ManageEngine
ADSelfService Plus

Login agent
Manual installation guide

Table of Contents

1. Introduction

ADSelfService Plus is an identity security solution that ensures secure and seamless access to enterprise resources and establishes a Zero Trust environment. With capabilities such as adaptive multi-factor authentication (MFA), single sign-on (SSO), 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-track application onboarding, improve password security, reduce help desk tickets, and empower remote workforces.

Highlights of the product:

- MFA
- Enterprise SSO
- Conditional access policies
- Self-service password reset and account unlock
- Password policy enforcement
- Password expiration notifications
- Multi-platform password synchronization
- Self-subscription to email groups
- Directory self-updates
- Employee search and organization chart

2. The ADSelfService Plus login agent

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

1. When ADSelfService Plus with Endpoint MFA has been purchased:

- Configure MFA for machine logins to secure Windows (including RDP logins and user access control prompts), macOS, and Linux logins.

2. When the ADSelfService Plus Professional edition is used:

- It 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 machines.

- Configure custom password policies created using the Password Policy Enforcer during native Windows logins.

- Update cached credentials over VPN when AD passwords are reset or changed from remote Windows machines.

3. System requirements

Windows

1. Windows 11
2. Windows 8.1
3. Windows 8
4. Windows 7
5. Windows Vista

MacOS

1. macOS 14 Sonoma
2. macOS 13 Ventura
3. macOS 12 Monterey
4. macOS 11 Big Sur
5. macOS 10.13 High Sierra
6. macOS 10.12 Sierra
7. OS X 10.11 El Capitan
8. OS X 10.10 Yosemite

Linux

1. Ubuntu 16.x-20.04.4
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 might 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

Methods of installation

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

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

In this document, we will discuss the first two methods of installation: via the ADSelfService Plus web portal and manual installation. Installation via GPOs and SCCM have been discussed separately.

i. Through the ADSelfService Plus admin portal:

Prerequisites

- 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.

- To install the login agent on machines present in a domain, a privileged user (Technician) must have the administrator credentials used in configuring that domain with ADSelfService Plus.

For Windows machines:

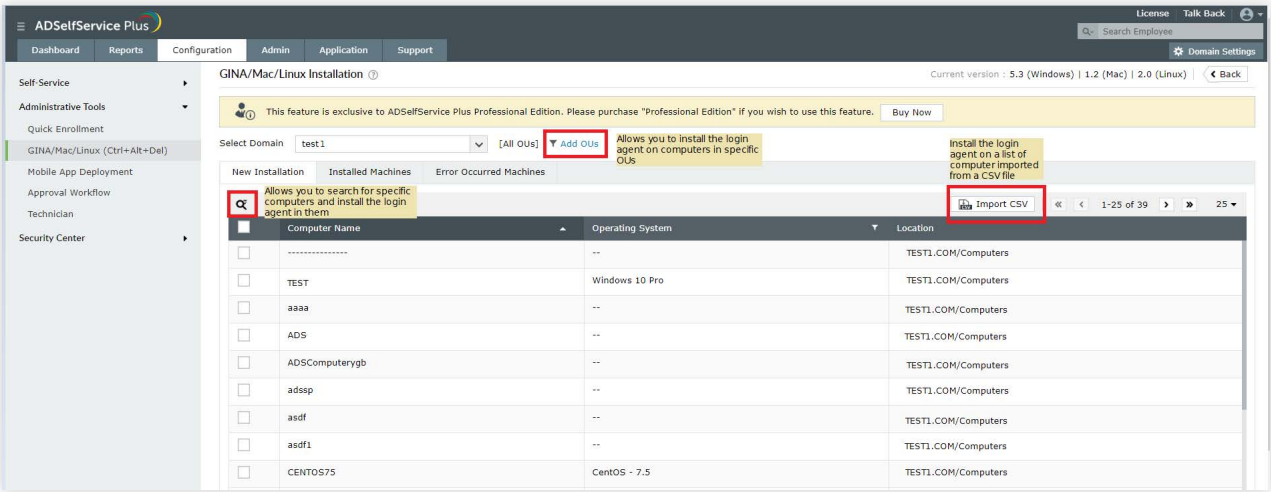
1. The client machines have to be connected to the domain network.
2. The service account whose credentials are provided during domain configuration in ADSelfService Plus should have Domain Admin privilege over the machine.
3. If ADSelfService Plus is installed as a Windows service, it should be run by a service account with Active Directory Domain Admin privileges.
4. The client computer's 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 the login agent is to be installed.

For macOS clients:

1. The Mac computer should be part of the Active Directory domain configured in ADSelfService Plus's domain settings
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.

For Linux clients:

1. The client computers should be connected to the domain network.
2. TThe 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.



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** and select the desired OUs. Click **OK.**

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

Import CSV: Allows you to 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 on which you want to install the login agent and click **Install.**

Customization:

The ADSelfService Plus login agent can be customized to suit your organization's requirements. These components of the login agent can be customized:

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

Follow these steps to customize 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** 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: Only BMP files can be used for icons. 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. 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 rescheduling, 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:

- To schedule installation of the login agent, you should have installed a valid SSL certificate in ADSelfService Plus, and configured the Access URL to use the HTTPS protocol.
  You can find the steps in this guide.
- Clicking the **Save** button will automatically enable the scheduler.
- To disable the scheduler, click the Disable icon under the Actions column.

Audit Trail:

ADSelfService Plus makes it easy to keep track of all the machines in which the login agent has been successfully installed, as well as track the machines on which 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 the 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 these steps:

Prerequisites for manual installation on Windows machines:

1. The client machines have to be connected to the domain network.
2. The technician who installs the Windows login agent must be a member of the Local *Administrator* group or have *Run* as *Admin* privilege on the machine.
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.

Steps to install the agent manually:

1. Copy the **ADSelfServicePlusClientSoftware.msi** file from the product **<Installation_Directory>/bin** folder.
2. Paste the **MSI** file in the **Machine** in which the login agent is to be installed.
3. Right-click and run the **MSI file** as an administrator.
4. Click **Next**. Enter the **hostname or IP Address**, and **Port number** of the machine on which ADSelfSevice Plus is running. If you have configured a **Context Path**, Enter the hostname in this format: *hostname/Context path.*
5. Copy the **Installation Key** from the product UI. To find it, log in to the ADSelfService Plus admin portal, go to **Configuration > Administrative Tools > GINA/MAC/LINUX (Ctrl + Alt + Del) > Manual Installation steps > GINA.** Click on the icon in step 4 to copy it.
6. Paste it into the **Installation Key** field in the installation wizard and click **Next.**
7. Follow the steps provided in the wizard and finish the installation process.

2. Using the command prompt:

When the login agent is installed manually using the MSI package on computers running Windows Vista and later operating systems with user account control (UAC) enabled, it might not function properly. In such cases, you can install the login agent manually through the command prompt as shown here:

1. Open the command prompt as an administrator and point it to the folder containing installer file.
2. Log in to the **ADSelfService Plus admin portal**. Go to **Configuration > Administrative Tools > GINA/Mac/Linux (Ctrl+Alt+Del) > Installation Help Guide >** **GINA Login Using SCCM (System Center Configuration Manager) - View Command**. Click **View Command** to view and copy the command.
3. Replace the MSI file name with the actual file path and run the modified command from the command prompt.

For example, change the MSI command to this format:

```
msiexec /i  "C:\Downloads\ADSelfServicePlusClientSoftware.msi"
SERVERNAME=abc.selfservice.com" PORTNO="443" PROTOCOL="https"
INSTALLATION_KEY="19d82629b4e540fc873df8775d3630cb" BUTTONTEXT=
"Reset Password / Unlock Account" BYPASS="true" FRAMETEXT="Can't logon?
Please click on Reset Password/Unlock Account button to reset your password
or unlock your account" GINAHOSTEXCLUDE="okta,onelogin"
WINDOWSLOGONTFA="true" MACHINEMFAUSAGESCENARIO="31"
```

SERVERNAME, PORTNO, and INSTALLATION_KEY are mandatory parameters. The full list of all the parameters that can be used during installation of the login agent is given below. If you want your client software to have the default layout, only enter the default command copied from the GUI; otherwise, you can customize it with any of the other parameters.

Note 1: 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	CORRESPONDING 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
INSTALLATION_KEY	InstallationKey	None	The installation key that links the ADSelfService Plus server and client securely
SERVERCONT-EXTPATH	ServerContextPath	None	The context path of the ADSelfService Plus server. To know more about the context path, click here.
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 or not when the ADSelfService Plus server is unreachable during machine logins
FRAMETEXT	FrameText	Can't log on? Please click the 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)
GINAHOSTEXCLUDE	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 identity providers (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 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	The server is unreachable due to intermittent network connectivity or improper SSL certification, or because 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 or not

WINDOWSLO-GONTFA	WindowsLogonTFA	FALSE	Determines whether MFA for machine login has been enabled
MACHINEMFAUS-AGESCENARIO*	MFAUsage ScenarioMask	5	Determines whether the MFA for machine logins feature will be enabled for specific scenarios or not based on the value provided. Learn more. **Scenario in which MFA is required** / **Corresponding 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
ISMACHINEMFAE-NFORCED*	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 Windows Native VPN) is enabled or not

VPN_SERVER_NAME	VpnServerName	None	Specifies the VPN server name
VPN_PORT_NO	VpnPortNo	None	Defines the ADSelfService Plus server's port number used to connect to VPN
PRE_SHARED_KEY	PreSharedKey	None	Defines the value of the pre-shared key configured while setting up Windows Native VPN for the cached credentials update feature
VPN_GROUP_NAME	VpnGroupName	None	Specifies the VPN group name used when configuring the Updating Cached Credentials Over VPN feature (required only when a Cisco AnyConnect VPN is used)
VPN_DOMAIN_NAME	VpnDomainName	None	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)
VPN_TYPE	VpnType	None	Defines the VPN connection behavior for cached credentials update based on the provider used This preset number key is used to denote the VPN provider

VPN PROVIDER	NUMBER VALUE
Custom VPN	0
Fortinet and Cisco IPSec	1
Windows Native VPN	2
Cisco AnyConnect	3
SonicWall NetExtender	4
Checkpoint Remote Access VPN and SonicWall Global VPN	5
Open VPN	6

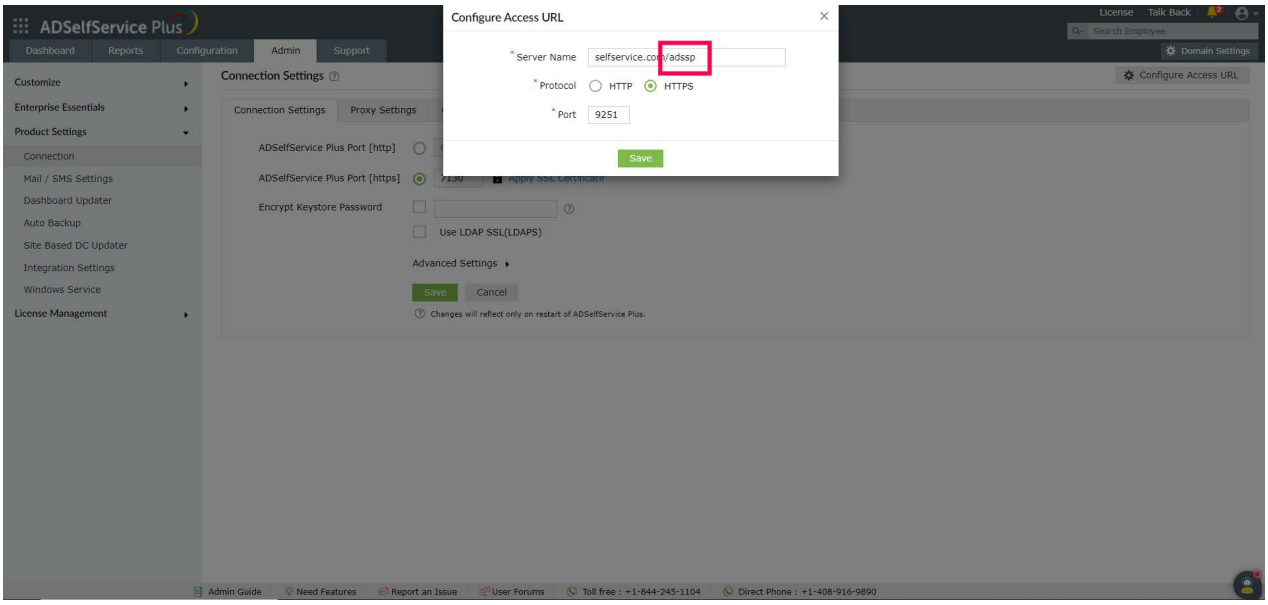
VPN_CLIENT_ LOCATION	VpnClientLocation	None	Specifies the VPN client location (example: **C:\Program Files (x86)\Fortinet\FortiClient\ FortiSSLVPNclient.exe)**
VPN_CONNECT_ CMD	VpnConnectCmd	None	VPN-provider-specific command that is used to connect to the VPN during cache credentials update
VPN_DISCONNECT _CMD	VpnDisconnectCmd	None	VPN-provider-specific command that is used to disconnect from the VPN during cache credentials update
WRAPPINGPRO-VIDER	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.*
CUSTOMTITLEI-CONPATH	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.*

These parameters pertain to the installation and customization of Offline MFA:

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	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.*
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.

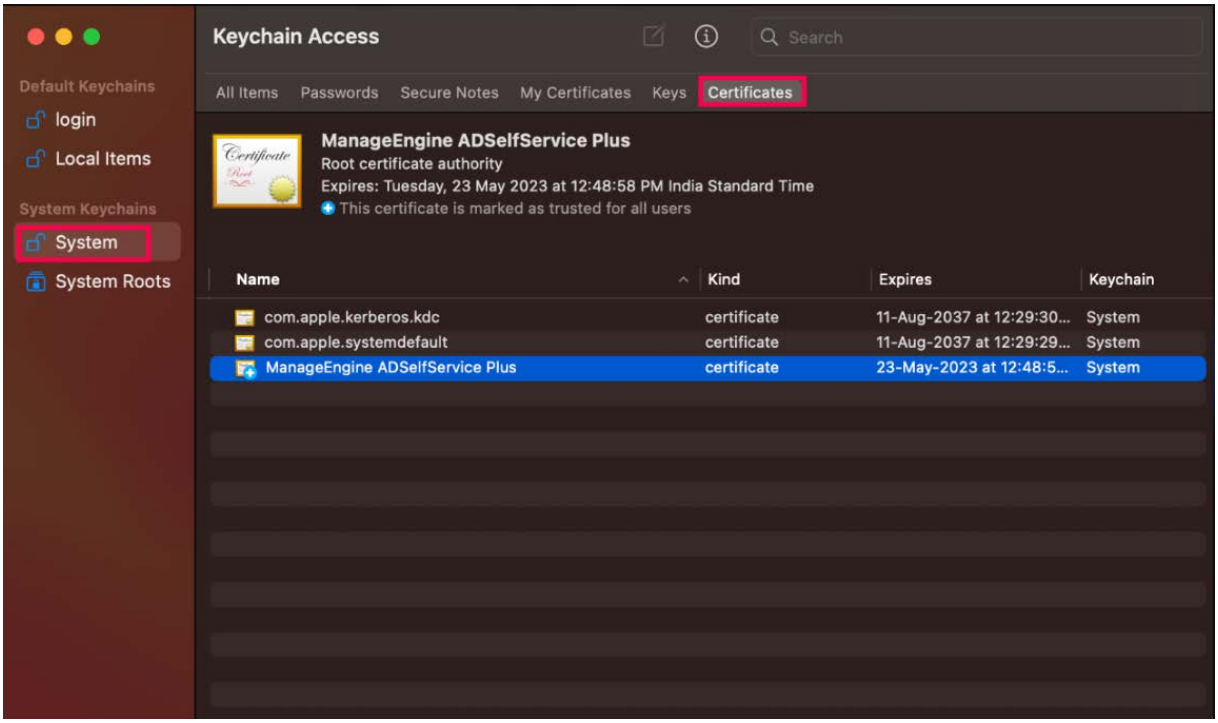
Note: If you are already using a third-party GINA/CP extension, use the **WRAPPINGPROVIDER** parameter in the ADSelfService Plus login agent installation command for seamless integration with the third-party GINA/CP extension.

For example, add the WRAPPINGPROVIDER parameter to the command:

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>}"**

For macOS clients

1. The Mac computer should be part of the Active Directory domain configured in ADSelfService Plus' domain settings.
2. The technician who installs the macOS login agent must have admin rights over the Mac.
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.



1. Using the installer package

1. Copy the **ADSelfServiceMacLoginAgent.pkg** file from the product **<Installation_ Directory>/bin** folder and paste it in the Mac in which the login agent is to be installed.
2. Double-click the PKG file to begin the installation process.
3. In the *Introduction* window, click **Continue.**
4. In the *Installation Type* window, select the install location and click **Install.**
5. You will be asked to enter your username and password. Please enter the credentials of an account with admin privileges.
6. Enter the **Server name/IP address** and **Port number,** of the machine on which ADSelfService Plus is running.
7. Copy the **Installation Key** from the product UI. To find it, log in to the ADSelfService Plus admin portal, go to **Configuration > Administrative Tools > GINA/MAC/LINUX (Ctrl + Alt + Del) > Manual Installation steps > macOS.** Click on the icon in Step 7 of the UI to copy it.
8. Paste it into the **Installation Key** field in the Mac when prompted and follow the instructions in the wizard to install the Mac login agent.

2. Using CLI installation

1. Copy the **ADSelfServiceMacLoginAgent.pkg** and **installMacAgent.sh** file from the product /bin folder and paste it into the Mac where the login agent is to be installed

2. Copy the macOS CLI command from the ADSelfService Plus admin portal. Go to **Configuration > Administrative Tools > GINA/MAC/LINUX (Ctrl + Alt + Del) > Installation Help Guide > Mac Login Agent CLI installation > View Command** to find it. It is shown in the pop-up screen that appears on clicking **View Command.**

3. Open the **Terminal** on the Mac, navigate to the **directory** that the installer package was copied to, then paste the **command,** and execute it.

pkg, serverName, portNumber, and **installationKey** are mandatory parameters.
The full list of all the parameters that can be used during installation of the macOS login agent is given below. If you want your client software to have the default layout, only enter the default command copied from the product GUI; otherwise, you can customize it with any of these parameters.

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	VALUES
serverName	The hostname of the server in which ADSelfService Plus is installed
portNumber	The port number for ADSelfService Plus
installationKey	The installation key that links the server and client securely
prodTitle	Enter the text to be displayed in the ADSelfService Plus window for password resets and account unlocks
restrictBadCert	Determines whether to restrict usage of expired, self-signed, or invalid SSL certificates during self-service actions and MFA, or not **Note:** We strongly advise against setting the login agent to work when the SSL certificate is invalid in your production environment, as it will severely impact security. Please disable this only for testing purposes.
loginMFA	Enter “true” if you want MFA to be enabled during login Enter “false” if you don't want MFA to be enabled
bypassMFAServer-Unreach	Enter “TRUE" if you want to bypass MFA for logins when the ADSelfService Plus server is unreachable. If not, enter “FALSE".
serverUnreachMsg	Enter the message to be displayed when the server is not reachable during endpoint MFA.
imagePath	Enter the file path for the Reset Password/Unlock Account button image
showRPUALink	Enter “TRUE" if you want to display the Reset Password/Unlock Account link and allow users to reset their password or unlock their accounts. If you only want MFA for logins to be enabled, enter “FALSE".
buttonText	Enter the text to be displayed in the Reset Password/Unlock Account button.
isMFAEnforced*	If it is "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.

PARAMETER	VALUES
serverName	This is the hostname of the server on which ADSelfService Plus is installed.
portNumber	This is the port number for ADSelfService Plus.
installationKey	This is the installation key that links the server and client securely.
prodTitle	Enter the text to be displayed in the ADSelfService Plus window for password resets and account unlocks.
restrictBadCert	This determines whether or not to restrict the 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 when the SSL certificate is invalid in your production environment as this will severely impact security. Please disable this only for testing purposes.
loginMFA	Enter “true” if you want MFA to be enabled during login. Enter “false” if you don't want MFA to be enabled.
bypassMFA	Enter “TRUE" if you want to bypass MFA for logins when the ADSelfService Plus server is unreachable. If not, enter “FALSE".
serverUnreachMsg	Enter the message to be displayed when the server is not reachable during endpoint MFA.
imagePath	Enter the file path for the Reset Password/Unlock Account buttons image.
showRPUALink	Enter “TRUE" if you want to display the Reset Password/Unlock Account link and allow users to reset their passwords and unlock their accounts. If you only want MFA for logins to be enabled, enter “FALSE".
buttonText	Enter the text to be displayed on the Reset Password and Unlock Account buttons.
isMFAEnforced*	If it is "TRUE", MFA will be enforced for all users accessing the machines, regardless of their enrollment status, self-service policy membership, or ADSelfService Plus connectivity status.

These parameters pertain to the installation and customization of offline MFA:

PARAMETER	VALUES
offlineMFA	This specifies whether or not offline MFA is enabled. (Default value: false)
localeId	This specifies the display language used for some parts of the login agent. (Default value: NONE)

Key	Language
de	German
fr	French
ja	Japanese
pl	Polish
tr	Turkish
zh	Simplified Chinese
es	Spanish

offlineWebLogoName	This specifies the file name and the format of the custom logo to be displayed during offline MFA. The file name must be in the format customLogo.png. The supported formats are JPG, JPEG, BMP, PNG, and GIF.

For Linux Clients

Prerequisites for installation on machines running Linux

1. The client computers should be connected to the domain network.

2. The technician who installs the Linux login agent, must be either a member of the Local *Admin* group, or present in the Sudoers file to execute commands with *root* privilege.

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.

Steps to install the login agent on machines running Linux

1. Copy the **installLinuxAgent.sh** and **ADSSPLinuxClient.tar.gz** files from the product **<Installation_Directory>/bin** folder and paste them into the target Linux machine where the login agent is to be installed.

2. Copy the Linux CLI command from the ADSelfService Plus admin portal. Go to **Configuration > Administrative Tools > GINA/MAC/LINUX (Ctrl + Alt + Del) > Installation Help Guide > Linux Login Agent CLI installation > View Command** to find it. It is shown in the pop-up that appears on clicking **View Command.**

3. Open the **Terminal** on the Linux machine, navigate to the **directory** that the installer package was copied to. Paste and execute the command.

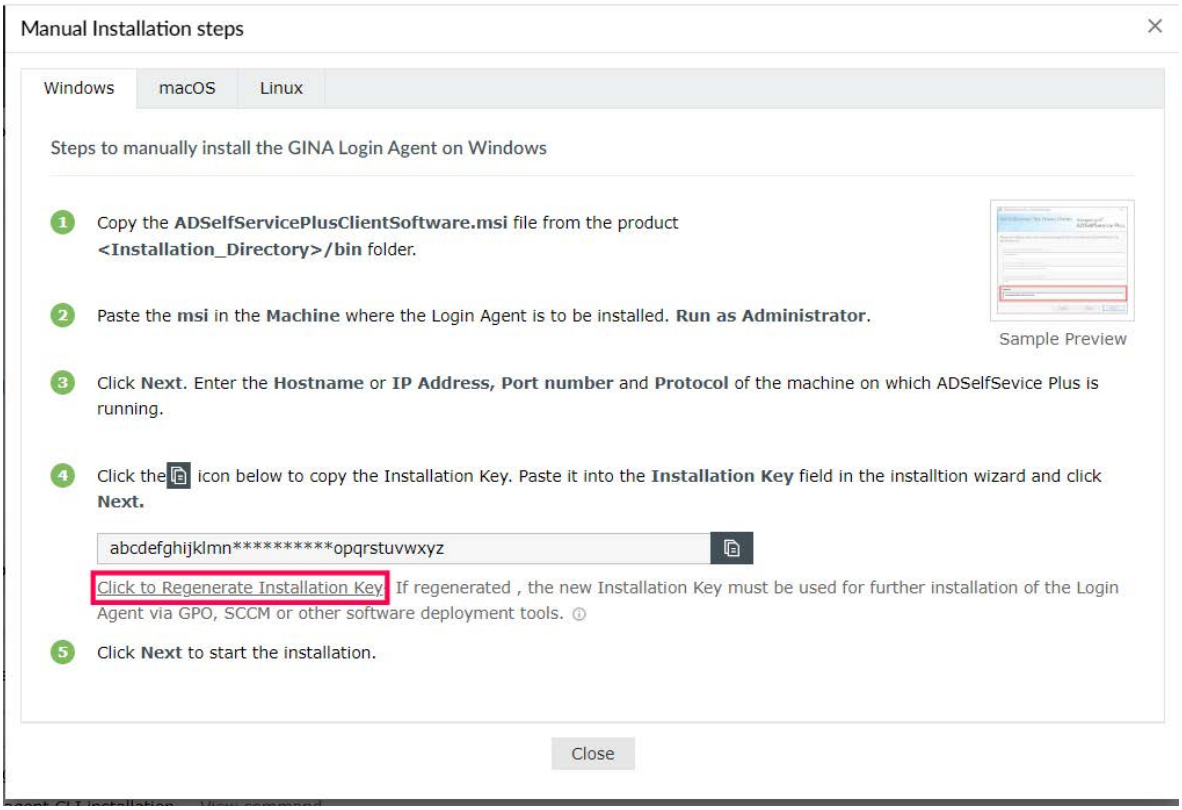
   In the command, **serverName, portNumber,** and **installationKey** are mandatory parameters. The full list of all the parameters that can be used during installation of the Linux login agent is given below. If you want your client software to have the default layout, only enter the default command copied from the product GUI; otherwise, you can customize it with any of the other parameters.

   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	VALUES
serverName	The hostname of the server in which ADSelfService Plus is installed
portNumber	The port number for ADSelfService Plus
installationKey	The installation key that links the server and client securely
title	Enter the title to be displayed
restrictBadCert	Enter “TRUE” if you want the login agent to work even when the SSL certificate applied is invalid. Enter “FALSE" if you don't want the login agent to work in that situation. **Note:** We strongly advise against setting the login agent to work when the SSL certificate is invalid in your production environment, as it will severely impact security. Please disable this only for testing purposes.
loginMFA	Enter “TRUE" if you want MFA to be enabled during login. Enter “FALSE" if you don't want MFA to be enabled.
bypassMFA	Enter “TRUE" if you want to bypass MFA for logins when the ADSelfService Plus server is unreachable. If not, enter “FALSE".
selfService	Enter “TRUE" if you want to display the Reset Password/Unlock Account link and allow users to reset their password or unlock their accounts. If you only want MFA for logins to be enabled, enter “FALSE".
linkText	Enter the link text to be displayed.
serverUnreachMsg	Enter the message to be displayed when the server is unreachable.
forceReboot	Defines whether a machine reboot is required or not after the agent has been installed.
defaultDomain	Enter the default domain that the Linux machines are binded to.
isMFAEnforced*	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.

5. 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.

6. 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 antivirus software. To resolve this issue:

   - Check if the Remcom.exe file exists in the bin folder of ADSelfService Plus Installation directory (**C:\ManageEngine\Program Files\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 reestablished 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 a console) or the Logon Tab (when run as a 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 is not enabled in the client computer. To resolve this issue:

- Configure Domain Settings (when run as a console), or the Logon Tab (when run as a 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 an antivirus solution, 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 the computer really exists. If so, ensure whether it is connected to the network.
- To check for connectivity, ping this computer from the server in which ADSelfService Plus is installed.
- Make sure the Remote Registry service is running in the client machine.

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 a console) or the Logon Tab (when run as a 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 error:

- Configure Domain Settings (when run as a console) or the Logon Tab (when run as a 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 and try to 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 a console) or the Logon Tab (when run as a service) with a different user account that has Domain Admin privileges.

Troubleshooting the macOS login agent installation

These errors that might arise while installing the login agent in macOS clients. Follow these solutions to resolve these errors:

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 the computer really exists. If so, ensure whether it is connected to the network.
   - To check for connectivity, ping this computer from the server in which ADSelfService Plus is 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 these steps:

- 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.
- Check the **Allow Administration by** box, 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 rebinding 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 these steps:

- Go to the **Terminal** window, execute the **sudo visudo** command, and navigate to the **#User privilege specification** section. Make sure the targeted account has root privileges, 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

These errors might arise while installing the login agent in Linux clients. Follow these solutions to resolve these errors:

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 these steps:

- Ensure if the computer really exists. If so, ensure whether it is connected to the network.
- To check for connectivity, ping this computer from the server in which ADSelfService Plus is 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, 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: The 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 these below:

- Go to the Terminal window, execute the **sudo visudo** command, and navigate to the **#User privilege specification** section. Make sure the targeted account has root privileges, 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 reinstall the Linux login agent from the ADSelfService Plus admin console.
- The **lightdm-webkit2-greeter** package might not be installed from opensuse.org due to insufficient file download permissions. Ensure the URL is allowed in the firewall.

7. 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 the 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 these steps:

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

3 **I am already using a third-party credential provider (CP). What precautions do I need to take during installation?**

If you are already using a third-party CP extension, follow these steps to seamlessly integrate the 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 this registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\ZOHO Corp\ADSelfServicePlus login agent

You can also try this command:

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

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

- Use that GUID in this command during installation:

```
msiexec.exe /i ADSelfServicePlusClientSoftware.msi SERVERNAME="" PORTNO=
WrappingProvider="{}" /qn
```

4 **I only want the Reset Password/Unlock Account link at the logon prompt and not on a separate tile (applies only to Windows Vista and later). How do I do this?**

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

HKEY_LOCAL_MACHINE\SOFTWARE\ZOHO Corp\ADSelfServicePlus login agent

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

Yes, it is possible. Use this command with your third-party distribution software:

```
msiexec /iADSelfServicePlusClientSoftware.msi SERVERNAME="" PORTNO="" /qn
```

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

Follow any one of these steps:

- Create a registry key, ProductTitle, under: **HKEY_LOCAL_MACHINE\SOFTWARE\ZOHO Corp\ADSelfServicePlus login agent**

- In the *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="" PORTNO=""
PROD_TITLE="" /qn<!--EndFragment-→ </body> </html>
```

7 **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 these steps:

- Take a backup of the **ResetUnlock.html file**. It can be found at *C:\Program Files\ManageEngine\ADSelfService Plus\webapps\adssp\html.*
- Edit the **ResetUnlock.html** file 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.**

8 **I want users to have access only to the Reset Password (or Unlock Account) functionality through the login agent. How do I enable this?**

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

9 **How do I customize the ADSelfService Plus login agent icon when I have installed it manually or through third-party distribution software?**

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

10 **What format should the CSV file used to import computers for installation be in?**

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

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

Our Products

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

ManageEngine
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 https://www.manageengine.com/products/self-service-password.

$ Get Quote | Download | Support