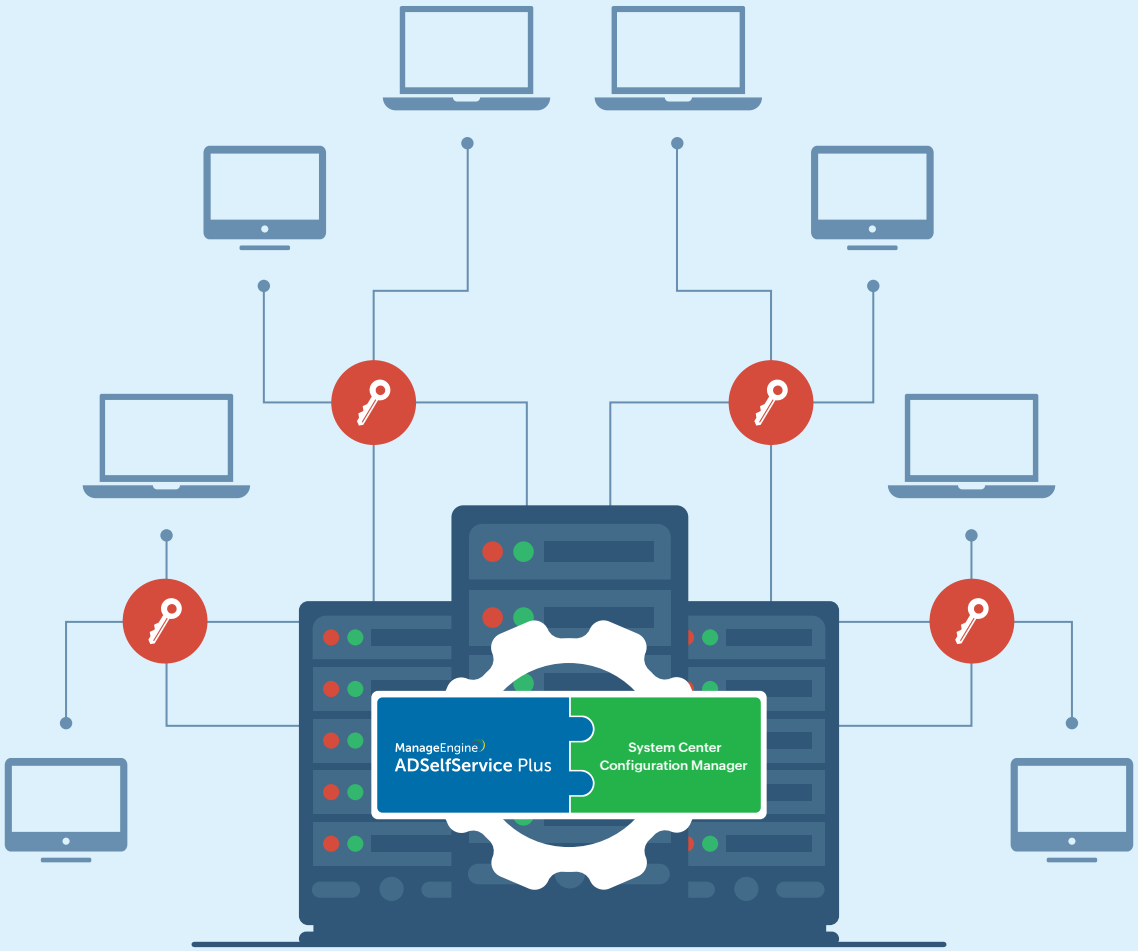
ManageEngine
ADSelfService Plus

Installing ADSelfService Plus client software using System Center Configuration Manager



www.adselfserviceplus.com

Table of Contents

Document Summary — 1

The ADSelfService Plus Login Agent — 1

ADSelfService Plus Login Agent installation using SCCM — 1

- Step 1: Create a network share — 1
- Step 2: Create an MSI package — 2
- Step 3: Deploy the MSI package — 12

Login Agent Installation Key — 18

Document summary

This document briefly describes the ADSelfService Plus login agent (GINA/Credential Provider agent) and its uses. This document will also guide you through the steps involved in installing the agent in a set of computers of a domain, using System Center Configuration Manager.

The ADSelfService Plus login agent

The ADSelfService Plus login agent is an extension of the standard Credential Provider from Microsoft. When installed, it can enable multi-factor authentication (MFA) for local Windows logins, RDP logins, and User Access Control actions to protect machines from credential-based attacks. It also adds a button labeled Reset Password/Unlock Account to the native Windows login screen, allowing users to reset their passwords and unlock their accounts directly from that screen.

ADSelfService Plus login agent installation using SCCM

System Center Configuration Manager (SCCM) is a systems management software product developed by Microsoft for managing large groups of computers running Windows NT, Windows Embedded, macOS (OS X), Linux, or UNIX, as well as many other operating systems. Using its software distribution capability, you can deploy ADSelfService Plus client software to the desired computers in a domain.

Prerequisites

1. The Endpoint MFA add-on for ADSelfService Plus is required to enable MFA for Windows logins. Visit the store to purchase the add-on.
2. The ADSelfService Plus Professional Edition is required to enable self-service password reset and account unlock on Windows login screens.
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.

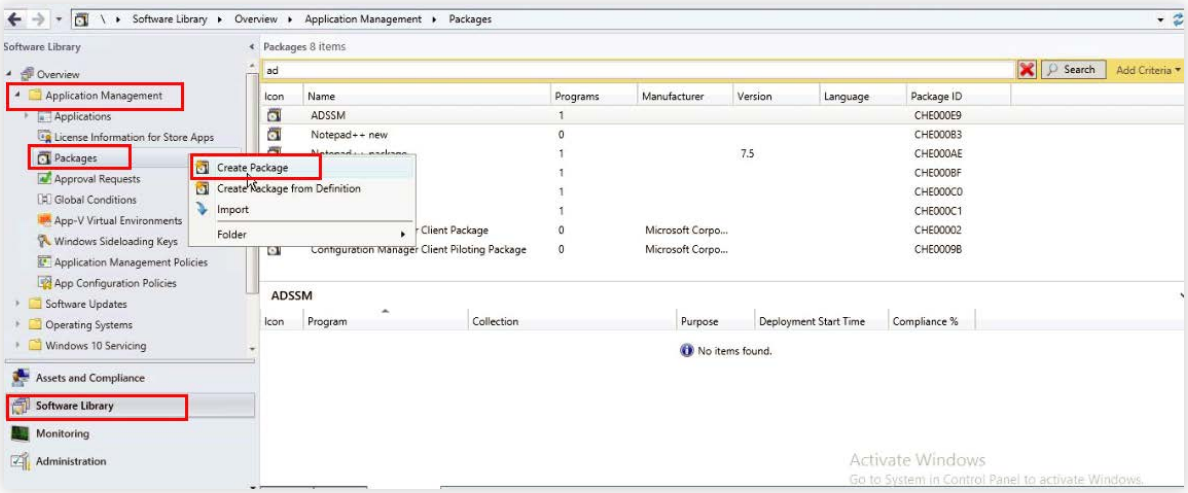
Step 1: Create a network share

1. Go to **[install_dir] > ManageEngine > ADSelfService Plus > bin.**
2. Copy the *ADSelfServicePlusClientSoftware.msi* file located in the **bin** folder, and paste it in a network share.

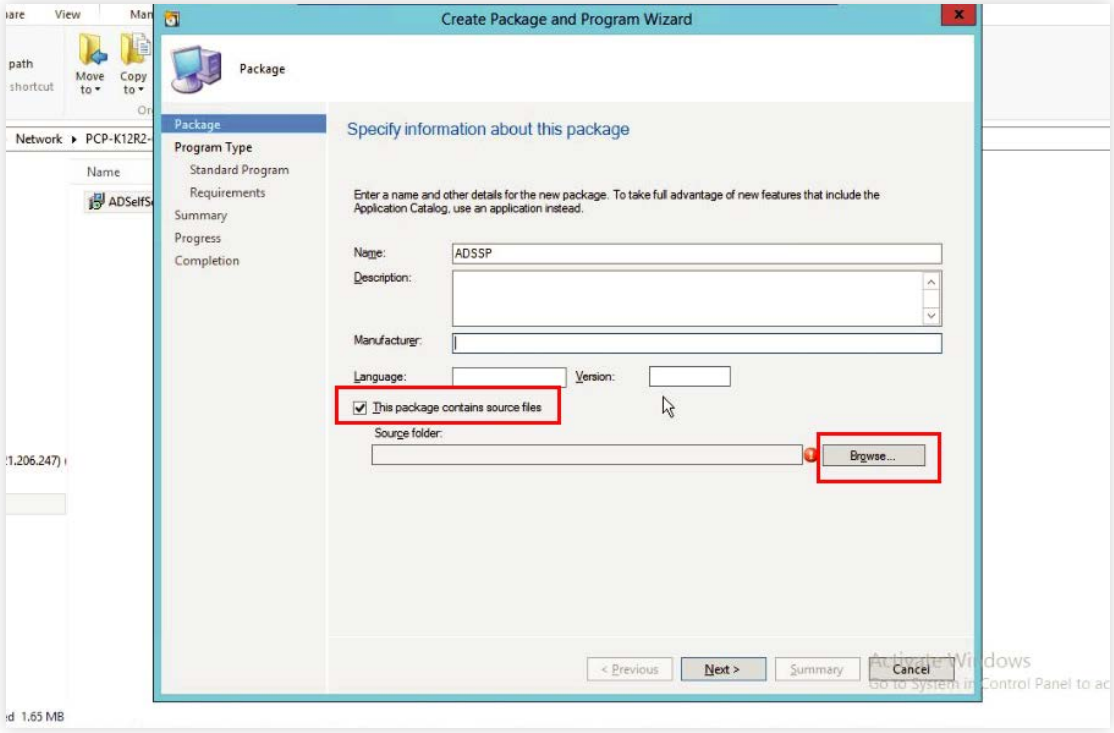
Note: Make sure that the SCCM administrator has read access to the network share in which the *ADSelfServicePlusClientSoftware.msi* file is located.

Step 2: Create an MSI package

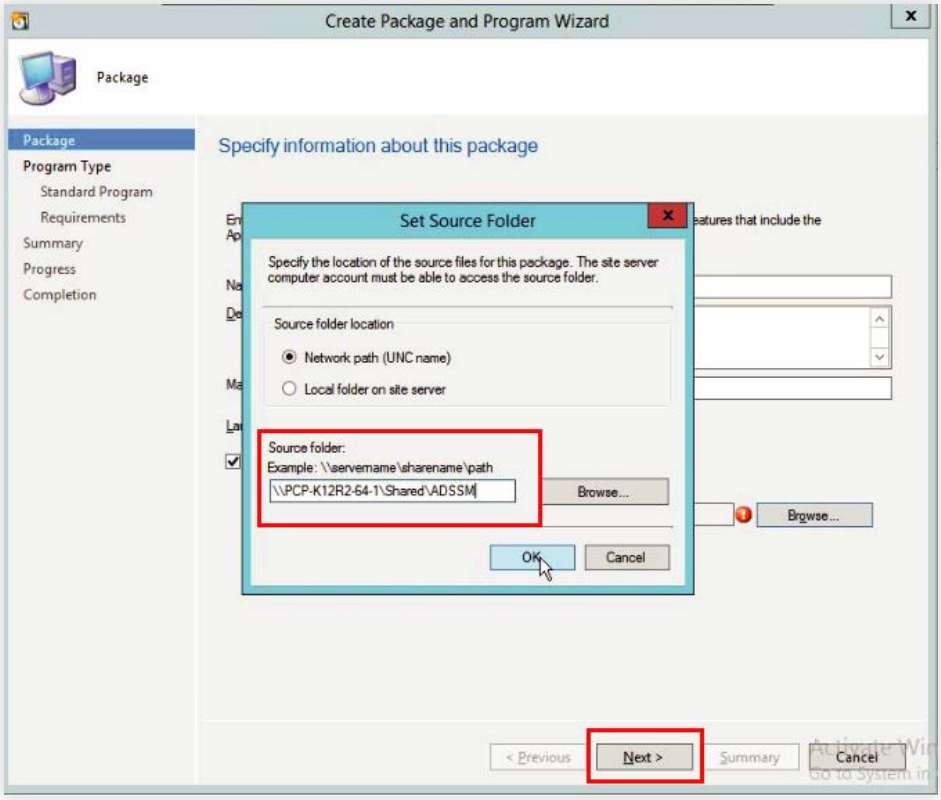
1. Go to the **System Center Configuration Manager** console.
2. Navigate to **Software Library > Application Management** drop-down **> Packages > Create Package.**



3. In the *Package* tab of the *Create Package and Program Wizard,* enter an appropriate **Name** for the package.
4. Provide a **Description**, the **Manufacturer** name, **Language**, and **Version** based on the requirements.
5. Click **Browse** next to the *Source folder* field.

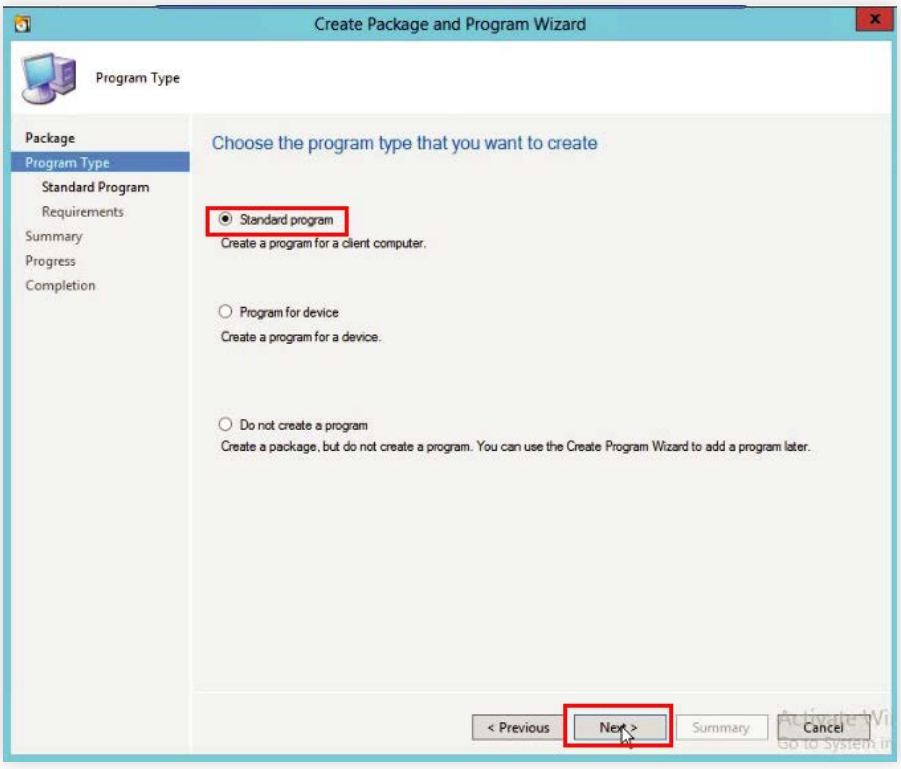


6. Enter the location of the Source folder (i.e. the network share which contains the required *ADSelfServicePlusClientSoftware.msi* file).



7. Click **Ok** and Click **Next.**

8. Select **Standard program** from the *Program Type* tab and click **Next.**



9. Enter the **Name** of the package.

10. In the Command field, enter the MSI command to be used for installation via SCCM.
    To find the command, log into the ADSelfService Plus admin portal and 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 Parameters** to view the command, then copy it.

      Example: msiexec /i "\\ADSelfServicePlusClientSoftware.msi" SERVERNAME=abc.selfservice.com" PORTNO="443" INSTALLATION_KEY="19d82629b4e540fc873df8775d3630cb" BUTTONTEXT="Reset Password / Unlock Account" BYPASS="true" FRAMETEXT="Can't log on? Please click on the 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 is connected to the domain controller." SHOWADSSPLINK="true" SHOWADSSPTILE="true" WINDOWSLOGONTFA="true" MACHINEMFAUSAGESCENARIO="31"

    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 shown above; 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	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 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.

SERVER CONTEXTPATH	ServerContextPath	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	Specifies the button text visible on the Windows login to launch the Reset Password/Account Unlock wizar.
BYPASS	Bypass	FALSE	Determines whether MFA should be bypassed when the ADSelfService Plus server is unreachable during machine logins.
FRAMETEXT	FrameText	Can't logon? Please click 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.)
GINAHOSTE-XCLUDE	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 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.

<table>
<tr><td>RESTRICTBADCERT</td><td>RestrictBadCert</td><td>TRUE</td><td>Determines whether the usage of expired, self-signed, or invalid SSL certificates during self -service actions and MFA is restricted or not.
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.</td></tr>
<tr><td>SERVERUNREACH</td><td>ServerUnreach</td><td>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.</td><td>Defines the error message to be displayed if the server is unreachable during password reset, account unlock, or MFA.</td></tr>
<tr><td>SHOWADSSPLINK</td><td>ShowADSSPLink</td><td>TRUE</td><td>Determines the ADSelfService Plus link in the Ctrl-Alt-Del screen.</td></tr>
<tr><td>SHOWADSSPTILE</td><td>ShowADSSPTile</td><td>TRUE</td><td>Determines whether the Reset Password/Account Unlock button is displayed as a credential tile on the login screen or not.</td></tr>
<tr><td>WINDOWSLO-GONTFA</td><td>WindowsLogonTFA</td><td>FALSE</td><td>Determines whether MFA for Machine Login has been enabled or not.</td></tr>
<tr><td>MACHINEMFAU-SAGESCENARIO*</td><td>MFAUsage ScenarioMask</td><td>5</td><td>Determines whether the MFA for Machine Logins feature will be enabled for specific scenarios or not based on the value provided. Learn more.
<table>
<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></td></tr>
</table>

Note 2: 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.

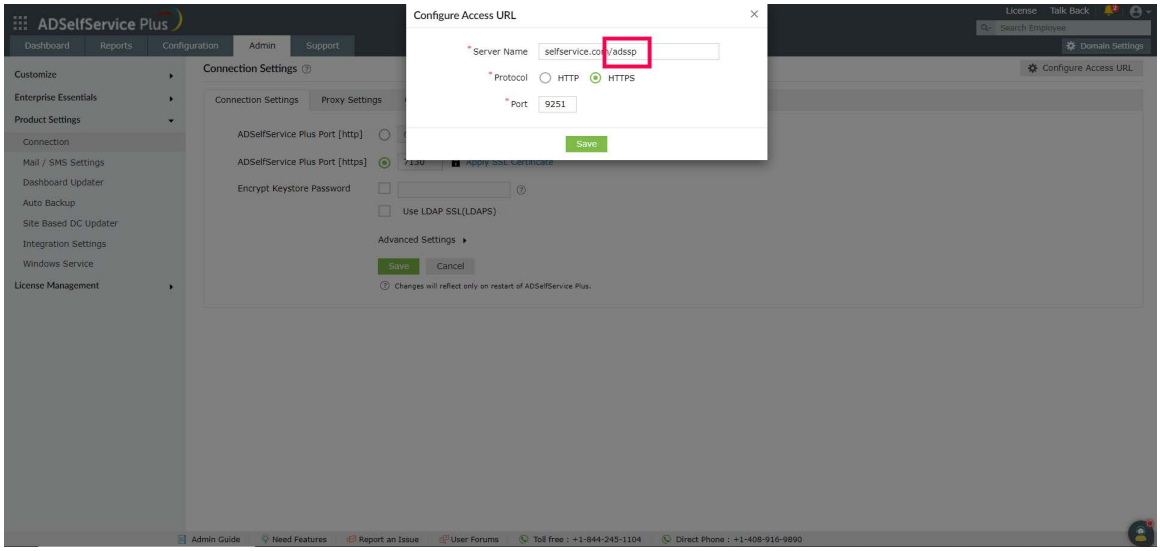
PARAMETER NAME	MATCHING REGISTRY VALUE	DEFAULT PARAMETER VALUE	DESCRIPTION
ISMACHINEMF-AENFORCED*	isMFAEnforced	FALSE	If set to true, MFA will be enforced for all users accessing the machines irrespective of their enrollment status, self-service policy membership, or ADSelfService Plus connectivity status.
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's name.
VPN_PORT_NO	VpnPortNo	None	Defines the ADSelfService Plus server's port number used to connect to the 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 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.

<table>
<tr><td>VPN_TYPE</td><td>VpnType</td><td>None</td><td>Defines the VPN connection behavior for cached credentials update based on the provider used. This pre-set 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>VPN_CLIENT_ LOCATION</td><td>VpnClientLocation</td><td>None</td><td>Specifies the VPN client location. (Example: C:\Program Files (x86)\ Fortinet\FortiClient\ FortiSSLVPN client.exe)</td></tr>
<tr><td>VPN_CONNECT_ CMD</td><td>VpnConnectCmd</td><td>None</td><td>VPN provider-specific command that is used to connect to the VPN during cache credentials update.</td></tr>
<tr><td>VPN_ DISCONNECT _ CMD</td><td>VpnDisconnectCmd</td><td>None</td><td>VPN provider-specific command that is used to disconnect from the VPN during cache credentials update.</td></tr>
<tr><td>WRAPPINGPRO- VIDER</td><td>WrappingProvider</td><td>None</td><td>GUID of your third-party GINA/CP extension.</td></tr>
<tr><td>IMAGEPATH</td><td colspan="2">GPO script parameter</td><td>Enter the file path of the BMP file to be used as the client software icon.
The filename should be reset_icon.bmp.</td></tr>
<tr><td>CUSTOMTITL- EICONPATH</td><td colspan="2">GPO script parameter</td><td>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.</td></tr>
</table>

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>DESCRIPTION</th></tr>
<tr><td>OFFLINEMFA</td><td>OfflineMFA</td><td>FALSE</td><td>Specifies whether offline MFA is enabled or not.</td></tr>
<tr><td>LOCALE_ID</td><td>LocaleId</td><td>NONE</td><td>Specifies the display language used for some parts of the login agent.<table><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></td></tr>
<tr><td>OFFLINE_WEB_LOGO_NAME</td><td>OfflineWebLogo-Name</td><td>NONE</td><td>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.</td></tr>
<tr><td>LOGOIMAGEPATH</td><td>GPO script parameter</td><td>NONE</td><td>Mentions the network share path of custom logo used during offline MFA (this will be copied to C:\\Windows\\System32\\ folder location).</td></tr>
</table>

Note 3: If your organization uses the context path functionality of the Tomcat Server, use the **SERVERCONTEXTPATH** parameter in the ADSelfService Plus login agent installation command.



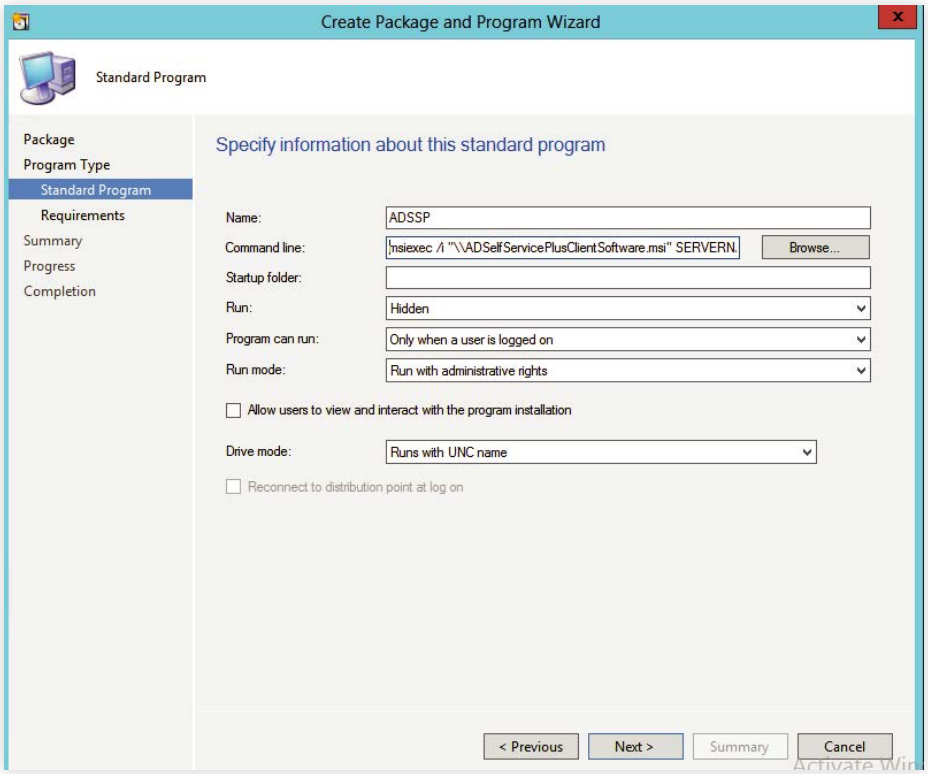
The context path can be found at the end of the ADSelfService Plus Access URL.
In this example, it is /adssp. If this parameter is used in the installation command, it will look like this example:

msiexec /i "\\ADSelfServicePlusClientSoftware.msi" SERVERNAME=abc.selfservice.com" PORTNO="443" INSTALLATION_KEY="19d82629b4e540fc873df8775d3630cb" SERVERCONTEXTPATH="/adssp"

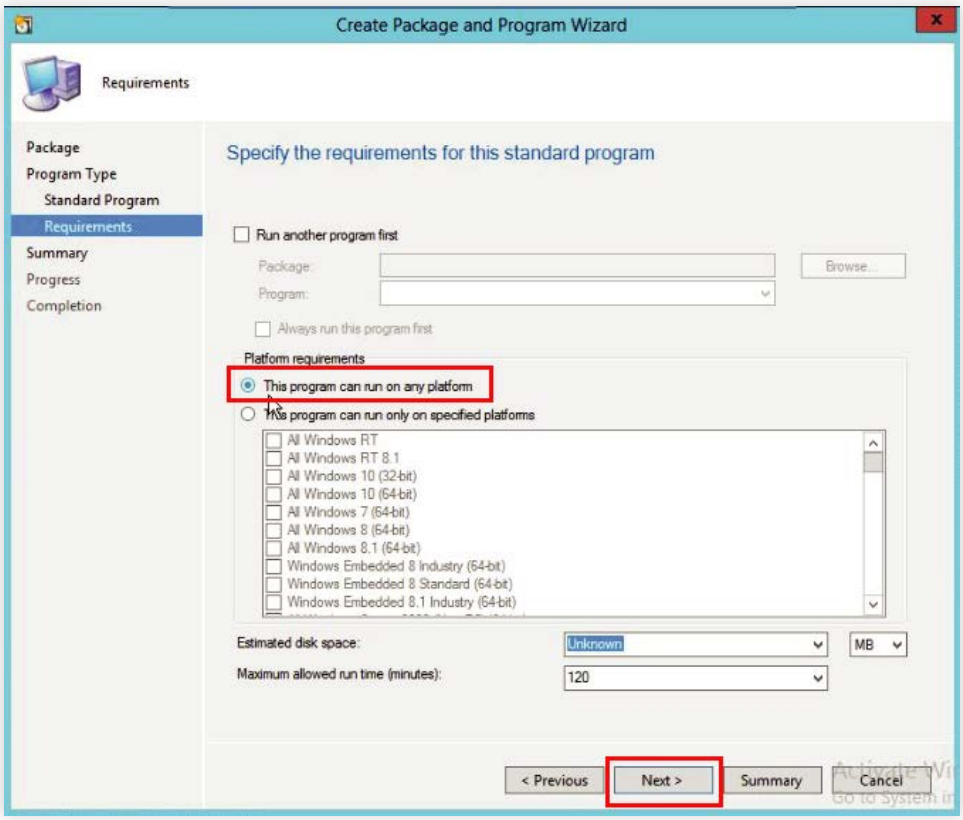
This functionality is available only for Windows clients.

Note 4: 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 10 and update the Command field with the new command for all new installations.

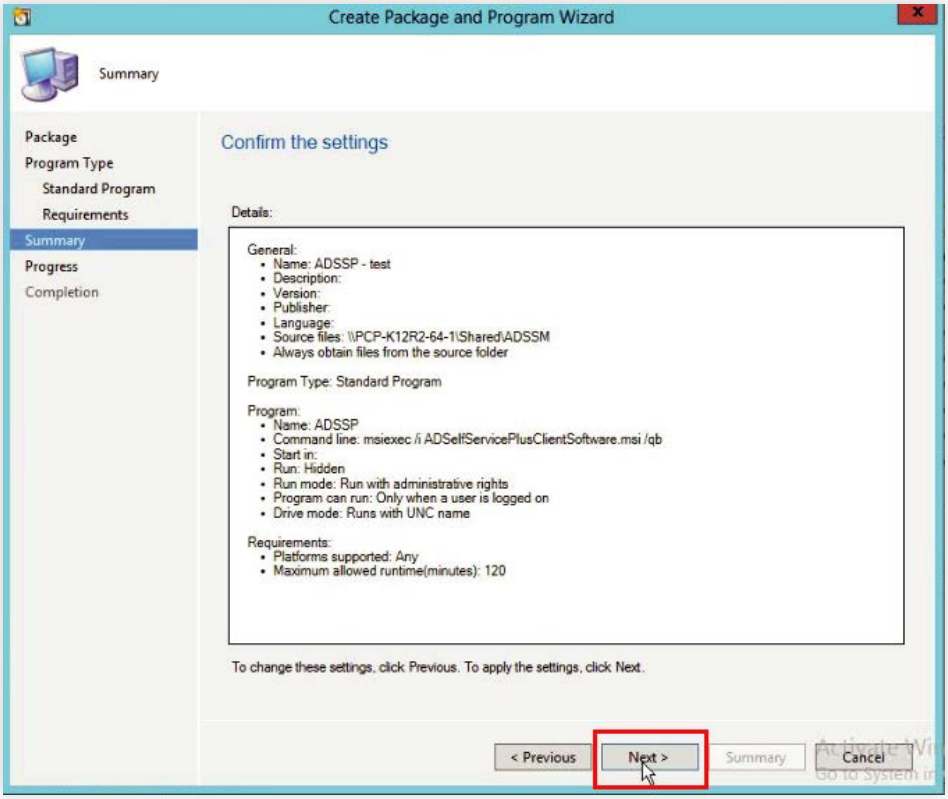
11. Select **Hidden** from the *Run* drop-down.
12. Select **Only when a user is logged on** option from the *Program can run* drop-down.
13. Select **Run with administrative rights** option from the *Run mode* drop-down.
    Click **Next**.



14. In the *Requirements* tab, select **This Program can run on any platform option** and then click **Next**.



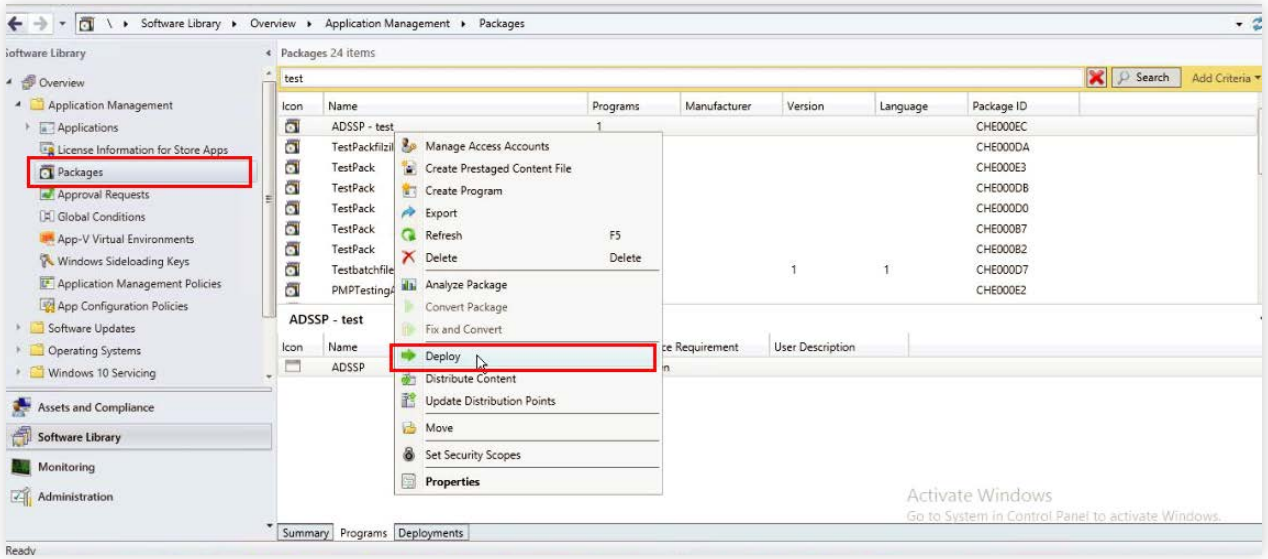
15. In the *Summary* tab, confirm the selected settings by clicking **Next.**



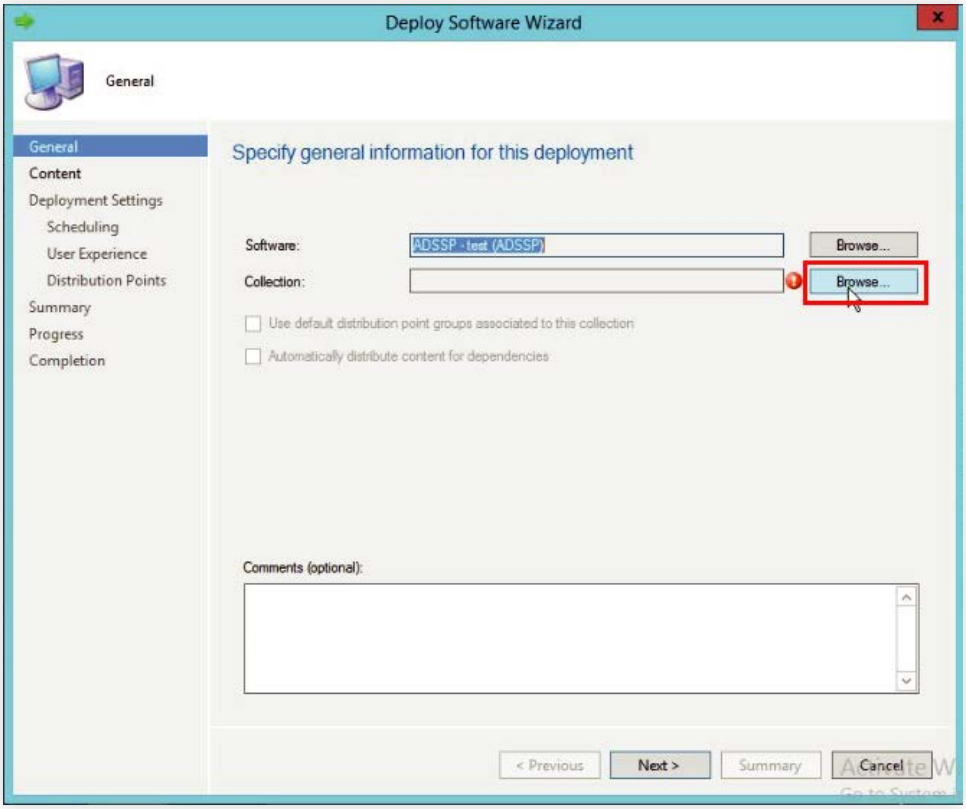
16. Click **Close** to finish.

Step 3: Deploy an MSI package

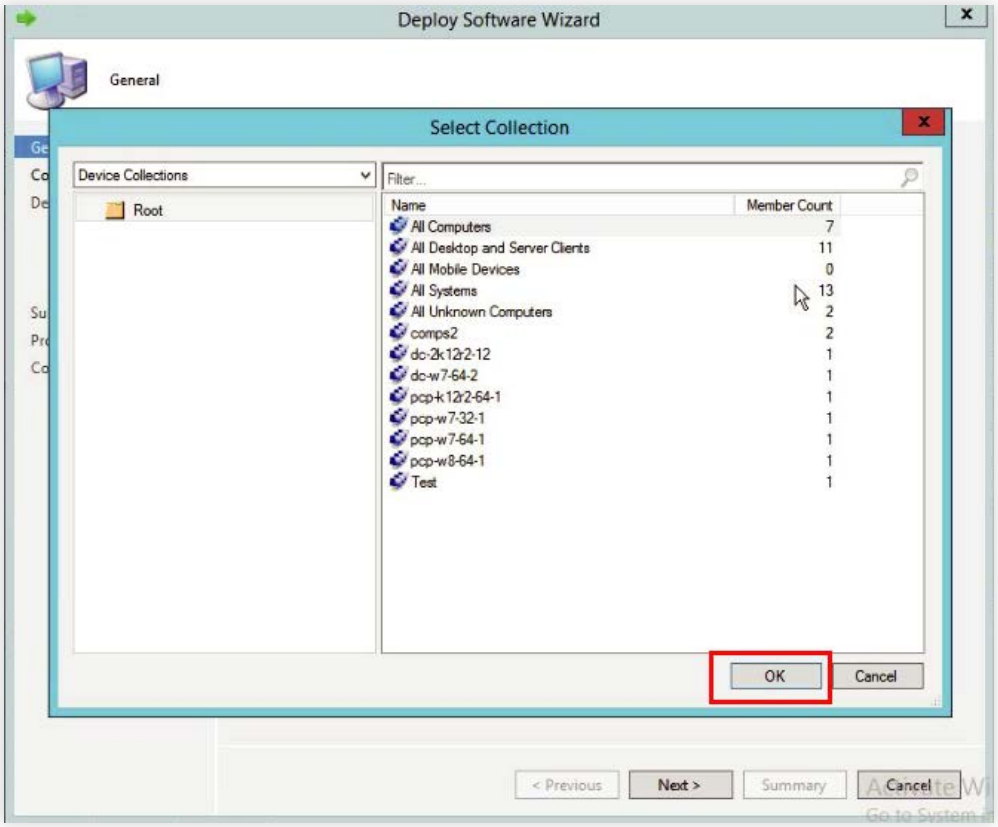
1. Select the **package** you have created in the *Packages* tab, then click **Deploy**.



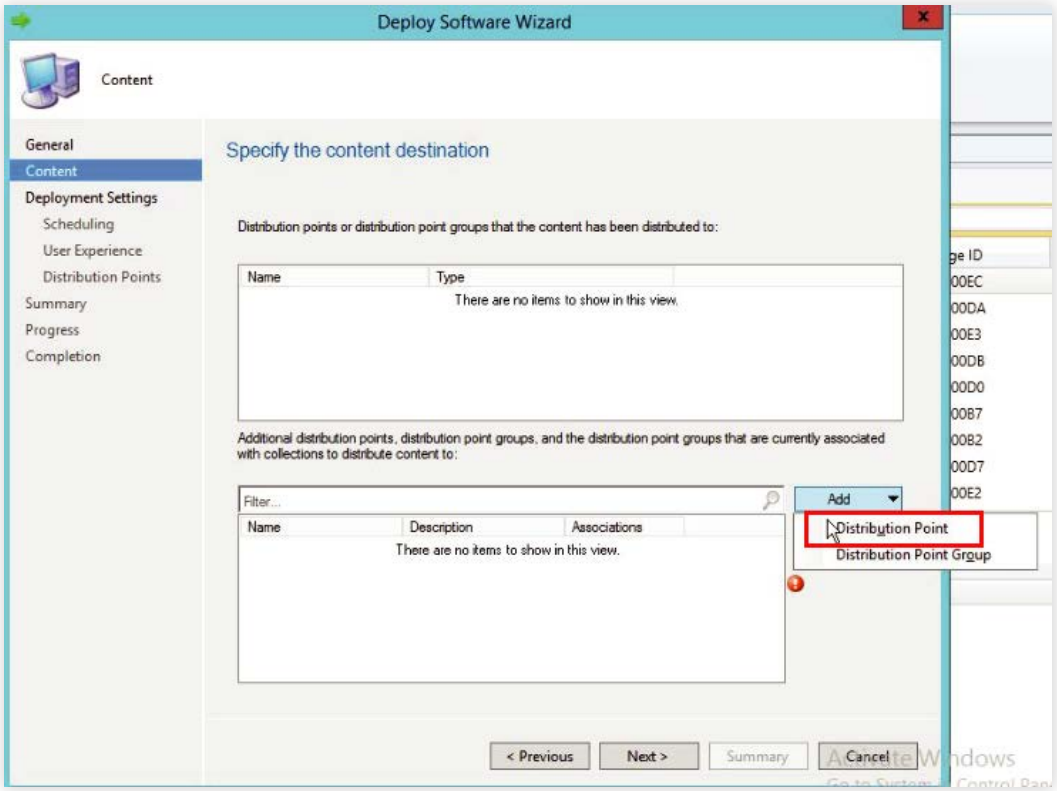
2. In the *Deploy Software Wizard*, click **Browse** next to the *Collection field.*



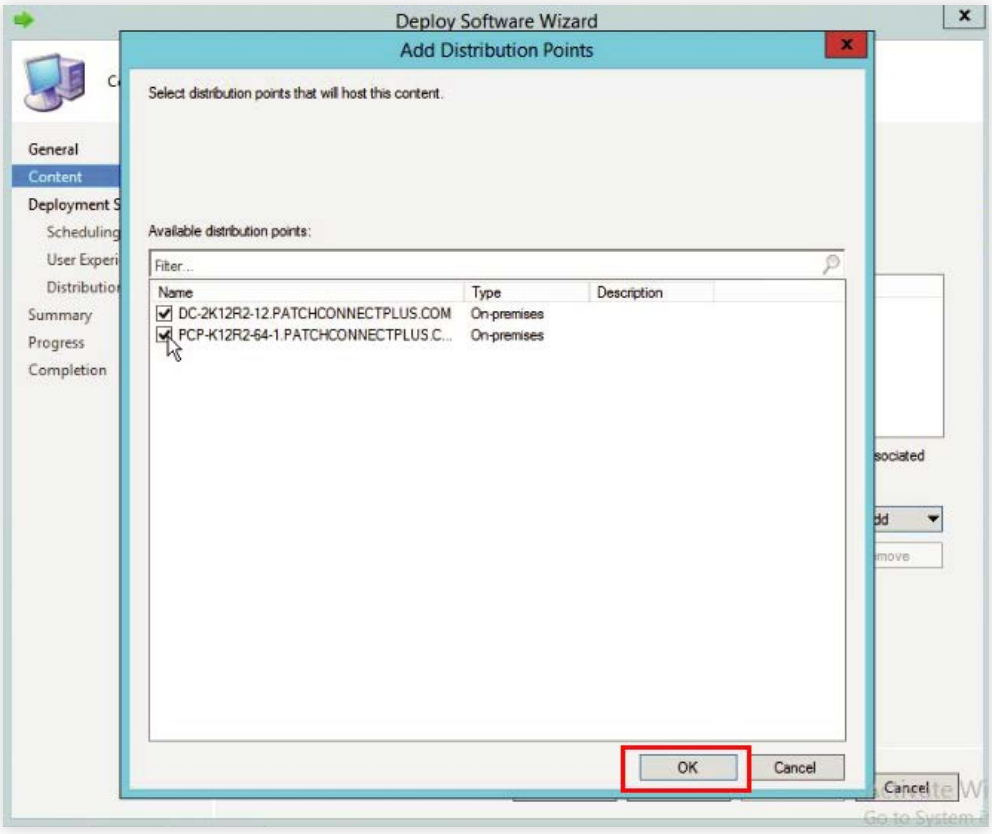
3. In the *Select Collection* window, select the **machines** in which the client software should be deployed, click **OK**, then click **Next**.



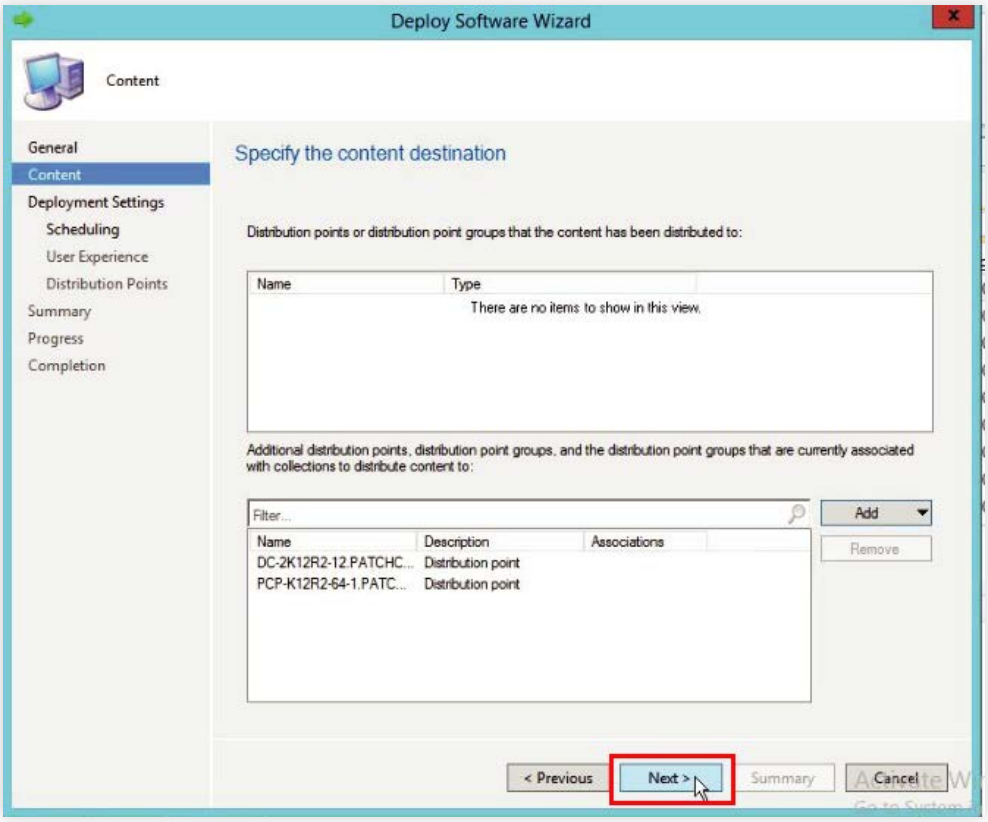
4. In the *Content* tab, select **Distribution Point** from the *Add* drop-down.



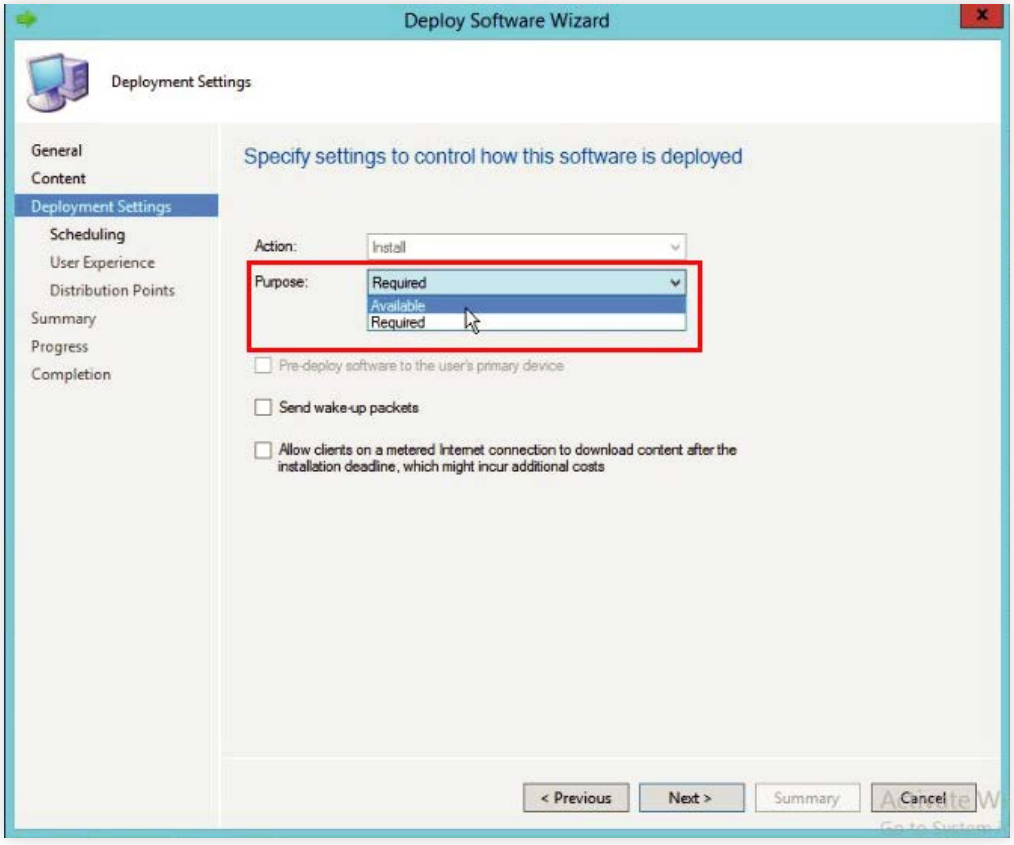
5. Select the required **Distribution Points** from the list provided, then click **OK**.



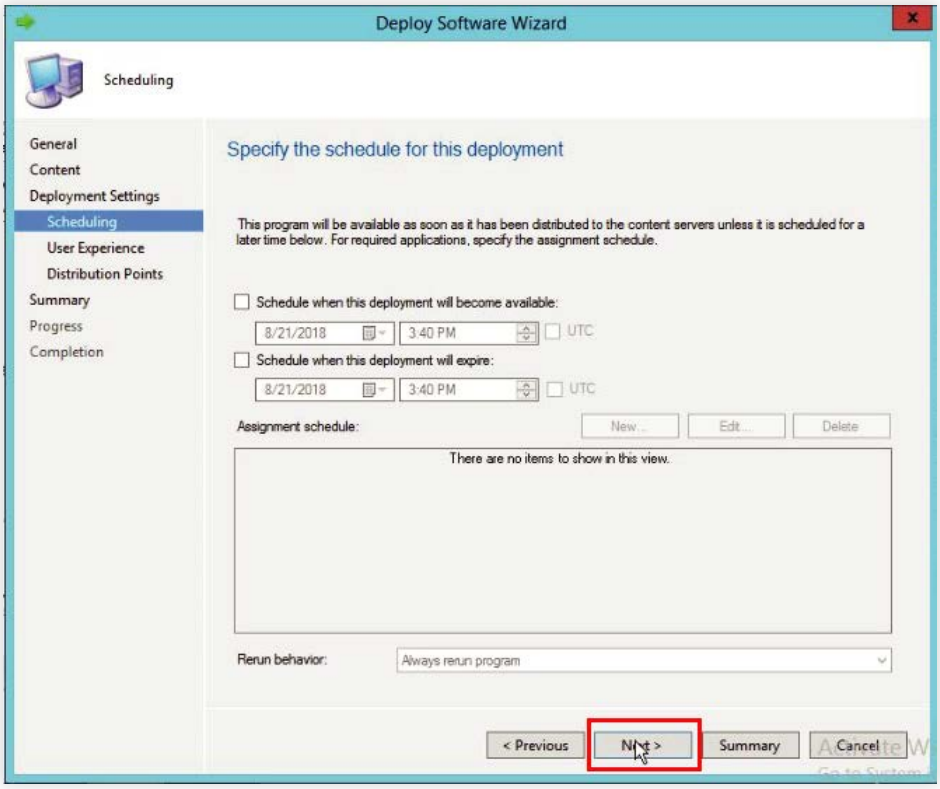
6. Make sure that the distribution points that you selected are shown in the list. Click **Next.**



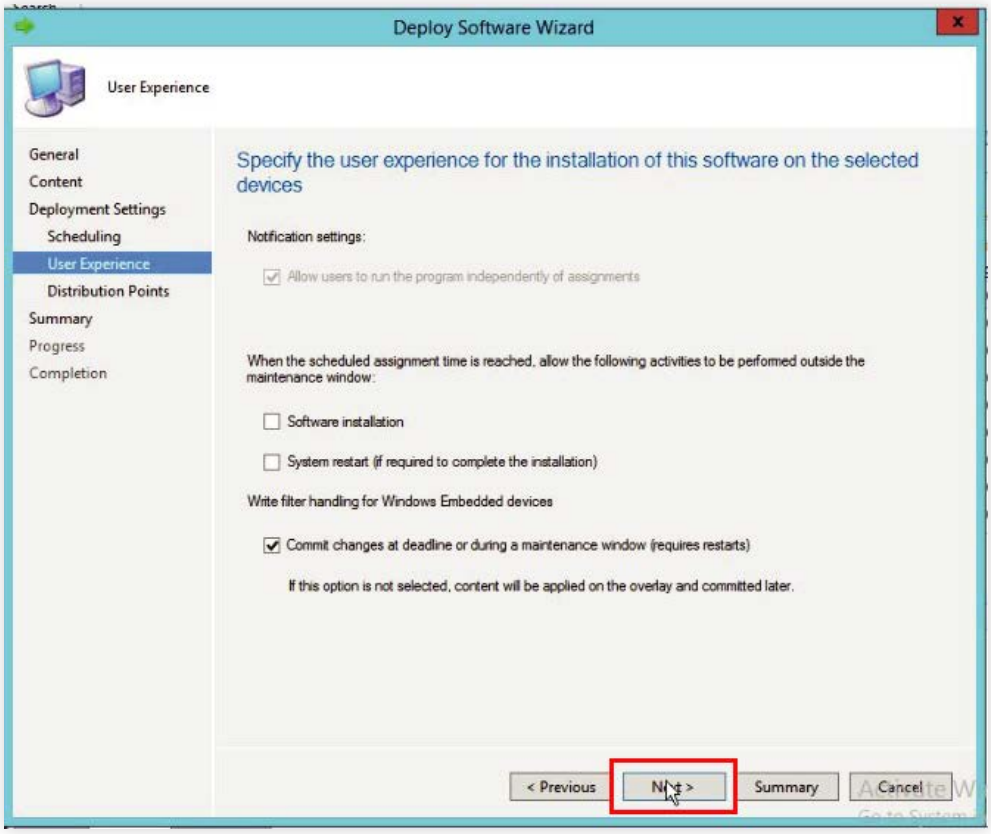
7. In the *Deployment Settings* tab, select **Required** to configure a custom schedule for installation of the client software. Click **Next.**



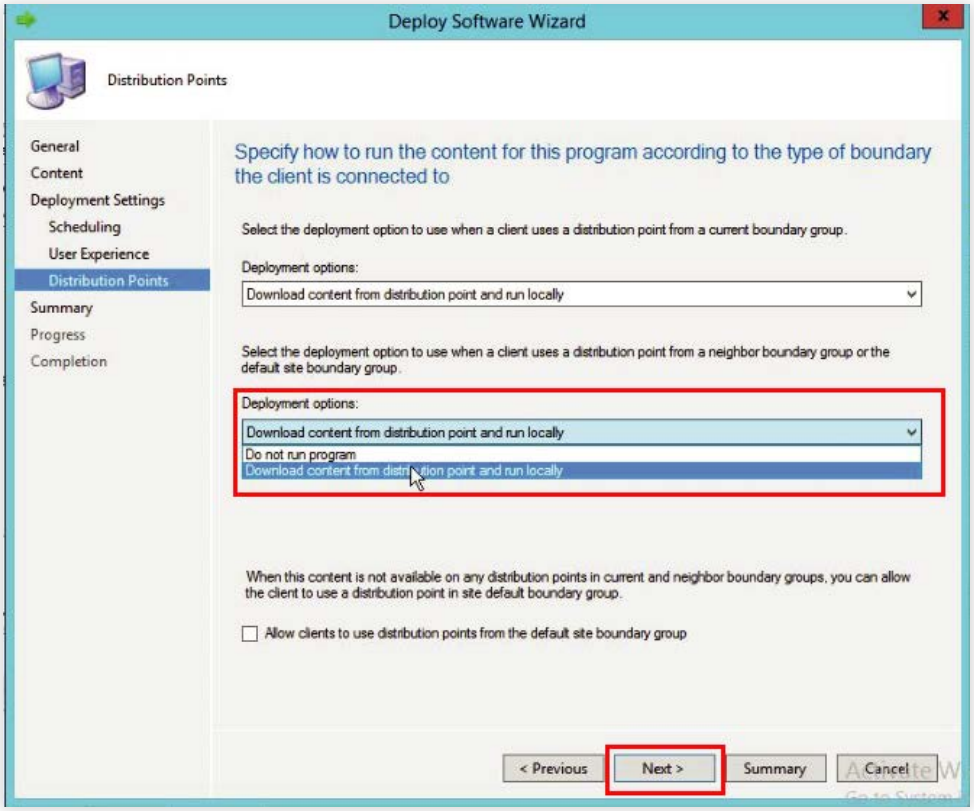
8. In the *Scheduling* tab, specify the schedule for the deployment. Click **Next.**



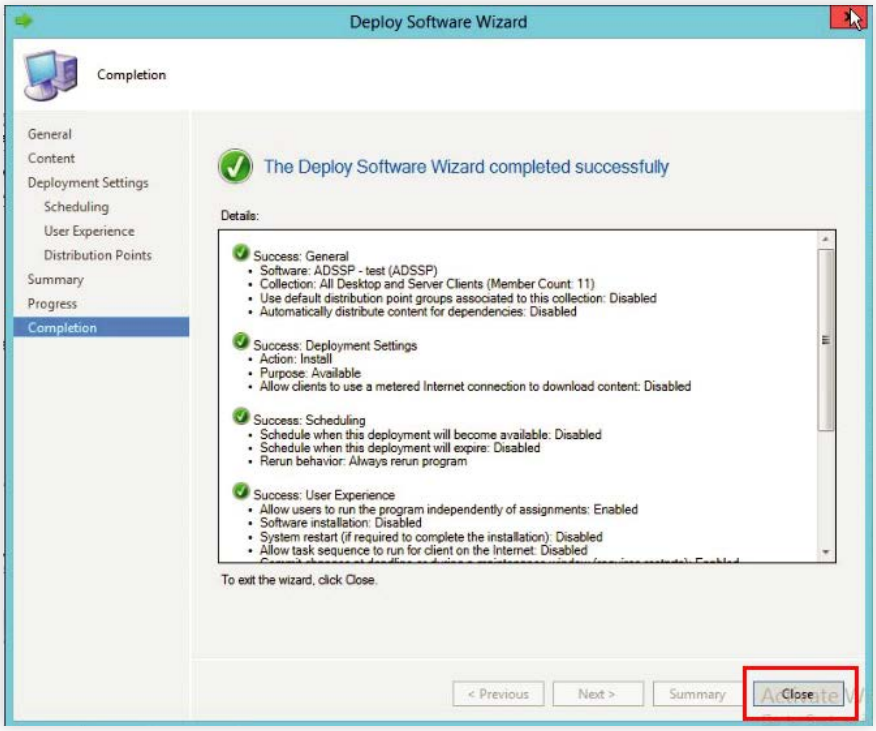
9. Make the necessary changes in the *User Experience* tab. Click **Next.**



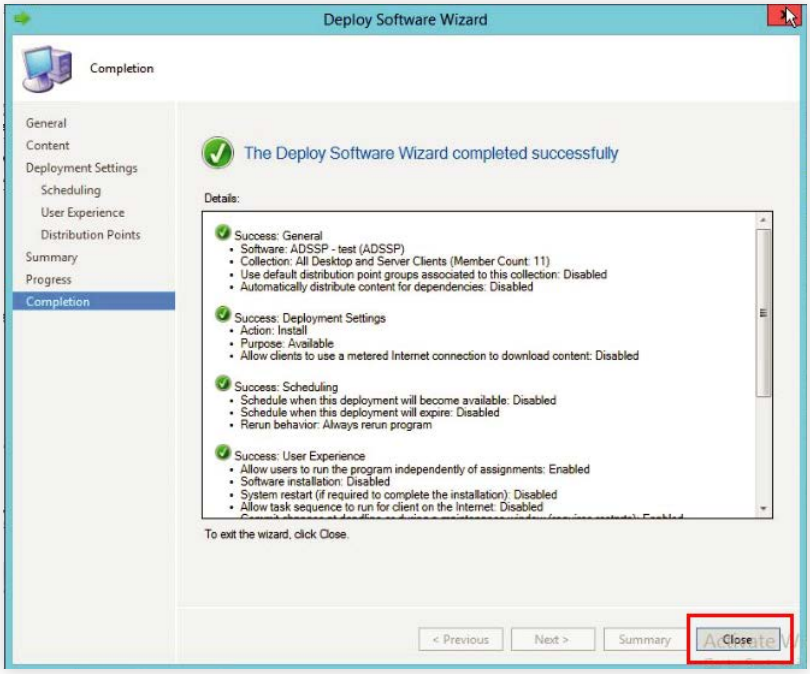
10. In the *Distribution Points* tab, choose **Download content from distribution point** as a deployment option. Click **Next.**



11. Confirm the settings chosen and click **Close.**



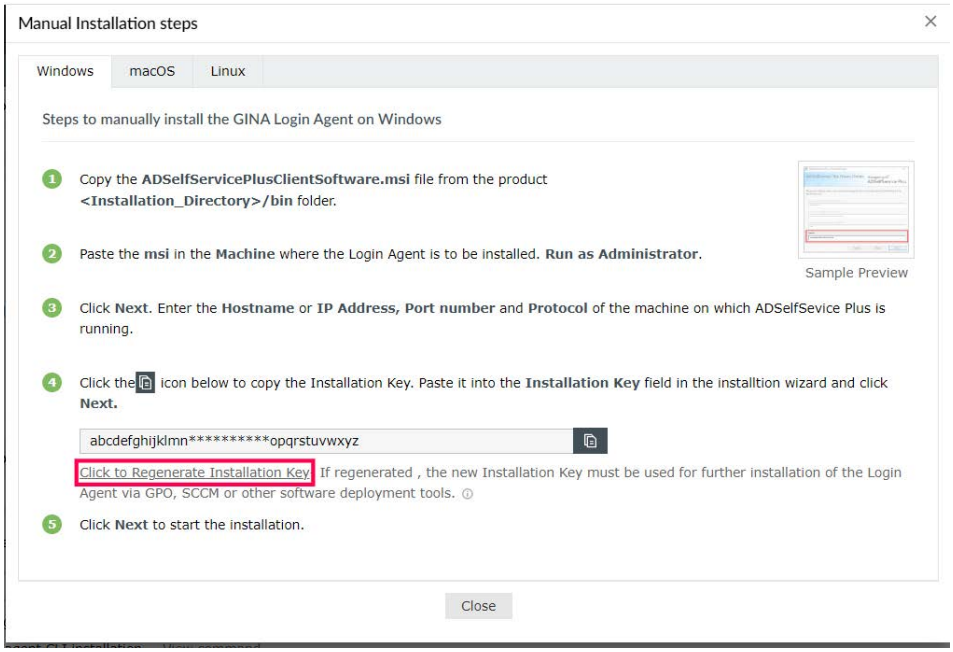
11. Confirm the settings chosen and click **Close.**



You have now deployed the *ADSelfServicePlusClientSoftware.msi* file on the selected client machines.

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.

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