





Guide to integrate

the ADSelfService Plus **login agent** with
third-party Winlogon extensions



Contents

Introduction	1
ADSelfService Plus login agent	1
Support for 3rd-party credential providers	2
Steps for bulk configuration via Group Policy	4
 Create a Group Policy Object	4
 Configure script settings to run ReinstallAgent.vbs at startup	6
 Configure Administrative Templates settings	13
 Apply the GPO	16
Troubleshooting tips	19

Introduction

ADSelfService Plus is an identity security solution that provides secure, seamless access to enterprise resources and facilitates workforce self-service. With ADSelfService Plus, end users can:

- 👉 Secure endpoint ([machine](#), [VPN](#), and [OWA](#)) logins and cloud application logins using adaptive MFA.
- 👉 Access multiple cloud applications seamlessly in a single click using SSO.
- 👉 Perform self-service [password resets](#) and [account unlocks](#).
- 👉 Synchronize [AD passwords](#) across all cloud applications in real time through the Password Sync Agent.
- 👉 Receive [password and account expiration notifications](#).
- 👉 Integrate, secure, audit, and improve the flexibility of [ITSM](#), [SIEM](#), and [IAM](#) tools.
- 👉 Update directory information and search the corporate or employee directories.

ADSelfService Plus login agent

When installed, the ADSelfService Plus login agent can enable MFA for local and remote machine logins as well as User Account Control prompts to protect machines from credential-based attacks. It also adds a button labeled **Reset Password / Unlock Account** to the native Windows login screen, allowing users to reset their passwords and unlock their accounts right from that screen.

The ADSelfService Plus login agent is an extension of the standard credential provider from Microsoft. Such credential provider extensions are now widely used by third-party software providers to offer a wide range of capabilities, like secure VPN access and full-disk encryption. However, some of these extensions may not be compatible with others, which limits the features that can be added to the Windows login screen.

The ADSelfService Plus login agent can be configured to work with your third-party credential provider extension. Below are some of the third-party credential providers supported by ADSelfService Plus:

- 👉 ZENworks Endpoint Security Agent
- 👉 Parallels Client
- 👉 Toshiba Logon Provider
- 👉 Cisco NAC Agent
- 👉 OneX Credential Provider
- 👉 RSA SecurID

Note: You need to configure the Windows Registry settings to make the ADSelfService Plus login agent compatible with the credential providers above. Please click [here](#) for the configuration steps. Additionally, by editing the Windows Registry settings, more third-party credential providers can be made compatible with the ADSelfService Plus login agent.

This document will provide you with all the information you need to seamlessly integrate the ADSelfService Plus login agent with your third-party credential provider extension.

Before installing the login agent, ensure that these prerequisites are met:

Prerequisites

1. ADSelfService Plus with Endpoint MFA is required to enable MFA for Windows logins. For more details, please contact sales@manageengine.com.
2. The ADSelfService Plus Professional edition is required to enable self-service password reset and account unlock on Windows login screens.
3. A valid SSL certificate must be installed in ADSelfService Plus, and the Access URL must be configured to use the HTTPS protocol. For the steps to do this, refer to [this guide](#).

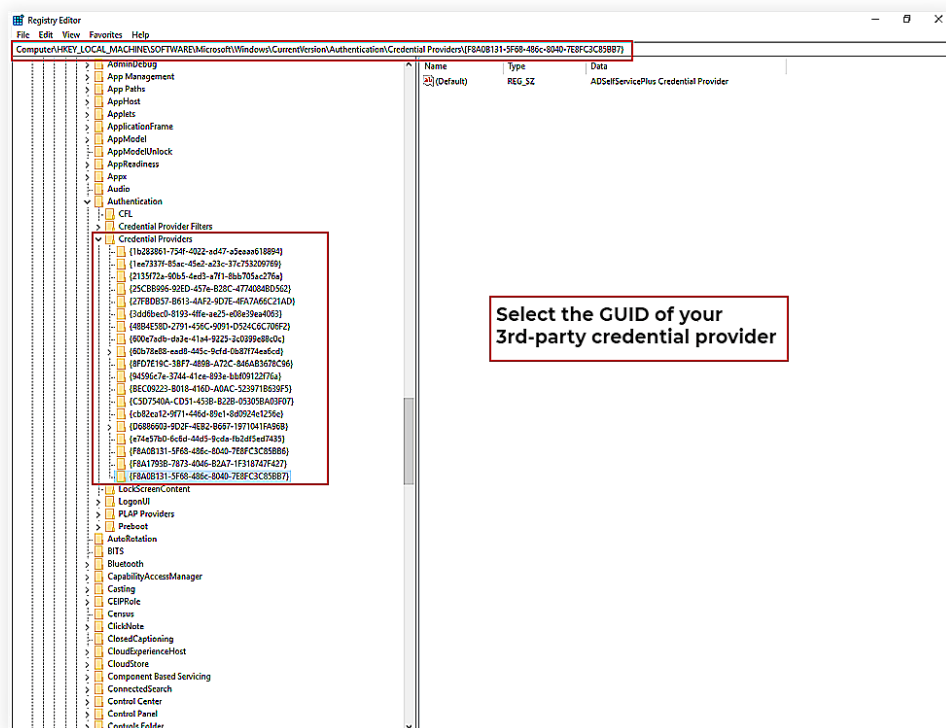
Support for third-party credential providers

Important note: Care must be taken before making any changes to Windows Registry. Make sure that you have backed up your Registry settings before proceeding further.

If the ADSelfService Plus login agent has not been installed yet, follow the steps given below:

1. Open the **Registry Editor** (open **Run** > type **regedit** and click **OK**).
2. Get the unique **global unique identifier** of your third-party Credential Provider from the registry key given below:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers



3. Use that GUID in the command shown below during the installation of the ADSelfService Plus login agent:

```
msiexec /i ADSelfServicePlusClientSoftware.msi
SERVERNAME=abc.selfservice.com" PORTNO="443" PROTOCOL="https"
INSTALLATION_KEY="19d82629b4e540fc873df8775d3630cb" WRAPPINGPROVIDER="
{<enter the GUID of your third-party GINA/CP extension>}"
```

Alternatively, if you have already installed the ADSelfService Plus login agent and plan to deploy a third-party credential provider in your environment, then follow the steps given below:

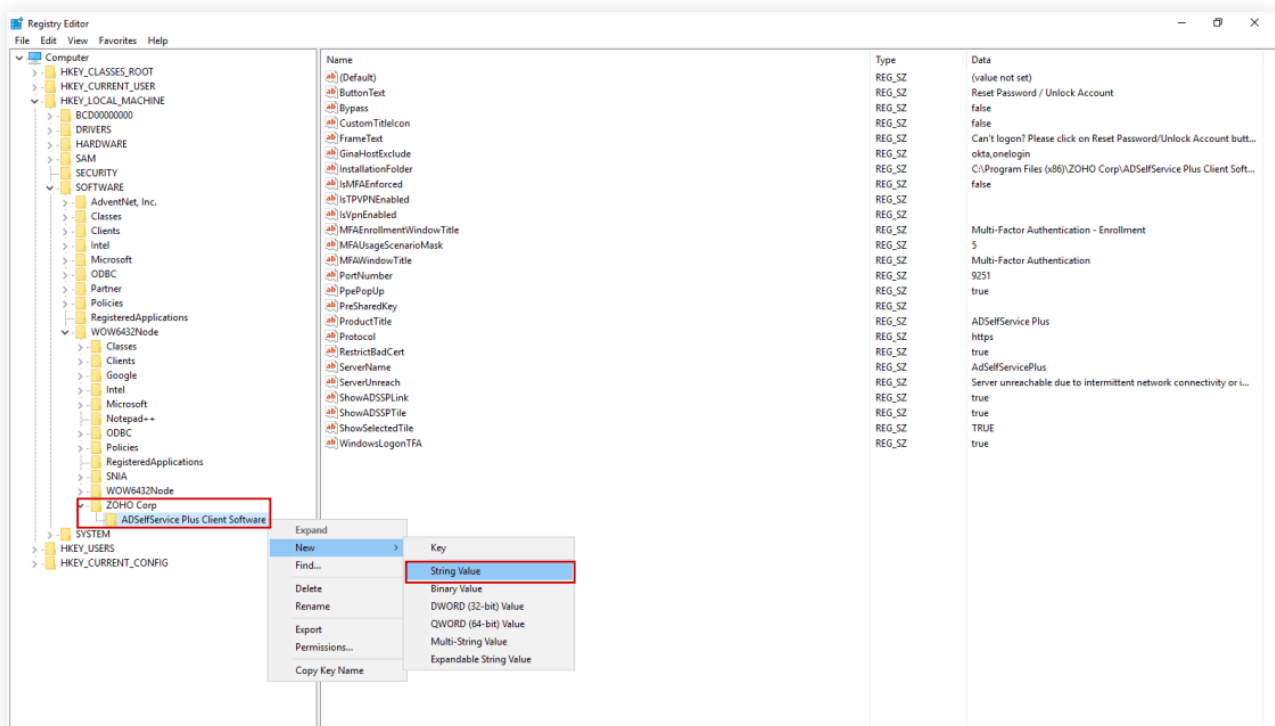
1. Open **Registry Editor** (open **Run**, type **regedit**, and click **OK**).
2. Navigate to **ADSelfService Plus Client Software > New > String Value** and create a new **String Value** called **WrappingProvider** in the following registry key:

For 32-bit machines

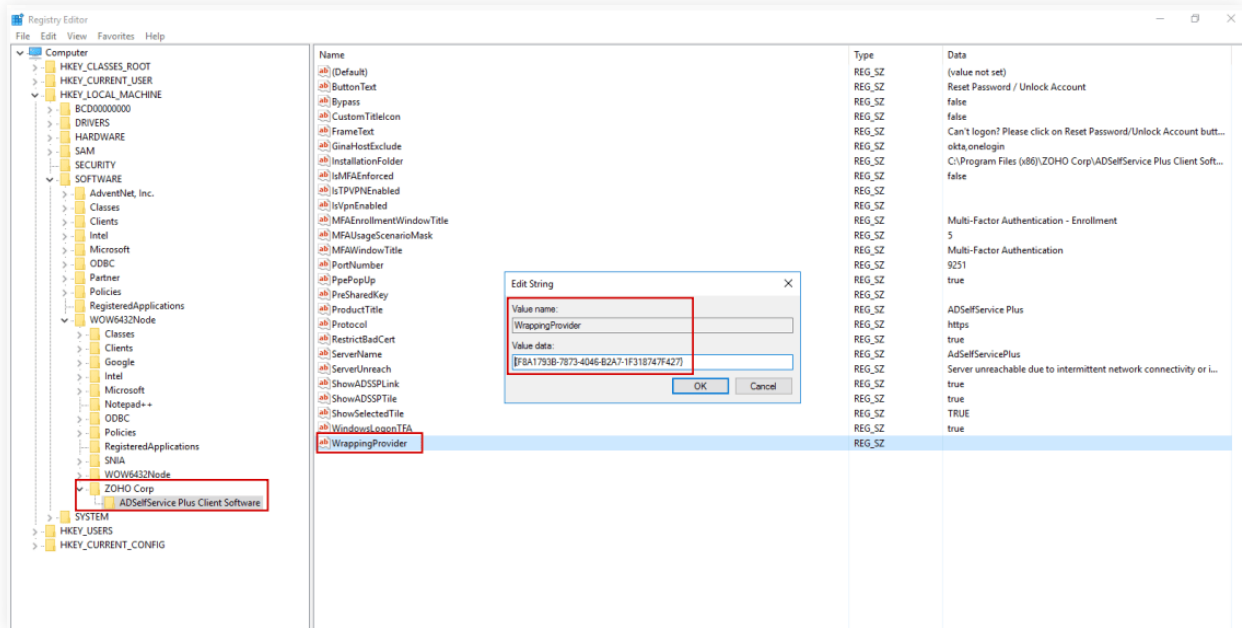
HKEY_LOCAL_MACHINE\SOFTWARE\ZOHOCorp\ADSelfService Plus Client Software

For 64-bit machines

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ZOHOCorp\ADSelfService Plus Client Software



3. Provide the GUID of your third-party credential provider as its value.



Steps for bulk configuration via Group Policy

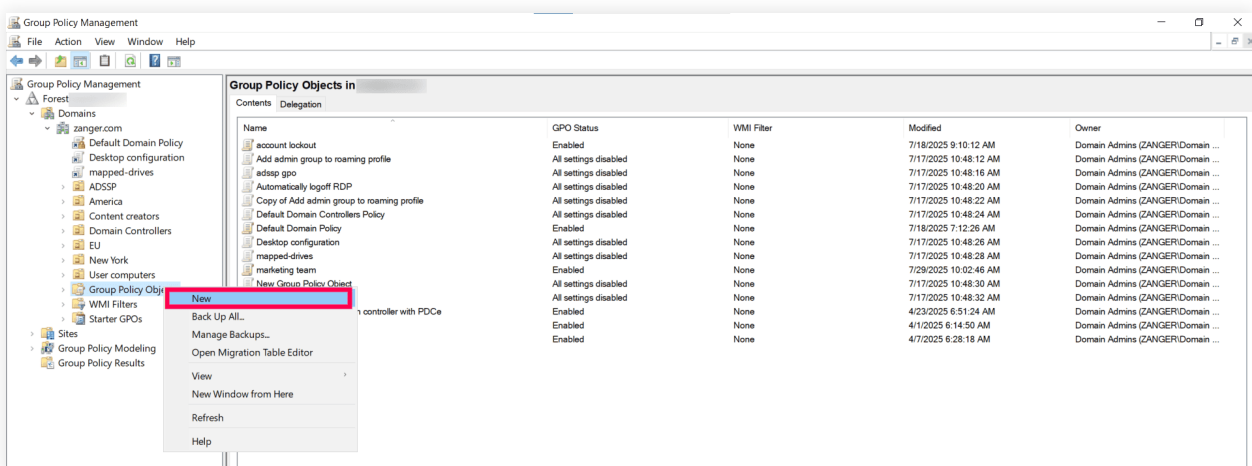
In a large IT environment, configuring credential providers individually for each machine is not feasible. In such cases, you can follow the bulk configuration steps given below to make your third-party credential providers compatible with the ADSelfService Plus login agent.

STEP 1 Create a Group Policy Object

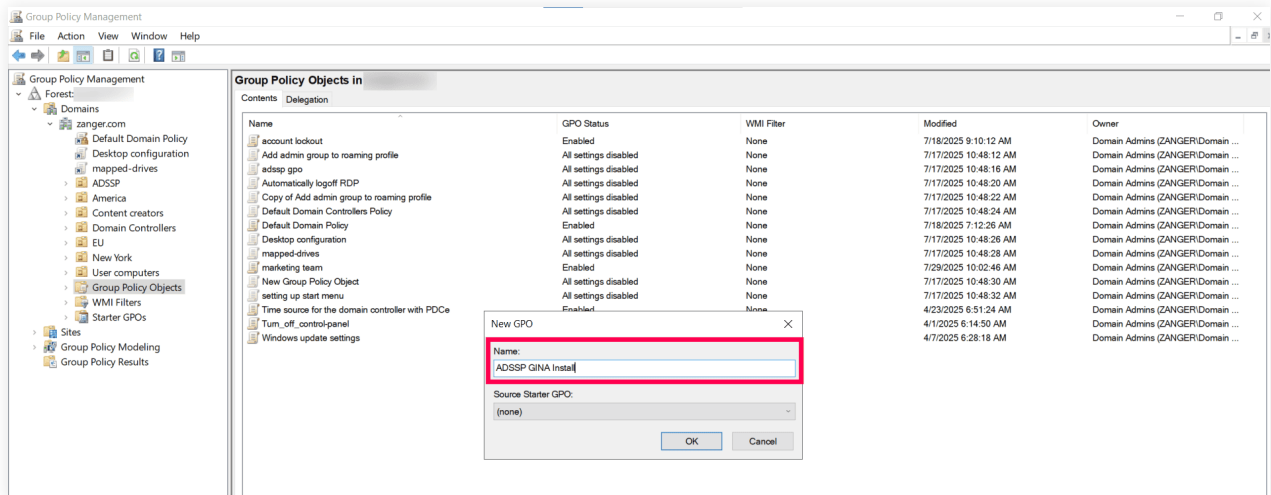
First, you have to create a new Group Policy Object (GPO). The GPO will be configured to run ConfigureCP.bat and will be applied to the group containing Windows Server machines running version 2008 and above and client machines running version Vista and above. Follow the steps given below to create a GPO:

For Windows Server 2008 and above

1. Open the **Group Policy Management** console.
2. On the left pane, right-click the **Group Policy Objects** container and select **New**.

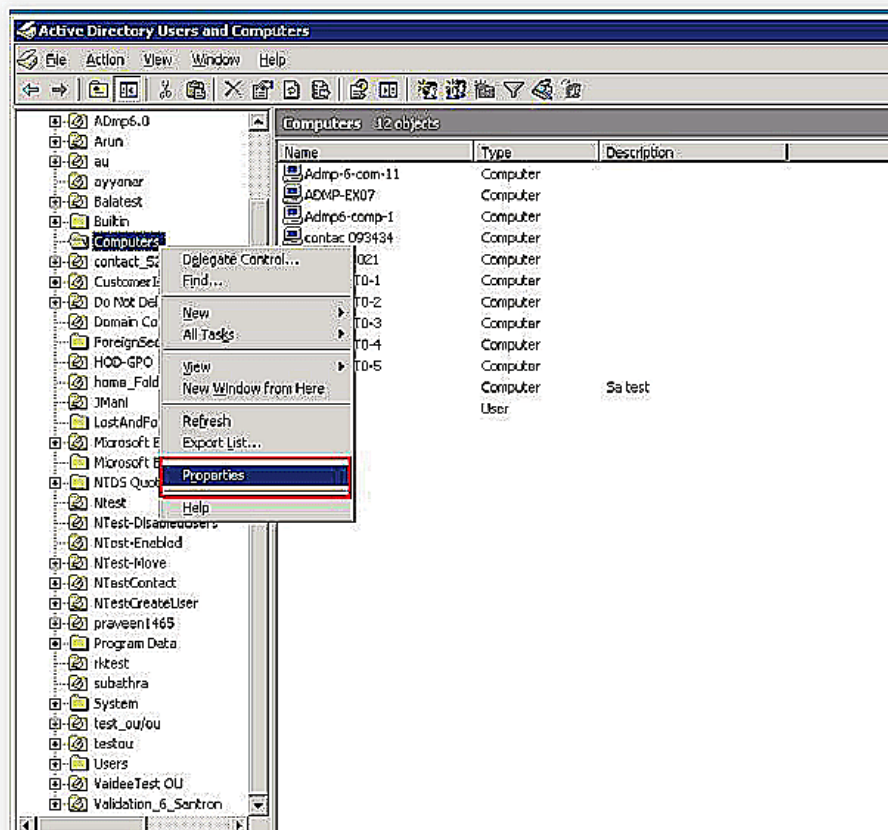


3. Give a descriptive name to the GPO and click **OK**.

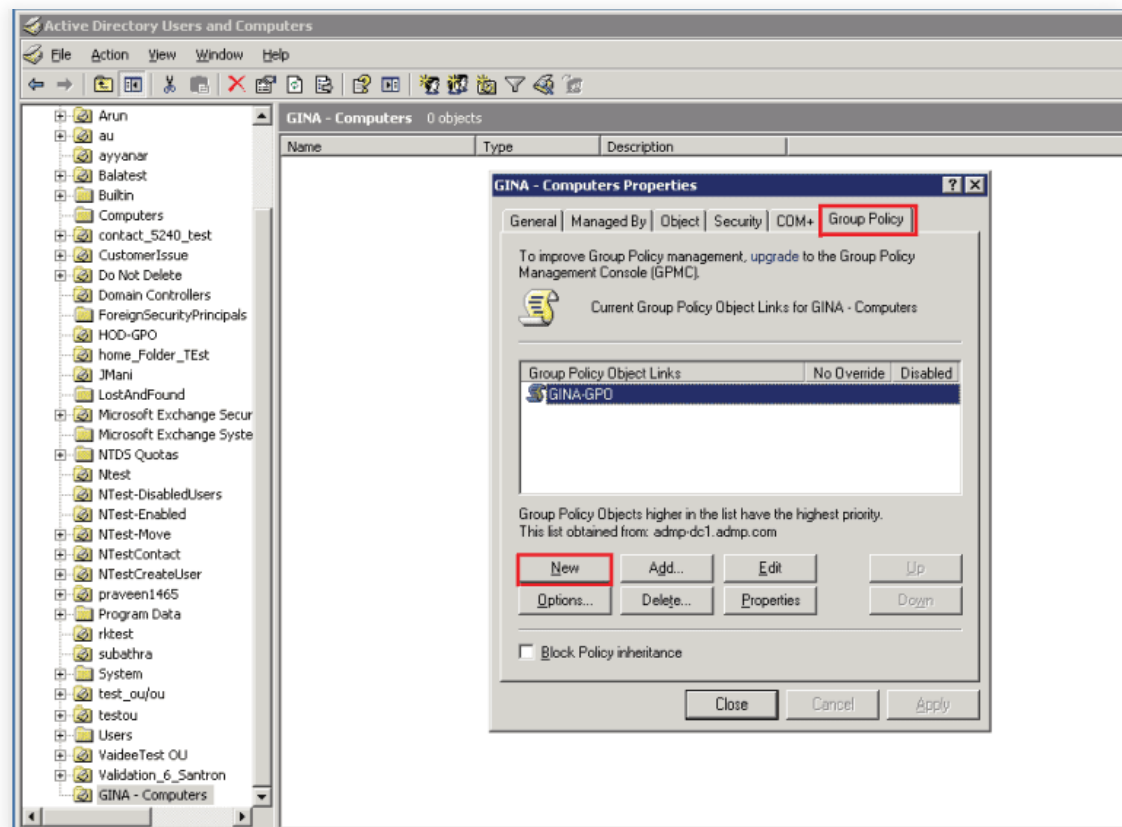


For Windows Server 2003 and Windows Server 2003 R2

1. Open the **Active Directory Users and Computers** console.
2. Right-click the parent container of all the computer objects (which are added to a group—refer to the best practice above) and select **Properties**.



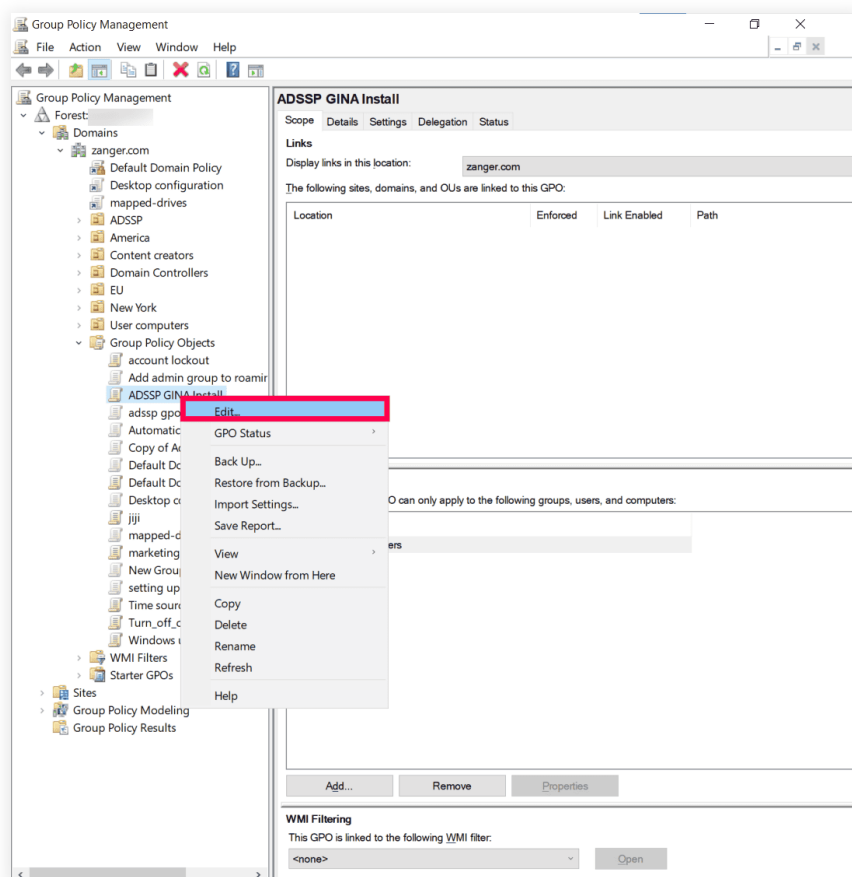
3. In the *Properties* dialog box that appears, select the **Group Policy** tab. Under this tab, click **New** to create a GPO.



STEP 2

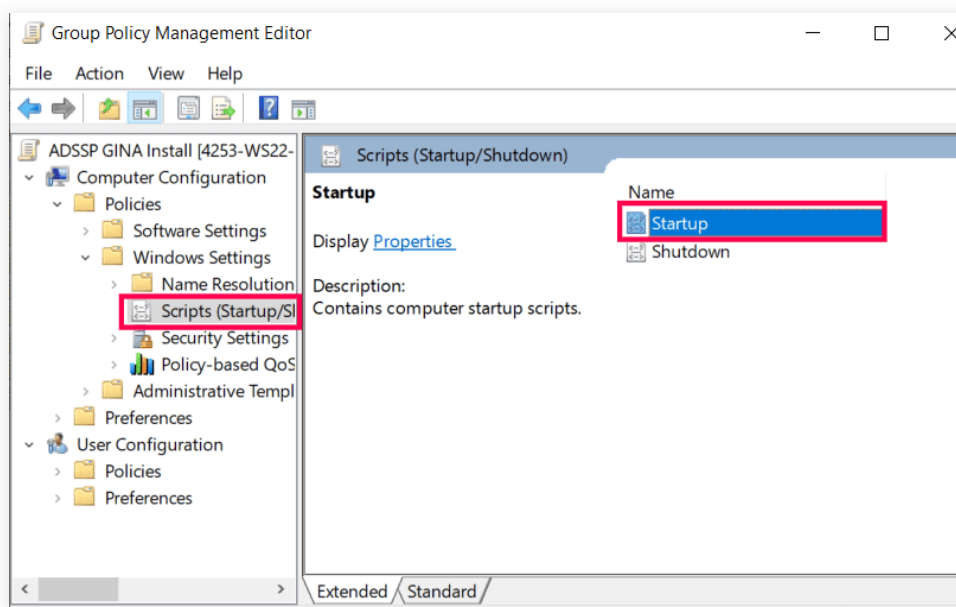
Configure script settings to run ReinstallAgent.vbs at start-up

1. Right-click the GPO you just created and click **Edit** to open the *Group Policy. Management Editor*.

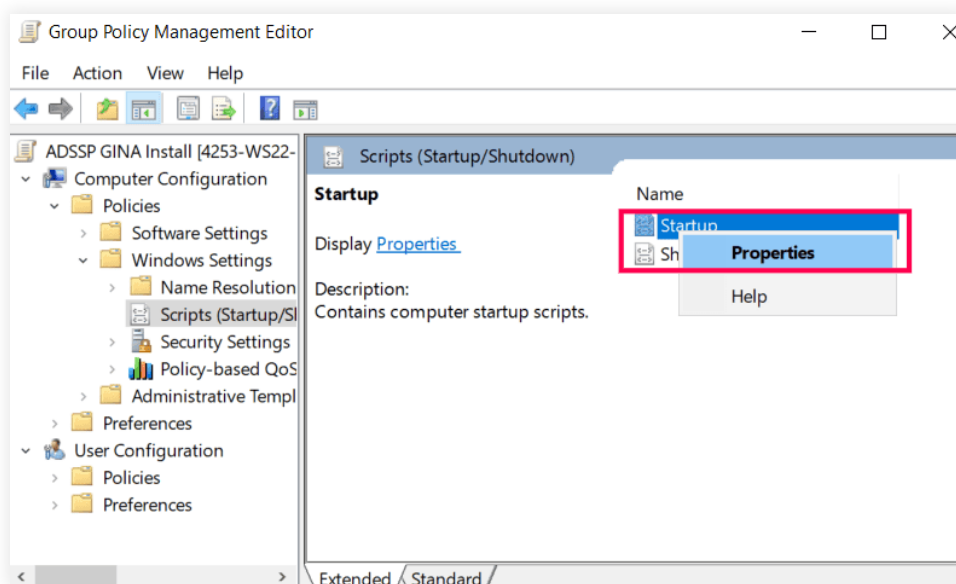


2. Depending on your operating system, do the following:

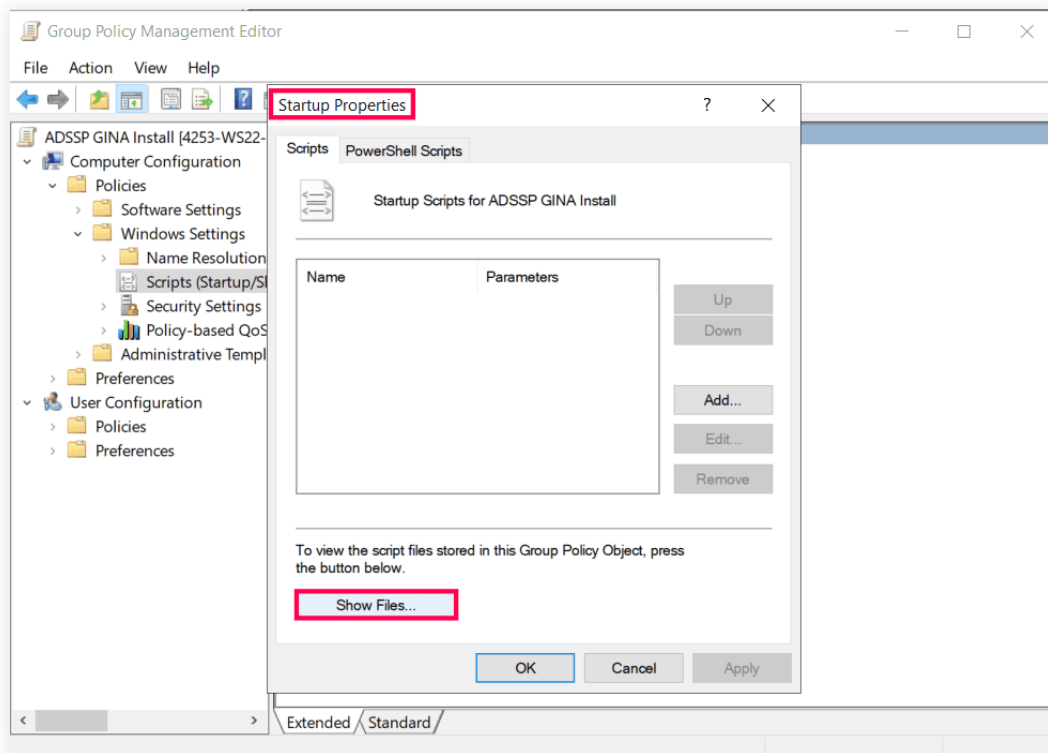
- **For Windows Server 2003 and Windows Server 2003 R2:** In the *Group Policy Object Editor*, on the left pane, double-click **Computer Configuration > Windows Settings > Scripts (Startup/Shutdown) > Startup**.
- **For Windows Server 2008 and above:** Double-click **Computer Configuration > Policies > Windows Settings > Scripts (Startup/Shutdown) > Startup**.



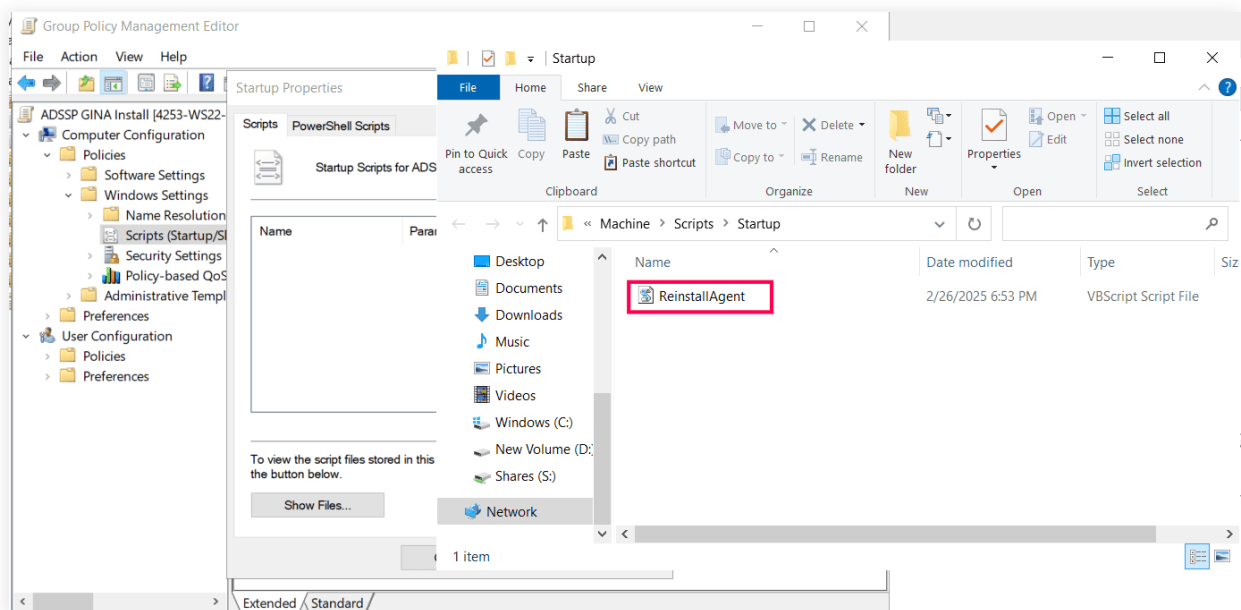
3. Right-click **Startup** and select **Properties**.



a. In the *Startup Properties* dialog box, click **Show Files**.



b. Paste the **ReinstallAgent.vbs** script file in the startup folder window that opens, then close the window.



c. In the **Script Parameters** field, enter **/MSIPATH:"%msifilepath%"** (replace **%msifilepath%** with the path to the Network Share folder location where **ADSelfServicePlusClientSoftware.msi** is stored).

Example: **/MSIPATH:"\\XYZ\Jone\ADSelfServicePlusClientSoftware.msi" /SERVERNAME:"XYZ" /PORTNO:"8888" /FRAMETEXT:"If you've forgotten your password." /BUTTONTEXT:"Reset Password" /PROD_TITLE:"ADSelfService Plus" /PROTOCOL:"https" /WRAPPINGPROVIDER:"{6f45dc1e5384-457a-bc13-2cd81b0d28ed}" /IMAGEPATH:"\\XYZ\Jone\key.png" /WINDOWSLOGONTFA:"true" /BYPASS:"false"**

MSIPATH is a mandatory parameter. If the admin would like to customize the installation, the following parameters can also be used during this step.

Notes: The starred(*) parameters are applicable only in cases where the server is offline or unreachable. Otherwise, the enforced status will be decided in real time based on the policy configuration settings in the product.

PARAMETER NAME	MATCHING REGISTRY VALUE	DEFAULT PARAMETER VALUE	DESCRIPTION
SERVERNAME	ServerName	The server on which ADSelfService Plus is running (based on the Access URL configured)	Specifies the ADSelfService Plus DNS hostname to be contacted, after the Windows login agent startup during machine logins or self-service password reset or account unlock.
PORTNO	PortNumber	The port number of the ADSelfService Plus server (based on the Access URL configured).	Defines the port number used by the ADSelfService Plus server.
SERVER-CONTEXTPATH	Server-ContextPath	None	The context path of the ADSelfService Plus server.
INSTALLATION_KEY	InstallationKey	None	The installation key that links the ADSelfService Plus server and agent securely.
BUTTONTEXT	ButtonText	Reset Password/Unlock Account	Specifies the button text visible on the Windows login to launch the Reset Password/Account Unlock wizard.
BYPASS	Bypass	FALSE	Determines whether MFA should be bypassed when the ADSelfService Plus server is unreachable during machine logins.
FRAMETEXT	FrameText	Can't logon? Please click Reset Password / Unlock Account button to reset your password or unlock your account.	Specifies the text to be displayed as the description. (Applicable only for Windows XP.)

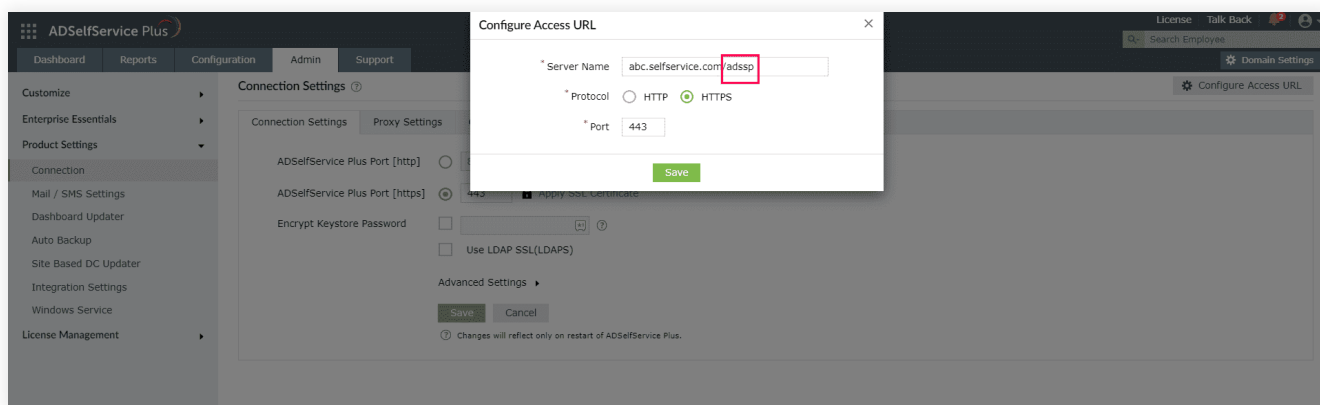
GINAHOSTEX-CLUDE	GinaHostExclude	okta, onelogin	Specifies the hosts to which a connection can be established from the login agent. By default, all hosts except the ADSelfService Plus server will be restricted. But this parameter must be used if SAML authentication is enabled for MFA and third-party IdPs are configured.
MFAENROLLMENT-WINDOWTITLE	MFAEnrollment WindowTitle	Multi-Factor Authentication - Enrollment	Defines the text that will be used as the title in the MFA enrollment window. Applicable only when enrollment is enforced for MFA for machine logins.
MFAWINDOW-TITLE	MFAWindowTitle	Multi-Factor Authentication	Defines the title of the MFA window displayed when MFA gets prompted by the login agent.
PPE_POPUP	PpePopUp	TRUE	Determines whether password policy requirements must be displayed in the Ctrl+Alt+Del change password screen or not.
PROD_TITLE	ProductTitle	ADSelfService Plus	Specifies the title to be displayed when the login agent window opens during self-service actions or MFA.
RESTRICTBAD-CERT	RestrictBadCert	TRUE	Determines whether to restrict usage of expired, self-signed, or invalid SSL certificates during self-service actions and MFA.
SERVERUNREACH	ServerUnreach	Server unreachable due to intermittent network connectivity or improper SSL certification, or as the Domain Controller configured in ADSelfService Plus is down. Please contact your administrator.	Defines the error message to be displayed if the server is unreachable during password reset, account unlock, or MFA.
SHOWADSSPLINK	ShowADSSPLink	TRUE	Determines the ADSelfService Plus link in the Ctrl+Alt+Del screen.
SHOWADSSPTILE	ShowADSSPTile	TRUE	Determines whether the Reset Password/ Account Unlock button is displayed as a credential tile on the login screen.

WINDOWSLOGONTFA	WindowsLogoTFA	FALSE	Determines whether MFA for Machine Login has been enabled.
MACHINEMFAUSAGESCENARIO*	MFAUsageScenarioMask	5	Determines whether the MFA for Machine Logins feature will be enabled for specific scenarios based on the value provided. Learn more.
		SCENARIO WHERE MFA IS REQUIRED	PARAMETER VALUE
		For machine login	1
		For locked machines	2
		For RDP server	4
		For UAC	8
		For RDP client	16

Note 1: If you wish to enable MFA for multiple scenarios, you will have to mention the value of the sum of those scenarios in the **MACHINEMFAUSAGESCENARIO** parameter.

For instance, if you want to enable MFA for both logging in to a machine and unlocking a machine, add their respective values (1 + 2) and pass the result (3) as the parameter.

Note 2: If your organization uses the [context path functionality of the Tomcat Server](#), use the **SERVERCONTEXTPATH** parameter in the ADSelfService Plus login agent installation command.



The context path can be found at the end of the ADSelfService Plus Access URL. In this example, it is **/adssp**. If this parameter is used in the installation command, it will look like this example:

```
msiexec /i "\\ADSelfServicePlusClientSoftware.msi"
SERVERNAME=abc.selfservice.com" PORTNO="443"
INSTALLATION_KEY="19d82629b4e540fc873df8775d3630cb"
SERVERCONTEXTPATH="/adssp"
```

This functionality is available only for Windows clients.

PARAMETER NAME	MATCHING REGISTRY VALUE	DEFAULT PARAMETER VALUE	DESCRIPTION
ISMACHINEMFA-ENFORCED*	isMFAEnforced	FALSE	If set to true, MFA will be enforced for all users accessing the machines irrespective of their enrollment status, self-service policy membership, or ADSelfService Plus connectivity status.
SHOW_SELECTED_TILE	ShowSelectedTile	TRUE	If set to true, the machine will prompt for a password by default at the machine login screen. If not, the prompt for the last login method used to access the machine will be displayed by default.
WRAPPINGPR-OVIDER	WrappingProvider	None	GUID of your third-party GINA/CP extension.
IMAGEPATH	GPO script parameter		Enter the file path of the BMP file to be used as the client software icon. The filename should be <i>reset_icon.bmp</i> .
CUSTOMTITLEI-CONPATH	GPO script parameter		Specifies the network share or path of the icon file used as the client software favicon. Ensure that the custom title icon is uploaded at C:\\Windows\\ System32\\ADSSPDesktop.ico . The filename should be <i>ADSSPDesktop.ico</i> .

Note: For Windows Server 2003 and Windows Server 2003 R2, the parameters for the script should be enclosed within double quotes to support multiple parameter values.

PARAMETER NAME	MATCHING REGISTRY VALUE	DEFAULT PARAMETER VALUE	DESCRIPTION	
OFFLINEMFA	OfflineMFA	FALSE	Specifies whether offline MFA is enabled or not.	
LOCALE_ID	LocaleId	NONE	Specifies the display language used for some parts of the login agent.	
			LANGUAGE	KEY
			Simplified Chinese	zh-cn
			Japanese	ja
			French	fr-fr
			German	de-de
			Turkish	tr
			Spanish	es-mx
			Polish	pl
OFFLINE_WEB_LOGO_NAME	OfflineWebLogo-Name	NONE	Specifies the filename and the format of the custom logo to be displayed during offline MFA. The filename must be in the format <i>customLogo.png</i> . The supported formats are <i>JPG, JPEG, BMP, PNG, and GIF</i> .	
LOGOIMAGEPATH	GPO script parameter	NONE	Mentions the network share path of custom logo used during offline MFA (this will be copied to <i>C:\\Windows\\System32\\folder location</i>).	

STEP 3

Configure Administrative Templates settings

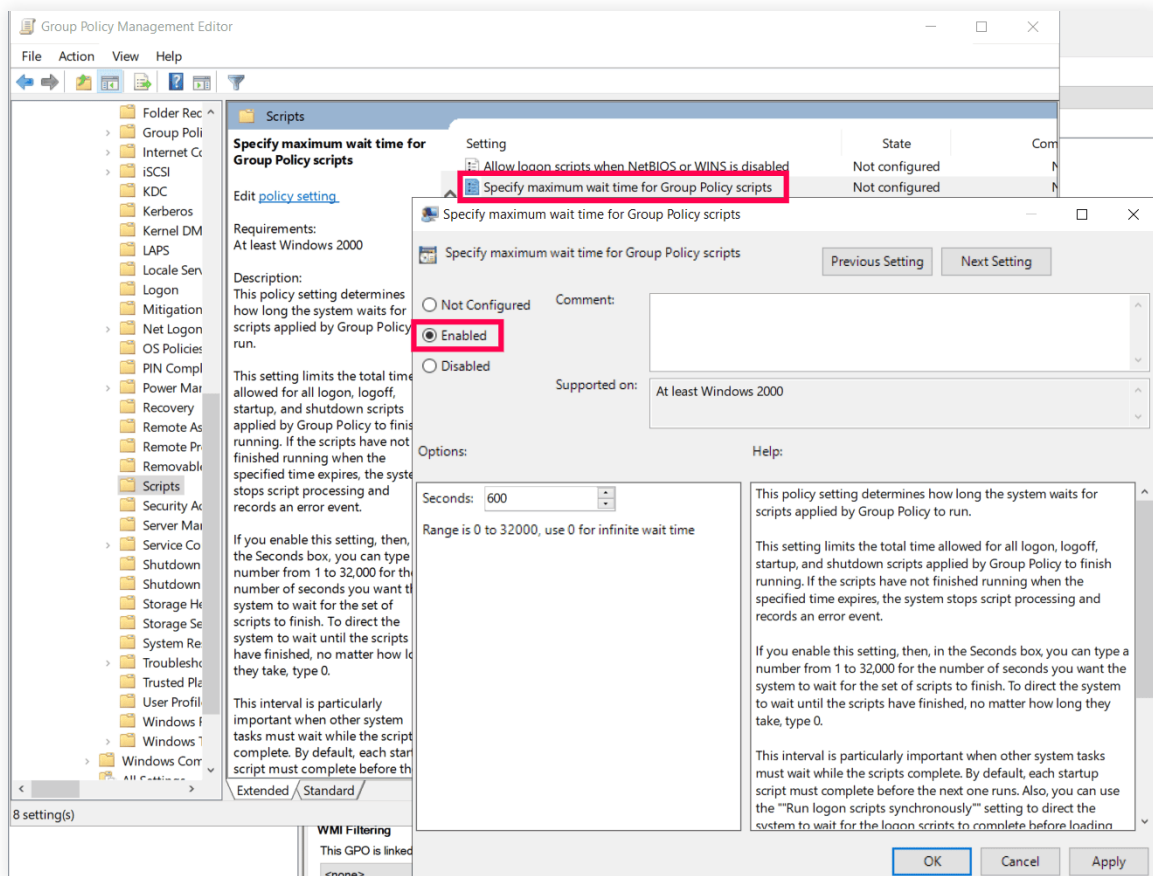
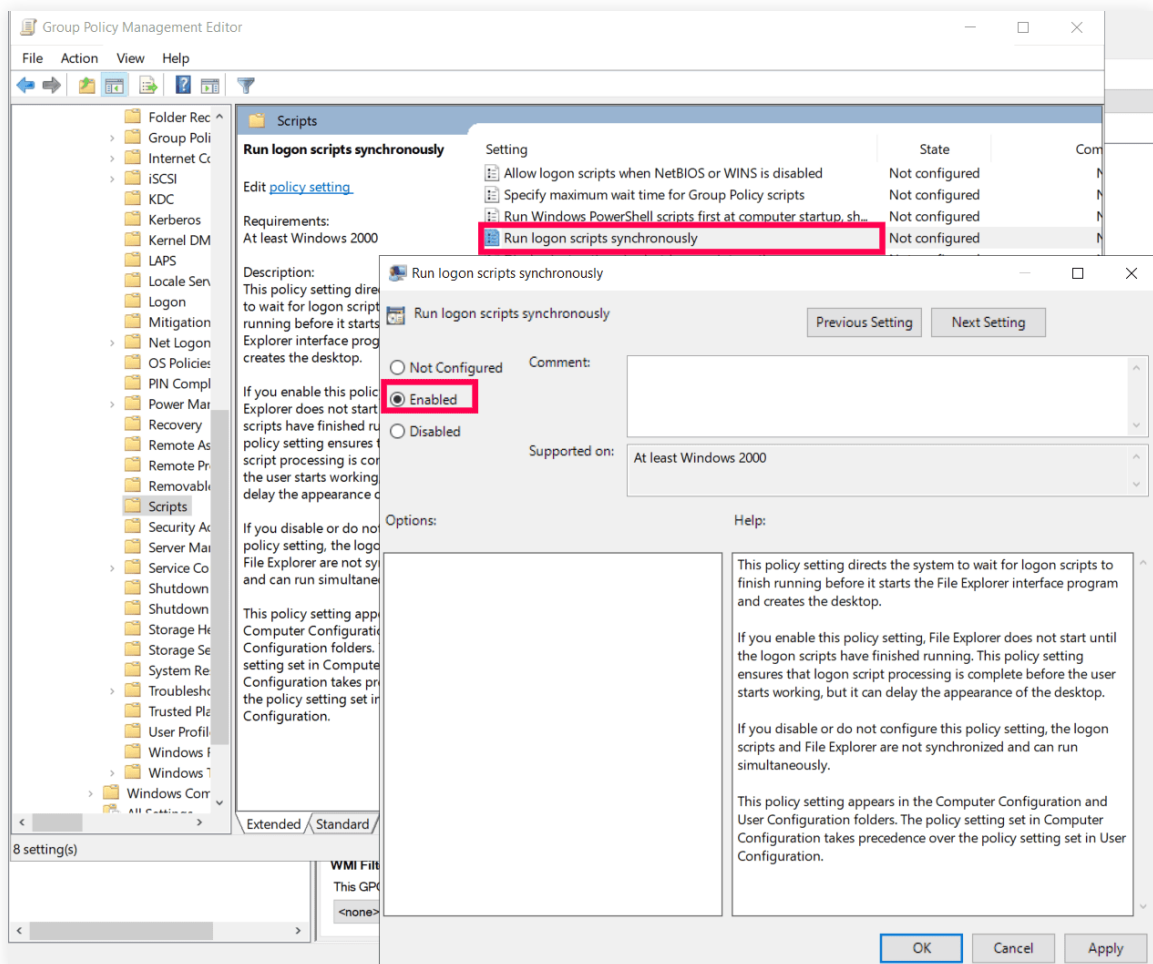
1. Depending on your operating system, do the following:

- **For Windows Server 2003 and Windows Server 2003 R2:** On the left pane of the *Group Policy Object Editor* window, double-click **Computer Configuration > Administrative Templates > System**.
- **For Windows Server 2008 and above:** On the left pane of the *Group Policy Management Editor* window, double-click **Computer Configuration > Policies > Administrative Templates > System**.

2. Under **System**, configure the following settings:

a. Scripts

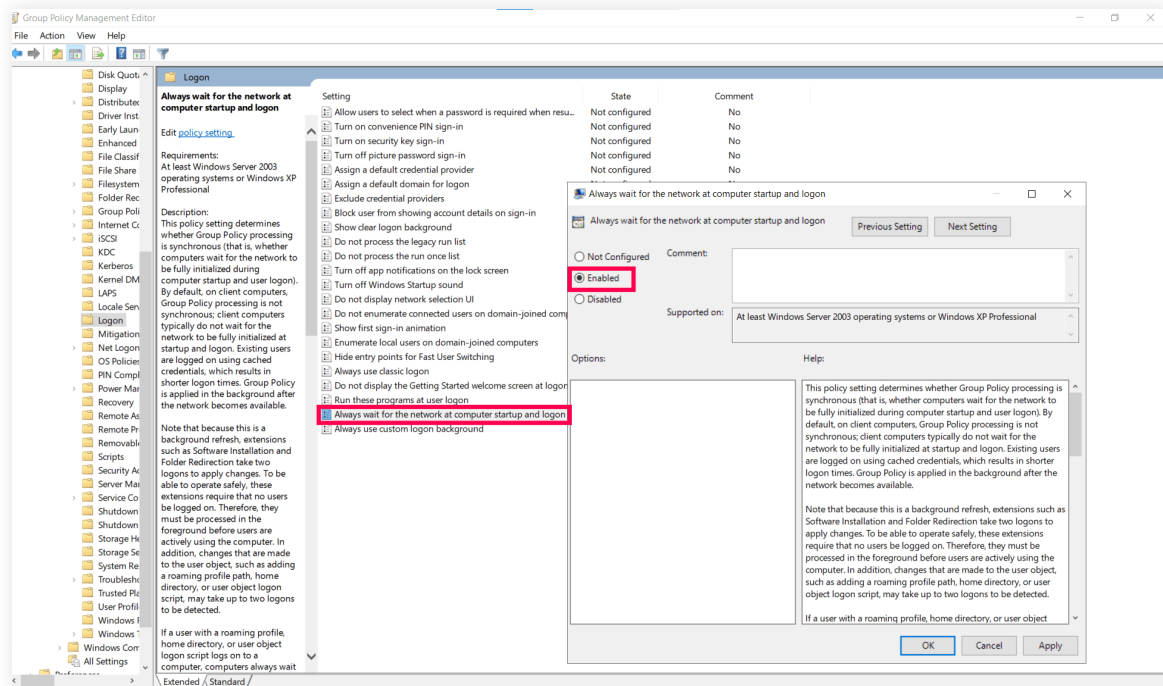
- On the right pane of the *Group Policy Management Editor*, double-click Run **logon scripts synchronously** and select **Enabled**. Click **Apply**, then click **OK**.
- Double-click **Specify maximum wait time for Group Policy scripts** and select **Enabled**. Click **Apply**, then click **OK**.



b. Logon

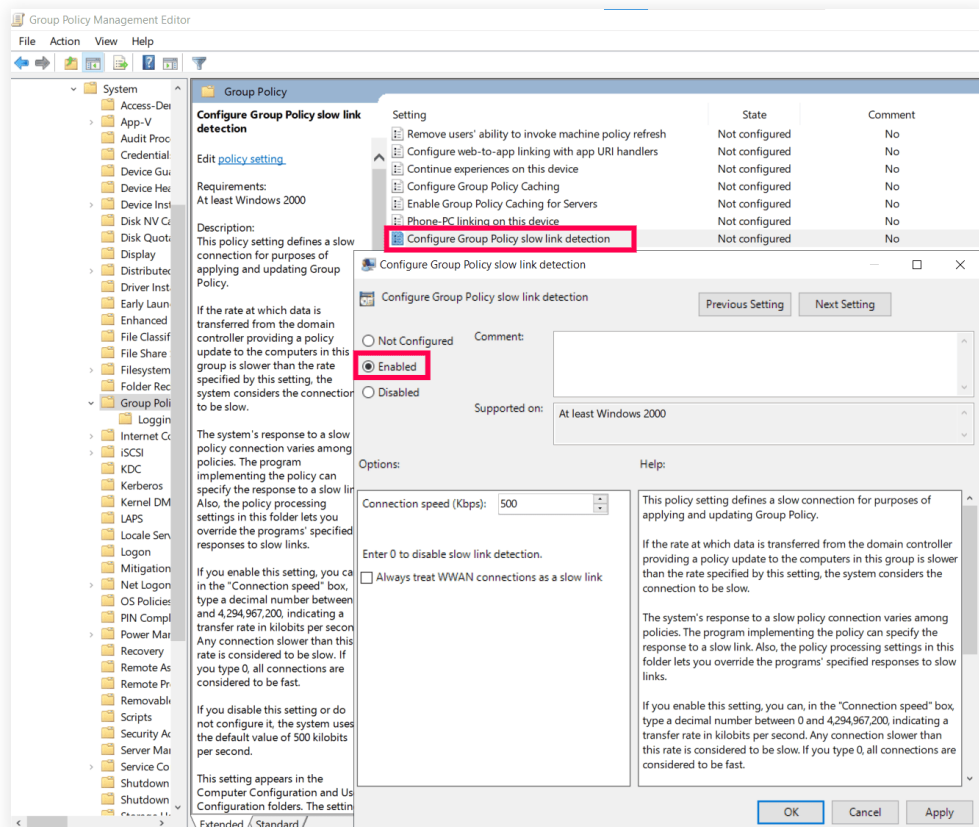
Double-click **Always wait for the network at computer startup and logon** and select **Enabled**.

Click **Apply**, then click **OK**.



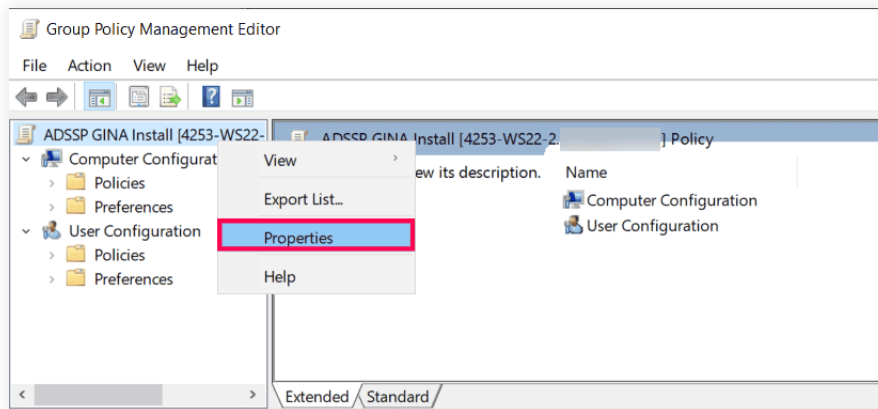
c. Group Policy

Double-click **Configure Group Policy slow link detection** and select **Enabled**. Click **Apply**, then click **OK**.



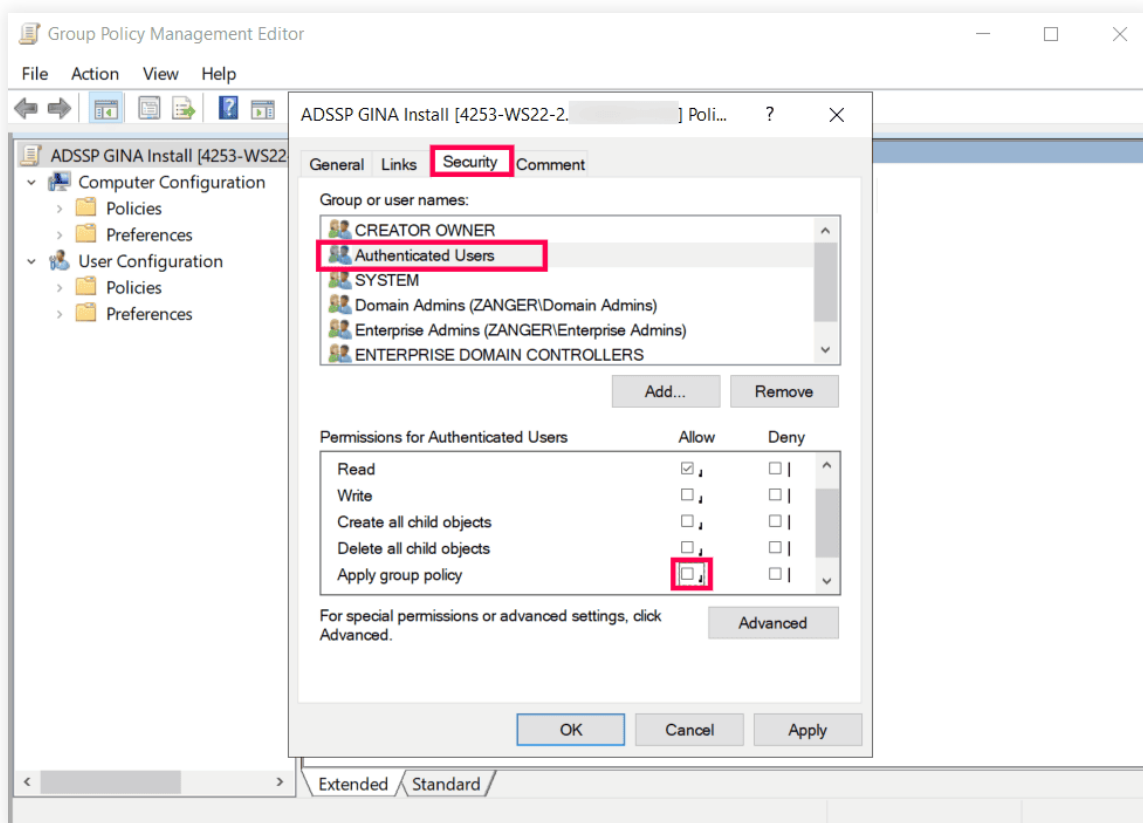
STEP 4**Apply the GPO**

1. On the left pane of the *Group Policy Management Editor*, right-click the **GPO** you are working on (available in the top-left corner) and select **Properties**.

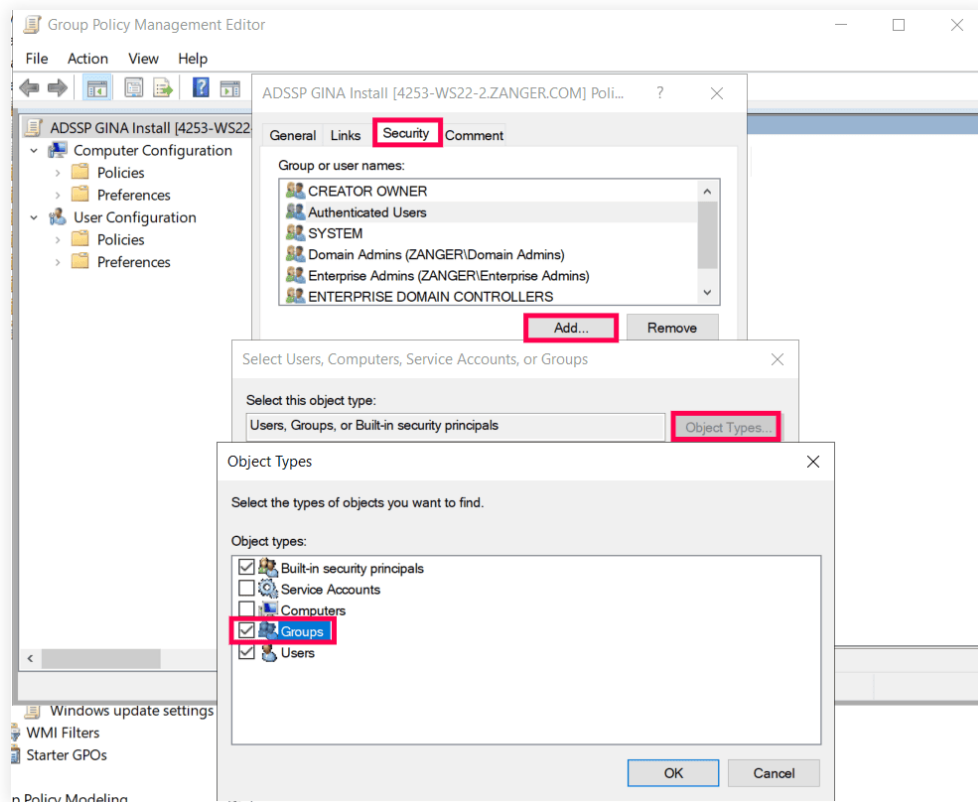


2. In the *Properties* dialog box that appears, click the **Security** tab.

Important note: On this tab, under *Permissions for Authenticated Users*, uncheck the **Apply Group Policy** permission before proceeding.

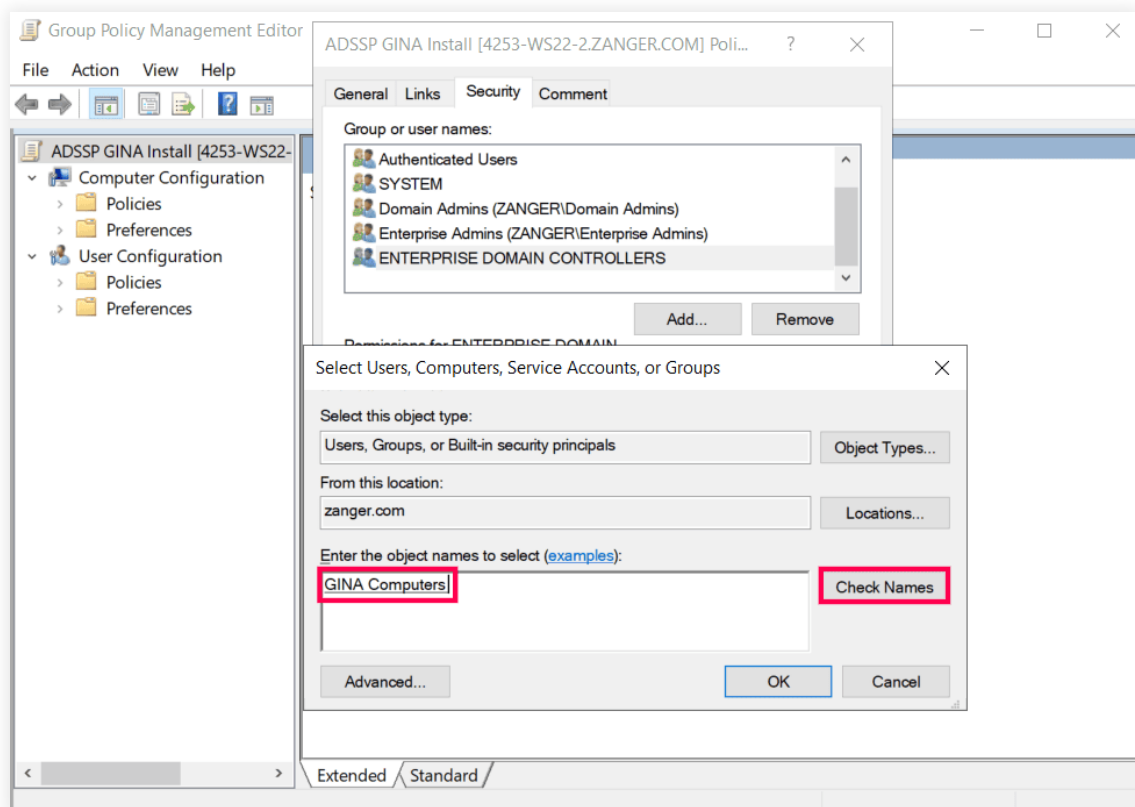


3. Click **Add** to open the *Select Users, Computers, or Groups* dialog box.
 - a. Click **Object Types** and make sure **Groups** is checked, then click **OK**.

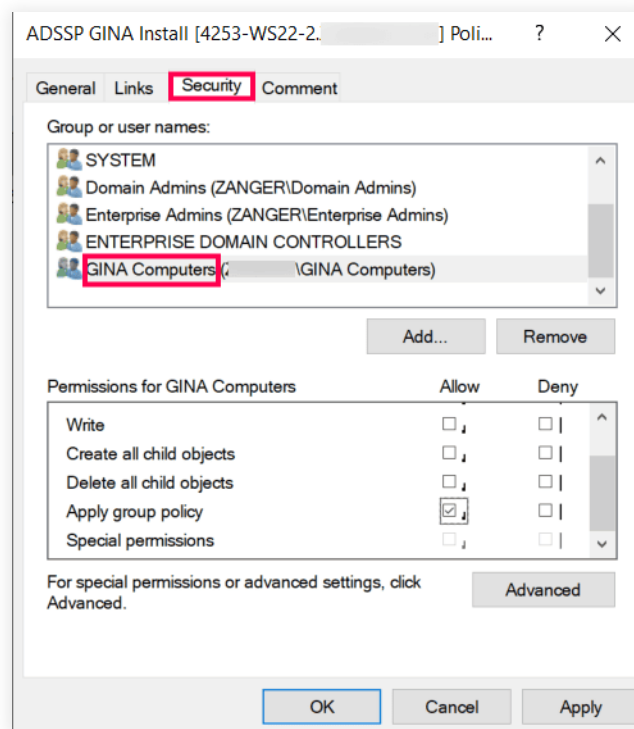


4. Enter the name of the group that contains all the computers set for login agent installation and click **Check Names**.

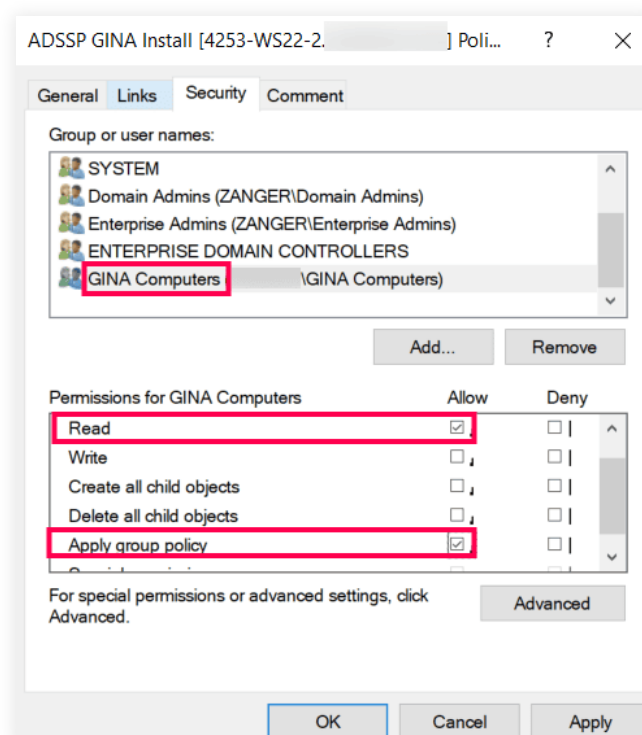
- Highlight the desired group and click **OK** to return to the **Security** tab.
- The group will now be added to the list of *Group or user names*.



5. With the newly added group highlighted, apply the following permissions:
- For *Read*, check **Allow**.
 - For *Apply group policy*, check **Allow**.
 - Click **Apply**, then click **OK**.



6. Reboot the computers to apply the GPO and wait until the next start-up for the **Reset Password/Unlock Account** button to appear on the Windows login screen.



To apply the GPO directly to computers:

If you prefer to apply the GPO directly to computers instead of the group, please follow the steps below:

1. Follow the first two steps as outlined above for applying the GPO.
2. Click **Object Types**. Make sure **Computers** is checked. Click **OK**.
3. Use **Check Names** to find the necessary computers. Highlight the computers you want to add and click **OK** to return to the **Security** tab.
4. Set the **Read** and **Apply Group Policy** permissions to **Allow**, for every computer that you just added.

Important note: After completing all these steps, remember to uncheck the **Apply Group Policy** permission.

5. Reboot all the client machines.

Troubleshooting tips

If you are experiencing any problems on the Windows login screen after installing the ADSelfService Plus login agent and making the Registry changes, try the following steps to solve the problem:

1. Restart your machine in Safe Mode.
2. Remove the registry key {B80B099C-62EA43cd9540-3DD26AF3B2B0} found under KEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers.

Our Products

AD360 | Log360 | ADManager Plus | ADAudit Plus | RecoveryManager Plus | M365 Manager Plus

ADSelfService Plus

ADSelfService Plus is an identity security solution to ensure secure and seamless access to enterprise resources and establish a Zero Trust environment. With capabilities such as adaptive multi-factor authentication, single sign-on, self-service password management, a password policy enhancer, remote work enablement, and workforce self-service, ADSelfService Plus provides your employees with secure, simple access to the resources they need. ADSelfService Plus helps keep identity-based threats out, fast-tracks application onboarding, improves password security, reduces help desk tickets, and empowers remote workforces. For more information about ADSelfService Plus, visit www.manageengine.com/products/self-service-password.

\$ Get Quote

↓ Download

🔗 Support