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

Table des matières

Introduction

Fond

Configuration

Déploiement sécurisé des terminaux

- Étape 1 : téléchargement du programme d'installation de Cisco Secure Endpoint
- Étape 2 : préparation du fichier Intune à l'aide de l'outil de préparation de contenu Win32
- Étape 3.Téléchargez le fichier IntuneWin Secure Endpoint vers le Centre d'administration Microsoft Intune

Déploiement sécurisé du client

- Étape 1 : téléchargement du déploiement complet du client sécurisé Cisco
- Étape 2. Préparation du fichier Intune, même procédure que pour l'étape 2 : Le fichier csc-deploy-full-Intune Test.intunewin est créé
- Étape 3.Téléchargez le fichier csc-deploy-full-intune Test.intunewin de l'étape 1 vers Microsoft Intune Admin Center

Script Install-CiscoSecureEndpoint.ps1

Install - Script CiscoXDRDeployment.ps1

Script Confirm-CSEInstall.ps1

Introduction

Ce document décrit le processus de déploiement de Cisco Secure Endpoint ou Secure Client à l'aide de Microsoft Intune.

Fond

Ce document décrit les étapes de création d'applications prises en charge par Microsoft Intune à partir des programmes d'installation Secure Endpoint/Secure Client, puis les utilise 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 via l'outil Intune Win32 Content Prep Tool, ainsi que la configuration et le déploiement de l'application via Intune.

Configuration

Déploiement sécurisé des terminaux

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

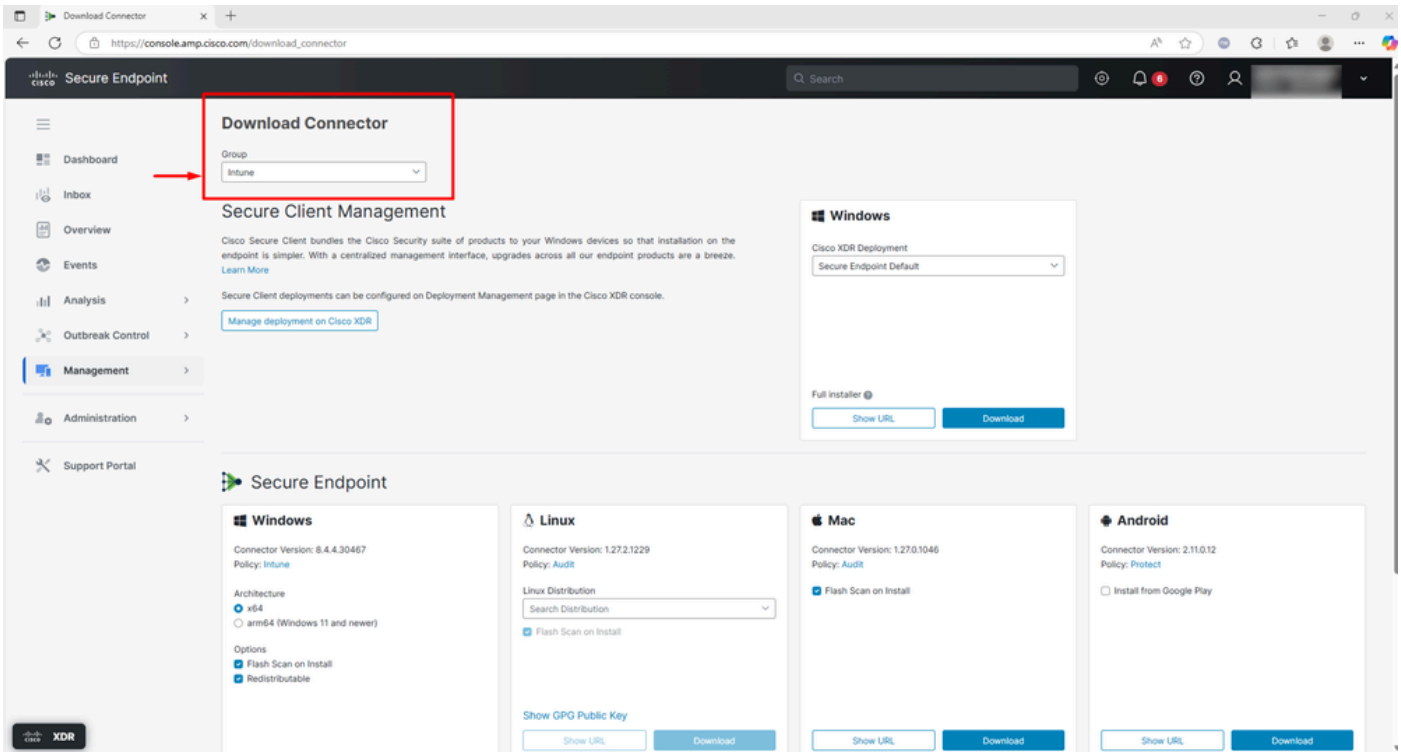
1. Connectez-vous à votre portail Secure Endpoint respectif, selon la région.

---

2. Accédez à l'onglet Management et sélectionnez Download Connector.

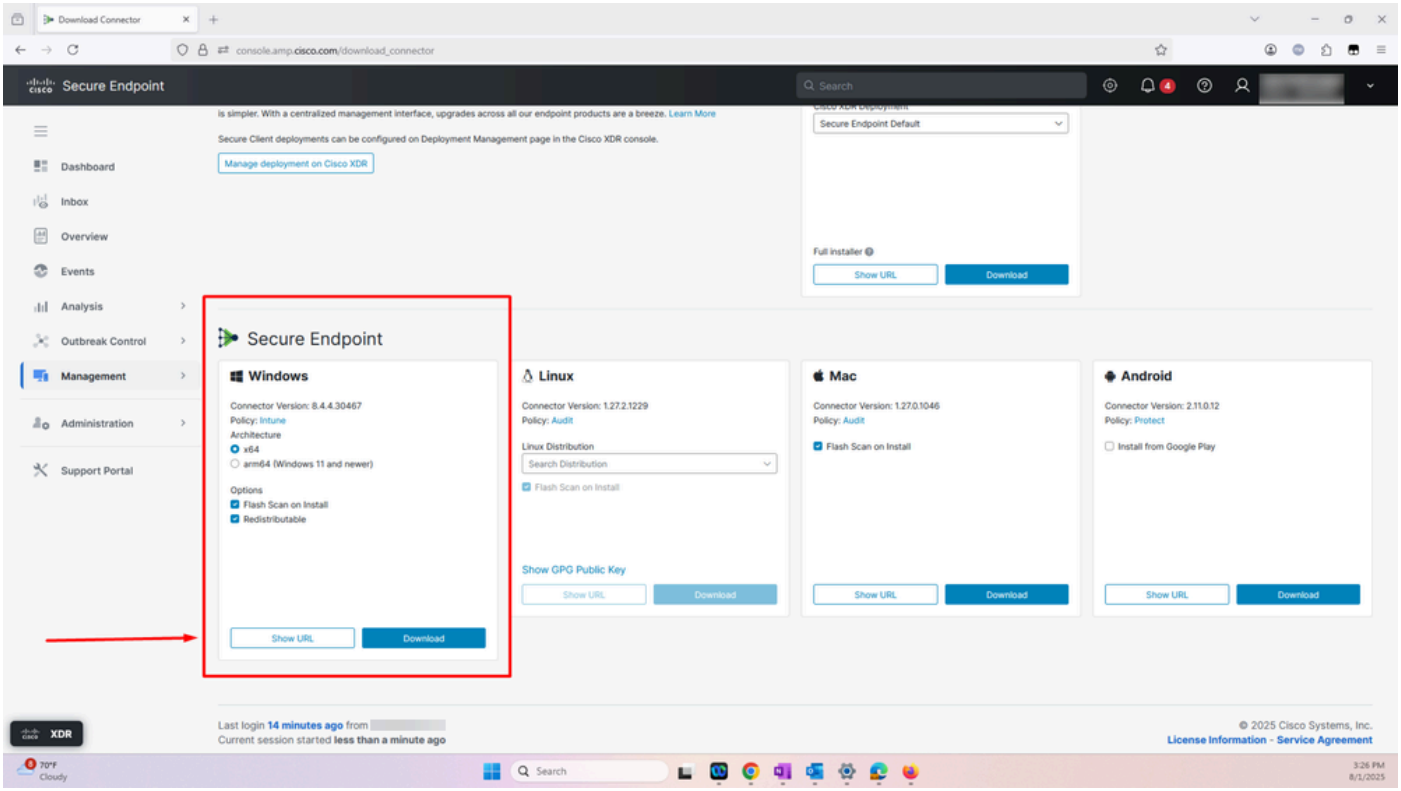
---

3. Sélectionnez le groupe de terminaux sécurisés auquel vous souhaitez enregistrer le connecteur.



---

4. Sélectionnez download et le programme d'installation d'EXE est téléchargé localement :



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 (pour 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 :

1. Téléchargez l'outil de préparation de contenu Win32 depuis Github.

---

2. Exécutez IntuneWinAppUtil.exe.

---

3. À l'étape suivante, remplacez le répertoire par le dossier contenant le fichier exécutable Cisco Secure Endpoint téléchargé à l'étape 1 et le script d'installation Powershell (Install-CiscoSecureEndpoint.ps1).

---

4. Spécifiez le nom du fichier de script pour le fichier d'installation, Install-CiscoSecureEndpoint.ps1.

---

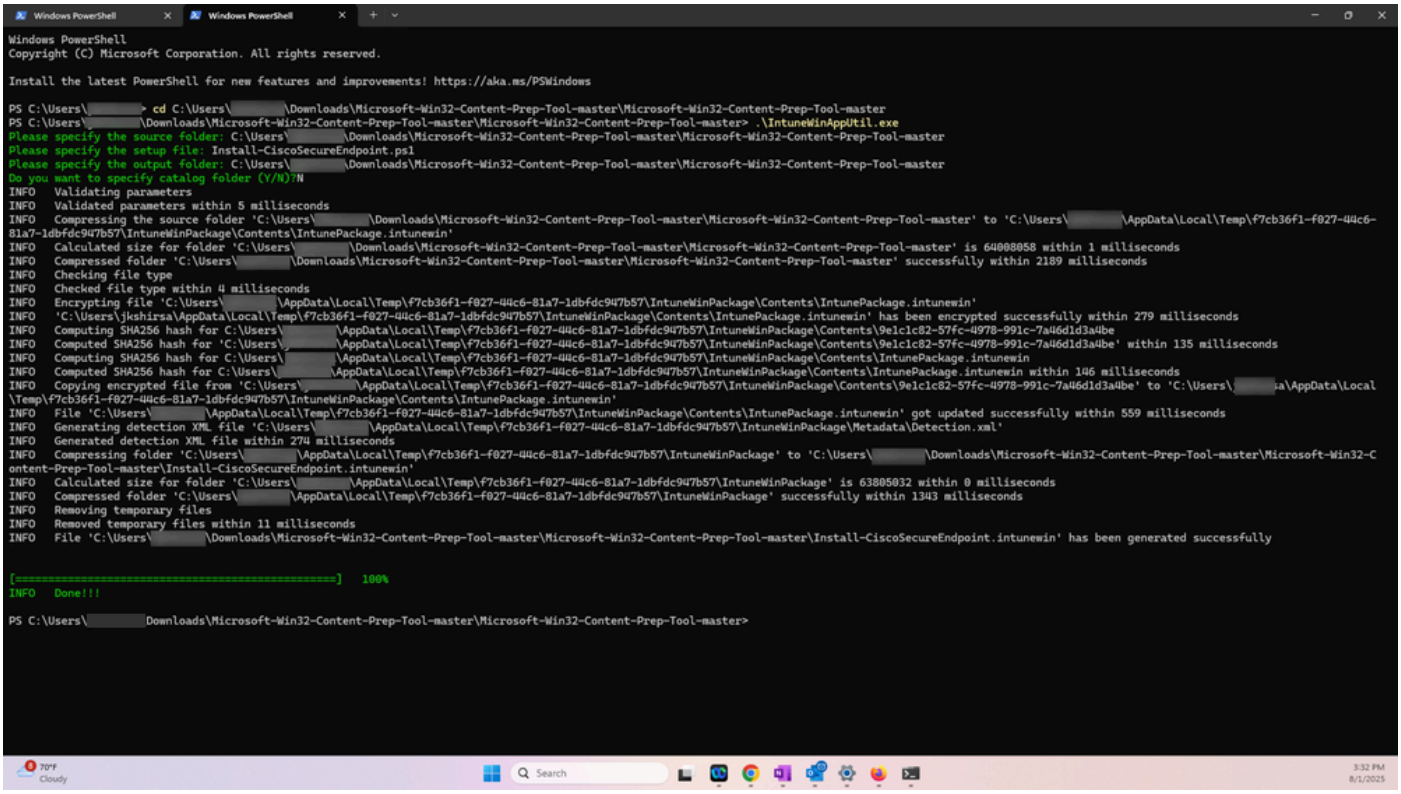
5. À l'étape suivante, spécifiez le dossier dans lequel le fichier Intunewin doit être généré.

---

6. Entrez N, lorsque vous êtes invité à spécifier le catalogue.

---

7. Le fichier Intunewin est généré comme indiqué dans la capture d'écran :

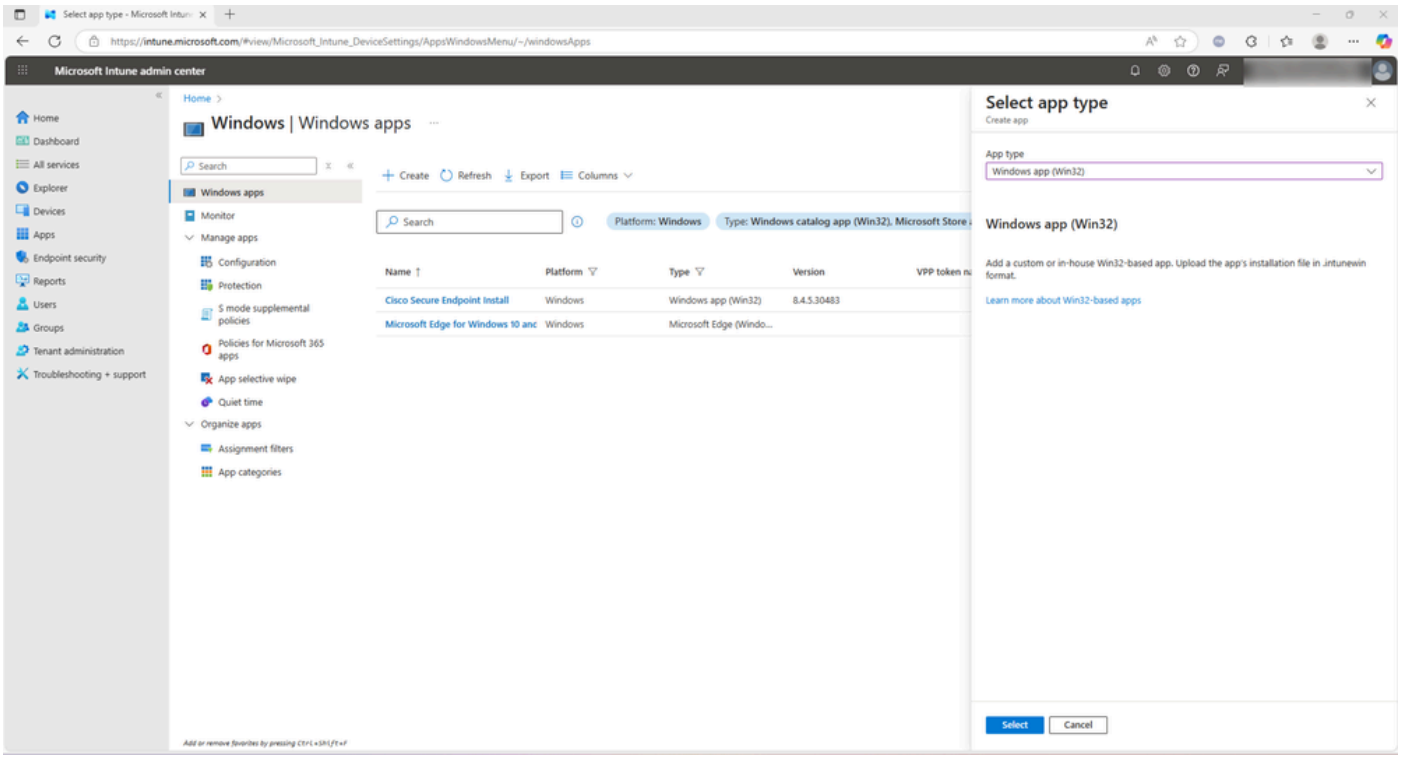


Étape 3. Télécharger le fichier IntuneWin Secure Endpoint vers le Centre d'administration Microsoft Intune

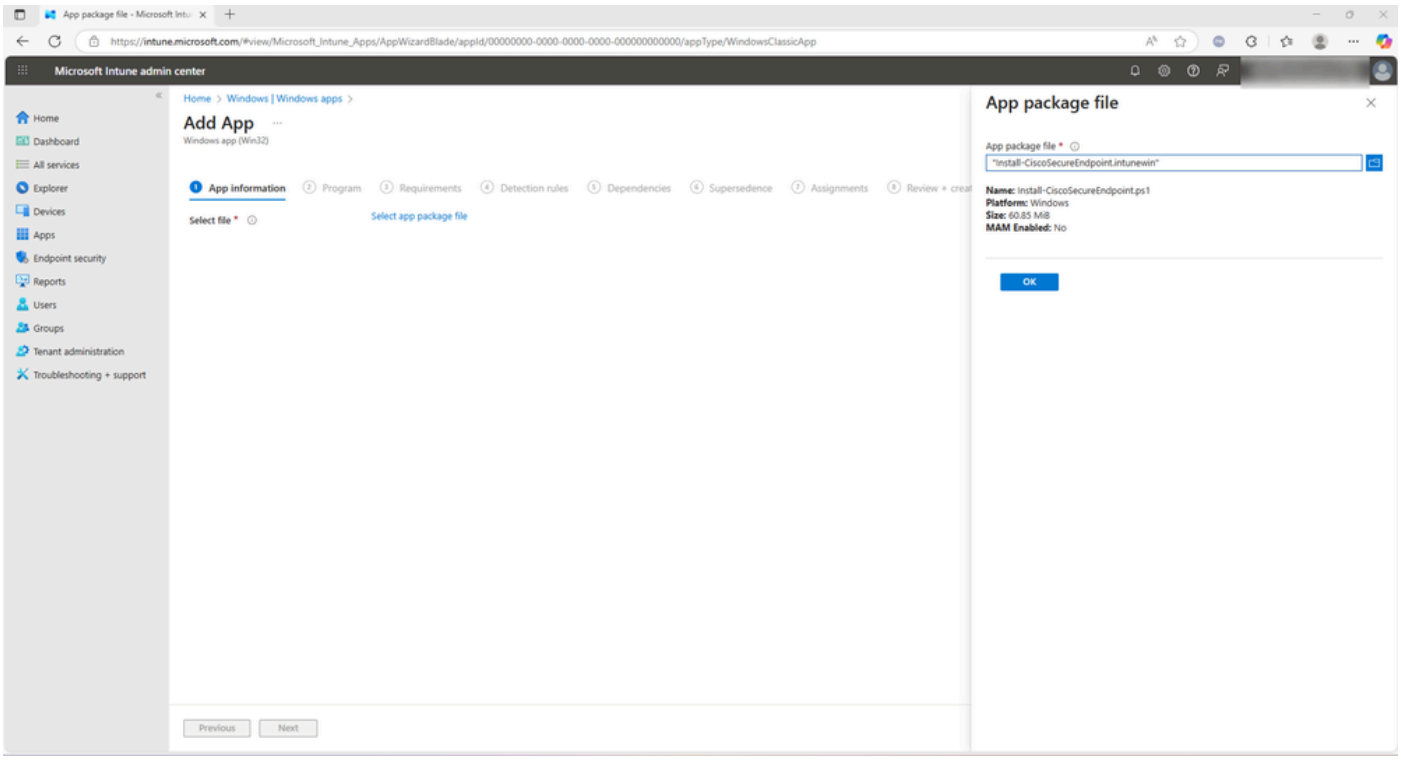
1. Connectez-vous au Centre d'administration Microsoft Intune.

---

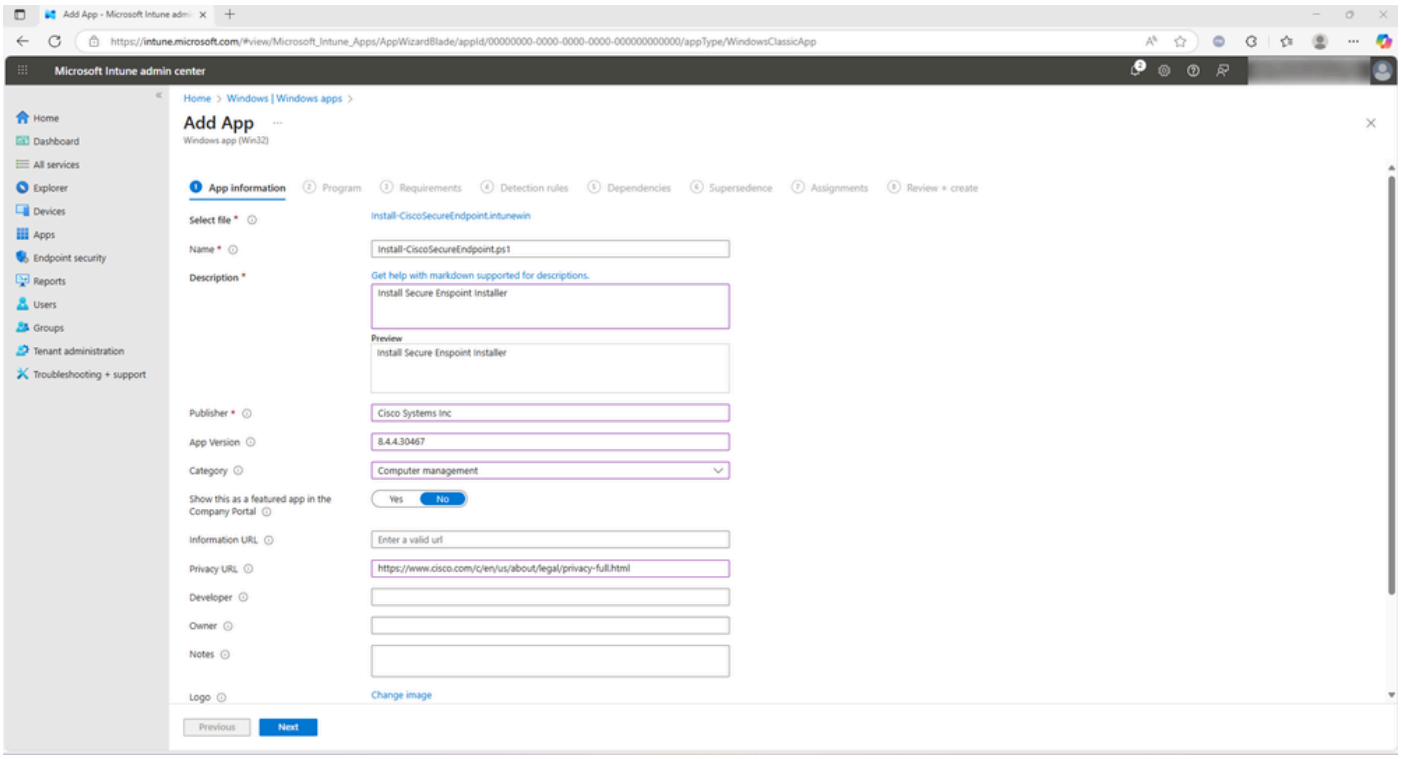
2. Accédez aux applications Windows dans le Centre d'administration Microsoft Intune et sélectionnez Type d'application - Win32 et sélectionnez ces deux actions décrites dans la capture d'écran :



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



4. Après avoir sélectionné OK, entrez les informations comme présenté dans la capture d'écran. Les champs facultatifs peuvent être laissés vides sur chaque onglet, puis cliquez sur Next.



---

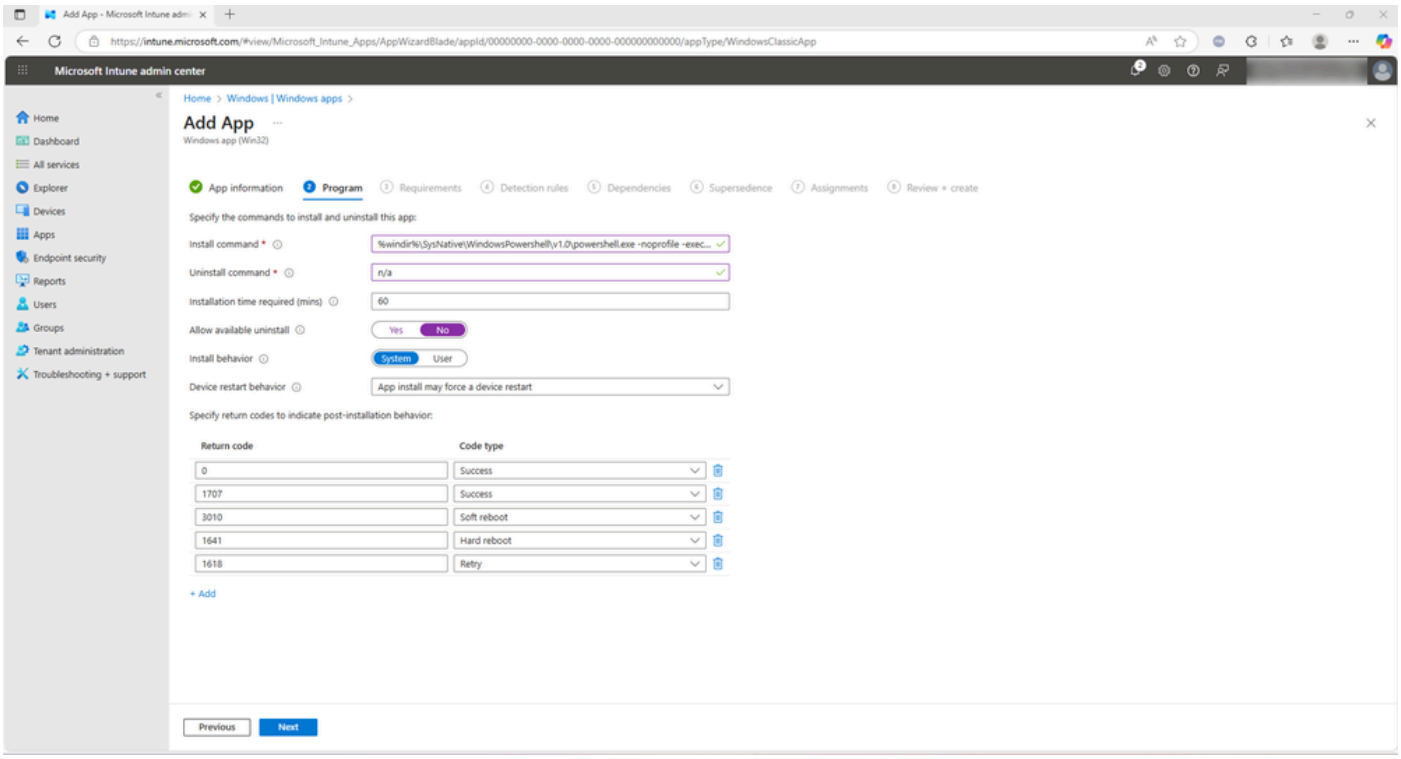
5. Exécutez la commande Install :

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

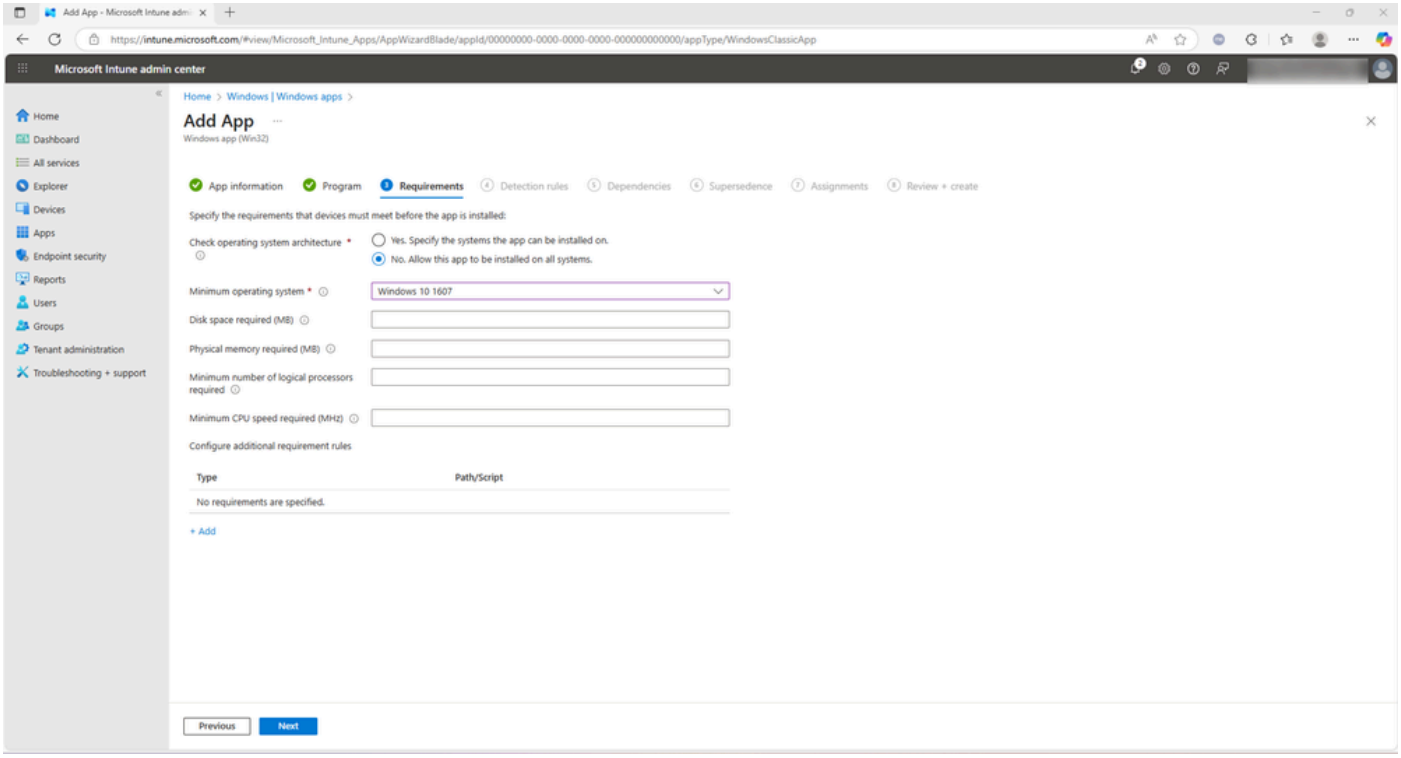
Remarque : Le code présenté est un exemple et n'importe quel code peut être utilisé comme commande d'installation pour ce programme d'installation.

---

6. Saisissez Uninstall comme n/a et la durée d'installation requise comme 60 (facultatif). Définissez Autoriser la désinstallation disponible sur Non, puis sélectionnez Comportement d'installation sur Système. Ajoutez des détails facultatifs supplémentaires avant de sélectionner Next.



7. Dans l'onglet Configuration requise, cochez Non. Autorisez 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 Next.



8. Sous l'onglet Règles de détection, le menu déroulant Format des règles propose deux options :

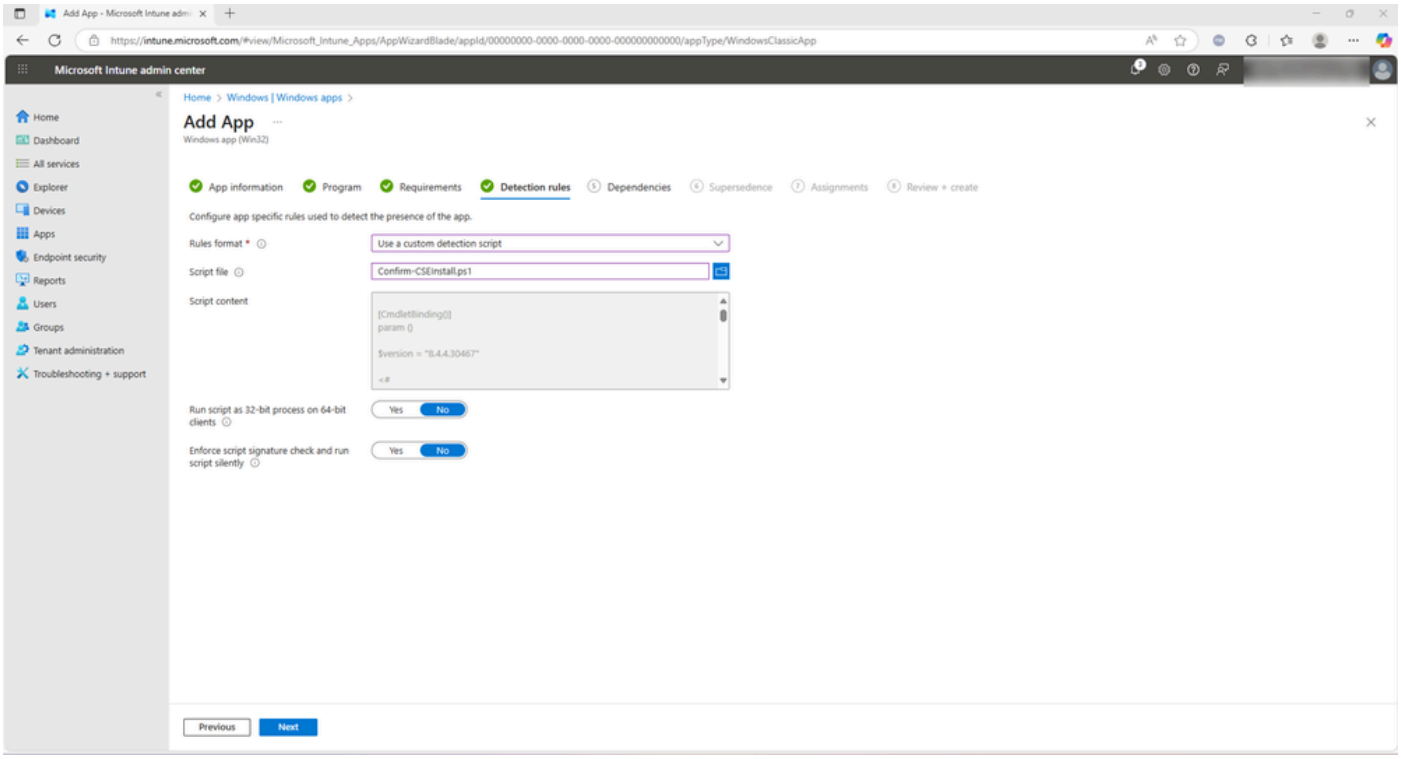
Configurer manuellement les règles de détection et Utiliser un script de détection personnalisé. Les deux options peuvent être sélectionnées en fonction des exigences de déploiement.

---

9. 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.

---

10. 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).



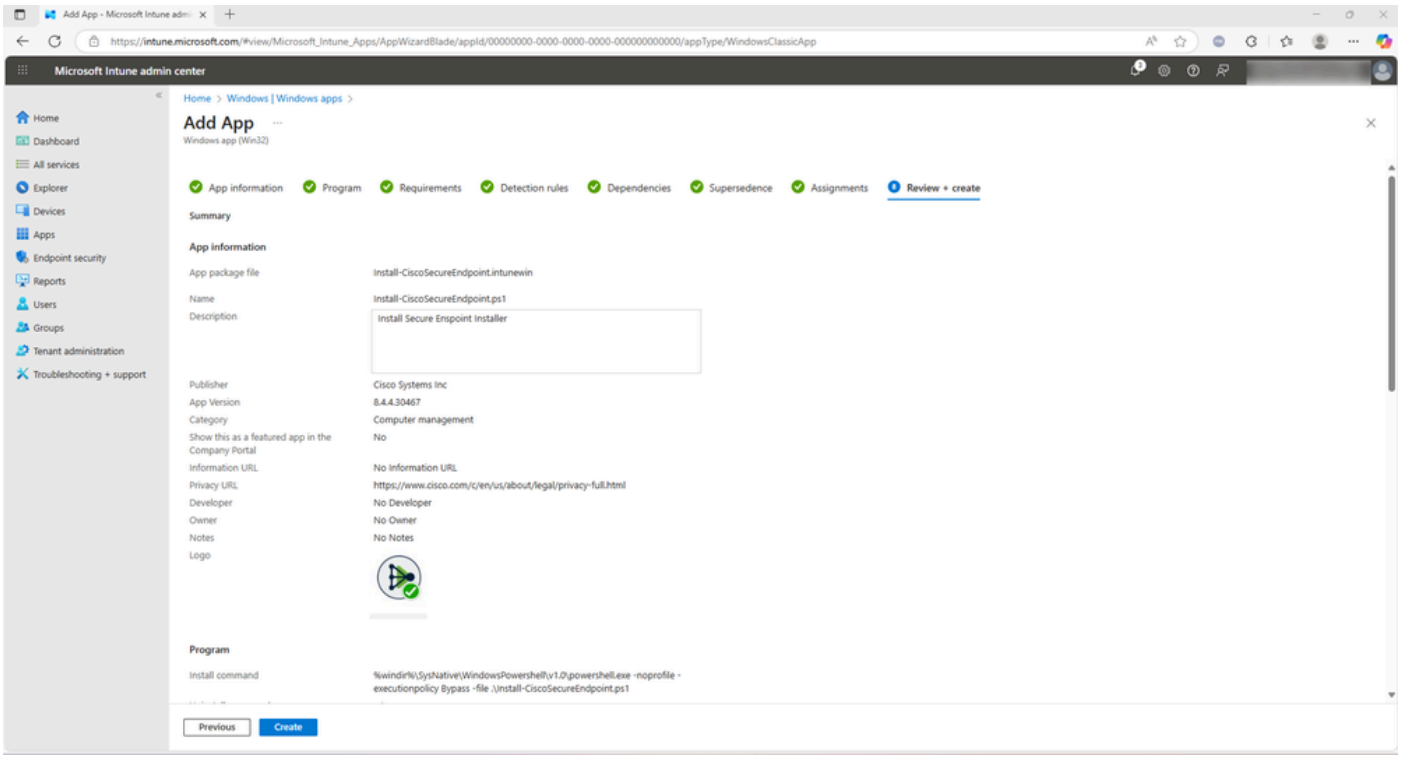
---

11. Cliquez sur Suivant 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.

---

12. (Les quelques onglets suivants sont facultatifs) Aucune dépendance ne doit être configurée ; affectez l'application au groupe requis et sélectionnez Vérifier + créer.



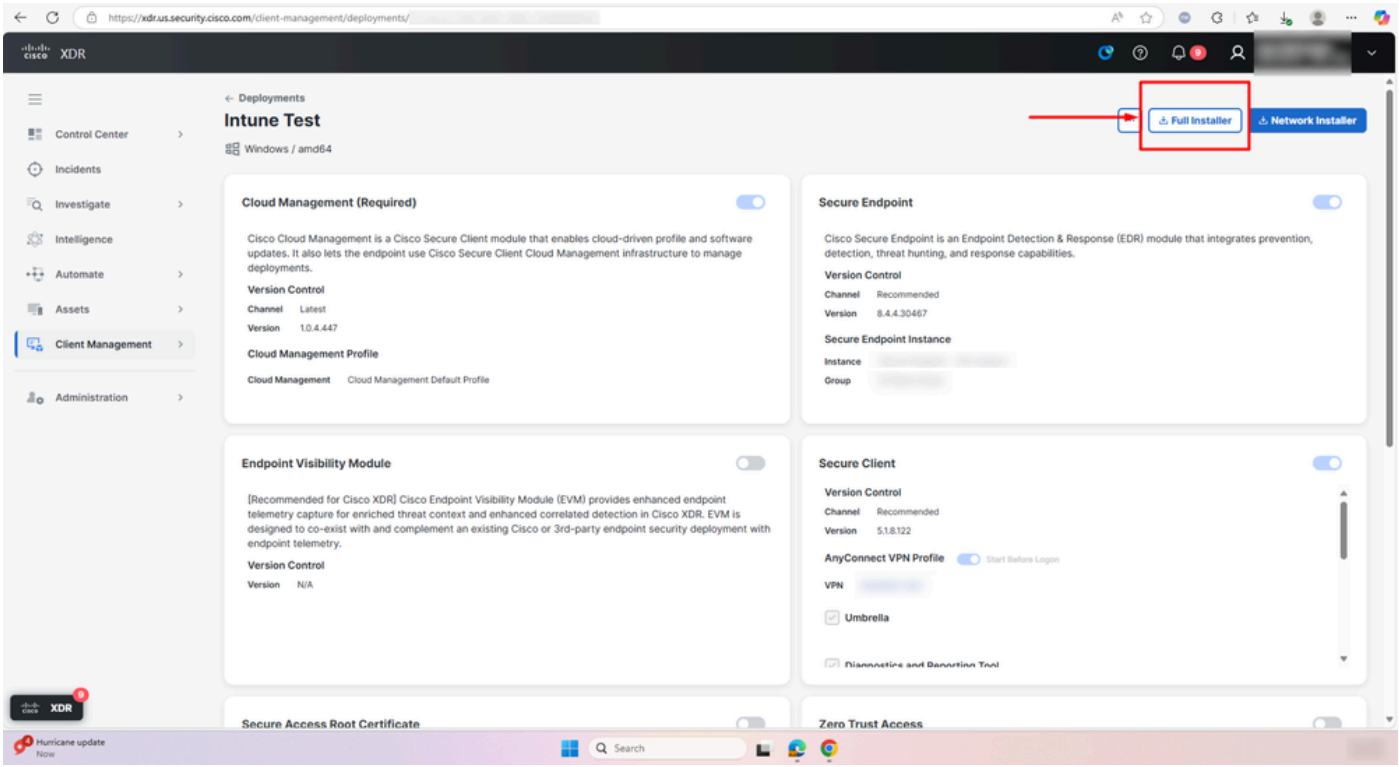
Déploiement sécurisé du client

Étape 1 : téléchargement du déploiement complet du client sécurisé Cisco

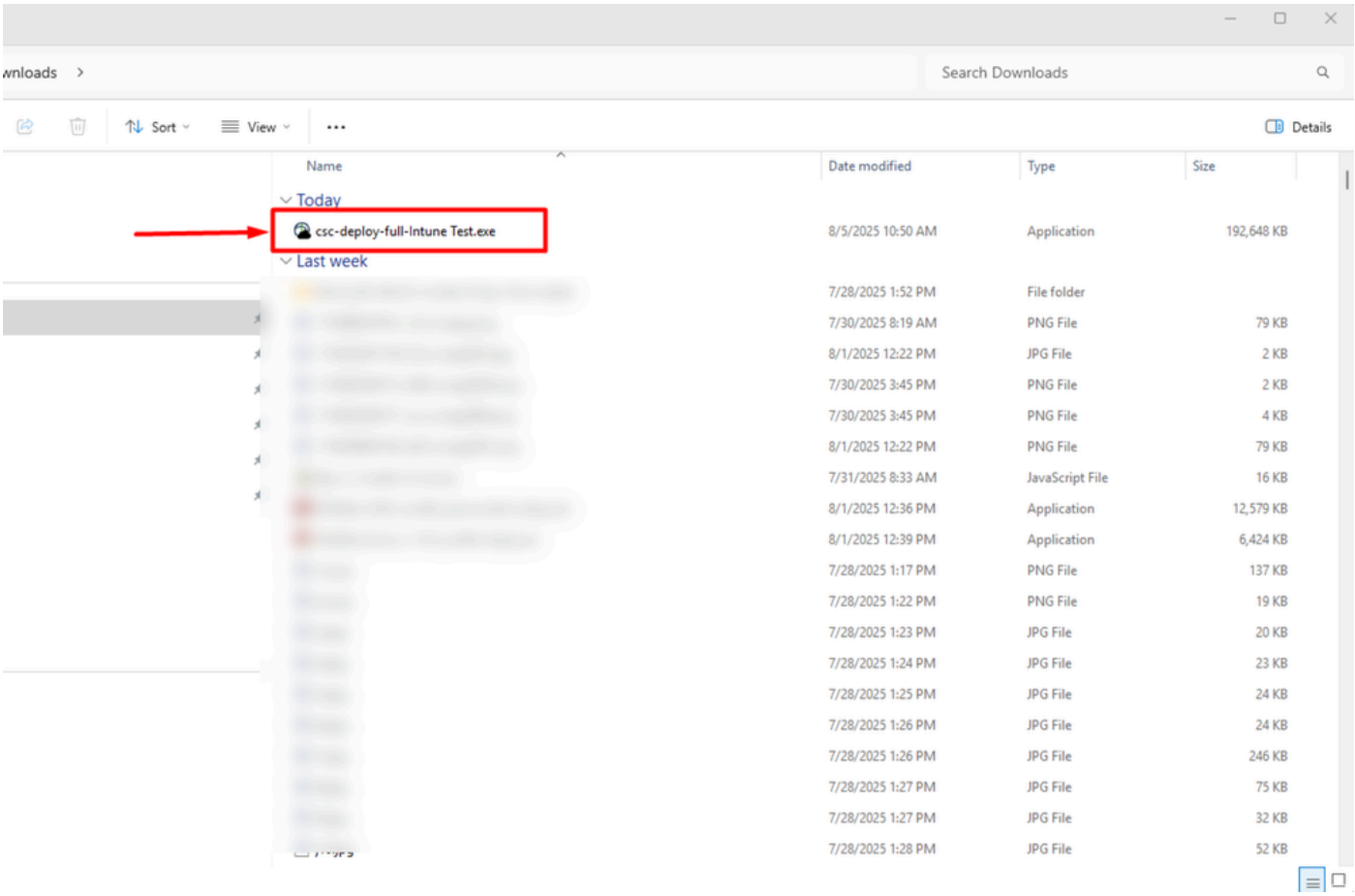
1. Connectez-vous à la console XDR ou Secure Client Cloud Management, selon la région.

---

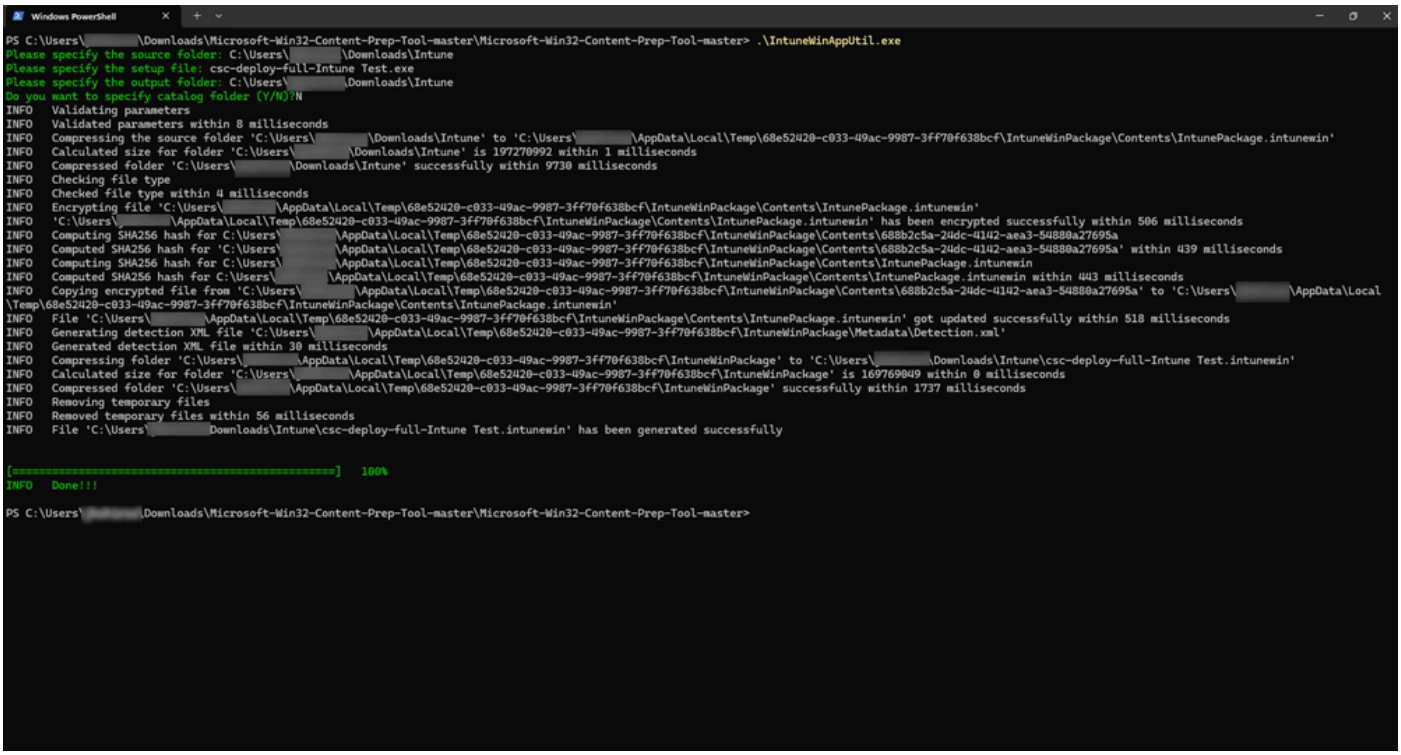
2. Créez un nouveau déploiement et sélectionnez Installation complète ou Installation réseau selon votre type de déploiement.



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

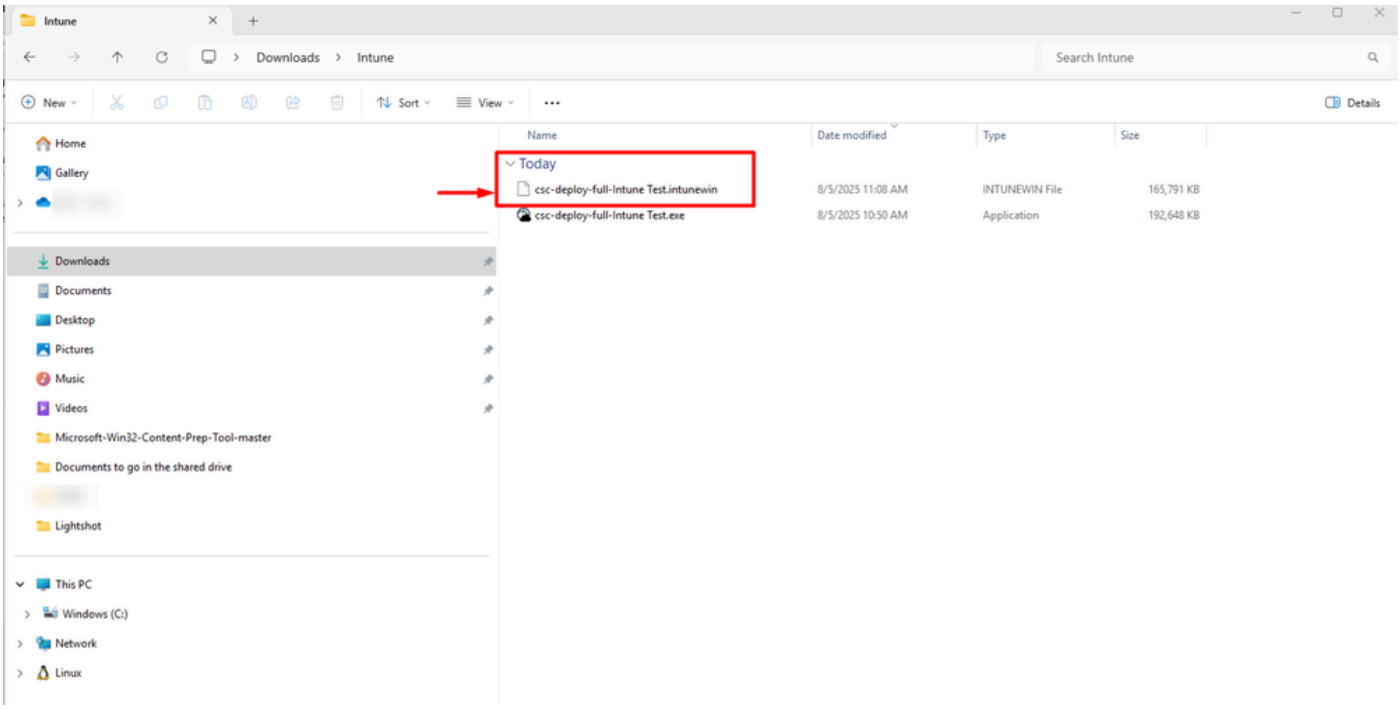


Étape 2. préparation du fichier Intune, même procédure que pour l’étape 2 : Le fichier csc-deploy-full-Intune Test.intunewin est créé



---

1. Les étapes précédentes de la capture d'écran aboutissent à la création d'un fichier csc-deploy-full-Intune Test.intunewin.



Étape 3. Téléchargez le fichier csc-deploy-full-intune Test.intunewin de l'étape 1 vers Microsoft Intune Admin Center

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

⚠ Mise en garde : Ce script d'installation doit être combiné avec l'installateur utilisant Intune Converter et le nom exact du script PS référencé dans la ligne de commande mentionnée à l'étape 3 de ce guide et placé dans Intune sous :

Ajouter une application > Programme > Commande Installer.

✎ Remarque : Les scripts de la section suivante sont des exemples pratiques de démonstrations utilisées dans les environnements de travaux pratiques pour créer ce guide. Vous pouvez les utiliser tels quels après les tests appropriés ou les modifier comme vous le souhaitez.

Script Install-CiscoSecureEndpoint.ps1

```
[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
}
```

Install - Script CiscoXDRDeployment.ps1

```
$exeName = <Your_XDR_Deployment.exe>
$exePath = Join-Path -Path $PSScriptRoot -ChildPath $exeName

if (-not (Test-Path $exePath)) {
    Write-Error "Executable not found: $exePath"
    exit 1
}

# Use silent mode - the most commonly documented switch for Cisco XDR / Secure Client installers
$arguments = "-q"   # or try "--quiet" if -q fails in your specific build

try {
    $process = Start-Process -FilePath $exePath -ArgumentList $arguments -NoNewWindow -Wait -PassThru

    if ($process.ExitCode -eq 0) {
        Write-Output "Cisco XDR installation completed successfully (exit code 0)."
        exit 0
    } else {
        Write-Error "Installation failed with exit code: $($process.ExitCode)"
        exit $process.ExitCode
    }
}
catch {
    Write-Error "Exception during installation: $_"
    exit 1
}
```

Script Confirm-CSEInstall.ps1



Conseil : Facultatif: Vous pouvez utiliser les règles de détection configurées manuellement dans Intune Management Portal.

```
[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 th
    the standard error (STDERR) stream, and the exit code. If the script exits with a nonzero value, the
    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
```



Remarque : Les scripts précédents sont uniquement à des fins pédagogiques et ne sont pas pris en charge par le TAC Cisco. Chaque environnement peut varier en fonction des règles ou des politiques et il est nécessaire d'effectuer des tests appropriés. Le dépannage des outils de déploiement tiers est considéré comme un effort et doit commencer par l'examen des journaux Intune à la fois sur le portail ou sur la station gérée.

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.