ManageEngine
ADSelfService Plus

Login Agent Installation Guide

Table of Contents

1. **Introduction** — 2
2. **ADSelfService Plus login agent** — 3
3. **System requirements** — 3
4. **Login agent installation** — 4
   - Prerequisites — 4
   - Methods of installation — 5
     - Through the ADSelfService Plus admin portal — 5
     - Manual installation — 8
       - For Windows machines — 8
         - 1. Using the MSI file — 8
         - 2. Using Command Prompt — 8
       - For macOS clients — 9
       - For Linux machines — 10
5. **Troubleshooting** — 11
6. **Frequently Asked Questions** — 20

1. Introduction

ADSelfService Plus is an integrated Microsoft Windows Active Directory (AD) self-service password management and single sign-on (SSO) solution. It helps reduce the IT help desk's workload, reduce the costs associated with help desk requests, improve employee productivity, and secure user accounts.

Highlights of the product:

- Self-service password reset and account unlock
- Multi-factor authentication for Windows, macOS, and Linux logins
- Enterprise single-sign on
- Multi-platform password synchronization
- Password expiration notification
- Password Policy Enforcer
- Directory Self-Update
- Employee Search and Organization Chart
- Self-subscription to email groups

2. ADSelfService Plus login agent

The ADSelfService Plus login agent can be installed in the Windows, macOS, and Linux machines in an organization. Upon installation, the login agent performs the following roles:

- Adds the Reset Password/Unlock Account option and enables end users to perform self-service password resets, and account unlocks directly from the logon screens of their machine.
- Configure the Endpoint MFA feature to secure native Windows, macOS and Linux logins.
- Configure the custom password policies created using the Password Policy Enforcer feature during native Windows, macOS and Linux logins.
- Updating cached credentials over VPN when AD passwords are reset or changed from remote machines.

ADSelfService Plus offers certain advanced settings to customize the login agent. These include:

- Restrict user access when there is an invalid SSL certificate - When this setting is enabled, users will not be able to access the Reset Password/Account Unlock portal if the SSL certificate applied in the product becomes invalid.
- Display the enforced password rules in a dialog box in the Windows password change screen - When this setting is enabled, a dialog box that mentions all the custom password policy rules is displayed when users reset their password in the Reset Password/Account Unlock portal.

3. System requirements

Windows

1. Windows 10
2. Windows 8.1
3. Windows 8
4. Windows 7
5. Windows Vista

MacOS

1. macOS 10.15 Catalina
2. macOS 10.14 Mojave
3. macOS 10.13 High Sierra
4. macOS 10.12 Sierra
5. OS X 10.11 El Capitan
6. OS X 10.10 Yosemite
7. OS X 10.9 Mavericks
8. OS X 10.8 Mountain Lion
9. Mac OS X 10.7 Lion
10. Mac OS X 10.6 Snow Leopard

Linux

1. Ubuntu - 16.x-19.x
2. Fedora - 27.x-31.x
3. CentOS - 7.X

Note:

While the ADSelfService Plus login agent has been officially tested and confirmed to run seamlessly on these three Linux distributions, it may support other Linux distributions as well. Please contact the support team (support@adselfserviceplus.com) to check if the Linux distribution used in your organization is supported.

4. Login agent installation

a. Prerequisites

These are the prerequisites for the installation of the ADSelfService Plus login agent in the machines in a domain.

For Windows machines:

1. The client machines have to be connected to the domain network.
2. The service account whose credentials are provided during domain configuration in ADSelfService Plus should have Domain Admin privileges.
3. If ADSelfService Plus is installed as a Windows service, it should be run by a service account with Active Directory Domain Admin privileges.
4. The client computers' administrative share should be accessible to the ADSelfService Plus server.
5. The Remote Registry service should be enabled in the Windows machines where the login agent is to be installed.
6. The ADSelfService Plus installation directory and the Remcom.exe file must be excluded from antivirus software in the ADSelfService Plus server and the Windows machines in which login agent is to be installed.

For macOS clients:

1. The client computers should be connected to the domain network.
2. The service account whose credentials are provided during domain configuration in ADSelfService Plus should have:
   - Permission to access the client computers through Remote Login.
   - Root privileges in the macOS clients.
   - Active Directory Domain Admin privileges.
3. Verify the client's integration with Active Directory.

For Linux clients:

1. The client computers should be connected to the domain network.
2. The Secure Shell Daemon (SSHD) service should be installed and active in the client.
3. The service account whose credentials are provided during domain configuration in ADSelfService Plus should have:
   - Permission to access the client computers through Remote Login.
   - Root privileges in the Linux clients.
   - Active Directory Domain Admin privileges.

b. Methods of installation

There are four ways through which the ADSelfService Plus login agent can be installed:

1. ADSelfService Plus Web Portal
2. Manual Installation
3. GPOs (Group Policy Objects)
4. SCCM (System Center Configuration Manager)

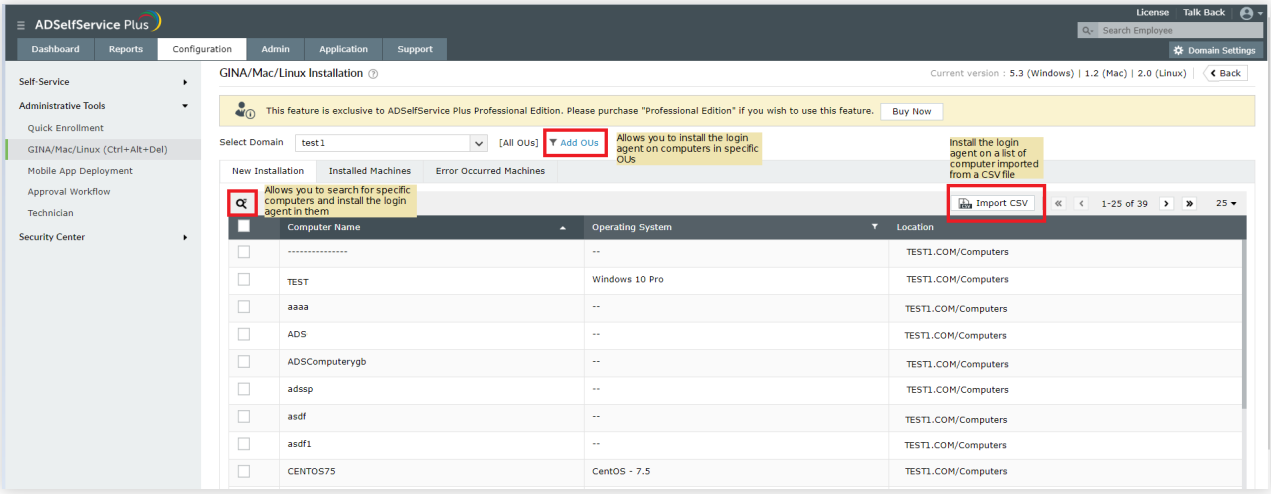
In this document, we will discuss the first two methods of installation - ADSelfService Plus Web Portal and Manual Installation. Installation via GPOs and SCCM will be discussed separately.

i. Through the ADSelfService Plus admin portal:

ADSelfService Plus admin portal is a simple and effective way to install the login agent.

Privileges Required:

To install the login agent on machines present in a domain, a user must possess the administrator credential used in configuring that domain with ADSelfService Plus.



Please follow the below steps for installation:

1. In the ADSelfService Plus web portal, go to **Configuration > Administrative Tools > GINA/Mac/Linux (Ctrl+Alt+Del) > GINA/Mac/Linux installation.**
2. Click **New Installation.**
3. Select a domain, and then the computers (on which you want to install the login agent).
4. Click **Install.**

OU Filter: Allows you to install the login agent on computers belonging to specific organizational units (OUs). Click on the OU filter icon, select the desired OUs and click **OK.**

Search: Use the Search icon to search for a specific computer and install the login agent. Click on the **Search** icon, enter the specific entry you want to search for in any of the columns and press **Enter.**

Import CSV: Allows you import a specific list of computers on which the login agent will be installed. Click Import CSV and choose the CSV file containing the names (or dnsHostNames) of the computers. Now in the list generated in the portal, select the computers in which you want to install the login agent and click **Install.**

Customization:

ADSelfService Plus login agent can be customized to suit your organization's requirements.

The following components of the login agent can be customized:

- Frame Text
- Button Text
- Icon
- Server name
- Port number

Follow the below steps for customizing the login agent:

1. In ADSelfService Plus web portal, go to **Configuration > Administrative Tools > GINA/Mac/Linux (Ctrl+Alt+Del) > GINA/Mac/Linux Customization.**
2. To edit the icon, click **Browse** and select the desired icon.
3. Enter the desired text in **Button Text** and **Frame Text** textbox fields.
4. Click on the edit icon and enter the **Server Name** and **Port Number** on which ADSelfService Plus is running.
5. Click **Save.**

Note:

Choose only BMP file for icon. The image should be 250 KB in size.

Automation:

You can automate the process of installation and customization of the login agent by using the scheduler option available in the application. To automate installation and customization of the login agent:

1. In ADSelfService Plus web portal, go to **Configuration > Administrative Tools > GINA Ctrl+Alt+Del) > GINA/Mac/Linux Schedulers.**
2. Enable the desired scheduler:
   i) **GINA/Mac/Linux Installation Scheduler** (for automating GINA/Mac/Linux installation).
   ii) **GINA/Mac/Linux Customization Scheduler** (for automating GINA/Mac/Linux Customization).
3. In case of re-scheduling, click on the **Edit** icon.
4. Select the domains in which the scheduler will be active.
5. Set the frequency (daily, weekly or monthly) to run the scheduler.
6. Click **Save.**

Note:

Clicking on the **Save** button will automatically enable the scheduler.

To disable the scheduler, click on the **Enable** icon under the **Actions** column.

Audit Trail:

ADSelfService Plus makes it easier to keep track of all the machines in which the login agent has been successfully installed, and where the installation has failed. To view this report:

1. In ADSelfService Plus web portal, go to **Configuration > Administrative Tools > GINA/Mac/Linux (Ctrl+Alt+Del) > GINA/Mac/Linux installation.**
2. Click **Installed Machines** - to view the machines in which the login agent has been successfully installed.
3. Click **Error Occurred Machines** - to view the machines in which the login agent installation has failed.

ii. Manual installation:

For Windows machines:

1. Using MSI package:

To install the login agent manually, you must run the MSI package of the login agent provided with ADSelfService Plus on each user's machine. The MSI package can be found in the installation directory (by default: ***C:\Program Files\ManageEngine\ADSelfService Plus\bin).***
To install the login agent manually, follow the below steps:

1. Copy the installer file (ADSelfSerivcePlusClientSoftware.msi) to the target machine (where you want to install the ADSelfService Plus login agent).
2. Open Command Prompt as an administrator and point it to the folder containing installer file.
3. Follow the steps provided in the wizard and finish the installation process.
4. Restart the machine.

2. Using Command Prompt:

When the login agent is installed manually using the MSI package on computers running Windows Vista and later Operating Systems with UAC (User Account Control) enabled, it may not function properly. In such cases, you can install the login agent manually through the command prompt as shown below:

1. Open command prompt as an administrator and point it to the folder containing installer file
2. Now, run the following command:

```
msiexec /iADSelfServicePlusClientSoftware.msi
SERVERNAME="<enter the name of the ADSelfService Plus server>"
PORTNO="<enter the port number>" PROTOCOL "<HTTPS>" /qn
```

If you are using HTTP as the protocol, then enter it instead of HTTPS,

Note 1:

To customize the login agent during the installation, use the following command:

```
msiexec.exe /i ADSelfServicePlusClientSoftware.msi
SERVERNAME="<enter the servername>" PORTNO="<enter the port number>"
PROTOCOL="HTTPS" NFRAMETEXT="<Can't login? Click on the Reset
Password/Unlock Account button to reset your password or unlock your
account with ADSelfService Plus>" BUTTONTEXT="Reset Password/Unlock
```

Note 2:

If you are already using a third party GINA/CP extension, use the following command to install the ADSelfService Plus login agent for seamless integration with the third party GINA/CP extension:

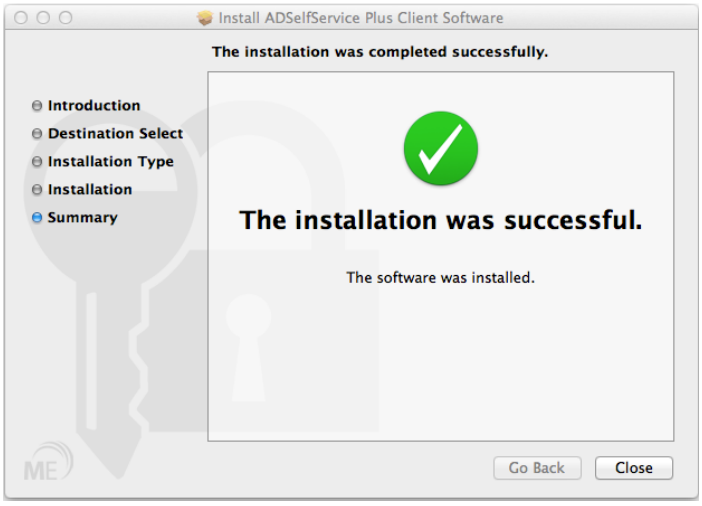
```
msiexec.exe /i ADSelfServicePlusClientSoftware.msi SERVERNAME="<enter the servername>" PORTNO="<enter the port number>" PROTOCOL="HTTPS" WrappingProvider="{<enter the GUID of your third-party GINA/CP extension>}" /qn
```

Where,
SERVER_NAME = hostname of the ADSelfService Plus server
PORTNO = port no of ADSelfService Plus (even if SSL is enabled)
PROTOCOL = http or https
FRAMETEXT = description text
BUTTONTEXT = text that appears on the login agent button
PROD_TITLE = title of the login agent window
WrappingProvider = GUID of your third-party GINA/CP extension

For macOS clients

1. Copy the ADSelfServicePlusMacLoginAgent.pkg (Location: ***install_dir>/bin/***) file to the macOS machine.
2. Double-click the **ADSelfServicePlusMacLoginAgent.pkg file** to begin the installation process.
3. Once you click the **Install** button, you'll be asked to enter your username and password. Please use the account information you use to log on to your Mac.

4. Enter the ADSelfService Plus server name and port number when prompted.



5. In the window that opens, click Close to complete the installation.

For Linux clients

1. Copy the installLinuxAgent.sh, ADSSPLinuxClient.tar.gz from this folder:
   <Install Directory>\bin (Default location: C:\ManageEngine\ADSelfService Plus\bin).
   Note:
   You need to copy the TAR file based on the client OS architecture. There will be two TAR files:
   i ADSSPLinuxClient.tar.gz for i686 clients (32-bit)
   ii ADSSPLinuxClient64.tar.gz for x86-64 clients (64-bit)
2. Paste the copied files in the Home folder of the Linux machine.
3. Launch the Linux terminal and execute the following commands:
   i sed -i 's/\r$//' installLinuxAgent.sh
   ii sudo bash installLinuxAgent.sh -install -serverName <adssp-server/IP> -portNumber <adssp-server-port> -protocol <adssp-server-protocol>

Where:

i serverName = The name of the machine in which ADSelfService Plus is deployed.
ii portNumber = The port number using which ADSelfService Plus is running.
iii protocol = The protocol with which ADSelfService Plus is running (http or https).

5. Troubleshooting

Troubleshooting the GINA/macOS/Linux login agent installation

The following errors may arise during the installation of the GINA login agent, follow the solutions provided to resolve them:

1. **Remcom.exe' is not recognized as an internal or external command, operable program or batch file.**

   This error occurs if the Remcom.exe file, which is used to install the login agent in remote machines, has been flagged and deleted by the antivirus software. To resolve this issue:

   - Check if the Remcom.exe file exists in the ***bin*** folder of ADSelfService Plus Installation directory ***(C:\ManageEngine\ADSelfService Plus\bin).***
   - If not, check if your antivirus software has removed the file. Configure your antivirus software to trust the Remcom.exe file.

2. **Could not Install login agent**

   This error occurs because of a network timeout while installing the login agent. Make sure the network connection is re-established and try to install the software again.

3. **Initiating Connection to Remote Service Failed**

   This error could occur if the target computer could not be contacted. To prevent this:

   - Ensure if such a computer really exists. If so, ensure whether it is connected to the network.
   - To check for connectivity, ping this computer from the server where ADSelfService Plus is installed.
   - Make sure Remote Registry service is running in the client machine.

4. **Couldn't connect to the machine, ADMIN$.Access is denied**

   This error may occur because admin share has not been enabled in the client computer. To resolve this issue:

   - Configure Domain Settings (when run as console) or the Logon Tab (when run as service) with a different user account that has Domain Admin privileges.
   - Enable admin share:

i. In the client computer, go to **Start > Run** and type gpedit.msc and hit **Enter.**

ii. Expand the **Administrative Templates > Network > Network Connections > Windows Firewall.**

iii. Click **Domain Profile** and double click **Windows Firewall: Allow inbound remote administration exception.**

iv. Select **Enabled** and click **OK.**

5 **Logon Failure: The target account name is incorrect.**

This error message can occur if two computers have the same computer name. One computer is located in the child domain; the other computer is located in the parent domain.

6 **Logon failure: unknown user name or bad password.**

This error message occurs when admin share might not be enabled in the client computer. To resolve this issue:

- Configure Domain Settings (when run as console) or the Logon Tab (when run as service) with a different user account that has Domain Admin privileges.
- Enable admin share:

i. In the client computer, go to **Start > Run** and type gpedit.msc and hit **Enter.**

ii. Expand the **Administrative Templates > Network > Network Connections > Windows Firewall.**

iii. Click **Domain Profile** and double click **Windows Firewall: Allow inbound remote administration exception.**

iv. Select **Enabled** and click **OK.**

7 **Couldn't Start Remote Service. Overlapped I/O operation is in progress.**

The Remote service couldn't be started either because the copy was blocked by antivirus or because the service couldn't be started automatically. To prevent this:

- In the client machine, go to the Services tab and check whether the Remote Registry and Server services have started. If not, enable these services.

8 **Another version of this product is already installed.**

This error occurs when another version of this login agent is already installed in the remote machine. To prevent this, uninstall the existing login agent from this machine.

9 **Another installation is already in progress.**

This error occurs when another installation is already in progress. To prevent this, try to install the login agent after a few minutes.

10 **Could not connect to the machine.**

This error could occur if the target computer could not be contacted. To prevent this:

- Ensure if such a computer really exists.
- If so, ensure it is connected to the network.
- To check for connectivity, ping this computer only from the server where ADSelfService Plus is installed.

11 **Network path not found/Invalid Credential.**

This error could occur if the target computer could not be contacted. To prevent this:

- Configure Domain Settings (when run as console) or the Logon Tab (when run as service) with a different user account that has Domain Admin privileges.
- Enable admin share:
  - i In the client computer, go to **Start > Run** and type gpedit.msc and hit **Enter.**
  - ii Expand the **Administrative Templates > Network > Network Connections > Windows Firewall.**
  - iii Click **Domain Profile** and double click **Windows Firewall: Allow inbound remote administration exception.**
  - iv Select **Enabled** and click **OK.**

12 **Couldn't copy ADSelfServicePlusClientSoftware.msi**

This error occurs because the ADSelfService Plus server has insufficient privileges to access the client machine. To prevent this:

- Configure Domain Settings (when run as console) or the Logon Tab (when run as service) with a different user account that has Domain Admin privileges.
- Enable admin share:
  i. In the client computer, go to **Start > Run** and type gpedit.msc and hit **Enter.**
  ii. Expand the **Administrative Templates > Network > Network Connections > Windows Firewall.**
  iii. Click **Domain Profile** and double click **Windows Firewall: Allow inbound remote administration exception.**
  iv. Select **Enabled** and click **OK.**

13 **Multiple connections to a server or shared resource by the same user.**

This error occurs when other applications or processes are using the same user account used by ADSelfService Plus to try and connect to the remote machine in which the login agent is to be installed. To resolve this issue:

- Disconnect all previous connections to the server or shared resource and try again.
- Configure Domain Settings (when run as console) or the Logon Tab (when run as service) with a different user account that has Domain Admin privileges.

Troubleshooting the macOS login agent installation

Below is the list of errors that may arise while installing the login agent in macOS clients and the solutions to resolve the error:

1. **Connection timed out.**

Possible cause: The macOS client, in which you are trying to install the login agent, is shut down or not connected to the domain network.

Solution:

- Start the client and ensure that it is connected to the domain network. Check the connection by pinging the macOS client from the ADSelfService Plus server. Once you're sure there is a connection, try installing the login agent again.
- If the connection to the Mac client is fine, then check the client's integration with AD.

2. **Connection refused.**

Possible cause: Remote Login has not been enabled.

Solution:

- Open the Mac client. Go to **Preferences** → **Sharing** and check if **Remote Login** is enabled.
- Check if the user account provided in the ADSelfService Plus **Domain Settings** has **Remote Login** access enabled.

3. **The network path was not found.**

Possible cause: The target computer could not be contacted.

Solution:

- Ensure if such a computer exists. If so, ensure that it is connected to the network.
- To check for connectivity, ping this computer from the server where ADSelfService Plus has been installed.

4. **Logon Failure: Unknown user name or bad password**

Possible cause: Incorrect username or password for the service account.

Solution:

- Provide the correct credentials for the service account. Also, go to the **Directory Editor** in the **Directory Utility** and check if the Active Directory node can be connected using the user credentials provided in the ADSelfService Plus **Domain Settings.**

5 **Permission denied.**

Possible cause: The service account does not have the required administrative privileges over the targeted macOS client.

Solution:

Provide admin privilege to the service account by following the steps below:

- In the targeted macOS client, go to System Preferences → Users & Groups → Login Options → Edit → Open Directory Utility.
- In the Service tab, click the Administrative section.
- Select the Allow Administration by checkbox, and include the service account used to run the ADSelfService Plus server.
- Click OK.
- Verify the macOS client's integration with AD.
  - Go to **Directory Utility** → **Directory Editor** → **<Your Active Directory node>.** If the connection is successful, you will be able to see the AD objects.
  - If the connection to the AD node fails, try pinging the Domain Controller (DC) from the macOS client.
  - If the DC is reachable and the problem persists, unbind it and try re-binding the macOS client with AD.

6 **Invalid service account credentials.**

Possible cause: Invalid or expired service account credentials in the **Domain Settings.**

Solution:

Update the correct service account credentials. Also, verify the macOS client's integration with AD.

7 **Insufficient privileges to the service account.**

Possible cause: The service account does not have the required root privilege to perform a remote installation of the package over the targeted macOS client.

Solution:

Provide root privilege to the service account by following the steps below:

- Go to the **Terminal** window and execute the command ***sudo visudo.*** Then, navigate to the **#User privilege specification** section. In the ***%admin ALL=(ALL) ALL*** replace ***%admin*** with the username i.e., ***<username> ALL=(ALL) ALL.***

8

No authentication details found for the domain.

Possible cause: Insufficient privileges for the service account in the **Domain Settings** of ADSelfService Plus.

Solution:

Provide the domain user credentials with admin privileges.

Troubleshooting the Linux login agent installation

Below is the list of errors that may arise while installing the login agent in Linux clients and the solutions to resolve the error:

1. **The network path was not found.**

Possible cause: This error could occur if the target computer could not be contacted.

Solution:

Provide admin privilege to the service account by following the steps below:

- Ensure if such a computer really exists. If so, ensure that it is connected to the network.
- To check for connectivity, ping this computer from the server where ADSelfService Plus has been installed.

2. **Connection timed out.**

Possible cause: The Linux machine, in which you are trying to install the login agent, is shut down or not connected to the domain network.

Solution:

- Start the client and ensure that it is connected to the domain network. Check the connection by pinging the machine from the ADSelfService Plus server. Once you're sure there is a connection, try to install the agent again.
- If the connection to the machine is fine, then check the Linux client's integration with AD.

3. **Connection refused.**

Possible cause: SSH server software is not active in the Linux client.

Solution:

Make sure the SSHD service is installed and active in the Linux client.

4. **Permission denied / Insufficient privileges to the service account.**

Possible cause: Service account configured in ADSelfService Plus does not have the required root privilege over the targeted Linux client.

Solution:

Provide root privilege to the service account by following the steps below:

- Go to the **Terminal** window and execute the command ***sudo visudo.*** Then, navigate to the **#User privilege specification** section. In the ***%admin ALL=(ALL) ALL*** replace ***%admin*** with the username i.e., ***<username> ALL=(ALL) ALL.***

5 **Invalid service account credentials.**

Possible cause: Invalid or expired service account credentials in the Domain Settings.

Solution:

Update the correct service account credentials.

- Log in to ADSelfservice Plus with admin privileges.
- Go to **Domain Settings.**
- Click the edit button and provide the service account credentials with the required privileges.

6 **Connection refused.**

Possible cause: Insufficient privileges for the service account in the Domain Settings of ADSelfService Plus.

Solution:

Provide the service account credentials with domain admin privileges.

7 **The operation failed while setting up dependencies.**

Possible causes:

- Poor network connection.
- Insufficient download permission.

Solution:

Check network connectivity in the Linux machine. If the network connection is established, check if the Linux package manager can contact the repository. If you can contact the repository, you can re-install the Linux login agent from the ADSelfService Plus admin console.

The **lightdm-webkit2-greeter** package might not be installed from opensuse.orgdue to insufficient file download permissions. Ensure the URL is allowed in the firewall.

6. Frequently Asked Questions

1 **After installing the ADSelfService Plus login agent, the Windows logon screen appears blank. I can't log in to Windows now. What should I do?**

You can try the following steps:

- Uninstall the login agent using ADSelfService Plus web portal.
- In case of Windows Vista and later - restart your machine in Safe Mode and remove registry key - "{B80B099C-62EA-43cd-9540-3DD26AF3B2B0}" found under:

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

2 **What precautions do I have to take regarding the login agent, when migrating ADSelfService Plus from one server to another?**

You have to change the Server Name and Port Number of ADSelfService Plus with that of the new server. Follow the below steps:

- In ADSelfService Plus web portal, go to **Configuration > Administrative Tools > GINA (Ctrl+Alt+Del) > GINA/Mac/Linux Customization.**
- Replace 'Server Name' and 'Port Number' of the old server with the new server in which ADSelfService Plus is running currently.

3 **I get an empty page (or a page with four empty square-like icons) when I click on the Reset Password/Unlock Account link at Windows logon prompt.**

This problem may arise, if you have configured the SSL (https) port number for the login agent. Changing the port number of the login agent back to http will solve this problem. To change the port number:

- In ADSelfService Plus web portal, go to **Configuration > Administrative Tools > GINA (Ctrl+Alt+Del) > GINA/Mac/Linux Customization.**
- Replace the Port Number to that of your HTTP port.

4 **I am already using a third party CP. What precautions do I need to take during installation?**

If you are already using a third party Credential Provider extension, follow the below steps to seamlessly integrate ADSelfService Plus login agent with your third party CP extension:
You can create a registry entry – 'WrappingProvider' with the third party CP extension's GUID as its value in the following registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\ZOHO Corp\ADSelfServicePlus login agent

You can also try the below command:

- Get the unique GUID of the third party CP extension from the below registry key:

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

- Use that GUID in the below command during installation:

```
msiexec.exe /i ADSelfServicePlusClientSoftware.msi
SERVERNAME="<enter the servername>" PORTNO="<enter the port number>"
PROTOCOL="HTTPS"  WrappingProvider="{<enter the GUID of your third-party
GINA/CP extension>}" /qn
```

5 **I only want the 'Reset Password/Unlock Account' link at the logon prompt and not a separate tile. (Applies only to Windows Vista and later)**

If you want to remove the ADSelfService Plus's login agent tile, set 'ShowADSSPTile' registry value as FALSE under:

HKEY_LOCAL_MACHINE\SOFTWARE\ZOHO Corp\ADSelfServicePlus login agent

6 **Is it possible to push the login agent using any other third party distribution software?**

Yes, it is possible. Use the following command with your third party distribution software:

```
msiexec /iADSelfServicePlusClientSoftware.msi SERVERNAME="<enter the name
of the ADSelfService Plus server>" PORTNO="<enter the port number>"
PROTOCOL "<HTTPS>" /qn
```

7 **How to change the title of ADSelfService Plus login agent window?**

Follow any one of the below steps:

- Create a registry key - 'ProductTitle' - under:
  HKEY_LOCAL_MACHINE\SOFTWARE\ZOHO Corp\ADSelfServicePlus login agent
- In ADSelfService Plus web portal, go to **Admin > Customize > Rebranding.** Replace the 'Browser Title' text with the text of your choice.
- Use the following command:

```
msiexec /iADSelfServicePlusClientSoftware.msi SERVERNAME="<enter the
name of the ADSelfService Plus server>" PORTNO="<enter the port number>"
PROTOCOL "<HTTPS>" PROD_TITLE="<title>" /qn
```

8 **How do I change the ManageEngine ADSelfService Plus logo in the login agent window?**

To change the logo in the login agent window, you have to edit the 'ResetUnlock.html' file by following the below steps:

- Take a backup of the 'ResetUnlock.html' file. It can be found at ***C:\Program Files\ManageEngine\ADSelfService Plus\webapps\adssp\html.***
- Edit **ResetUnlock.html** and change the image (logo) at ***<img src="../images/adssp-logo.gif">.*** Provide the full path to the location of your logo as the value for 'img src'.

9 **I want users to have access only to the 'Reset Password' (or 'Unlock Account') functionality through the login agent.**

- Take a backup of the **ResetUnlock.html** file. It can be found at ***C:\Program Files\ManageEngine\ADSelfService Plus\webapps\adssp\html.***
- Edit ResetUnlock.html. Delete the portion of the code that points to **'Reset Password'** or **'Unlock Account'** as you desire.

10 **How to customize the ADSelfService Plus login agent icon when I have installed it manually or through a 3rd party distribution software?**

Make sure the icon is a '.bmp' file of 48x48 pixels. Rename the bmp file as 'reset_icon.bmp' and put it in the **System32 *(C:\Windows\System32\)*** folder of users' machines.

11 **What should be the format of the CSV file used to import computers for installation?**

The first line of the CSV file will be taken as the header.

- If the CSV file contains names of the computers, then the first line (header) should be - **Name.**
- If the CSV file contains dnsHostNames of the computers, then the first line (header) should be - **dnsHostName.**