ManageEngine
ADSelfService Plus

Login agent installation via Group Policy Object (GPO)

www.adselfserviceplus.com

Table of Contents

Document Summary ---- 1

ADSelfService Plus login agent ---- 1

ADSelfService Plus login agent Installation via GPO ---- 2

- Step 1: Create a GPO and name it ---- 2
- Step 2: Configure script settings to run *Reinstall Agent.vbs* at startup ---- 5
- Step 3: Configure Administrative Templates settings ---- 13
- Step 4: Apply the GPO ---- 15

Login Agent Installation Key ---- 19

Testing and diagnostics ---- 20

Document summary

This document describes ADSelfService Plus login agent, its uses, and the method to install it using a GPO. The document is written for a system administrator with a basic understanding of the Windows operating system, Active Directory (AD), and enterprise software deployment. However, care has been taken to keep the installation steps as simple as possible.

The ADSelfService Plus login agent

With the ever-changing technological landscape, attackers are finding new methods to crack user credentials and gain access to their AD domain accounts. Although good password hygiene and advanced password policies can help create strong passwords, depending only on a single level of authentication isn't a secure move.

Moreover, when using web-based self-service software, end users no longer need help desk personnel for password reset and account unlock operations. However, using web-based self-service means that a user who has forgotten their password, and therefore has no access to their machine, either needs a colleague's machine or a dedicated kiosk to carry out the required self-service operations.

ADSelfService Plus addresses the above scenarios through its login agent. The ADSelfService Plus login agent is an extension of the standard Windows login screen. When installed, it enables MFA for Windows logins and 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 compatible with the following operating systems:

- Windows Vista
- Windows 7
- Windows 8
- Windows 8.1
- Windows 10
- Windows 11
- Windows Server 2003
- Windows Server 2003 R2
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

ADSelfService Plus login agent installation via GPO

Important: Before starting with the steps below, place the *ReinstallAgent.vbs* and *ADSelfServicePlusClientSoftware.msi* files in a **network shared folder** on your server.

The *ADSelfServicePlusClientSoftware.msi* file is available in the **bin** directory of the ADSelfService Plus installation folder. The default location is *C:\Program Files\ManageEngine\ADSelfService Plus\bin.*

The *ReinstallAgent.vbs* file is available for download from the ADSelfService Plus admin portal. Log in to the product admin portal and go to **Configuration > Administrative Tools > GINA /Mac/Linux (Ctrl+Alt+Del).** Under the *Installation Help Guide* section, click on **GINA Login Using GPO (Group Policy Object).** Download the file using the link available in Step 5.

Note: If a new Installation Key is generated, the admin will need to download the *ReinstallAgent.vbs* file from the product admin portal and use it to replace the existing file it in the Network Share.

Best practice: Create a group and add all the computers on which you want to install the ADSelfService Plus login agent. Create a GPO and apply it to this group.

Prerequisites

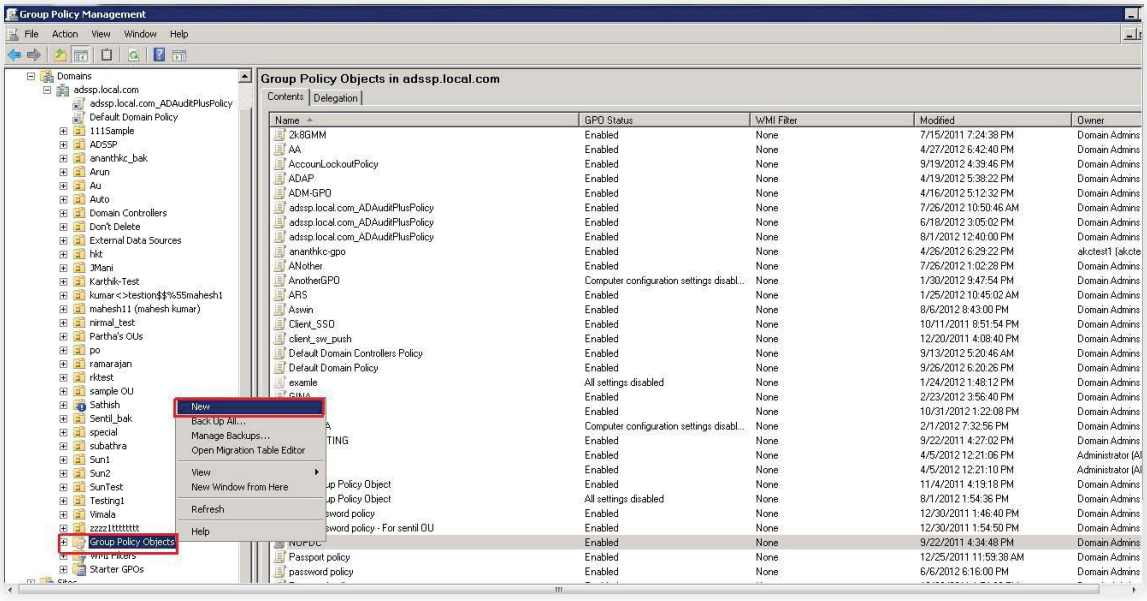
1 The Endpoint MFA add-on for ADSelfService Plus is required to enable MFA for Windows logins. Visit the store to purchase the add-on.
2 The ADSelfService Plus Professional Edition is required to enable self-service password reset and account unlock on Windows login screens.
3 A valid SSL certificate must be installed in ADSelfService Plus and the Access URL must be configured to use the HTTPS protocol. You can find the steps in this guide.

For successful installation, do the following steps in order.

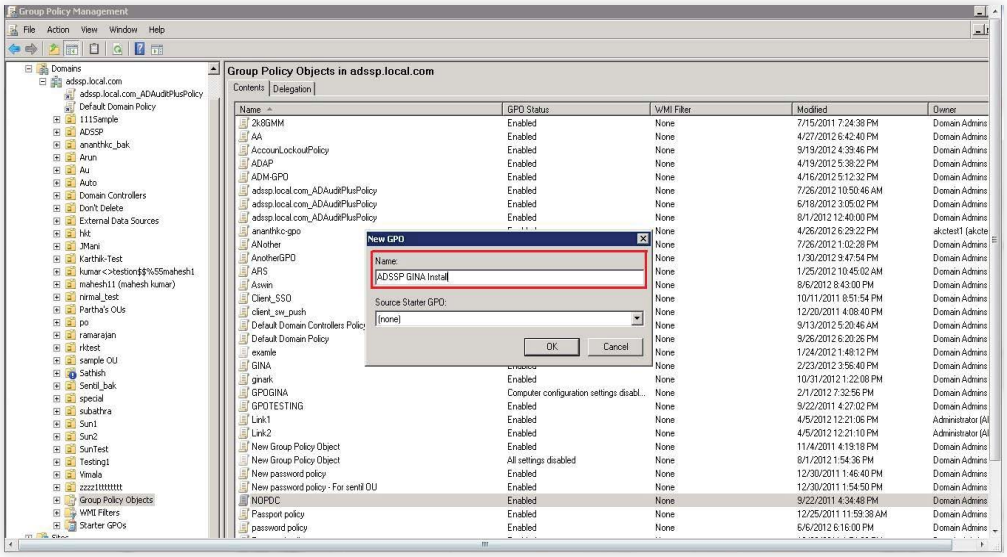
Step 1: Create a GPO and name it

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.**

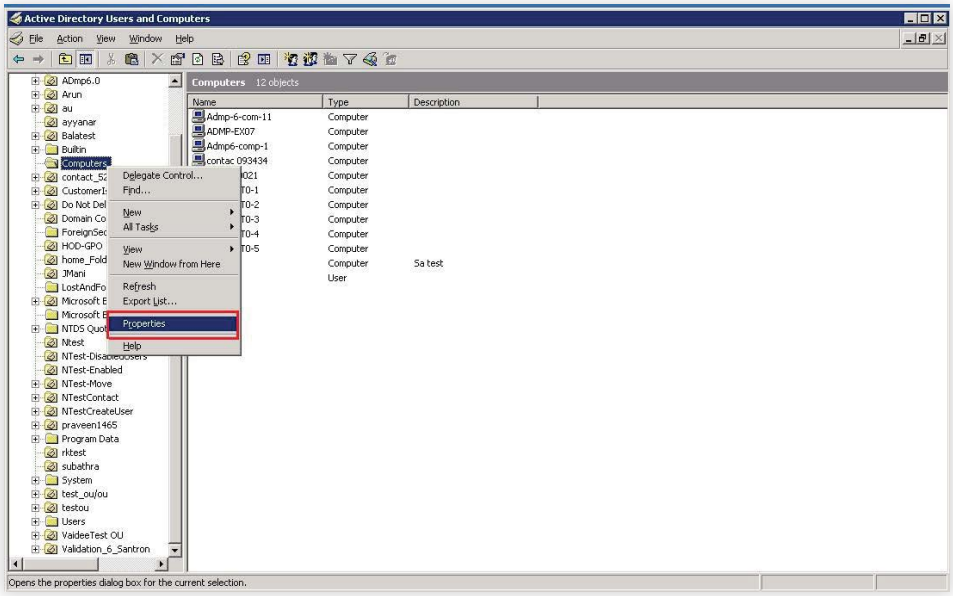


3. Give a descriptive name to the GPO and click **OK.**

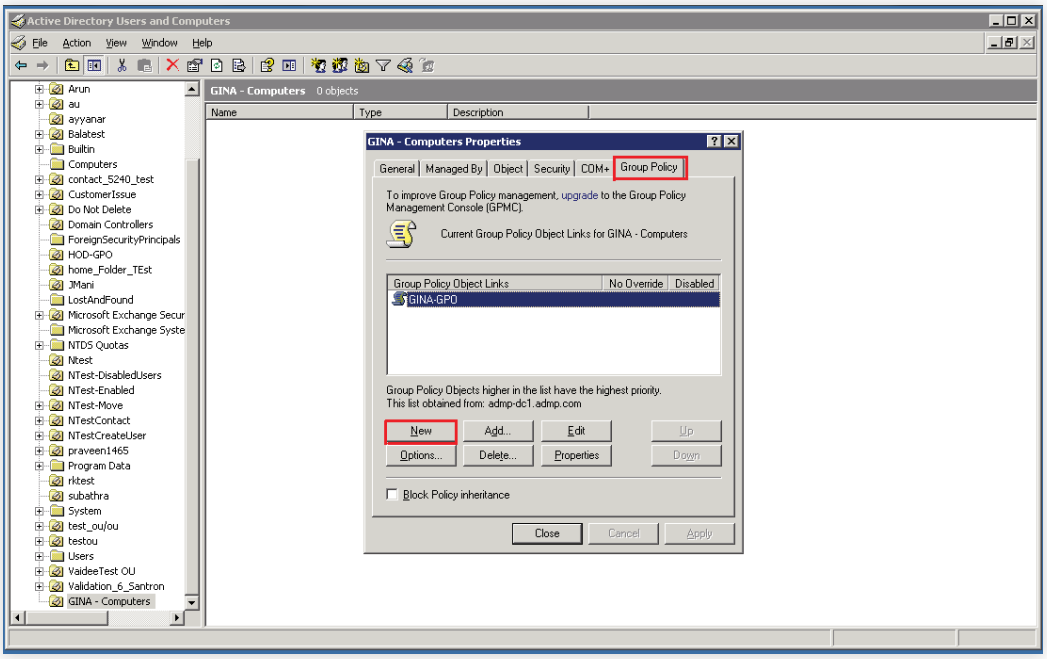


For Windows Server 2003 and Windows Server 2003 R2

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.**

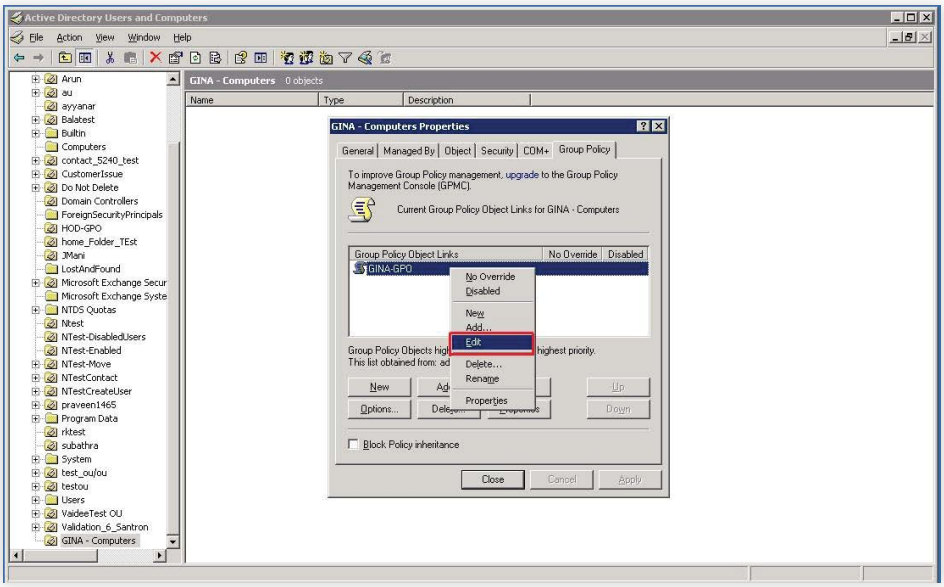


3. In the *Properties* dialog box that appears, select the **Group Policy** tab. Under this tab, click **New** to create a GPO.



Step 2: Configure script settings to run *ReinstallAgent.vbs* at start-up

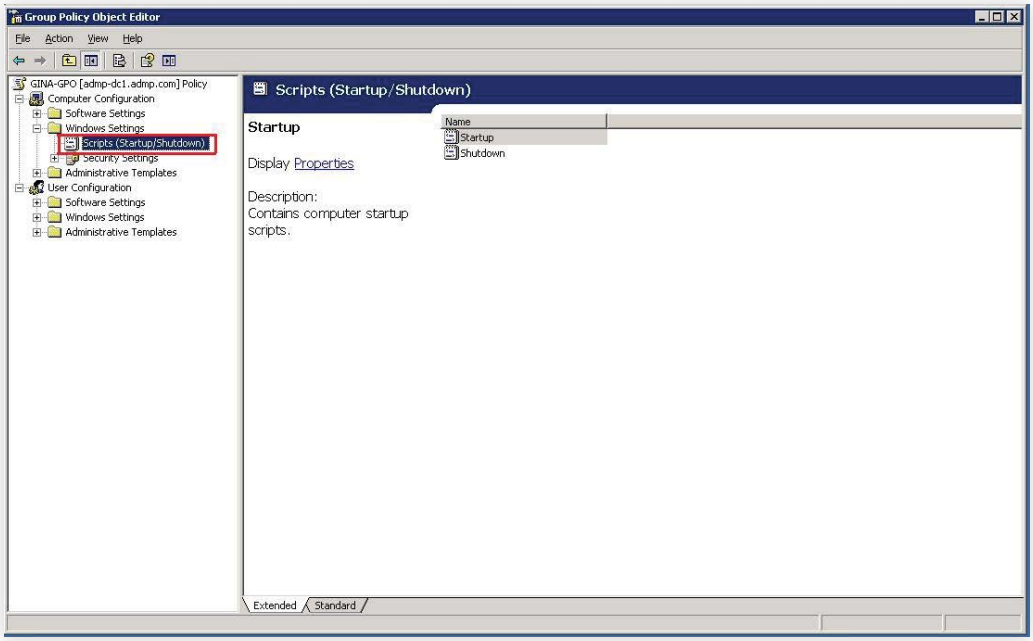
1. Right-click the GPO you just created and click **Edit** to open the *Group Policy Object Editor.*



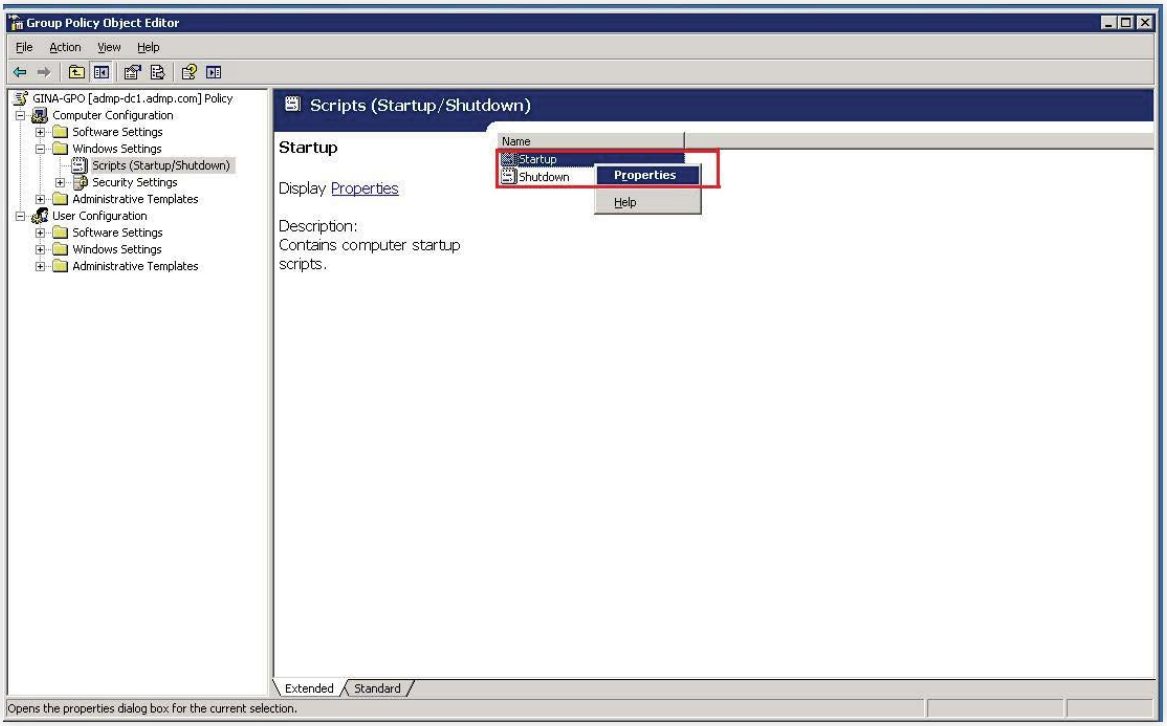
2. Depending on your operating system, do the following:

- **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.**

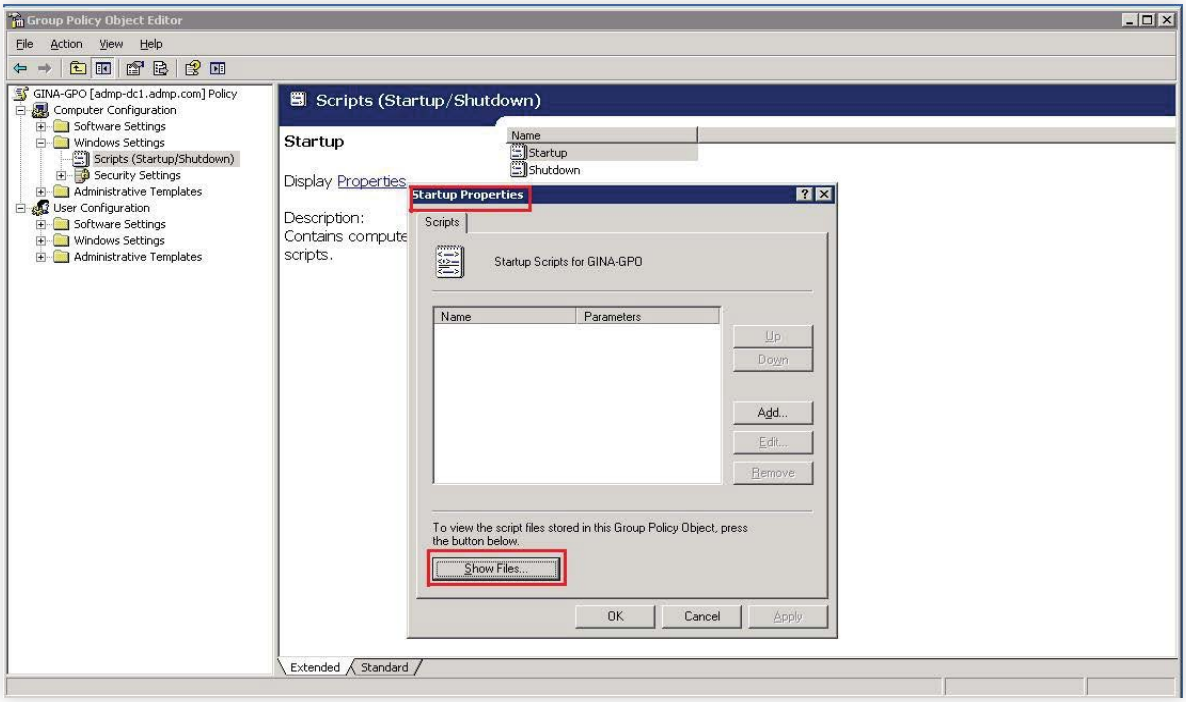
- **For Windows Server 2008 and above:** Double-click **Computer Configuration > Policies > Windows Settings > Scripts (Startup/Shutdown) > Startup.**



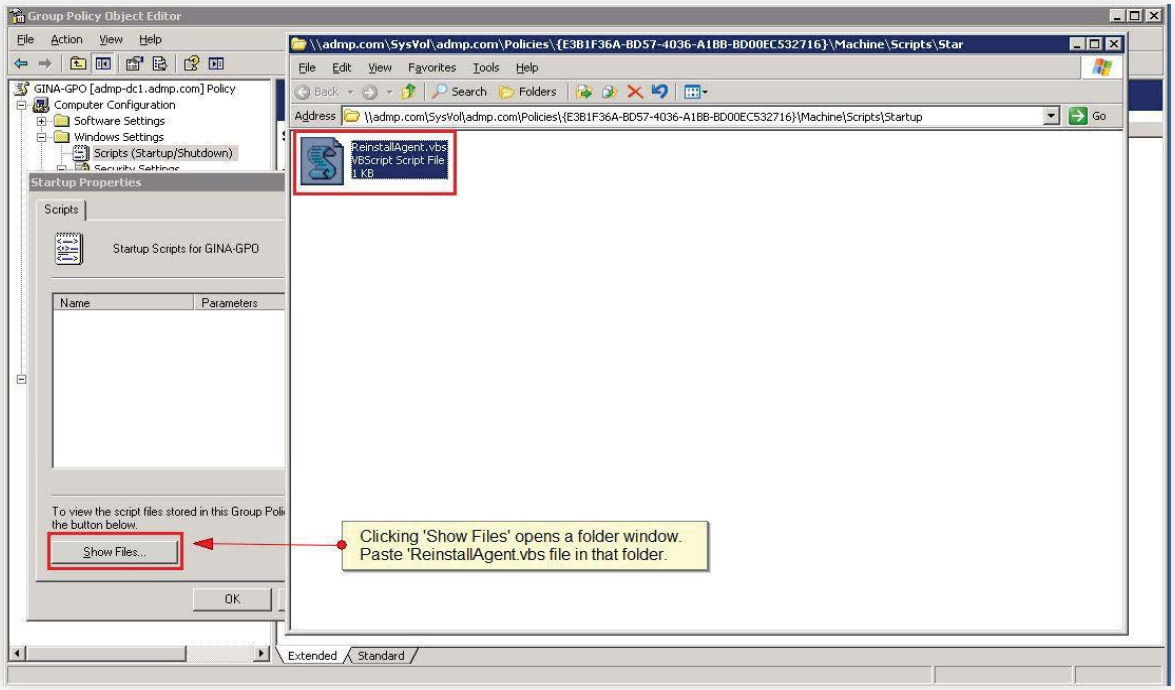
3. Right-click **Startup** and select **Properties.**



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%"** (here, 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 parameters in the following table can also be used during this step.

Note: 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 GINA login agent startup during machine login or self-service password rest and 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. To know more about the context path, click here.
INSTALLATION_KEY	InstallationKey	None	The installation key that links the ADSelfService Plus server and client securely.
BUTTONTEXT	ButtonText	"Reset Password / Unlock Account"	Specifies the button text visible on the Windows login to launch the Reset Password/Account Unlock wizar.
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.)
GINAHOSTE-XCLUDE	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.
MFAWINDOWTITLE	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.
RESTRICTBADCERT	RestrictBadCert	TRUE	Determines whether to restrict usage of expired, self-signed, or invalid SSL certificates during self-service actions and MFA. **Note:** We strongly advise against setting the login agent to work even when the SSL certificate is invalid in your production environment, as it will severely impact security. Please disable this only for testing purposes.
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.

WINDOWSLO-GONTFA	WindowsLogonTFA	FALSE	Determines whether MFA for Machine Login has been enabled.
MACHINEMFA-USAGESCENARIO*	MFAUsage ScenarioMask	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: 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.

PARAMETER NAME	MATCHING REGISTRY VALUE	DEFAULT PARAMETER VALUE	DESCRIPTION
ISMACHINEMF-AENFORCED*	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.
IS_VPN_ENABLED	IsVpnEnabled	None	Specifies whether the cached credentials update feature is enabled or not.
IS_TP_VPN_ ENABLED	ISTPVPNEnabled	None	Specifies whether a third-party VPN (VPN providers other than the native Windows VPN) is enabled.
VPN_SERVER_ NAME	VpnServerName	None	Specifies the VPN server's name.

<table>
<tr><td>VPN_PORT_NO</td><td>VpnPortNo</td><td>None</td><td>Defines the ADSelfService Plus server's port number used to connect to VPN.</td></tr>
<tr><td>PRE_SHARED_KEY</td><td>PreSharedKey</td><td>None</td><td>Defines the value of the pre-shared key configured while setting up the Native Windows VPN for the cached credentials update feature.</td></tr>
<tr><td>VPN_GROUP_NAME</td><td>VpnGroupName</td><td>None</td><td>Specifies the VPN group name used when configuring Updating Cached Credentials over VPN feature. Required only when a Cisco AnyConnect VPN is used</td></tr>
<tr><td>VPN_DOMAIN_NAME</td><td>VpnDomainName</td><td>None</td><td>Defines the domain name to which the VPN should be connected during cached credentials update. Applicable only when SonicWall NetExtender or a custom VPN provider is used.</td></tr>
<tr><td>VPN_TYPE</td><td>VpnType</td><td>None</td><td>Defines the VPN connection behavior for cached credentials update based on the provider used. This pre-set number key is used to denote the VPN provider.
<table>
<tr><th>VPN PROVIDER</th><th>NUMBER VALUE</th></tr>
<tr><td>Custom VPN</td><td>0</td></tr>
<tr><td>Fortinet and Cisco IPSec</td><td>1</td></tr>
<tr><td>The native Windows VPN</td><td>2</td></tr>
<tr><td>Cisco AnyConnect</td><td>3</td></tr>
<tr><td>SonicWall NetExtender</td><td>4</td></tr>
<tr><td>Checkpoint Remote Access VPN and SonicWall Global VPN</td><td>5</td></tr>
<tr><td>Open VPN</td><td>6</td></tr>
</table></td></tr>
<tr><td>VPN_CLIENT_LOCATION</td><td>VpnClientLocation</td><td>None</td><td>Specifies the VPN client location. (Example: C:\Program Files (x86)\ Fortinet\FortiClient\ FortiSSLVPN client.exe)</td></tr>
</table>

VPN_CONNECT_CMD	VpnConnectCmd	None	VPN provider-specific command that is used to connect to the VPN during cache credentials update.
VPN_DISCONNECT_CMD	VpnDisconnectCmd	None	VPN provider-specific command that is used to disconnect from the VPN during cache credentials update.
WRAPPINGPROVIDER	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 *reset_icon.bmp*.
CUSTOMTITLEICONPATH	GPO script parameter		Specifies the network share or path of the icon file used as client software favicon. Ensure that the custom title icon is uploaded at **C:\\Windows\\System32\\ADSSPDesktop.ico.** The filename should be *ADSSPDesktop.ico.*

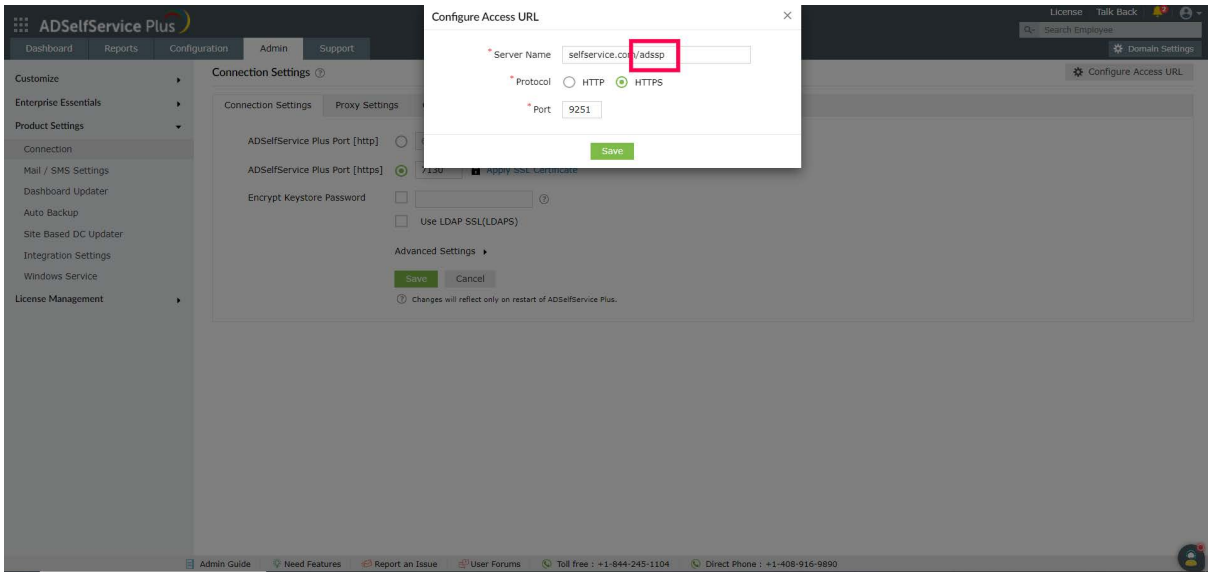
Note: For Windows Server 2003 and Windows Server 2003 R2, the parameters for the script should be enclosed within double quotes to support multiple parameter values.

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.
OFFLINE_WEB_LOGO_NAME	OfflineWebLogoName	NONE	Specifies the filename and the format of the custom logo to be displayed during offline MFA. The filename must be in the format *customLogo.png*. The supported formats are *jpg, jpeg , bmp, png, and gif.*

LANGUAGE	KEY
Simplified Chinese	zh-cn
Japanese	ja
French	fr-fr
German	de-de
Turkish	tr
Spanish	es-mx
Polish	pl

LOGOIMAGEPATH	GPO script parameter	NONE	Mentions the network share path of custom logo used during offline MFA (this will be copied to *C:\\Windows\\System32\\ folder location).*

Note: 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.

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 > Administrative Templates > System.**

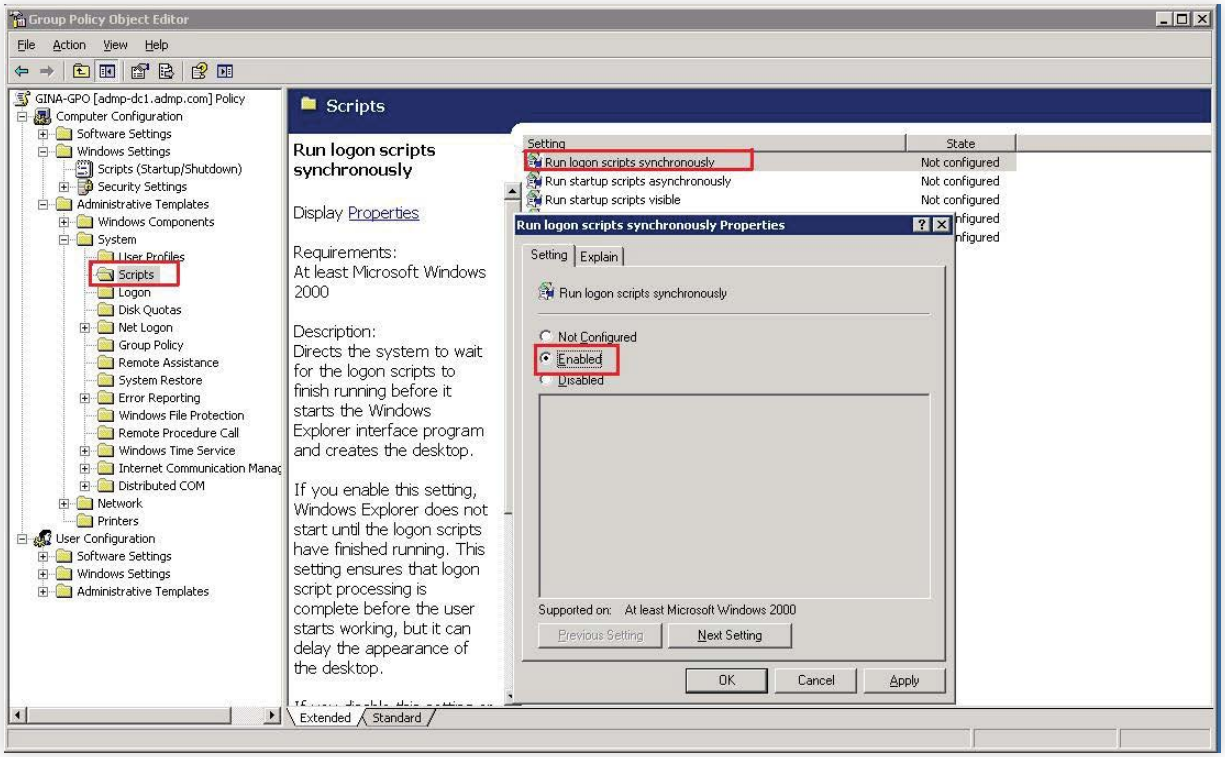
2. Under **System,** configure the following settings:

a. Scripts:

- On the right pane of the *Group Policy Object 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.**

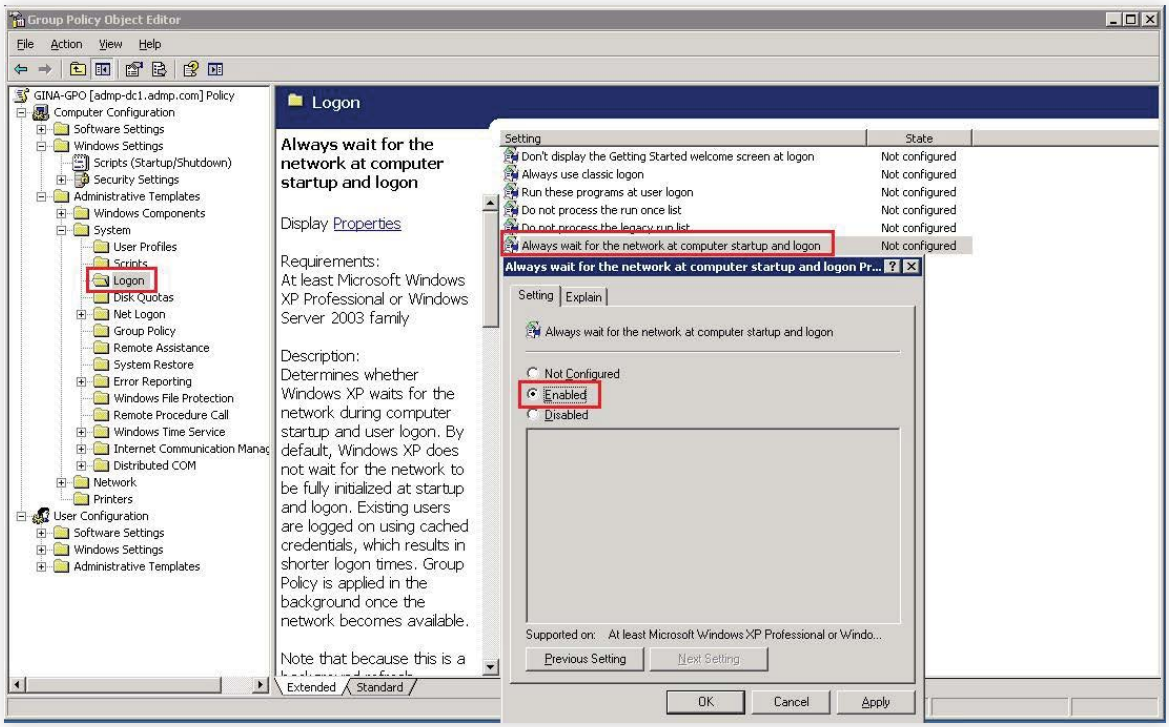
  Click **Apply**, then click **OK.**



b. Logon

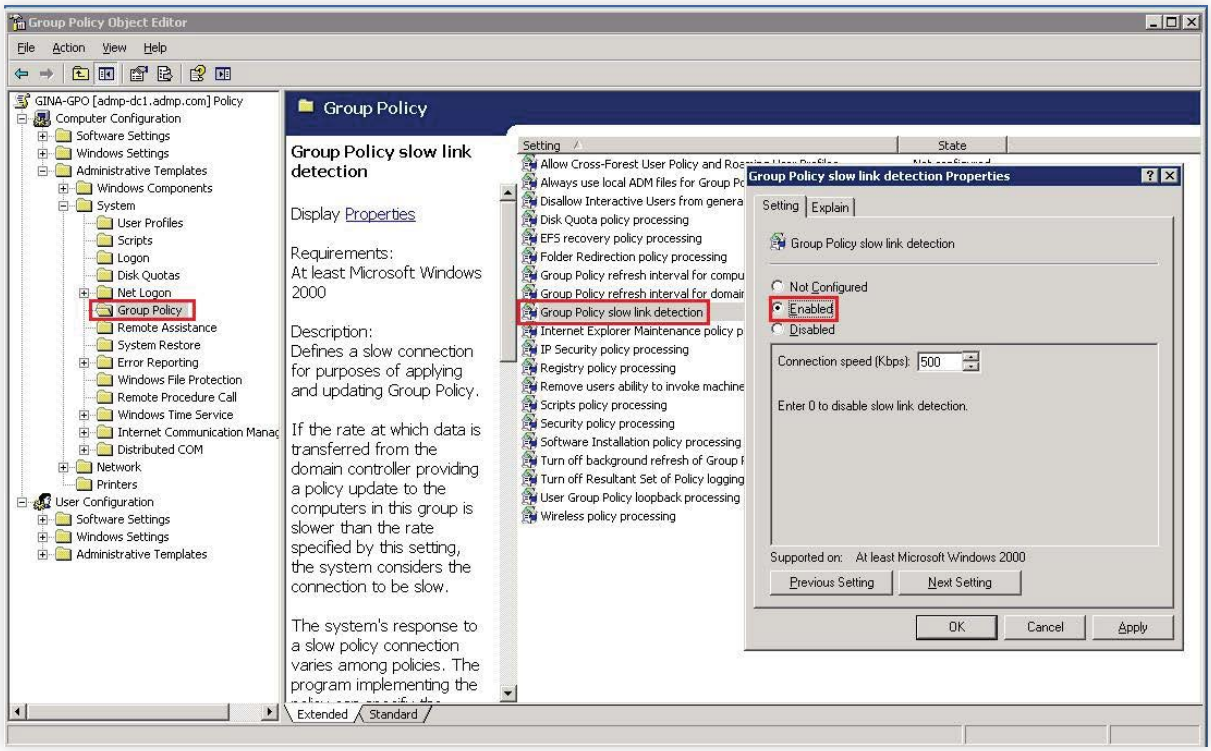
- Double-click **Always wait for the network at computer startup and logon** and select **Enabled.**

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



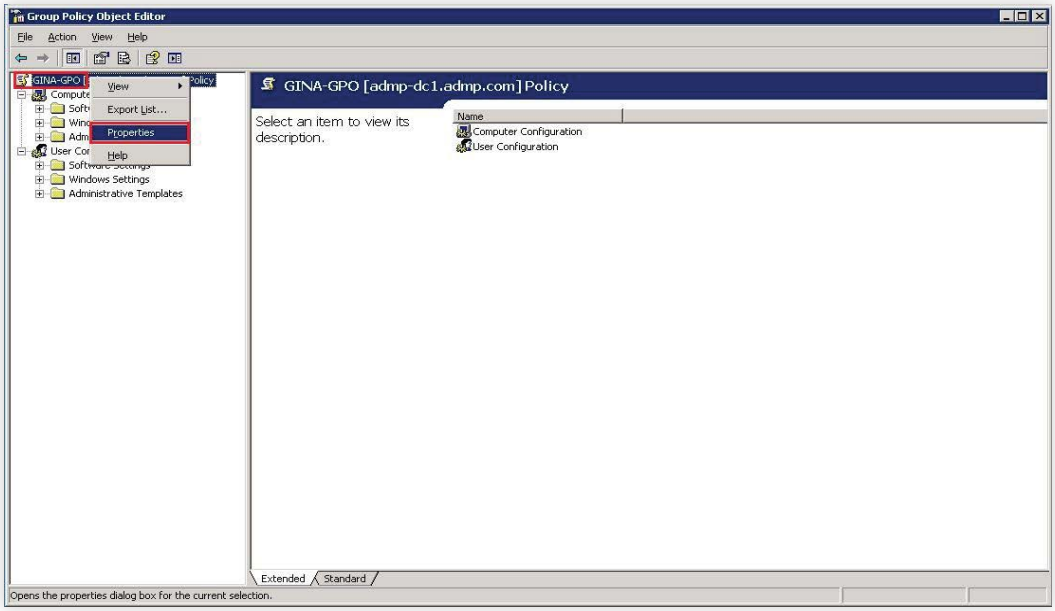
c. Group Policy

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



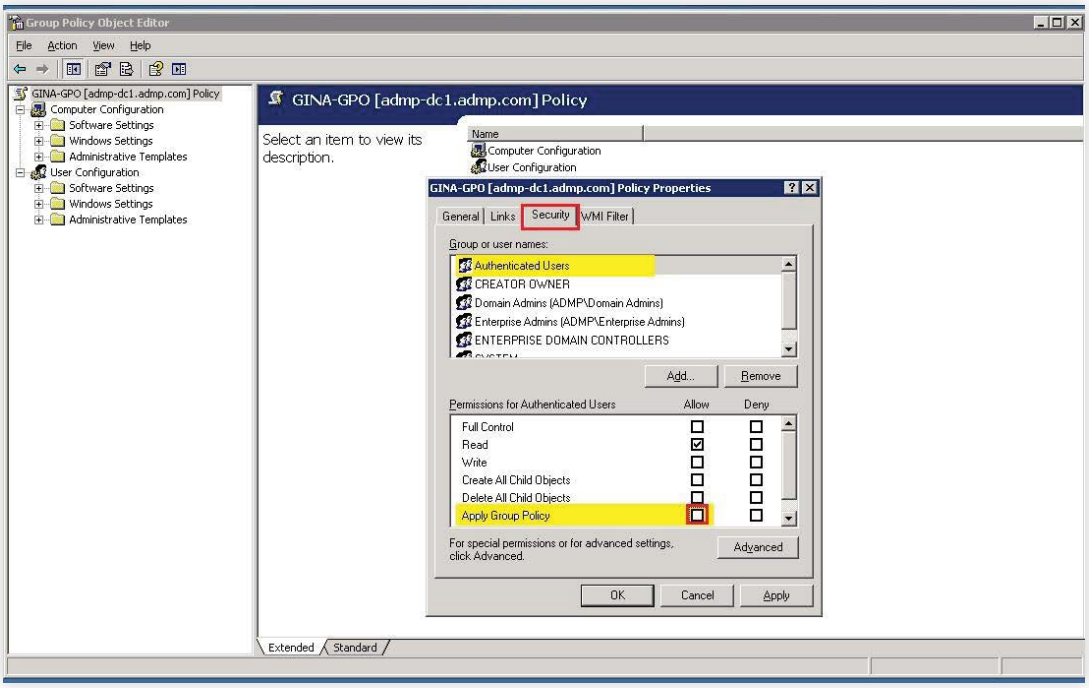
Step 4: Apply the GPO

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



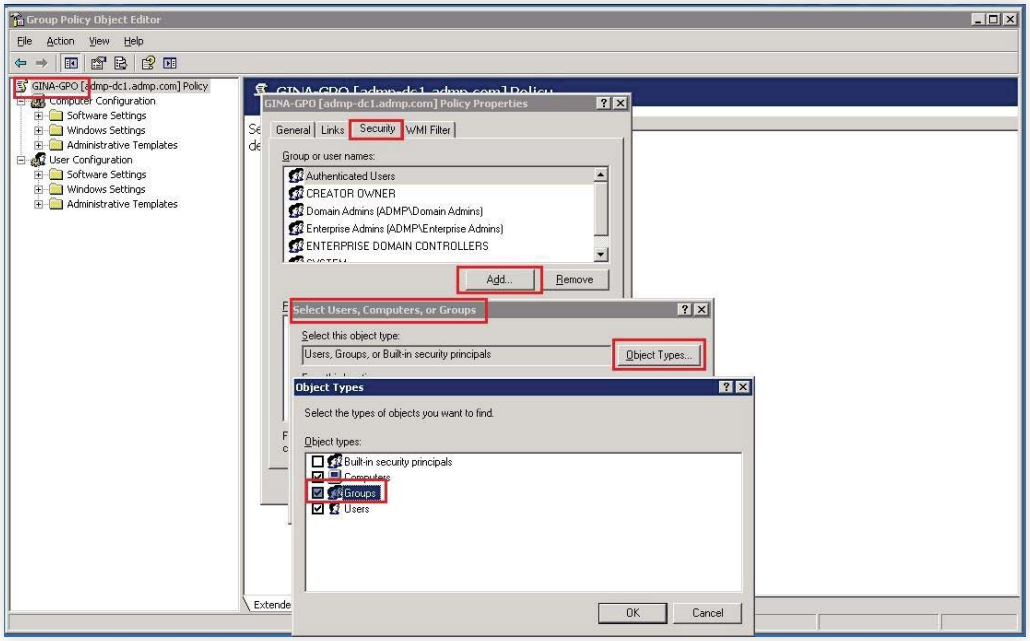
2. In the Properties dialog box that appears, click the **Security** tab.

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



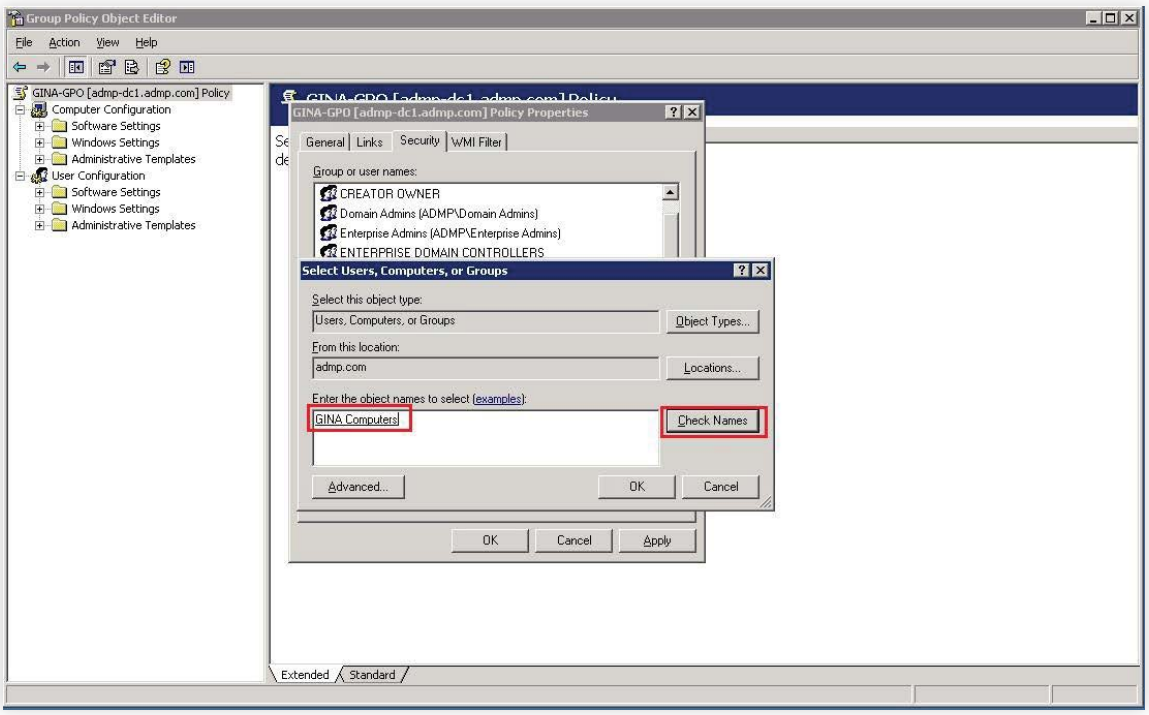
3. Click **Add** to open the *Select Users, Computers, or Groups* dialog box.

   a. Click **Object Types** and make sure **Groups** is checked, then click **OK.**

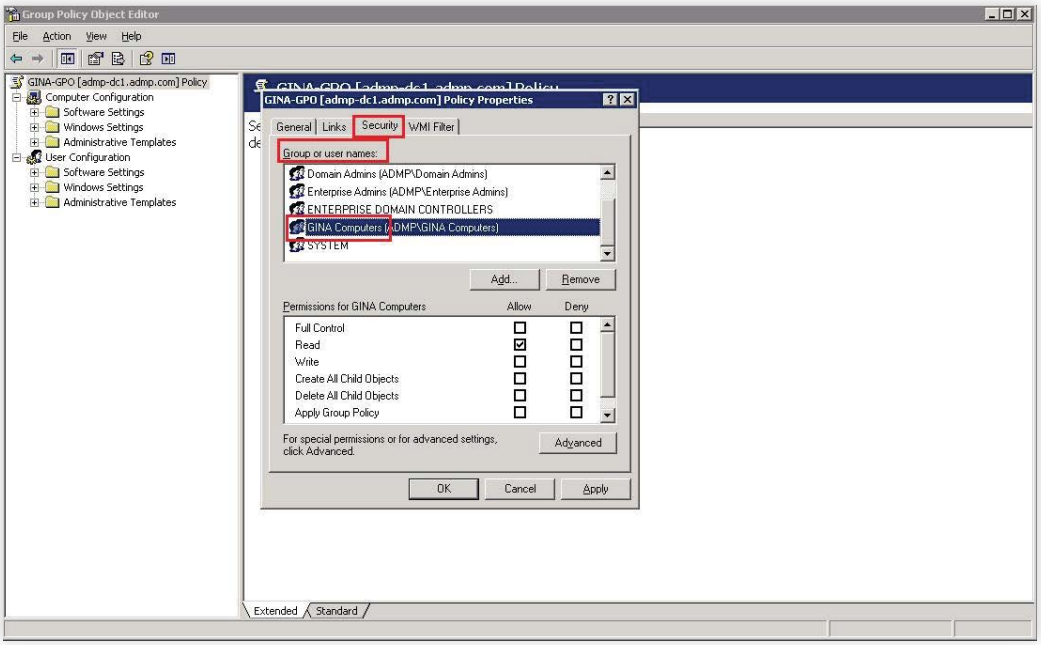


4. Enter the name of the group that contains all the computers set for login agent installation and click **Check Names.**

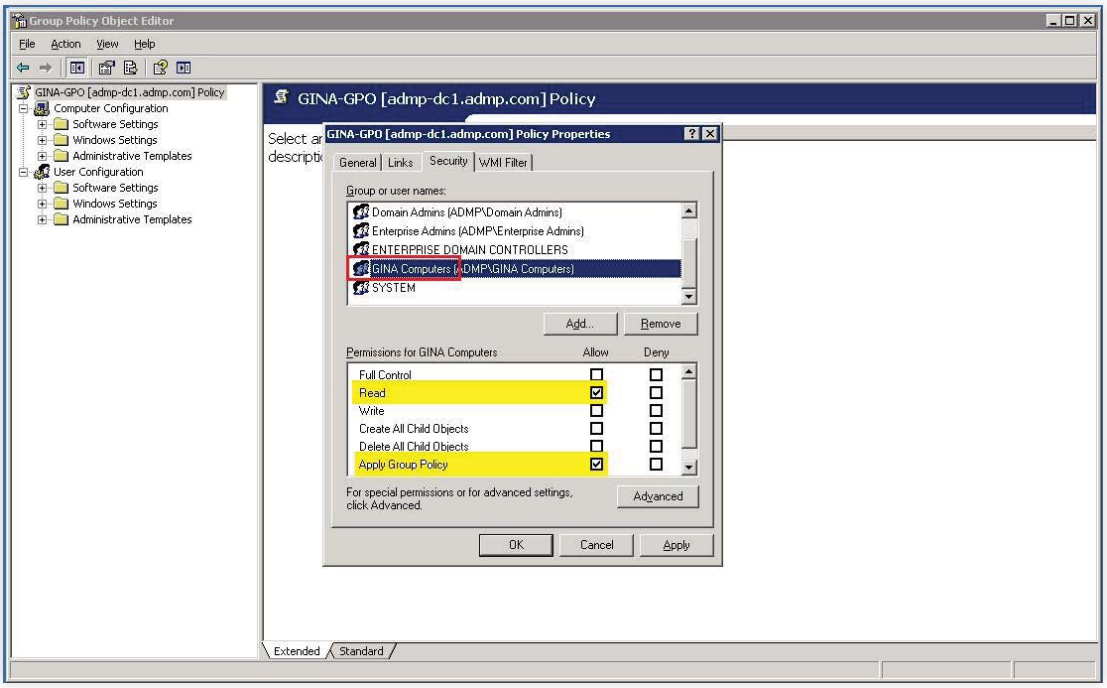
- Highlight the desired group and click **OK** to return to the *Security* tab.
- The group will now be added to the list of *Group or user names.*



5. With the newly added group highlighted, apply the following permissions:
   a. For *Read*, check **Allow.**
   b. For *Apply Group Policy,* check **Allow.**
   c. 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 logon 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:

a. Follow steps 1 and 2 shown above.

b. Click **Object Types**. Make sure **Computers** is checked. Click **OK.**

c. Use **Check Names** to find the necessary computers. Highlight the computers you want to add and click **OK** to return to the **Security** tab.

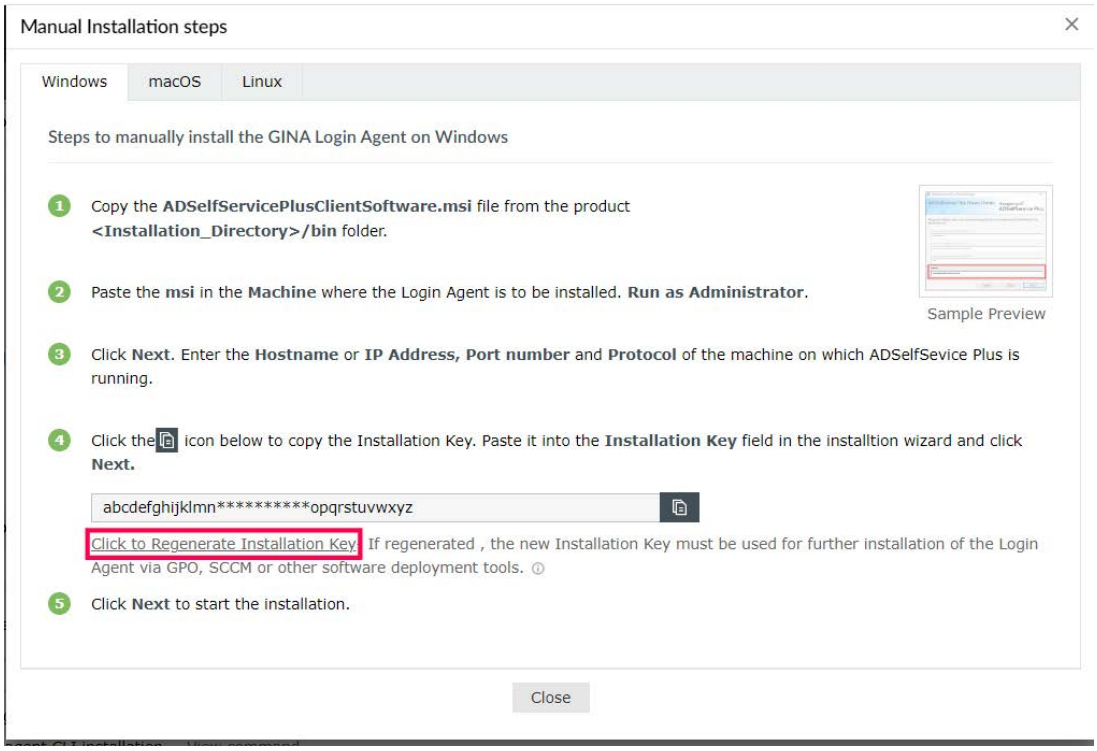
d. Set the *Read* and *Apply Group Policy* permissions to **Allow**, for every computer that you just added.

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

f. Reboot all the client machines.

Login Agent Installation Key

The Installation Key links the ADSelfService Plus Server and Client securely. To generate a new Installation Key, login to ADSelfService Plus' Admin portal, and go to **Configuration > Administrative Tools > GINA /Mac/Linux (Ctrl+Alt+Del).** Under the *Installation Help Guide* section, click on **Manual Installation Steps.** Regenerate the Installation Key using the link in Step 4.



Note:

- Please treat the Installation Key like a password. It is sensitive information and must not be shared. Please regenerate a new Installation Key using the link in the product GUI if the current Installation Key is compromised.

- If a new Installation Key is regenerated, copy the command with the new Installation Key from the product admin portal and update the Installation Command field with the new command for all new installations.

- The generation of a new Installation Key will not affect the existing installations of the Login Agent on installed machines.

Testing and diagnostics

To test whether the installation was successful:

1. In the *Command Prompt* of your client machines, type **gpresult /v.**
2. Ensure that:

- The GPO you configured appears under the subheading *Applied Group Policy Objects.*
- *ReinstallAgent.vbs* appears under the subheading *Startup scripts.*

To diagnose, please check the *AdsspScriptlog.txt* file in the Windows directory (stored in C:\\Windows by default) or go to **Start > Run** and type **%windir%\AdsspScriptlog.txt.**

If you need any further assistance or have any questions, send us an email at support@adselfserviceplus.com, or give us a call at +1.408.916.9890.

Visit: www.adselfserviceplus.com