

Installing ADSelfService Plus client software using System Center Configuration Manager

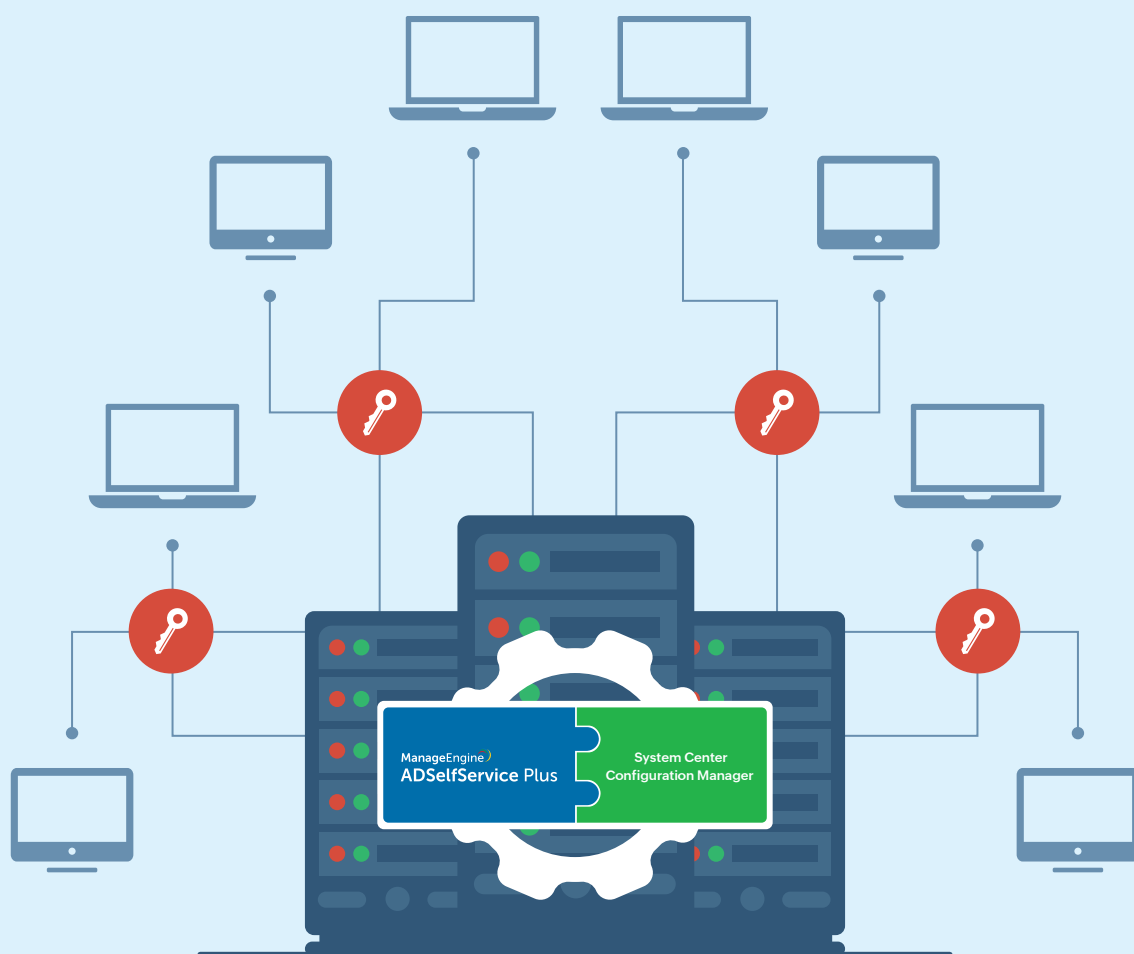


Table of Contents

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. ADSelfService Plus with Endpoint MFA is required to enable MFA for endpoints.
[Visit the store](#) to purchase Endpoint MFA.
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](#).

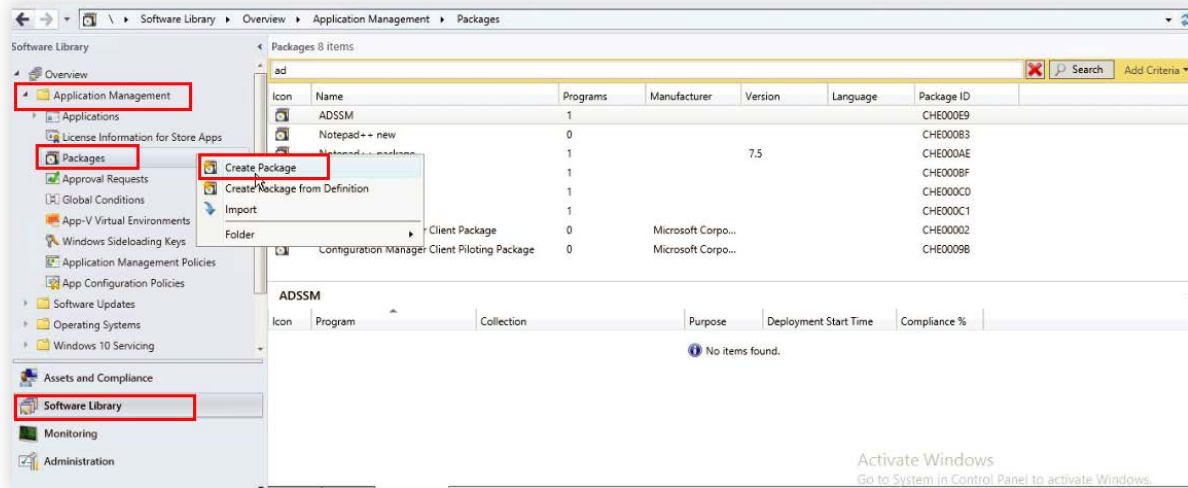
Step 1: Create a network share

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.

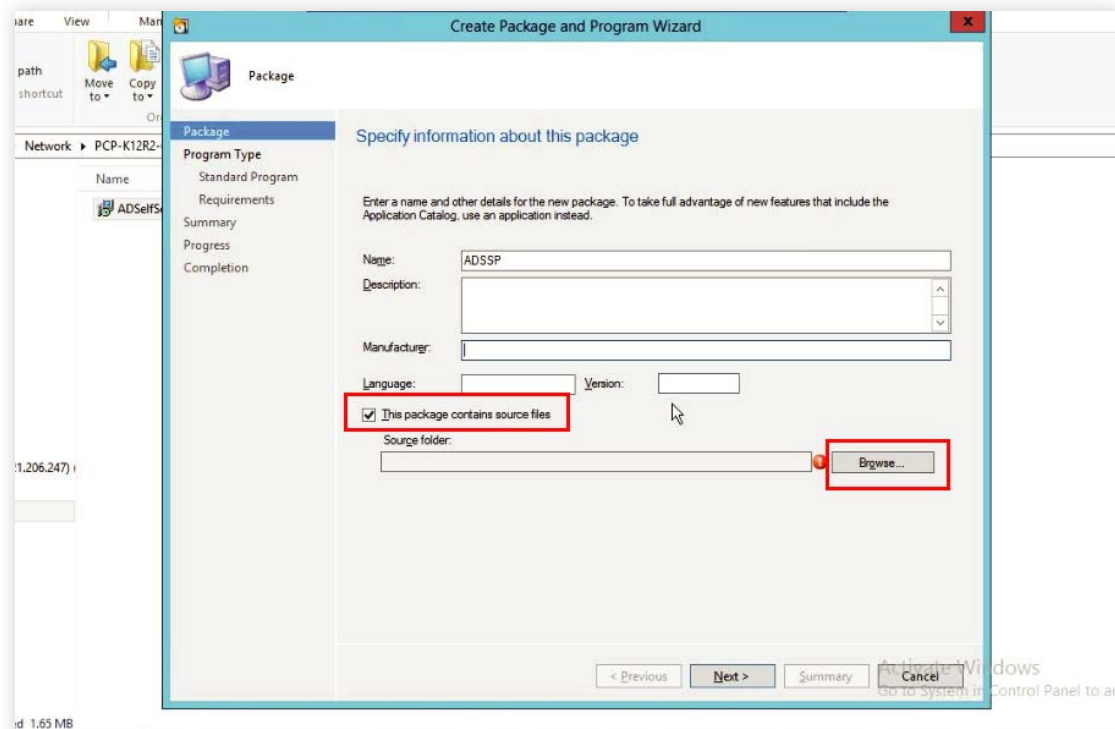
Note: Make sure that the SCCM administrator has read access to the network share in which the *ADSelfServicePlusClientSoftware.msi* file is located.

Step 2: Create an MSI package

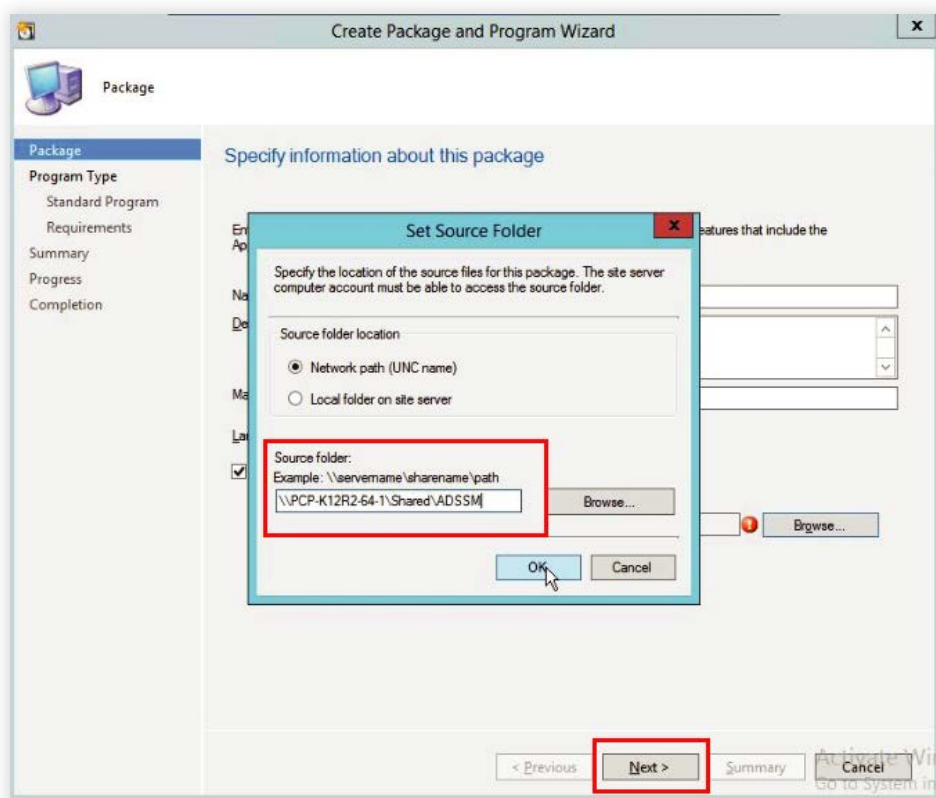
1. Go to the **System Center Configuration Manager** console.
2. Navigate to **Software Library > Application Management** drop-down
> **Packages > Create Package**.



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.

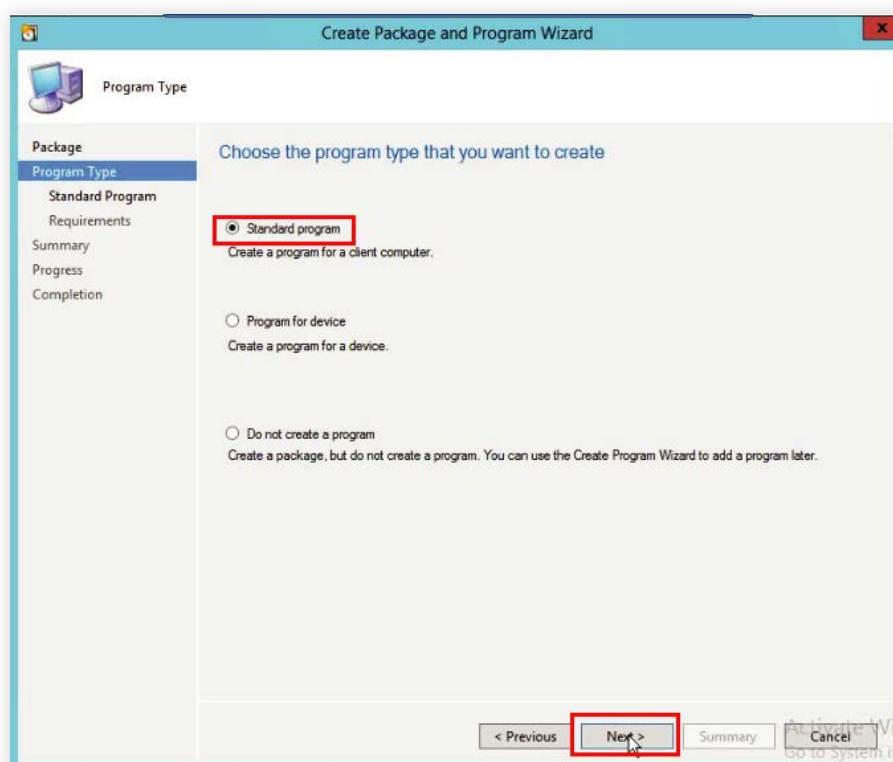


6. Enter the location of the Source folder (i.e. the network share which contains the required *ADSelfServicePlusClientSoftware.msi* file).



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 reset 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 wizard.
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.

RESTRICTBADCERT	RestrictBadCert	TRUE	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.	
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 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.	
WINDOWSLOGONTFA	WindowsLogonTFA	FALSE	Determines whether MFA for Machine Login has been enabled or not.	
MACHINEMFAUSAGESCENARIO*	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 where 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 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.

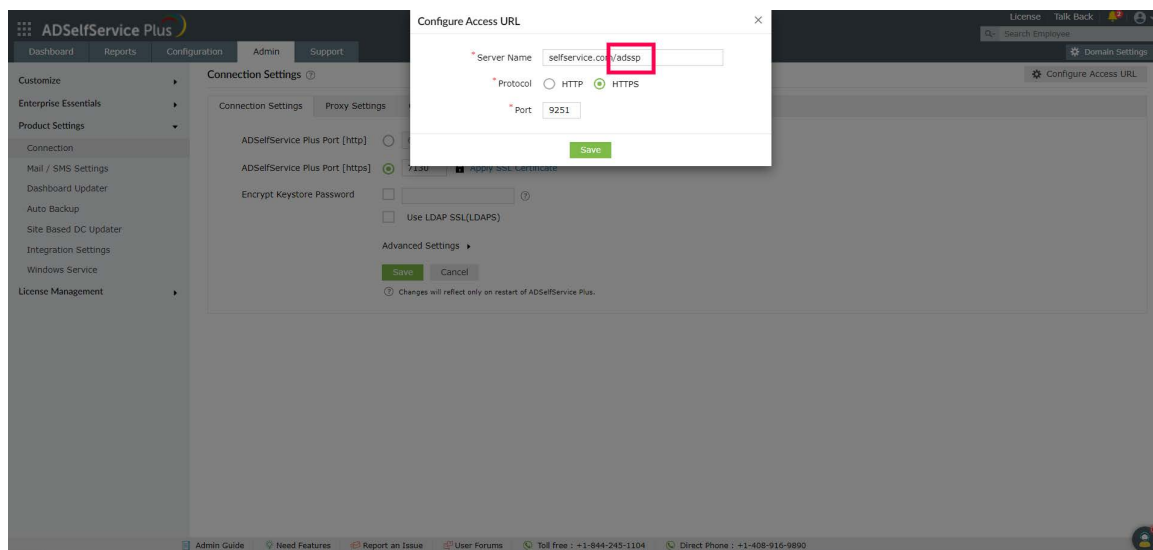
PARAMETER NAME	MATCHING REGISTRY VALUE	DEFAULT PARAMETER VALUE	DESCRIPTION
ISMACHINEMFAENFORCED*	isMFAEnforced	FALSE	If set to true, MFA will be enforced for all users accessing the machines irrespective of their enrollment status, self-service policy membership, or ADSelfService Plus connectivity status.
IS_VPN_ENABLED	IsVpnEnabled	None	Specifies whether the cached credentials update feature is enabled or not.
IS_TP_VPN_ENABLED	ISTPVPNEabled	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.

VPN_TYPE	VpnType	None	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.	
			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\FortiSSLVPN client.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.	
WRAPPINGPROVIDER	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 <i>reset_icon.bmp</i> .	
CUSTOMTITLEICONPATH	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 <i>ADSSPDesktop.ico</i> .	

The following 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	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 <i>jpg</i> , <i>jpeg</i> , <i>bmp</i> , <i>png</i> , and <i>gif</i> .	
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 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.



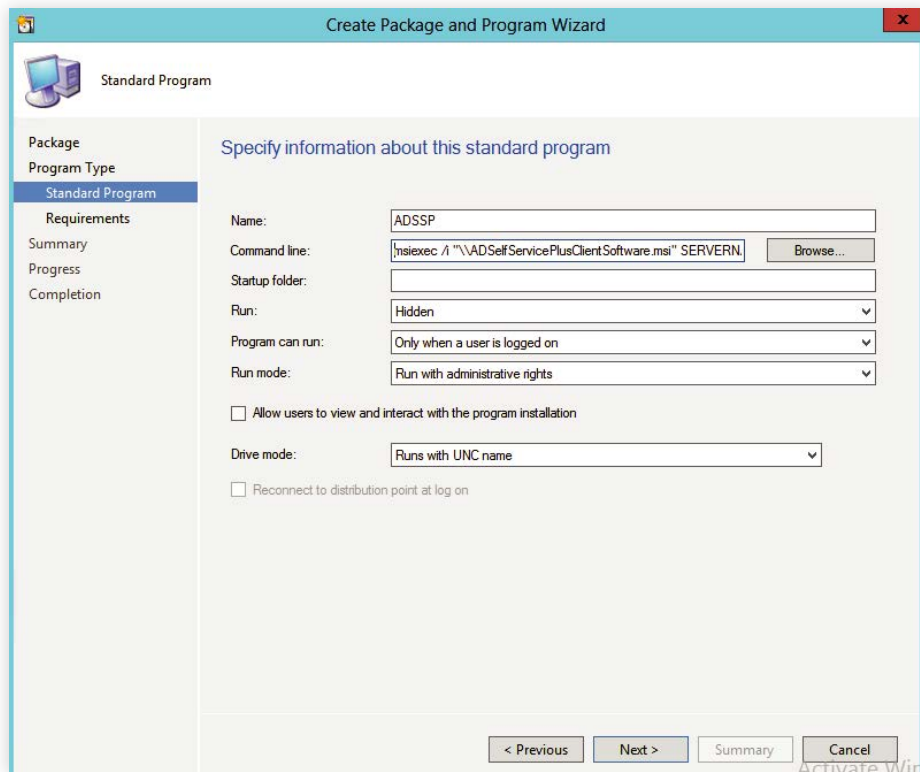
The context path can be found at the end of the ADSelfService Plus Access URL. In this example, it is /adssp. If this parameter is used in the installation command, it will look like this example:

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

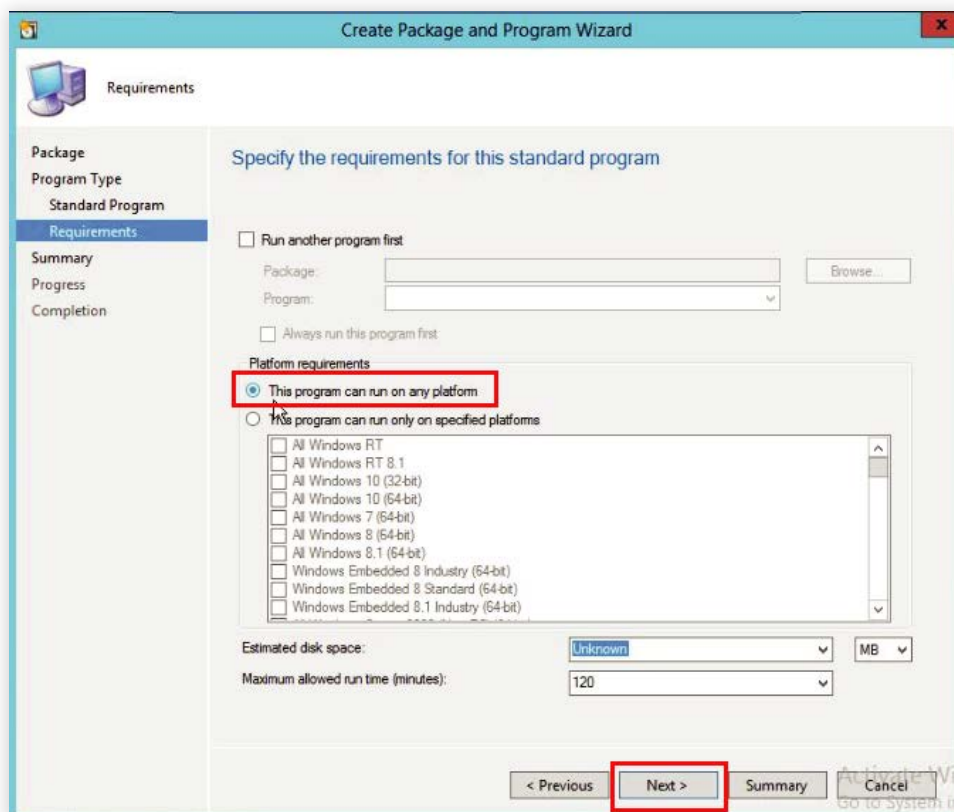
This functionality is available only for Windows clients.

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.

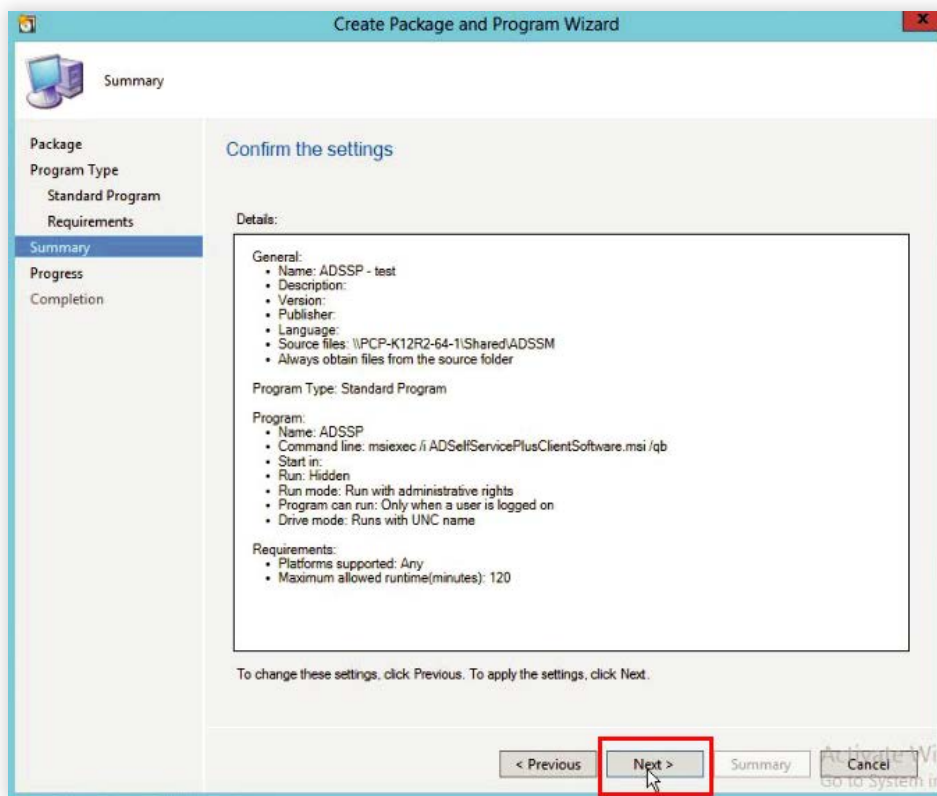
11. Select **Hidden** from the *Run* drop-down.
12. Select **Only when a user is logged on** option from the *Program can run* drop-down.
13. Select **Run with administrative rights** option from the *Run mode* drop-down.
Click **Next**.



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



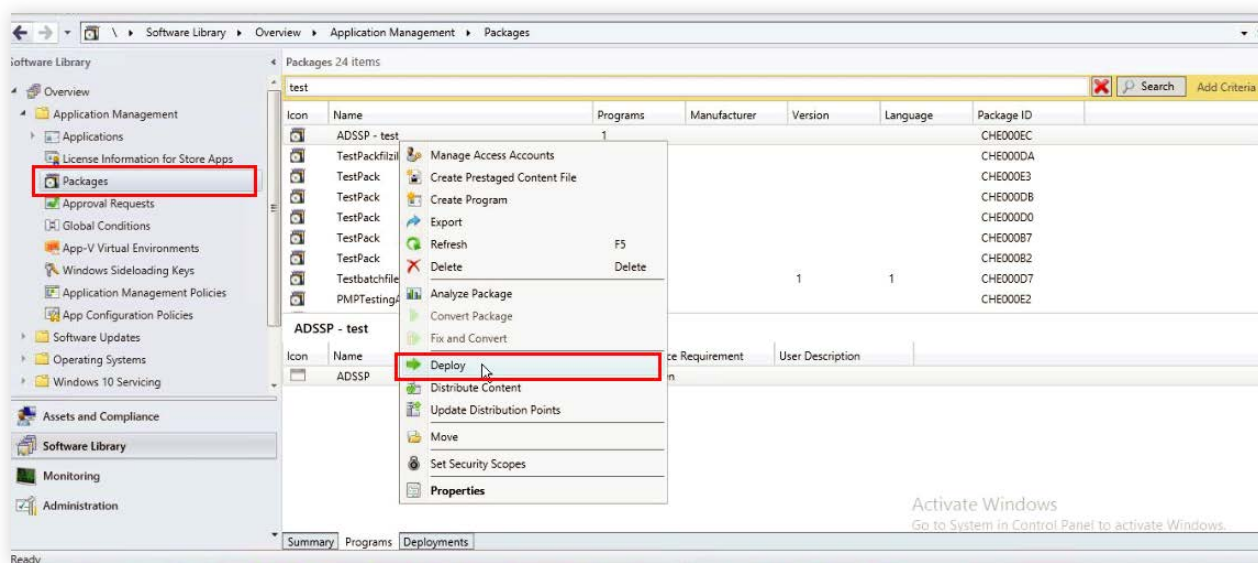
15. In the *Summary* tab, confirm the selected settings by clicking **Next**.



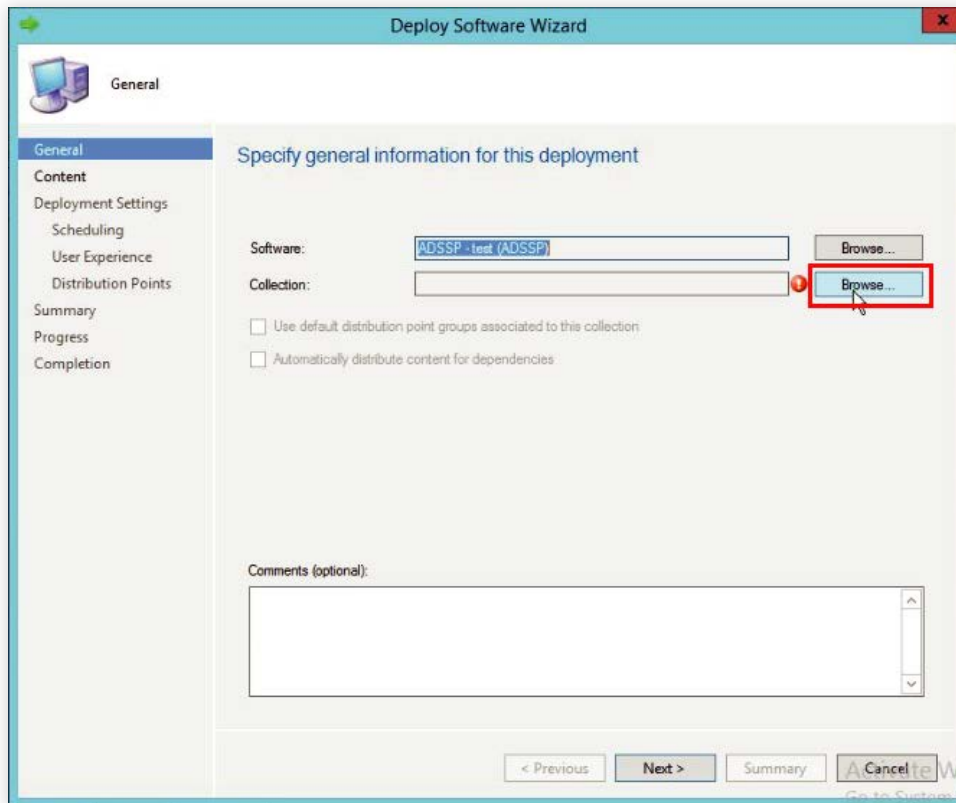
16. Click **Close** to finish.

Step 3: Deploy an MSI package

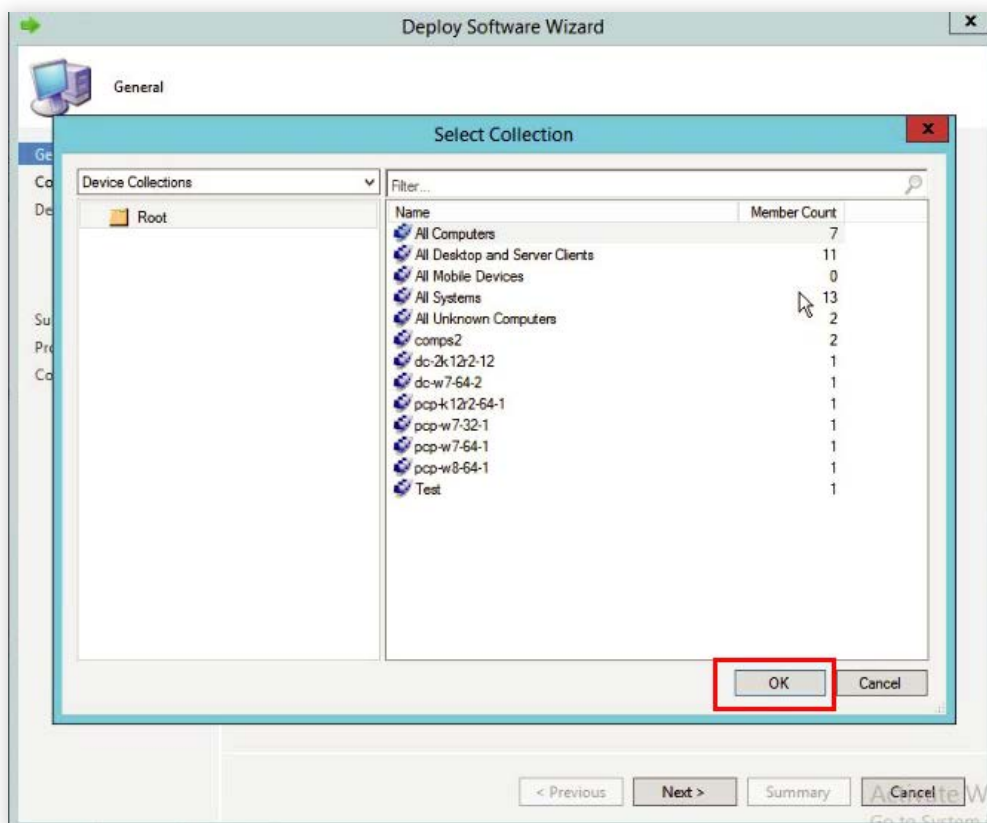
1. Select the **package** you have created in the *Packages* tab, then click **Deploy**.



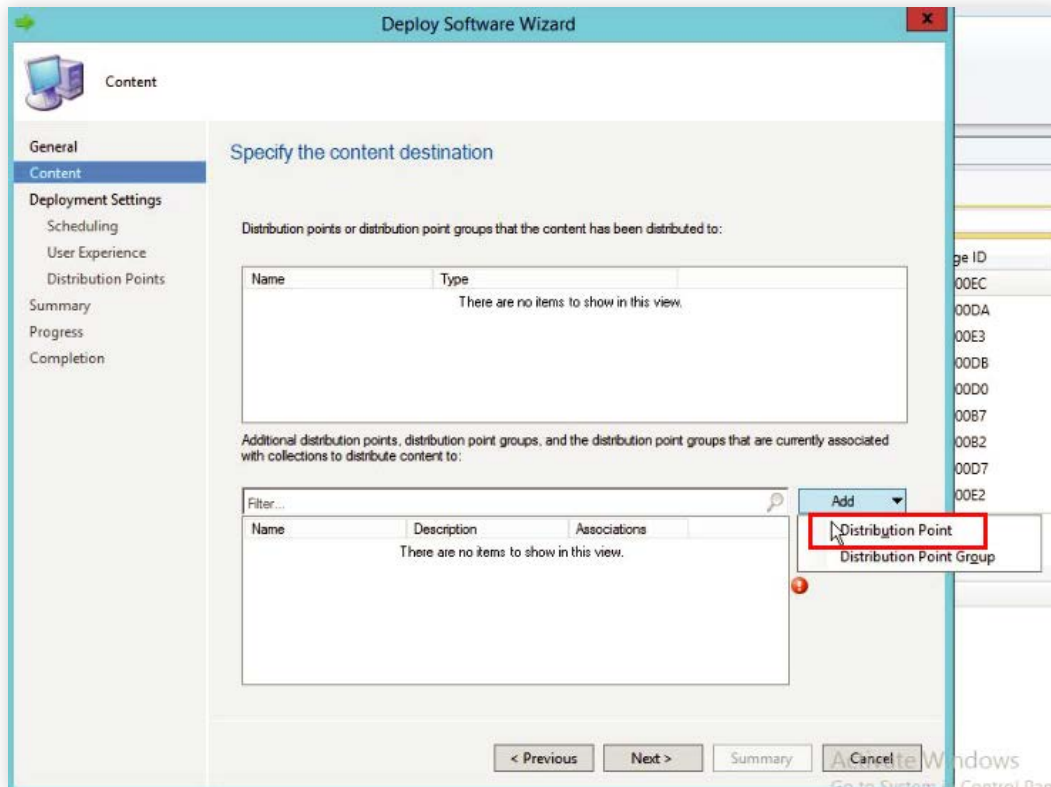
2. In the *Deploy Software Wizard*, click **Browse** next to the *Collection* field.



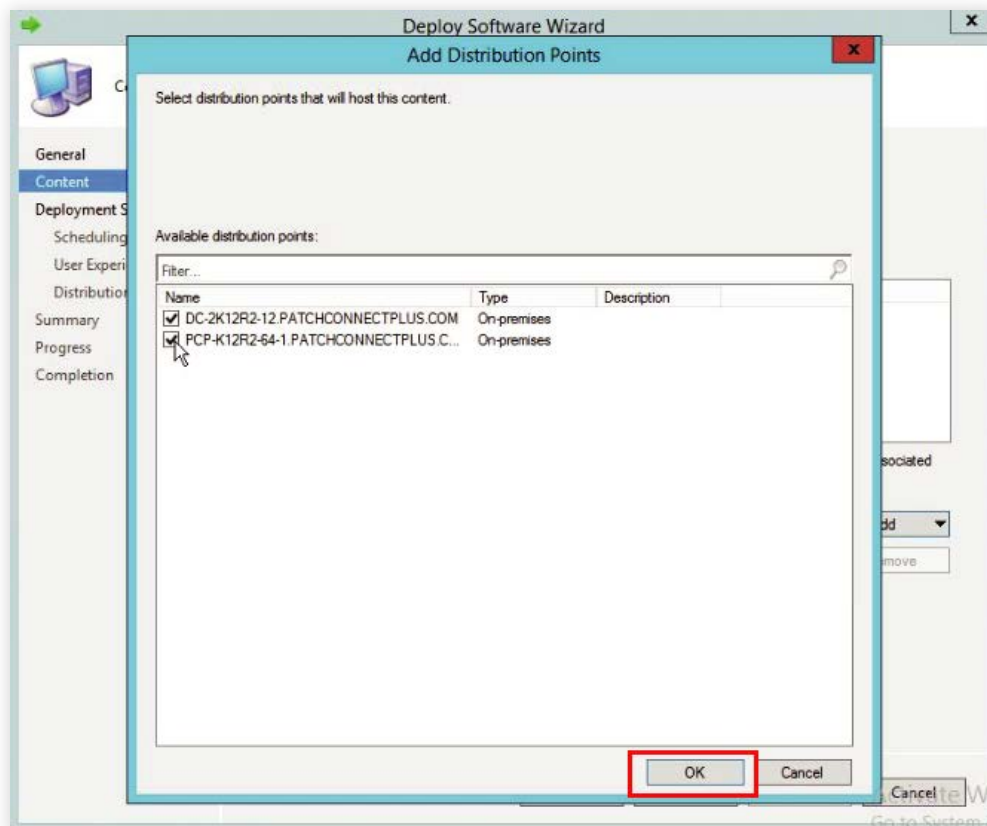
3. In the *Select Collection* window, select the machines in which the client software should be deployed, click **OK**, then click **Next**.



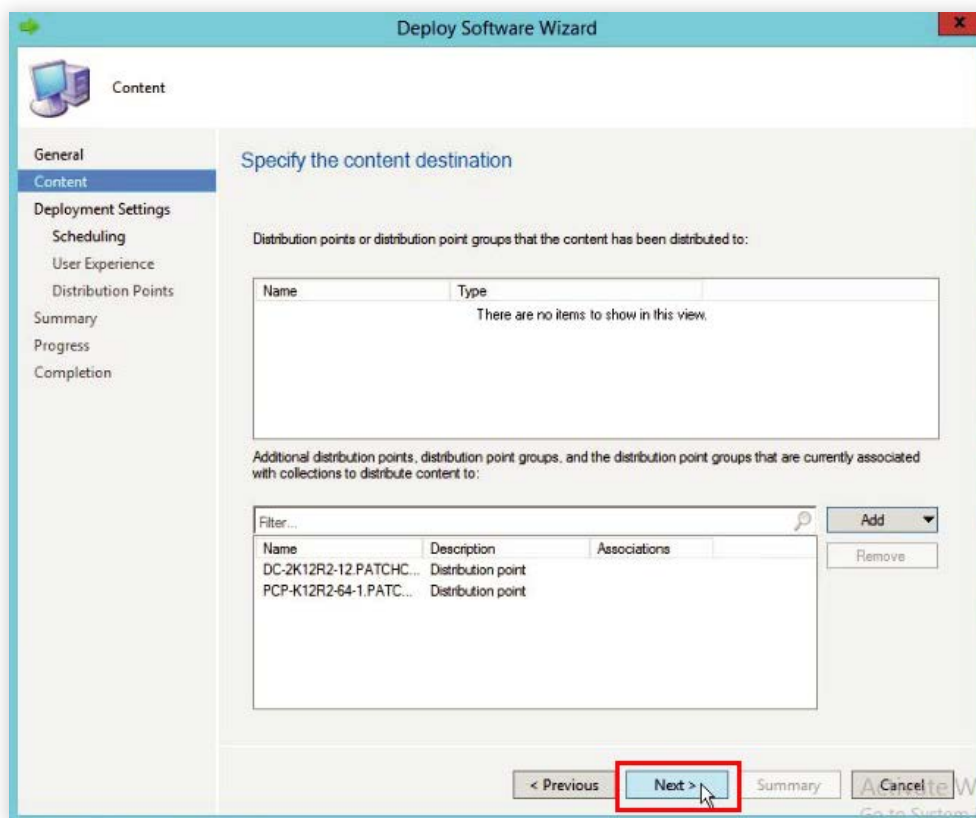
4. In the *Content* tab, select **Distribution Point** from the *Add* drop-down.



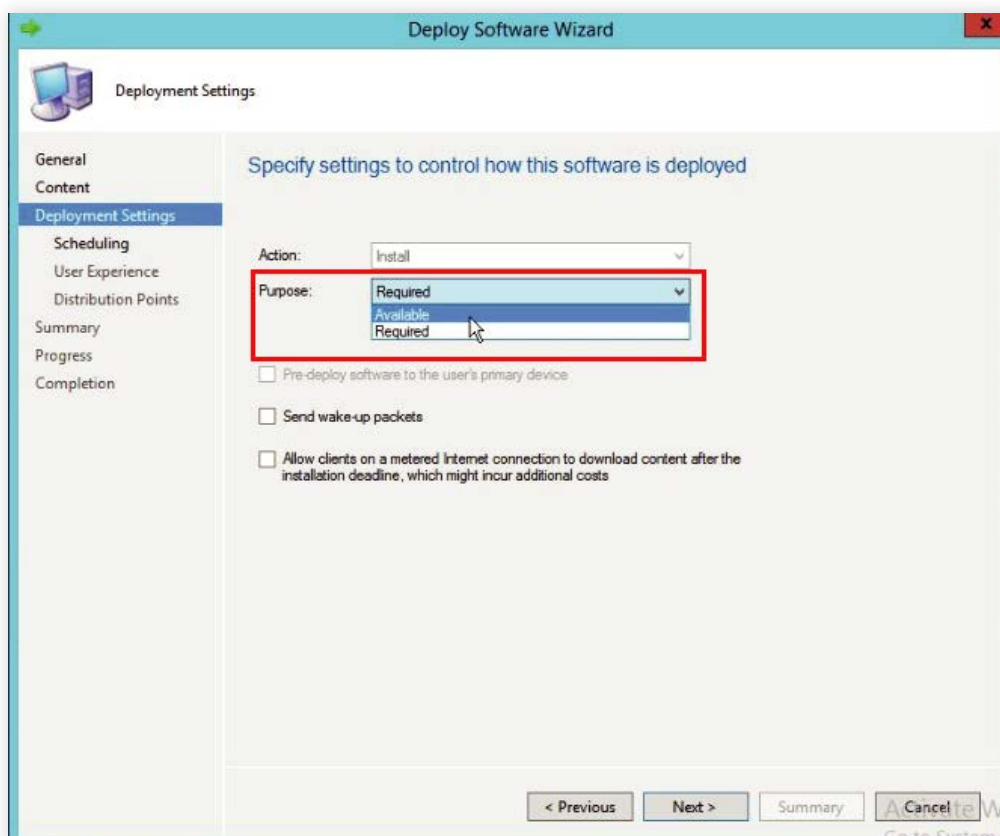
5. Select the required **Distribution Points** from the list provided, then click **OK**.



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**.



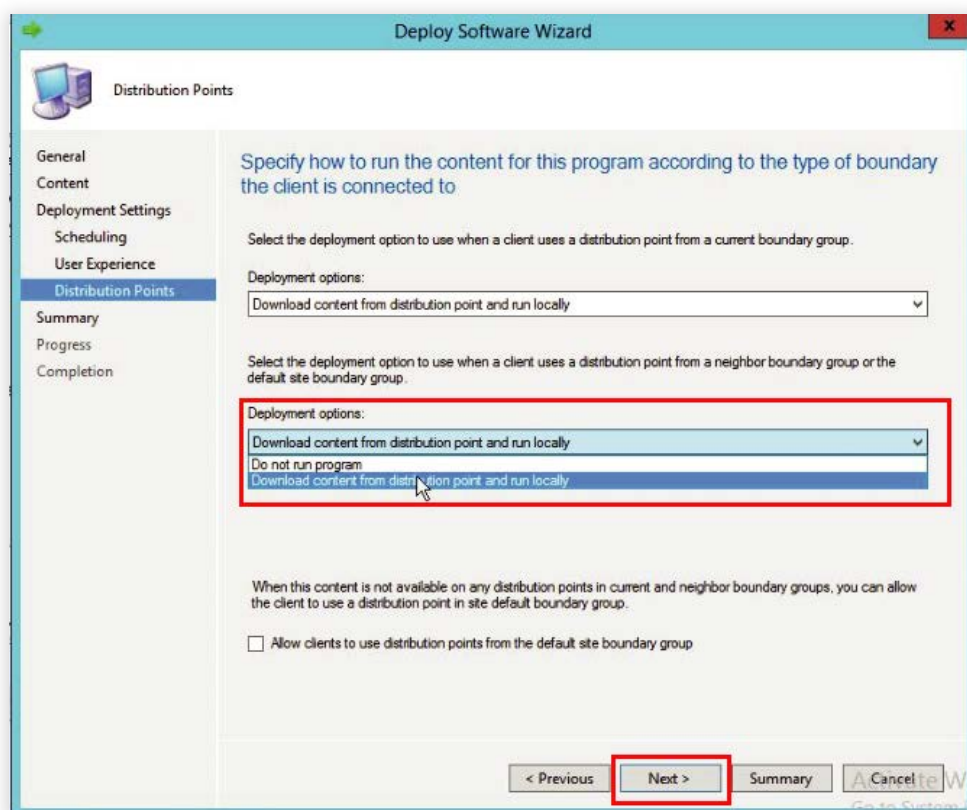
8. In the *Scheduling* tab, specify the schedule for the deployment. Click **Next**.

The screenshot shows the 'Deploy Software Wizard' window with the 'Scheduling' tab selected in the left-hand navigation pane. The main area is titled 'Specify the schedule for this deployment'. It contains a text box explaining that the program will be available as soon as it has been distributed to the content servers unless it is scheduled for a later time. Below this, there are two checkboxes: 'Schedule when this deployment will become available:' and 'Schedule when this deployment will expire:'. Each checkbox is followed by a date and time selector (8/21/2018 3:40 PM) and a 'UTC' checkbox. Below these, there is an 'Assignment schedule:' section with 'New...', 'Edit...', and 'Delete' buttons. A large empty box below this section contains the text 'There are no items to show in this view.' At the bottom, there is a 'Rerun behavior:' dropdown menu set to 'Always rerun program'. The bottom navigation bar includes '< Previous', 'Next >' (highlighted with a red box), 'Summary', and 'Cancel' buttons.

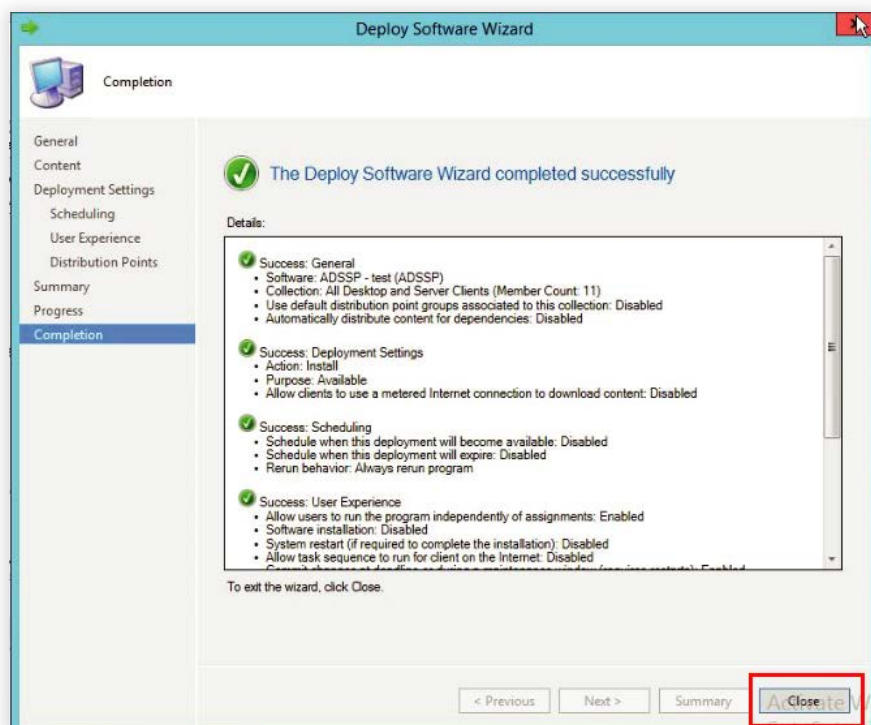
9. Make the necessary changes in the *User Experience* tab. Click **Next**.

The screenshot shows the 'Deploy Software Wizard' window with the 'User Experience' tab selected in the left-hand navigation pane. The main area is titled 'Specify the user experience for the installation of this software on the selected devices'. It contains a 'Notification settings:' section with a checked checkbox 'Allow users to run the program independently of assignments'. Below this, there is a text box stating 'When the scheduled assignment time is reached, allow the following activities to be performed outside the maintenance window:'. This is followed by two unchecked checkboxes: 'Software installation' and 'System restart (if required to complete the installation)'. Below these, there is a 'Write filter handling for Windows Embedded devices' section with a checked checkbox 'Commit changes at deadline or during a maintenance window (requires restarts)'. A note below this checkbox states 'If this option is not selected, content will be applied on the overlay and committed later.' The bottom navigation bar includes '< Previous', 'Next >' (highlighted with a red box), 'Summary', and 'Cancel' buttons.

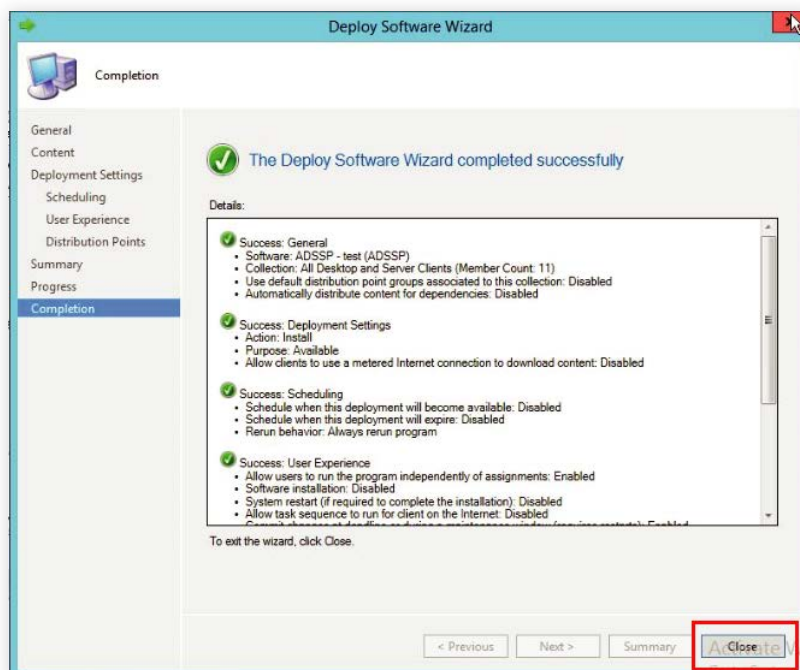
10. In the *Distribution Points* tab, choose **Download content from distribution point** as a deployment option. Click **Next**.



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



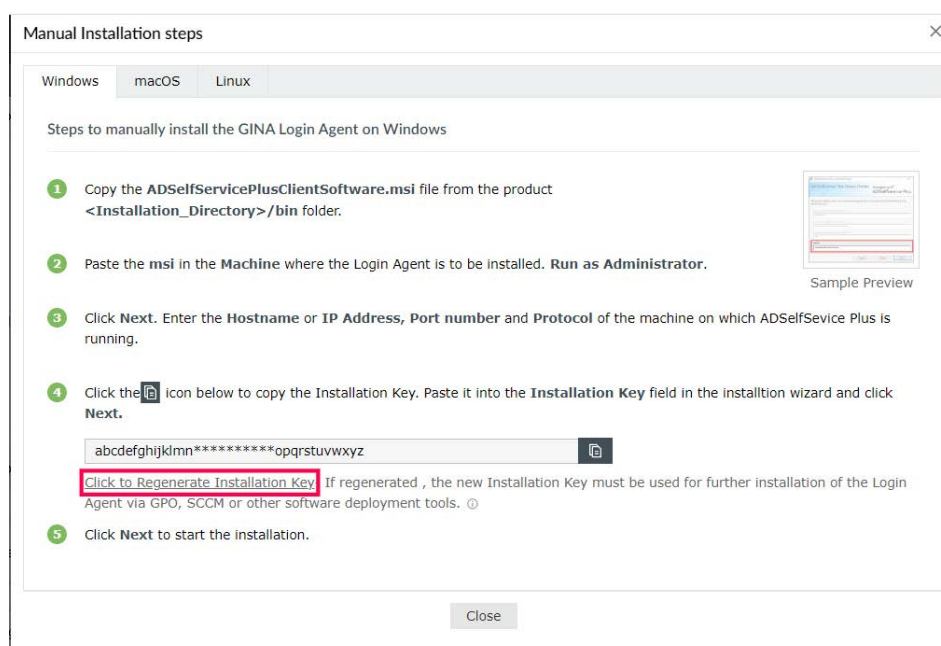
11. Confirm the settings chosen and click **Close**.



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

Our Products

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

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**