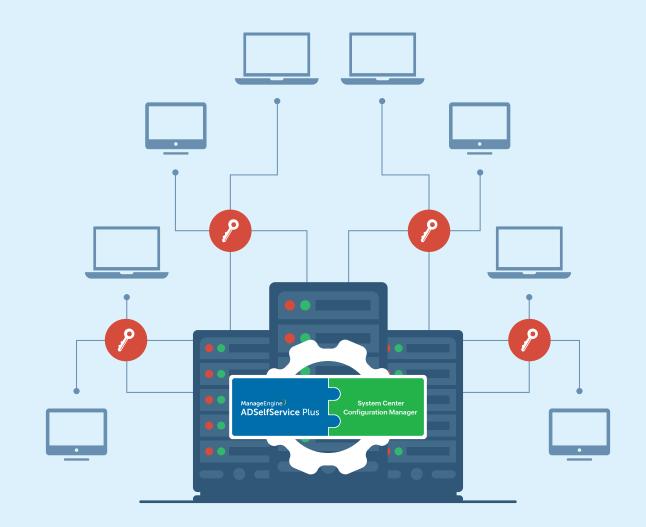
ManageEngine) ADSelfService Plus

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

- 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.

oftware Library	< Packag	es 8 items								
@ Overview	ad								Search	Add Criteria
Application Management	lcon	Name		Programs	Manufacturer	Version	Language	Package ID		
Applications	a	ADSSM		1				CHE000E9		
License Information for Store Apps	O	Notepad++ new		0				CHE000B3		
Packages	a	Netword eachana	7	1		7.5		CHEOOOAE		
Approval Requests	ate Package			1				CHEOOOBF		
Global Conditions		rom Definition		1				CHE000C0		
App-V Virtual Environments	port			1				CHE000C1		
Windows Sideloading Keys	der	•	r Client Package	0	Microsoft Corpo			CHE00002		
Application Management Policies	0	Configuration Manag	er Client Piloting Package	0	Microsoft Corpo			CHE0009B		
App Configuration Policies										
Software Updates	ADS									
Operating Systems	lcon	Program	Collection		Purpose	Deploym	nent Start Time	Compliance %		
Windows 10 Servicing	+				🕕 No ite	ms found.				
F Assets and Compliance										
🗊 Software Library										
Monitoring										
Administration							Activ	ate Windows		

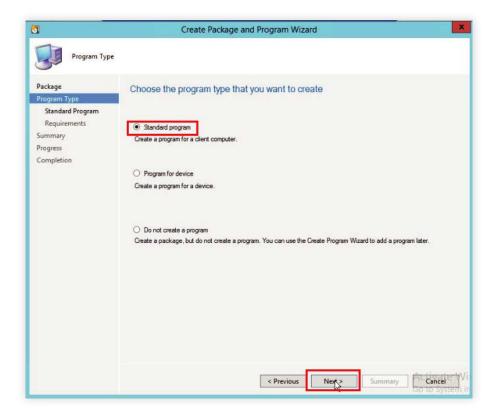
- 3. In the *Package* tab of the *Create Package* and *Program Wizard*, enter an appropriate **Name** for the package.
- 4. Provide a **Description**, the **Manufacturer** name, **Language**, and **Version** based on the requirements.
- 5. Click **Browse** next to the *Source folder* field.

are View Mar	1	Create Package and Program Wizard
bath thortcut to to to	Package	
or Network ، PCP-K12R2- Name الطاعة ADSelfS	Package Program Type Standard Program	Specify information about this package Enter a name and other details for the new package. To take full advantage of new features that include the Application Catalog, use an application instead. Name: ADSSP Description:
206.247)		Language: Version: Source files
1.65 MB		<u>Revious</u> <u>Next ></u> <u>Summary</u> <u>At Local of Vi</u> dows <u>So to System in</u> Control Pan

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

	Create Package and Program Wizard	X
Package Package Program Type Standard Program Requirements Summary Progress Completion	Specify information about this package Fin Set Source Folder No Specify the location of the source files for this package. The site server computer account must be able to access the source folder. Source folder location Na Local folder on site server Lat Source folder.	
	Source tolder: Example: \\servemame \sharename \path \\PCP-K12R2-64-1\Shared\ADSSM Browse OK Cancel	
		Cancel

- 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	РреРорUр	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 self-signed, or invalid during self -service ac restricted or not. Note: We strongly adv the login agent to wo SSL certificate is inval production environm severely impact security this only for testing put	SSL certificates tions and MFA is vise against setting rk even when the lid in your ent, as it will rity. Please disable
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 t Password/Account Ur displayed as a creden screen or not.	nlock button is
WINDOWSLO- GONTFA	WindowsLogonTFA	FALSE	Determines whether N Login has been enable	
MACHINEMFAU- SAGESCENARIO*	MFAUsage ScenarioMask	5	Determines whether t Machine Logins featu for specific scenarios value provided. Learn	re will be enabled or not based on the
			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
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	lsVpnEnabled	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.

VPN_TYPE	VpnType	rpe None	Defines the VPN connection cached credentials update provider used. This pre-set is used to denote the VPN p	based on the number key
			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 loc (Example: C:\Program File Fortinet\FortiClient\ FortiS client.exe)	s (x86)\
VPN_CONNECT_ CMD	VpnConnectCmd	None	VPN provider-specific com used to connect to the VPN credentials update.	
VPN_ DISCONNECT _ CMD	VpnDisconnectCmd	None	VPN provider-specific com used to disconnect from th cache credentials update.	
WRAPPINGPRO- VIDER	WrappingProvider	None	GUID of your third-party GII extension.	NA/CP
IMAGEPATH	GPO script paramete	r	Enter the file path of the BM used as the client software The filename should be <i>res</i> e	icon.
CUSTOMTITL- EICONPATH	GPO script paramete	۶r	Specifies the network share the icon file used as client s favicon. Ensure that the cus is uploaded at C:\\Window System32\\ADSSPDesktop filename should be ADSSPL	oftware stom title icon s\\ o.ico. The

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 langu some parts of the login age	•
			LANGUAGE	KEY
			Simplified Chinese	zh-cn
			Japanese	ја
			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 custom logo to be disp offline MFA. The filename r format customLogo.png. T formats are <i>jpg, jpeg, bmp,</i>	layed during nust be in the he supported
Logoimagepath	GPO script parameter	NONE	Mentions the network share custom logo used during o (this will be copied to C:\\V System32\\ folder location,	ffline MFA /indows\\

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.

III ADSelfService Plu		Configure Access URL	X License - Talk Back 🐙 😁 -
Dashboard Reports	Configuration Admin Support:	Server Name selfservice.com/adssp	Q- Search Employee
Customize	, Connection Settings @	*Protocol O HTTP O HTTPS	🏶 Configure Access URL
Enterprise Essentials Product Settings Connection Mail / SMS Settings Dashboard Updater Auto Backup		Save	
Site Based DC Updater Integration Settings Windows Service License Management		Advanced Settings > Suive Cancel © Changes will reflect only on researt of ADSet/Service Plus.	
	📄 Admin Guide 🔗 Need Features 🔗 Repo	t an Issue 🖉 User Forums 💿 Toll free : +1-844-245-1104 💿 Direct Phone :	+1-408-916-9890

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**.

Standard Prog Package Program Type Standard Program		on about this standard program	
Requirements Summary Progress	Name: Command line: Startup folder:	ADSSP Insiexec // "\\ADSelfServicePlusClientSoftware.msi" SERVERN	Browse
Completion	Run: Program can run: Run mode:	Hidden Only when a user is logged on Run with administrative rights and interact with the program installation	v v v
	Drive mode:	Runs with UNC name	v

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

Requirements			
ackage rogram Type Standard Program	Specify the requirements for this	standard program	
Requirements	Run another program first		
ummary	Package:		Browse
rogress ompletion	Program:		~
ompreadu	Always run this program first		
	Platform requirements		
	This program can run on any platform		
	O 10 program can run only on specified pla	tforms	
	Al Windows RT Al Windows RT 8.1 Al Windows T0 (32-bit) Al Windows 10 (64-bit) Al Windows 7 (64-bit) Al Windows 8 (64-bit) Al Windows 8 (64-bit) Windows Embedded 8 Industry (64-bit) Windows Embedded 8 Standard (64-bit) Windows Embedded 8 Standard (64-bit) Windows Embedded 8 Standard (64-bit)	it)	<
	Estimated disk space:	Unknown	✓ MB ✓
	Maximum allowed run time (minutes):	120	~

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

3	Create Package and Program Wizard
Summary	
Package Program Type Standard Program Requirements	Confirm the settings
Summary Progress Completion	General: • Name: ADSSP - test • Description: • Varian: • Publisher: • Language: • Source files: IVPCP-K12R2-64-1/Shared/ADSSM • Always obtain files from the source folder Program Program: • Name: ADSSP • Name: ADSSP • Name: ADSSP • Command line: misexec /i ADSelfServicePlusClientSoftware.msi /qb • Start in: • Run: Hidden • Run mode: Run with administrative rights • Program can run: Only when a user is logged on • Drive mode: Runs with UNC name Requirements: • Platforms supported: Any • Maximum allowed runtime(minutes): 120 To change these settings, click Previous. To apply the settings, click Next.
	< Previous Next > Summary Go to System in

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**.

oftware Library	< Packag	es 24 items									
Overview	test								×	₽ Search	Add Criteria -
 Application Management 	Icon	Name		Programs	Manufacturer	Version	Language	Package ID			
Applications	O	ADSSP - tes	ų	1	-			CHE000EC			
License Information for Store Apps	0	TestPackfilzi	1 🦢 Manage Access Accounts					CHEOOODA			
Packages	0	TestPack	😭 Create Prestaged Content File					CHE000E3			
Approval Requests	0	TestPack	🚼 Create Program					CHEOOODB			
(F) Global Conditions		TestPack	A Export					CHE000D0			
App-V Virtual Environments	O	TestPack	G Refresh	F5				CHE000B7			
Windows Sideloading Keys	a	TestPack	X Delete	Delete				CHE000B2			
Application Management Policies	a	Testbatchfile	Commission of the second second		-	1	1	CHE000D7			
App Configuration Policies	ā	PMPTesting	Convert Package					CHE000E2			
Software Updates	ADS	SP - test	Fix and Convert								
Operating Systems	lcon	Name	🚸 Deploy 📐		ce Requirement	User Description	n				
🕴 🚰 Windows 10 Servicing	. =	ADSSP	Distribute Content		n						
Assets and Compliance			Update Distribution Points								
Software Library			🔒 Move		_						
Monitoring			Set Security Scopes								
			Properties				1.11	11 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1			
Administration			1					ate Windows System in Control I			

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

•	Deploy Software Wizard	*
General		
General Content Deployment Settings	Specify general information for this deployment	
Scheduling User Experience Distribution Points Summary Progress Completion	Software: ADSSP .teet (ADSSP) Collection: Use default distribution point groups associated to this collection Automatically distribute content for dependencies	
	Comments (optional):	1.

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

	Select Collection	
Device Collections	✓ Filter	P
Root	Name All Computers All Desktop and Server Clients All Mobile Devices All Systems Comps2 Comps2 Code 2k12/2-12 Code 2k1	Member Count 7 11 0 13 2 2 1 1 1 1 1 1 1 1 1 1 1 1
		OK Cancel

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

		Deploy Software Wizard			
Content					
General Content	Specify the c	ontent destination			
Deployment Settings Scheduling User Experience	Distribution points	or distribution point groups that the content has bee	n distributed to:		
Distribution Points	Name	Туре			ge ID 00EC
Summary		There are no items to show in t	his view.		OODA
Progress					OOE3
Completion					OODB
					00000
					0087
	Additional distribu	tion points, distribution point groups, and the distribut	ion point groups that are curre	ntly associated	0082
	with collections to	distribute content to:			00D7
	Filter	distribute content to:	P	Add 🔫	00D7 00E2
		distribute content to: Description Association		Add 💌	00E2
	Filter		ns		00E2 pint
	Filter	Description Association		Distribution Po	00E2 pint
	Filter	Description Association There are no items to show in this view.	ns	Distribution Po	00E2 pint pint Group

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

2		Software Wiz stribution Poi		×	
Caneral ntent ployment S Scheduling	Select distribution points that will host this content. Available distribution points:				
User Experi	Fiter			P	
Distribution mmary ogress mpletion	Name ■ DC-2K12R2-12 PATCHCONNECTPLUS.COM ■ PCP-K12R2-64-1.PATCHCONNECTPLUS.C	Type On-premises On-premises	Description		
					sociated
					dd 🔹
					move
					move

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

	Deploy Software Wizard	
Content		
General Content	Specify the content destination	
Deployment Settings Scheduling User Experience	Distribution points or distribution point groups that the content has been distributed to:	
Distribution Points	Name Type	
Summary	There are no items to show in this view.	
rogress		
	Additional distribution points, distribution point groups, and the distribution point groups that are currently assoc with collections to distribute content to:	ated
	Filter P Add	•
	Name Description Associations Remo	/6
	DC-2K12R2-12.PATCHC Distribution point PCP-K12R2-64-1.PATC Distribution point	

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

•		Deploy Software Wizard
Deployment Se	ettings	
General Content Deployment Settings	Specify se	ettings to control how this software is deployed
Scheduling User Experience	Action:	Install
Distribution Points	Purpose;	Required V Available
Summary Progress		Required 12
Completion	Allow clier	ke-up packets nts on a metered internet connection to download content after the n deadline, which might incur additional costs
		< Previous Next > Summary A Cancel to M

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

•	Deploy Software Wizard
Scheduling	
General Content Deployment Settings	Specify the schedule for this deployment
Scheduling User Experience Distribution Points	This program will be available as soon as it has been distributed to the content servers unless it is scheduled for a later time below. For required applications, specify the assignment schedule.
Summary	Schedule when this deployment will become available:
Progress	8/21/2018 🗐 - 3:40 PM 🔄 🗌 UTC
Completion	Schedule when this deployment will expire :
	8/21/2018 回一 3:40 PM
	Assignment schedule: New Edt Delete
	Rerun behavior: Aways rerun program v

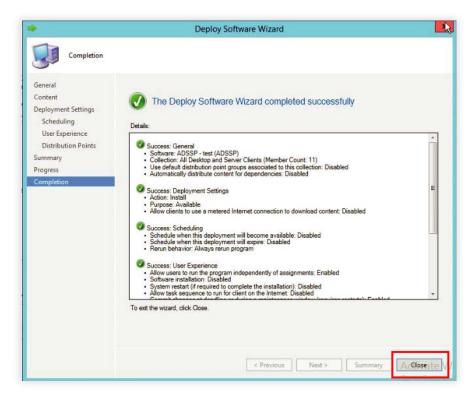
9. Make the necessary changes in the User Experience tab. Click **Next**.

	Deploy Software Wizard
User Experience	
General Content Deployment Settings	Specify the user experience for the installation of this software on the selected devices
Scheduling	Notification settings:
User Experience Distribution Points Summary	Allow users to run the program independently of assignments
Progress Completion	When the scheduled assignment time is reached, allow the following activities to be performed outside the maintenance window: Software installation System restart (if required to complete the installation) Write filter handling for Windows Embedded devices Commit changes at deadline or during a maintenance window (requires restarts) If this option is not selected, content will be applied on the overlay and committed later.
	< Previous Nitz > Summary A Cancel te

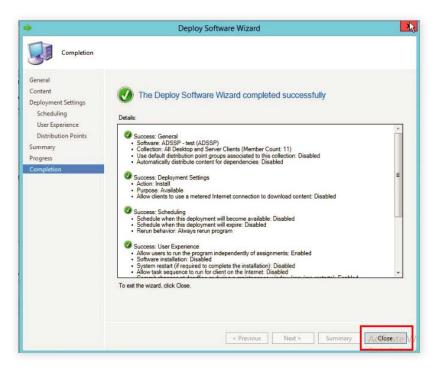
10. In the *Distribution Points* tab, choose **Download content from distribution point** as a deployment option. Click **Next**.

Distribution P	unte
Se Distribution P	
General Content Deployment Settings	Specify how to run the content for this program according to the type of boundary the client is connected to
Scheduling User Experience	Select the deployment option to use when a client uses a distribution point from a current boundary group. Deployment options:
Distribution Points Summary	Download content from distribution point and run locally
Progress Completion	Select the deployment option to use when a client uses a distribution point from a neighbor boundary group or the default site boundary group.
	Deployment options:
	Download content from distribution point and run locally
	Do not run program Download content from distriction point and run locally
	When this content is not available on any distribution points in current and neighbor boundary groups, you can allow the client to use a distribution point in site default boundary group.
	< Previous Next > Summary A.Cancelto

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.

anual	Insta	llation step			
Winde	ows	macOS	Linux		
Step	is to m	anually insta	the GINA Login Agent on Windows		
0	0000		ervicePlusClientSoftware.msi file rectory>/bin folder.	rom the product	Production to the lines
2	Paste the msi in the Machine where the Login Agent is to be installed. Run as Administrator.				Sample Preview
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 installation wizard and click Next.				
	abcdefghijklmn******opqrstuvwxyz				
	_	-	<u>Installation Key</u> If regenerated , th CM or other software deployment too	e new Installation Key must be used for further installars. \odot	ation of the Login
5	Click	Next to star	the installation.		
				Close	

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.

O Support