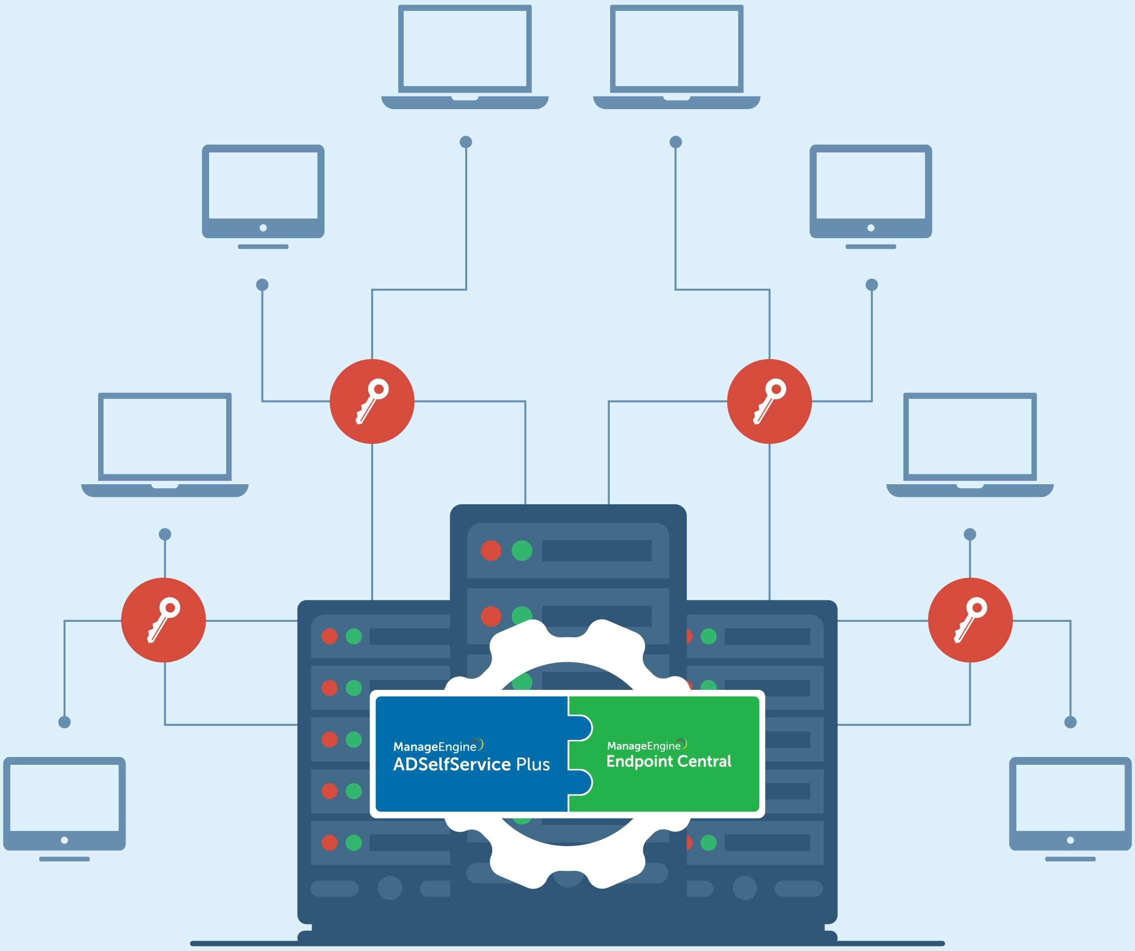
ManageEngine
ADSelfService Plus

# Login agent installation via Endpoint Central



www.adselfserviceplus.com

# Table of Contents

# Document summary

This document will guide you through the steps involved in installing the ManageEngine ADSelfService Plus login agent (GINA/macOS/Linux agent) using ManageEngine Endpoint Central. This document is written with the assumption that you are a system administrator with basic knowledge of Endpoint Central.

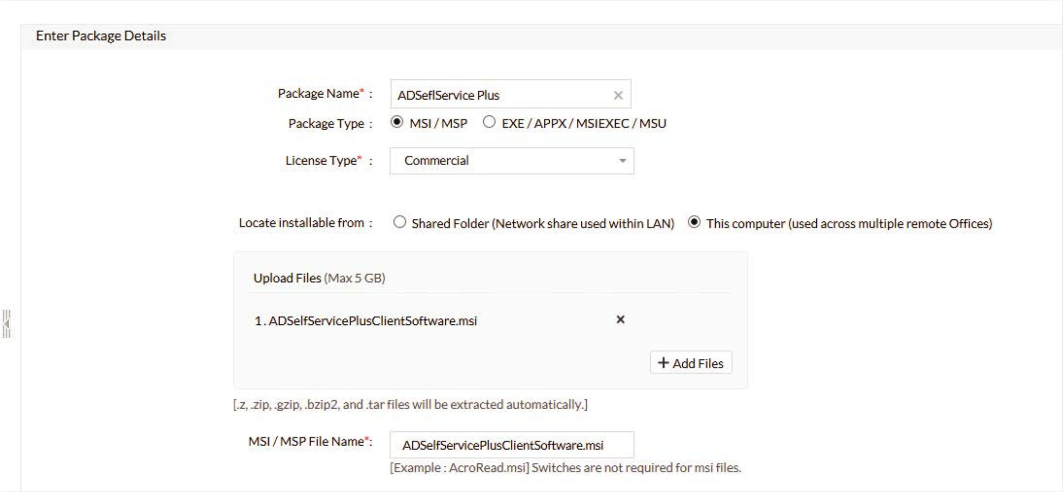
# Prerequisites

- 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.

# Steps for installing the login agent on Windows machines

## Step 1: Creating an MSI packagev

- Log in to **Endpoint Central** as an admin.
- Navigate to **Software Deployment > Packages > Add Package** and select **Windows** or **Mac** based on your requirements.
- Skip the **Network Share** configuration settings.
- On the **Enter Package Details** page, enter a **Package Name,** and click the MSI/MSP radio button.



Enter Package Details

Package Name* : ADSeflService Plus

Package Type : ● MSI / MSP ○ EXE / APPX / MSIEXEC / MSU

License Type* : Commercial

Locate installable from : ○ Shared Folder (Network share used within LAN) ● This computer (used across multiple remote Offices)

Upload Files (Max 5 GB)

1. ADSelfServicePlusClientSoftware.msi

[.z, .zip, .gzip, .bzip2, and .tar files will be extracted automatically.]

MSI / MSP File Name*: ADSelfServicePlusClientSoftware.msi

[Example : AcroRead.msi] Switches are not required for msi files.

- Select **Commercial** from the **License Type** drop-down.
- In the **Local installable form** field, click **This computer (used across multiple remote offices).**
- Click **Add Files**. In the window that opens, select the **ADSelfServicePlusClientSoftware.msi** file located in the bin folder (by default, it's located at **C:\Program Files\ManageEngine\ADSelfService Plus\bin).**
- Back on the Package Details page, enter the name of the MSI file you have selected in the **MSI / MSP File Name** field.

- 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 Parameters.** Click **View Parameters** to view and copy the command.
- Remove the msiexec /i "\\*ADSelfServicePlusClientSoftware.msi*" at the beginning of the command as well as the *qb* at the end, and paste the modified command into the **MSI/MSP Properties for installation** field.

For example, if the SCCM command in the UI is in this format:

```
msiexec /i  "\\ADSelfServicePlusClientSoftware.msi"  SERVERNAME=abc.selfservice.com"
PORTNO="443" INSTALLATION_KEY="19d82629b4e540fc873df8775d3630cb"
BUTTONTEXT="Reset Password / Unlock Account" BYPASS="true" FRAMETEXT="Can't login?
Please click on Reset Password/Unlock Account button to reset your password or unlock your
account" GINAHOSTEXCLUDE="okta,onelogin" MFAENROLLMENTWINDOWTITLE="Multi-Factor
Authentication - Enrollment" MFAWINDOWTITLE="Multi-Factor Authentication"
PPE_POPUP="true" PROD_TITLE="ADSelfService Plus" RESTRICTBADCERT="false"
SERVERUNREACH="This action requires you to be verified with MFA. Please make sure the
ADSelfService Plus server is reachable, has a proper SSL certificate, and connected to the domain
controller. " SHOWADSSPLINK="true" SHOWADSSPTILE="true" WINDOWSLOGONTFA="true"
MACHINEMFAUSAGESCENARIO="31"
```

then remove the msiexec /i "\\ADSelfServicePlusClientSoftware.msi" at the beginning and paste the modified command into the **MSI/MSP Properties for installation field**:

```
SERVERNAME=abc.selfservice.com" PORTNO="443"
INSTALLATION_KEY="19d82629b4e540fc873df8775d3630cb" BUTTONTEXT="Reset Password /
Unlock Account" BYPASS="true" FRAMETEXT="Can't login? Please click on Reset
Password/Unlock Account button to reset your password or unlock your account"
GINAHOSTEXCLUDE="okta,onelogin" MFAENROLLMENTWINDOWTITLE="Multi-Factor
Authentication - Enrollment" MFAWINDOWTITLE="Multi-Factor Authentication"
PPE_POPUP="true" PROD_TITLE="ADSelfService Plus" RESTRICTBADCERT="false"
SERVERUNREACH="This action requires you to be verified with MFA. Please make sure the
ADSelfService Plus server is reachable, has a proper SSL certificate, and connected to the domain
controller. " SHOWADSSPLINK="true" SHOWADSSPTILE="true" WINDOWSLOGONTFA="true"
MACHINEMFAUSAGESCENARIO="31"
```

**Note 1:** The full list of all the parameters that can be used during installation of the login agent is given in the tabular column below. If you want your client software to have the default layout, only enter the default command shown above; otherwise, you can customize it with any of the other parameters.

**Note 2:** The starred (*) parameters are applicable only in cases where the server is offline or unreachable. Otherwise, the enforced status will be decided in real time based on the policy configuration settings in the product.

| PARAMETER NAME | MATCHING REGISTRY VALUE | DEFAULT PARAMETER VALUE | DESCRIPTION |
|---|---|---|---|
| **SERVERNAME** | ServerName | The server on which ADSelfService Plus is running (based on the Access URL configured) | Specifies the ADSelfService Plus DNS hostname to be contacted after GINA login agent startup during machine login or self-service password rest o account unlock. |
| **PORTNO** | PortNumber | The port number of the ADSelfService Plus server (based on the Access URL configured) | Defines the port number used by the ADSelfService Plus server. |
| **SERVER CONTEXTPATH** | ServerContext Path | None | The context path of the ADSelfService Plus server. To learn more about the context path, click here. |
| **INSTALLATION_ KEY** | InstallationKey | None | The installation key that links the ADSelfService Plus server and client securely. |
| **BUTTONTEXT** | ButtonText | Reset Password / Unlock Account | Determines whether MFA should be bypassed or not when the ADSelfService Plus server is unreachable during machine logins. |
| **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 logon? 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). |
| **GINAHOST-EXCLUDE** | 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. This parameter must be used if SAML authentication is enabled for MFA and third-party IdPs are configured. |

| | | | |
|---|---|---|---|
| **MFAENROLLMEN 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 polic requirements must be displayed on 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 o expired, self-signed, or invalid SSL certificates during self -service actions vvand MFA, or not.<br>**Note:** We strongly advise against setting the login agent to work even when the SSL certificate is invalid in your production environment, as it willseverely impact security. Please disable this only for testing purposes. |
| **SERVERUNREACH** | ServerUnreach | Server unreachable due to intermittent network connectivity or improper SSL certification, or as the Domain Controller configured in ADSelfService Plus is down. Please contact your administrator. | Defines the error message to be displayed if the server is unreachable during password reset, account unlock, or MFA. |
| **SHOWADSSPLINK** | ShowADSSPLink | TRUE | Determines the ADSelfService Plus link on 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. |
| **WINDOWSLOGONTFA** | WindowsLogonTFA | FALSE | Determines whether MFA for machine login has been enabled or not. |

<table>
<tr><td rowspan="7"><b>MACHINEMFAUSAGESCENARIO*</b></td><td rowspan="7">MFAUsage ScenarioMask</td><td rowspan="7">5</td><td colspan="2">Determines whether the MFA for machine login feature will be enabled for specific scenarios or not based on the value provided. Learn more.</td></tr>
<tr><th>Scenario where MFA is required</th><th>Corresponding Parameter Value</th></tr>
<tr><td>For machine login</td><td>1</td></tr>
<tr><td>For locked machines</td><td>2</td></tr>
<tr><td>For RDP server</td><td>4</td></tr>
<tr><td>For UAC</td><td>8</td></tr>
<tr><td>For RDP client</td><td>16</td></tr>
</table>

**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 |
|---|---|---|---|
| **ISMACHINEMFAENFORCED*** | 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 credential 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's name. |
| **VPN_PORT_NO** | VpnPortNo | None | Defines the ADSelfService Plus server's port number used to connect to a VPN. |

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

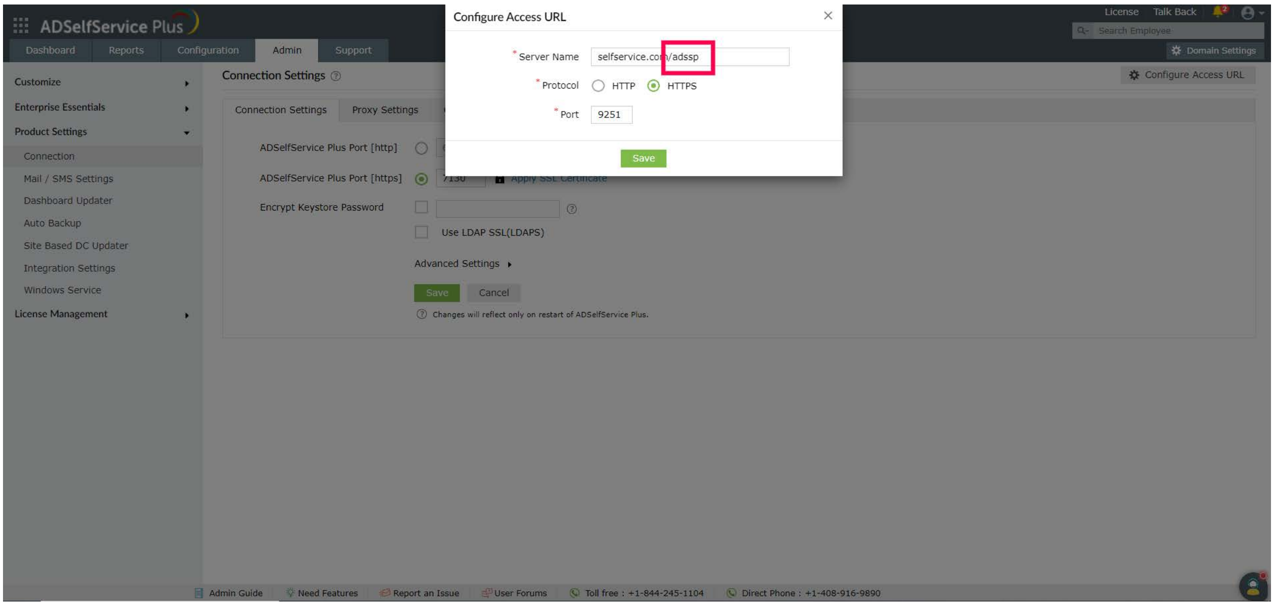
| | | | |
|---|---|---|---|
| **VPN_DISCONNECT _CMD** | VpnDisconnectCmd | None | A VPN-provider-specific command used to disconnect from the VPN during cached credential updates. |
| **WRAPPINGPROVIDER** | WrappingProvider | None | The GUID of your third-party GINA/CP extension. |
| **IMAGEPATH** | GPO script parameter | | Enter the file path of the BMP file to be used as the client software icon.<br>The filename should be reset_icon.bmp. |
| **CUSTOMTITLEICONPATH** | GPO script parameter | | Specifies the network share or path of the icon file used as a client software favicon. Ensure that the custom title icon is uploaded at **C:\\Windows\\System32\\ADSSPDesktop.ico.** The *filename should be ADSSPDesktop.ico.* |

The following parameters pertain to the installation and customization of offline MFA:

<table>
<tr><th>PARAMETER NAME</th><th>MATCHING REGISTRY VALUE</th><th>DEFAULT PARAMETER VALUE</th><th colspan="2">DESCRIPTION</th></tr>
<tr><td><b>OFFLINEMFA</b></td><td>OfflineMFA</td><td>FALSE</td><td colspan="2">Specifies whether offline MFA is enabled or not.</td></tr>
<tr><td rowspan="9"><b>LOCALE_ID</b></td><td rowspan="9">LocaleId</td><td rowspan="9">NONE</td><td colspan="2">Specifies the display language used for some parts of the login agent.</td></tr>
<tr><th>LANGUAGE</th><th>KEY</th></tr>
<tr><td>Simplified Chinese</td><td>zh-cn</td></tr>
<tr><td>Japanese</td><td>ja</td></tr>
<tr><td>French</td><td>fr-fr</td></tr>
<tr><td>German</td><td>de-de</td></tr>
<tr><td>Turkish</td><td>tr</td></tr>
<tr><td>Spanish</td><td>es-mx</td></tr>
<tr><td>Polish</td><td>pl</td></tr>
</table>

| | | | |
|---|---|---|---|
| **OFFLINE_WEB_LOGO_NAME** | OfflineWebLogo-Name | 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 the 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.



Configure Access URL

* Server Name: selfservice.com/adssp

* Protocol: ○ HTTP ● HTTPS

* Port: 9251

Connection Settings

ADSelfService Plus Port [http] ○

ADSelfService Plus Port [https] ● 7130 Apply SSL Certificate

Encrypt Keystore Password □

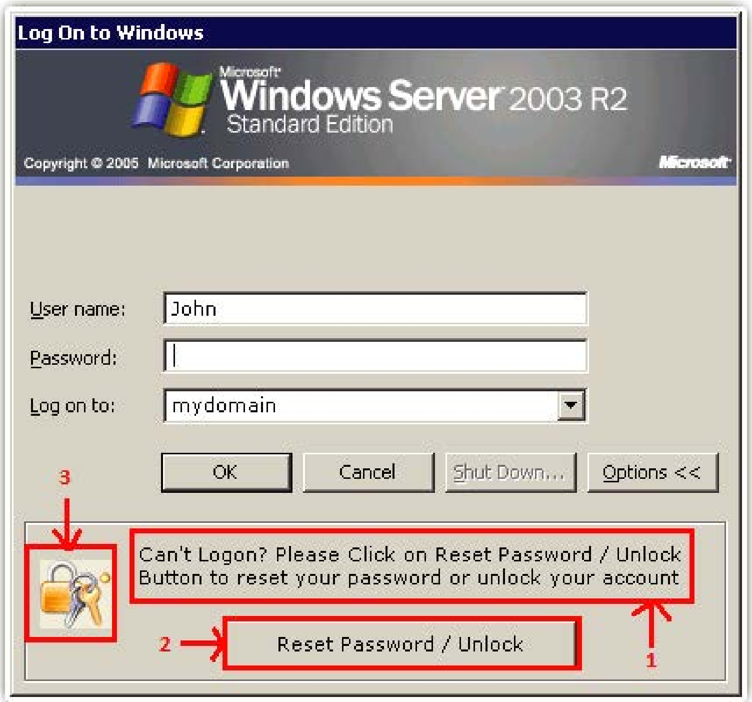
□ Use LDAP SSL(LDAPS)

Changes will reflect only on restart of ADSelfService Plus.

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.



Log On to Windows

Microsoft Windows Server 2003 R2 Standard Edition

Copyright © 2005 Microsoft Corporation

User name: John

Password:

Log on to: mydomain

OK
Cancel
Shut Down...
Options <<
3
Can't Logon? Please Click on Reset Password / Unlock Button to reset your password or unlock your account
2
Reset Password / Unlock
1

Figure 1. Frame text, button text, and icon for Windows XP/Windows Server 2003 and below.

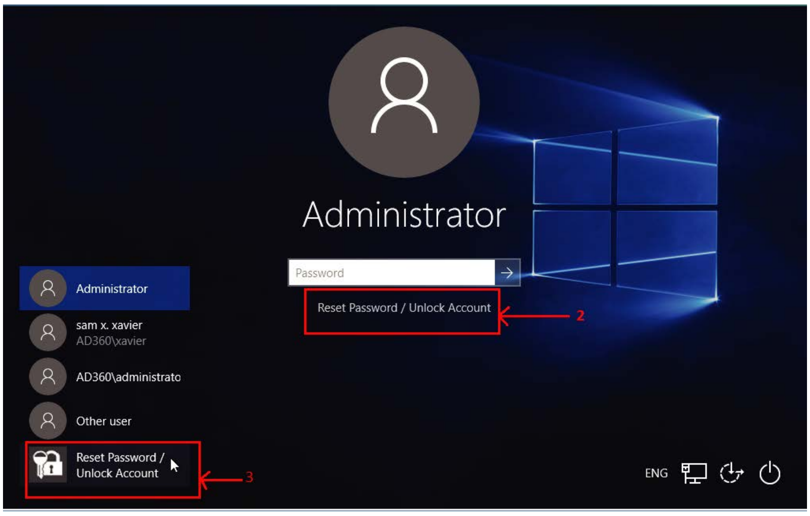


Figure 2. Button text and icon for Windows 8, Windows Server 2012, and above.

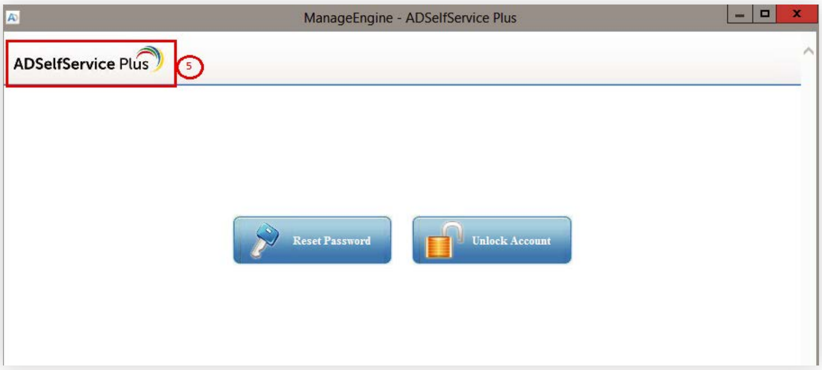
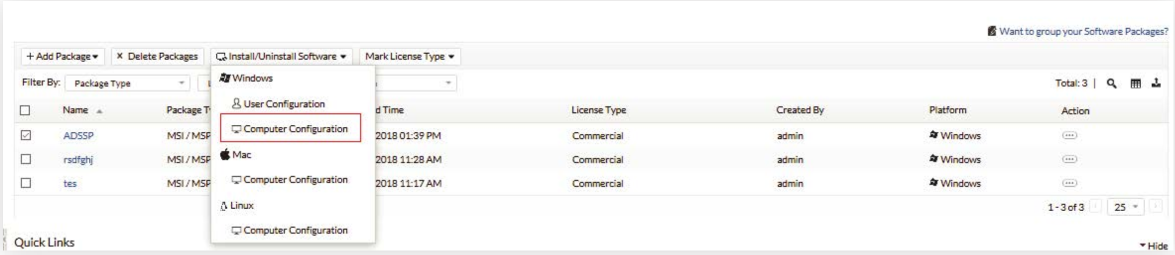


Figure 3. Product title text.

- Click **Add Package.**
- You have now created a software package that you can deploy to the computers in your domain.

## Step 2: Deploying an MSI package

- Select the **package** you have created in the **Packages** tab. Select **Computer Configuration** from the **Install/Uninstall Software** drop-down.



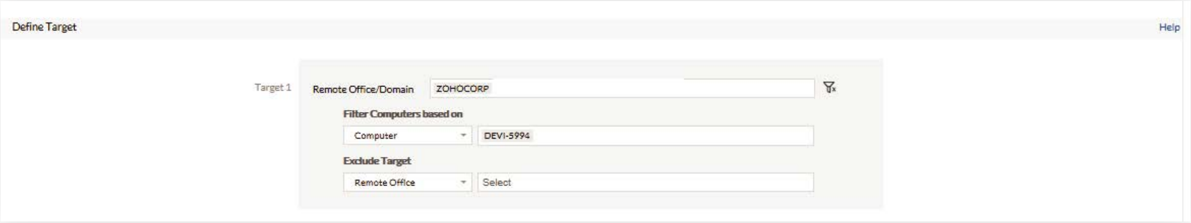
Filter By: Package Type

Total: 3

| ☐ | Name | Package T | d Time | License Type | Created By | Platform | Action |
|---|---|---|---|---|---|---|---|
| ☑ | ADSSP | MSI / MSP | 2018 01:39 PM | Commercial | admin | Windows | ⋯ |
| ☐ | rsdfghj | MSI / MSP | 2018 11:28 AM | Commercial | admin | Windows | ⋯ |
| ☐ | tes | MSI / MSP | 2018 11:17 AM | Commercial | admin | Windows | ⋯ |

1 - 3 of 3 25

- On the Install/Uninstall Windows Software page that opens, enter a **Name.**
- In the *Define Target* section, select the required domains and computers to which you'd like to deploy the **MSI package.**



Define Target

Target 1

Remote Office/Domain: ZOHOCORP

Filter Computers based on: Computer — DEVI-5994

Exclude Target: Remote Office — Select

- Click **Deploy Immediately.**

Note: If a new installation key is generated, copy the command with the new installation key from the ADSelfService Plus admin portal and update the MSI/MSP Properties for installation field with the new command for all new installations.

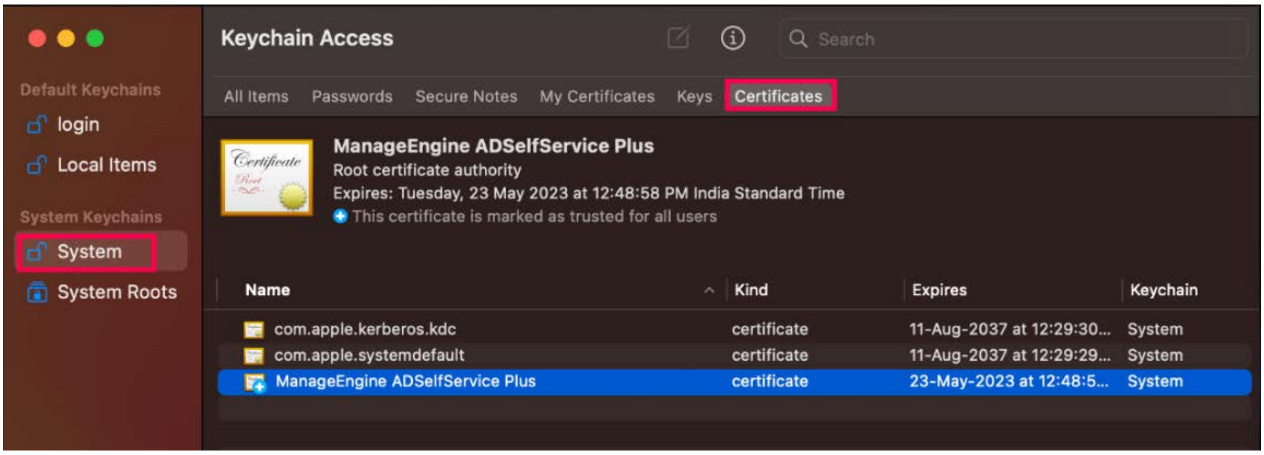
# Steps for installing the login agent on macOS machines

## Before you begin (mandated for macOS 13 and later)

The ADSelfService Plus SSL certificate should be trusted in the Keychain Access app on macOS. This is mandatory for machines running macOS version 13 (Ventura) or later. To do this:

- Open the **Keychain Access** app on the Mac running macOS version 13 (Ventura) or later.
- Download and include ADSelfService Plus' certificate authority certificate in the System Keychain, under the Certificates tab.

- Expand the trust section of the certificate and mark **When using the certificate** to **Always Trust.**



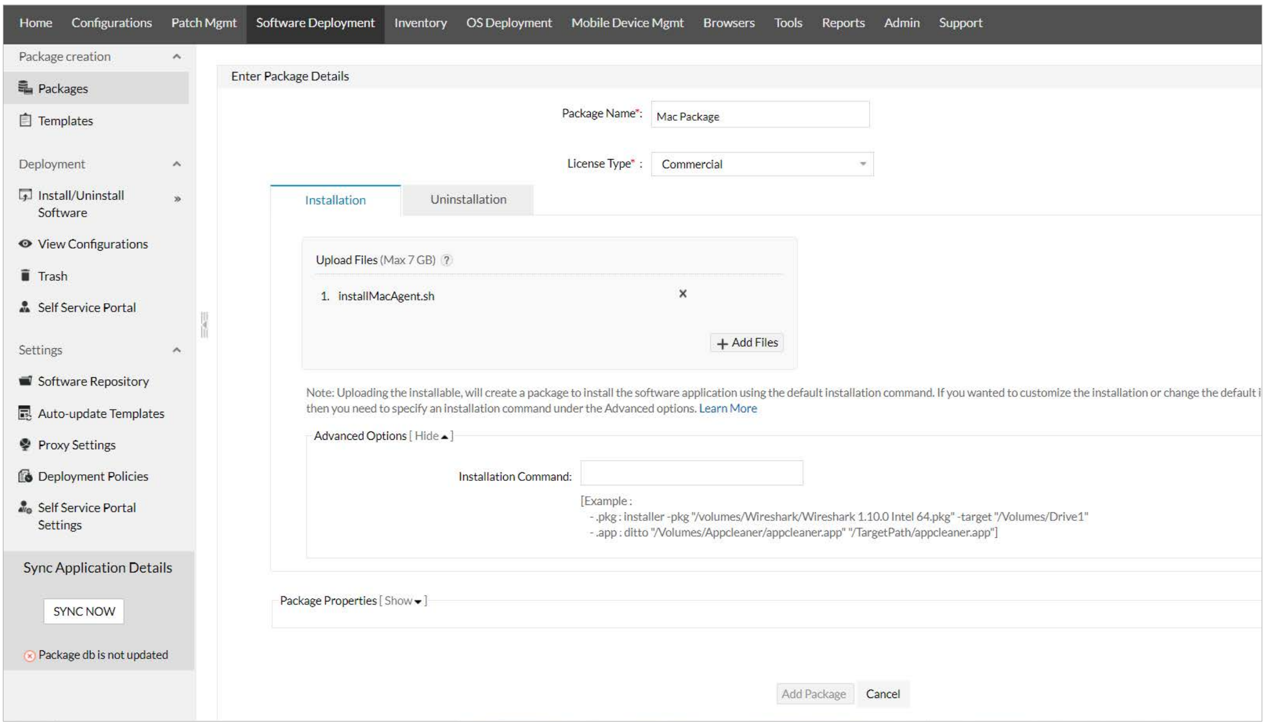
**ManageEngine ADSelfService Plus**
Root certificate authority
Expires: Tuesday, 23 May 2023 at 12:48:58 PM India Standard Time
This certificate is marked as trusted for all users

| Name | Kind | Expires | Keychain |
|---|---|---|---|
| com.apple.kerberos.kdc | certificate | 11-Aug-2037 at 12:29:30... | System |
| com.apple.systemdefault | certificate | 11-Aug-2037 at 12:29:29... | System |
| ManageEngine ADSelfService Plus | certificate | 23-May-2023 at 12:48:5... | System |

## Step 1: Creating a macOS package

1. Log in to **Endpoint Central** as an admin.

2. Navigate to **Software Deployment > Packages > Add Package** and select **Windows** or **Mac** based on your requirements.



Enter Package Details

Package Name*: Mac Package

License Type* : Commercial

Upload Files (Max 7 GB)

1. installMacAgent.sh

Note: Uploading the installable, will create a package to install the software application using the default installation command. If you wanted to customize the installation or change the default i
then you need to specify an installation command under the Advanced options. Learn More

Installation Command:

```
[Example :
  - .pkg : installer -pkg "/volumes/Wireshark/Wireshark 1.10.0 Intel 64.pkg" -target "/Volumes/Drive1"
  - .app : ditto "/Volumes/Appcleaner/appcleaner.app" "/TargetPath/appcleaner.app"]
```

3. Enter a **Package Name.**

4. Select **Commercial** from the **License Type** drop-down.

5. Click on the **Installation** tab.

6. In the *Upload Files* section that appears, click **Add Files** and then select **Choose Files.**

7. In the window that opens, browse and select the **installMacAgent.sh** file located in the bin folder (by default, it's located at **C:\Program Files\ManageEngine\ADSelfService Plus\bin).** The **installMacAgent.sh** file will be uploaded.

8. Follow the steps above to upload the **ADSelfServicePlusMacLoginAgent.pkg** as well.

9. Copy the macOS CLI command from the product 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's the pop-up that appears when clicking **View Command.**

**pkg, serverName, portNumbe**r 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 the following 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 |
|---|---|
| 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.<br>**Note:** We strongly advise against setting the login agent to work even when the SSL certificate is invalid in your production environment, as it will severely impact security. Please disable this only for testing purposes. |
| LoginMFA | Enter “true” if you want MFA to be enabled during login. Enter “false” if you don't want MFA to be enabled. |
| BypassMFAServerUnreach | Enter “true” if you want to bypass login MFA 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. |
| 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 login MFA to be enabled, enter “false.” |
| ButtonText | Enter the text to be displayed on the Reset Password/Unlock Account button. |

| | |
|---|---|
| **IsMFAEnforced*** | If 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. |
| **ImagePath** | Enter the file path for the Reset Password/Unlock Account button image. |

10. In **Endpoint Central**, click **Show** in the *Advanced Settings* section. In the section that appears, enter the copied command in the *Installation Command* field.

11. Click **Add Package**.

You have now created a software package that you can deploy to the computers in your domain.

## Step 2: Deploying the package

1. In the **Packages** tab, select the package you have created.

2. Select **Computer Configuration** from the **Install/Uninstall Software** drop-down.

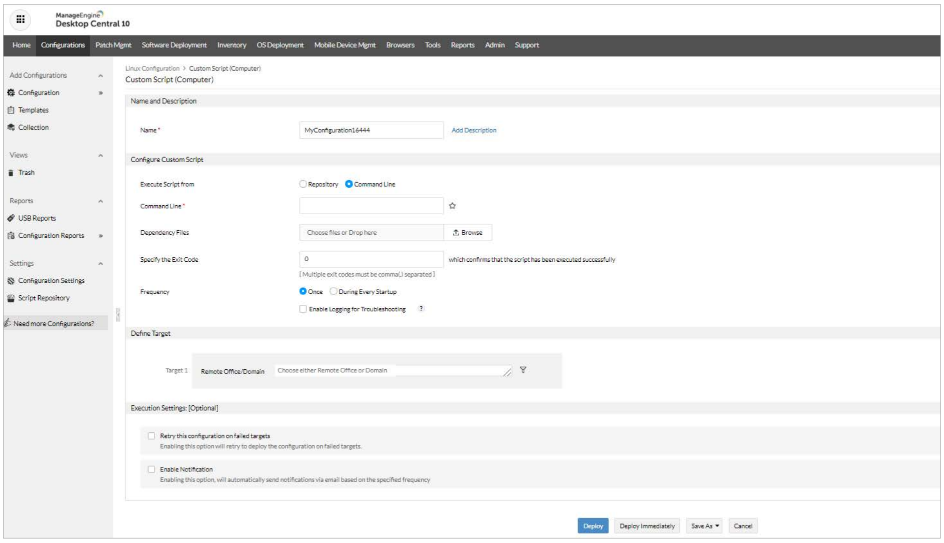
3. In the **Install/Uninstall Windows Software** page that opens, enter a **Name**. In the **Define Target** section, select the required domains and computers to which you'd like to deploy the MSI package.

4. Click **Deploy Immediately.**

**Note:** If a new installation key is generated, the admin will need to copy the command with the new installation key from the product admin portal as described in step 9 and update the Installation Command field with the new command for all new installations (step 10).

# Steps for installing the login agent on Linux machines

1. Log in to Endpoint Central's admin portal. Navigate to **Configurations**. Under *Add Configurations*, hover over **Configurations** and select **Linux**.



Linux Configuration > Custom Script (Computer)

Custom Script (Computer)

Name and Description

Name*: MyConfiguration16444

Configure Custom Script

Execute Script from: ○ Repository ● Command Line

Command Line*:

Dependency Files: Choose files or Drop here

Specify the Exit Code: 0 which confirms that the script has been executed successfully

[ Multiple exit codes must be comma(,) separated ]

Frequency: ● Once ○ During Every Startup

□ Enable Logging for Troubleshooting ?

Define Target

Target 1 Remote Office/Domain: Choose either Remote Office or Domain

Execution Settings: [Optional]

□ Retry this configuration on failed targets
Enabling this option will retry to deploy the configuration on failed targets.

□ Enable Notification
Enabling this option, will automatically send notifications via email based on the specified frequency

2. On the **Add Configurations** page that opens up, click **Computer** under **Custom Script.**

3. In the **Custom Script (Computer)** section that opens, provide a **Name** for the configuration.

4. Under **Execute Script From,** select **Command Line.**

5. Copy the Linux CLI command from the product 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's the pop-up that appears when clicking **View Command**.

**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 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.<br>**Note:** We strongly advise against setting the login agent to work even when the SSL certificate is invalid in your production environment, as it will severely impact security. Please disable this only for testing purposes. |
| 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 login MFA 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 login MFA 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 bound 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. |

6. In **Endpoint Central**, click **Show** in the **Advanced Settings** section. In the section that appears, enter the copied command in the **Installation Command** field.
Note: If a new Installation Key is generated, the admin will need to copy the command with the new Installation Key from the product admin portal as described in step 5 and update the **Installation Command** field with the new command for all new installations (step 6).

7. In the **Dependency Files** field, click **Browse**. In the window that opens, select the **installLinuxAgent.sh** file located in the bin folder (by default, it's located at **C:\Program Files\ManageEngine\ADSelfService Plus\bin).** The installLinuxAgent.sh file will be uploaded.

8. Follow the steps above to upload the **ADSSPLinuxClient.tar.gz** and **ADSSPLinuxClient64.tar.gz** files as well.

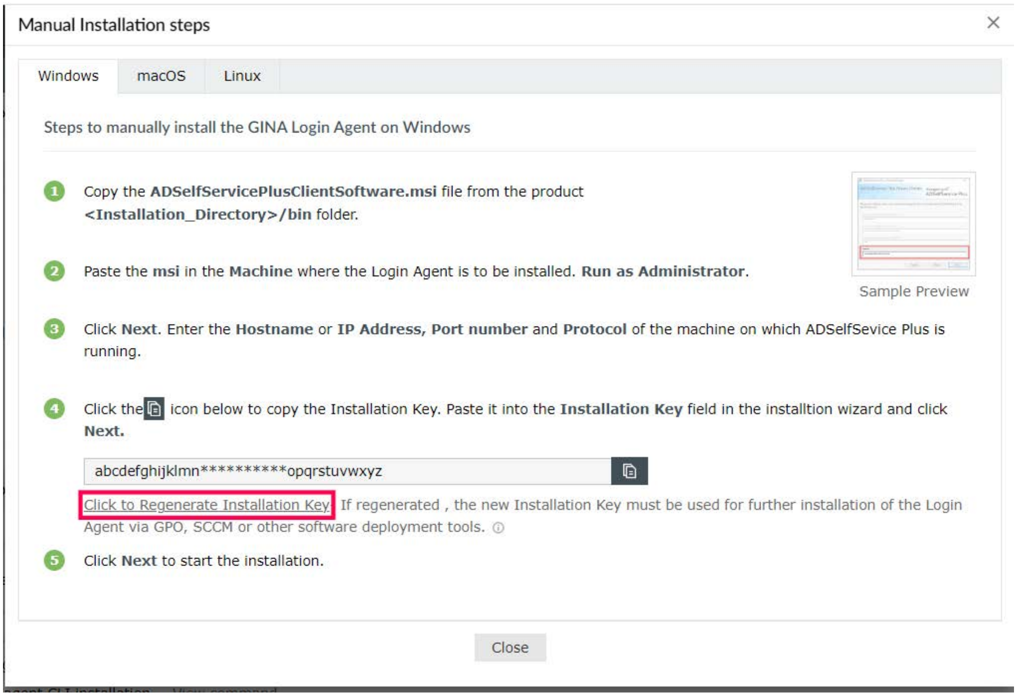
9. Specify the **Exit Code** as **0**.

10. In the **Define Target** section, select the domains and computers to which you'd like to deploy the MSI package.

11. Click **Deploy Immediately**.

## Login agent Installation Key

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


Manual Installation steps

Steps to manually install the GINA Login Agent on Windows

1. Copy the **ADSelfServicePlusClientSoftware.msi** file from the product **<Installation_Directory>/bin** folder.
2. Paste the **msi** in the **Machine** where the Login Agent is to be installed. **Run as Administrator.**
3. Click **Next.** Enter the **Hostname** or **IP Address, Port number** and **Protocol** of the machine on which ADSelfSevice Plus is running.
4. Click the icon below to copy the Installation Key. Paste it into the **Installation Key** field in the installtion wizard and click **Next.**

abcdefghijklmn**********opqrstuvwxyz

Click to Regenerate Installation Key If regenerated , the new Installation Key must be used for further installation of the Login Agent via GPO, SCCM or other software deployment tools.

5. Click **Next** to start the installation.

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.

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