

通过MS Intune调配安全客户端Umbrella漫游安全

目录

[简介](#)

[前提条件](#)

[将安全客户端MSI文件转换为.intunewin格式](#)

[在Intune门户中上传和配置安全客户端核心VPN .intunewin](#)

[在Intune门户中上传和配置安全客户端Umbrella模块.intunewin](#)

[确认](#)

简介

本文档介绍如何使用MS Intune调配安全客户端Umbrella漫游安全模块。

前提条件

- 访问Umbrella控制面板
- 访问MS Intune门户
- 安全客户端Umbrella模块配置文件orginfo.json
- 所需版本的安全客户端预部署包
- [Microsoft Win32内容准备工具](#)

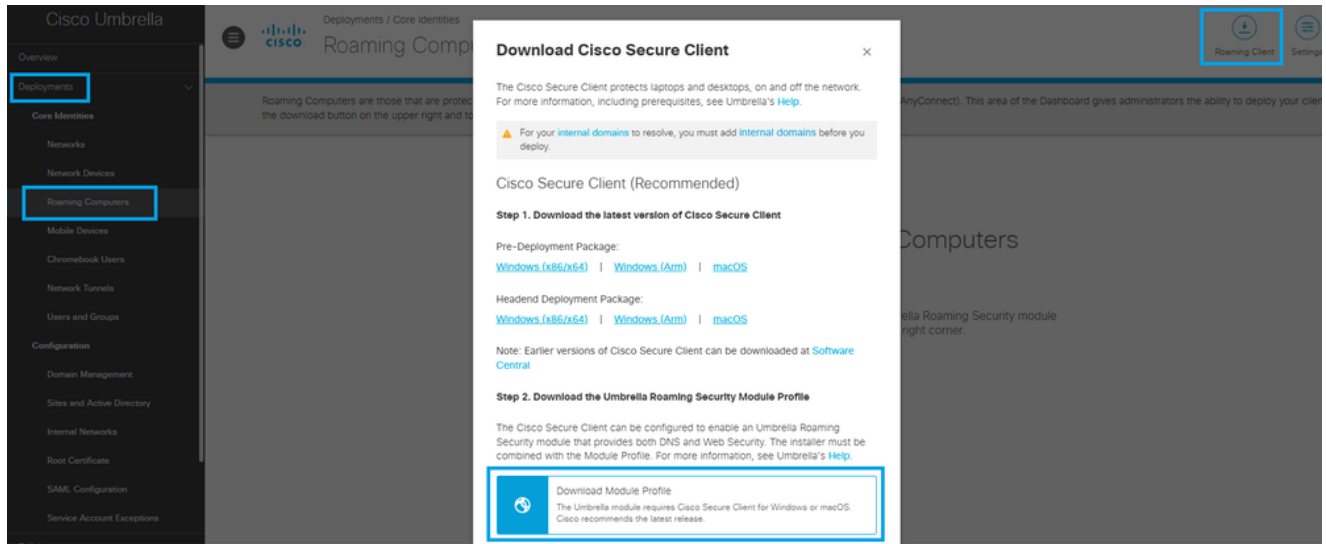
本指南使用Windows应用(Win32)方法。将和文件cisco-secure-client-win-5.0.05040-core-vpn-predeploy-k9.msicisco-secure-client-win-5.0.05040-umbrella-predeploy-k9.msi，转换为格式.intunewin。



警告：Windows Autopilot与此进程不兼容。使用标准Intune组或设备分配VPN和Umbrella应用程序。

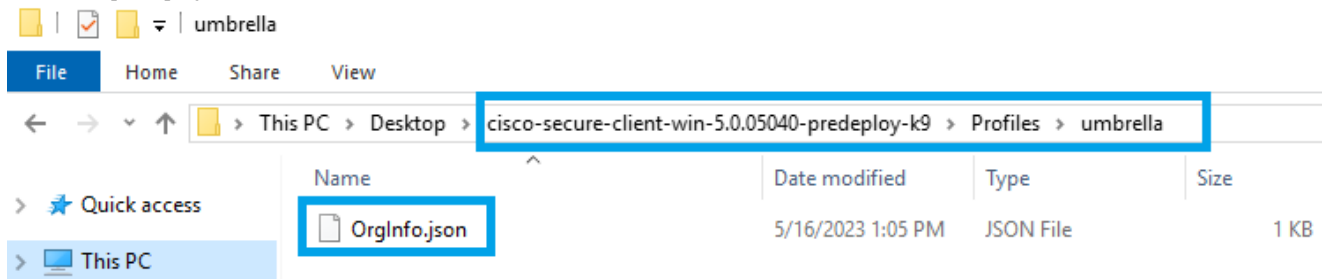
将安全客户端MSI文件转换为.intunewin格式

1. `orginfo.json` 访问Umbrella Dashboard并从部署(Deployments)>漫游客户端(Roaming Clients)>下载(Download)>下载模块配置文件(Download Module Profile)下载安全客户端Umbrella模块配置文件(Secure Client Umbrella Module Profile)。



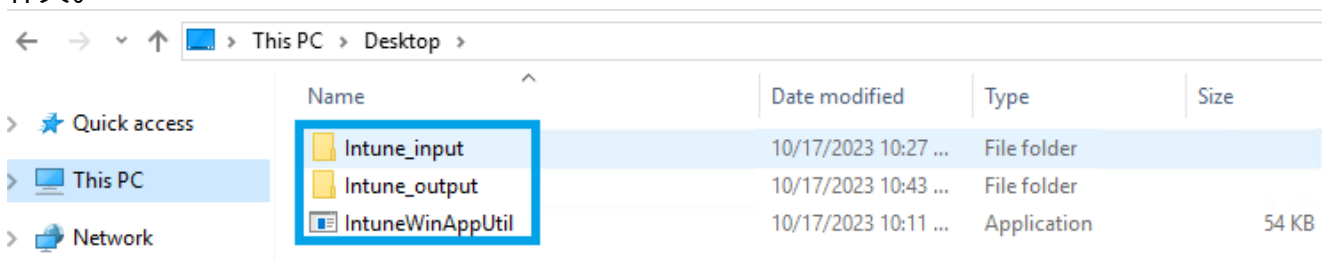
20109693592980

2. 解压安全客户端预部署软件包后，将Umbrella配置文件放orginfo.json在目\cisco-secure-client-win-5.0.05040-predeploy-k9\Profiles\umbrella录中。



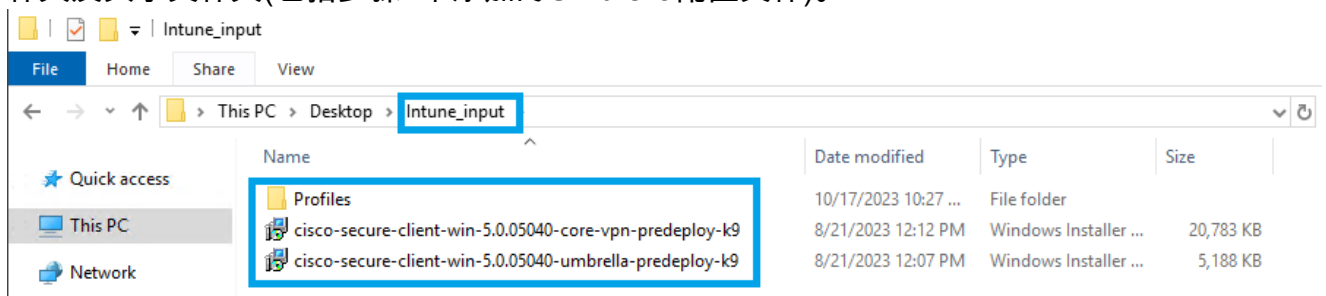
20109945693716

3. 下载[Microsoft Win32内容准备工具](#)。
4. 创建文件夹并添加IntuneWinAppUtilapplication。此外，在您的计算机上创建Input和Output文件夹。



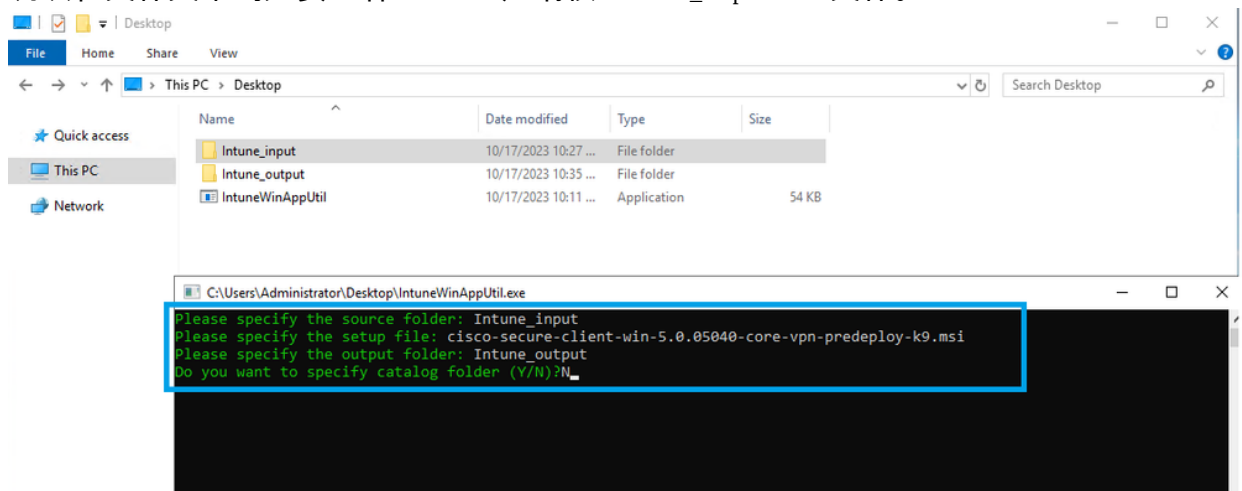
20115546066964

5. 在文Intune_input文件夹中，添加安全客户端VPN核心和Umbrella MSI文件。另外，复制Profiles文件夹及其子文件夹(包括步骤2中添加的Umbrella配置文件)。

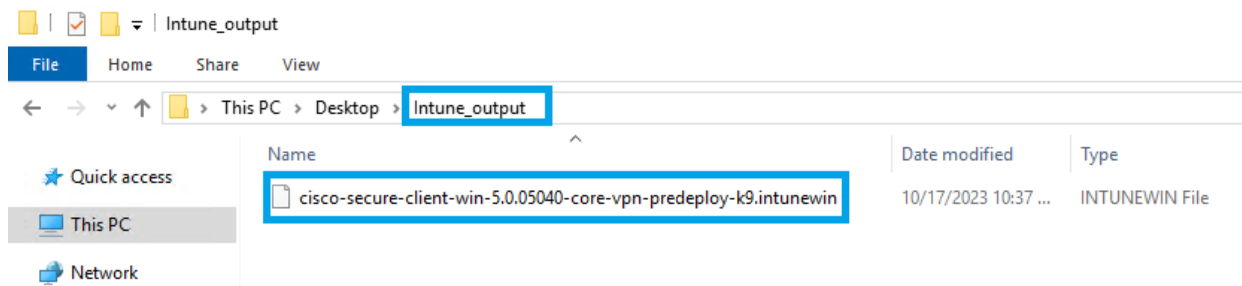


20110243105684

6. 打开IntuneWinAppUtil.exe application并指定Intune_input为源文件夹、安全客户端核心VPN MSI作为源设置文件Intune_output和输出文件夹。这会生成安全客户端核心VPN.intunewin文件。
- 确认在文件夹中创建安全客.intunewin户端核心Intune_outputVPN文件。

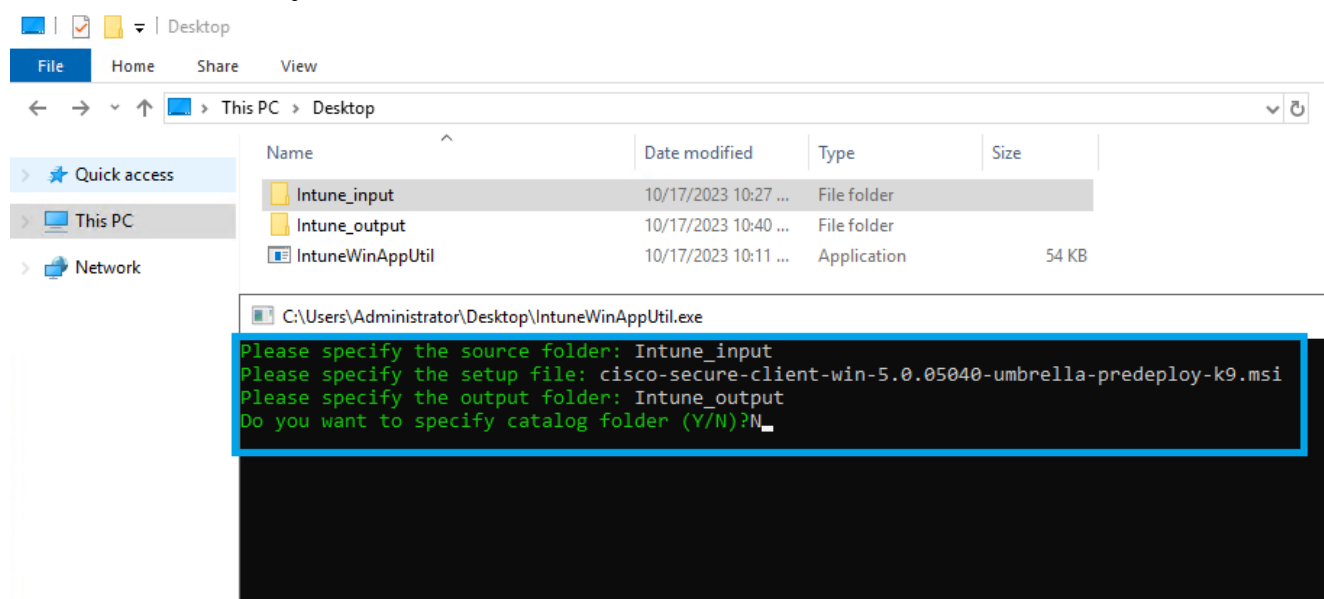


20110510904980



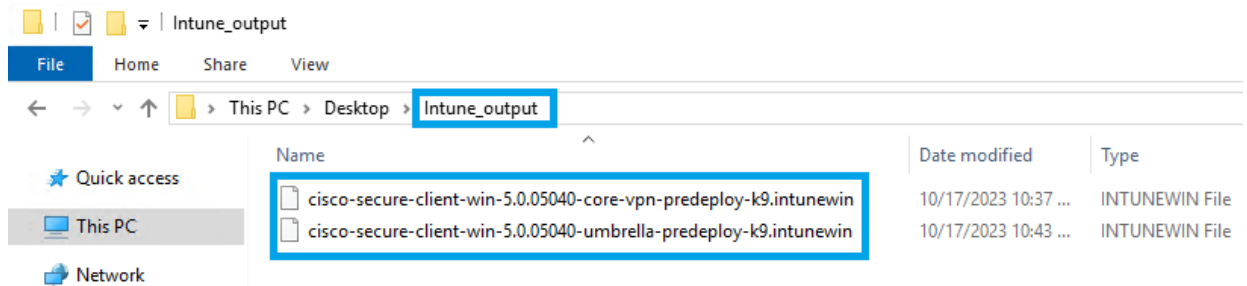
20110579164820

7. 对安全客户端Umbrella模块MSI文件重复第6步。嵌入的Umbrella配置文件创建安全客户端.intunewinUmbrellafile。



20110729750676

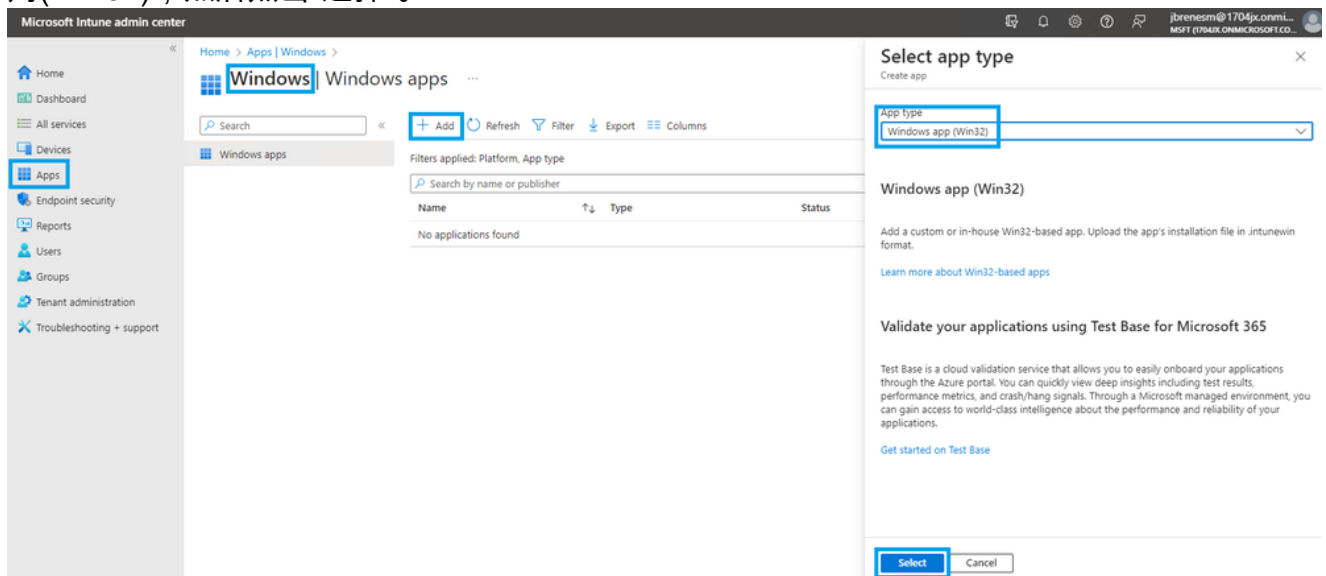
- 确认在文件夹中创建安全 .intunewin 客户端 Intune_outputUmbrellafile。



20110832832020

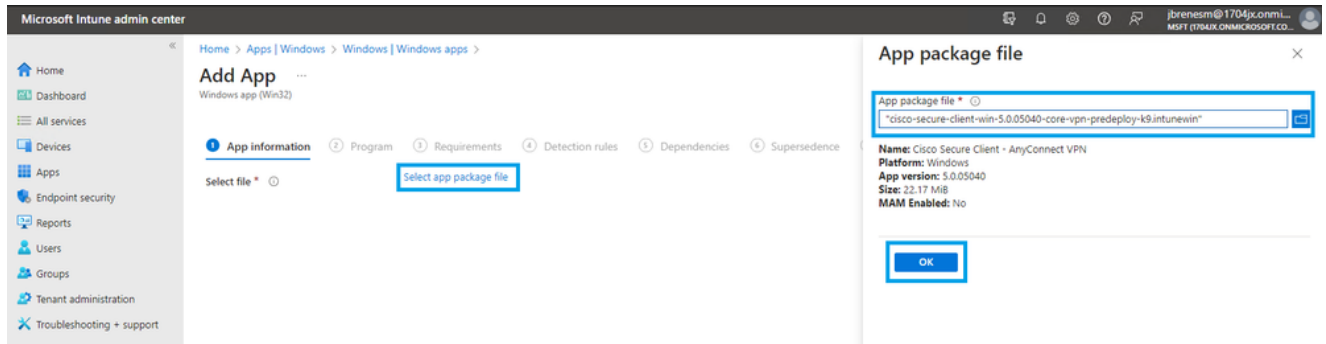
在Intune门户中上传和配置安全客户端核心VPN .intunewin

1. 在Home > Apps > Windows下访问MS Intune门户。对于“选择”应用类型，请选择Windows应用(Win32)，然后点击“选择”。



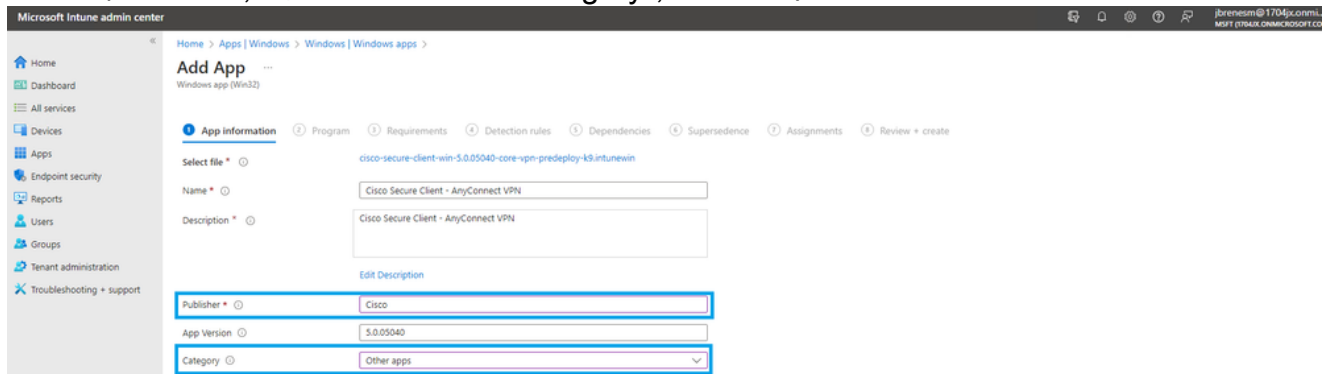
20112513277204

2. 点击Select app package file，上传Secure Client Core VPN文.intunewin件，然后点击OK。



20112597413396

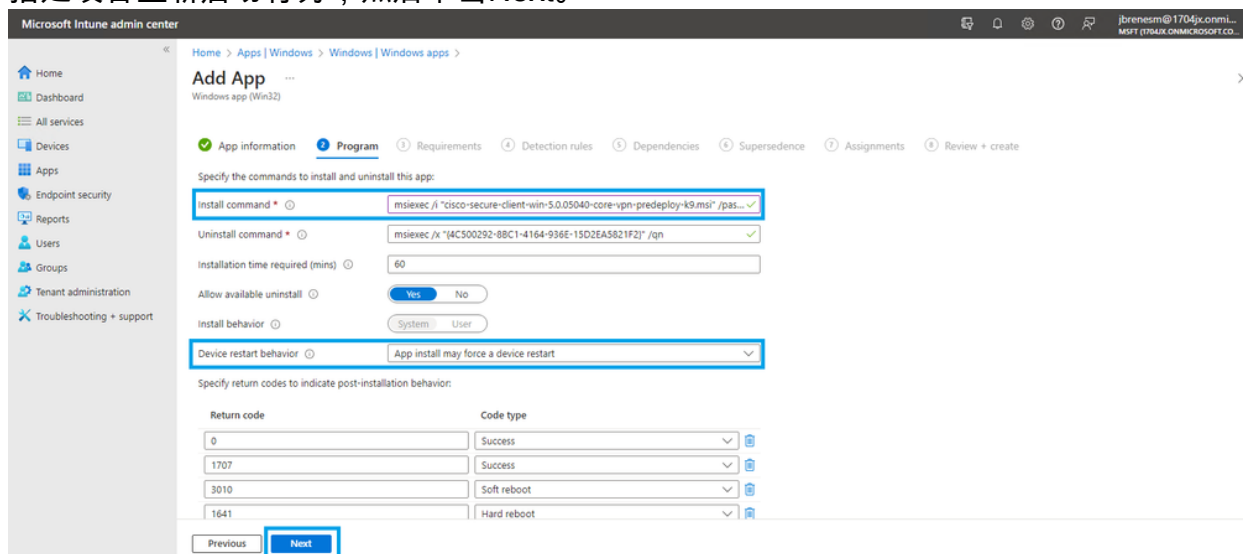
3. 指定所需的信息，例如PublisherandCategory，然后单击Next。



20112682982036

4. 输入安装命令参数。使用默认设置或参阅《安全客户端管理指南》获取支持的参数。例如，要使用被动模式并禁用VPN模块（因此仅Umbrella模块显示在UI中），然后登录vpninstall.log：

- `msiexec /i "cisco-secure-client-win-5.0.05040-core-vpn-predeploy-k9.msi" /passive PRE_DEPLOY_DISABLE_VPN=1 /lvx*vpninstall.log`
- 指定设备重新启动行为，然后单击Next。



20112813814036

5. 为需要安全客户端核心VPN的设备指定OS架构和最低操作系统版本。还可以设置其他要求。

The screenshot shows the 'Add App' page in the Microsoft Intune admin center, specifically the 'Requirements' tab. The page is for adding a 'Windows app (Win32)'. The 'Requirements' tab is selected, and the 'Specify the requirements that devices must meet before the app is installed' section is visible. The 'Operating system architecture' is set to '64-bit' and the 'Minimum operating system' is set to 'Windows 10 1607'. There are input fields for 'Disk space required (MB)', 'Physical memory required (MB)', 'Minimum number of logical processors required', and 'Minimum CPU speed required (MHz)'. Below these is a section for 'Configure additional requirement rules' with a table for 'Type' and 'Path/Script'. The table currently has one row with 'No requirements are specified.' and an '+ Add' button. At the bottom, there are 'Previous' and 'Next' buttons.

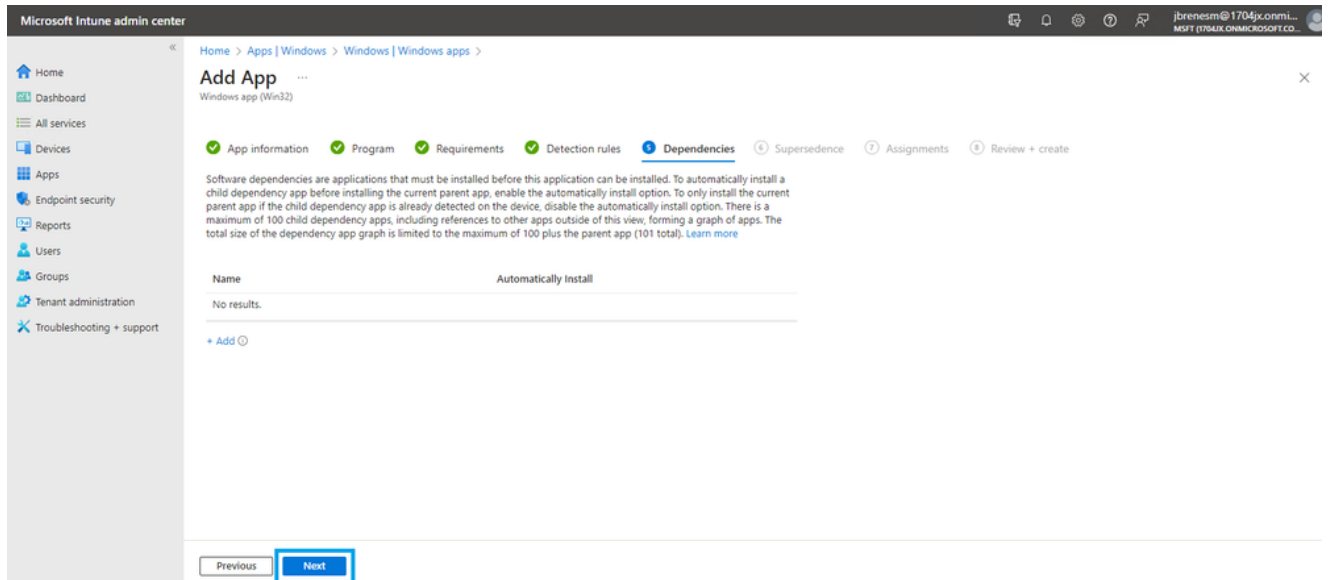
20112918066836

6. 或者，配置检测规则以检查安全客户端核心VPN是否存在。在本示例中，将任何安全客户端.msi核心VPN版本的检测规则类型设置为。

The screenshot shows the 'Add App' page in the Microsoft Intune admin center, specifically the 'Detection rules' tab. The page is for adding a 'Windows app (Win32)'. The 'Detection rules' tab is selected, and the 'Configure app specific rules used to detect the presence of the app.' section is visible. The 'Rules format' is set to 'Manually configure detection rules'. Below this is a table for 'Type' and 'Path/Code'. The table has one row with 'MSI' and '(4C500292-88C1-4164-936E-15D2EA5821F2)'. There is an '+ Add' button. To the right, a 'Detection rule' dialog box is open, showing 'Rule type' set to 'MSI', 'MSI product code' set to '(4C500292-88C1-4164-936E-15D2EA5821F2)', and 'MSI product version check' set to 'No'. At the bottom, there are 'Previous', 'Next', and 'OK' buttons.

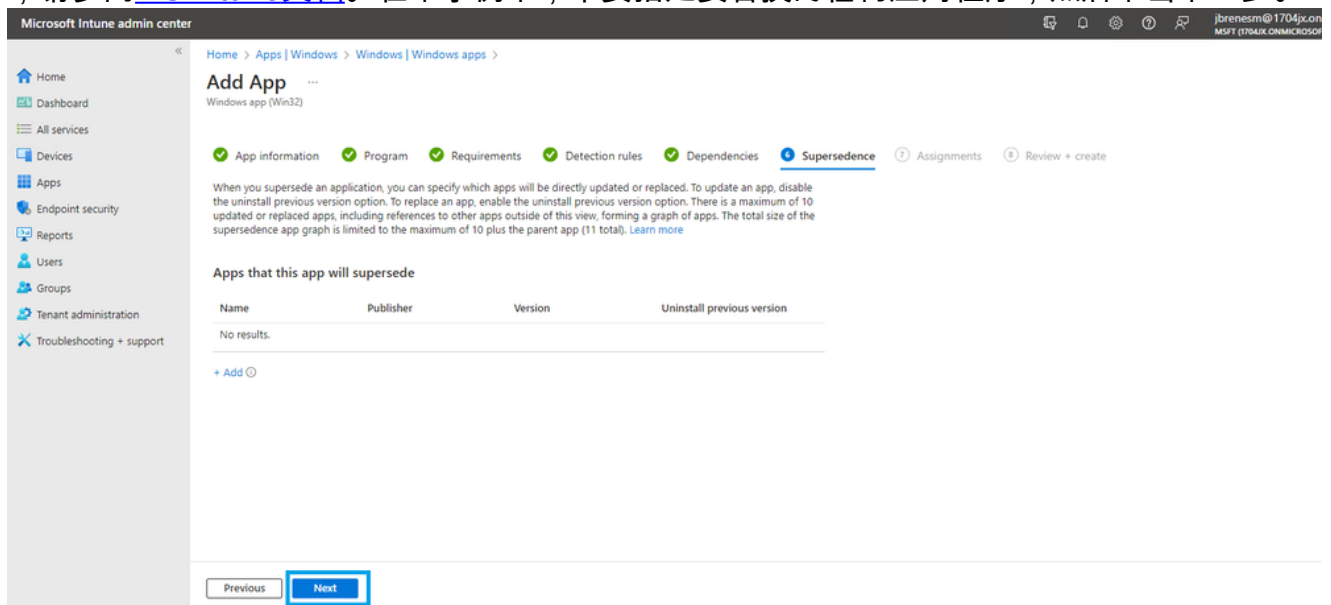
20113069368724

7. 单击Next，跳过Secure Client Core VPN的Dependencies部分。



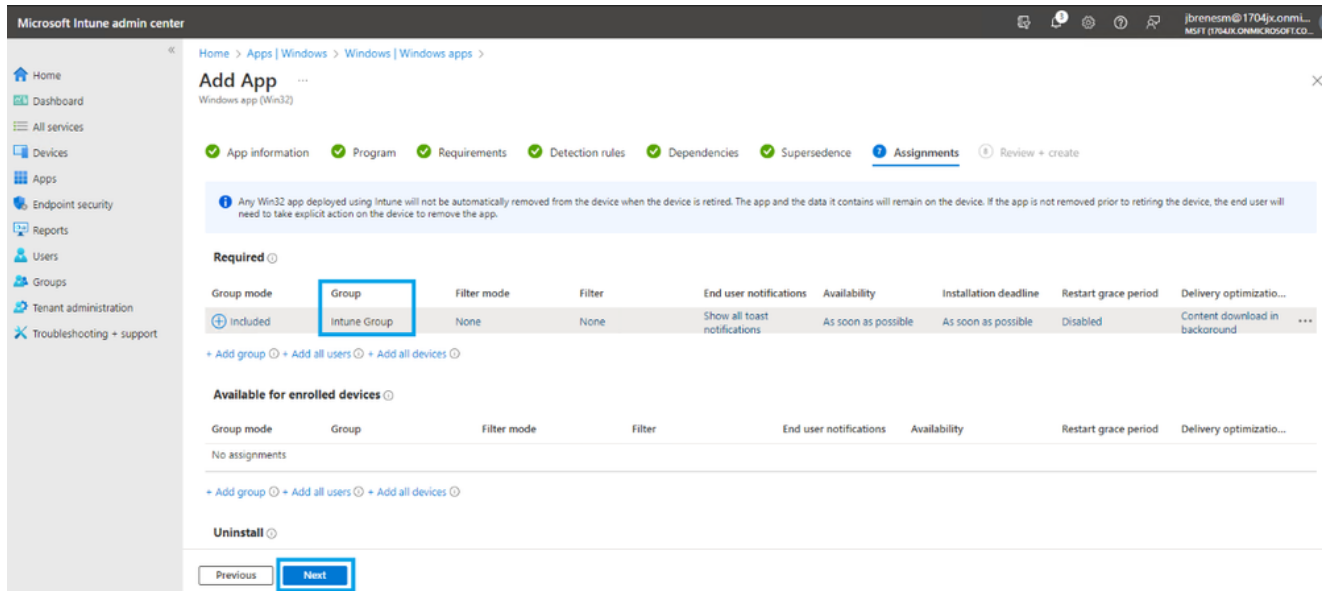
20113130954388

8. 或者，配置Substances以更新或替换现有应用程序。这仅适用于Win32应用。有关详细信息，请参阅[MS Intune文档](#)。在本示例中，不要指定要替换的任何应用程序，然后单击下一步。



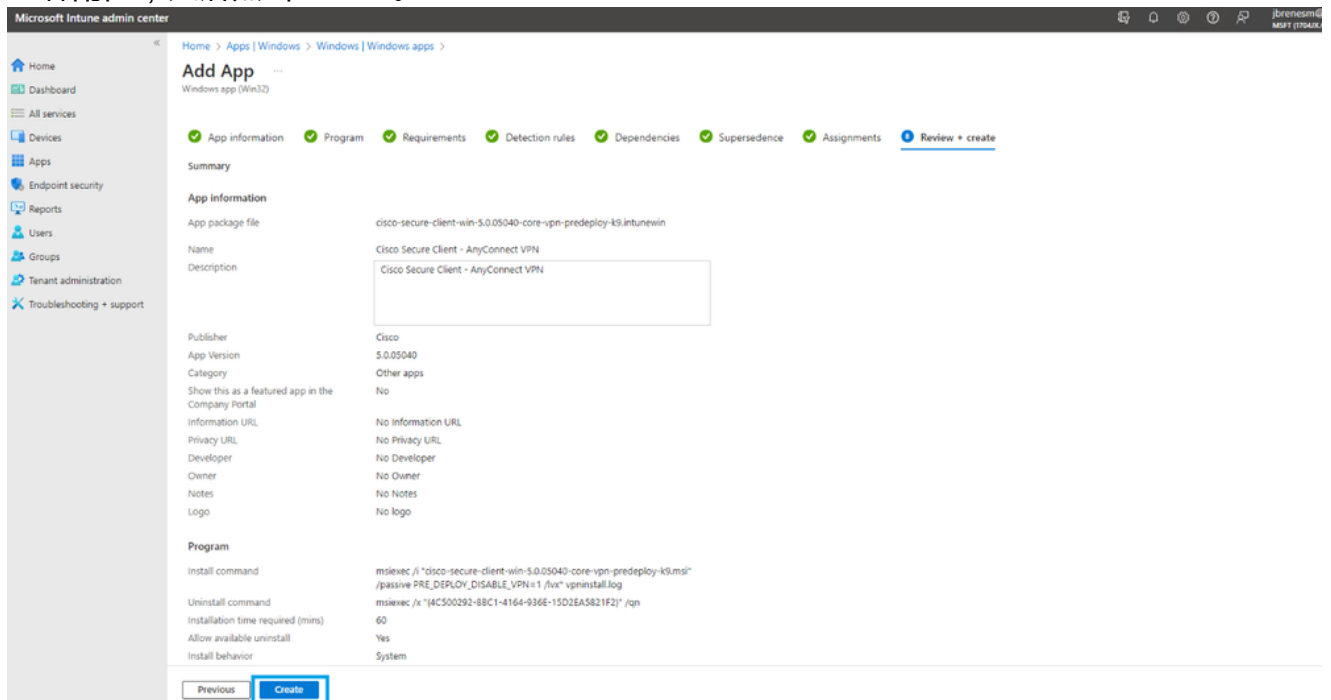
20113224899220

9. 为需要安装安全客户端VPN核心的组或设备指定分配。点击Nextator assignment。



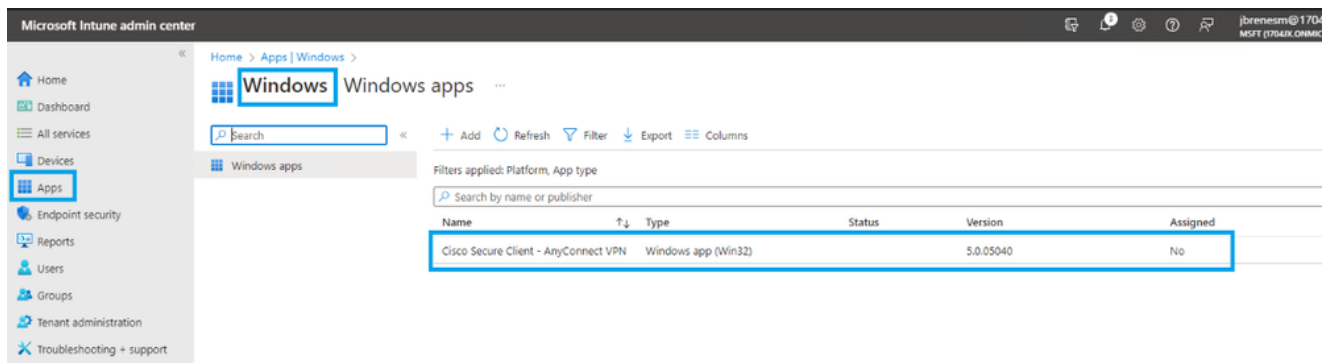
20114450720404

10. 查看配置，然后点击Create。



20113349733652

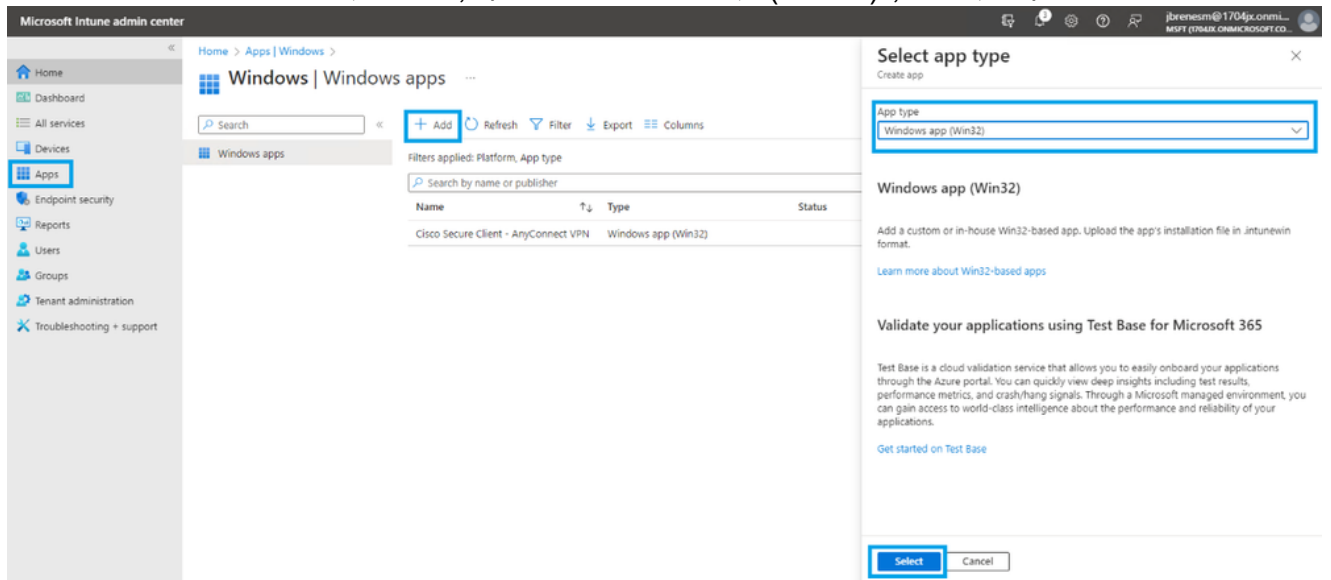
11. 创建后，请返回MS Intune门户中的Home > Apps > Windows以查看新创建的AnyConnect核心VPN Win32应用。



20113372533652

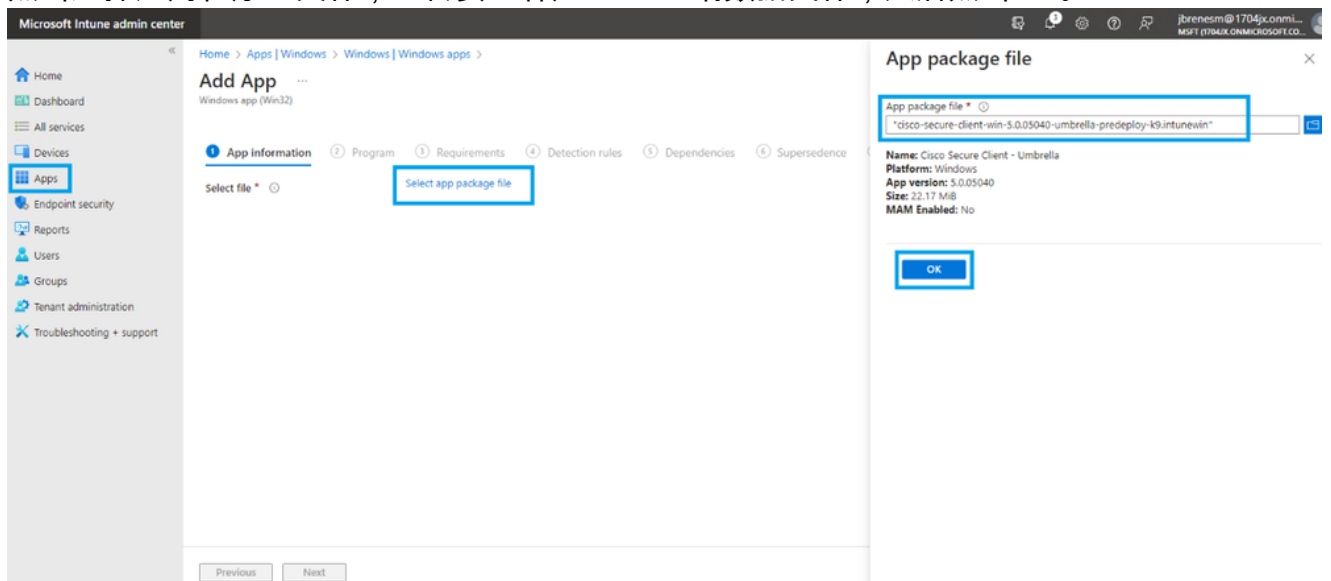
在Intune门户中上传和配置安全客户端Umbrella模块.intunewin

1. 对Secure Client Umbrella Module重复此过程。在MS Intune门户中，转至Home > Apps > Windows。对于“选择”应用类型，请选择Windows应用(Win32)，然后点击“选择”。



20113516023828

2. 点击选择应用程序包文件，上传安全客户.intunewin端数据文件，然后点击OK。



20113626878740

3. 指定所需的信息，例如Publisher和Category，然后单击Next。

Microsoft Intune admin center

Home > Apps > Windows > Windows apps >

Add App

Windows app (Win32)

1 App information 2 Program 3 Requirements 4 Detection rules 5 Dependencies 6 Supersede 7 Assignments 8 Review + create

Select file *

Name *

Description *

[Edit Description](#)

Publisher *

App Version

Category

Show this as a featured app in the Company Portal ☐ ☒

Information URL

Privacy URL

[Previous](#) [Next](#)

20113677228180

4. 输入安装命令参数。使用默认设置或参阅《安全客户端管理指南》获取支持的参数。例如，要使用被动模式并记录到umbrellainstall.log：

- `msiexec /i "cisco-secure-client-win-5.0.05040-umbrella-predeploy-k9.msi" /passive /lvx* umbrellainstall.log`
- 指定设备重新启动行为，然后单击Next。

Microsoft Intune admin center

Home > Apps > Windows > Windows apps >

Add App

Windows app (Win32)

1 App information 2 Program 3 Requirements 4 Detection rules 5 Dependencies 6 Supersede 7 Assignments 8 Review + create

Specify the commands to install and uninstall this app:

Install command *

Uninstall command *

Installation time required (mins)

Allow available uninstall ☒ ☐

Install behavior ☐ ☒

Device restart behavior

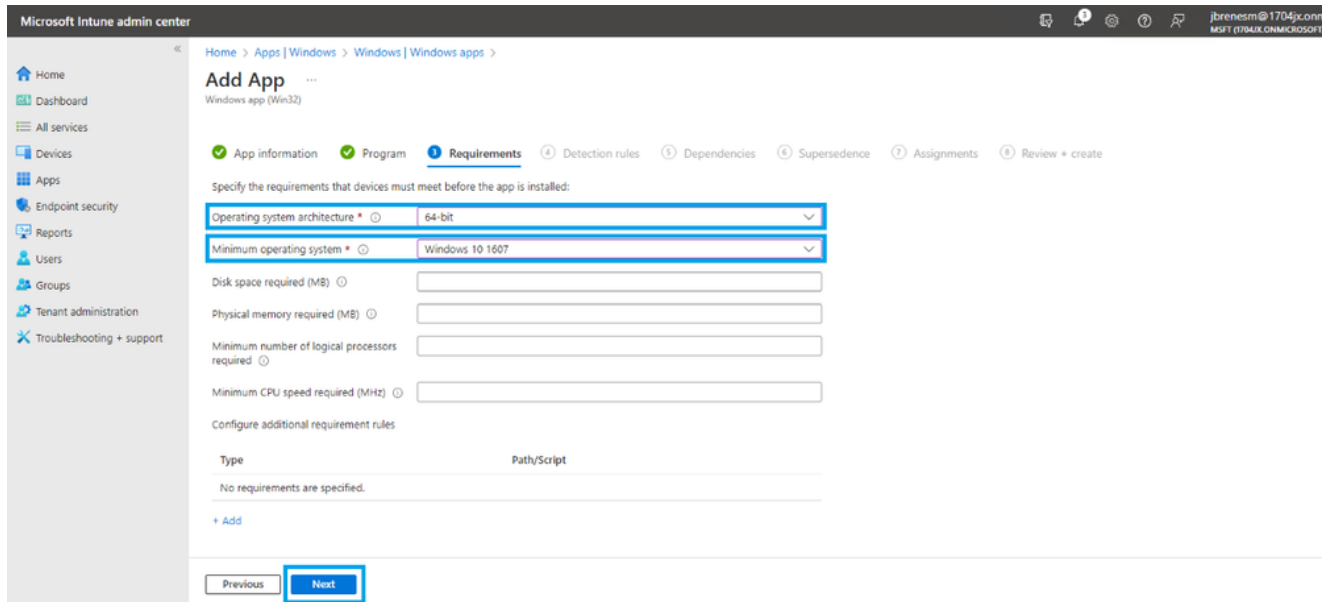
Specify return codes to indicate post-installation behavior:

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

[Previous](#) [Next](#)

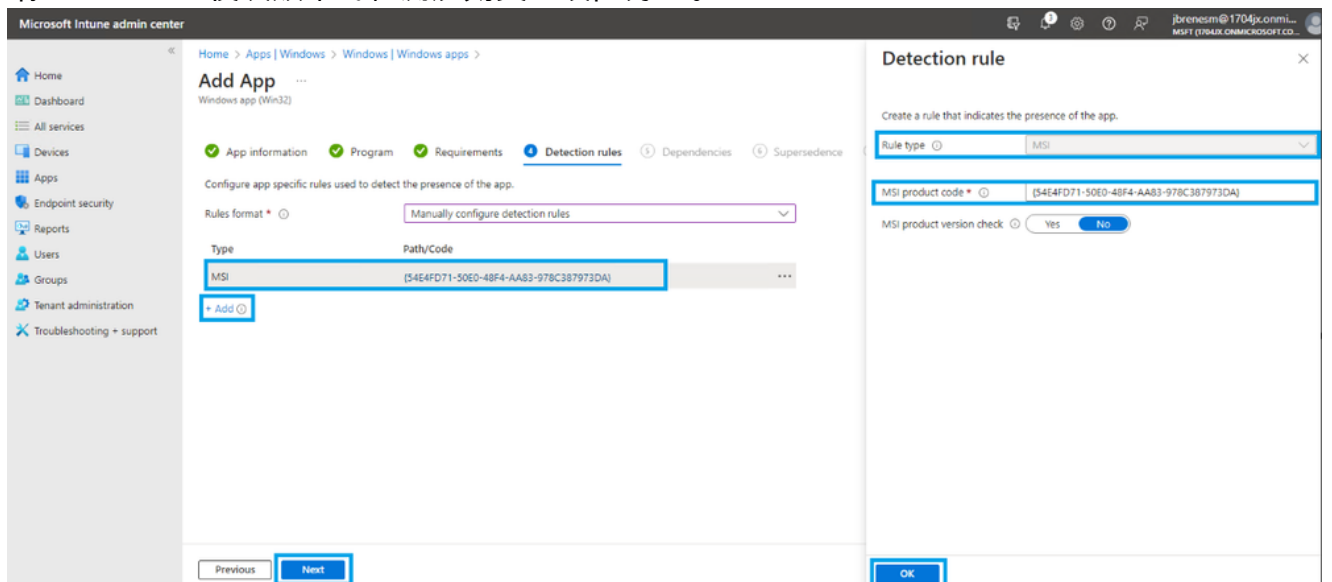
20113856190740

5. 为需要安全客户端Umbrella模块的设备指定OS architecture和最低操作系统版本。还可以设置其他要求。



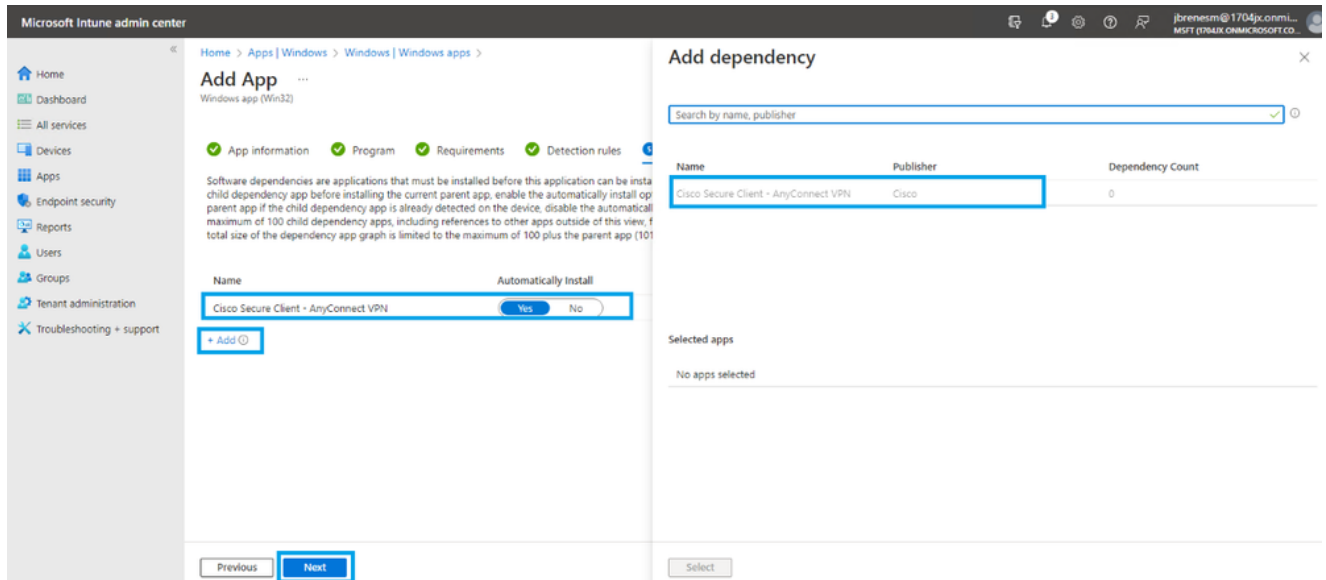
20113968568980

6. 或者，配置检测规则以检查安全客户端Umbrella模块是否存在。在本示例中，将任何安全客户端Umbrella.msi模块版本的检测规则类型设置为as。



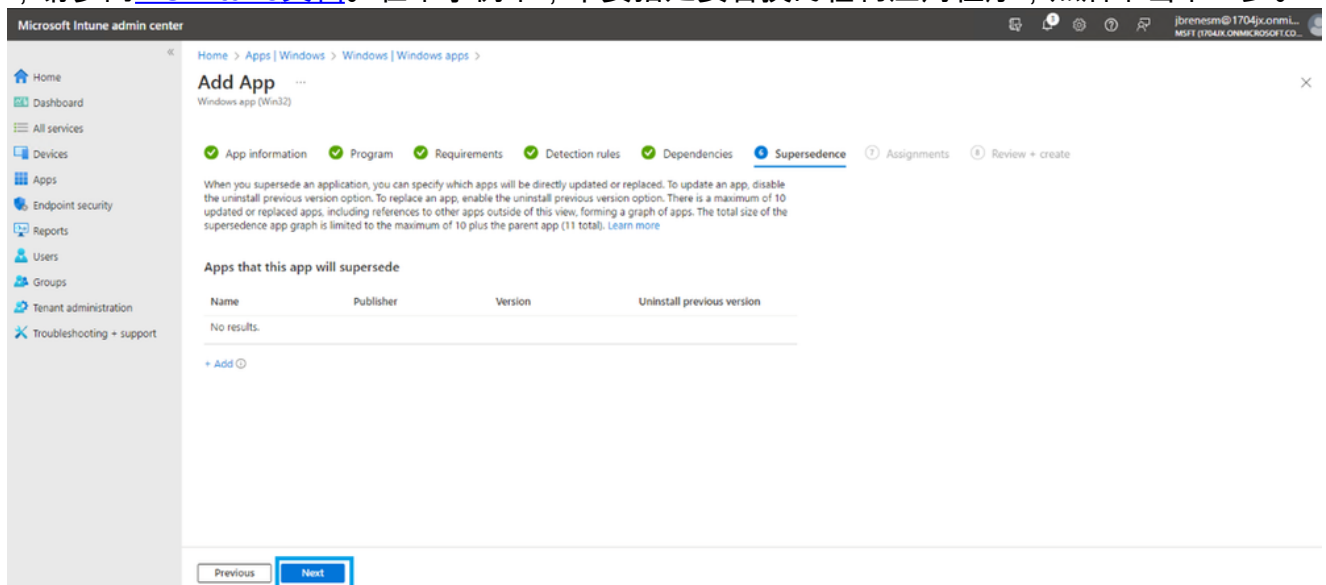
20114138920724

7. 在Dependencies部分中，指定Secure Client Core VPN模块并setAutomatically Installto Yes。如果未安装安全客户端核心VPN，则Intune会在安全客户端Umbrella模块之前安装它。点击Next。



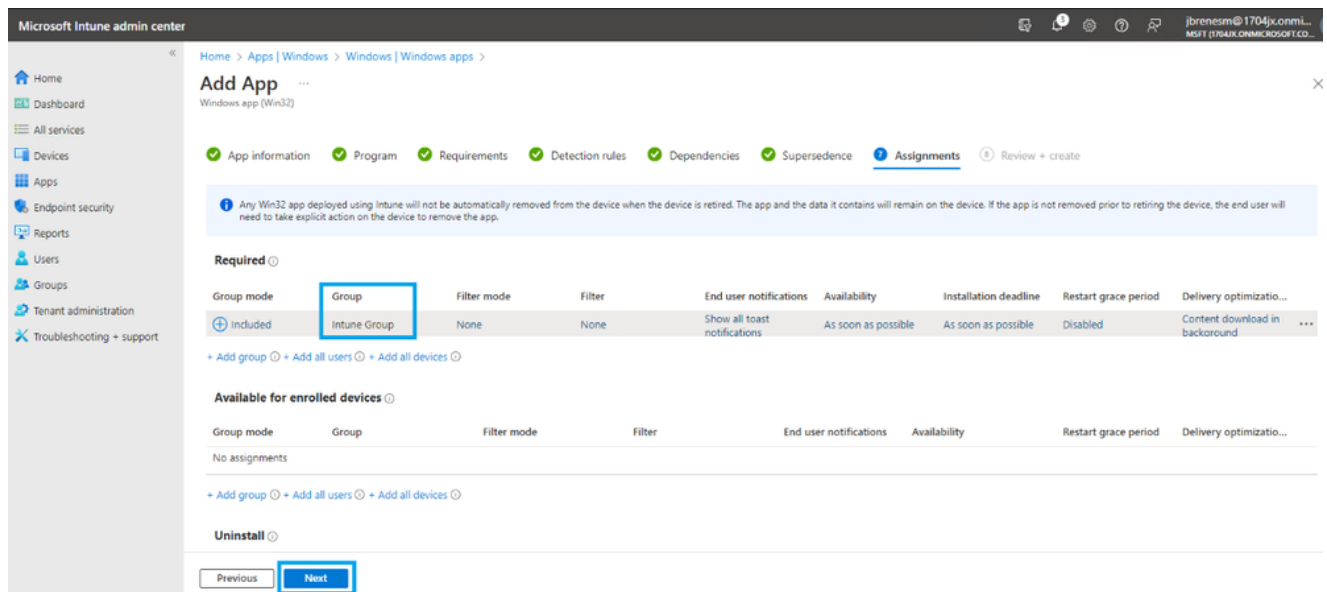
20114235246740

8. 或者，配置Substances以更新或替换现有应用程序。这仅适用于Win32应用。有关详细信息，请参阅[MS Intune文档](#)。在本示例中，不要指定要替换的任何应用程序，然后单击下一步。



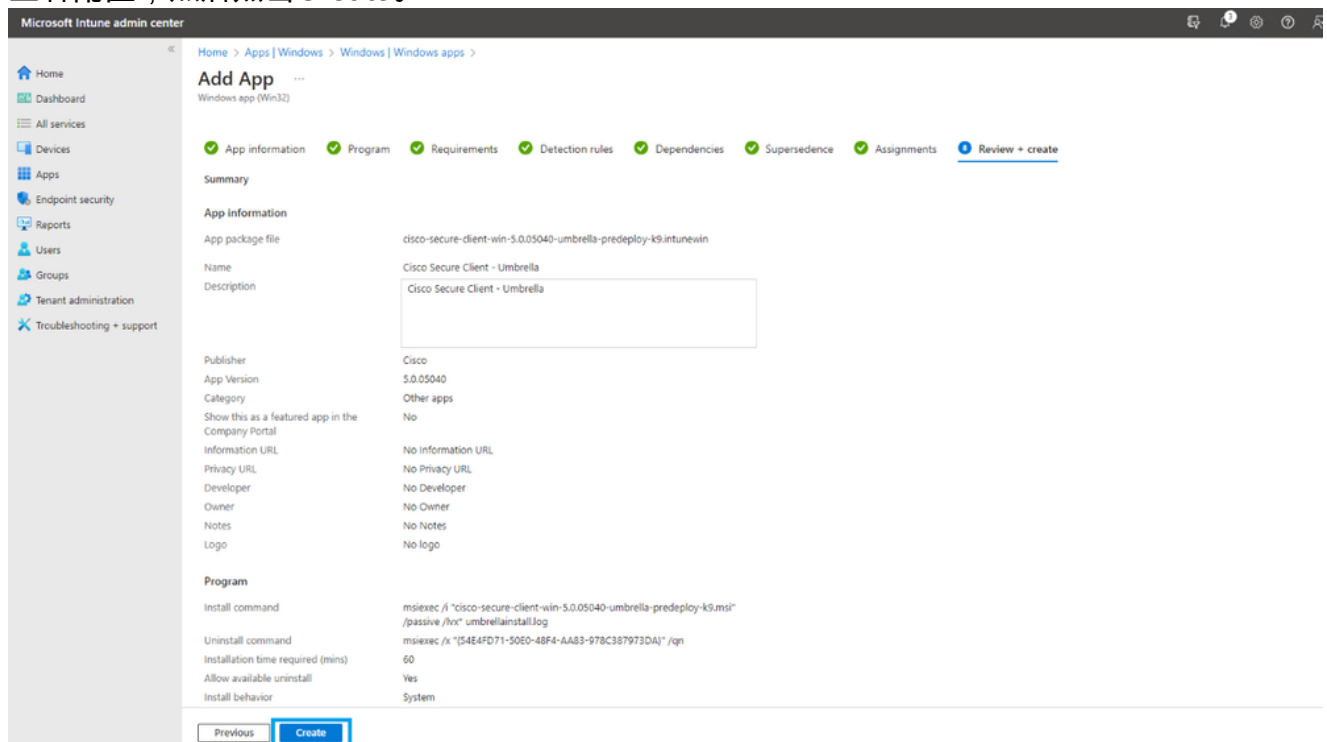
20114285889044

9. 为需要安全客户端Umbrella模块的组或用户指定分配。在本示例中，分配给名为“Intune组”的设备组。还可以设置其他参数。点击Next。



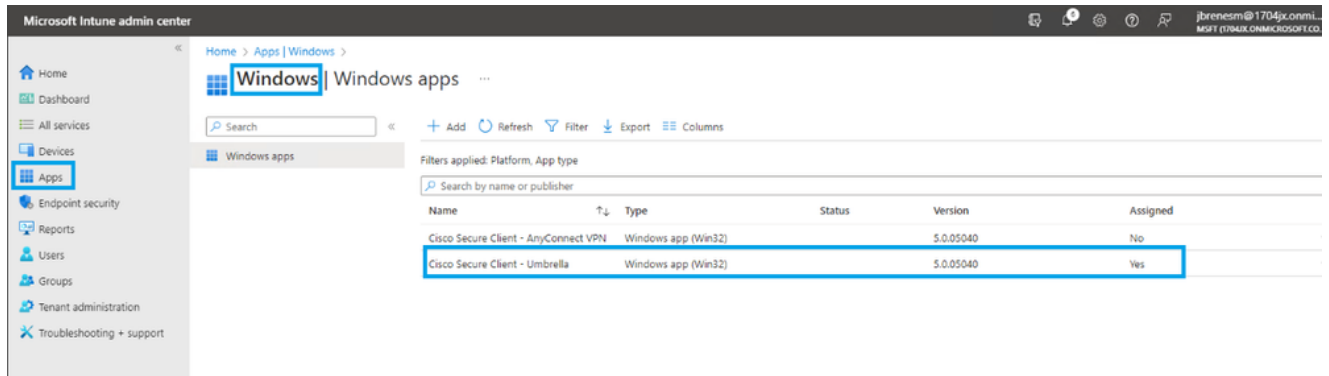
20114450720404

10. 查看配置，然后点击Create。



20114540608916

11. 创建后，请返回MS Intune门户Home > Apps > Windowsto，以验证是否已创建和分配安全客户端Umbrella模块Win32应用。等待部署到所选设备或用户。



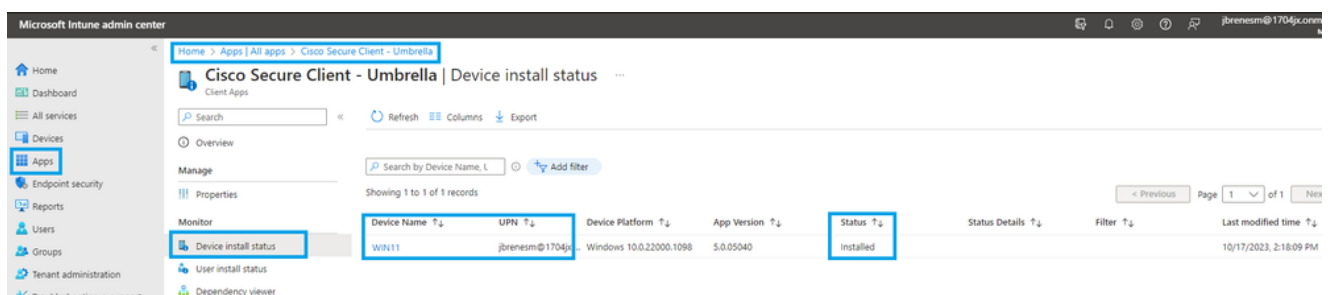
20114630676244

确认

1. 导航到主页>应用>所有应用，然后点击Cisco Secure Client - Umbrella，查看成功的安装。

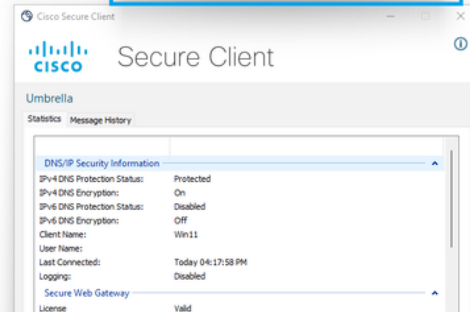
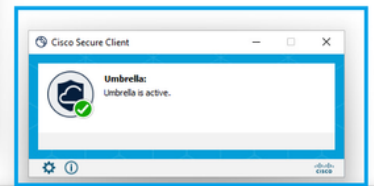
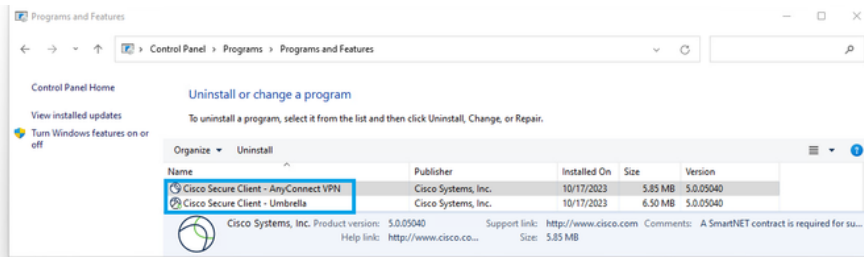


20117335896980



20117374902676

2. 在目标PC上，验证安全客户端核心VPN和Umbrella module均已安装，并且只有Umbrella module UI可见。



20117776753940

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。