Guide to integrate ADSelfService Plus **client software** with **third party** Winlogon extensions
Contents

ADSelfService Plus - Introduction: ................................................................................................................ 3
ADSelfService Plus Client Software: .............................................................................................................. 3
Support for 3rd party GINA/Credential Provider agents: ............................................................................. 5
  For Credential Providers: ................................................................................................................................................ 5
  For GINA: ................................................................................................................................................................................ 7
    Cisco VPN client .................................................................................................................................... 7
    Sophos safeguard disk encryption ........................................................................................................ 7
    Checkpoint Full Disk Encryption (pre-boot authentication is not supported) ......................................... 7
    Other 3rd Party GINA clients ............................................................................................................. 8
    VPN GINA Clients ................................................................................................................................ 10
Steps for Bulk Configuration via Group Policy: ........................................................................................... 11
  Step 1: Create Group Policy Objects ...................................................................................................................... 11
  Step 2: Configure Script settings ................................................................................................................ 14
  Step 3: Important Settings: ........................................................................................................................................... 20
  Step 4: Applying the GPO ....................................................................................................................................... 23
Troubleshooting Tips: ......................................................................................................................................... 29
**ADSelfService Plus - Introduction:**

ADSelfService Plus is a secure, web-based, end-user password reset management program. With ADSelfService Plus, end-users can:

- Self-service Reset Password
- Self-service Unlock Account
- Receive Password/Account Expiry Notification
- Self-service Update directory information
- Search Corporate/Employee directory
- Winlogon (Ctrl+Alt+Del) Password Reset

It helps administrators to delegate the task of password reset and account unlock to end-users, while minimizing the cost and effort involved with help desk calls.

**ADSelfService Plus Client Software:**

With web-based self-service softwares, the end-users need not rely on helpdesk personnel for reset password/account unlock operations anymore. But, there is still a small element of dependency involved: the user, who has forgotten the password needs a neighbor’s machine or a dedicated kiosk to carry out the required self-service operations. ADSelfService Plus, with the help of its Client Software, eliminates such dependencies by adding a button labeled ‘Reset Password/Unlock Account’ to native Windows log-on prompt.

ADSelfService Plus Client Software is an extension of the standard GINA/Credential Provider from Microsoft. Such GINA/Credential Provider extensions are now widely used by 3rd party software providers to offer a wide range of functionality like ‘Secure VPN access’ and ‘Full Disk Encryption’. But, some of these extensions may not be compatible with others, and thus limits the features that can be added to the Windows logon screen.

Fear not! ADSelfService Plus Client Software can be configured to work with your 3rd party GINA/Credential Provider extension. Some of the 3rd party GINA/Credential Provider agents supported by ADSelfService Plus are:
**CREDENTIAL PROVIDER AGENTS**

- Zenworks Endpoint Security agent
- 2X agent
- Toshiba Logon Provider
- Cisco NAC agent
- OneX Credential Provider

**Note:** You need to configure the Windows registry settings to make ADSelfService Plus Client Software compatible with the above mentioned Credential Provider agents. Please [click here](#) for the configuration steps.

**GINA AGENTS**

- Sophos Safeguard Disk Encryption
- Cisco VPN client
- Checkpoint Full Disk Encryption

**Note:** ADSelfService Plus has built-in support for the above mentioned GINA agents. Hence, no configuration is required from your side.

Additionally, by editing the Windows registry settings, more 3rd party GINA/Credential Provider agents can be made compatible with ADSelfService Plus Client Software. This document will provide you with all the information you need to seamlessly integrate ADSelfService Plus Client Software with your 3rd party GINA/Credential Provider extension.
Support for 3rd party GINA/Credential Provider agents:

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

For Credential Providers:

1) Open **Registry Editor** (open Run → type regedit → press OK).

2) Get the unique **GUID** (Global Unique Identifier) of your 3rd 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 Client Software:

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

4) **Reboot** the machine
Alternatively, if you have already installed ADSelfService Plus Client software and plan to deploy a 3rd party Credential Provider in your environment, then try the steps given below:

1) Open Registry Editor (open Run → type regedit → press OK).
2) 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

![Registry Editor Screenshot](image-url)
3) Provide the unique **GUID** of your 3rd party Credential Provider as its value.

For GINA:

**Note:** ADSelfService Plus has built-in support for the following GINA agents:

- Cisco VPN client
- Sophos safeguard disk encryption
- Checkpoint Full Disk Encryption (pre-boot authentication is not supported)

No configuration is required from your side for the above mentioned GINA agents.

4) **Reboot** the machine
Other 3rd Party GINA clients

To configure other 3rd party GINA agents, try the steps given below:

1) Open **Registry Editor** (open Run → type `regedit` → press OK).
2) Create a **String Value** called ‘GinaDLL’ in the following registry key:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
3) Provide '<install_dir>\ZOHO Corp\ADSelfService Plus Client Software\ADSSPGina.dll' (for 32-bit machine) or '<install_dir>\ZOHO Corp\ADSelfService Plus Client Software\ADSSPGina64.dll' (for 64-bit machine) as its value.

E.g.: C:\Program Files\ZOHO Corp\ADSelfService Plus Client Software\ADSSPGina.dll

4) Now, create a String Value called 'OrigGina.dll' in the following registry entry:

   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

5) Provide 'XYZ.dll' as its value, where 'XYZ' is the name of your 3rd party GINA. Please contact your 3rd party GINA provider for information on the exact GINA file.

6) Reboot the machine.
 VPN GINA Clients

If you are using a 3rd party VPN Gina client, then it must be loaded first before any other GINA agents. In such cases, follow the steps given below:

1) Open **Registry Editor** (open Run → type regedit → press OK).
2) Create a **String Value** called ‘GinaDLL’ in the following registry key:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

3) Provide ‘XYZ.dll’ as its value, where ‘XYZ’ is the name of your 3rd party GINA

4) Now, create a **String Value** that points to ADSelfService Plus GINA in you 3rd party's registry key.

   **For example:**
   Let’s assume that you are using Sophos Safeguard Disk Encryption GINA component in your environment. Open the registry editor and make the registry changes as shown below:

   1) HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
      "GinaDLL"="SGGINA.DLL"
   2) HKEY_LOCAL_MACHINE\SOFTWARE\Utimaco\SGLogon (3rd party registry key)
      "Original Gina"="ADSSPGina.dll"

5) Provide ‘<install_dir>\ZOHO Corp\ADSelfService Plus Client Software\ADSSPGina.dll’ (for 32-bit machine) or ‘<install_dir>\ZOHO Corp\ADSelfService Plus Client Software\ADSSPGina64.dll’ (for 64-bit machine) as its value.

6) **Reboot** the machine.
Steps for Bulk Configuration via Group Policy:

In a large IT environment, configuring GINA/Credential Provider agents individually for each machine is not feasible. In such cases, you can follow the bulk configuration steps given below, to make your 3rd party GINA/Credential Provider agents compatible with ADSelfService Plus Client Software:

**Important:** Before starting with the process, download [ConfigureGINA.bat](#) and [ConfigureCP.bat](#) files (download and extract from the zipped folder) and place them in a network shared folder of the server.

**Best Practice:** For GINA, add all the computers running Windows Server 2003/XP to one group. For Credential Provider, add all the computers running Windows Server 2008/R2/Vista/7 to another group.

**Step 1: Create Group Policy Objects**

First, you have to create two new Group Policy Objects (GPOs). One of the GPO will be configured to run ConfigureGINA.bat, and will be applied to the group containing Windows Server 2003/XP machines. The other GPO will be configured to run ConfigureCP.bat, and will be applied to the group containing Windows Server 2008/R2/Vista/7 machines.

Follow the steps given below to create a GPO:

**FOR WINDOWS SERVER 2003**

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

3) In the properties dialog box that appears, select Group Policy tab. In this tab, click New to create a Group Policy Object.
FOR WINDOWS SERVER 2008 AND LATER

1) Open **Group Policy Management** console

2) In the left pane, right-click **Group Policy Objects** container and select **New**

3) Give a descriptive name to the Group Policy Object and click **OK**
Step 2: Configure Script settings

After creating the two GPOs, you have to configure the script settings in each of these GPOs to run the respective batch files. Follow the steps given below:

1) Right-click the **Group Policy Object** that you have just created and click **Edit** to open the GPO Editor
2) In the GPO editor, on the right pane, double-click **Computer Configuration → Windows Settings → Scripts (Startup/Shut Down) → Startup**

(In Windows Server 2008 and later, **Computer Configuration → Policies → Windows Settings → Scripts (Startup/Shut Down) → Startup**
3) Right-click **Startup** and select **Properties**

a. In the **Startup Properties** dialog box, click **Show Files**
b. Paste the **ConfigureGINA.bat** and **ConfigureCP.bat** files in the ‘Startup folder’ window that opens, and then close the window.

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

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

   i. Under **Script Name**, click **Browse** and select **ConfigureGINA.bat** or **ConfigureCP.bat** depending on the GPO you are working on.
ii. For **GINA GPO**, you have to provide XYZ.dll as **Script Parameter**, where XYZ is the name of your third party GINA (Please refer your 3rd party GINA provider).
iii. For **Credential Provider GPO**, you have to enter the **GUID** of your third party Credential Provider as **Script Parameter**.

For example, let’s say the GUID of your 3rd party Credential Provider is 6f45dc1e-5384-457a-bc13-2cd81b0d28ed, then the syntax for the parameter is:

**WINDOWS SERVER 2003:**

```
"{6f45dc1e-5384-457a-bc13-2cd81b0d28ed}"
```

**WINDOWS SERVER 2008 AND LATER:**

```
{6f45dc1e-5384-457a-bc13-2cd81b0d28ed}
```

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

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

**Important:** Before setting the parameter, check the accessibility of ConfigureGINA.bat and ConfigureCP.bat
Step 3: Important Settings:
Once you have completed the above mentioned steps, configure the ‘Administrative Template Settings’ as shown below:

Administrative Template Settings

1) On the left pane of GPO Editor window, go to Computer Configuration → Administrator Templates → System
2) Under System, configure the following settings:
   i. **Scripts** –
      • In the right pane of the GPO editor, double-click Run logon scripts synchronously and Enable it. Click Apply, and then OK.
- Double-click **Maximum wait time for Group Policy scripts** and Enable it. Click Apply, and then OK.
ii. **Logon** –

- Double-click *Always wait for the network at startup and logon* and enable it. Click **Apply**, and then **OK**.
iii. **Group Policy –**
- Double-click **Group Policy slow link detection** and **Enable it**. Click **Apply**, and then **OK**.

---

**Step 4: Applying the GPO**

Once the Administrative Template settings are configured, apply the GPOs to the desired computers in the network.
1) On the left pane of the GPO editor, right-click on the GPO you are working on (available on the top left corner of the GPO editor), and select Properties.

2) Click Security Tab, in the properties dialog box that appears.

IMPORTANT NOTE: In the Security Tab, remember to uncheck ‘Apply Group Policy’ permission for ‘Authenticated Users’ before proceeding further.
3) Now, click **Add** to open the **Select Users, Computers or Groups** dialog box. There, click **Object Types** button and make sure **Groups** is checked, and then click **OK**.
4) **Enter the name of the group** (that contains all the Windows Server 2003/XP computers or all the Windows Server 2008/R2/Vista/7 based on the GPO you are working on) and click **Check Names**. Highlight the desired group and click **OK** to return to the ‘Security’ tab.
5) The group will now be added to the list of ‘Group or User Names’ under ‘Security Tab’
6) With the newly added group highlighted, apply the following permissions:

- **Read** → Allow
- **Apply Group Policy** → Allow

Click **Apply**, and then **OK**.

7) **Reboot** the computers to apply the GPO and wait till the next startup for the settings to take effect.
To apply the GPO directly to Computers:
In case you prefer to apply the GPO directly to computers instead of the group, please follow the steps given below:

a. Follow steps 1 and 2 shown above.
b. Click **Object Types** button. Make sure **Computers** is checked. Click **OK**.
c. 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.
d. Set **Read** and **Apply Group Policy** permissions to **Allow** for each and every computer that you just added.
e. **IMPORTANT NOTE:** After completing all these steps, remember to **uncheck 'Apply Group Policy'** permission for **Authenticated Users**.
f. **Reboot** all the client machines.

**Troubleshooting Tips:**
If you are experiencing any problems in the Windows logon screen after installing ADSelfService Plus Client software and making the registry changes, try the following steps to solve the problem:

- Restart your machine in **Safe Mode**
- In case of **Windows Vista and later**, remove the registry key: "{B80B099C-62EA43cd-9540-3DD26AF3B2B0}" found under HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers
- In case of **Windows XP**, remove the registry entry - "GinaDLL" found under HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon.

ADSelfService Plus is an integrated self-service password management and single sign-on solution. It helps improve productivity by allowing users to reset their forgotten passwords, unlock their accounts, and update their contact information in Active Directory. It enhances the end-user experience with a real-time password synchronizer and enterprise single sign-on. ADSelfService Plus’ Android and iOS mobile apps as well as GINA/Credential Provider login agents facilitate self-service actions for end users, anywhere, any time.