ManageEngine
ADSelfService Plus

Guide to integrate

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

www.adselfserviceplus.com

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 5
- Configure important settings 9
- Apply the GPO 11

Troubleshooting tips 15

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 logon 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 logon 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

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:

License prerequisites

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

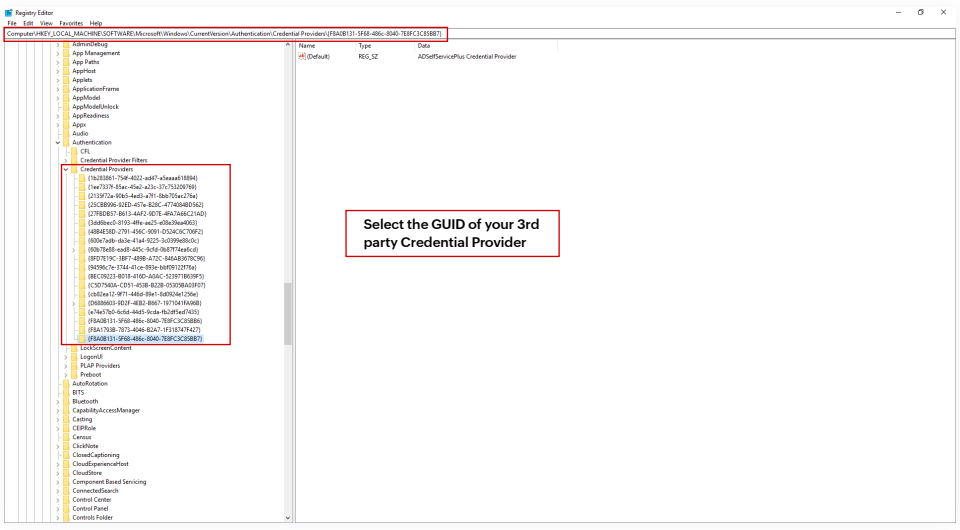
Support for third-party Credential Providers

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 installation of ADSelfService Plus login agent:

   msiexec.exe /i ADSelfServicePlusClientSoftware.msi SERVERNAME="SERVER_NAME" PORTNO="8888" WrappingProvider="<GUID>" /qn

4. **Reboot** the machine.

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:

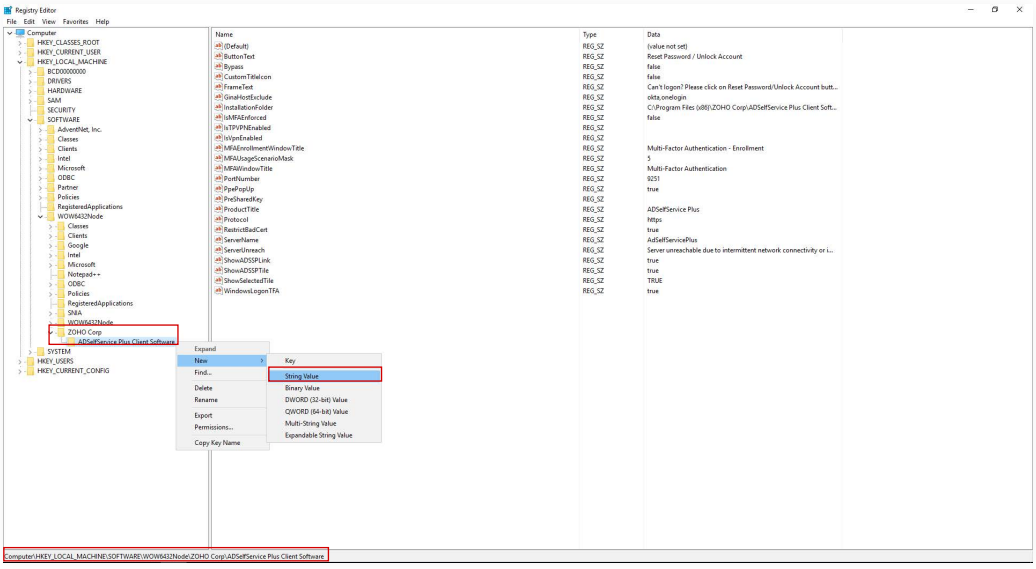
1. Open Registry Editor (open **Run >** type **regedit >** press **OK**).
2. Navigate to **ADSelfService Plus Client Software > New > String Value** and create a new **String Value** called **WrappingProvider** in the following registry key:

For 32-bit machines:

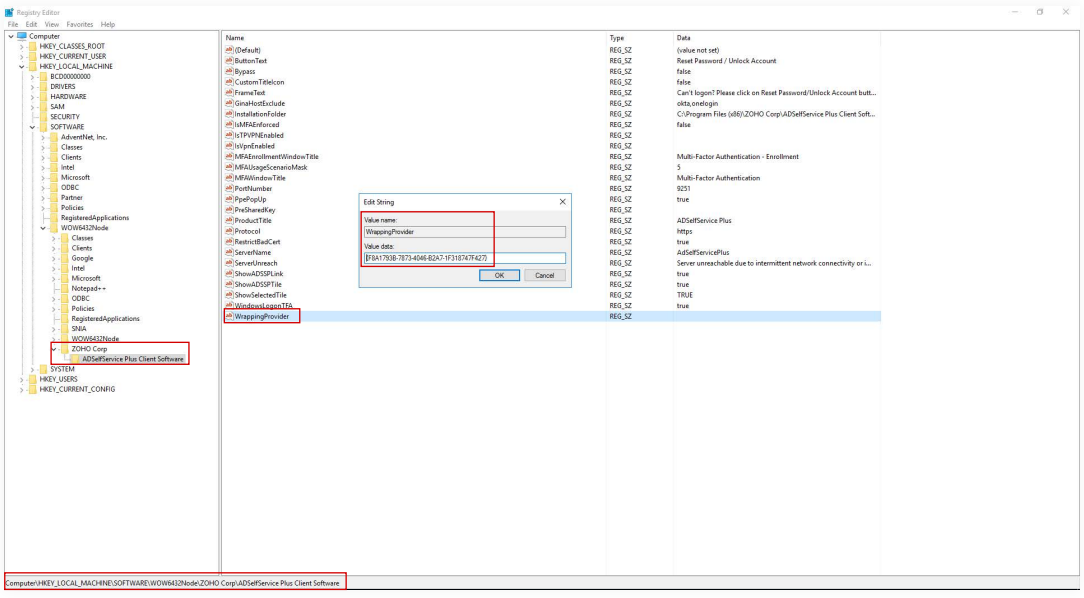
HKEY_LOCAL_MACHINE\SOFTWARE\ZOHO Corp\ADSelfService Plus Client Software

For 64-bit machines:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ZOHO Corp\ADSelfService Plus Client Software



3. Provide the unique **GUID** of your third-party Credential Provider as its value.



4. **Reboot** the machine.

Steps for bulk configuration via Group Policy

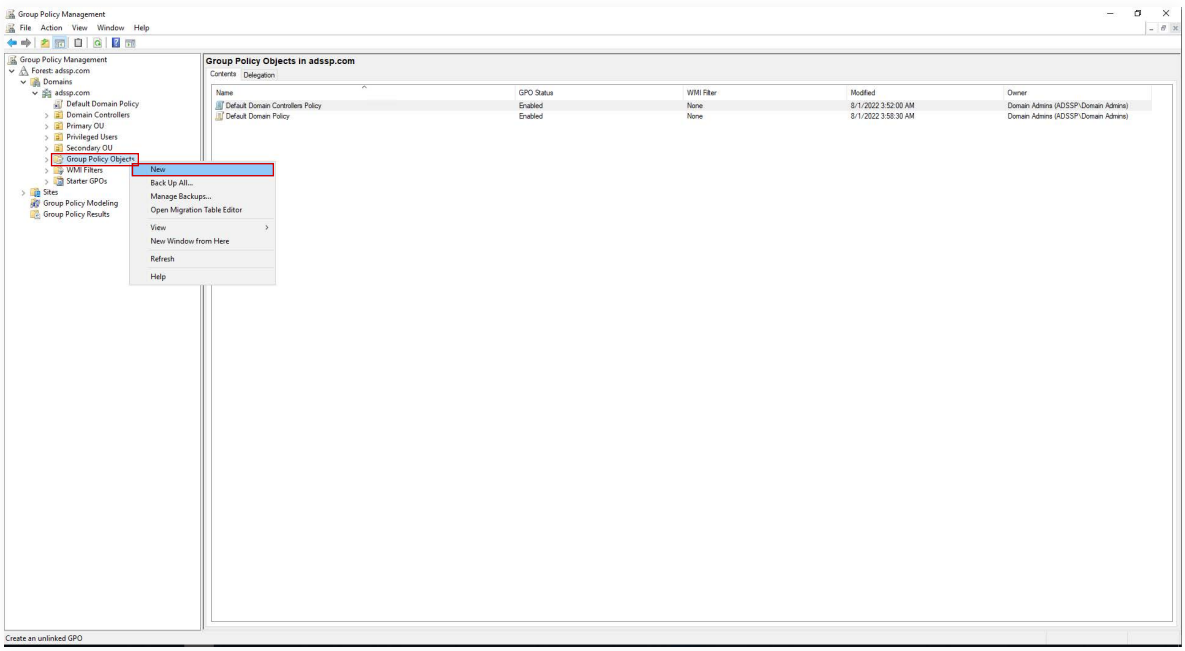
In a large IT environment, configuring credential providers individually for each machine is not feasible. In such cases, you can follow the bulk configuration steps given below to make your third-party credential providers compatible with the ADSelfService Plus login agent.

Important: Before starting with the process, download the ConfigureCP.bat files (download and extract it from the zipped folder) and place it in one of the server's shared network folders.

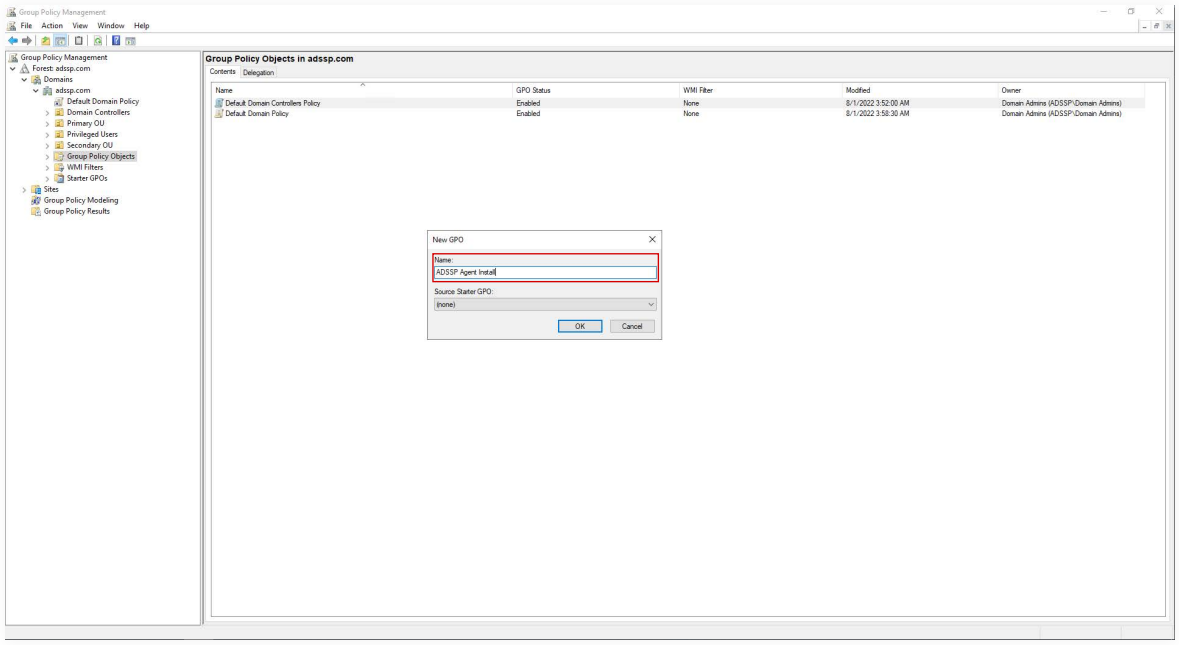
STEP 1 Create a Group Policy Object

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:

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



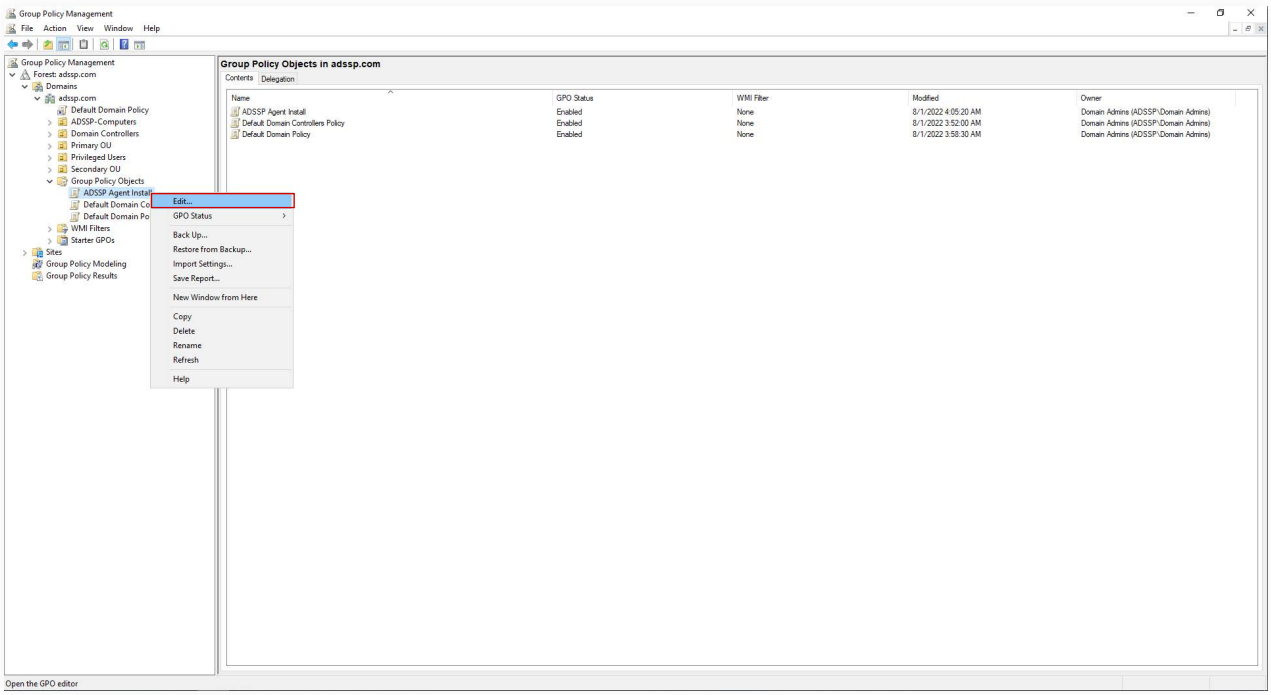
3. Give a descriptive name to the GPO and click **OK.**



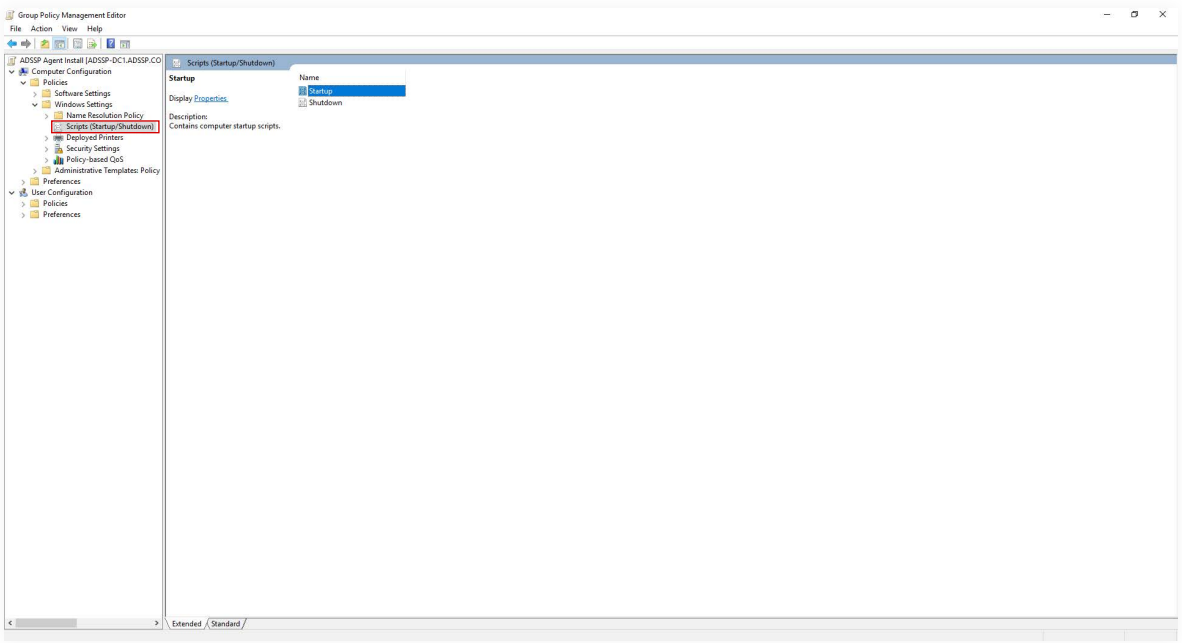
STEP 2 Configure script settings

After creating the GPO you have to configure its script settings to run the batch file. Follow the steps given below:

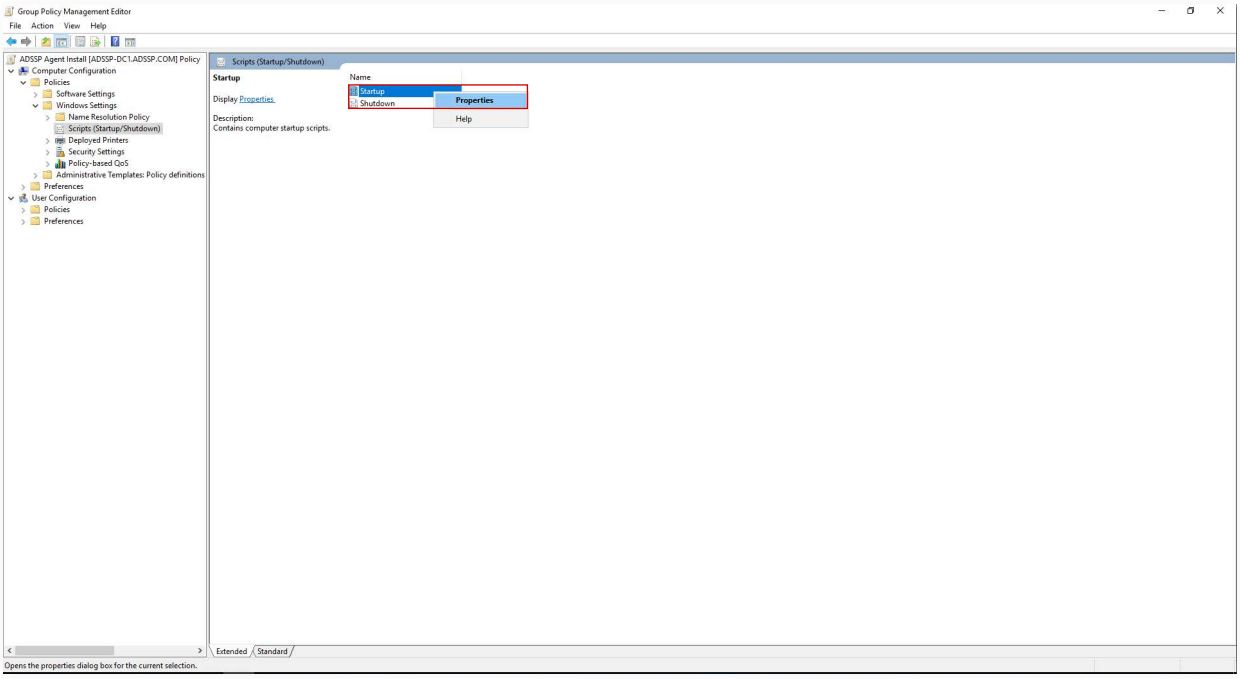
1. Right-click the **GPO** that you just created and select **Edit** to open the Group Policy Management Editor.



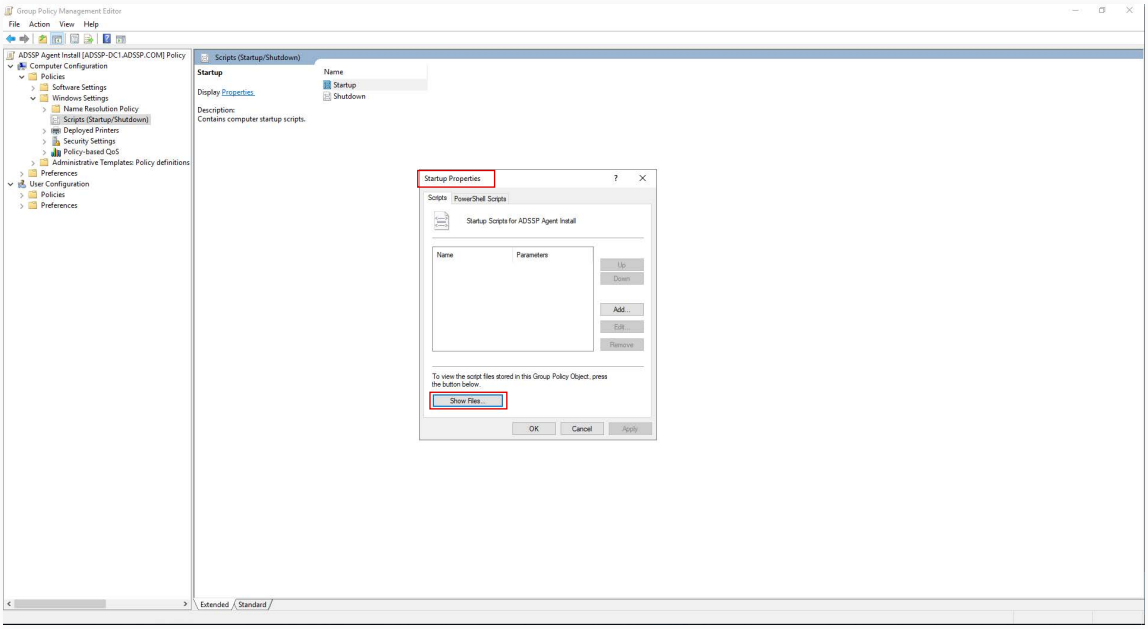
2. In the Group Policy Management Editor, on the right pane, double-click **Computer Configuration > Policies >Windows Settings > Scripts (Startup/ShutDown) > Startup.**



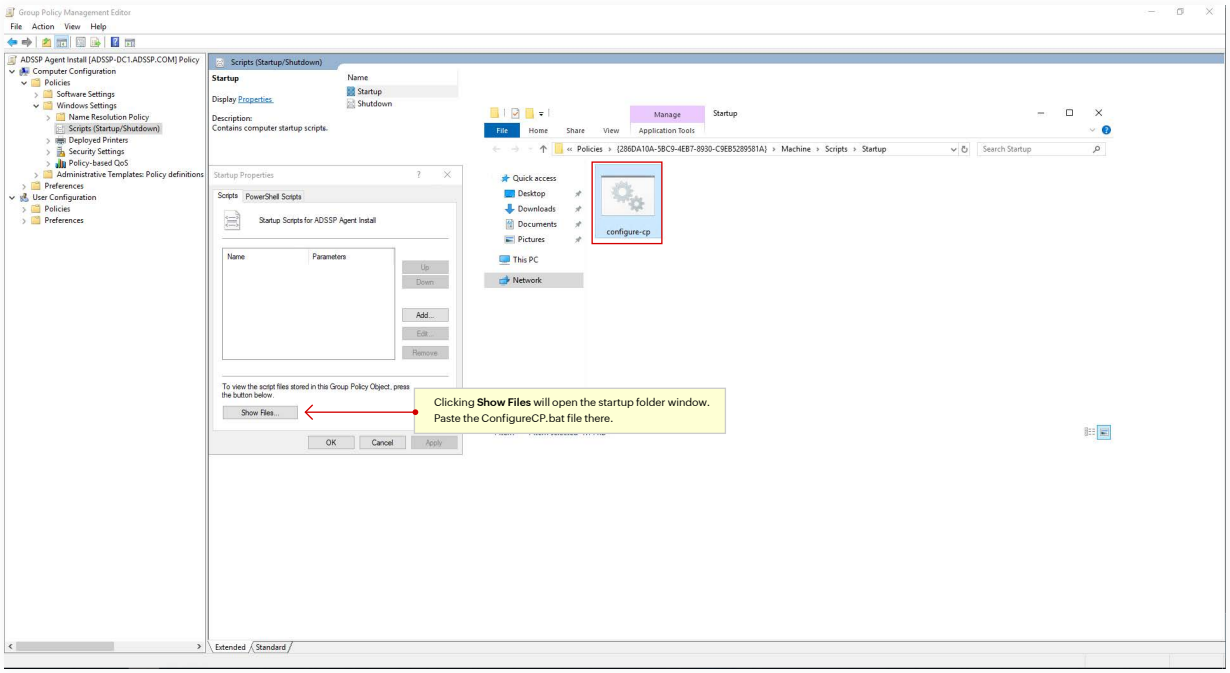
3. Right-click **Startup** and select **Properties.**



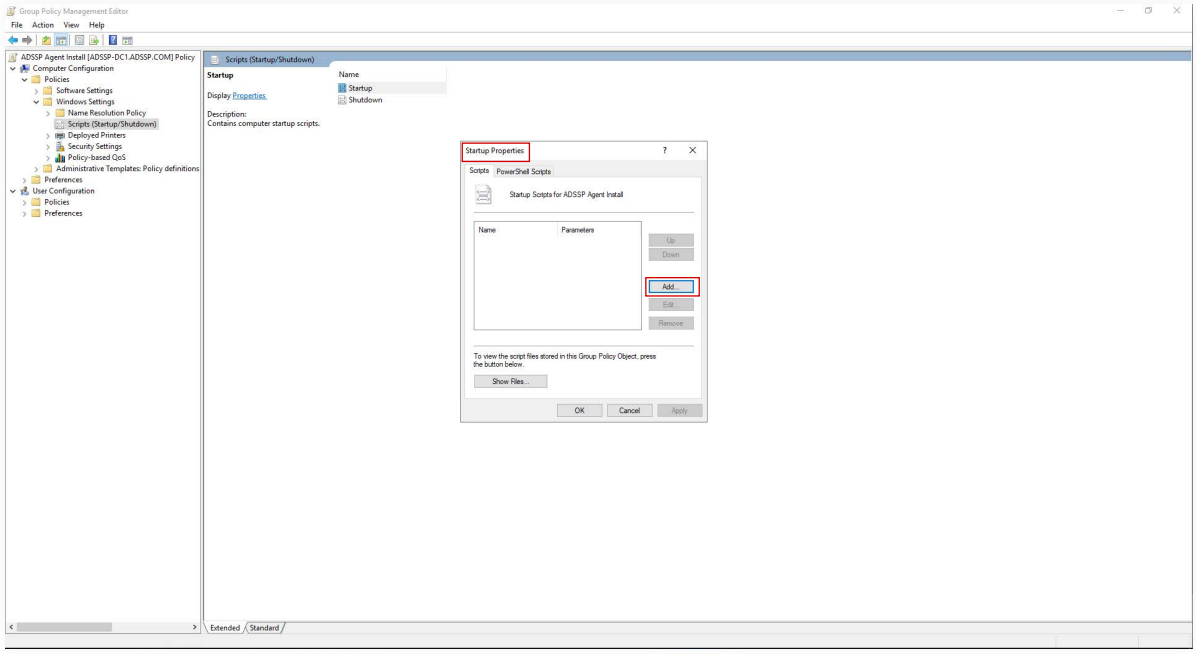
4. In the *Startup Properties* dialog box, click **Show Files.**



5. Paste the *ConfigureCP.bat* file into the *Startup* folder that opens, and then close the window.



6. Click **Add** in the *Startup Properties* dialog box.

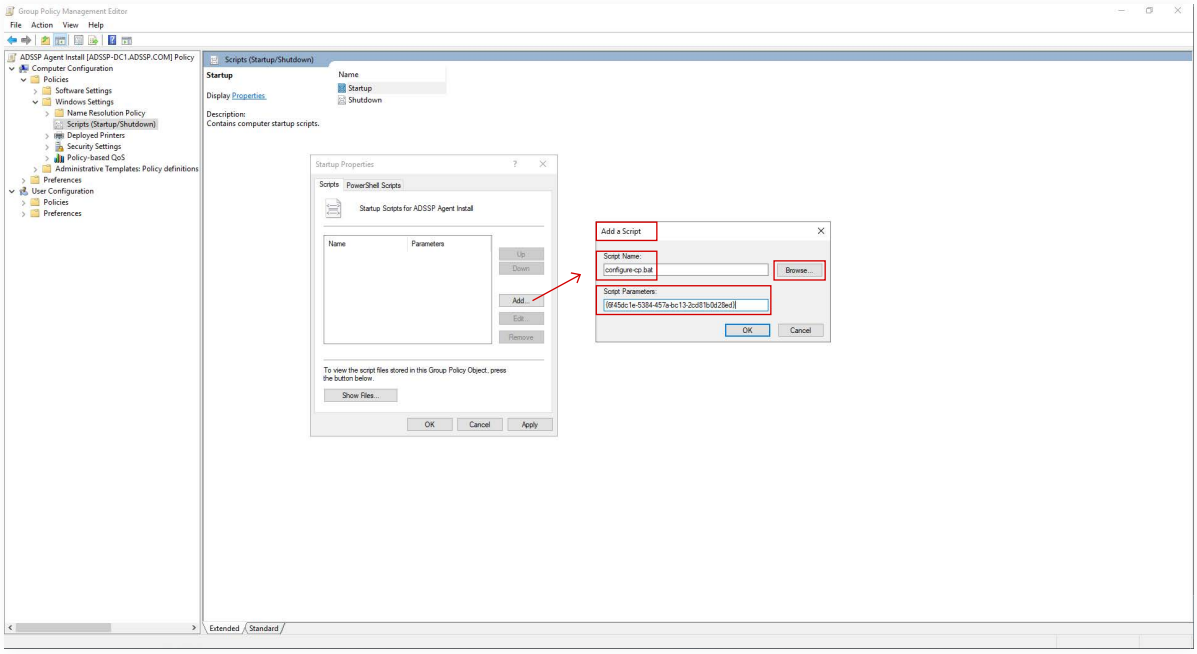


7. In the *Add a Script* dialog box do the following:

   i. Under *Script Name*, click **Browse** and select ***ConfigureCP.bat.***

   ii. Enter the GUID of your third-party Credential Provider as *Script Parameter.*

> For example, if the GUID of your third-party credential provider is 6f45dc1e-5384- 457a-bc 13-2cd81b0d28ed, then the syntax for the parameter is {6f45dc1e-5384-457a-bc 13-2cd81b0d28ed}.



iii. Once set, click **OK** to return to the *Startup Properties* dialog box.

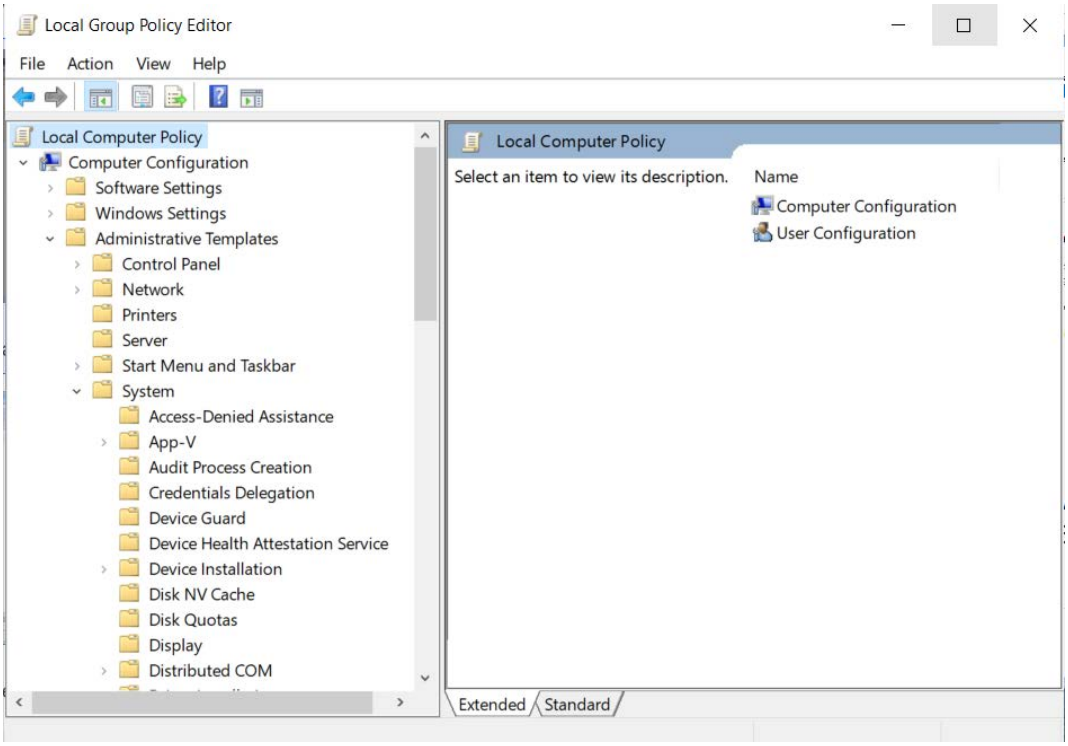
8. Click **Apply** first and then click **OK** to complete the procedure.

Important: Before setting the parameter, check the accessibility of the *ConfigureCP.bat* file.

STEP 3 Configure important settings

Once you have completed the steps above, configure the Administrative Template settings as shown below:

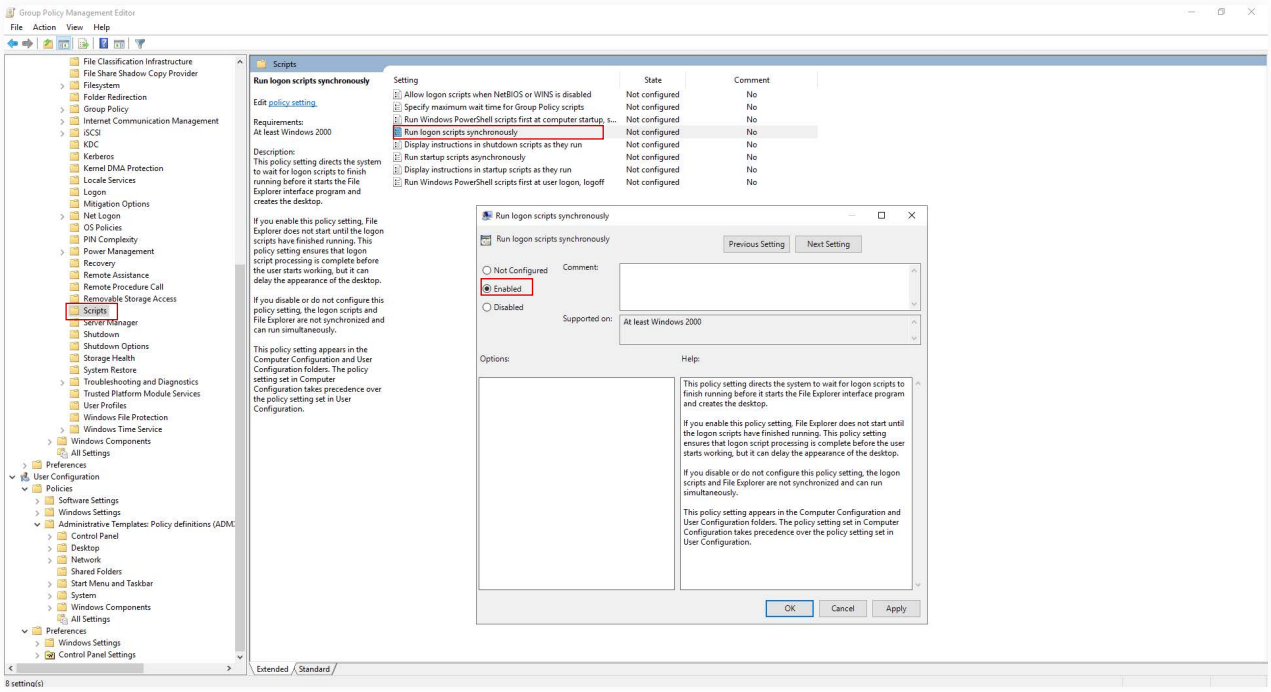
1. On the left pane of the Group Policy Management Editor, go to **Computer Configuration > Administrator Templates > Systvem.**



2. Under System, configure the following settings:

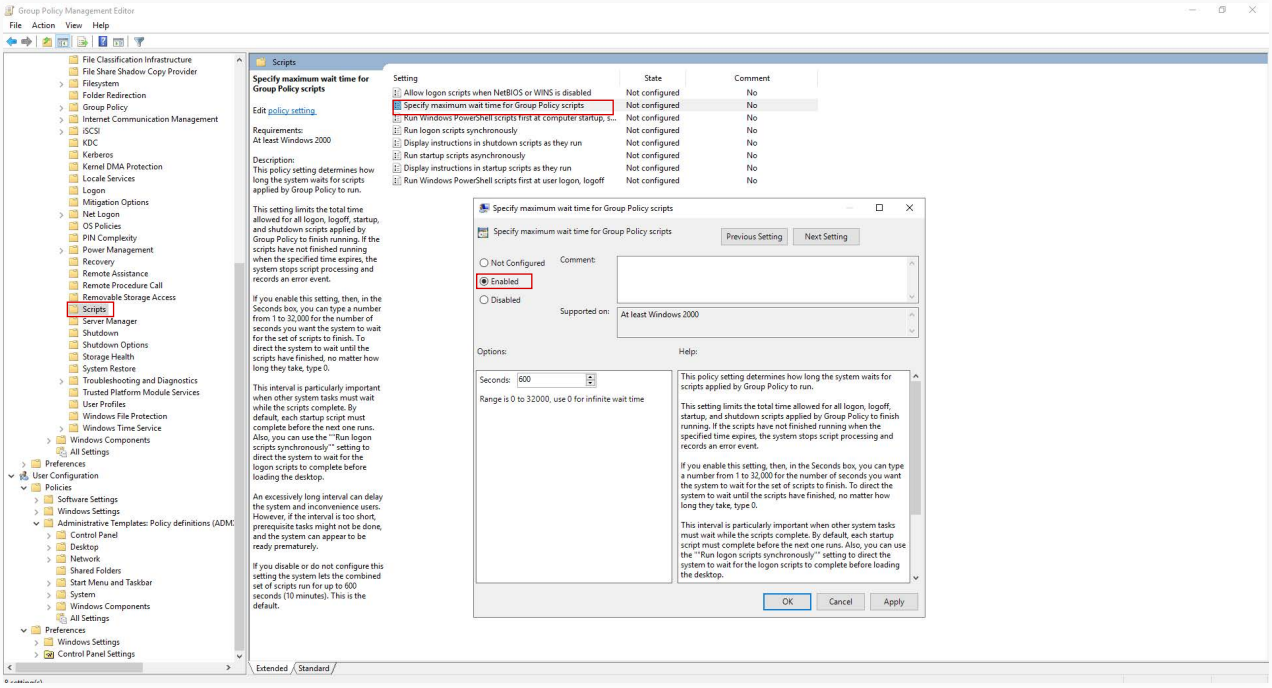
a. Scripts

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



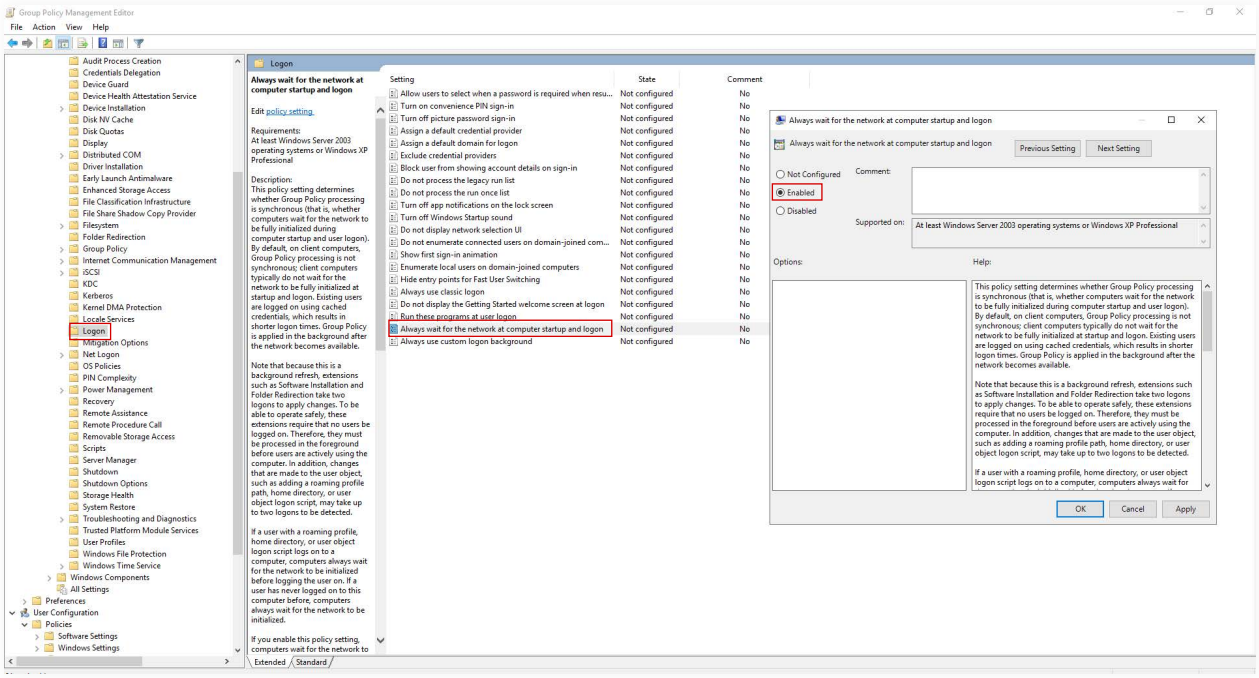
- Double-click **Specify maximum wait time for Group Policy scripts** and select **Enabled.**

  Click Apply, then **OK.**



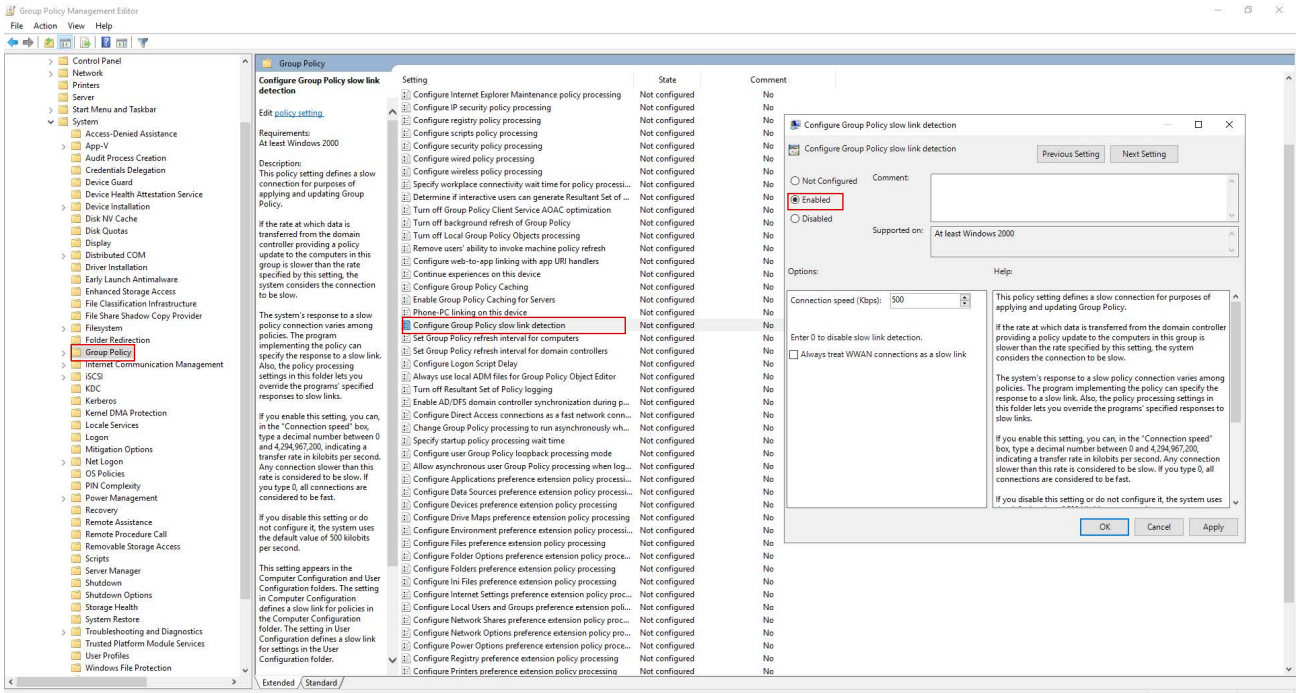
b. Logon

- Double-click **Always wait for the network at computer startup and logon** and **Enabled.** Click **Apply,** and then **OK.**



c. Group Policy

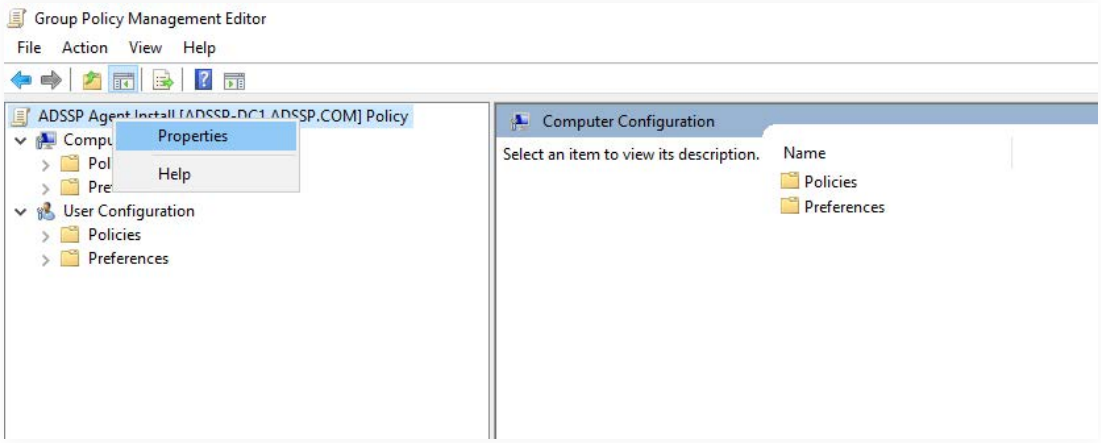
- Double-click **Configure Group Policy slow link detection** and select **Enabled**. Click **Apply**, then **OK**.



STEP 4 Apply the GPO

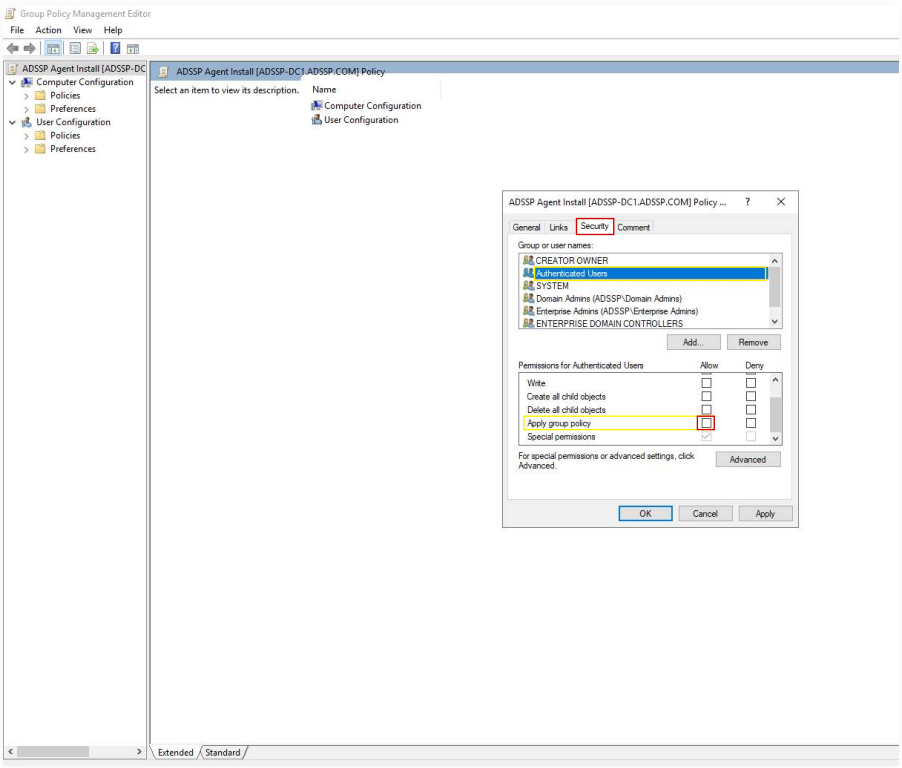
Once the Administrative Template settings are configured, apply the GPO to the desired computers in the network by following the steps below:

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.**

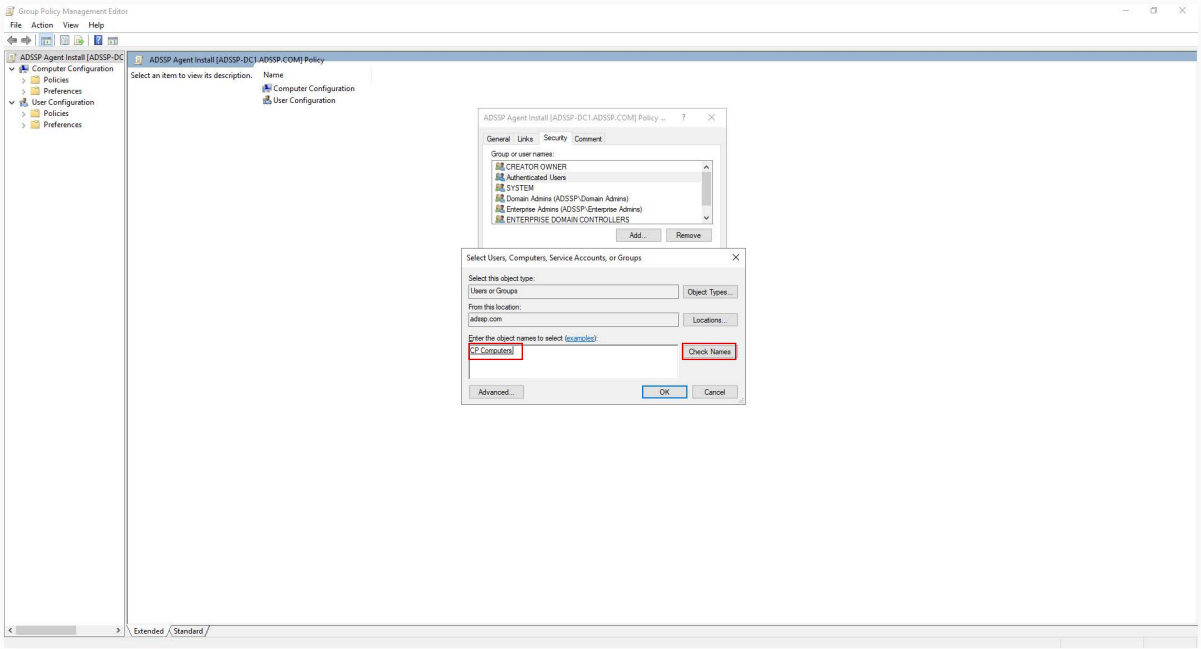


2. Click **Security** tab, in the properties dialog box that appears.

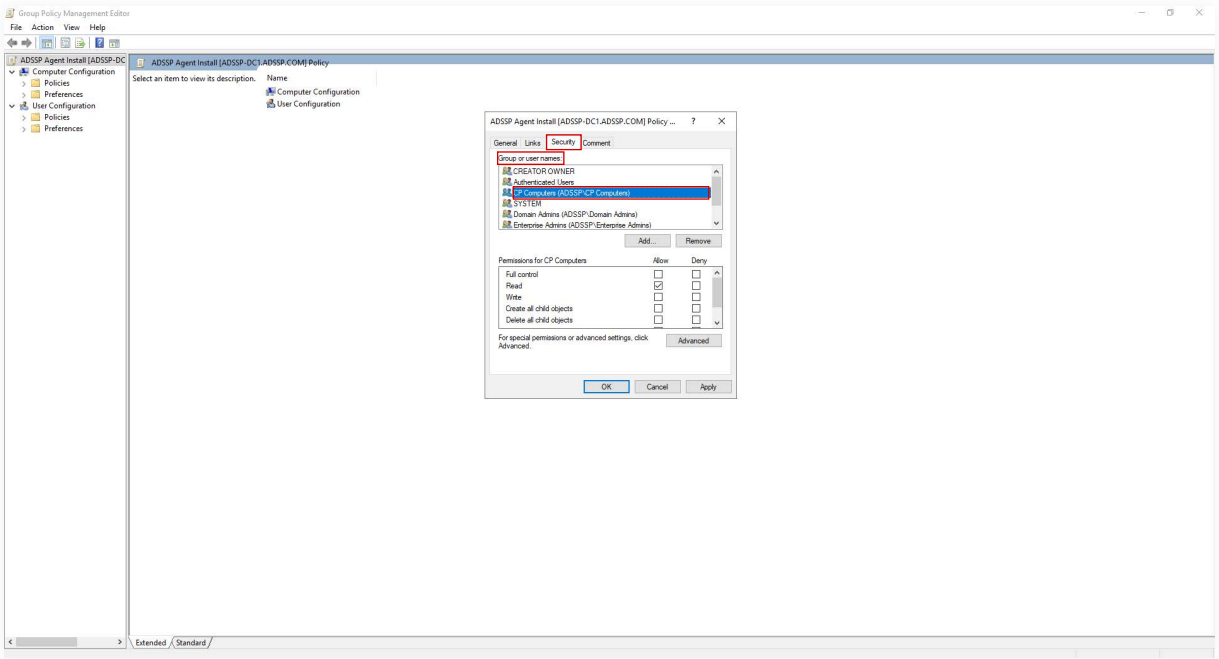
Important note: On the **Security** tab, remember to uncheck the **Apply group policy** permission under **Authenticated Users** before proceeding further.



3. Enter the name of the group that contains all the computers running Windows Server 2008 and above as well as Windows Vista and above, then click **Check Names**. Highlight the desired group and click **OK** to return to the **Security** tab.

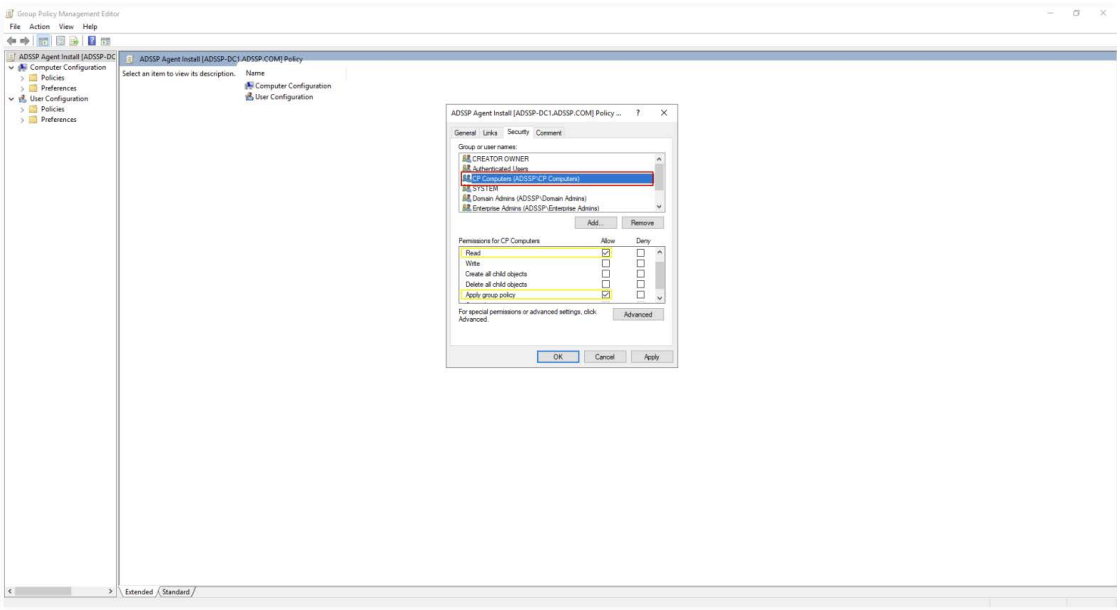


The group will now be added to the list of *Group or user names* under the **Security** tab



4. With the newly added group highlighted, set the Read and Apply group policy permissions to **Allow**.

5. Click **Apply,** then **OK**.



6. Reboot the computers to apply the GPO and wait until the next startup for the settings to take effect.

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

1. Follow steps 1 and 2 shown above.
2. Click **Object Types**. Make sure **Computers** is checked. Click **OK.**
3. Use **Check Names** to find the necessary computers. Highlight the desired computers you want to add and click **OK** to return to the **Security** tab.

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

Important note: After completing all of these steps, remember to uncheck the **Apply group policy** permission under **Authenticated Users.**

4. **Reboot** all the client machines.

Troubleshooting tips

If you are experiencing any problems on the Windows logon 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.*