ManageEngine
PAM360

Installing PAM360 Windows Agent in Multiple Endpoints

ManageEngine PAM360

Table of Contents

Deploying PAM360 Agent in Endpoints using Microsoft System Center Configuration Manager (SCCM) 3

1. Installing PAM360 Agent using SCCM 3
2. Uninstalling PAM360 Agent using SCCM 7

Deploying PAM360 Agent in Endpoints via Windows Group Policy Objects (GPO) 9

1. Installing the PAM360 Agent via Windows Group Policy Objects (GPO) 9
2. Uninstalling the PAM360 Agent via Windows Group Policy Objects (GPO) 18

Deploying PAM360 Agent in Endpoints using Endpoint Central 25

1. Installing PAM360 Agent using Endpoint Central 25
2. Uninstalling PAM360 Agent using Endpoint Central 31

Notes:

- The deployment methods outlined in this document are exclusively applicable to Windows-based resources.
- Ensure that the PAM360 has uninterrupted access to all target machines intended for agent deployment.
- Beginning with build 7500, the agent installer has been streamlined into a single executable (.EXE) file, replacing the earlier ZIP package format for simplified deployment.

Deploying PAM360 Agent in Endpoints using Microsoft System Center Configuration Manager (SCCM)

System Center Configuration Manager (SCCM), developed by Microsoft, streamlines IT management in large-scale environments by deploying agents to centrally manage and monitor devices. The bulk agent installations are crucial for saving time and ensuring consistency, especially in extensive IT infrastructures. SCCM's capabilities empower administrators to deploy client agents to multiple endpoints simultaneously, maintaining a standardized and secure computing environment.

Prerequisite:

Download the agent installation script zip accordingly and extract the script files **PAM360AgentInstallationSCCM.ps1** and **PAM360AgentUninstallationSCCM.ps1**.

- For agent file as a zip, download the SCCMAgentScript.zip and ensure the SHA256 value:
  88133a952631c51a40450613703d0a1ebefa675b92b07ef024ce2c7fab80bcd1
- For agent file as an exe, download the SCCMAgentScript-7500.zip and ensure the SHA256 value:
  44569a48901331e5c3e9222de681ba6b22e7c7d30382b08dbba7463c7311e0ef

1. Installing PAM360 Agent using SCCM

Follow the below steps to install the PAM360 agent in bulk using SCCM:

1. To begin the PAM360 agent installation process, log in to PAM360 and navigate to '**Admin >> PAM360 Agents**'.
2. Download the **Windows Agent** (.zip or .exe) to the preferred network path and ensure to copy the **Agent Key** value.
3. Open the **PAM360AgentInstallation.ps1** script file in an editor from the extracted folder and do the steps as follows:
   i. Enter the network path in the **$AgentZipSource** or **$AgentExeSource** variable

where the PAM360 Windows Agent is downloaded. For example - "**\\zylker.com\PAM360\PAM360_WindowsAgent_CS.zip** or **\\zylker.com\PAM360\PAM360AgentInstaller.exe**".

ii. Add a destination path of the endpoints or target machines in the **$AgentDestinationPath** variable, for example, **c:\Program Files (x86)**. This is the location where the agent file will be copied; $Process will install agent modules and also unpack the installer files on the target endpoints, so ensure that this path is available on all the target machines. **Note:** From build 7500 onwards, the PAM360 agent installer files will be unpacked on the default location - **C:\Program Files (x86)\ManageEngine\PAM360AgentInstaller**. Manually changing this location is restricted and prevents the agent from being installed.

iii. Enter the copied **Agent Key** and the agent module as required to complete the **PAM360AgentInstallation.ps1** script file updates:

a. If you are installing the agent as a service for password management, self-service privilege elevation, and zero trust implementation, enter 1,2,3. For example, "**./AgentInstaller.exe install <a560f6385298754c> 1,2,3**"

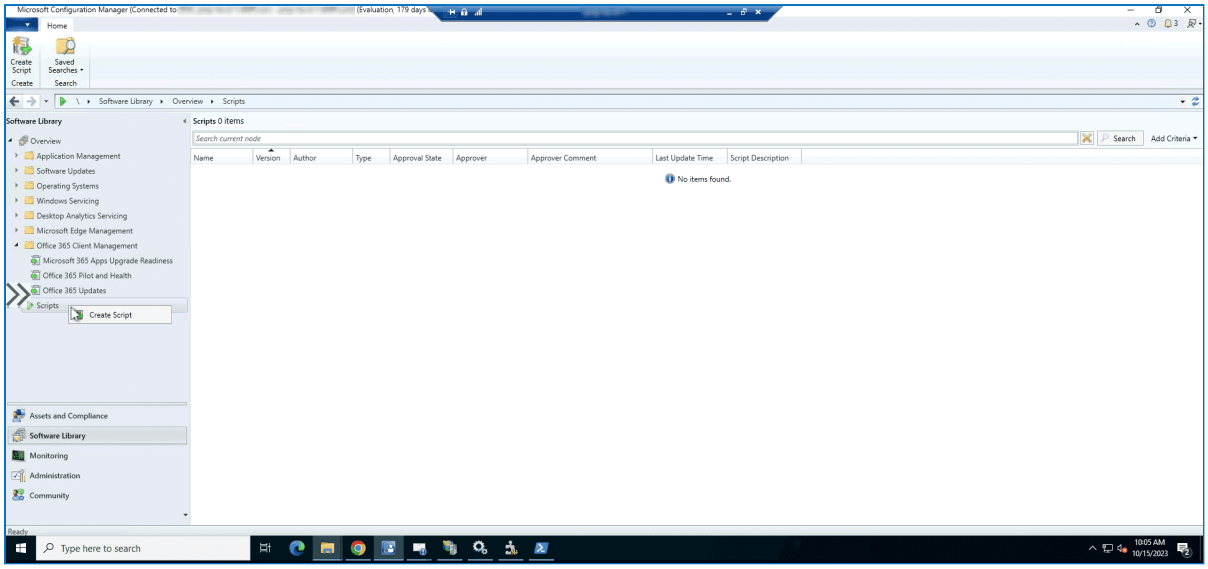
b. If you are installing the agent as a service for password management, enter 1. For example, "**./AgentInstaller.exe install <a560f6385298754c> 1**"

c. If you are installing the agent as a service for self-service privilege elevation, enter 2. For example, "**./AgentInstaller.exe install <a560f6385298754c> 2**"

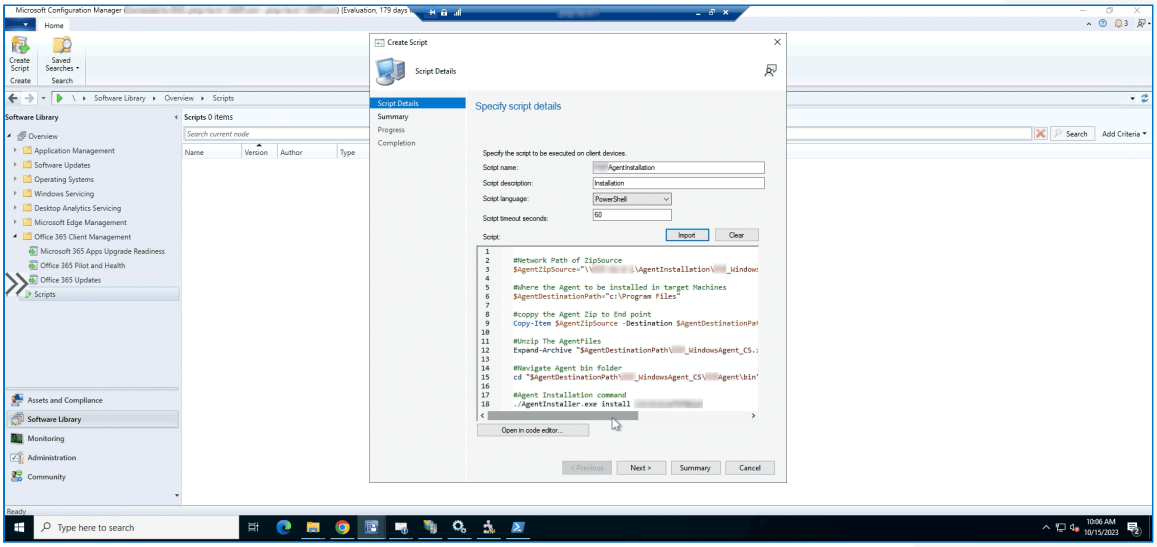
d. If you are installing the agent as a service for zero trust implementation, enter 3. For example, "**./AgentInstaller.exe install <a560f6385298754c> 3**"

You can also enter a different combination based on your agent's installation requirements.

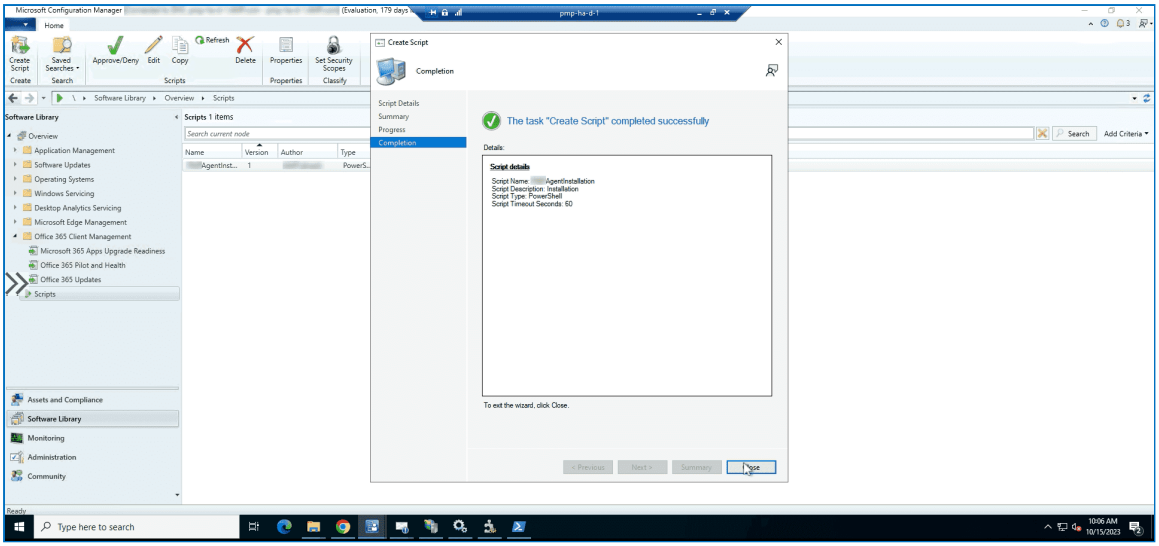
4. Now, open the **Microsoft Configuration Manager Console** and select **Software Library**.
5. On the page that changes, navigate to **Overview >> Office 365 Client Management >> Script** and select **Create Script**.



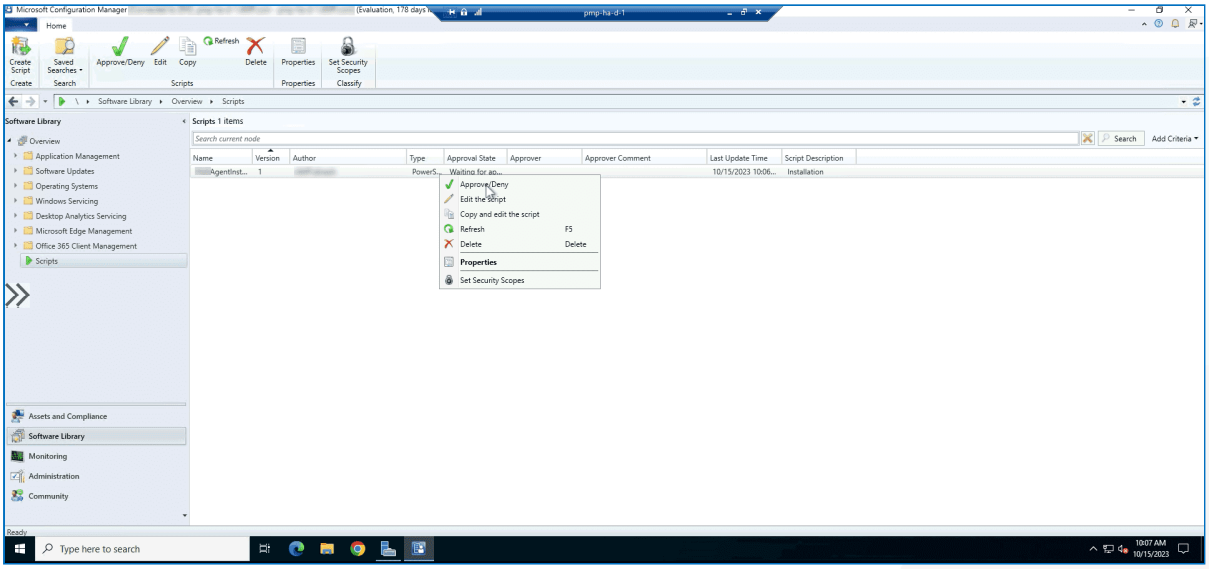
6. In the script dialogue box that opens,
   a. Enter the **Script name**. For example, **PAM360AgentInstallation**
   b. Enter the **Script description**. For example, **PAM360 Resource Agent Installation in Endpoints**.
   c. Select the Script language as **PowerShell** and set the Script timeout seconds as required, preferably to **60**.
   d. Use the **Import** button to import the updated **PAM360AgentInstallation.ps1** script file.



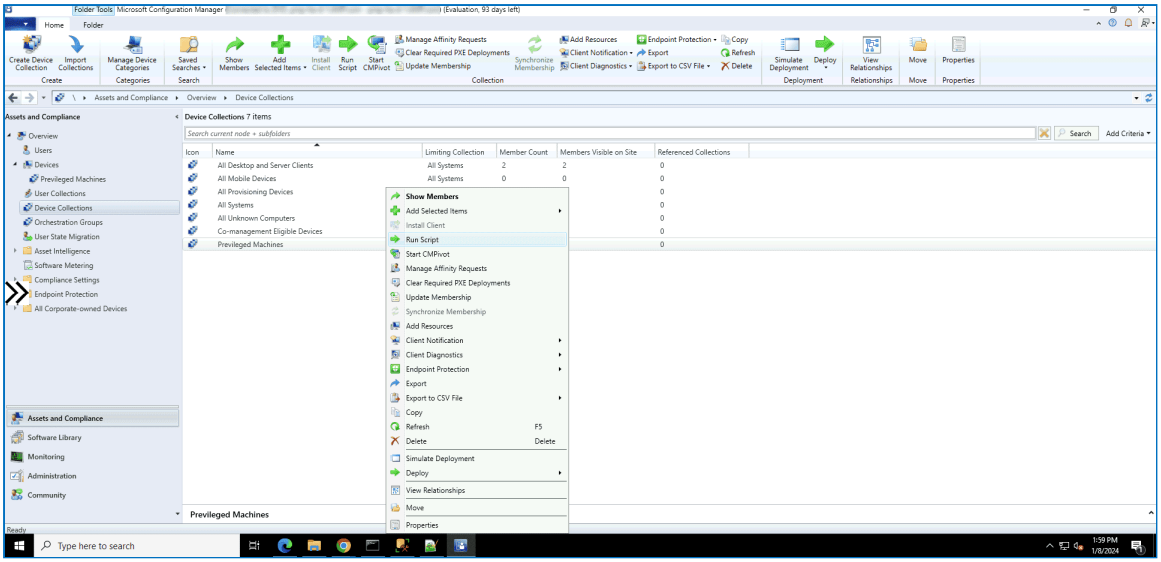
   e. Validate the details and click **Next >** to complete the script creation process.



7. Inform another user with the Microsoft administrator privilege to validate (**Approve/Deny**) and approve the created script for bulk agent installation.



8. Once the created script is validated by another administrator, you can execute the script on the relevant target devices/device groups to install the PAM360 agent. To do so,
   a. Navigate to **Overview >> Device Collections** from the **Assets and Compliance** section.
   b. Right-click over the required device group and click **Run Script** to execute the script in the selected endpoints or target machines in bulk.



9. Upon successful completion, the agent will be installed with the respective modules in the target devices or endpoints available in the selected device group.

2. Uninstalling PAM360 Agent using SCCM

Follow the below steps to uninstall the PAM360 agent in bulk using SCCM:

1. Open the **Microsoft Configuration Manager Console** and select **Software Library**.
2. On the page that changes, navigate to **Overview >> Office 365 Client Management >> Script** and select **Create Script**.
3. In the script dialogue box that opens,
   a. Enter the **Script name**. For example, **PAM360AgentUninstallation**
   b. Enter the **Script description**. For example, **PAM360 Resource Agent Uninstallation from Endpoints**.
   c. Select the Script language as **PowerShell** and set the Script timeout seconds as required, preferably to **60**.
   d. Use the **Import** button to import the **PAM360AgentUninstallation.ps1** script file.
   e. Validate the details and click **Next >** to complete the script creation process.
4. Inform another user with the Microsoft administrator privilege to validate (**Approve/Deny**) and approve the created script for bulk agent uninstallation.

5. Once the created script is validated by another administrator, you can execute the script on the relevant target devices/device groups to uninstall the PAM360 agent. To do so,
   a. Navigate to **Overview >> Devices** from the **Assets and Compliance** section.
   b. Right-click over the required device group and click **Run Script** to execute the script in the selected endpoints or target machines in bulk.
6. Upon successful completion, the agent will be uninstalled from the target devices or endpoints available in the selected device group.

Deploying PAM360 Agent in Endpoints via Windows Group Policy Objects (GPO)

Prerequisites

- Refer to the steps detailed in this help page to download the PAM360 Windows agent (.zip or .exe) from the PAM360 interface, and copy the **Agent Key**. Save the key in a secure location, as this must be added to the PAM360 PowerShell script later.
- If you already have agents installed in the endpoints, follow these steps to uninstall the agents in bulk using the uninstallation script. This script will uninstall both the C++ and C agents.
- Create a Domain with all the target machines that need to be included in the GPO to be the endpoints where the agent is to be installed.
- Download the agent installation script zip accordingly and extract the script files **PAM360AgentInstallationScript.ps1** and **PAM360AgentUninstallationScript.ps1**.
    - For agent file as a zip, download the GPOAgentScript.zip and ensure the SHA256 value: **2b8c64703bd0bbcc30d5cb7e336826474ad47306b91f44261b49f9f6a8990702**
    - For agent file as an exe, download the GPOAgentScript-7500.zip and ensure the SHA256 value: **d3b9aaf07a18f331fce9b49ddb3c3e087460571bc726b7fa204f47b43f40fd9d**

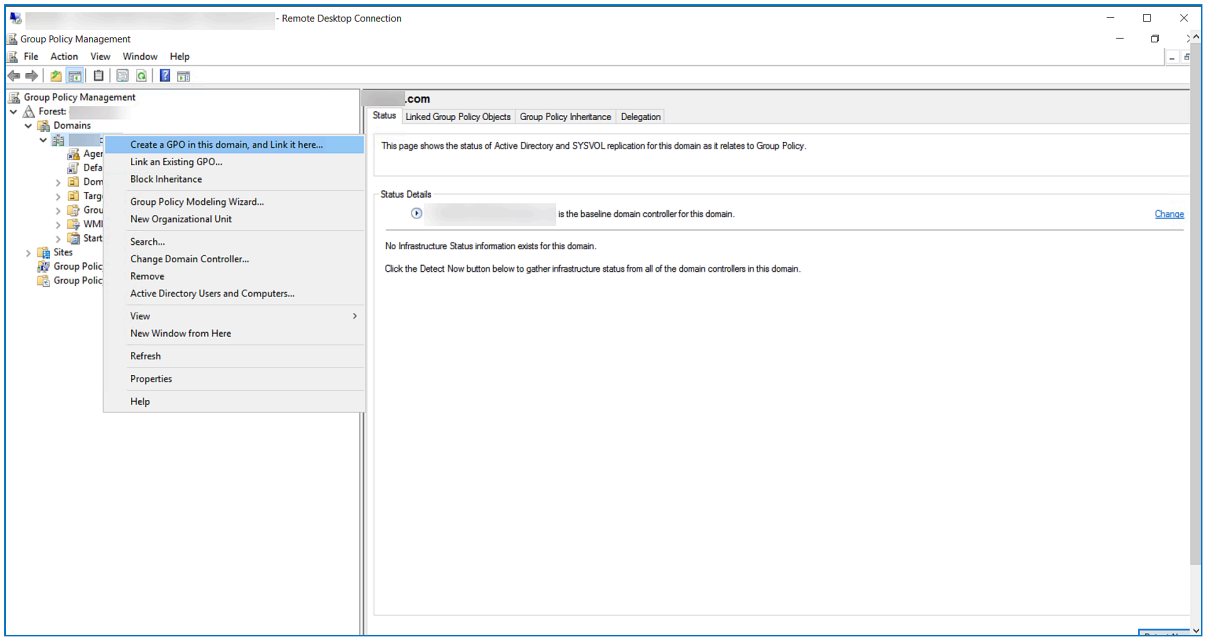
1. Installing the PAM360 Agent via Windows Group Policy Objects (GPO)

This section details the steps needed to install the PAM360 Agent in multiple endpoints using Windows Group Policy Objects (GPO).

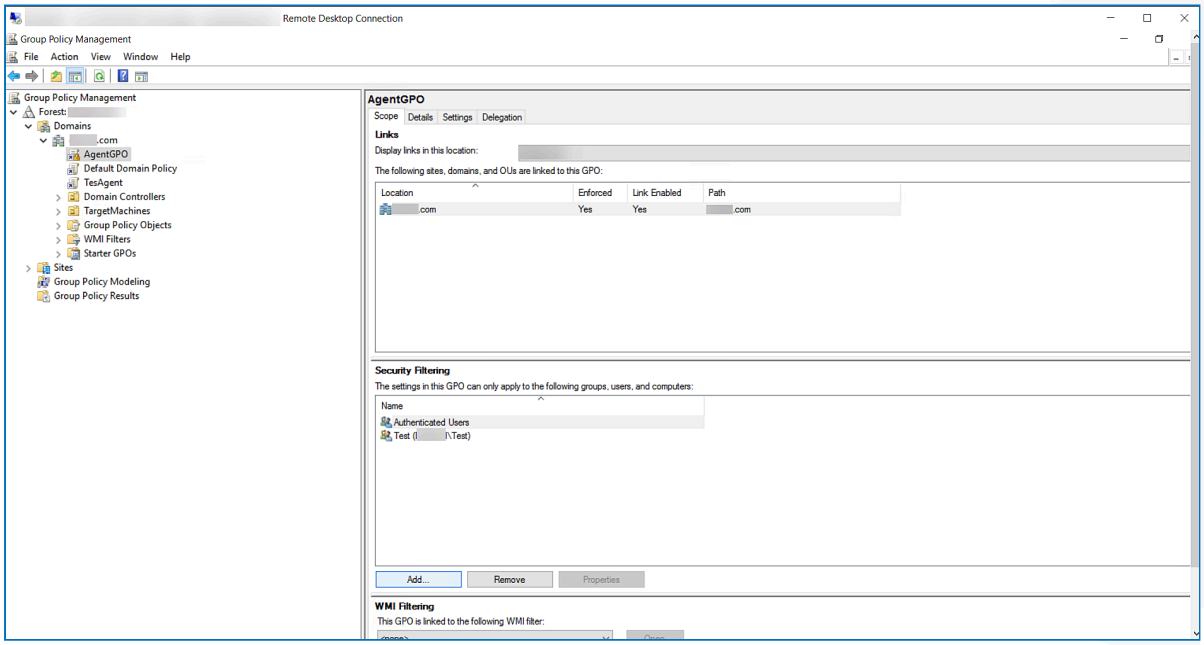
a. Steps to Create a GPO in the Domain and to Add Target Machines

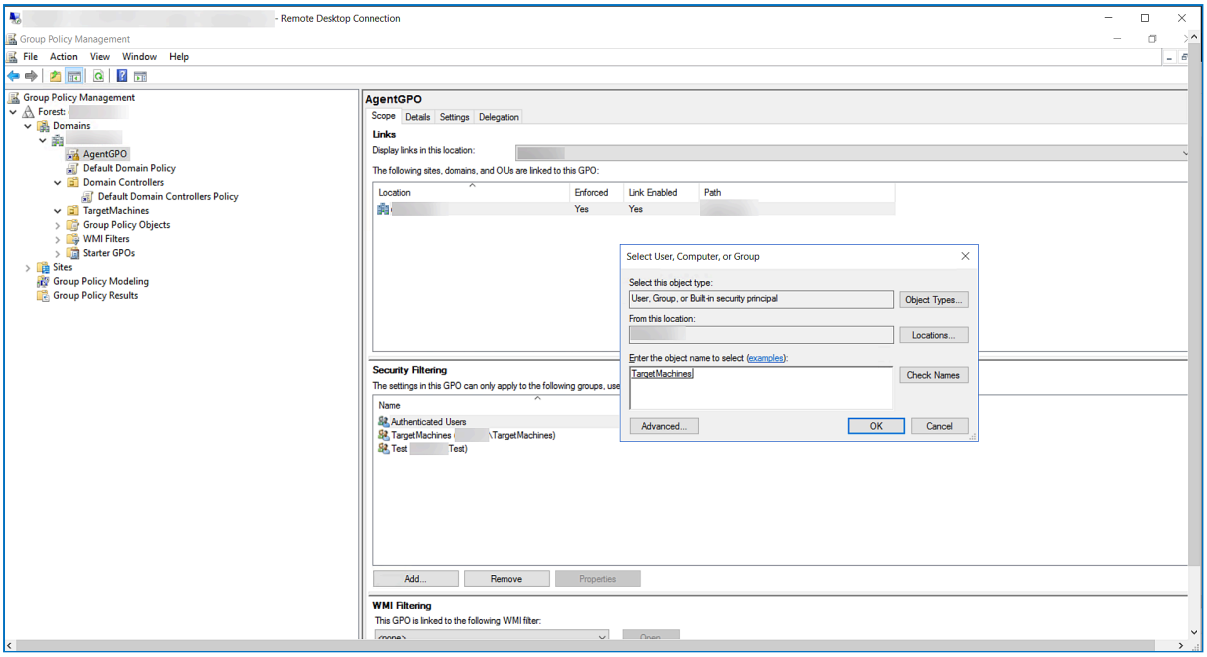
1. Open the **Server Manager** and navigate to **Tools >> Group Policy Management** from the top right corner.
2. Right-click the domain name, click **Create a GPO in this domain, and Link it**

here...

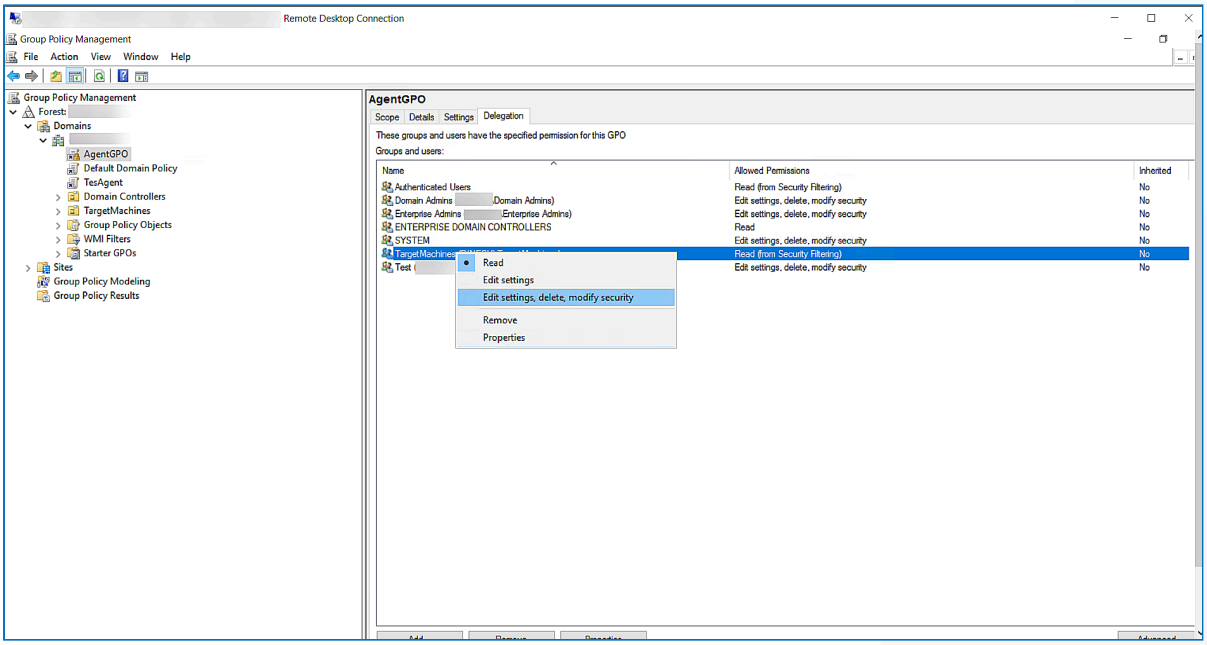


3. Enter a name for the new GPO and save - AgentGPO. Provide a name for the new GPO, for example, AgentGPO. Now, click the newly created GPO under **Scope >> Security Filtering**, and click **Add**. In the **Select User**, **Computer**, or **Group** window, enter the target machine names or the name of the group name that contains all the target endpoints or the names of the target machines individually and click **OK**.





4. Switch to the **Delegations** tab. Right-click the group you have added and provide full access permission as shown below.

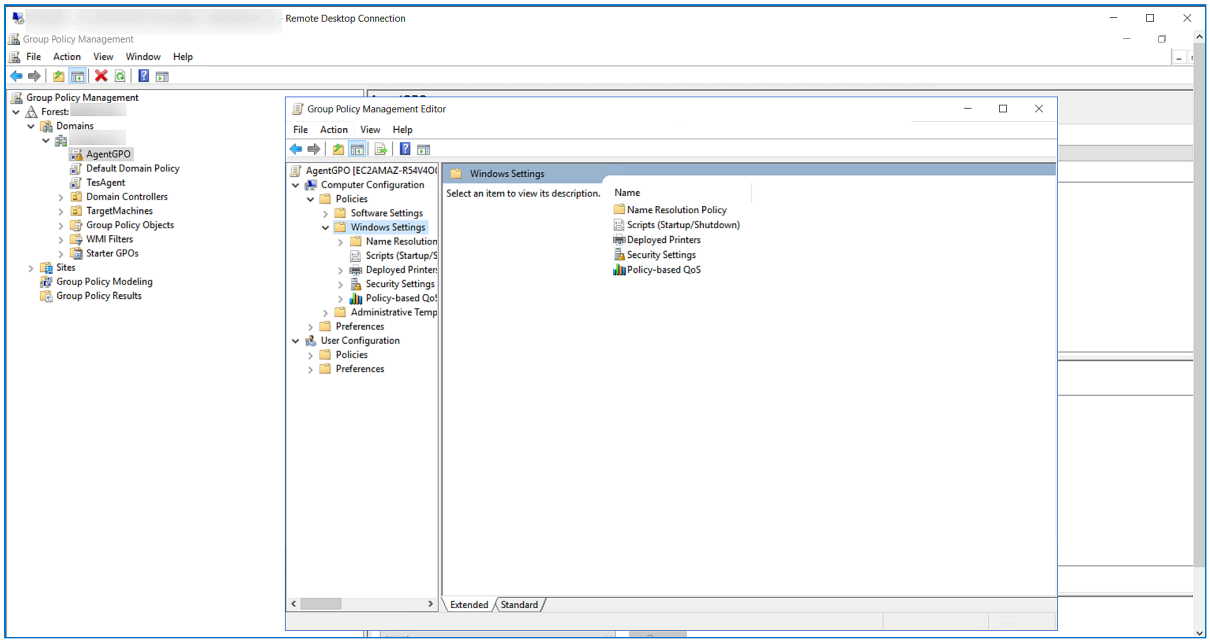


You have successfully created a **Group Policy** and added the target machines where the PAM360 agent is to be installed.

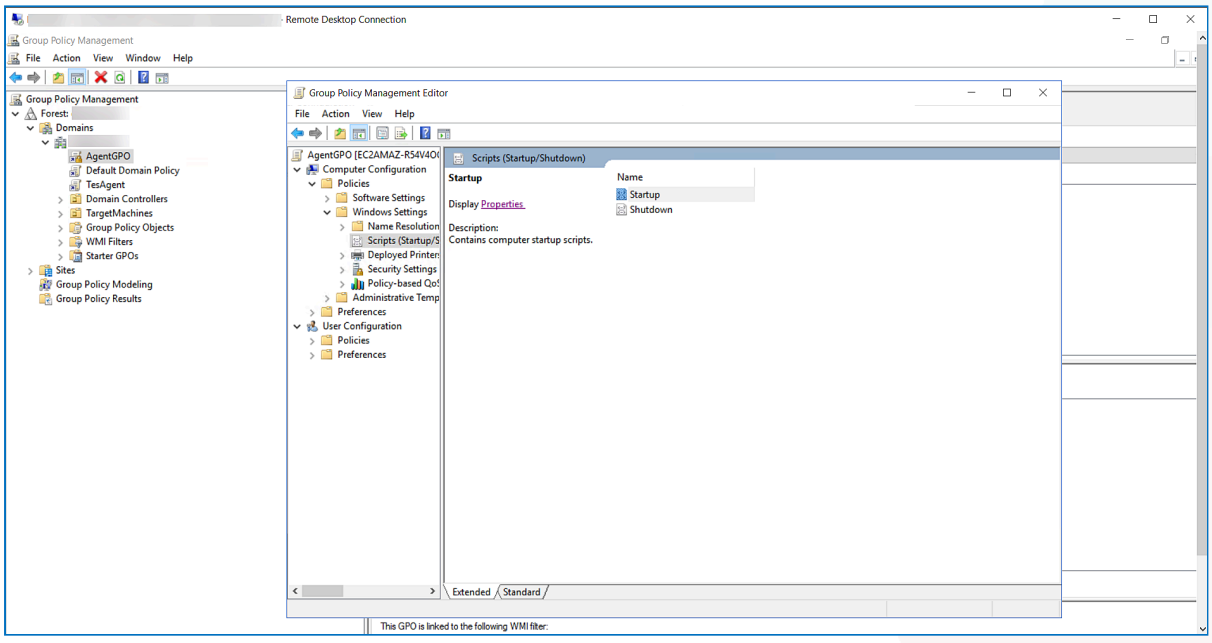
b. Steps to Add the Installation Script and Agent Installation Zip in the GPO

1. Now right-click the GPO name from the left pane and click **Edit settings, delete,**

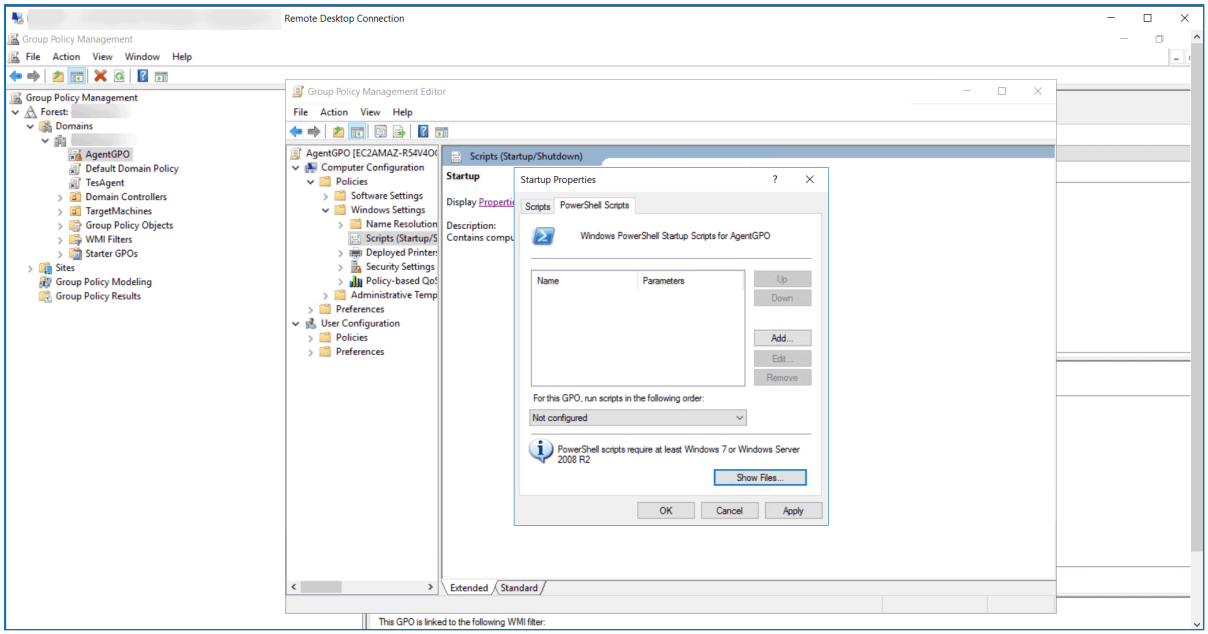
modify security. The **Group Policy Management Editor** window will open.



2. Navigate to the **Policies >> Windows Settings** folders. Double-click **Scripts**. In the Scripts window, click **Startup** and then click **Properties**.



3. Switch to the **PowerShell Scripts** tab and click **Show Files**. The network directory will open. Now, copy the path of the network location.



4. Open the extracted **PAM360AgentInstallationScript.ps1** file and do the steps as follows:

   i. Paste the network location path copied in the previous step as the source variable. For example - "**\\zylker.com\PAM360\PAM360_WindowsAgent_CS.zip** or **\\zylker.com\PAM360\PAM360AgentInstaller.exe**".

   ii. Add a destination path of the endpoints or target machines in the **$AgentDestinationPath** variable, for example, **c:\Program Files (x86)**. This is the location where the agent file will be copied; $Process will install agent modules and also unpack the installer files on the target endpoints, so ensure that this path is available on all the target machines. **Note:** From build 7500 onwards, the PAM360 agent installer files will be unpacked on the default location - **C:\Program Files (x86)\ManageEngine\PAM360AgentInstaller**. Manually changing this location is restricted and prevents the agent from being installed.

   iii. Append the following data beside "**./AgentInstaller.exe install $args**" as required:

      a. If you are installing the agent as a service for password management, self-service privilege elevation, and zero trust implementation, enter 1,2,3. For example, "**./AgentInstaller.exe install $args 1,2,3**"

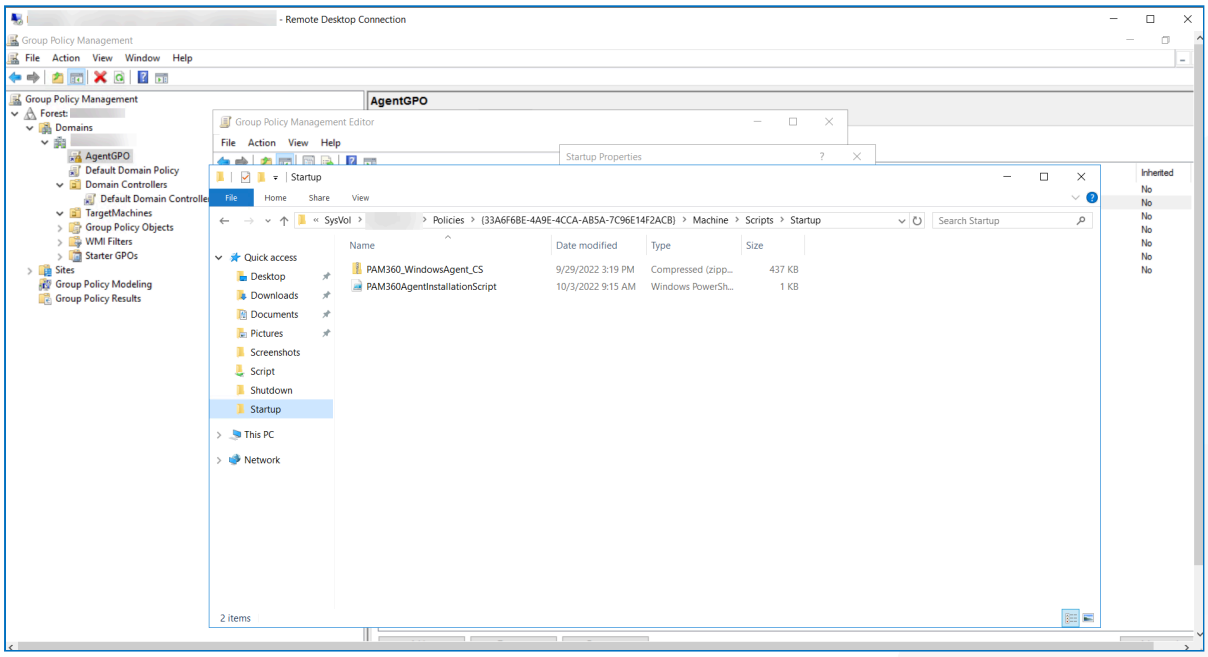
b. If you are installing the agent as a service for password management, enter 1. For example, "**./AgentInstaller.exe install $args 1**"

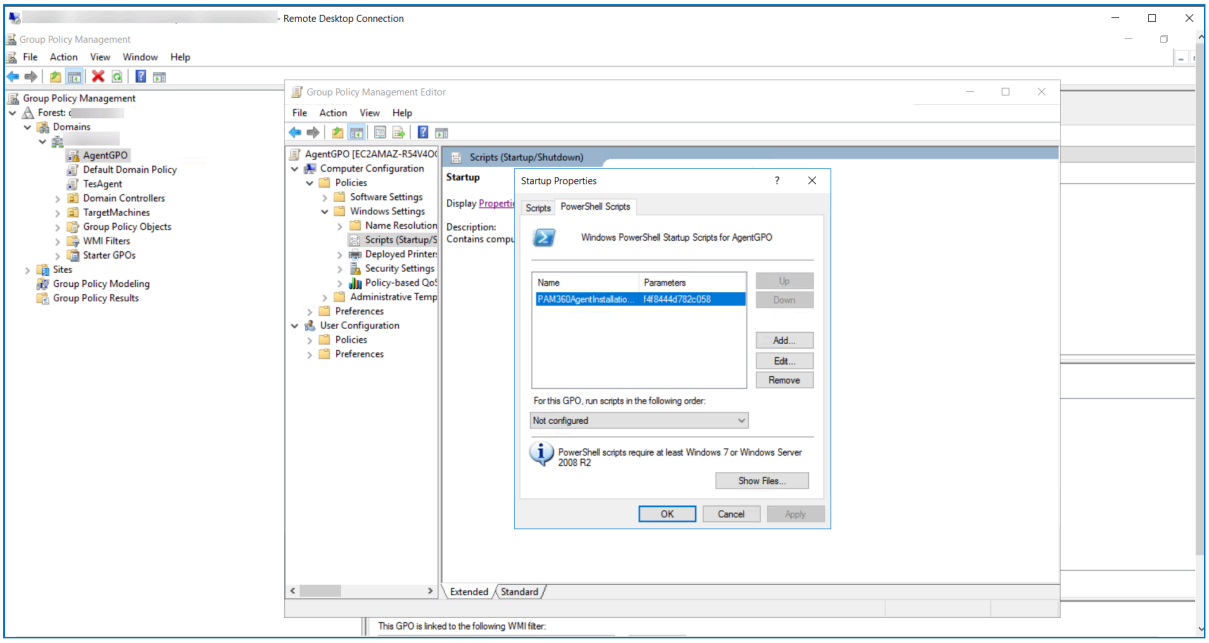
c. If you are installing the agent as a service for self-service privilege elevation, enter 2. For example, "**./AgentInstaller.exe install $args 2**"

d. If you are installing the agent as a service for zero trust implementation, enter 3. For example, "**./AgentInstaller.exe install $args 3**"

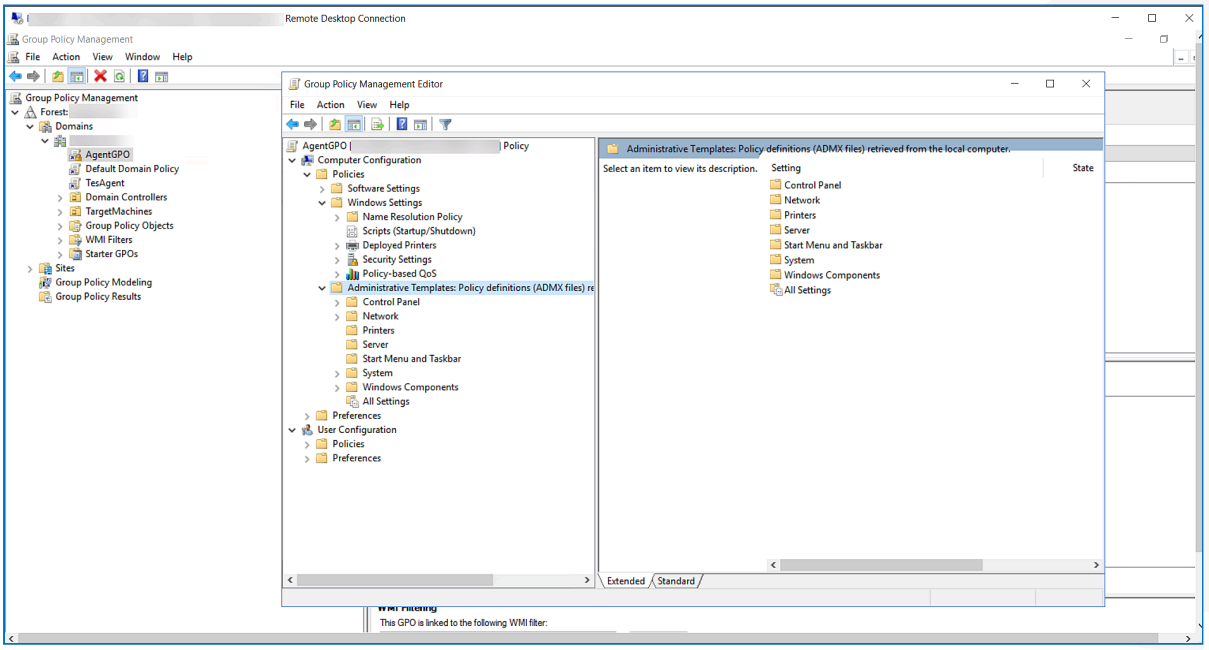
You can also enter a different combination based on your agent installation requirements.

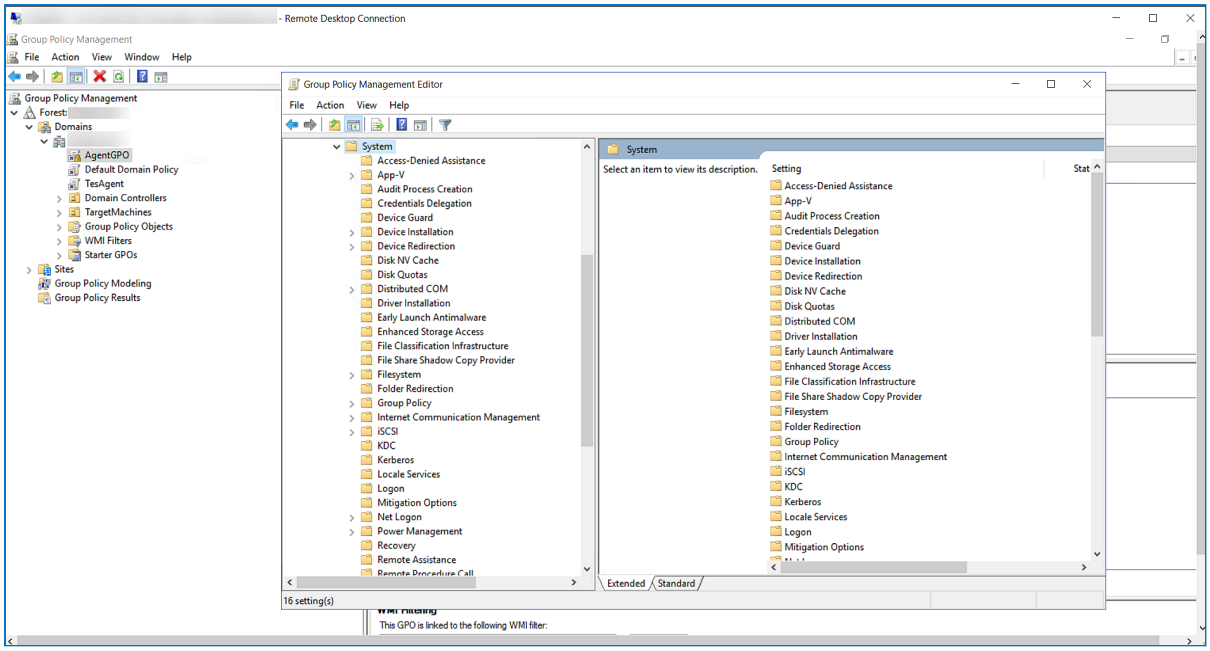
5. Now, paste the PAM360 agent PowerShell script file and the Agent installation zip or PAM360AgentInstaller.exe in the GPO network location.

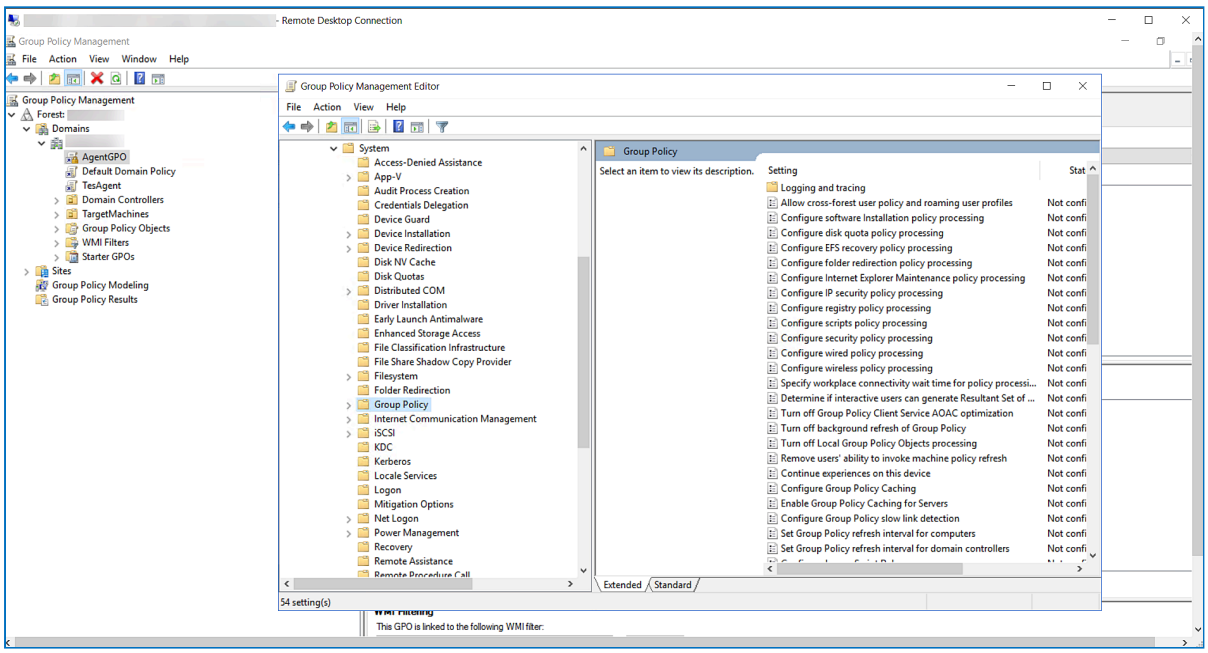


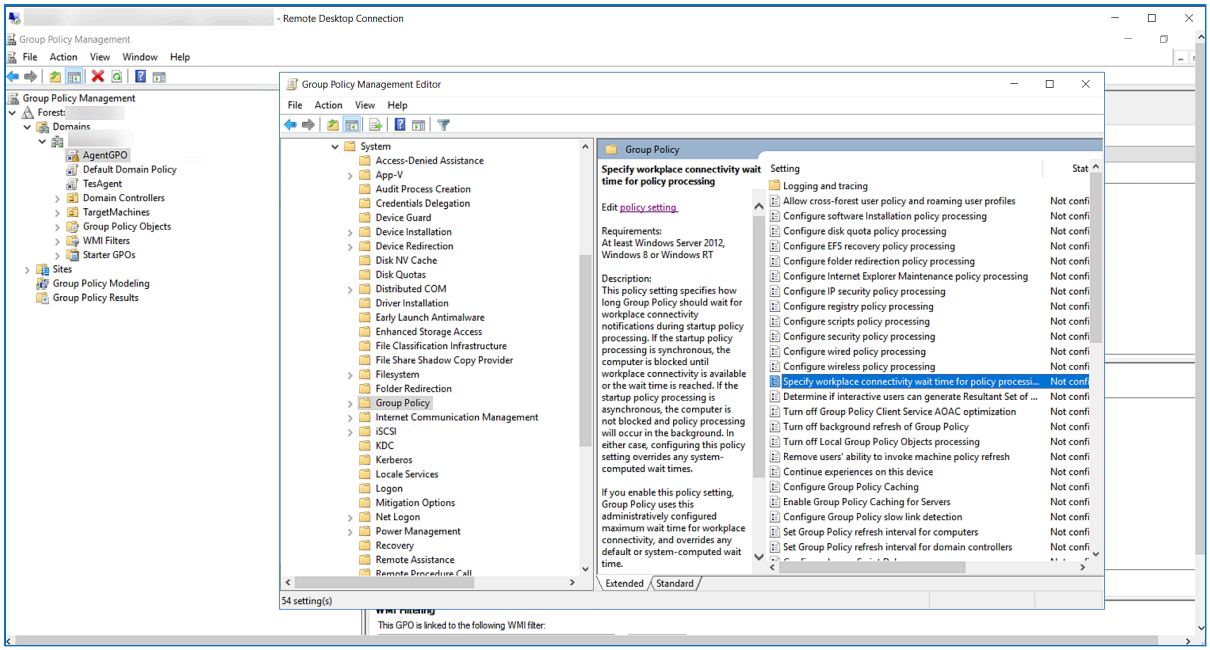


6. Click **Add** and add the **PAM360AgentInstallationScript** file name under **Script Name** and the agent installation key copied from PAM360 under **Script Parameters**. Click **Apply** and **OK** again to save the settings.
7. In the **Group Policy Management Editor**, navigate to **Administrative Templates >> System** and open the **Group Policy**.
8. Under the Group Policy folder, right-click **Specify workplace connectivity wait time for policy processing**.

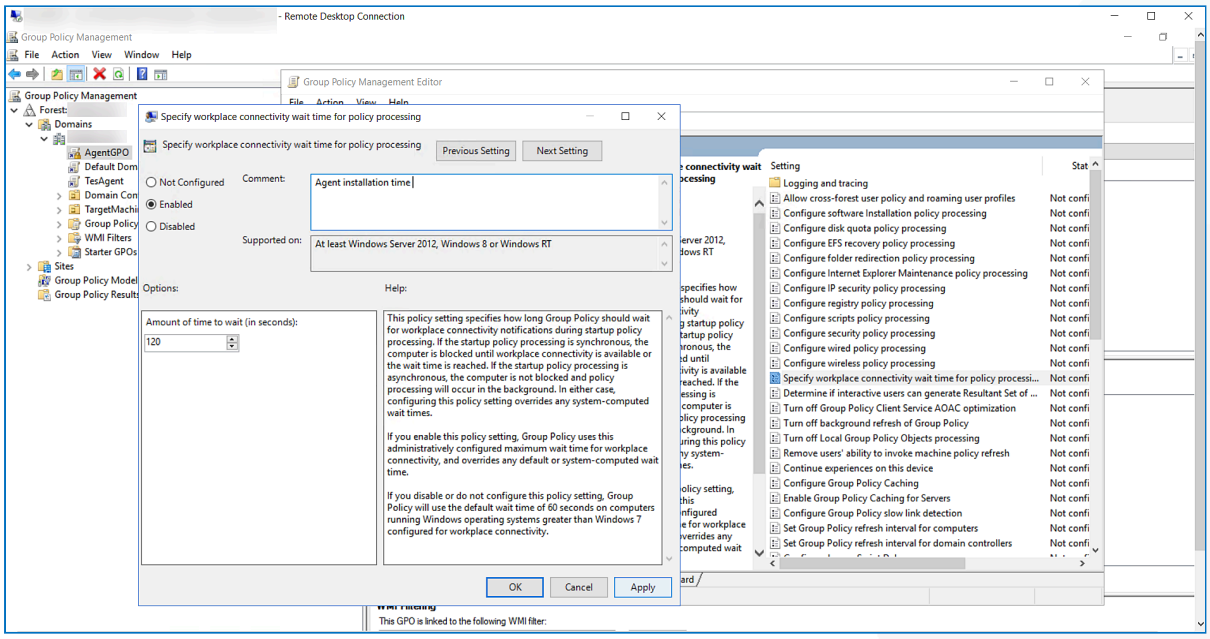



- Remote Desktop Connection
Group Policy Management
File Action View Window Help
Group Policy Management
Forest:
Domains
AgentGPO
Default Domain Policy
TesAgent
Domain Controllers
TargetMachines
Group Policy Objects
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Group Policy Management Editor
File Action View Help
System
Access-Denied Assistance
App-V
Audit Process Creation
Credentials Delegation
Device Guard
Device Installation
Device Redirection
Disk NV Cache
Disk Quotas
Distributed COM
Driver Installation
Early Launch Antimalware
Enhanced Storage Access
File Classification Infrastructure
File Share Shadow Copy Provider
Filesystem
Folder Redirection
Group Policy
Internet Communication Management
iSCSI
KDC
Kerberos
Locale Services
Logon
Mitigation Options
Net Logon
Power Management
Recovery
Remote Assistance
Remote Procedure Call
System
Select an item to view its description.
Setting
Stat
Extended
Standard
16 setting(s)
This GPO is linked to the following WMI filter:


- Remote Desktop Connection
Group Policy Management
File Action View Window Help
Group Policy Management
Forest:
Domains
AgentGPO
Default Domain Policy
TesAgent
Domain Controllers
TargetMachines
Group Policy Objects
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Group Policy Management Editor
File Action View Help
System
Access-Denied Assistance
App-V
Audit Process Creation
Credentials Delegation
Device Guard
Device Installation
Device Redirection
Disk NV Cache
Disk Quotas
Distributed COM
Driver Installation
Early Launch Antimalware
Enhanced Storage Access
File Classification Infrastructure
File Share Shadow Copy Provider
Filesystem
Folder Redirection
Group Policy
Internet Communication Management
iSCSI
KDC
Kerberos
Locale Services
Logon
Mitigation Options
Net Logon
Power Management
Recovery
Remote Assistance
Remote Procedure Call
Group Policy
Select an item to view its description.
Setting
Stat
Logging and tracing
Allow cross-forest user policy and roaming user profiles
Configure software Installation policy processing
Configure disk quota policy processing
Configure EFS recovery policy processing
Configure folder redirection policy processing
Configure Internet Explorer Maintenance policy processing
Configure IP security policy processing
Configure registry policy processing
Configure scripts policy processing
Configure security policy processing
Configure wired policy processing
Configure wireless policy processing
Specify workplace connectivity wait time for policy processi...
Determine if interactive users can generate Resultant Set of ...
Turn off Group Policy Client Service AOAC optimization
Turn off background refresh of Group Policy
Turn off Local Group Policy Objects processing
Remove users' ability to invoke machine policy refresh
Continue experiences on this device
Configure Group Policy Caching
Enable Group Policy Caching for Servers
Configure Group Policy slow link detection
Set Group Policy refresh interval for computers
Set Group Policy refresh interval for domain controllers
Not confi
Extended
Standard
54 setting(s)
This GPO is linked to the following WMI filter:



9. From this window, click the **Enabled** option. Enter the **Amount of time to wait** as 120 seconds and click **Apply** and **OK** to save the settings.

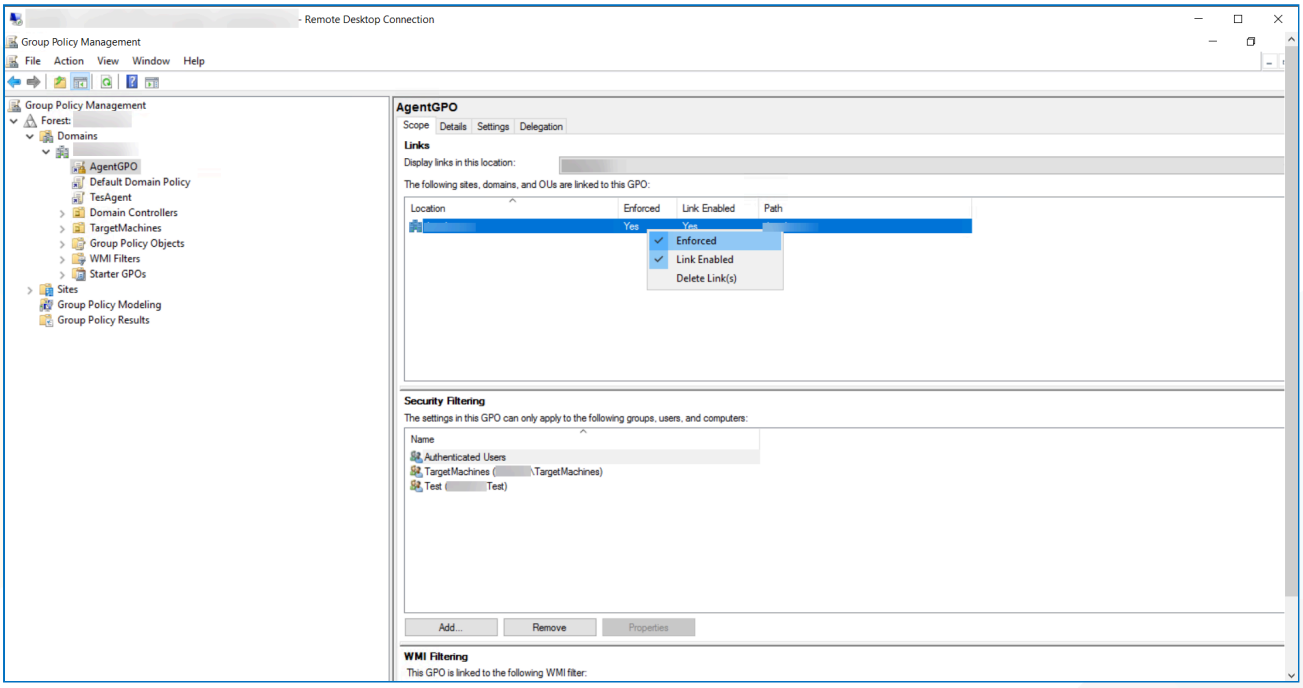


10. The GPO will be applied. Once you restart all the target endpoints, the PAM360 Agent PowerShell script will be invoked, and the agent will be installed in the target machines.
11. After the successful installation of the agent, disable the startup script for the GPO you created (AgentGPO in this example). This will ensure that the script is not invoked every time the target machines are restarted.

c. Troubleshooting Steps

Ensure that the AgentGPO has a higher precedence than the other GPOs. This is to make sure that the other GPOs do not override the permissions of the AgentGPO.

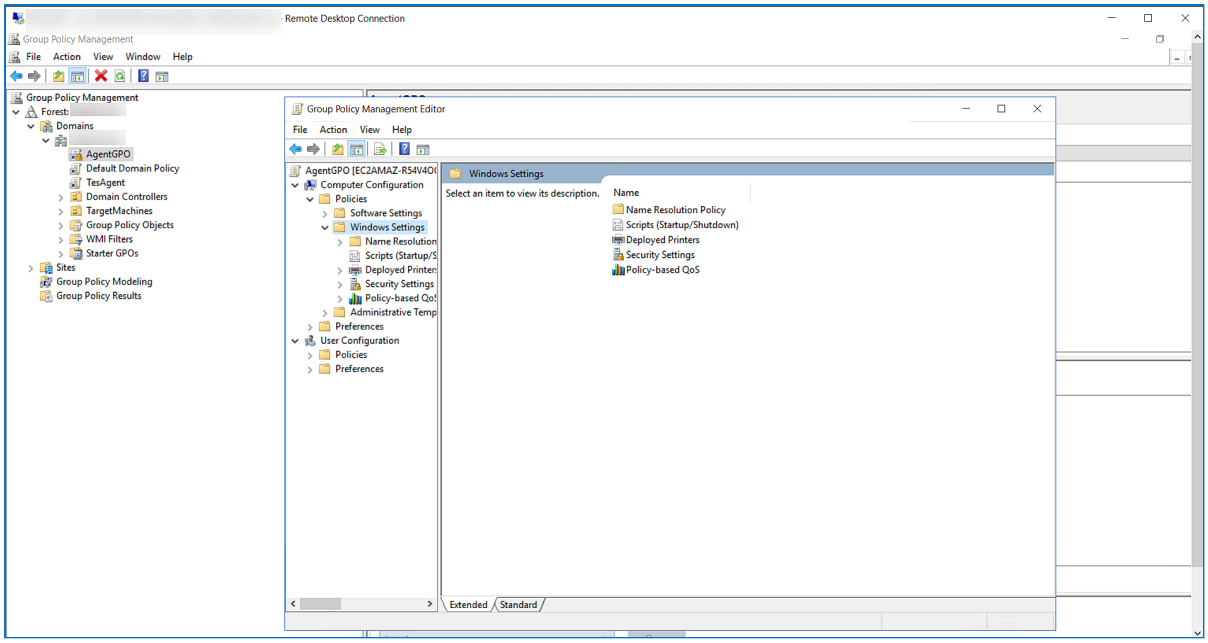
To check this, click the GPO name, right-click the **Enforced** option, and check if it is enabled.



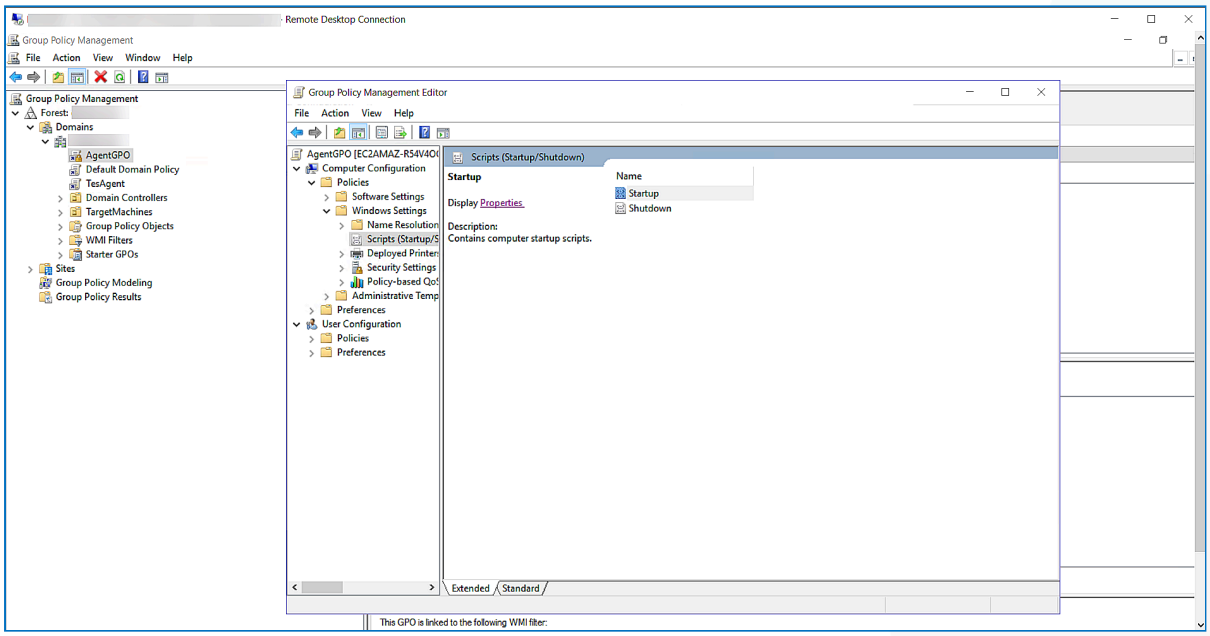
2. Uninstalling the PAM360 Agent via Windows Group Policy Objects (GPO)

a. Steps to Add the Uninstallation Script in the GPO

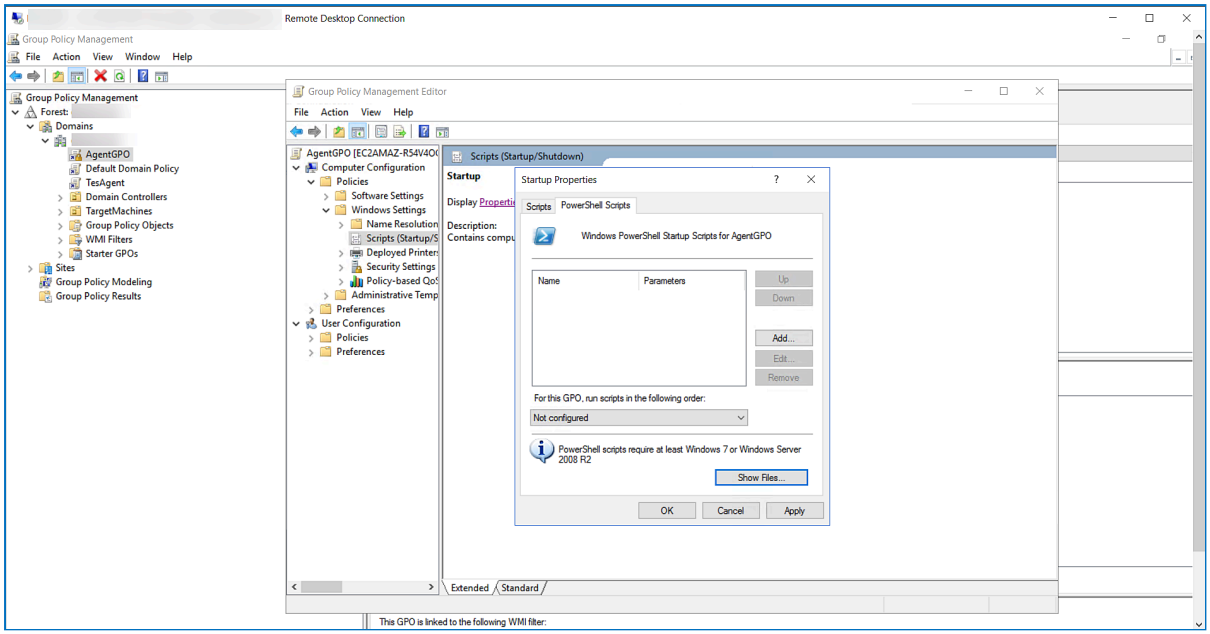
1. Right-click the name of the GPO you created from the left pane and click **Edit settings**, **delete**, **modify security**. The **Group Policy Management Editor** window will open.



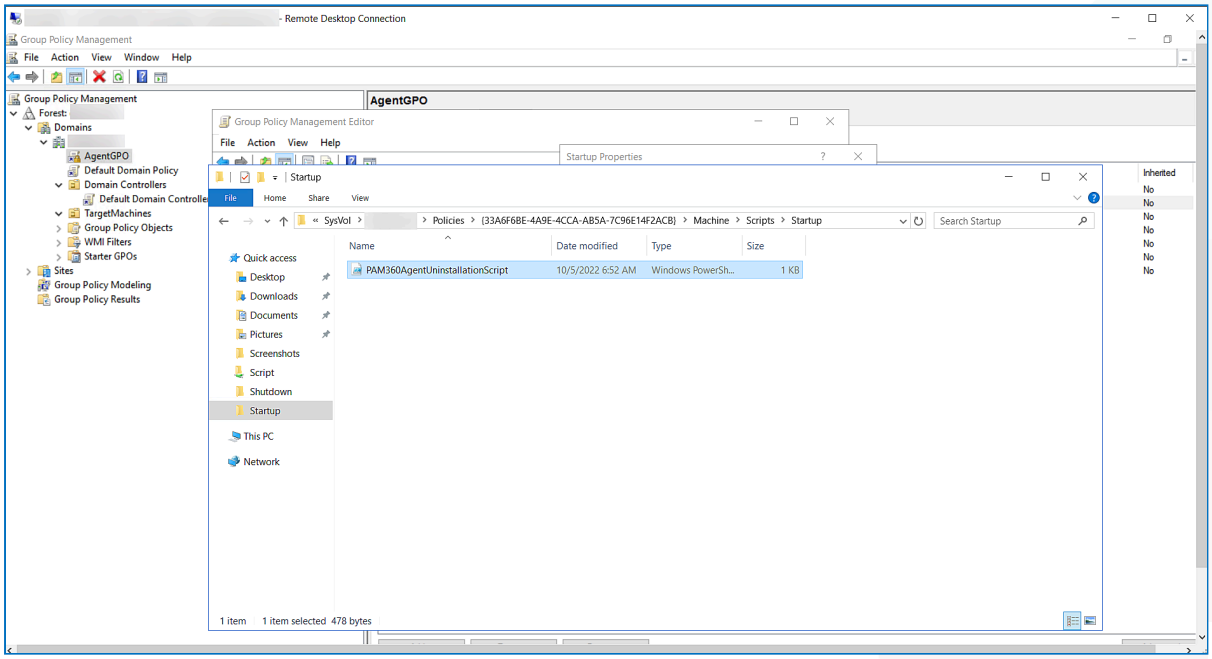
2. Navigate to the **Policies >> Windows Settings** folders and double-click the **Scripts**. In the Scripts window that opens, click **Startup** and then click **Properties**.

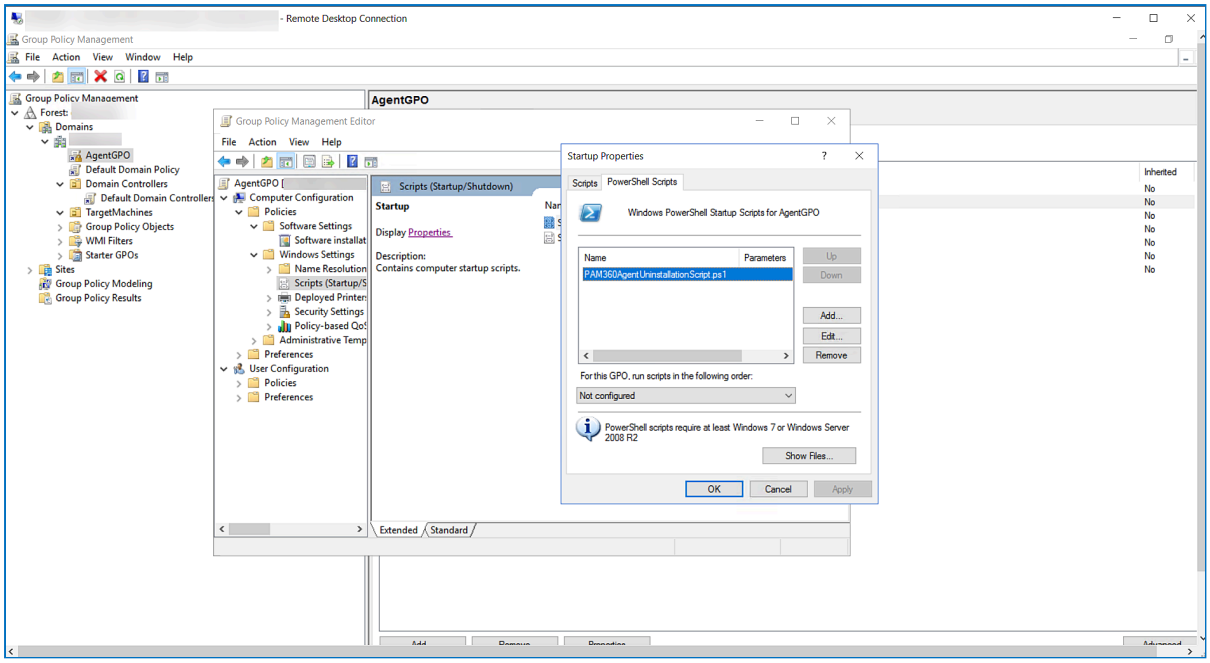


3. Switch to the **PowerShell Scripts** tab and click **Show Files**. The network directory will open.

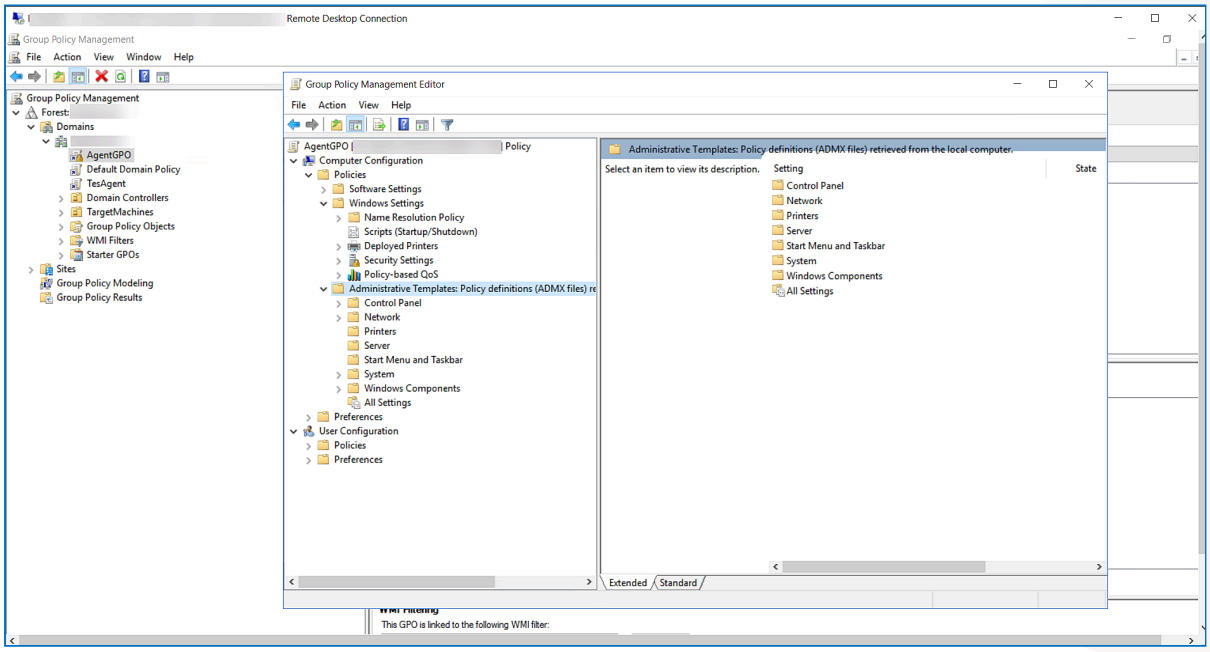


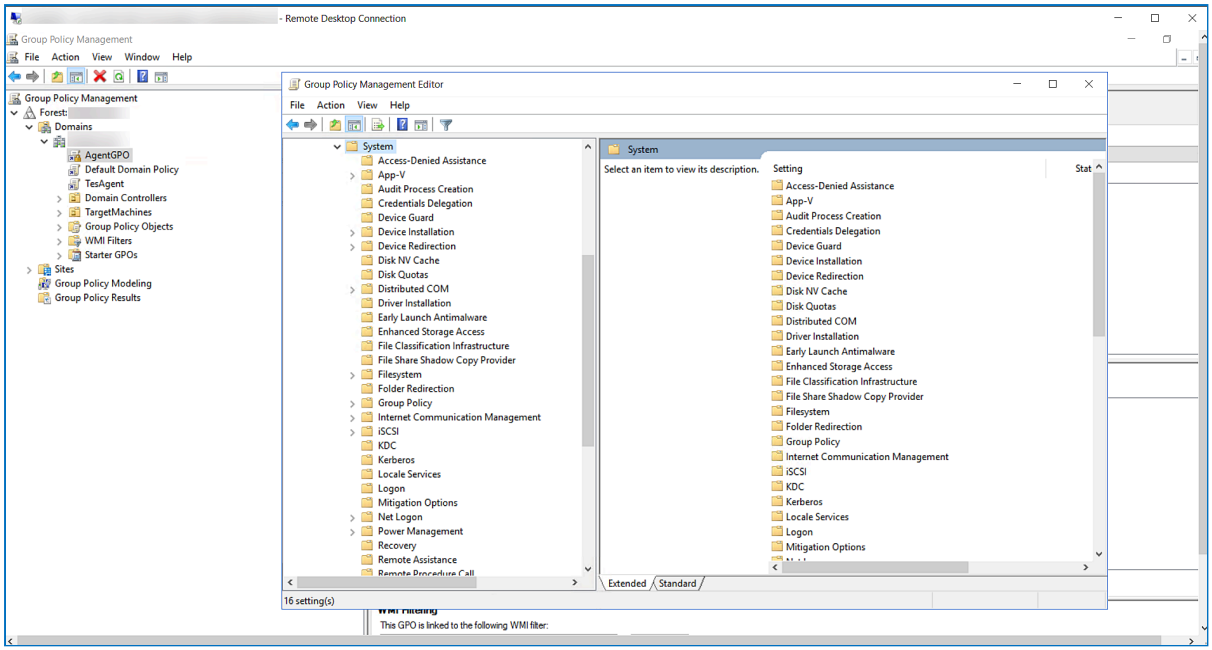
4. Now, paste the PAM360 agent Uninstallation PowerShell script file in the GPO network location.

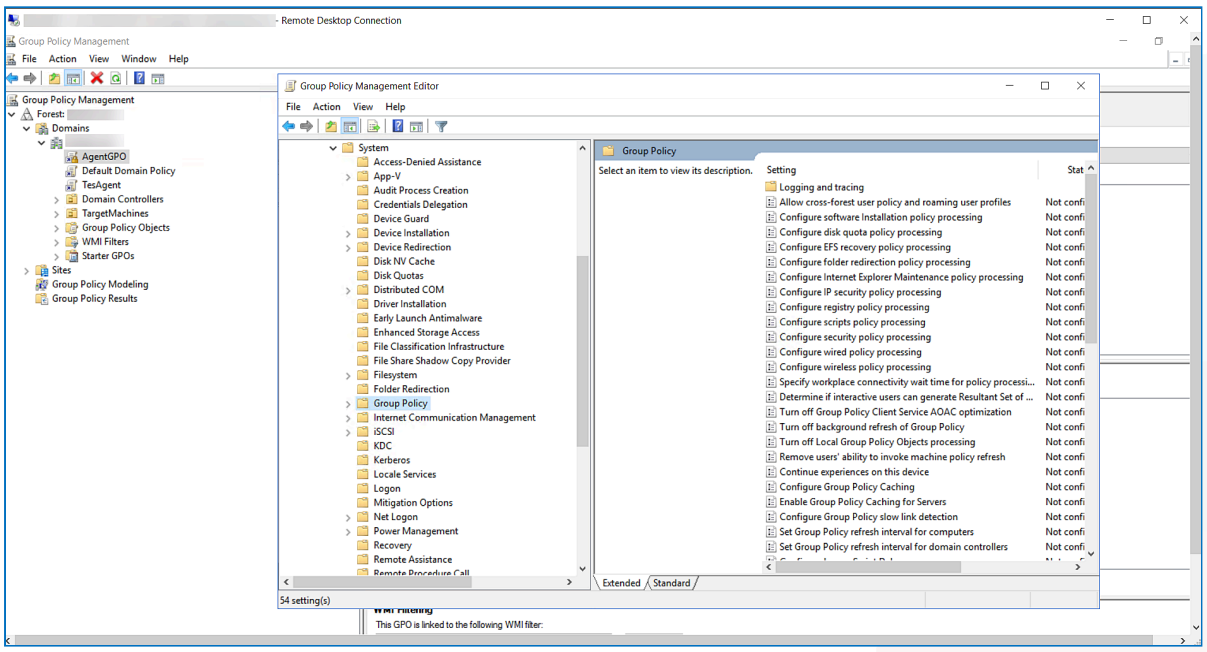


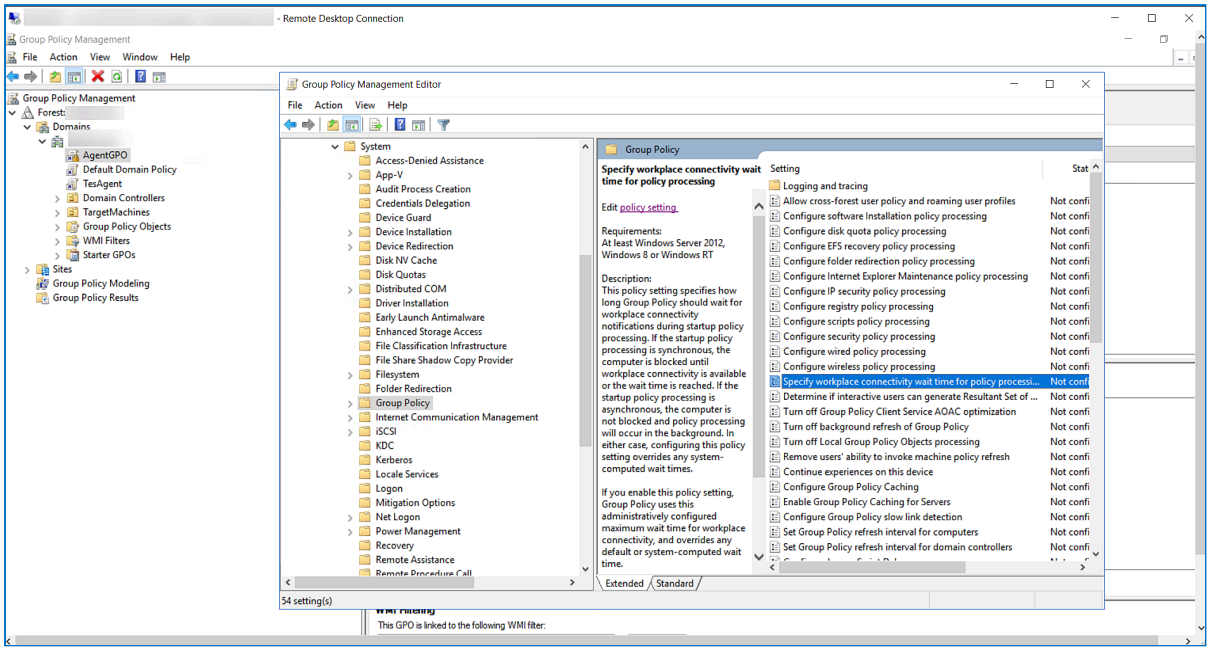


5. Click **Add** and add the PAM360AgentUninstallationScript file name under the **Script Name**. Click **Apply** and **OK** again to save the settings.
6. In the **Group Policy Management Editor**, navigate to **Administrative Templates >> System** and open the **Group Policy**.
7. Under the **Group Policy** folder, right-click **Specify workplace connectivity wait time for policy processing**.

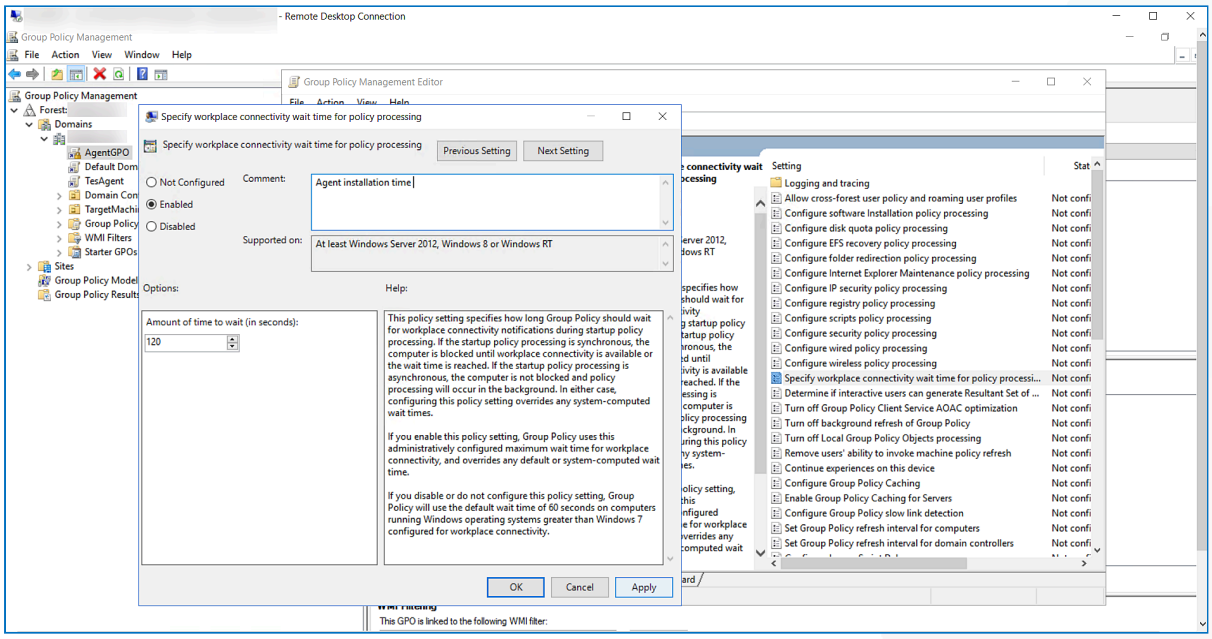



- Remote Desktop Connection
Group Policy Management
File Action View Window Help
Group Policy Management
Forest:
Domains
AgentGPO
Default Domain Policy
TesAgent
Domain Controllers
TargetMachines
Group Policy Objects
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Group Policy Management Editor
File Action View Help
System
Access-Denied Assistance
App-V
Audit Process Creation
Credentials Delegation
Device Guard
Device Installation
Device Redirection
Disk NV Cache
Disk Quotas
Distributed COM
Driver Installation
Early Launch Antimalware
Enhanced Storage Access
File Classification Infrastructure
File Share Shadow Copy Provider
Filesystem
Folder Redirection
Group Policy
Internet Communication Management
iSCSI
KDC
Kerberos
Locale Services
Logon
Mitigation Options
Net Logon
Power Management
Recovery
Remote Assistance
System
Select an item to view its description.
Setting
Extended
Standard
16 setting(s)
This GPO is linked to the following WMI filter:


- Remote Desktop Connection
Group Policy Management
File Action View Window Help
Group Policy Management
Forest:
Domains
AgentGPO
Default Domain Policy
TesAgent
Domain Controllers
TargetMachines
Group Policy Objects
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Group Policy Management Editor
File Action View Help
System
Access-Denied Assistance
App-V
Audit Process Creation
Credentials Delegation
Device Guard
Device Installation
Device Redirection
Disk NV Cache
Disk Quotas
Distributed COM
Driver Installation
Early Launch Antimalware
Enhanced Storage Access
File Classification Infrastructure
File Share Shadow Copy Provider
Filesystem
Folder Redirection
Group Policy
Internet Communication Management
iSCSI
KDC
Kerberos
Locale Services
Logon
Mitigation Options
Net Logon
Power Management
Recovery
Remote Assistance
Group Policy
Select an item to view its description.
Setting
Logging and tracing
Allow cross-forest user policy and roaming user profiles
Configure software Installation policy processing
Configure disk quota policy processing
Configure EFS recovery policy processing
Configure folder redirection policy processing
Configure Internet Explorer Maintenance policy processing
Configure IP security policy processing
Configure registry policy processing
Configure scripts policy processing
Configure security policy processing
Configure wired policy processing
Configure wireless policy processing
Specify workplace connectivity wait time for policy processi...
Determine if interactive users can generate Resultant Set of ...
Turn off Group Policy Client Service AOAC optimization
Turn off background refresh of Group Policy
Turn off Local Group Policy Objects processing
Remove users' ability to invoke machine policy refresh
Continue experiences on this device
Configure Group Policy Caching
Enable Group Policy Caching for Servers
Configure Group Policy slow link detection
Set Group Policy refresh interval for computers
Set Group Policy refresh interval for domain controllers
Not confi
Extended
Standard
54 setting(s)
This GPO is linked to the following WMI filter:



8. From this window, click the **Enabled** option. Enter the **Amount of time to wait** as 120 seconds. Click **Apply** and **OK** to save the settings.



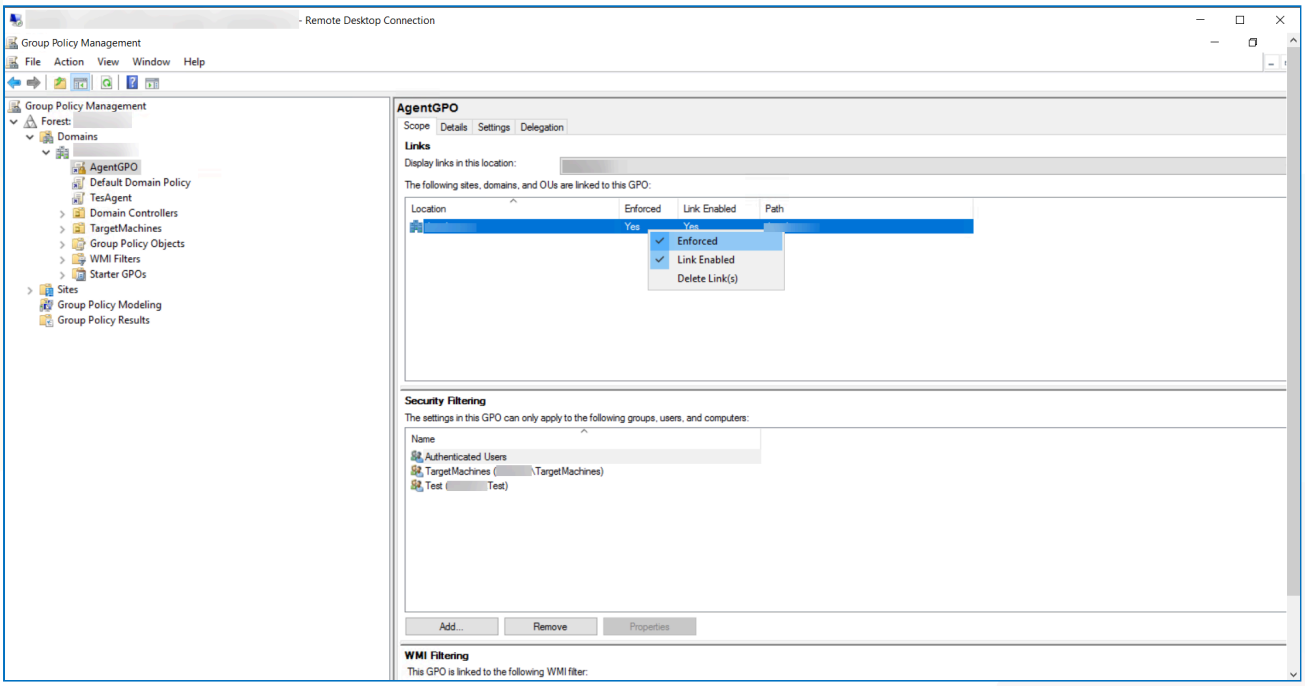
9. The GPO will be applied. Once you restart all the target endpoints, the PAM360 Agent PowerShell script will be invoked and the agent will be uninstalled in the target machines.
10. After successful uninstallation, disable the startup script for the GPO you created (AgentGPO in this example). This will ensure that the script is not invoked every time the target machines are restarted.

Once you have uninstalled the old agents, follow the steps in this link to install the C#/Go agent using GPO.

b. Troubleshooting Steps

Ensure that the AgentGPO has a higher precedence than the other GPOs. This is to make sure that the other GPOs do not override the permissions of the AgentGPO.

To check this, click the GPO name, right-click the **Enforced** option and check if it is enabled.



Deploying PAM360 Agent in Endpoints using Endpoint Central

Endpoint Central (formerly Desktop Central) is a Windows Desktop Management solution that allows users to deploy software, patch management, configurations, etc. PAM360 now allows users to install and uninstall PAM360 Agent in bulk using Endpoint Central.

Prerequisite: Download the agent installation script zip accordingly and extract the support script files for bulk installation:

- For agent file as a zip, download the ECAgentScript.zip and ensure the SHA256 value:
  b61f52a1cc213ba69dc7a369074d5d294247954f78110f049483805bde10958a
- For agent file as an exe, download the ECAgentScript-7500.zip and ensure the SHA256 value:
  8ac30b03a5a04b934df7e4e9570e2b2c48db7f8292b31cf57f716cbb7bfb7ad1

1. Installing PAM360 Agent using Endpoint Central

Follow the below steps to install the PAM360 agent in bulk using Endpoint Central:

a. Upload a script file in the Endpoint Central
b. Create a collection and deploy

a. Upload a Script File in the Endpoint Central

1. To begin the PAM360 agent installation process, log in to PAM360 and navigate to **Admin >> PAM360 Agents**. Download the **Windows Agent** (.zip or .exe) and ensure to copy the **Agent Key** value.
2. From the extracted agent script file folder, take the following steps in the respective files based on your agent installation type:
   a. For resource agent installation, open the **ResourceAgentBulkInstallation.bat** file with administrative privileges. Update the following attributes:

i. Enter your PAM360 **Agent Key**.

ii. Input the numbers next to the **Agent Key** based on the desired services. Use **1, 2,3** to indicate the agent installations for **Password Management**, **Self-Service Privilege Elevation**, and **Zero Trust Implementation**. Installation scenarios can include **1,2,3** or **1** or **2** or **3** or **1,2** or **1,3** or **2,3**. For example:

```
AgentInstaller.exe install  275b68f389c09c70g 1,2,3
```

b. For user agent installation, open the **UserAgentBulkInstallation.bat** file with administrative privileges. Update the following attributes:

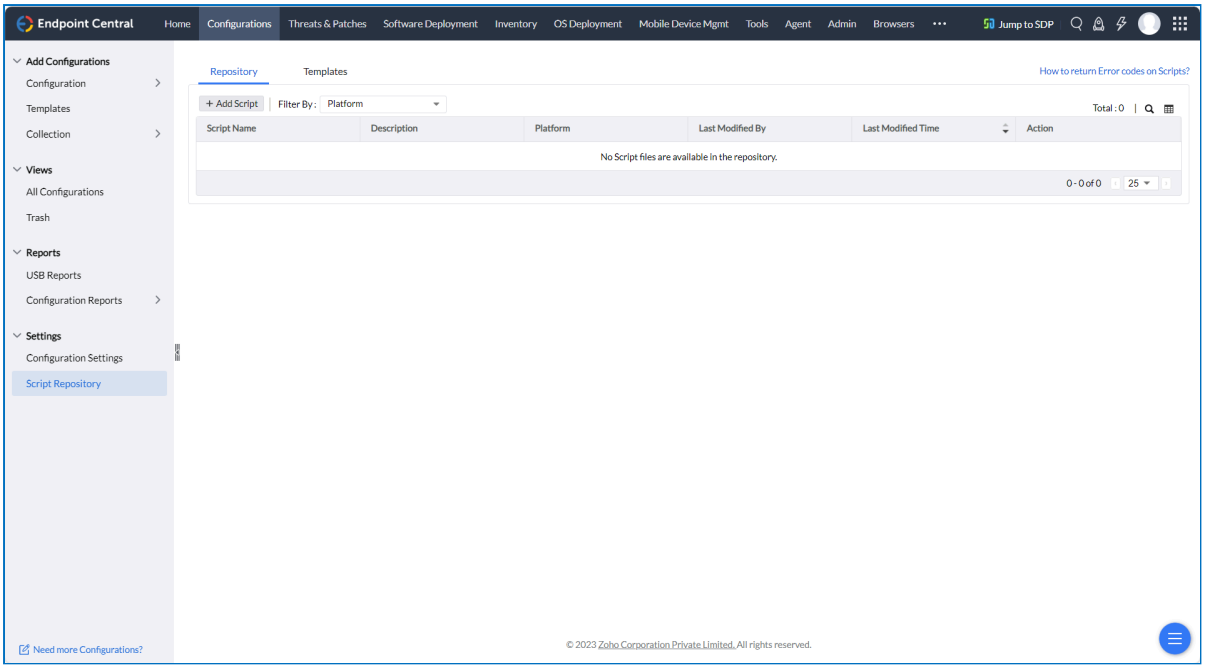
i. Enter the user machine names where the user agent to be installed along with the respective PAM360 user names to establish a mapping for trust score calculation in Zero Trust.

Note: Ensure that the machine names used by the user and the PAM360 usernames are identical, including case-sensitive words.

ii. Enter your PAM360 **Agent Key**. For example:

```
set input_string=johndoe-266=John Doe,emilydavis-451=Emily Davis,ashley-094=Ashley Taylor,Chirs-650=Chris Williams
.
.
.
AgentInstaller.exe install 275b68f389c09c70g userdevice %result%
```

3. Log in to **Endpoint Central** and navigate to '**Configurations >> Settings >> Script Repository**'.



4. Click **+ Add Script**.

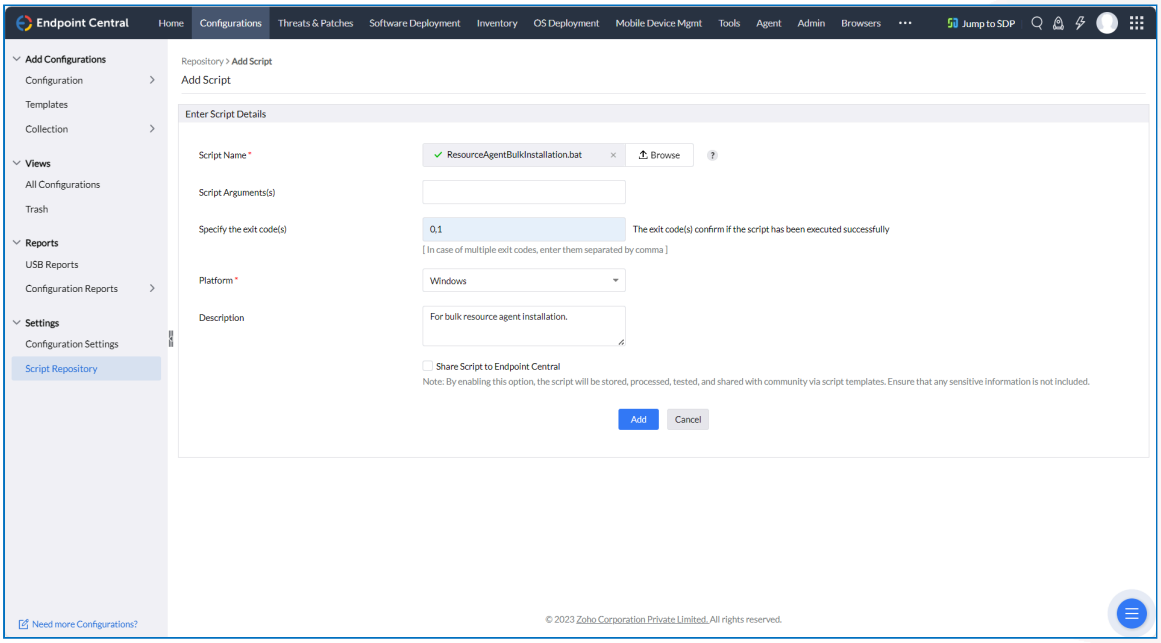
   i. Click **Browse** under **Script Name** and upload the following file as required:

      a. **ResourceAgentBulkInstallation.bat** - For bulk resource agent installation

      b. **UserAgentBulkInstallation.bat** - For bulk user agent installation

   ii. Now, **Specify the exit code(s)** as **0,1**.

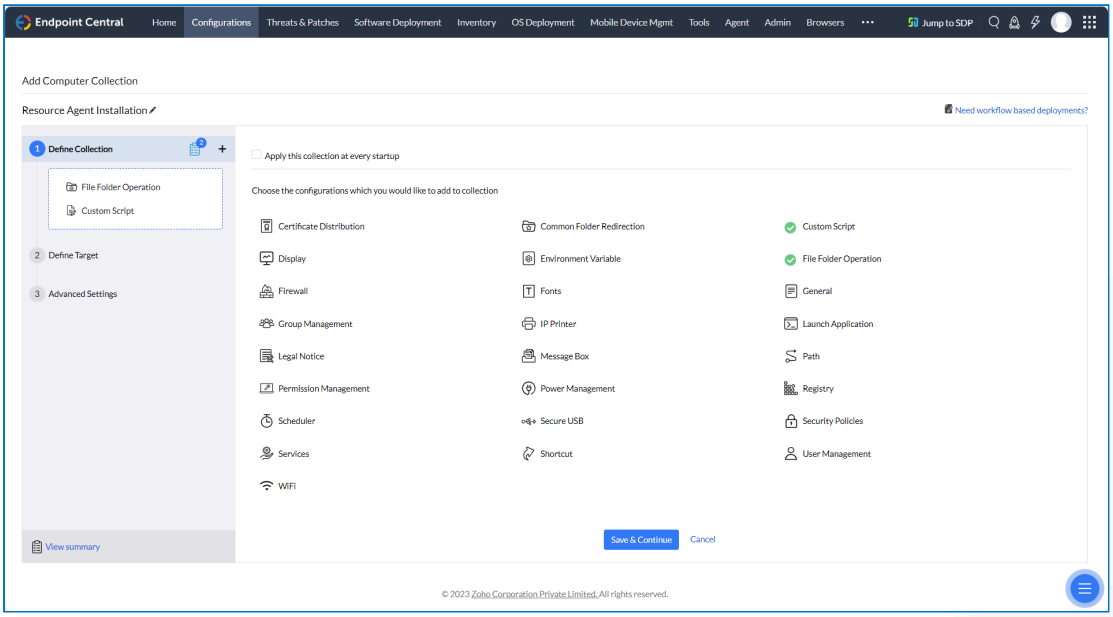
   iii. Select the **Platform** as **Windows** and click **Add**.



5. Now, you have successfully uploaded a script file to **Endpoint Central**.

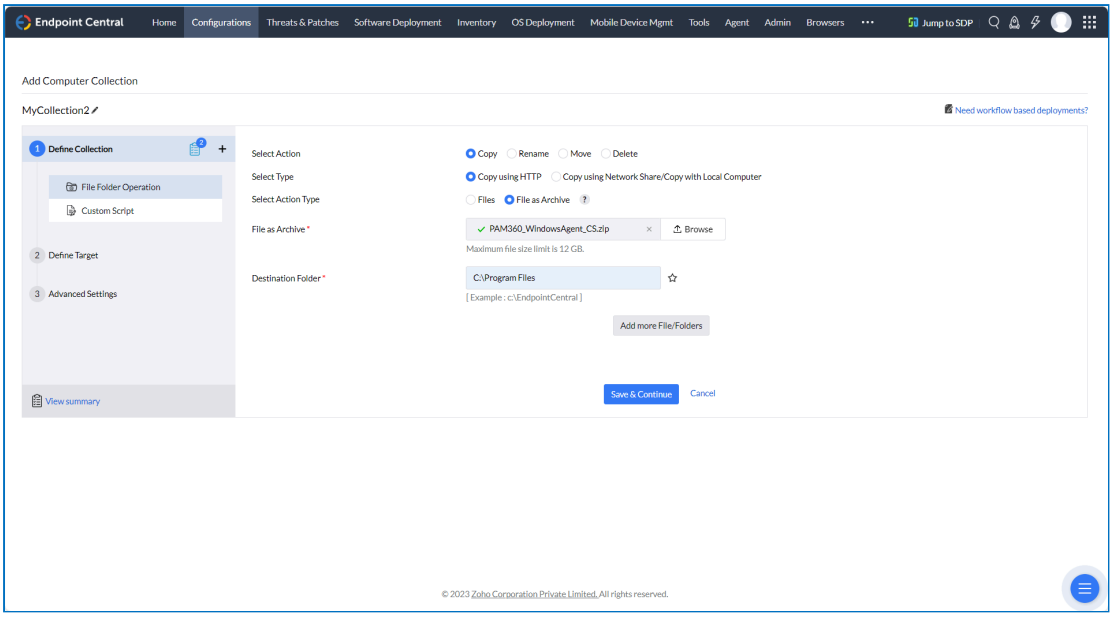
b. Create a Collection

1. In **Endpoint Central**, navigate to '**Configurations >> Add Configurations >> Collections >> Computer Collections**'.
2. In the GUI that appears, edit the name of the collection and do the steps that follow:
   - **i.** In **Define Collection**,
     a. Select **Custom Script** and **File Folder Operation.**



     b. Now, under **Define Collection** on the left, click **File Folder Operation**.
     c. **Browse** and upload the downloaded **WindowsAgent.zip** or **PAM360AgentInstaaller..exe** in the **Files** field.
     d. Enter the **Destination Folder** file path (*E.g., "C:\Program Files (*86)"*) to unzip, and click **Save & Continue**.

     Notes: For agent file as zip, kindly make sure that the **Destination Folder** file path mentioned is the same as that of the path mentioned in the **Agent.bat** file. From build 7500 onwards, for agent file as .exe, the PAM360 agent installer files will be unpacked on the default destination folder - **C:\Program Files (x86)\ManageEngine\PAM360AgentInstaller**. Manually changing this destination folder is restricted and prevents the agent from being installed.



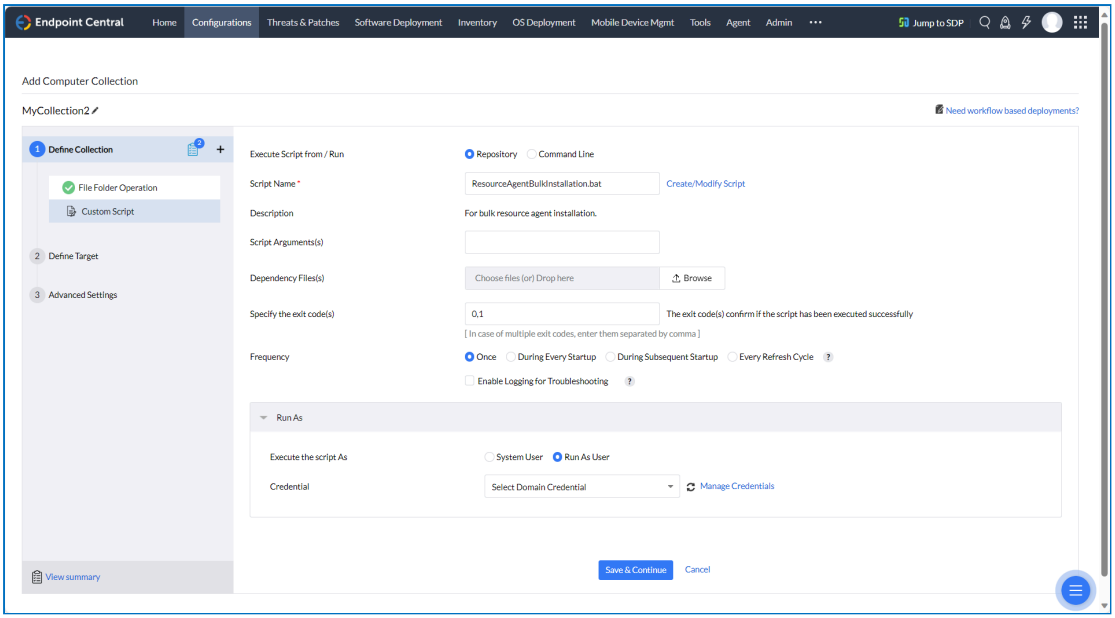
e. Now, under **Custom Scripts**, select **Repository** in the **Execute Script from/Run** field.

f. Search and select **ResourceAgentBulkInstallation.bat** or **UserAgentBulkInstallation.bat** (uploaded in step 1) as the **Script Name**.

g. **Specify the exit code(s)** as **0,1** and enable the **Enable Logging for Troubleshooting** checkbox.

h. Under **Run As**, select the **Execute the Script** field with **Run as User** and mention the credentials of the domain account with relevant permissions.

i. Click **Save and Continue**.



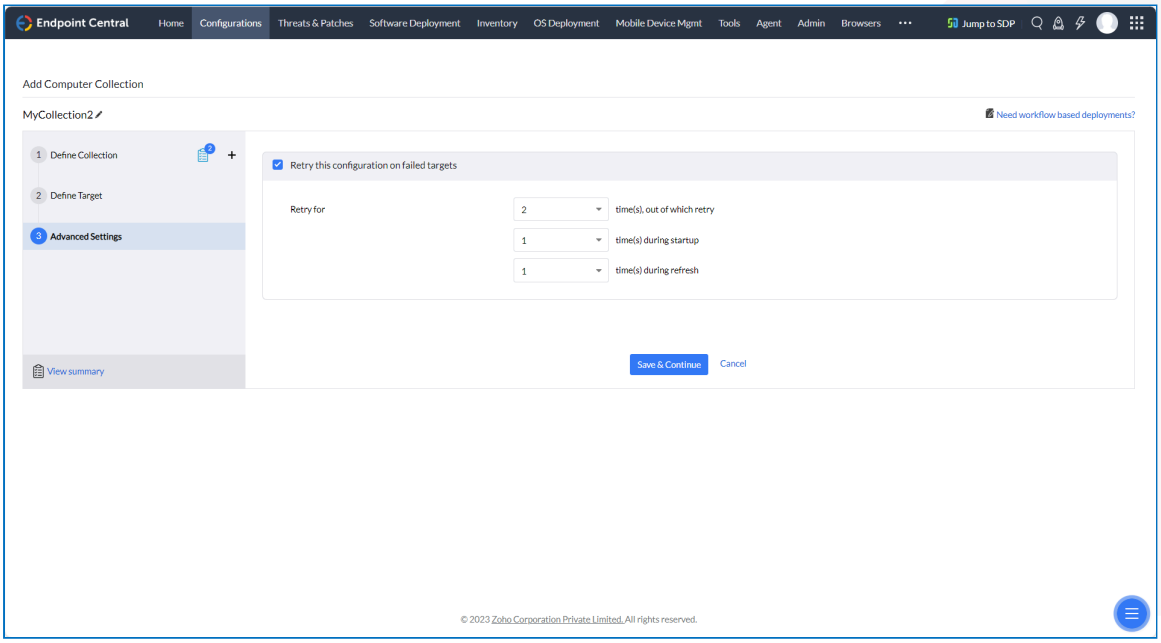
ii. Now, under **Define Target**,

a. Select the required **Remote Office/Domain** from the dropdown.

b. Click the filter icon and under **Filter Computers based on**, select **Computer** and select the desired machine.

c. Click **Save and Continue**.

iii. Under **Advanced Settings**, enable **Retry this configuration on failed targets** and click **Save and Continue** to deploy.



3. Now, you have successfully deployed the PAM360 Agent using Endpoint Central.

To check the status of your deployment, navigate to '**Configuration >> Views >> All Configuration**'.

2. Uninstalling PAM360 Agent using Endpoint Central

Follow the below steps to uninstall the PAM360 agent in bulk using Endpoint Central:

a. Upload a script file in the Endpoint Central
b. Create a collection and deploy

a. Upload a Script File in the Endpoint Central

1. Log in to **Endpoint Central** and navigate to '**Configurations >> Settings >> Script Repository**'.
2. Click **Add Script**.
   i. Click **Browse** under **Script Name** and upload the **UninstallAgent.bat** file available from the extracted script files zip.
   ii. Now, **Specify the exit code(s)** as **0,1**.
   iii. Select the **Platform** as **Windows** and click **Add**.
3. Now, you have successfully uploaded a script file to **Endpoint Central**.

b. Create a Collection

1. In **Endpoint Central**, navigate to '**Configurations >> Add Configurations >> Collections >> Computer Collections**'.
2. In the GUI that appears, edit the name of the collection and do the steps that follow:
   i. In **Define Collection**,
      a. Select **Custom Script**.
      b. Now, under **Custom Scripts** on the left, select **Repository** in the **Execute Script from/Run** field.
      c. Search and select **UninstallAgent.bat** (uploaded in step 1) as the **Script Name**.
      d. **Specify the exit code(s)** as **0,1** and enable the **Enable logging for**

Troubleshooting checkbox.

e. Click **Save and Continue**.

ii. Now, under **Define Target**,

a. Select the required **Remote Office/Domain** from the dropdown.

b. Click the filter icon and under **Filter Computers based on**, select **Computer** and select the desired machine.

c. Click **Save and Continue**.

iii. Under **Advanced Settings**, enable **Retry this configuration on failed targets** and click **Save and Continue** to deploy.

3. Now, you have successfully uninstalled the PAM360 Agent using Endpoint Central.

ManageEngine

280,000 organizations across 190 countries trust ManageEngine to manage their IT

4141 Hacienda Drive Pleasanton,
CA 94588, USA

US : +1 888 204 3539
UK : +44 (20) 35647890
Australia : +61 2 80662898

ManageEngine
PAM360

pam360-support@manageengine.com

Toll Free : +1 888 720 9500