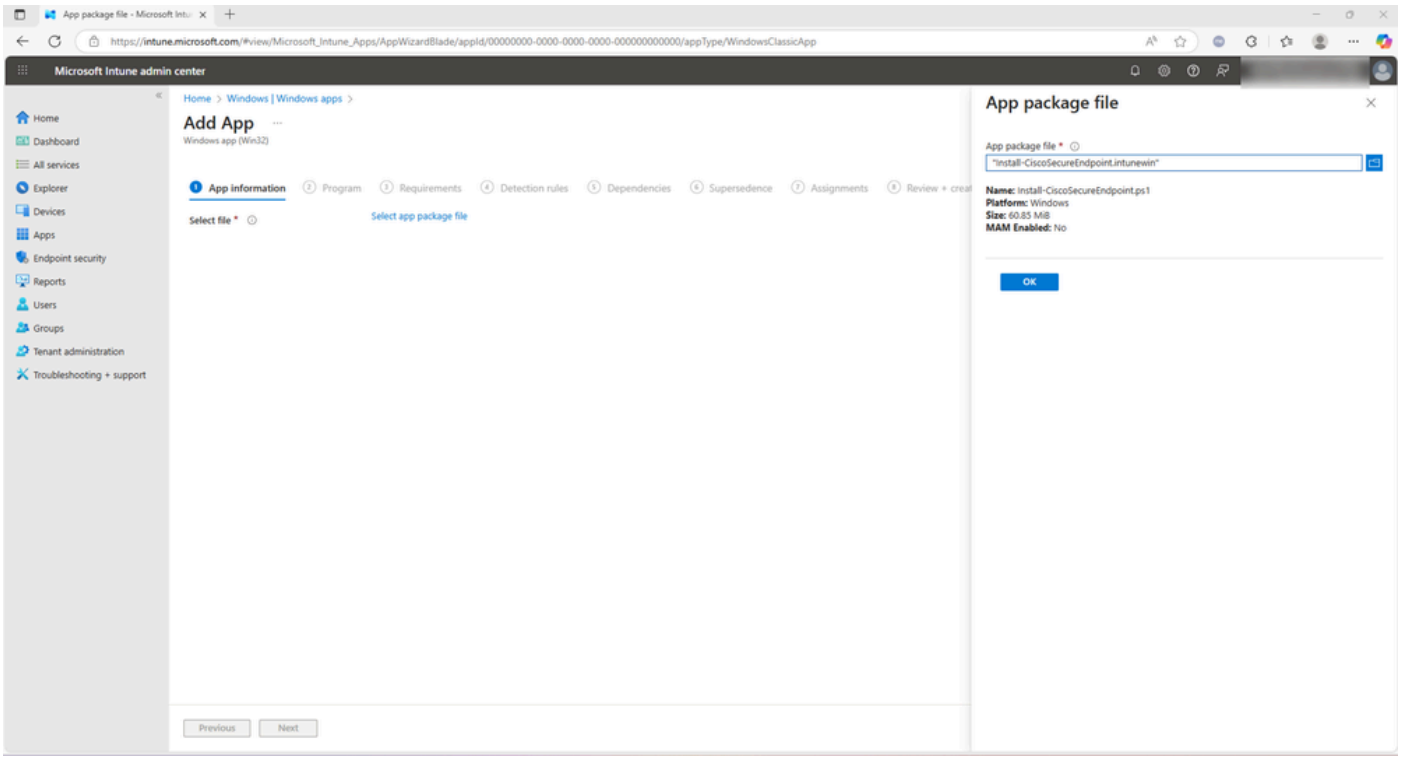
Attenersi alla procedura seguente:

- Accedi a Microsoft Intune Admin Center
- Passare alle applicazioni Windows in Microsoft Intune Admin Center e selezionare Tipo di applicazione - Win32 e selezionare

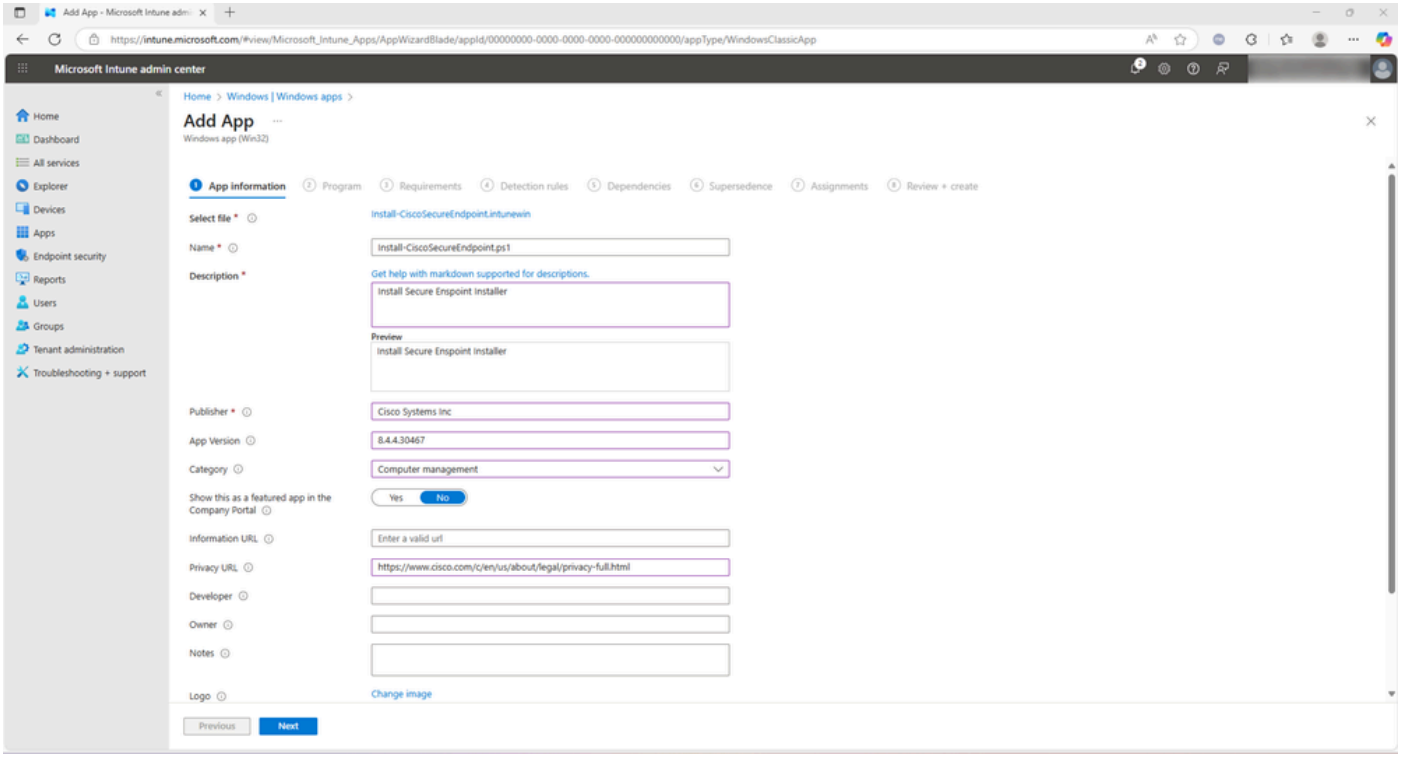
Queste due azioni sono mostrate nello screenshot:



- Nel passaggio successivo, caricare il file Secure Endpoint Intunewin creato nel passaggio 2 e selezionare OK



- Dopo aver selezionato OK, immettere le informazioni come presentate nello screenshot. I campi facoltativi possono essere lasciati vuoti in ogni scheda. Procedere al passaggio successivo selezionando Avanti

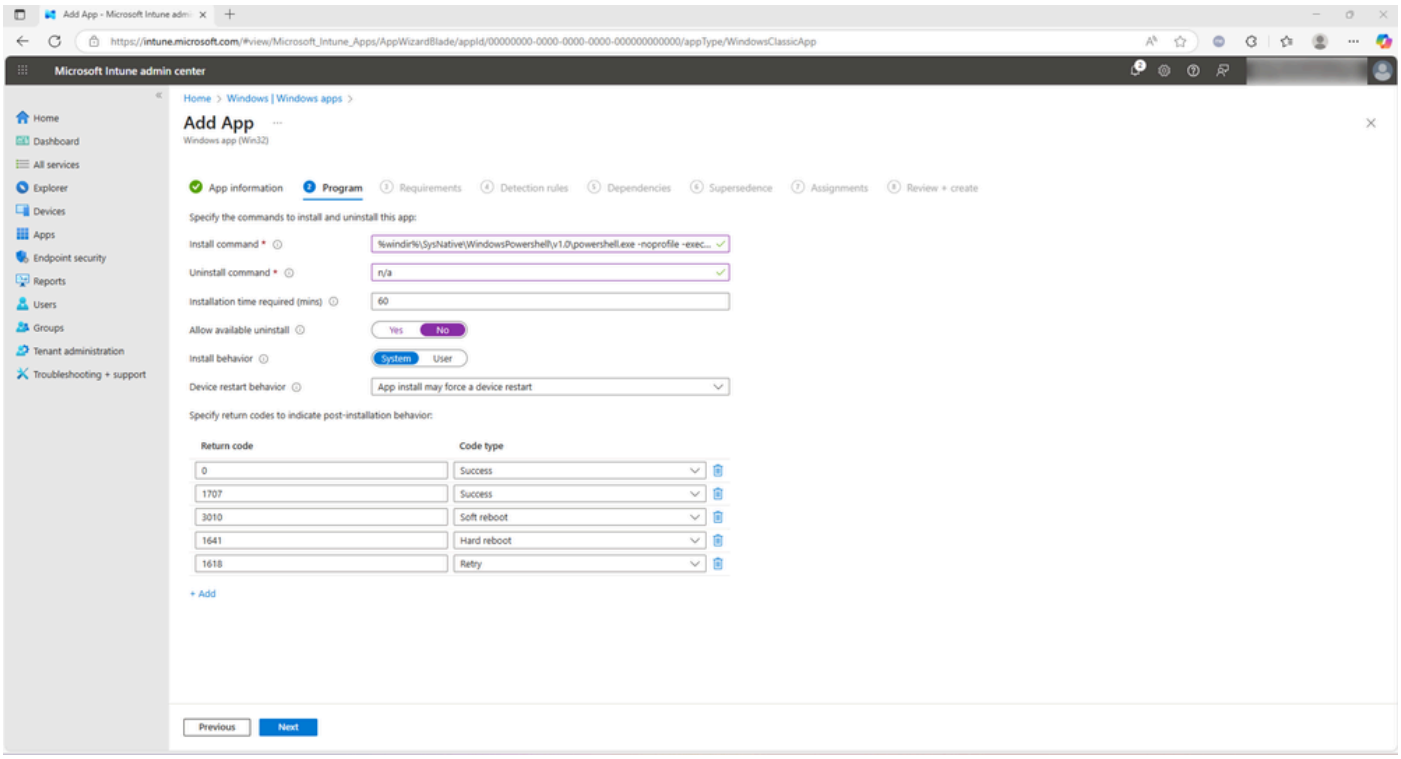


- Immettere il comando Install come mostrato:

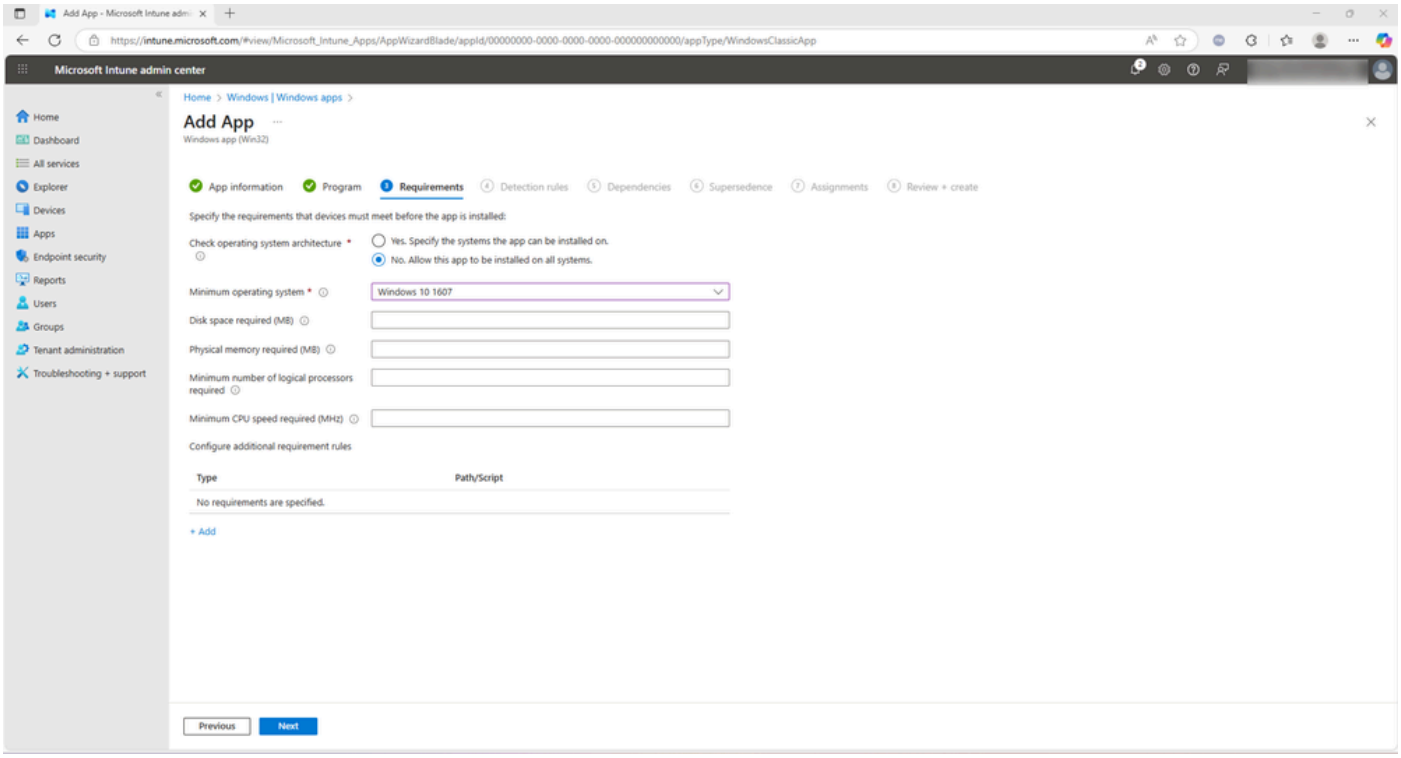
```
%windir%\SysNative\WindowsPowershell\v1.0\powershell.exe -noprofile -executionpolicy Bypass -file
```

Si noti che il codice qui presentato funge da esempio e può essere utilizzato come comando di installazione per questo programma di installazione

- Immettere Uninstall come n/a e il tempo di installazione richiesto come 60 (facoltativo). Impostare Consenti disinstallazione disponibile su No, selezionare Installa comportamento come sistema e immettere eventuali dettagli facoltativi prima di selezionare Avanti



- Nella scheda Requisiti, selezionare No. Consenti l'installazione dell'app in tutti i sistemi e selezionare il sistema operativo minimo. Compilare e facoltativamente i campi e selezionare Avanti

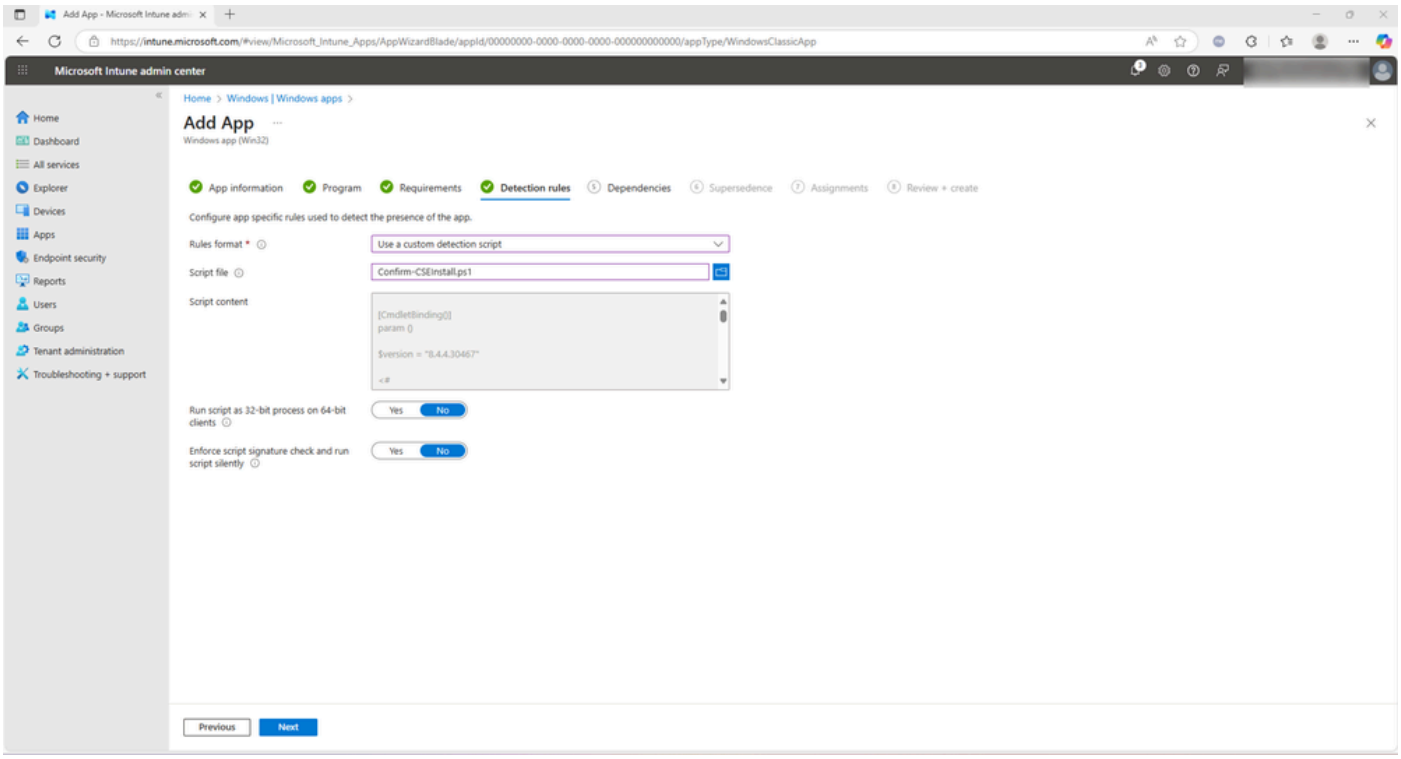


- Nella scheda Regole di rilevamento, il menu a discesa Formato regole fornisce due opzioni: Configurare manualmente le regole di rilevamento e utilizzare uno script di rilevamento personalizzato. È possibile selezionare entrambe le opzioni in base ai requisiti di distribuzione.

- Quando si sceglie Configura manualmente le regole di rilevamento, è possibile definire un

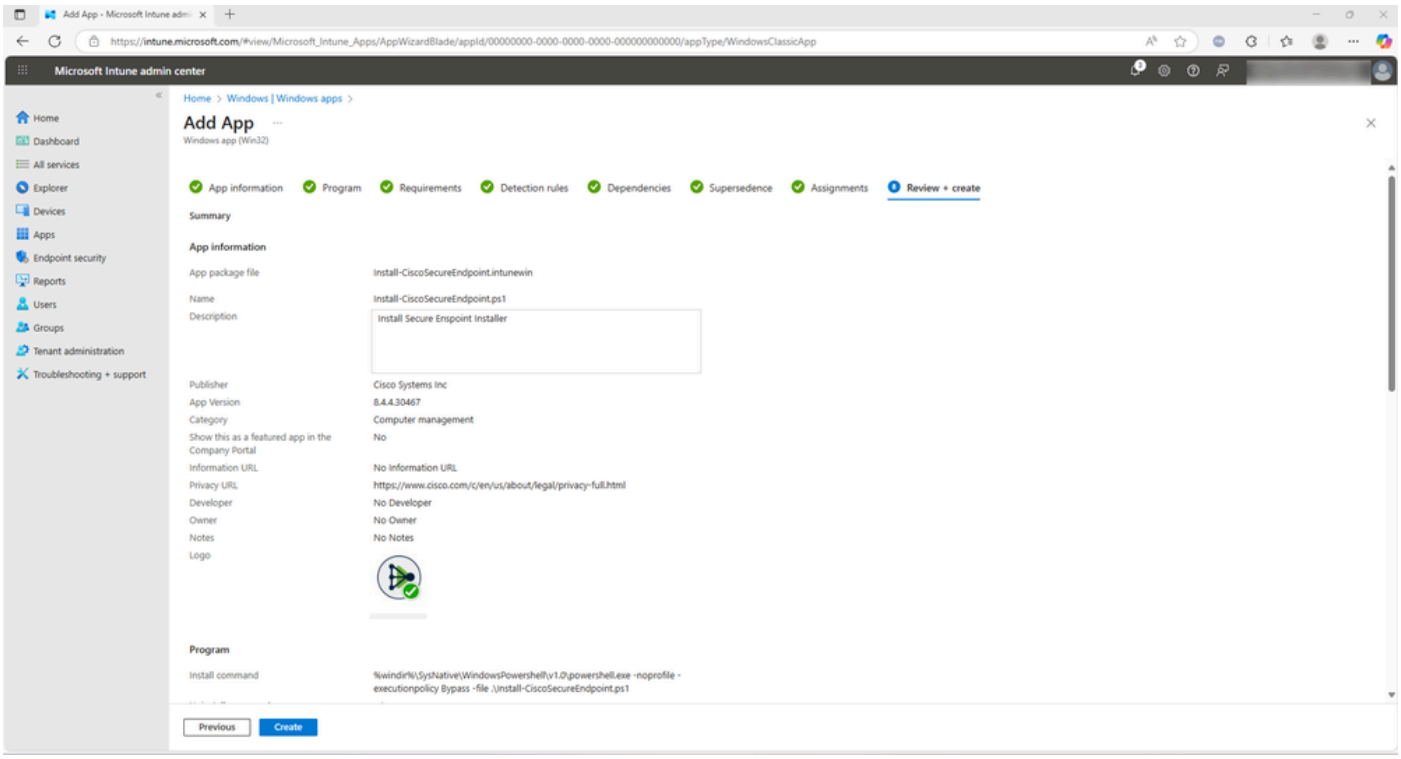
tipo di regola quale MSI, File o Registro di sistema per rilevare la presenza dell'applicazione. In questo documento è stata selezionata l'opzione alternativa Usa script di rilevamento personalizzato.

- Per verificare la corretta installazione di Cisco Secure Endpoint, viene utilizzato uno script di PowerShell denominato Confirm-CSEInstall.ps1. ed è elencato alla fine di questo documento.



- Selezionare Avanti per continuare. Nota: È possibile creare uno script di rilevamento personalizzato specifico per questo processo di distribuzione in base all'ambiente e ai criteri di rilevamento.

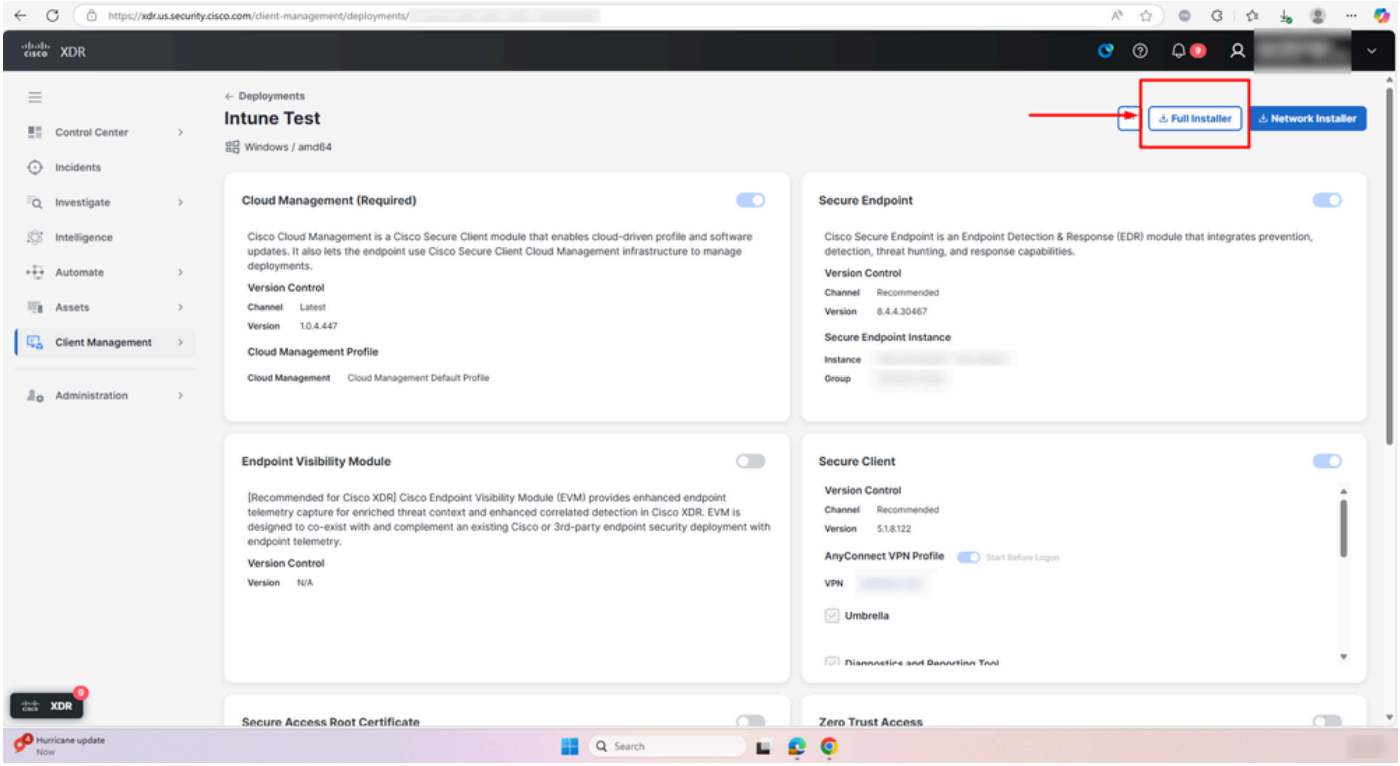
- Le schede successive sono facoltative. Non è necessario configurare alcuna dipendenza, assegnare l'applicazione al gruppo richiesto e selezionare Revisione + Crea



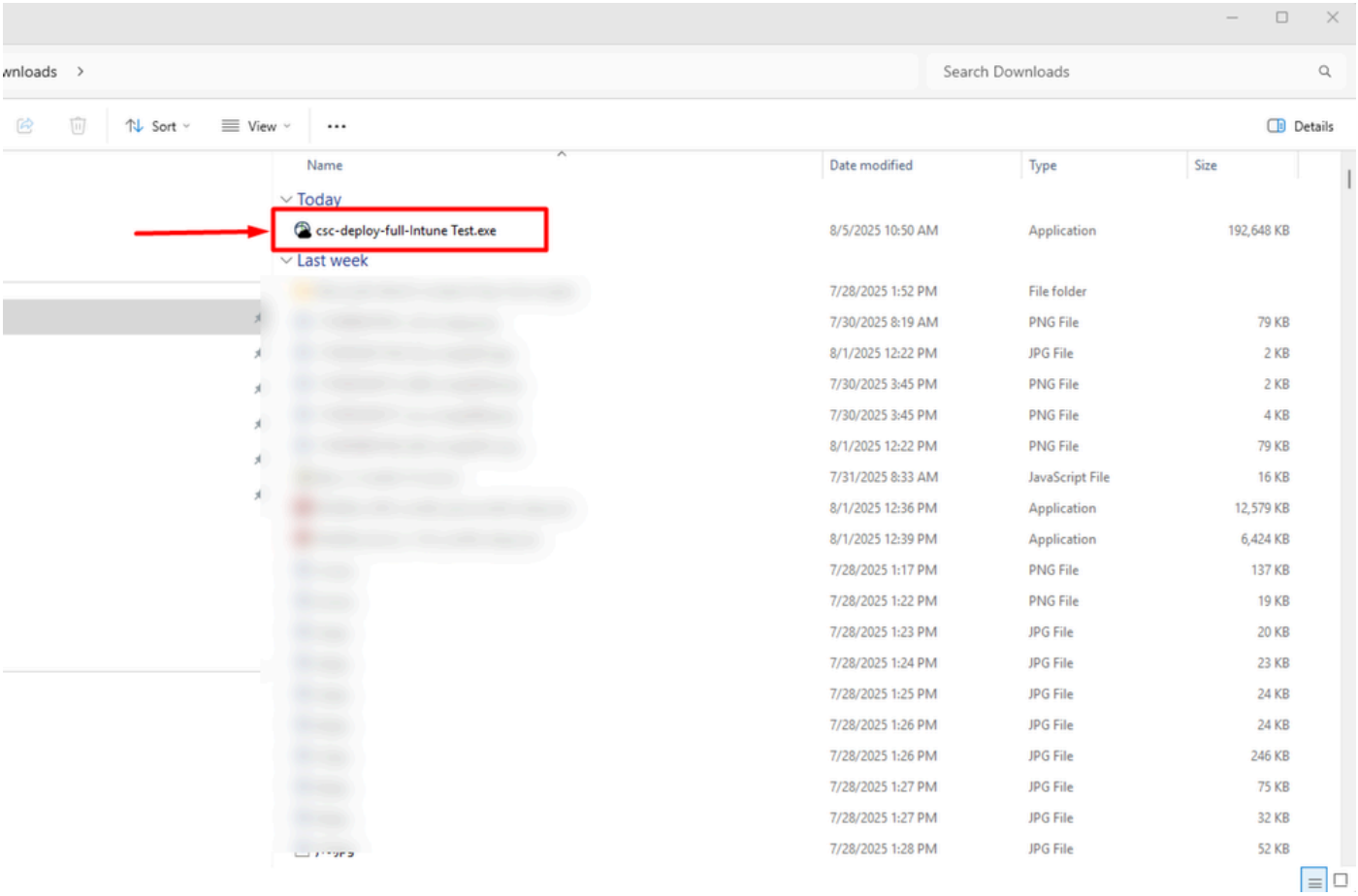
Installazione client sicura

Passaggio 1. Scaricare l'installazione completa di Cisco Secure Client

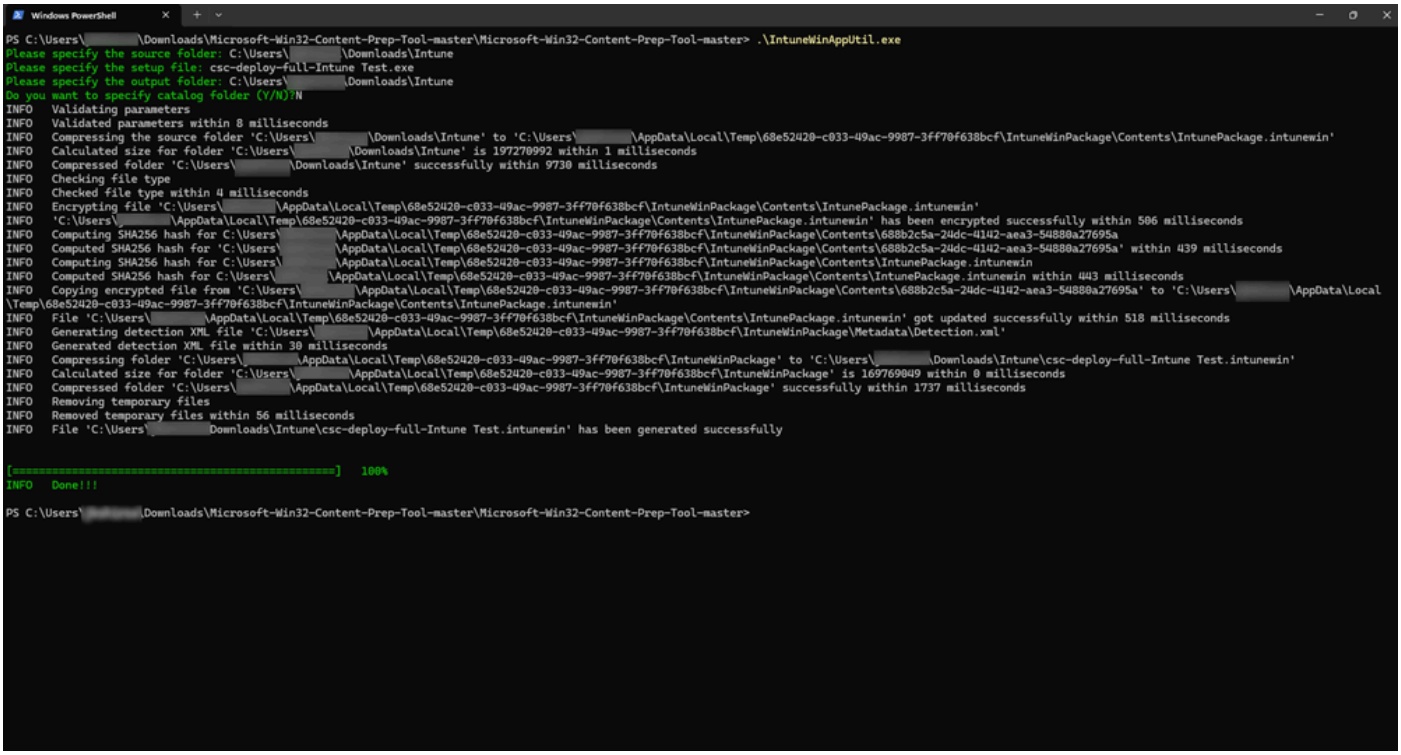
- Accedere alla console XDR o Secure Client Cloud Management, a seconda del paese: https://apps.security.cisco.com/overview
- Creare una nuova distribuzione e selezionare Installazione completa o Installazione di rete a seconda del tipo di distribuzione



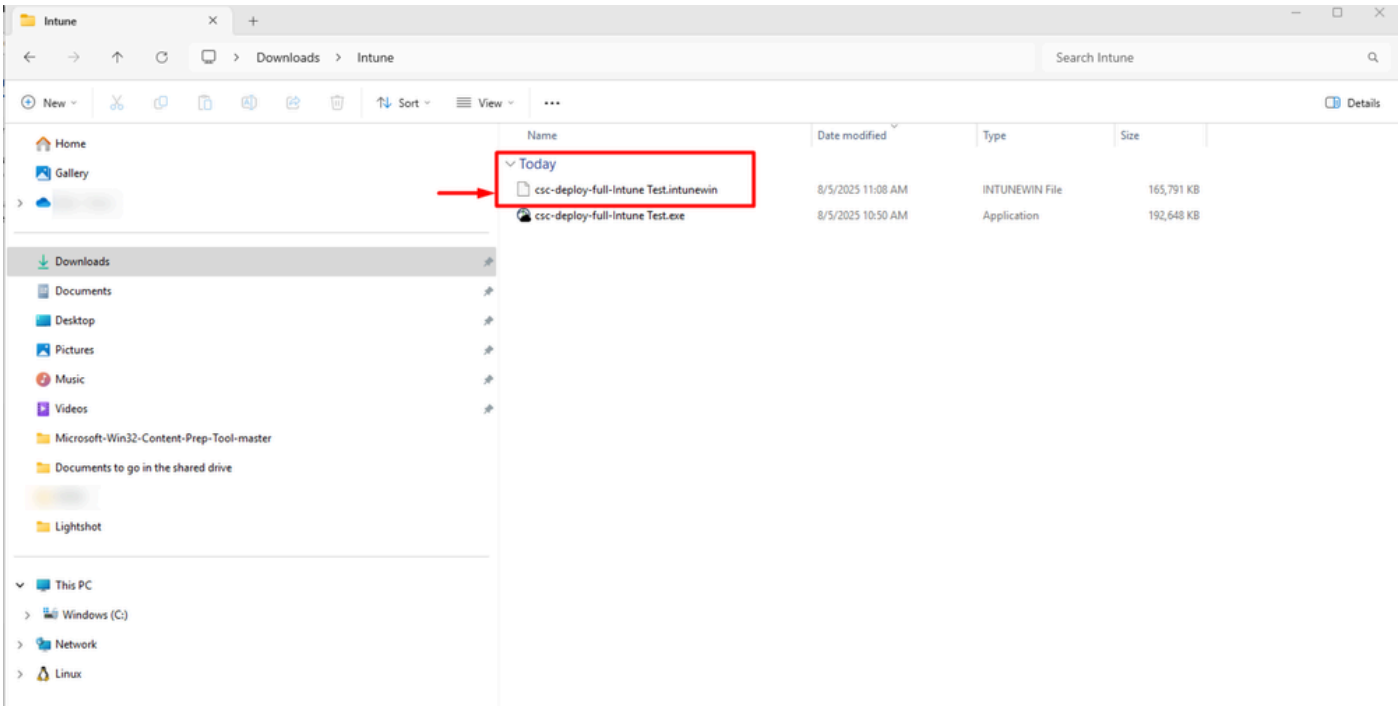
- Un file csc-deploy-full-Intune Test.exe viene scaricato come mostrato nello screenshot.



Passaggio 2. Preparare il file di Intune seguendo la stessa procedura al passaggio 2. In questo modo viene creato il file csc-deploy-full-Intune Test.intunewin.



- I passaggi precedenti determinano la creazione di un file csc-deploy-full-Intune Test.intunewin, come mostrato nello screenshot.



Passaggio 3. Caricare il file Test.intunewin csc-deploy-full-intune dalla parte 1 in Microsoft Intune Admin Center come indicato nei passaggi precedenti.

Il processo di distribuzione di Cisco Secure Endpoint con Intune è stato completato.

Script Install-CiscoSecureEndpoint.ps1

```
[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
}
```

Script Confirm-CSEInstall.ps1

```
[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
```

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).