Pathfinder Deployment Guide

Version 3.0, January 2022

Table of Content

Scope

Pathfinder is Sygnia's proprietary, light-weight agent, enabling (or supplementing) data collection and response on servers and workstations including binary and memory data collection, executing response operations and accounting for 3rd party collectors installation and configuration as part of a Velocity deployment.

This document covers Pathfinder's deployment guide in regard to both manual and automated installation, such as via SCCM/GPO.

If you have any additional questions regarding further deployment types or supported OS, please contact your Sygnia representative or support.

Prerequisites

- **Privileges**
  - Administrative privileges are required to install Pathfinder (in case Pathfinder wasn't run as such, operation shall be aborted)
- **Communication**
  - Communications between endpoints where Pathfinder is deployed and Velocity over port 443 needs to be permitted
  - Disable SSL inspection on above traffic (Velocity and pathfinder leverage pinned certificate to authenticate and communicate securely)
- **Available disk space:** 1GB (in order to allow Pathfinder to execute operations)

Supported OS versions

Windows	Mac OS	Linux
• Windows XP SP2*	• El Capitan (OS X 10.11)	• CentOS 6
• Windows Vista*	• Sierra (macOS 10.12)	• CentOS 7
• Windows 7	• High Sierra (macOS 10.13)	• Ubuntu 16
• Windows 8	• Mojave (macOS 10.14)	• Ubuntu 18
• Windows 10	• Catalina (macOS 10.15)	
• Windows 11	• Big Sur (macOS 11)	
• Windows Server 2003*	• Monterey (macOS 12)	
• Windows Server 2008*		
• Windows Server 2012		
• Windows Server 2016		
• Windows Server 2019		
• Windows Server 2022		

* - Deprecated, 2.8.0 is the latest Pathfinder version that is supported on this platform.

Supported Modes of Operation

Pathfinder supports two modes; service and transient.

- **Service Mode:** When running in service mode, Pathfinder will register itself as a system service, and will send a heartbeat to Velocity every 1 minute, checking for pending operations. In addition, once every 15 minutes Pathfinder will run to collect basic endpoint information (Processes, Services, Network adapters, Disks, etc.).
  Note: If you require changing the time interval please contact your Sygnia representative or support).
- **Transient mode:** When running in transient mode, no service shall be created, and Pathfinder will run only until the machine is restarted, or the Pathfinder process is killed.

Installation Formats

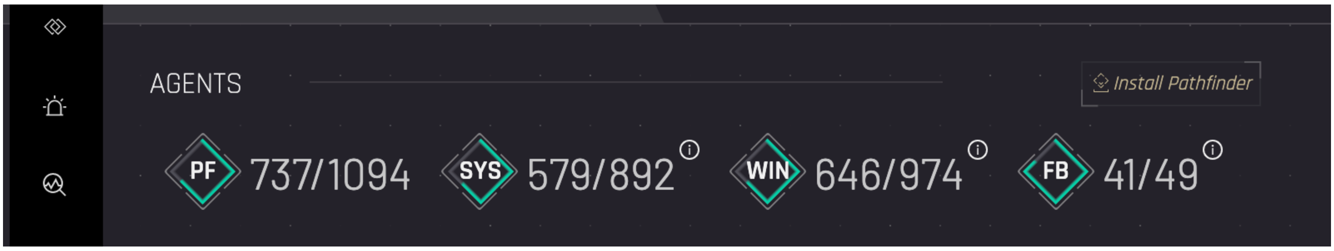
Sygnia recommends deploying Pathfinder as per the below compatibility table

	Windows	Linux	Mac OS
Installation File Format	msi	Installer script (wrapping rpm/deb files)	Installer script (wrapping pkg file)
Installation Directory for service mode	Program Files\Velocity\Pathfinder	/usr/sbin/pathfinder	/Applications/Pathfinder
Installation Directory for transient mode	%TEMP%\Pathfinder	/tmp/pathfinder	/tmp/pathfinder
Log Directory for both service/transient	ProgramData\Velocity\Pathfinder.	/var/log/velocity/pathfinder	/var/log/velocity/pathfinder
Working Directory	%TEMP%\pathfinder	/tmp/pathfinder	/tmp/pathfinder

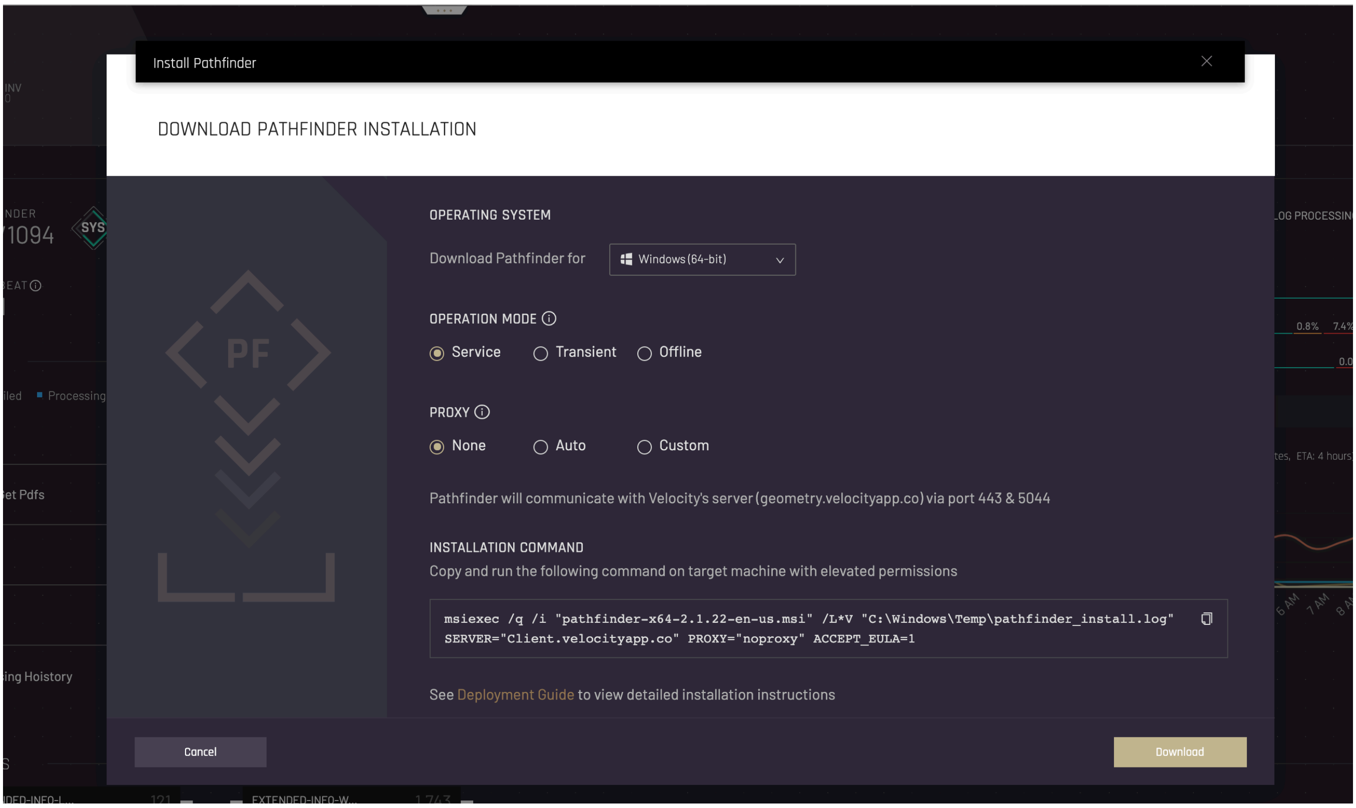
Download Pathfinder

In order to download the OS applicable Pathfinder installation package, please follow these steps

1. Login into Velocity
2. On Agent section in **Dashboard**, click the **Install Pathfinder** button



3. On the PF installation wizard, Specify requested operation system, operation mode and proxy settings
4. Copy the listed command line using the Copy button to use in windows command line\ Linux\Mac terminal
5. Click the **Download** button to download Pathfinder installation file



OPERATING SYSTEM

Download Pathfinder for: Windows (64-bit)

OPERATION MODE ⓘ

● Service ○ Transient ○ Offline

PROXY ⓘ

● None ○ Auto ○ Custom

Pathfinder will communicate with Velocity's server (geometry.velocityapp.co) via port 443 & 5044

INSTALLATION COMMAND

Copy and run the following command on target machine with elevated permissions

```
msiexec /q /i "pathfinder-x64-2.1.22-en-us.msi" /L*V "C:\Windows\Temp\pathfinder_install.log"
SERVER="Client.velocityapp.co" PROXY="noproxy" ACCEPT_EULA=1
```

See Deployment Guide to view detailed installation instructions

Manual Installation

For Windows based endpoints:

1. Once installation file was downloaded, you can follow either step #2 or #3
2. **Install using command line:**
   2.1 Copy and paste the command from the wizard and run it in an elevated console
3. **Install using msi installer:** Double click Pathfinder.msi file

   3.1 Insert Server's Address (E.g., example.velocityapp.co)
4. Validate installation by accessing Velocity's web console and view the agent on the requested machine or contact your Sygnia's representative to validate it on your behalf

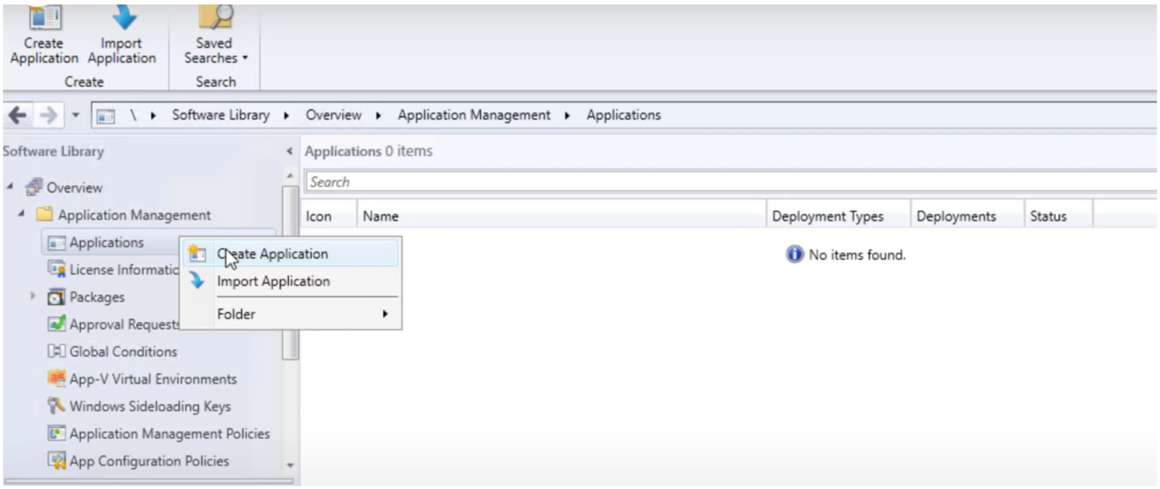
For Linux/Mac based endpoints:

1. Once installation file was downloaded:
2. Run script as root:
    4.1 For Linux: `sudo ./pathfinder-{version}-installer-linux.sh`
    4.2 For macOS: `sudo ./pathfinder-{version}-installer-macos.sh`
3. Validate installation by accessing Velocity's web console and view the agent on the requested machine or contact your Sygnia's representative to validate it on your behalf

SCCM Installation

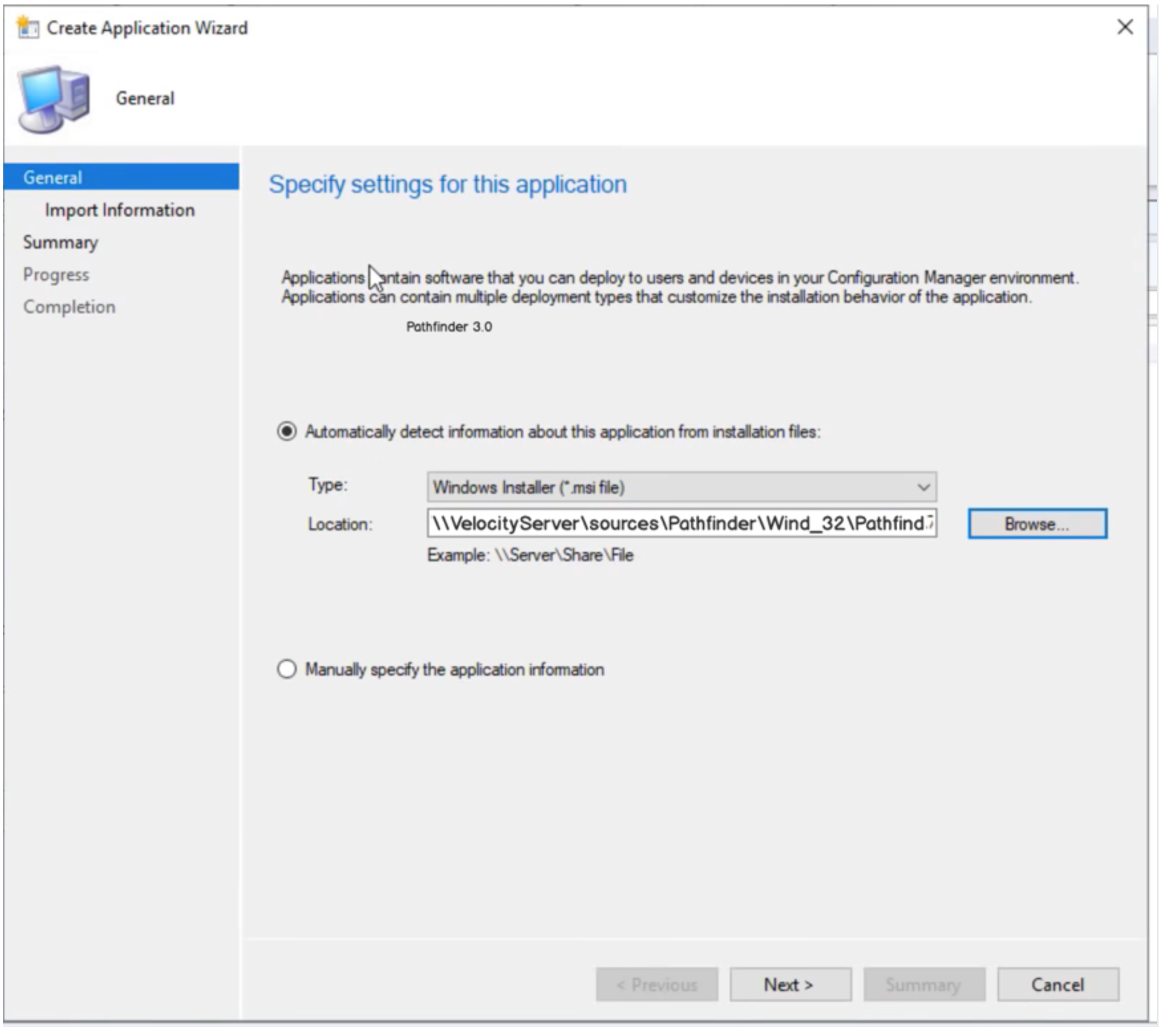
Follow the below steps to install pathfinder via System Center Configuration Manager

1. Download Pathfinder's msi installation file from Velocity's (see Pathfinder's [Supported Installation formats]() section above for specifics)
2. In the Configuration Manager console, choose **Software Library** > **Application Management** > **Applications**
3. Right click **Applications** and choose **Create Application** to open **Create Application Wizard**



4. On the **General** page of the **Create Application Wizard**:
    4.1 Choose **Automatically detect information about this application from installation files**
    4.2 **Type**: Choose **Windows Installer (*.msi file)**
    4.3 **Location**: Type/browse the location of the **Pathfinder-x86-3.0.0-en-us.msi**. installation file

    Note: *location must be specified in the following format \\Server\Share\File in order to allow Configuration Manager to locate the installation files.*



Specify settings for this application

Applications contain software that you can deploy to users and devices in your Configuration Manager environment. Applications can contain multiple deployment types that customize the installation behavior of the application.

Pathfinder 3.0

● Automatically detect information about this application from installation files:

Type: Windows Installer (*.msi file)

Location: \\VelocityServer\sources\Pathfinder\Wind_32\Pathfind

Example: \\Server\Share\File

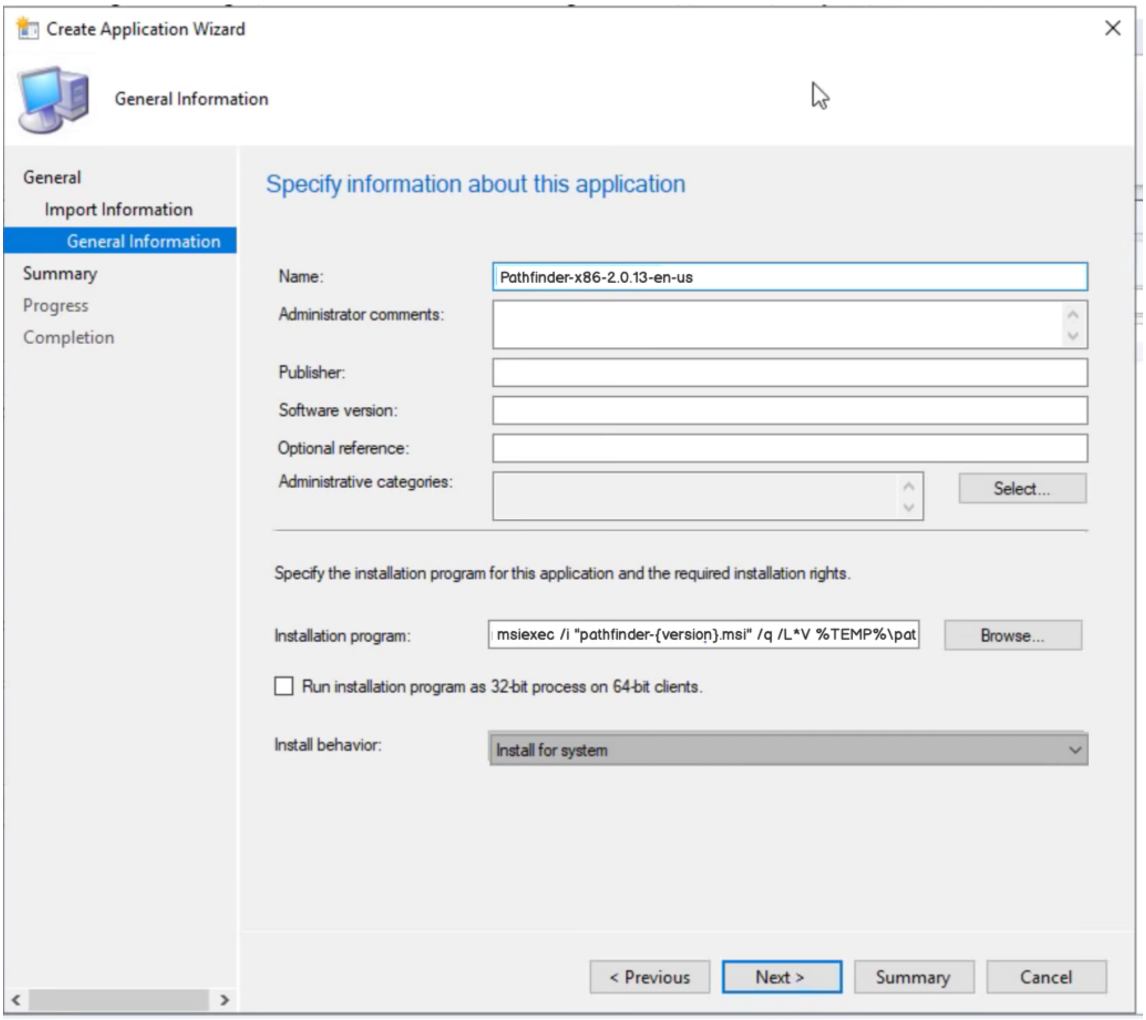
○ Manually specify the application information

5. On the **Import Information** page Choose **Next** again
6. On the **General Information** page modify the following:

6.1 **Installation program**: use command from Pathfinder installation wizard in Velocityx

6.2 **Install behavior:** Install for system

6.3 click **Next**



Create Application Wizard

General Information

Specify information about this application

Name: Pathfinder-x86-2.0.13-en-us

Administrator comments:

Publisher:

Software version:

Optional reference:

Administrative categories:

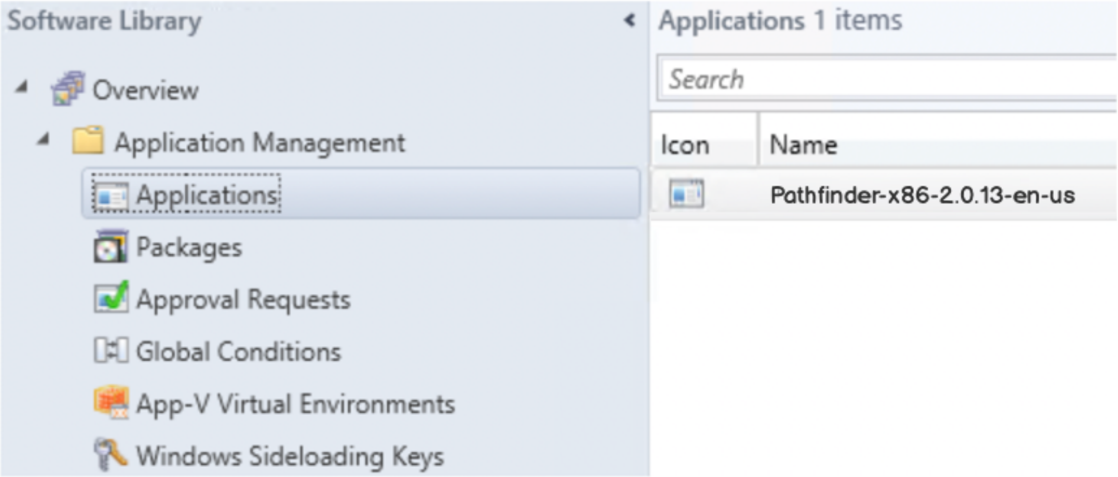
Specify the installation program for this application and the required installation rights.

Installation program: msiexec /i "pathfinder-{version}.msi" /q /L*V %TEMP%\pat

□ Run installation program as 32-bit process on 64-bit clients.

Install behavior: Install for system

7. View Summary page to confirm Pathfinder settings and complete the wizard
8. To find the app in the **Software Library** workspace, expand **Application Management**, and then choose **Applications**. For this example, you'll see:



Icon	Name
	Pathfinder-x86-2.0.13-en-us

GPO Installation

Use one of the two following methods to install pathfinder via Group policy Object:

Method1: create an MST file to install pathfinder (installation requires machine reboot)

1. In order to enable GPO Based deployment, user must first generate an MST file containing server configuration using Microsoft Orca tool:

   Note: *in case user need to first Install Microsoft's Orca, it can be downloaded form* *here* *(installation can be found inside Windows SDK)*

   1.1. Right click pathfinder MSI -> Edit with Orca

   1.2. Under Transform menu, click New Transform

   1.3. Click on Property table

   1.4. Under Tables menu, click Add Row

   1.5. Fill in Property: SERVER, Value: <velocity server>

   1.6. Under Transform menu, click Generate Transform

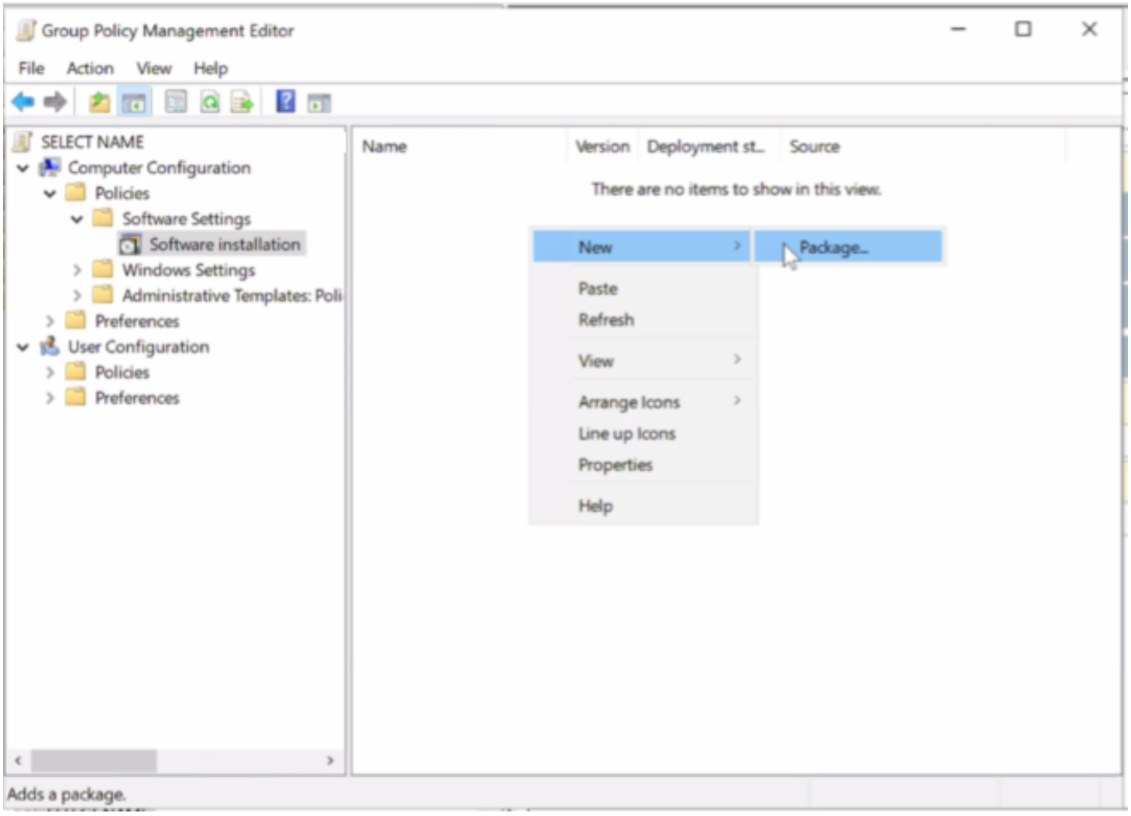
   1.7. Save MST in the same directory as MSI file

Once MST was generated, create deployment in GPO:

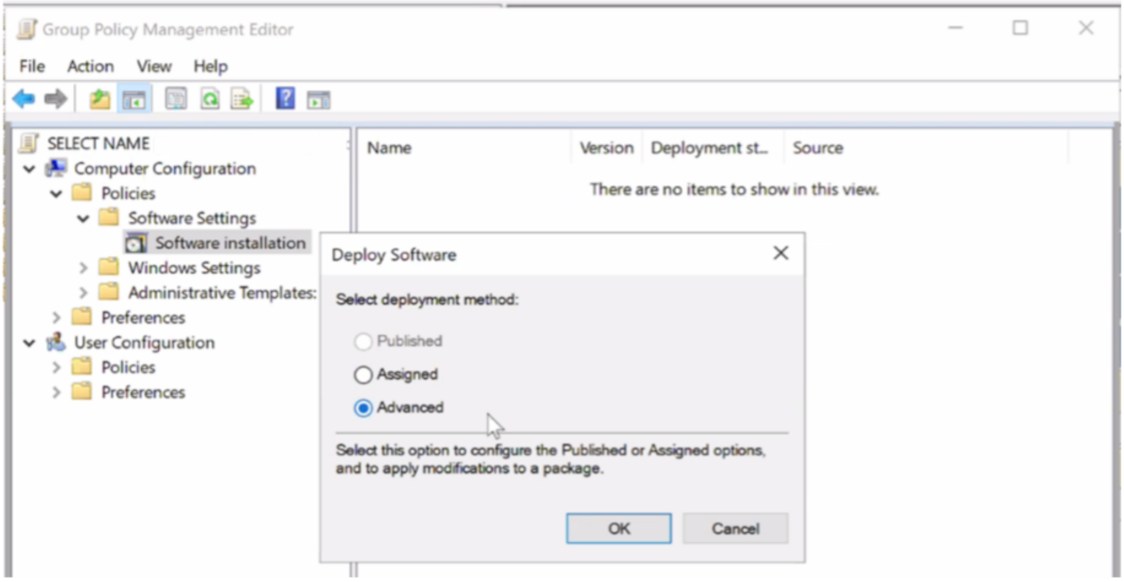
2. Create a new policy or select an existing one
3. In **Group Policy Management Editor**:

   3.1. Right click to add a new software installation package

   3.2. Browse and open Pathfinder's MSI file



4. Choose **Advanced** in **Select deployment method**, then click **OK**



There are no items to show in this view.

Select deployment method:

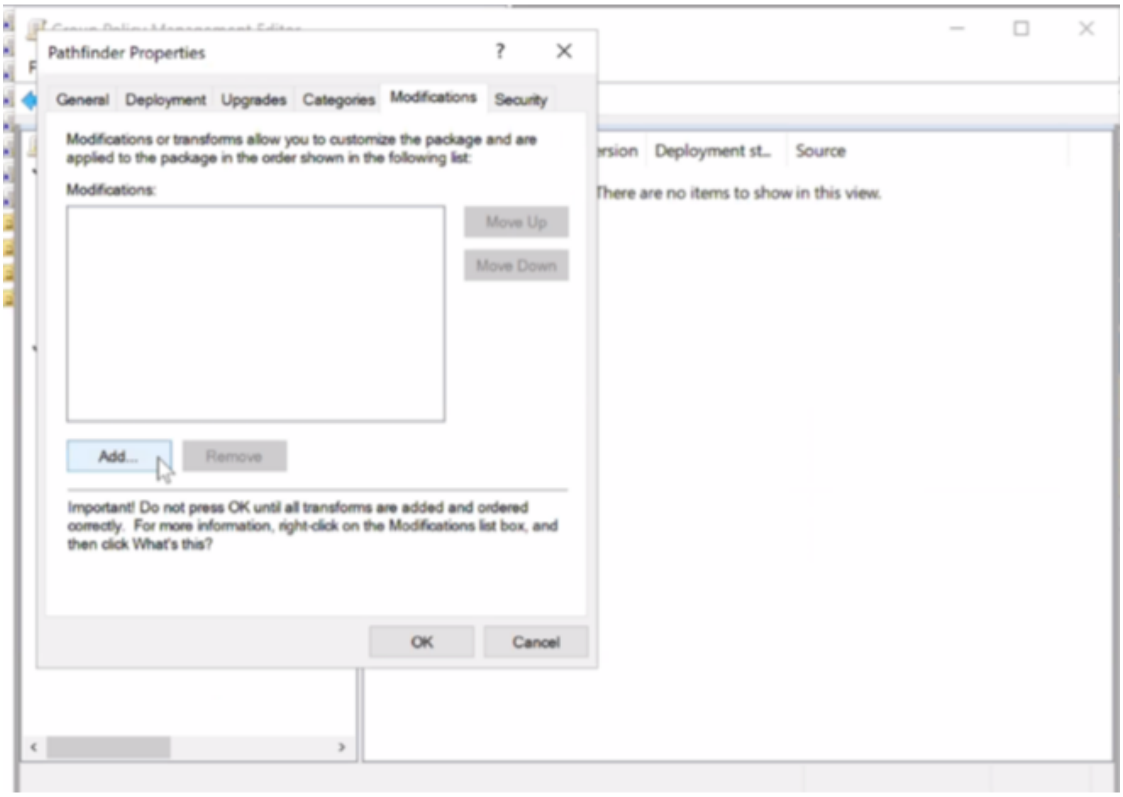
○ Published

○ Assigned

● Advanced

Select this option to configure the Published or Assigned options, and to apply modifications to a package.

5. In Modifications tab, click Add, and select the MST file generated in step1 of this section



Modifications or transforms allow you to customize the package and are applied to the package in the order shown in the following list:

Modifications:

Important! Do not press OK until all transforms are added and ordered correctly. For more information, right-click on the Modifications list box, and then click What's this?

There are no items to show in this view.

6. Click OK to save package

Method2: Use installation powershell script and MSI file to immediately install Pathfinder

1. Upload the installation script and the MSI files to a shared Netlogon folder on Domain Controller. Set the $PFMSI32 and $PFMSI64 variables (in the PF_Installation.ps1 file) to the MSI's network path.
2. Create a GPO to apply the installation script. Link the script to the root of the domain.
3. Remove "Authenticated Users" from the security filtering and add specific test computers.
4. Add the task: Computer Config => Preferences => Control Panel => Schedule Task => New =>

Immediate Task.

5. Configure the task:
    a. Run as SYSTEM
    b. Mark "Run with highest privileges"
    c. Mark "Hidden"
    d. Action program: powershell.exe.
    e. Action arguments: -ExecutionPolicy Bypass -file "\\<domain-controller>\<folder path>\PF_Installation.ps1"
    f. Settings tab: If the task fails, restart every 5 minutes, up to 3 times. Stop if runs longer then 2 hours
6. Connect to test machines, run GPUpdate, and check if the service "Pathfinder" is up and running.
    a. If not, check if the GPO was applied (gpresult) and if the task was created (Event Viewer, Applications => Microsoft => Windows => TaskScheduler =>Operational).
7. Apply the GPO on all computers by adding "Authenticated Users" to the security filtering.
8. Repeat in all Active Directory domains.

Contents of PF_Installation.ps1:

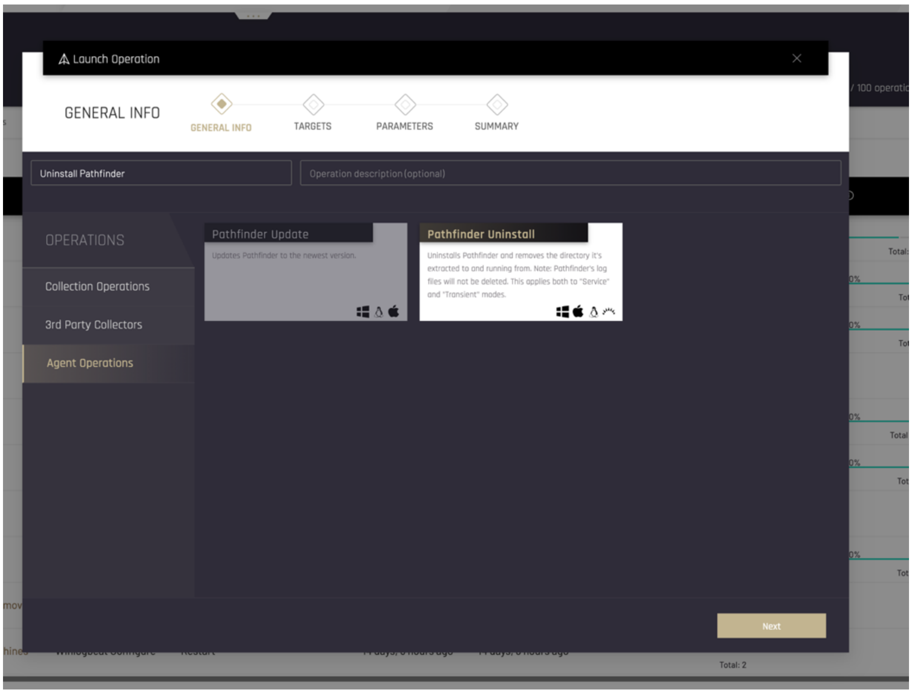
```
$serviceName = "PathfinderSvc"
$PFMSI64 = "\\<shared-folder-path>\pathfinder-x64-3.0.0-en-us.msi"
$PFMSI32 = "\\<shared-folder-path>\pathfinder-x86-3.0.0-en-us.msi"

If (-not (Get-Service $serviceName -ErrorAction SilentlyContinue))
{
   if([Environment]::Is64BitOperatingSystem)
   {
            cmd /c msiexec.exe /i "$PFMSI64" /q /L*V %TEMP%\pathfinder_install.log SERVER="<velocity-server>" MODE="service"
ACCEPT_EULA=1
   }
   Else
   {
         cmd /c msiexec.exe /i $PFMSI32 /q /L*V %TEMP%\pathfinder_install.log SERVER=”<velocity-server>" MODE="service"
ACCEPT_EULA=1
   }
}
```

Uninstall Pathfinder

Uninstall Pathfinder by launching an operation using Velocity UI or by manually running the commands below per each operation system:

Note: Uninstalling Pathfinder doesn't uninstall 3rd party collectors that were installed via Pathfinder. (3rd party collectors removal can be done by accessing 3rd party collectors section on Launch operation wizard and executing the Removal Operation of the collector of interest)

1. **Uninstall Pathfinder via Velocity UI:**
   - 1.1 Access Operations screen using the navigation menu and click Launch Operation
   - 1.2 Under Agent Operations section, select Pathfinder Uninstall operation and click next
   - 1.3 Select target machines and click next
   - 1.4 Click Launch Operation



Uninstall Pathfinder

Operation description (optional)

Pathfinder Update

Updates Pathfinder to the newest version.

Pathfinder Uninstall

Uninstalls Pathfinder and removes the directory it's extracted to and running from. Note: Pathfinder's log files will not be deleted. This applies both to "Service" and "Transient" modes.

2. **For Windows based endpoints run the following commands:**
   - 2.1. wmic Product Where Name='Pathfinder' Call Uninstall /NoInteractive
   - 2.2. msiexec.exe /quiet /x<PRODUCT_CODE> (product code can be found in config.ini after PF installation)
   - 2.3. msiexec /quiet /x pathfinder-{arch}-{version}-en-us.msi (with original MSI used for installation)
3. **For Linux based endpoints run one of the following commands (relative to file installation type):**
   - 3.1. rpm -e pathfinder
   - 3.2. dpkg -r pathfinder
4. **For Mac based endpoints run the following command:**
   - 4.1. sudo /Applications/Pathfinder/uninstall.sh