Déployer Cisco Secure Endpoint/Secure Client à l'aide de Microsoft Intune

Table des matières

Introduction

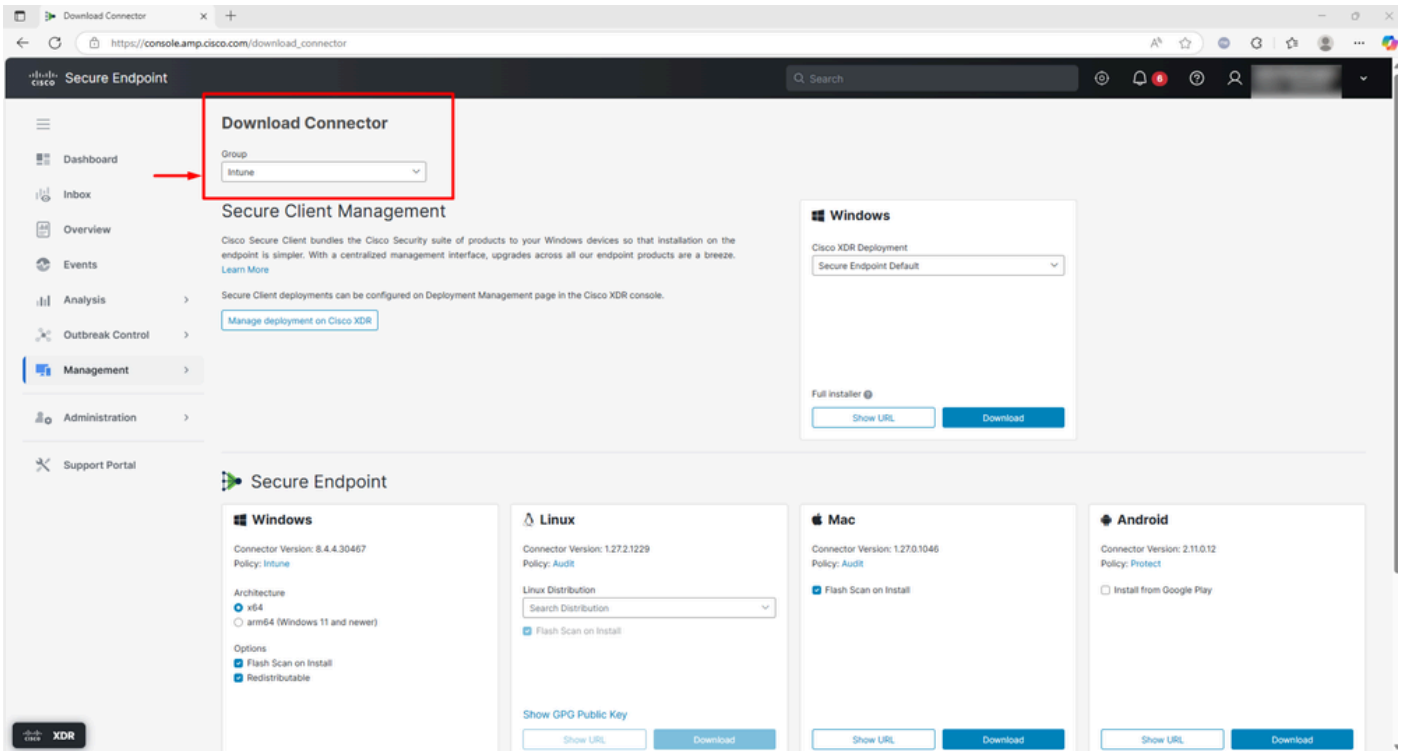
Ce document décrit le processus de déploiement de Cisco Secure Endpoint ou Secure Client à l'aide de Microsoft Intune. Le document décrit la procédure à suivre pour créer des applications prises en charge par Microsoft Intune à partir des programmes d'installation Secure Endpoint/Secure Client, puis l'utiliser pour le déploiement à l'aide du centre d'administration Microsoft Intune. Plus précisément, le processus inclut le conditionnement du programme d'installation de Cisco Secure Endpoint en tant qu'application Win32 à l'aide de l'outil Intune Win32 Content Prep Tool, suivi de la configuration et du déploiement de l'application via Intune. Nous avons utilisé l'outil officiel Microsoft Prep Tool pour créer l'application.

Configuration

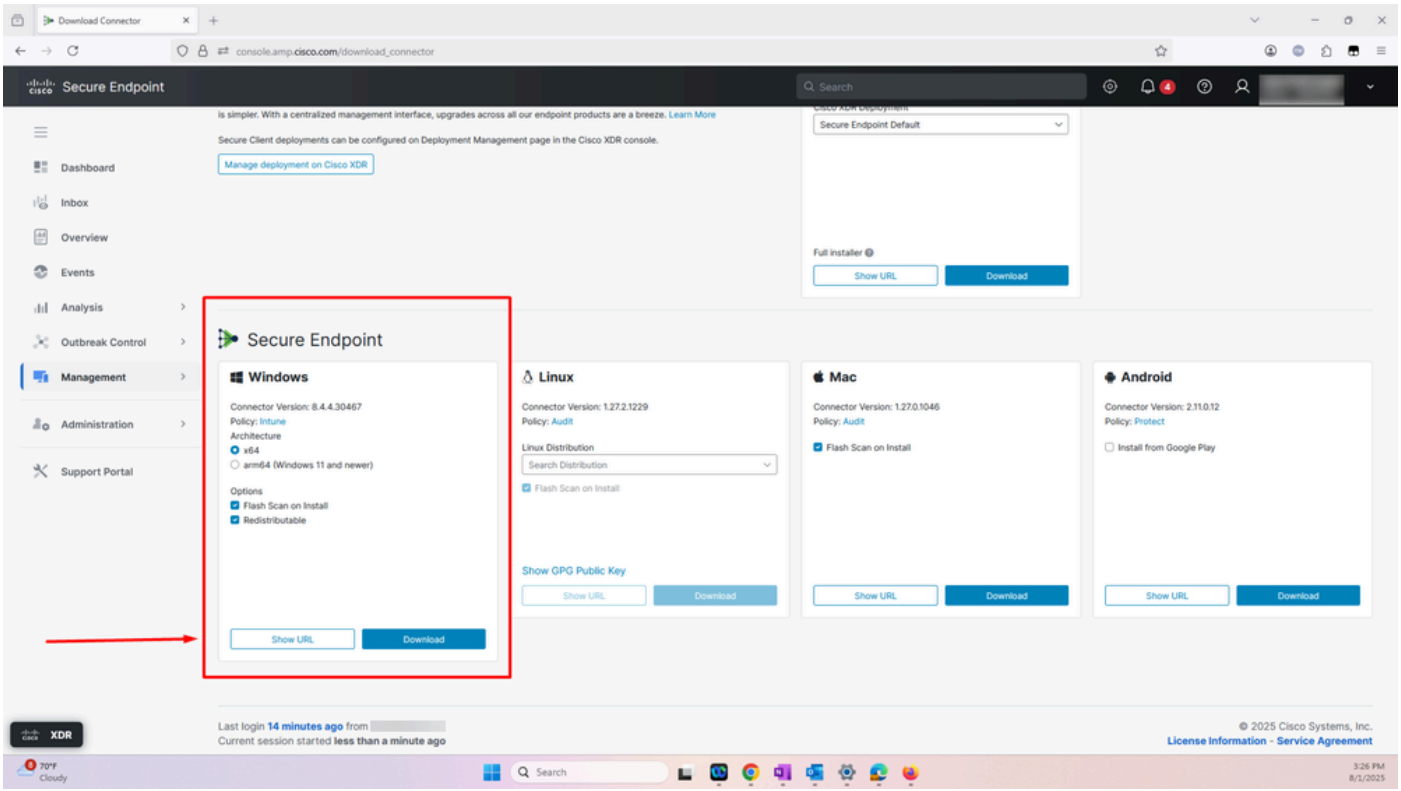
Déploiement sécurisé des terminaux

Étape 1 : téléchargement du programme d'installation de Cisco Secure Endpoint

- Connectez-vous à votre portail Secure Endpoint respectif, selon la région : https://apps.security.cisco.com/overview
- Accédez à l'onglet Management et sélectionnez Download Connector
- Sélectionnez le groupe de terminaux sécurisés auquel vous souhaitez enregistrer le connecteur



- Sélectionnez download et le programme d'installation EXE est téléchargé localement, comme indiqué dans la capture d'écran



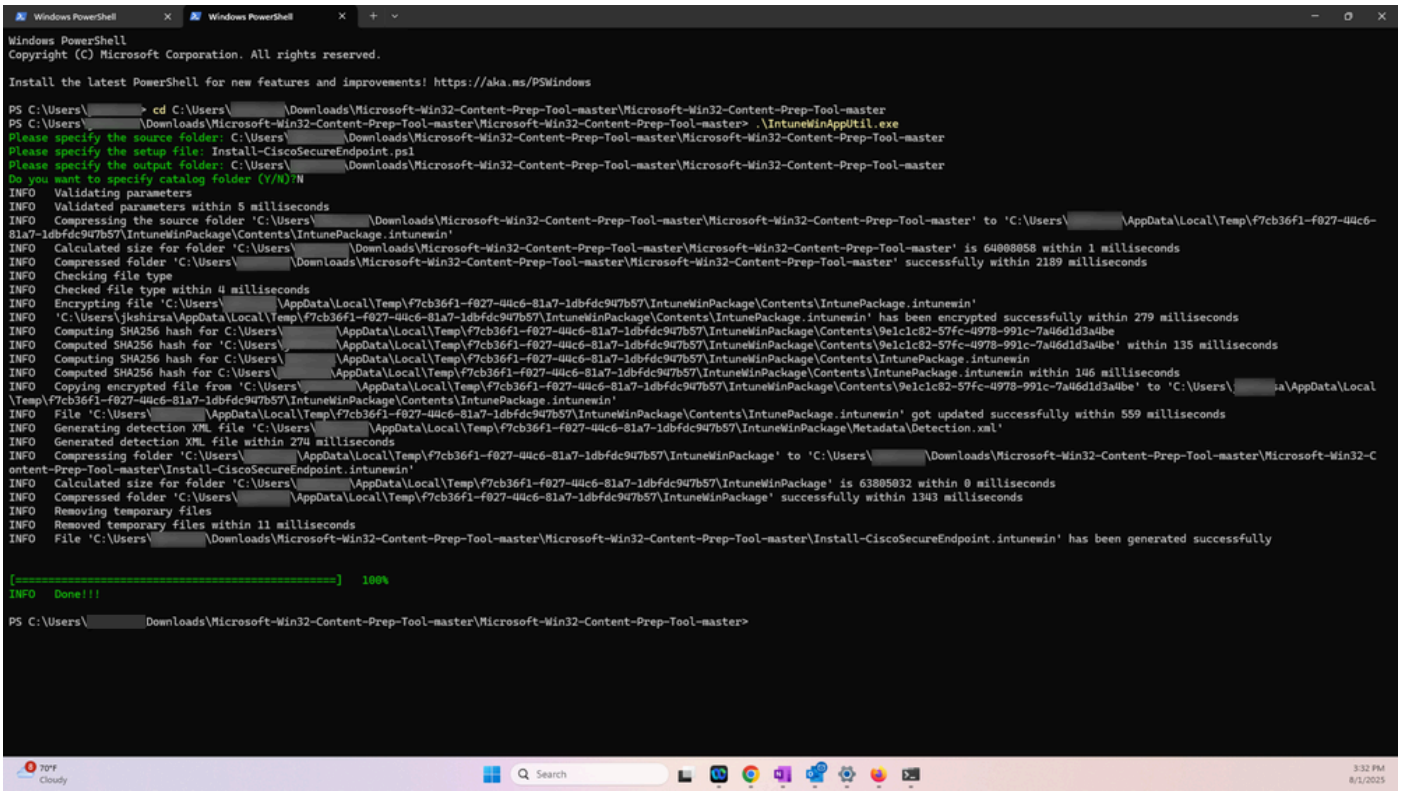
Étape 2 : préparation du fichier Intune à l'aide de l'outil de préparation de contenu Win32

L'outil de préparation de contenu Win32 est un utilitaire fourni par Microsoft Intune pour aider les administrateurs informatiques à préparer les applications Win32 (c'est-à-dire les applications de

bureau Windows traditionnelles) pour le déploiement via Microsoft Intune. L'outil convertit les programmes d'installation d'applications Win32 (comme .exe, .msi et les fichiers associés) dans un format de fichier .intunewin, qui est requis pour déployer ces applications via Intune.

Pour préparer le fichier Intune, procédez comme suit :

- Téléchargez l'outil de préparation de contenu Win32 depuis Github. Téléchargement : https://github.com/microsoft/Microsoft-Win32-Content-Prep-Tool
- Exécuter IntuneWinAppUtil.exe
- À l'étape suivante, accédez au dossier contenant le fichier exécutable Cisco Secure Endpoint téléchargé à l'étape 1 et le script d'installation PowerShell (Install-CiscoSecureEndpoint.ps1)
- Spécifiez ensuite le nom du fichier de script pour le fichier d'installation : Install-CiscoSecureEndpoint.ps1
- À l'étape suivante, spécifiez le dossier dans lequel le fichier Intunewin doit être généré
- Entrez N, lorsque vous êtes invité à spécifier le catalogue
- Le fichier Intunewin est généré comme indiqué dans la capture d'écran :

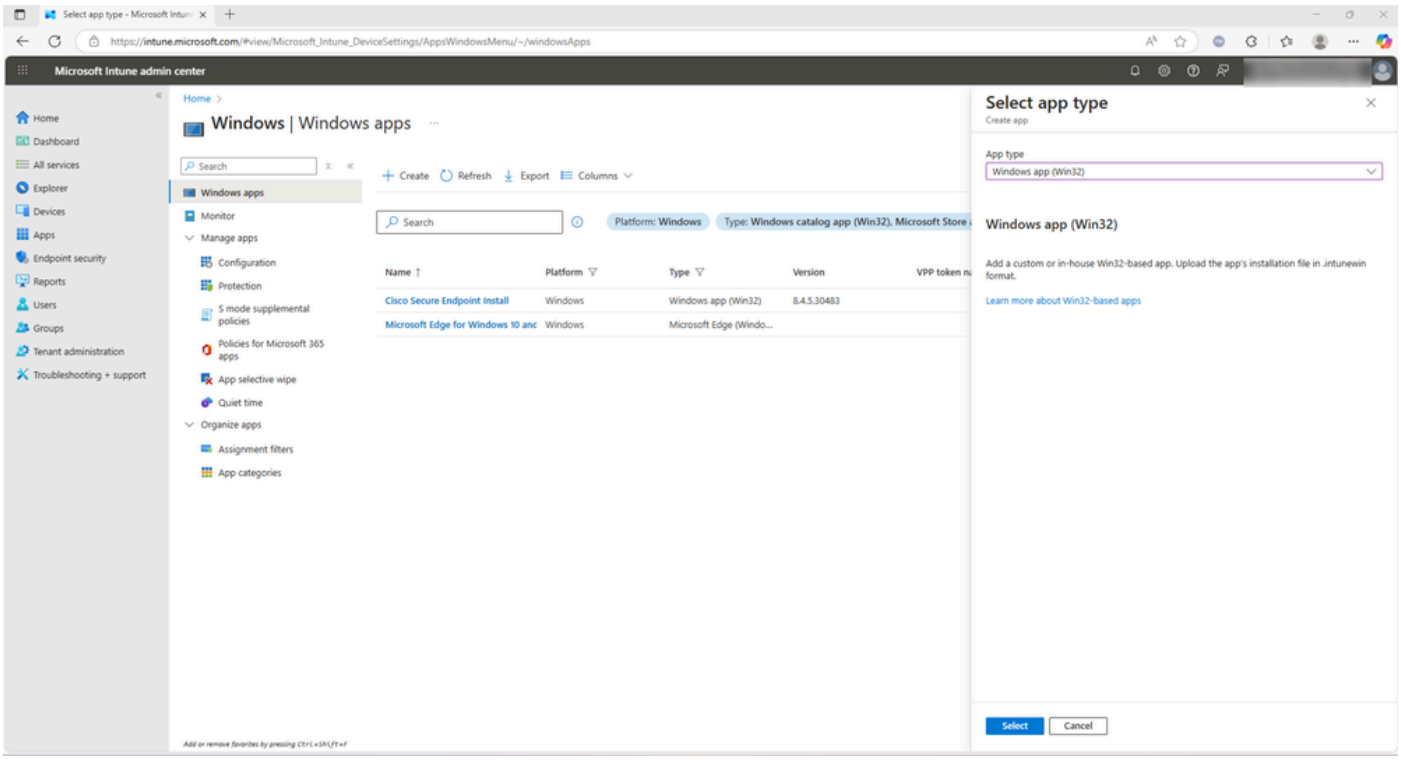


Étape 3. Téléchargez le fichier IntuneWin Secure Endpoint vers le Centre d'administration Microsoft Intune.

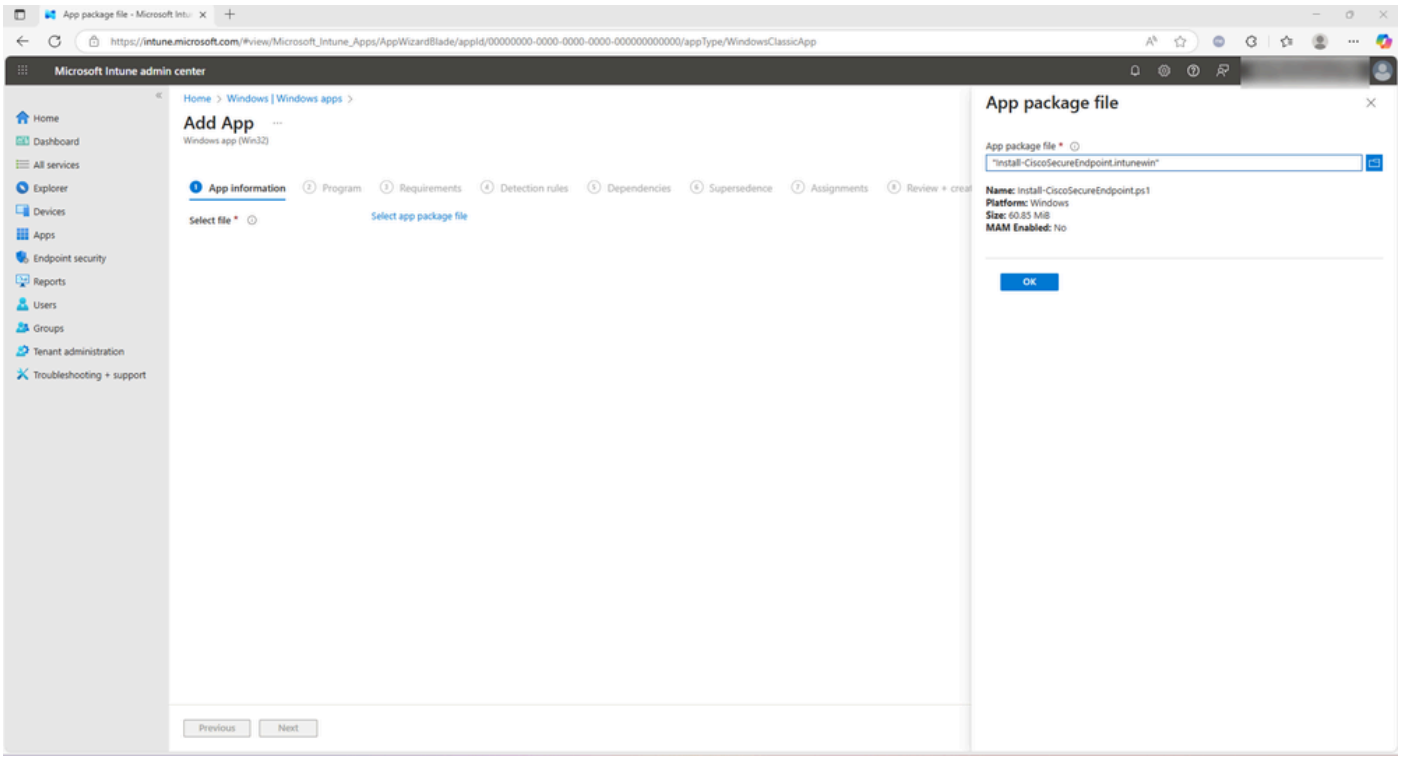
Procédez comme suit :

- Se connecter au Centre d'administration Microsoft Intune
- Accédez aux applications Windows dans le Centre d'administration Microsoft Intune et sélectionnez Type d'application - Win32 et sélectionnez

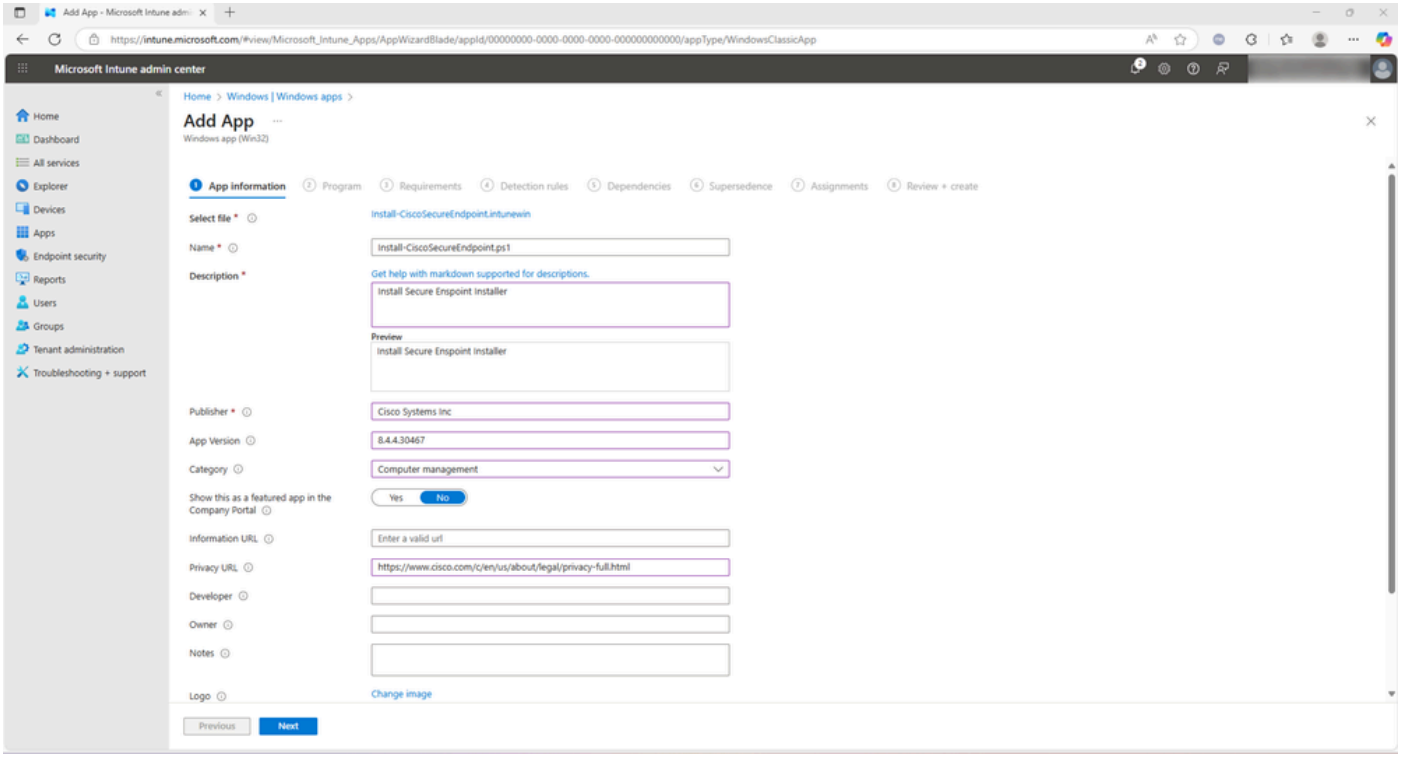
Ces deux actions sont illustrées dans la capture d'écran :



- À l'étape suivante, téléchargez le fichier Secure Endpoint Intunewin créé à l'étape 2 et sélectionnez OK



- Après avoir sélectionné OK, entrez les informations comme présenté dans la capture d'écran. Les champs facultatifs peuvent être laissés vides sur chaque onglet. Passez à l'étape suivante en sélectionnant Next

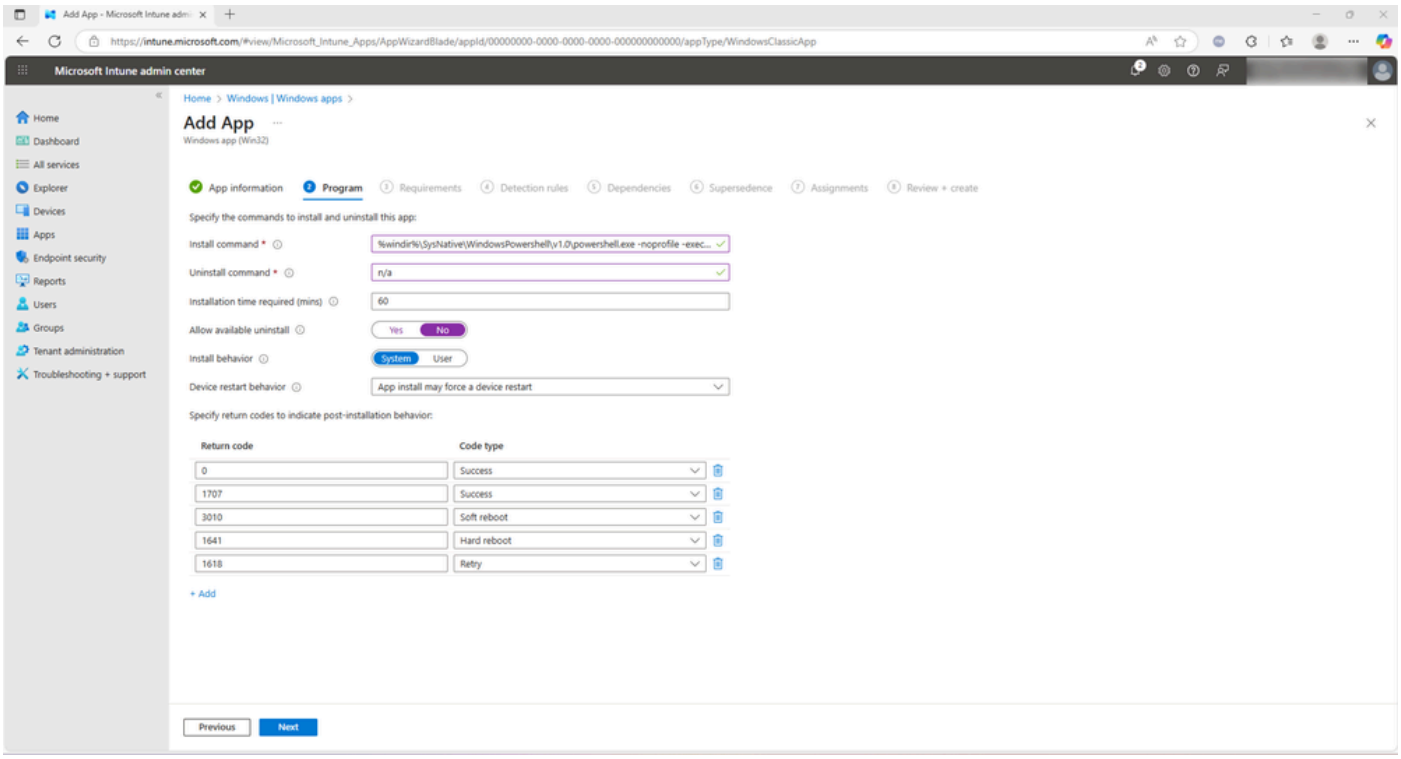


- Entrez la commande Install comme indiqué :

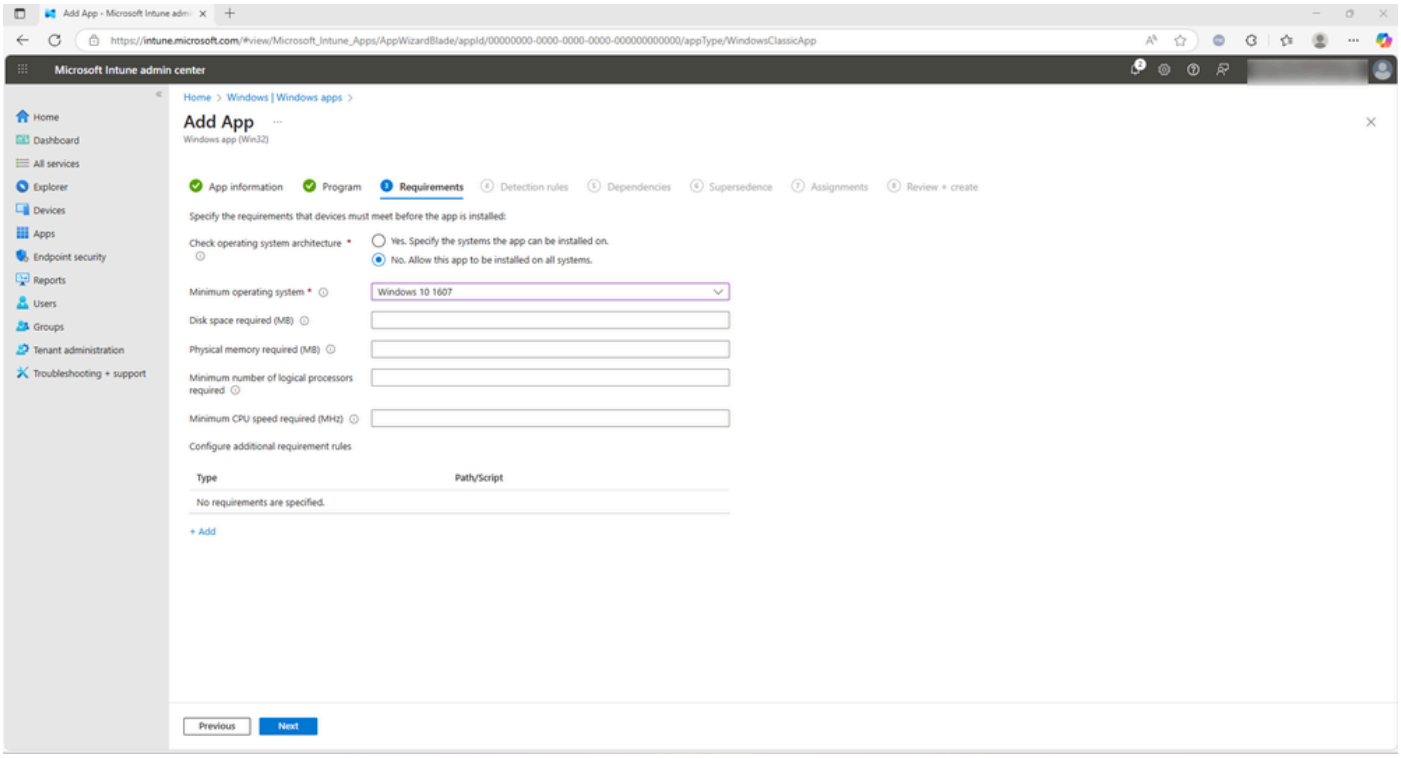
```
%windir%\SysNative\WindowsPowershell\v1.0\powershell.exe -noprofile -executionpolicy Bypass -file
```

Notez que le code présenté ici sert d'exemple et que tout code peut être utilisé comme commande d'installation pour ce programme d'installation

- Entrez Uninstall comme n/a et la durée d'installation requise comme 60 (facultatif). Définissez Autoriser la désinstallation disponible sur Non, sélectionnez Comportement d'installation sur Système et entrez les détails facultatifs avant de sélectionner Suivant



- Dans l'onglet Configuration requise, cochez Non. Autoriser l'installation de cette application sur tous les systèmes et sélectionnez le système d'exploitation minimum. Remplissez les champs facultatifs si vous le souhaitez et sélectionnez Suivant

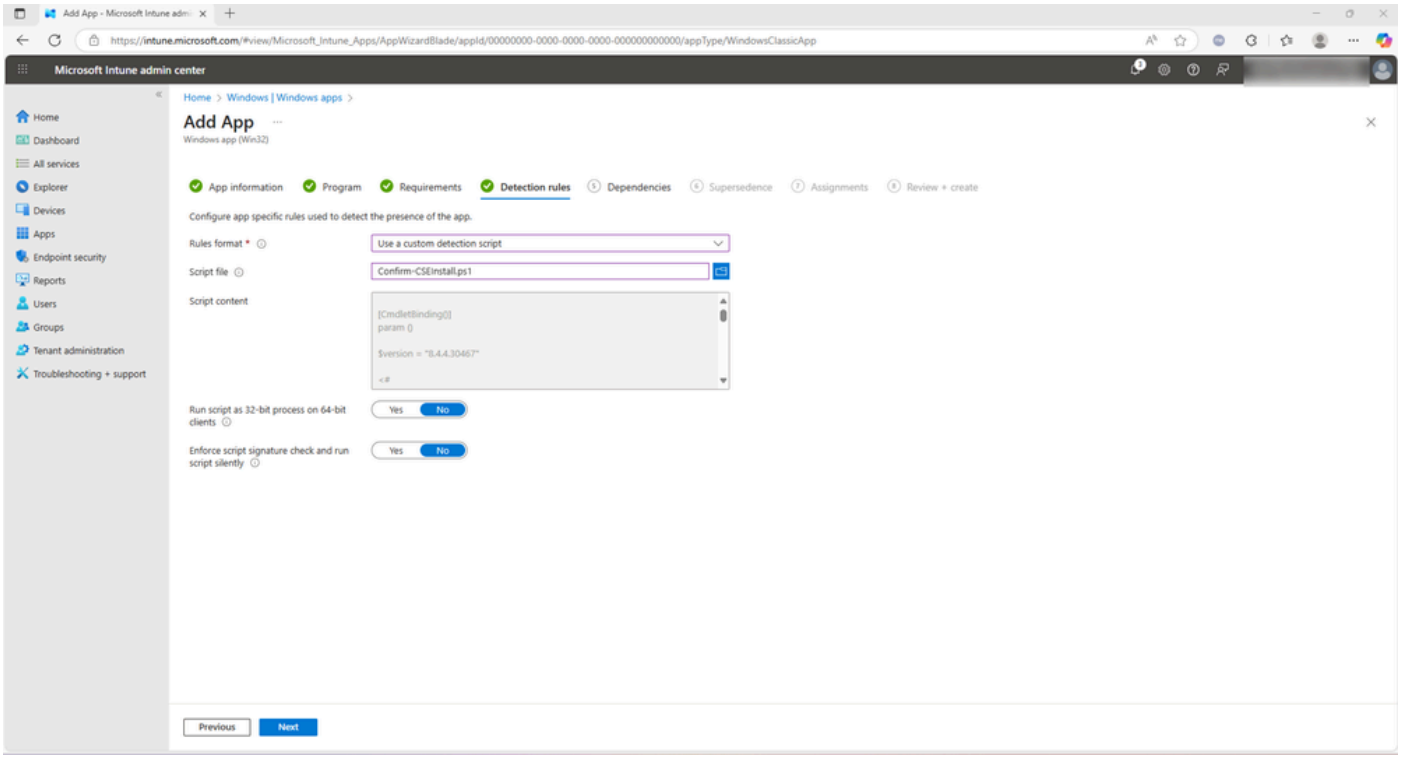


- Dans l'onglet Règles de détection, le menu déroulant Format des règles propose deux options : Configurez manuellement les règles de détection et utilisez un script de détection personnalisé. Les deux options peuvent être sélectionnées en fonction des exigences de déploiement.

- Lorsque vous choisissez Configurer manuellement les règles de détection, vous pouvez

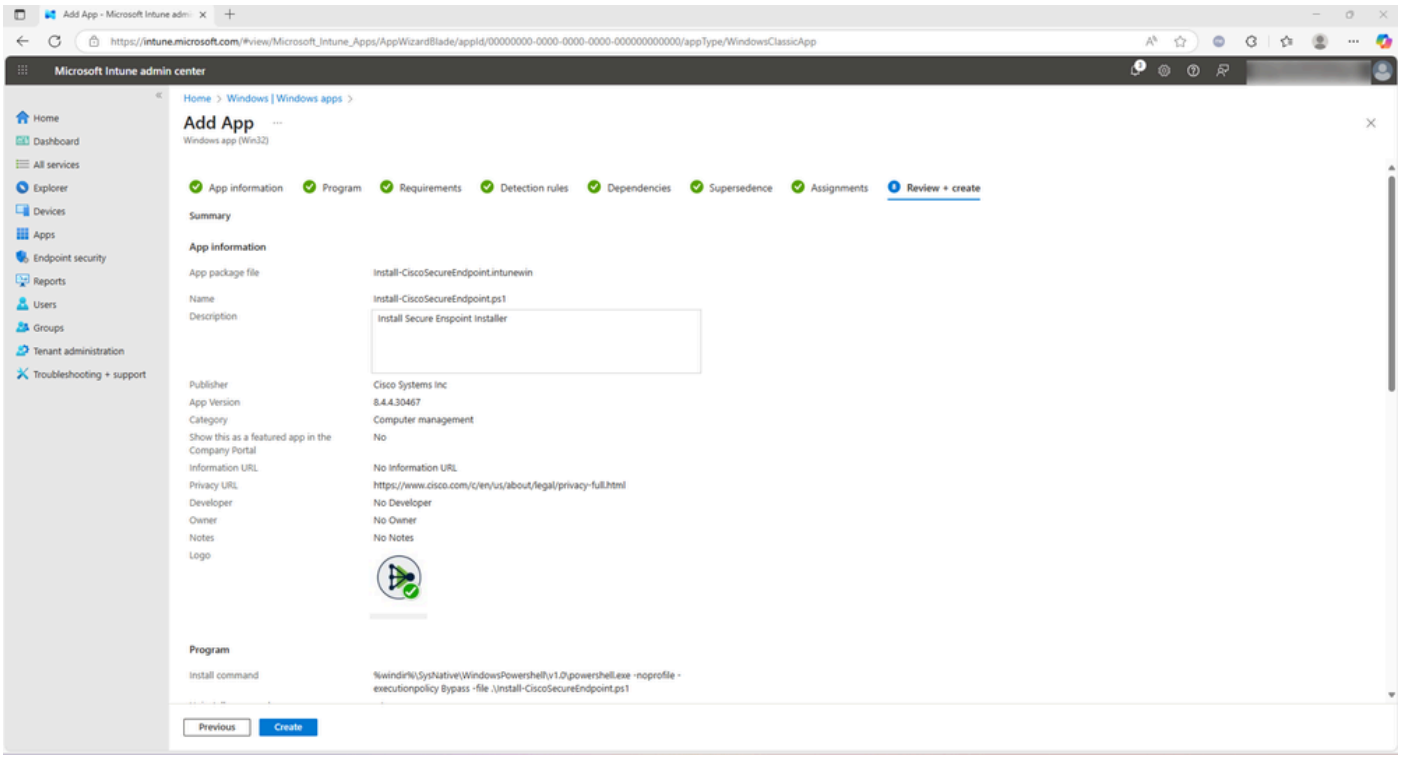
définir un type de règle tel que MSI, Fichier ou Registre pour détecter la présence de l'application. Dans ce document, l'option alternative, Utiliser un script de détection personnalisé, a été sélectionnée.

- Un script PowerShell nommé Confirm-CSEInstall.ps1 est utilisé pour vérifier la réussite de l'installation de Cisco Secure Endpoint. Il est répertorié au bas de ce document.



- Sélectionnez Next pour continuer. Remarque : Un script de détection personnalisé peut être créé spécifiquement pour ce processus de déploiement afin de répondre à votre environnement et à vos critères de détection.

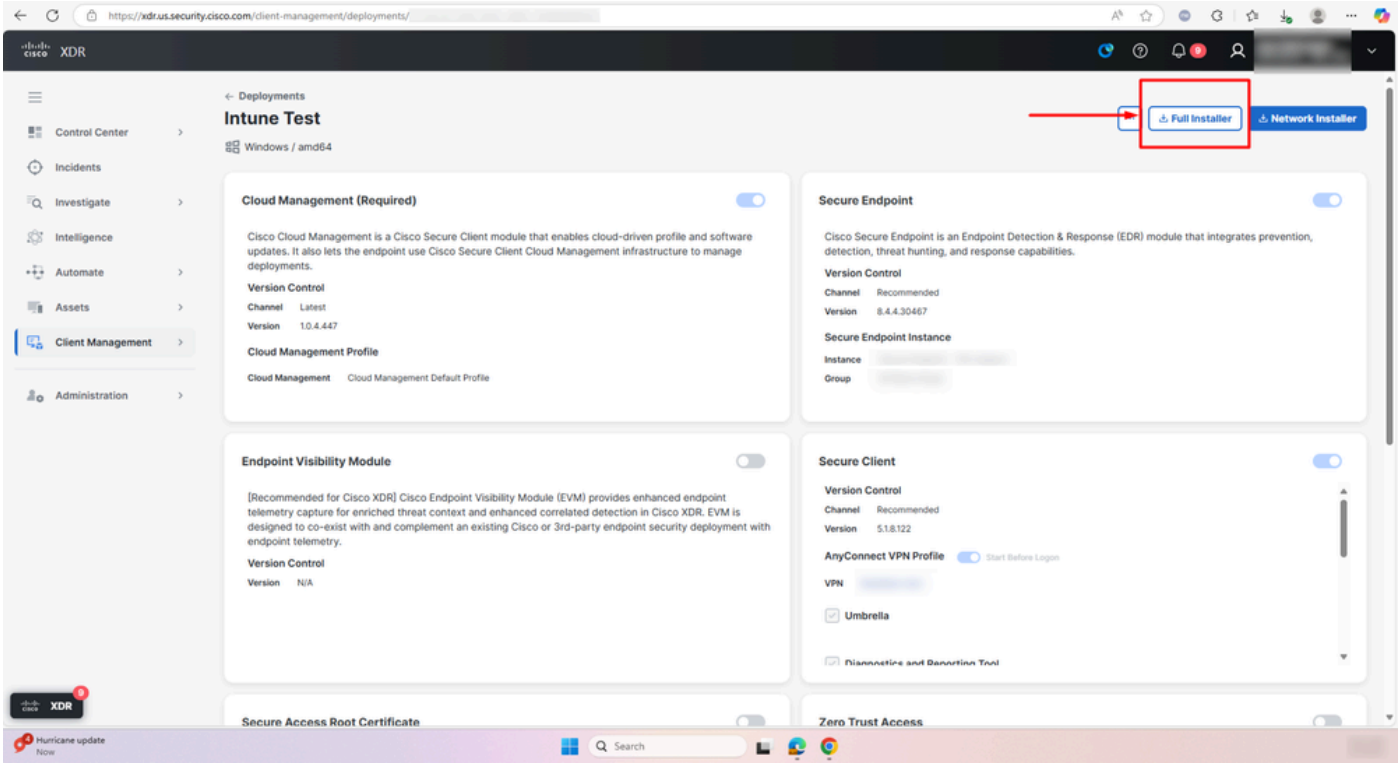
- Les onglets suivants sont facultatifs. Aucune dépendance n'a besoin d'être configurée, affectez l'application au groupe requis et sélectionnez Vérifier + créer



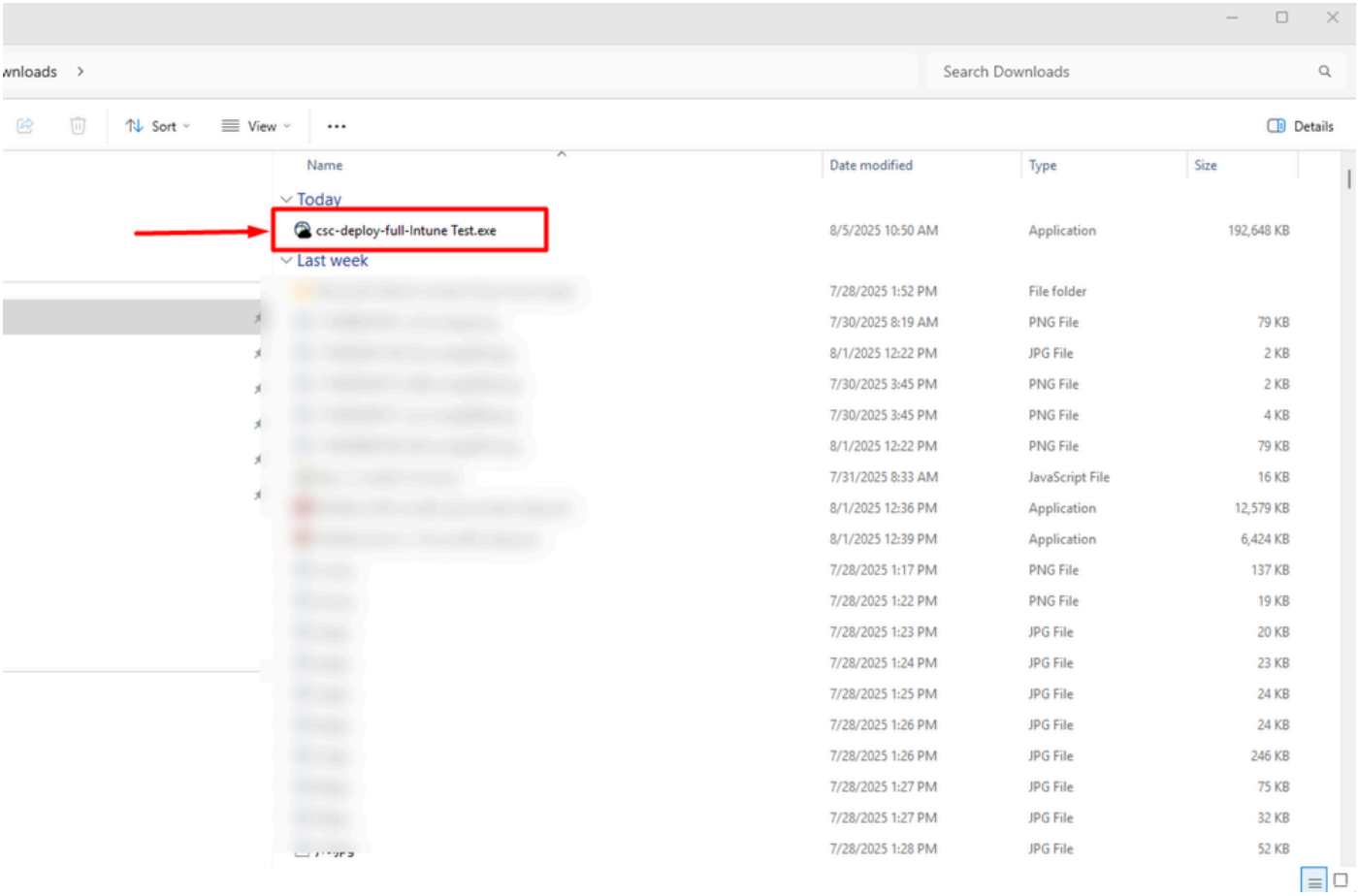
Déploiement sécurisé du client

Étape 1 : téléchargement du déploiement complet du client sécurisé Cisco

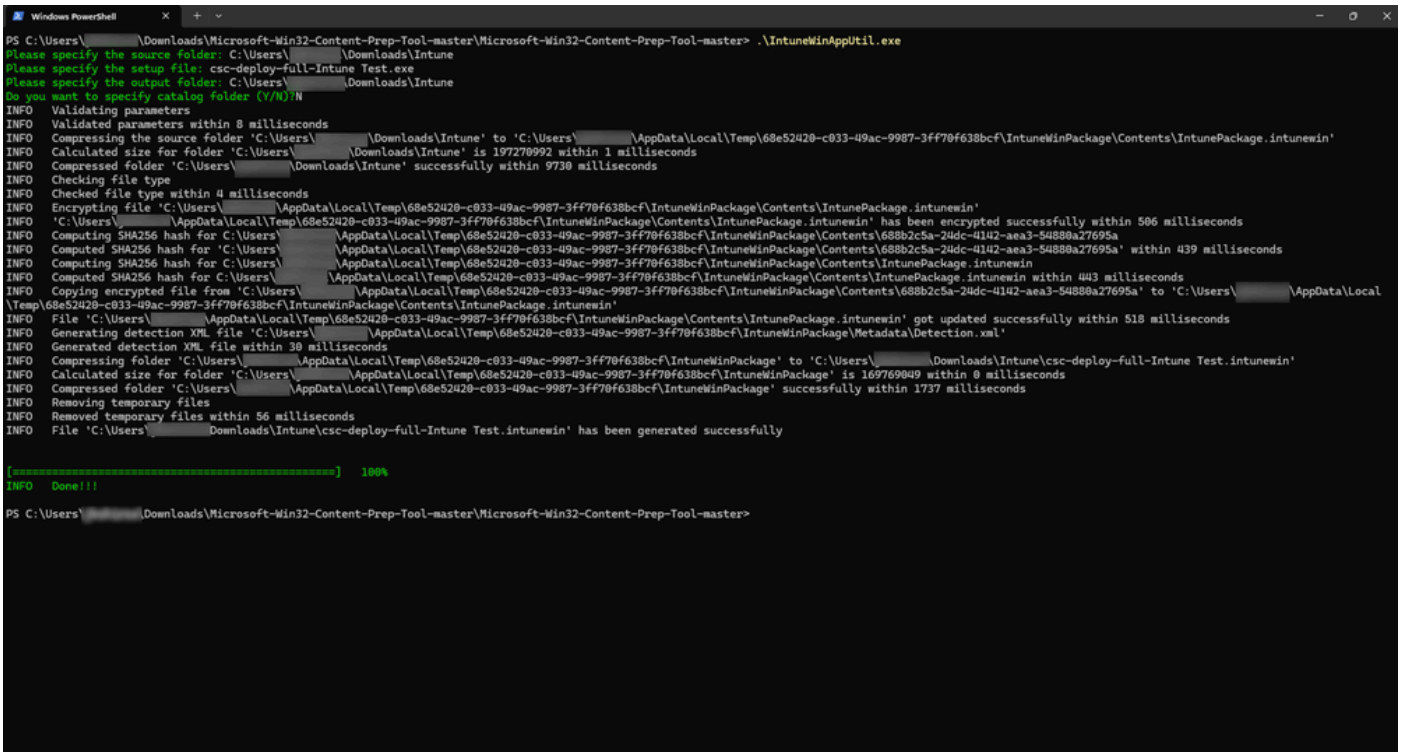
- Connectez-vous à la console XDR ou Secure Client Cloud Management, selon la région : https://apps.security.cisco.com/overview
- Créez un nouveau déploiement et sélectionnez Installation complète ou Installation réseau selon votre type de déploiement



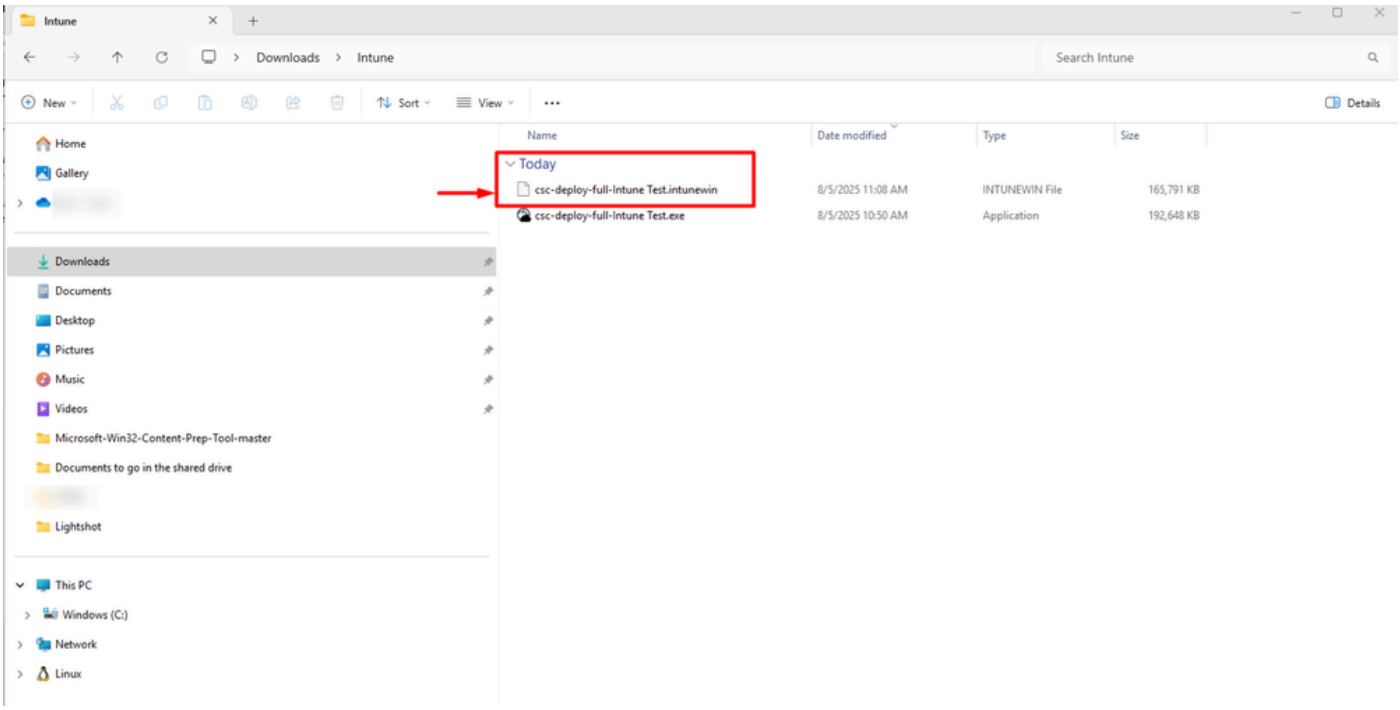
- Un fichier csc-deploy-full-Intune Test.exe est téléchargé, comme illustré dans la capture d'écran.



Étape 2. Préparez le fichier Intune en suivant la même procédure à l'étape 2. Ceci crée le fichier csc-deploy-full-Intune Test.intunewin.



- Les étapes ci-dessus entraînent la création d'un fichier csc-deploy-full-Intune Test.intunewin, comme indiqué dans la capture d'écran.



Étape 3. Téléchargez le fichier csc-deploy-full-intune Test.intunewin de la partie 1 vers le Centre d'administration Microsoft Intune, conformément aux étapes indiquées ci-dessus.

Le processus de déploiement de Cisco Secure Endpoint à l'aide d'Intune est ainsi terminé.

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
```

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.