ManageEngine ADSelfService Plus

ADSelfService Plus **Evaluator's guide**

www.adselfserviceplus.com

Table of Contents

Document overview	2
ADSelfService Plus overview	2
Features and benefits	2
Self-service password reset and account unlock	2
Enterprise single sign-on	
Password synchronization	
Multi-factor authentication	
Password expiration notification	
Password policy enforcer	
Conditional access	4
Self-service directory update	4
Employee directory search and organization chart	4
Mail group subscription	4
ADSelfService Plus architecture	4
Roll out ADSelfService Plus	5
1. Password self-service deployment	5
2. Password and endpoint security	
3. One-identity configuration	
4. Directory self-service deployment	
5. Supplementary features	
Configure security settings in ADSelfService Plus	
1. Implement failover and secure gateway features:	
2. Configure SSL and LDAPS	
3. Allow or restrict admin portal access based on IP addresses	
4. Set the session expiration time	
5. Manage product licenses	
6. Configure CAPTCHA:	
Other important settings	
1. Configure the dashboard updater	
2. Configure email and SMS servers for notifications	
3. Enable auto-backup of the database	
4. Configure technicians for product administration	
5. Rebrand and personalize the portal	

Document overview

This document will provide IT admins evaluating ManageEngine ADSelfService Plus a glimpse into the product's architecture, its major features, security settings, and other important settings that will help them get started with the evaluation.

ADSelfService Plus overview

ManageEngine ADSelfService Plus is an integrated self-service password management and single sign-on (SSO) solution for on-premises and cloud applications. It offers self-service password reset and account unlock, endpoint and VPN multi-factor authentication (MFA), SSO to enterprise applications, Active Directory (AD)-based multi-platform password synchronization, password expiration notification, and password policy enforcer. It also provides Android and iOS mobile apps that facilitate self-service for end users anywhere, at any time. ADSelfService Plus helps reduce IT expenses associated with help desk calls, improves the security of user accounts, and spares end users frustration due to computer downtime.

Features and benefits

• Self-service password reset and account unlock

Enables users to reset their forgotten AD domain passwords and unlock their locked out accounts without admin intervention. Users can reset their password from:

- A web browser using the ADSelfService Plus user portal.
- The logon screens of Windows, macOS, and Linux machines using the ADSelfService Plus login agent.
- A mobile device using the ADSelfService Plus mobile app or mobile browser portal.

Benefit: Empowers users to reset their passwords and unlock their accounts to help reduce the number of help desk tickets and unburdening help desk personnel. It also improves user productivity as passwords can be reset and accounts can be unlocked swiftly.

• Enterprise single sign-on

Reduce the number of logins performed by the user by enabling enterprise SSO for Security Assertion

Markup Language (SAML) applications like Google Workspace, Microsoft 365, and Salesforce. **Benefit**: Users can use a single password to log in to and access multiple enterprise applications. This makes handling application accounts easier for them.

• Password synchronization

This feature allows users to synchronize their AD domain password across their user accounts in integrated on-premises and cloud applications like Microsoft SQL Server, ADFS, Microsoft 365, Google Workspace, and Salesforce.

Benefit: Any changes to the domain password results in the changes being reflected across the integrated applications as well.

• Multi-factor authentication

MFA improves security through additional layers of identity verification along with the existing credential-based authentication. ADSelfService Plus implements additional identity verification steps for the following:

- Self-service password reset and account unlock.
- Local and remote machine (Windows, macOS, and Linux), and VPN logins.
- SSO for enterprise applications.
- ADSelfService Plus portal logins.

The product supports up to 18 authentication techniques including biometrics, Google Authenticator, Microsoft Authenticator, time-based one-time password (TOTP), and Security Questions and Answers. **Benefit**: Even if attackers misappropriate users' credentials, they still need to complete the successive stages of authentication to gain access to the resource rendering the exposed passwords useless.

• Password expiration notification

Password expiration notifications can be sent through email and SMS, or as push notifications. The product allows sending multiple reminder notifications on specific days leading to the expiration. **Benefit:** Notify users about their impending domain password expiration and remind them to change their passwords before they lose access to their machines.

• Password policy enforcer

Advanced password policy controls can be set for an organization in addition to the native domain and fine-grand password policies offered by AD. These advanced password policies can be used to set password controls that are not available in the native policies like:

- Mandatory inclusion of Unicode characters.
- Restriction of character repetition of consecutive characters from usernames and old passwords.
- Restriction on the usage of weak passwords, dictionary words, and palindromes.

Benefit: Users can be required to adhere to these policies strictly, thereby preventing them from setting

weak passwords that may jeopardize the security of an organization.

Conditional access

Automate access decisions to organizational resources using risk factors such as IP address, time of access, the device used, and the user's geolocation.

Benefit: IT admins can set pre-defined conditions based on these risk factors that provide users with complete and unrestricted access, limited access, or no access to the resource.

• Self-service directory update

Allow users to update their AD profile information like email address and mobile number without IT admin intervention. IT admins can also create modification rules that auto-populate values for certain attributes based on other attribute values provided.

Benefit: This helps decrease the help desk workload while improving user productivity.

• Employee directory search and organization chart

Allow users to search for information on other users (users, contacts, and groups) in the organization, and view the Organization Chart that displays all the employees in the organizational hierarchy. **Benefit:** This helps users discover details about other users from a single portal.

• Mail group subscription

Provide users with the ability to subscribe themselves to organizational email groups.

Benefit: This lets users get access to the email groups they need without help desk assistance.

ADSelfService Plus architecture



Roll out ADSelfService Plus

1. Password self-service deployment

i. Configure self-service policies

Self-service policies need to be created to deploy self-service password reset, self-service account unlock, change password, and self-update. While creating a policy, the required features will be configured and specific domains, organizational units (OUs), and groups will be assigned to the policy. Only users belonging to the selected OUs and groups will have access to the features configured.

- 1. Navigate to the **Configuration** tab.
- 2. Click on the Add New Policy button on the bottom-right of the webpage.

Note: By default, when ADSelfService Plus discovers domains, it sets up one policy for every domain that it discovers. If that fits your requirements, you can retain it; otherwise, you can edit it.

ADSelfService Plus						License Talk Back 🕒 🗸
Dashboard Reports	Configuration	Admin	Support			🔅 Domain Settings
Self-Service	▼ Pol	icy Configura	ition 💿			Password Self-Service Modes 👻
Policy Configuration	a	dselfservice -	IT Admin 🧪			
Multi-factor Authentication						
Password Expiration Notification	on	Reset Pa	ssword	a naeeworde (without europying old naee	(house	
Password Policy Enforcer		Litable us	ers to sell-servic	e passwords (without supplying old pas	sswoid).	
Password Sync/Single Sign Or	1	Unlock A	ccount	air accounts using self-authentication in	fo	
Conditional Access				an accounts doing beir dachendedeon in		
Directory Self Service		Self Upd Enable us	ate ers to self-servio	e update Active Directory. Choose a Se	If Update Layout.	
Administrative Tools	•					
Security Center	•	Enable us	Password ers to change th	eir passwords (by supplying old passwo	ords).	😻 Select OUs/Groups 🛛 🖗 Advanced
					Save Policy Cancel	
	Ava	ilable Policie	5			+ Add New Policy
	a	Ē				≪ < 1-3 of 3 > ≫
	A	ctions	Advanced	Policy Name	Permissions	Domain Name
	/	a 6	ġ.	adselfservice - IT Admin	Reset Password, Unlock Account, Self Update, Change Password	SELFSERVICE
	/	a 6	ġ.	adselfservice - HR	Reset Password, Unlock Account, Self Update, Change Password	SELFSERVICE
	/	6 B	ġ.	adselfservice - Users	Reset Password, Unlock Account, Self Update, Change Password	SELFSERVICE
	Admin Guide	🌣 Need Featur	es 🛛 🥵 Report a	an Issue 🖉 User Forums 🚫 Toll fr	ree : +1-844-245-1104 🕓 Direct Phone : +1-408-916-9890	G

- 3. Enter an appropriate **Policy Name**.
- 4. From the list of self-service features provided, select features for your user base. You need to select at least one self-service feature.
- 5. Click on the **Select OU(s)/Groups** button.
- 6. Select the domain on which the policy is to be applied. Here, you have a choice; you can either apply

the policy to all users in the selected domain, or only to specific users based on their OU or group membership.

- 7. Click **OK**.
- 8. Click Save Policy.

<u>Learn how</u> the ADSelfService Plus login agent can be configured and self-service features can be enabled for users' Windows, macOS, and Linux login screens. <u>Click here</u> to learn how to deploy the ADSelfService Plus mobile app that enables end users to perform self-service features, password change, and identity verification from their mobile devices.

ii. Configure identity verification

Once domain users are made part of a self-service policy, their identities need to be verified so that they can use the self-service password reset or account unlock features via the ADSelfService Plus' end-user portal, ADSelfService Plus mobile app, and Windows, macOS, and Linux login screens. Identity verification by MFA relies on the information provided by users during enrollment with ADSelfService Plus.

- 1. Security Questions and Answers
- 2. Email Verification
- 3. SMS Verification
- 4. Google Authenticator
- 5. Microsoft Authenticator
- 6. Duo Security
- 7. RSA SecurID
- 8. RADIUS Authentication
- 9. Push Notification Authentication
- 10. Fingerprint/Face ID Authentication
- 11. QR Code-Based Authentication
- 12. TOTP Authentication
- 13. SAML Authentication
- 14. AD Security Questions
- 15. YubiKey Authentication
- 16. Zoho OneAuth TOTP Authentication
- 17. Smart Card Authentication
- 18. Custom TOTP Authenticator

By clicking on the above links you can view the configuration steps for each of these methods.

You can enable certain MFA methods for a specific set of users and can fix the number of authentications users must complete in order to verify their identity. Admins also have the option of forcing users to verify

their identities with certain MFA methods. To know more about configuring MFA, click here.

iii. Enable user enrollment

In order to perform identity verification, users need to enroll with ADSelfService Plus by providing certain information. The information provided varies based on the MFA method configured. ADSelfService Plus simplifies the enrollment process by offering multiple enrollment options:

- Enrollment without user's intervention: Administrators enter the user's enrollment information.
- Enrollment by users: Users provide the enrollment information

Enrollment without user's intervention

• Import enrollment data from CSV file:

You can import the existing security questions and answers along with the user's mobile numbers and email IDs that are stored in a CSV file format. This imported information is then used to enroll users. **Click here** for further details.

• Import enrollment data from external database:

Connect the organization's data sources like MS SQL, PostgreSQL, Oracle, and MySQL with ADSelfService Plus. Once ADSelfService Plus has been given sufficient permission to access the database server, data can be fetched and users can be automatically enrolled. <u>Learn</u> the configuration steps.

Enrollment by users:

Users can enroll with ADSelfService Plus using the ADSelfService Plus client portal, ADSelfService Plus mobile app, and the Mobile Web App. In order to enforce user enrollment, you can implement the following measures:

• Enrollment notification:

When ADSelfService Plus is deployed in an organization, the administrator could use enrollment notification to inform employees of the product and encourage them to enroll themselves with it. <u>Bookmarked here</u> are the steps for enabling the email and SMS server necessary for the notification. This option, when enabled, sends an email or push notification to all users who have not yet enrolled with ADSelfService Plus. You can also set up a scheduler to send notifications to non-enrolled users regularly. <u>Click here</u> for further details.

• Force enrollment:

Here, the non-enrolled users are searched for within the selected domain or policy, and their accounts are associated with a logon script. The logon script forces them to enroll when they log into their machines.

Automatic periodic linking of non-enrolled users' accounts with a logon script for forced enrollment can also be accomplished using a scheduler. For steps on how to enable Force Enrollment for non-enrolled users, **click here**.

iv. Make it easier for end users to access the self-service functionalities

ADSelfService Plus self-service password reset and account unlock feature can be used through methods other than the default web portal. Here are the alternate media for accessing the self-service features:

- Login screens of users' Windows, macOS, and Linux machines: Install the ADSelfServicePlus login agent in the target user machines to allow users to access self-service password reset and account unlock features. The login agent can be <u>deployed onto users' machines from the</u> <u>ADSelfService Plus admin portal</u>, installed <u>manually</u>, and installed via <u>GPO</u> or <u>Microsoft System</u> <u>Center Configuration Manager</u> (SCCM).
- **Mobile devices**: <u>Deploy</u> the ADSelfService Plus mobile app onto users' mobile devices and enable them to perform self-service password reset and account unlock actions right from their mobile device. Alternately, users can manually install the app onto their devices and configure it.

2. Password and endpoint security

i. Enforce endpoint MFA:

ADSelfService Plus' endpoint MFA feature helps secure Windows, macOS and Linux, and VPN logins using 18 authentication methods.

MFA for Windows, macOS, and Linux machines

Prerequisites

 SSL must be enabled: Log in to the ADSelfService Plus web console with IT admin credentials. Navigate to Admin > Product Settings > Connection. Select the ADSelfService Plus Port [https] option. Refer to this guide to learn how to apply for an SSL certificate and enable HTTPS.

ManageEngine ADSelfService Plus

ADSelfServ	vice Plus		License Talk Back 😝 🗸
	Reports Cor	onfiguration Admin Support	🔅 Domain Settings
Customize	•	Connection Settings ③	Configure Access URL
Enterprise Essentials	•	Connection Settings Drovy Settings General Settings	
Product Settings	•	connection octaings Traxy octaings octain octaings	
Connection		ADSelfService Plus Port [http] O 8888	
Mail / SMS Settings	5	ADSelfService Plus Port [https] 9251 Apply SSL Certificate	
Dashboard Updater	r		
Auto Backup		Encrypt Keystore Password	
Integration Settings	s	Use LDAP SSL(LDAPS)	
Windows Service		Advanced Settings	
License Management	,	Save Cancel ⑦ Changes will reflect only on restart of ADSelfService Plus.	

- Install ADSelfService Plus login agent for Windows, macOS, and Linux on the machines where you want to enable MFA. Click here for the steps to install the ADSelfService Plus login software.
- Enable the required authentication methods. For the steps on enabling the authentication methods, refer to the Authenticators section.

Steps to enforce MFA for Windows, macOS, and Linux machines:

- 1. Go to **Configuration > Self-Service > Multi-factor Authentication > MFA for Endpoints**.
- 2. Select a policy from the **Choose the Policy** drop-down. This will determine which authentication methods are enabled for which sets of users.
- 3. In the **MFA for Machine Login** section, check the **Enable the second authentication factor** box and select the authentication method from the drop-down.
- 4. Click Save Settings.

ADSelfService Plus				License Q- Search Employee	Talk Back 🛛 🐣 🕶
Dashboard Reports	Configu	ration Admin Support			🌣 Domain Settings
Self-Service	-	Multi-factor Authentication ③		 How to 	make users enroll?
Policy Configuration		Choose the Policy adselfserviceplus			
Multi-factor Authentication		Authenticators Setup MFA for Reset/Unlock	MFA for Endpoints	MFA Enrollment	Advanced
Password Expiration Notification Password Policy Enforcer Password Sync/Single Sign On Conditional Access		MFA for Machine Login Supported : Windows/macOS/Linux	Enable 1 v authentication factors. Select the authenticators required Google Authenticator v ①		
Directory Self Service Administrative Tools Security Center	• •	MFA for VPN Login Supported: VPN providers that support RADIUS authentication	Enable 1 v authentication factors, Select the authenticators required No factor selected v		
		Note • VPN MFA is applicable only when • Download ADSelfService Plus NP • View the architectural diagram ill	Windows Network Policy Server (NPS) is used as RADIUS server. S Extension and install it in the Windows servers(2008 R2 & above) where the Network policy Server(IAS) service is active. Learn more ustrating the high-level VPH multi-factor authentication flow.		
			Save Settings Cancel		

MFA for VPN

Prerequisites:

- Professional edition license of ADSelfService Plus.
- Configure your VPN server to use RADIUS authentication.
- For RADIUS authentication, you must use a Windows server (Windows Server 2008 R2 and above) with Network Policy and Access Services (NPS) role enabled.
- Enable HTTPS in ADSelfService Plus (go to Admin > Product Settings > Connection).

Note: If you are using an untrusted certificate in ADSelfService Plus to enable HTTPS, you must disable the Restrict user access when there is an invalid SSL certificate option in Configuration > Administrative Tools > GINA/Mac/Linux (Ctrl+Alt+Del) > GINA/Mac/Linux Customization > Advanced.

- In AD, set users' Network Access Permission to Control access through NPS Network Policy in their Dial-in properties.
- The Access URL you have configured in Configure Access URL (go to Admin > Product Settings > Connection > Configure Access URL) will be used by the NPS extension to communicate with the ADSelfService Plus server. Make sure you have updated the Access URL before installing the NPS extension.
- In the Windows NPS server, where the NPS extension is going to be installed, set the **Authentication** settings of the **Connection Request Policy** to **Authenticate requests on this server**.

Step 1: Enable the required authenticators

Based on whether the RADIUS client (the VPN server) supports RADIUS challenge-response or not, the authentication methods you can enable for VPN logins may vary.

By default, the following two authentication methods are supported:

- Push Notification Authentication
- Fingerprint/Face ID Authentication

Note:

- When you enable **Push Notification** or **Fingerprint/Face ID Authentication**, make sure the ADSelfService Plus server is reachable by the users (through the internet) from their mobile devices.
- RADIUS authentication timeout should be set to at least 60 seconds in the VPN server's RADIUS authentication configuration settings.

When RADIUS challenge-response is supported by the RADIUS client, the following authentication methods

can be enabled:

- ADSelfService Plus TOTP Authentication
- Google Authenticator
- Microsoft Authenticator
- YubiKey OTP (hardware key authentication)

Step 2: Enable MFA for VPN in ADSelfService Plus

- 1. Log in to ADSelfService Plus as an admin.
- 2. Go to Configuration > Self-Service > Multi-Factor Authentication > MFA for Endpoints.
- 3. Select a policy from the **Choose the Policy** drop-down. This policy will determine the users for whom MFA for VPN login will be enabled. To learn more about creating an OU or a group-based policy, click here.
- 4. In the **MFA for VPN Login** section, check the **Enable the second authentication factor** box, and select an authentication method from the drop-down.
- 5. Click Save Settings.

ADSelfService Plus			Q- Search Employe	Talk Back 🛛 🕹 🗸
Dashboard Reports	Configu	ation Admin Support		🔅 Domain Settings
Self-Service	-	Multi-factor Authentication ①	✓ How to	make users enroll?
Policy Configuration		Choose the Policy adselfserviceplus		
Multi-factor Authentication		Authenticators Setup MFA for Reset/Unlock MFA for Endpoints	MFA Enrollment	Advanced
Password Expiration Notificatio Password Policy Enforcer Password Sync/Single Sign Or Conditional Access Directory Self Service	n	MFA for Machine Login Enable 1 • authentication factors. Supported : Windows/macOS/Linux Select the authenticators required No factor selected • @ Access URL		
Administrative Tools Security Center		MFA for VPN LOgin Supports: VPN providers that support RADIUS authentication (Records) authenticators required Google Authenticator, Microsoft Authy v		
		Note • VPN MFA is applicable only when Windows Network Policy Server (NPS) is used as RADIUS server. • Download ADSelfService Plus NPS Extension and install it in the Windows servers(2008 R2 & above) where the Network policy Server(IAS) service is active. Learn more • View the architectural diagram illustrating the high-level VPN multi-factor authentication flow.		
		Save Settings Cancel		

Step 3: Install the NPS extension

 Log in to ADSelfService Plus as an admin, and go to Configuration > Self-Service > Multi-Factor Authentication > MFA for Endpoints. Download the NPS extension using the link provided in the Notes section.

MFA for VPN Login upported: VPN providers that support RADIUS uuthentication	Enable 2 v authentication factors	rs. Google Authenticator, Microsoft Authe 🗸
Note • VPN MFA is applicable only when Window Download ADSelfService Plus NPS Exten View the architectural diagram illustrating	vs Network Policy Server (NPS) is used as ision and install it in the Windows servers(2 ng the high-level VPN multi-factor authenti	; RADIUS server. (2008 R2 & above) where the Network policy Server(IAS) service is active. Learn more tication flow.
	Save Settings Cancel	

- 2. Copy the extension file (*ADSSPNPSExtension.zip*) to the Windows server, which you have configured as the RADIUS server. Extract the ZIP file's content and save it in a location.
- Open Windows PowerShell as administrator and navigate to the folder where the ZIP file's content is located.
- 4. Execute the following command:
 - PS C:\> .\setupNpsExtension.ps1 <operation>
 - where, the operation can by install, uninstall, or update.
 - 1. Install: installs the NPS extension plugin.
 - 2. Uninstall: uninstalls the NPS extension plugin.
 - 3. Update: updates the extension to newer versions and configuration data.
- 5. After installation, you will be prompted to restart the NPS (IAS) Windows service. Proceed with the restart.

ii. Configure conditional access

- 1. Log in to ADSelfService Plus as an admin.
- 2. Navigate to **Configuration > Self-Service > Conditional Access**.
- 3. Click Configure New Conditional Access (CA) Rule.
- 4. Enter a CA Rule Name and Description.
- 5. Select the **Conditions** from **IP Address**, **Device**, **Business hours**, **Geolocation** based on your requirement.
- 6. Now, create a Criteria with the conditions you have enabled. You can use AND, OR, and NOT operators to formulate the logic. Each condition is assigned a number: IP Address is 1, Device is 2, and so on. You can use these numbers and the allowed operators to create the Criteria. For example, 1 AND (2 OR 3) and 1 AND (3 OR (NOT 4))
- 7. In the **Associate Policies** drop-down, select the policies that will be applied to users who pass these criteria.
- 8. Click Configure.

III ADSelfSe	ervice Plus)			License Talk Back Q- Search Employee
Dashboard	Reports	Config	uration Admin		🔅 Domain S
Self-Service		•	Configure New Condi	ional Access (CA) Rule	$\langle \epsilon \rangle$
Policy Configurat Multi-factor Auth	ation hentication		CA Rule Name	Description	
Password Expira	ation Notificatio	n	Conditions	IP Address-Based (1)	*
Password Policy Password Sync/S	Enforcer Single Sign On			Static IPs	
Conditional Acce	ess			Proxy Server IPs	
Directory Self Se	ervice			VPN IP address	
Administrative Tool Security Center	ols			Note • Use " as wildcard to select all addresses within a certain class of IP address. Can only be used in the Individual IPs field. Field. • Please enter only IPv4 addresses. IPv6 is not supported.	
				Device-Based (2)	*
				Business Hours-Based (3)	*
				Location-Based (4)	*
				Criteria : (-)	
			Associate Policies	Select Policy v	
				Add Cancel	
				Note • To formulate criteria, supported operators include AND, OR, and NOT. • Conditional Access Rules does not apply to loopback addresses. • Conditional Access will not take effect for VPN MFA.	

iii. Configure password policies

- 1. Log in to the ADSelfService Plus admin portal.
- 2. Navigate to the **Configuration** tab. Under the **Self-Service** section, select the **Password Policy Enforcer**.
- 3. Enable Enforce Custom Password Policy.
- 4. In this section, you can manage:
 - Characters: Restrict the number of special characters, numbers, and Unicode characters used in passwords.
 - •. **Repetition:** Enforce a password history check during password reset, and restrict the consecutive repetition of a specific character from the username (e.g. "aaaaa" or "user01").
 - o. Patterns: Restrict keyboard sequences, dictionary words, and palindromes.
 - •. Length: Specify the minimum and maximum password length.
- 5. You can also enable users to **bypass complexity requirements** when the password length exceeds a predefined limit (say, 20 characters).
- 6. Enter the number of policy settings the user's password must comply with during self-service password reset and password change operations.
- 7. Enforce the configured password policy settings during password resets from the **ADUC console** and the **change password screen**.
- 8. To help users create passwords that comply with the enforced policy settings, you can display the password policy requirement on the reset and change password pages.

9. Click Save.

Dashboard Reports	Configuration Admin Support				
Self-Service	Password Policy Enforcer (2)				
Policy Configuration	Select the Policy testpolicy				
Multi-factor Authentication					
Password Expiration Notification	Enforce Custom Passwora Policy				
Password Policy Enforcer	Restrict Characters 5/7				
Password Sync/Single Sign On	Restrict Repetition 2/4 Minimum password length 8				
Conditional Access	Restrict Pattern 2/3 Maximum password length 15				
Directory Self Service	Restrict Length 1/2				
Administrative Tools					
Security Center	•				
	Override all complexity rules if password length is at least 20 3				
	Password must satisfy at least of the above complexity requirements. 7				
	Show this policy requirement in Reset and Change Password pages Customize View				
	Enforce this policy in GINA/CP (Ctrl+Alt+Del) screen and ADUC Password resets through Password Sync Agent.				
	Save Cancel				

iv. Implement password expiration notifications

- The <u>email and SMS server</u> must be configured for password expiration notification can be config ured. (The bookmark will point you to the steps for enabling the email and SMS server as also featured in the "Other important settings" section.)
- 2. Navigate to the Configuration tab. Under Self-Service, select Password Expiration Notification.
- 3. Select the domains, OUs, or groups for which you want to send notifications.
- 4. Enter the **Scheduler Name** and select the **Notification Type**.
- 5. From the *Notify via* drop-down, select the **method** through which you want to send notifications (SMS, email, push notification, or any combination of the three).
- 6. Configure the Notification Frequency as:
 - Daily
 - Weekly
 - **On specific days**: For instance, you can choose to email the first password expiration reminder when it's 15 days to password expiration, the second when it's 10 days, the third when it's seven days, the fourth when it's three days, and so on.
- 7. Set the **Schedule Time** to generate the notification message at a specific time.

- Type in the notification Subject and Message in their respective fields. There are character limitations for the notification messages based on the notification method chosen. To learn more about these limitations, refer to the character limits section.
- 9. You can attach any valid file (less than 25MB) along with the notification email.
- 10. Set priority levels for the email notifications as **High**, **Medium**, or **Low** by clicking on the ! icon at the top-right corner of the message field.

ADSelfService Plus					License Talk Back 💽 🗸 Q Search Employee
Dashboard Reports Con	figuration Admin Su	pport			🔅 Domain Settings
Self-Service •	Password/Account Expire	ation Notification ③			Mail/Mobile Attributes 🛞
Policy Configuration Multi-factor Authentication	Select Domain ADSEL	FSERVICE v	* Scheduler Name Notify Via	Soon-to-expire Password Notification Scl	
Password Expiration Notification		· · · · · ·	,		
Password Sync/Single Sign On	Notification Frequency	Daily V			📺 Schedule Time 🛛 🔅 Advanced
Conditional Access Directory Self Service	Notify users during the	last 7 days before expiration.			
Administrative Tools	* Subject	Password/Account Expiration Notification			
Security Center	* Message	$\mathscr{P} \mid B I \sqcup \mid F \cdot \mid 10^{-} \mid \blacksquare \mid \Xi^{-} \boxminus^{-} \mid \boxtimes \mathscr{P} \mid \phi$			1
		Dear % <u>userName</u> %, Your password will expire on %dateTime%. So, please change your passwo	rd as soon as possibl	2.	
		Thank you.			
		Regards Administrator			G
					Macros Access URL
	Please use %dateTime %noOfDay	0 days to notify users when their passwords/accounts are about to expire today. 6% - use this macro to insert the date and time of expiration in the message. s% - use this macro to insert the number of days left till expiration.			
		Save	Cancel		

3. One-identity configuration

i. Implement enterprise single sign-on

ADSelfService Plus can integrate with more than 100 enterprise applications and also custom SAML applications for SSO. To configure SSO for applications:

- Navigate to Configuration > Self-Service > Password Sync/Single Sign On > Add Application, and select the desired application.
- 2. Click **IdP details** in the top-right corner of the screen.
- In the pop-up that appears, copy the required URLs displayed and download the certificate or metadata file as needed.
- 4. Complete the configuration in the selected application using the URLs, certificate, and metadata file.
- 5. Switch back to ADSelfService Plus.

- 6. Enter the **Application Name** and **Description**.
- 7. In the Assign Policies field, select the policies for which SSO needs to be enabled.
- 8. Select Enable Single Sign-On.
- 9. Provide other information as required and click Add Application.

ADSelfService Plus	License Taik Back 😁 -						
Dashboard Reports Config	guration Admin Support	🗱 Domain Settings					
← All	Zoho 🕜	< Back					
Search 🔎	Add New Application						
Spotinst							
\land StatusCast	Application Name Description	IdP Details 🕀 Advanced					
StatusDashboard	* Domain Name						
🛞 Statushub	* Assian Policies Selected						
Statuspage.io							
SugarCRM	Single Sign On 🕥						
🖶 Sumologic	Configure SAML-SSO for Zoho						
ϟ Syncplicity	C Enable Single Sign-On						
🛞 Tableau	SANI Redirect IIP						
Targetprocess							
 ThousandEyes 	* ACS URL						
💶 Trello	Password Sync 🛞						
📵 UserEcho	Configure Password Synchronizer for Zoho						
🛷 Velpic	Enable Password Sync						
🗹 Weekdone							
See WhosOnLocation	* API Auth Token						
Workplace by Facebook	Add Analication. Correct						
🖌 Wrike	Caller						
Z Zendesk							

ii. Enable multi-platform password synchronization

Multi-platform password synchronization requires that the users' AD accounts be linked with accounts from the other applications through attributes. Account linking can either be <u>automated</u> or done <u>manually</u>. Native password change synchronization (changes through the Ctrl+Alt+Del console and resets through the Active Directory Users and Computers portal) works only when the <u>password sync agent</u> has been installed on the domain controllers in your domain. Once that is done:

- 1. Navigate to **Configuration > Self-Service > Password Sync/Single Sign On**.
- 2. Select the **desired** application.
- 3. Enter the Application Name and Description.
- 4. In the Assign Policies field, select the policies for which password sync needs to be enabled.
- 5. Select Enable Password Sync.
- 6. Enter other information as required. Refer to the <u>admin guide</u> for further details.
- 7. Click Add Application.

ADSelfService Plus)		License Talk Back 🕑 🗸 Q- Search Employee
Dashboard Reports	Config	figuration Admin Support	🔅 Domain Settings
← All		SalesForce (1)	< Back
Search	P	Add New Application	
📶 Rollbar			
SalesForce	•	Application Name Description	IdP Details
S Samanage		* Domain Name	
gr SAP NetWeaver		* Assign Policies All Policies Selected 🗸	
Screensteps			
Service Now		Single Sign On () Configure SAML-SSO for Safesforce	
👪 Showdme			
🍏 Shuffirr		Enable Single Sign-On	
😫 Slack	- 1	* SAML Redirect URL	
Small Improvements			
Spotinst		Password Sync. () Configure Password Synchronizer for Salesforce	
🐟 StatusCast			
 StatusDashboard 		C Enable Password Sync	
Statushub		* Username	
🕤 Statuspage.io		* Password	
🌓 SugarCRM		Security Taken	
🛨 Sumologic	_		
n Syncplicity	_	* Client ID	
🛞 Tableau		Client Secret	
Targetprocess			
O ThousandEyes		Add Application Cancel	

4. Directory self-service deployment

i. Configure a self-update layout

Create a layout

- 1. Navigate to **Configuration > Self-Service > Directory Self Service > Self Update Layout.**
- 2. Click on Create New Layout link.
- 3. Enter the Layout name in the text box and click Save.
- 4. Click on the drop-down menu and select **General Attributes** or **Custom Attributes**.
- 5. Choose any or all of the fields displayed below the selected attribute.
- 6. Click on any field on the left, then drag and drop it into the layout page on the right.
- 7. Instantly a **Field Selection** popup will appear. An administrator can work on Field Customization of the field properties.
- 8. Optional: Click on **New Group** to create new groups.

Cather Layord (* Cather Layord (* Cather Layord (*) Cather Layord (*) Cather Layord (*) Field Selection (*) Field Selection (*) Security Nake it Mathematical Layord (*) Security Nake it </th <th>III ADSelfService Plus</th> <th>License</th> <th>Talk Back 🛛</th>	III ADSelfService Plus	License	Talk Back 🛛
Outske Layard 0 Radia Carlow Radia Carlow <td>Dashhoard Reports Configuration Admin Support</td> <td>Ce Search Employee</td> <td>Domain Setting</td>	Dashhoard Reports Configuration Admin Support	Ce Search Employee	Domain Setting
El cod Indicado nala Indicado nala <tr< td=""><td>Customize Layout 🕐</td><td></td><td>C Back</td></tr<>	Customize Layout 🕐		C Back
Leptic Leptic <td>E Layout View</td> <td>Modification Rules</td> <td>Advanced</td>	E Layout View	Modification Rules	Advanced
Pield Selection Pield Selection <td>User Profile • Layout</td> <td></td> <td></td>	User Profile • Layout		
Very output Very output </td <td>Display Name 🗄 Full name</td> <td>▲ Add</td> <td>New Group</td>	Display Name 🗄 Full name	▲ Add	New Group
Uppergrame Uppergrame Uppergrame Uppergrame <td>Logon name i Uer Iogon name (uropi</td> <td></td> <td></td>	Logon name i Uer Iogon name (uropi		
Treepone number Treepone numbe	i tesphone nunder c-mail Display Name Logon name		
Set Catalant Field Selection Field Name Employee Id Select Field Type Single Line Text Pathenes Pathenes Pathenes Pathenes Catalant Pathenes Catalant Pathenes Pathenes <td>E-mail</td> <td></td> <td></td>	E-mail		
Contract Contract Contract Contract Contract Contract Select Field Type Single Line Text Chracter Length 255 Appearance Help Card Validations Cardet Letters Only Bread Address Only Letters Only Security Letters Only Letters Only Security Letters Only Security Letters Only Letters Only Security Security Letters Only	t Last name ☐ Initials		
Contait Casters Casters Caster Field Name Employee Id Select Field Type Single Line Text Options - Security Make it Mandatory ReadOnly Character Length 255 Appearance Initial value Help Card Validation E-mail Address Only Letters Only Letters Only Letters Only Letters Only	Employee Id Employee Rumber		
Tield Selection Field Name Field Name Field Name Field Name Field Name Email Address Only Numbers Only	Contact •		
Center Attributes Field Selection Field Name Employee Id Select Field Type Select Field Type Options - Security Make It Make It Make It Make It Mandatory ReadOnly Character Length 255 Appearance Help Card Validation E-mail Address Only Done Number Sonly Done Number Sonly Latters Only Latters Only	Audress / Organization /		
Field Selection Field Name Employee Id Select Field Type Select Field Type <	Custom Attributes		
Field Selection Field Name Field Name Employee Id Select Field Type Single Line Text Options - Security Make it Mandatory ReadOnly Character Length 255 Appearance Initial value Help Card Validation E-mail Address Only Done Numbers Only + xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx			
Field Name Employee Id Select Field Type Single Line Text Options - Security Make it Mandatory ReadOnly Character Length 255 Appearance Initial value Help Card Validation E-mail Address Only Done Cancel	Field Selection (7) Help X		
Field Name Employee Id Select Field Type Single Line Text Options - Security Make it Mandatory ReadOnly Character Length 255 Appearance Initial value Help Card Validation E-mail Address Only Numbers Only Phone Number Format Letters Only +xxxxxxxxxxx Uise Comma to give multiple phone formats.] Dorne			
Select Field Type Single Line Text Options - Security - Make it Mandatory Make it Mandatory Character Length 255 Appearance Initial value Help Card Validation E-mail Address Only Done Letters Only +xxxxx-xxxx [Use Comma to give multiple phone formats.] Done Cancel	Field Name Employee Id		
Options - Security Make it Mandatory ReadOnly Character Length 255 Appearance Initial value Help Card Validation E-mail Address Only Numbers Only Phone Number Format Letters Only **xxxx xxxx [Use Comma to give multiple phone formats.] Done Cancel	Select Field Type Single Line Text		
Security Make it Mandatory ReadOnly Character Length 255 Appearance Initial value Help Card Validation E-mail Address Only Numbers Only Phone Number Format Letters Only *xxxxxxxxxxxxxxxxxx [Use Comma to give multiple phone formats.]			
Security Make it Mandatory ReadOnly Character Length 255 Appearance Help Card Validation E-mail Address Only Phone Number S Only E-mail Address Only Classed Custor Comma to give multiple phone formats.] Cancel Cancel	Options +		
Make it Mandatory Character Length 255 Appearance Initial value Help Card Validation E-mail Address Only Numbers Only Phone Number Format Letters Only **xxxx xxxx xxxx [Use Comma to give multiple phone formats.] Done Cancel	Security		
Character Length 255 Appearance Initial value Help Card Validation Validation Phone Number S Only Numbers Only Phone Number Format Letters Only **xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	Make it Mandatory ReadOnly		
Appearance Initial value Help Card Validation E-mail Address Only Phone Number S Only I texts only I texts only I texts only Cuse Comma to give multiple phone formats.] Done Cancel	Character Length 255		
Initial value Help Card Validation E-mail Address Only Numbers Only Phone Number Format Letters Only **xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	Appearance		
Help Card Validation E-mail Address Only Numbers Only Phone Number Format Letters Only #x-xxxx xxxxxxxxxxx [Use Comma to give multiple phone formats.]	Initial value		
Help Card Validation E-mail Address Only Numbers Only Phone Number Format Letters Only **x-xxx *xxxx [Use Comma to give multiple phone formats.]			
Validation E-mail Address Only Numbers Only Phone Number Format Letters Only +x-xxxx-xxxx [Use Comma to give multiple phone formats.] Done Cancel	Help Card		
E-mail Address Only Numbers Only Phone Number Format Letters Only +x-xoc xocx [Use Comma to give multiple phone formats.] Done Cancel	Validation		
Phone Number Format Letters Only +x-xxxx+xxxe+xxxxx [Use Comma to give multiple phone formats.] Done Cancel	E-mail Address Only Numbers Only		
TX-XX-XXXXX [Use Comma to give multiple phone formats.] Done Cancel	Prone number Format Letters Only		
Done Cancel	Use Comma to give multiple phone formats,]		
Done Cancel	Free according to		
	Done Cancel		

Configure user modification rules

These rules help administrators to specify the fields that should be automatically updated whenever a user account is modified. These rules can be created as per the organizational policies and requirements to automatically update the required fields. Changes made by the users using the Profile tab are used. <u>Learn</u> how to enable this option.

ii. Configure employee search and organization chart

Employee search

- 1. Navigate to **Configuration > Self-Service > Directory Self Service > Employee Search**.
- 2. Select the **Enable Employee Search** checkbox. **Select the policy** to which employee search is going to be enabled.
- 3. Choose the domains from the **Filter Domains** dropdown field, which are to be involved in Employee Search. Searching can be performed at the OU or group level too.

- i. Click on Add OUs.
- ii. Select the OUs from the pop-up and click on **OK**.
- 4. You would be provided with three tabs: Users, Contacts, and Groups.
- 5. Enable the Users/Contacts/Groups checkboxes:
 - i. Select the desired **Display Columns.**
 - ii. You can configure the order in which the **Display Columns** appear by clicking on the up and down arrow buttons.
 - iii. Configure the **Search Criteria** and choose the desired **Search Criteria Options.** You can configure the order of the search criteria options using the up and down arrow buttons.

iv. Click **Save** to store the configured settings.

Organizational chart

- 1. Under Employee Search, click Advanced.
- 2. Select **Enable Organization Chart** checkbox to allow employees to view the searched account's position in the organizational hierarchy.

ADSelfService Plu	s)								Lio Q- Search Emp	nse Talk	Back 😫 -
Dashboard Reports	Conf	iguration Admin								🌣 Dor	nain Settings
Self-Service Policy Configuration Multi-factor Authentication Password Expiration Notificat Password Policy Enforcer	• ion	Employee Search Enable Employe Select Policy Filter Domains	e Search adselfserviceplus ADSELFSERVICEPLUS.com	× ×						Embed	C Back
Password Sync/Single Sign C Conditional Access Directory Self Service	n	User Search	Contact Search	Group Search						\$ /	\dvanced
Administrative Tools Security Center	;	Fnable Organ Hide Urmanz Exclude disal Show Employ Don't show p Use jpegPhot Show only use	ization Chart aged users in Organization Ch oled users from Employee Sez ree Search & Organization Ch hotos in Employee Search & (o attribute for photos leref from the same forest in th	art. arch and Organization (art on Login Page also Organization Chart he search results ⑦	thart.						
						Save Can	cel				

iii. Configure email group subscription

- 1. Go to **Configuration > Self-Service > Directory Self Service > Mail Group Subscription.**
- 2. Click **Add New** to create a new email group subscription.
- 3. Enter the email group subscription Name and Description.
- 4. Select the desired domain.
- 5. Select Mail Groups by clicking the plus [+] icon.
- 6. Select Users by clicking the plus [+] icon.
- 7. Select **Allow users to see group members** option if you want to allow the users to see the members of a group.
- 8. Click Save.

ADSelfS	ervice Plus	\mathbf{O}						
Dashboard	Reports	Confi	guration	Admin	Suppo	rt		
Self-Service		•	Add N	ew Mail Group	o Subscr	ription		
Policy Configur	ation			* N	ame			Description
Multi-factor Au	thentication							
Password Expi	ration Notificatio	on		Select Dor	main	AUTOSSP1	~	
Password Polic	y Enforcer			Select Mail Gro	oups	- Select Mail Groups -	+	
Password Sync	/Single Sign Or	ı					_	
Conditional Ac	cess			[°] Select U	lsers	- Select Users -	+	
Directory Self	Service				~	Allow users to see group members.		
Administrative To	ols	- • J				Save Cancel		
Security Center								

5. Supplementary features

i. Windows, macOS, and Linux login agent configuration

The ADSelfService Plus login agent is a software which, when installed on Windows, macOS, and Linux domain computers, provides users with the option to reset AD passwords and unlock accounts from their login screen. Installing the login agent also enables the Endpoint MFA feature for Windows, macOS, and Linux logons.

The login agent can either be pushed onto the client computers using the <u>admin portal, GPOs</u>, <u>SCCM</u>, third-party endpoint management solutions like ManageEngine <u>Desktop Central</u>, or be installed manually.

ii. Mobile app deployment

The ADSelfService Plus mobile app lets domain users perform AD password resets and account unlocks using their mobile device. It also lets users enroll themselves for certain MFA methods. The mobile app is also used to receive push notifications for:

- Notifying users upon successful completion of self-service actions.
- Impending password and account expiration.
- Enrollment reminders.

With the app, the users can also authenticate themselves using one of the MFA methods like time-based one-time-passcode, push notifications, fingerprint-based, and QR codes. The mobile app can be either manually installed by the user or <u>pushed onto the mobile devices by the administrator</u>.

iii. Enterprise application integration

ADSelfService Plus allows integration with external solutions like ADManager Plus, ManageEngine ServiceDesk Plus, Splunk, Syslog Server, and Have I Been Pwned? Integrating with these solutions allows the product to exchange data and information with these applications to achieve the capabilities mentioned below:

1. **ManageEngine ADManager Plus**: It enables customizable workflows that help streamline and monitor AD tasks. With this capability, users can raise requests to access resources which can be reviewed by a designated authority before the IT admin executes the task. When ADSelfService Plus is integrated with ADManager Plus, admins have complete control over all the self-service actions performed by users. User

actions are configured to be approved by the admin using ADManager Plus before being updated in AD. To integrate ADSelfService Plus with ADManager Plus:

- i. Navigate to Admin > Product Settings > Integration Settings.
- ii. Click the **ADManager Plus** tile.
- iii. In the Server Name or IP field, enter the name of the server in which ADManager Plus is installed.



- iv. Enter the Port Number used by ADManager Plus.
- v. Select the **Protocol** (HTTP/HTTPS) enabled in ADManager Plus from the drop-down list.
- vi. Click Save.

2. **ServiceDesk Plus**: It is an IT request tracking, and asset and change management solution. When this is integrated with ADSelfService Plus, IT requests are automatically created in the solution when self-service actions are performed by the user. This helps admins track users' self-service actions and follow up on them if needed. To integrate ADSelfService Plus and ServiceDesk Plus:

- i. Navigate to Admin > Product Settings > Integration Settings.
- ii. Click the ServiceDesk Plus tile.
- iii. In the Server Name or IP field, enter the name of the server in which ServiceDesk Plus is installed.
- iv. Enter the **Port Number** used by ServiceDesk Plus.
- v. Select the **Protocol** (HTTP/HTTPS) enabled in ServiceDesk Plus from the drop-down.
- vi. Enter the **API Key** generated in ServiceDesk Plus for a technician with login permissions.
- vii. Click Save.

API Key Generation

х

API Key : A8DBCC98-EAF5-4A04-B828-1D20CBEEEEE7

Note: Please copy the API key generated above and save the technician details to map this key to the technician. The key will not be mapped if technician details is not saved.

ADSelfService Pl	lus							License Talk Back 🕑 - Q. Search Employee
Dashboard Reports	Config	guration Ad	min Suppor	t				🗱 Domain Settings
Customize		Integration S	ettings - Service	Desk Plus				< Back
Enterprise Essentials				10 H	10			
Product Settings	•			Server Name or	- IP			
Connection				* Port Num	ber			
Mail / SMS Settings				Proto	ocol HTTP 🗸			
Dashboard Updater				* API H	<ev <="" th=""><th></th><th>Generate Kev</th><th></th></ev>		Generate Kev	
Auto Backup							,	
Integration Settings					Save			
Windows Service								
License Management	•							
Admin Gui	ida 🔅 Na	ad Fasturar 🔗	Penort an Isrue	C User Forums	Toll free : +1-844-245-1104	Direct Phone	+ + 1-409-016-0900	A
Admin Gu	ide wilde	eu reacurds	Report an ISSUE	er oser rorums	(* 100 11 CC . +1/044-245-1104	Con Direct Phone	. +1-400-910-9030	9

3. **Splunk**: It is a security information and event management (SIEM) solution that provides insight into application usage and user actions by processing large volumes of log data. It allows admins to spot operational problems and security issues within the organization early and proceed with reporting, diagnosing, and fixing them. Upon integrating ADSelfService Plus with the Splunk server, you can forward ADSelfService Plus' log data to the Splunk server for detailed auditing. To integrate ADSelfService Plus with Splunk:

Prerequisite:

The first step of the integration process is to generate an HTTP event collector token using Splunk:

- i. Log in to Splunk as an administrator.
- ii. Navigate to Settings > Data Inputs > HTTP Event Collector.
- iii. Click New Token.
- iv. Specify a name for the token and retain the default values for the other fields.
- v. Click **Save** and the authentication token will be generated.

Once the HTTP event collector token is generated:

- i. Navigate to Admin > Product Settings > Integration Settings.
- ii. Click the **Splunk Server** tile.
- iii. Click Enable forwarding of logs to splunk
- iv. Enter the details including **Splunk Server Name** and **HTTP Event Collector Port** number.
- v. Select **True** or **False** in the SSL Enabled drop-down.
- vi. Specify the **HTTP Event Collector Token** generated for ADSelfService Plus in the **Authentication Token** field.
- vii. Click Save.

ADSelfSe	ervice Plus)										Q- Search E	License Talk Bac mployee	ik 🙆 -
Dashboard	Reports	Config	uration	Admin	Support								🛱 Domain	Settings
Customize		•	Integratio	on Settings	- Splunk S	erver 🕜							<	Back
Enterprise Essentia	als	•	🗸 Enal	ble forward	ing of logs t	o splunk								
Product Settings		•				* Comment	. 10							
Connection						Server Name of	rip							
Mail / SMS Sett	ings				*нтт	P Event Collector F	Port							
Dashboard Upd	ater					SSL Enab	led Fals	e 🗸						
Auto Backup						Authoritan Tal								
Integration Sett	tings					Autnentication io	ken							
Windows Servic	e						Sav	re						
License Manageme	ent	•												
	Admin Guide	🔅 Nee	d Features	😢 Report a	in Issue	PUser Forums	🕓 Toll free	: +1-844-245-1104	S Direct Pho	one : +1-408-916-989	0			

4. **Syslog server**: A Syslog server is used to receive system logs or incidents from its network devices. The data received by the server is then stored and reported to software that analyzes it and puts forth information that can help admins monitor the network's devices and resolve any issues. ADSelfService Plus can be integrated with any Syslog server and the product logs can be forwarded to the server for in-depth analysis. To integrate ADSelfService Plus with a Syslog server:

- i. Log in to ADSelfService Plus as default Admin.
- ii. Navigate to Admin > Product Settings > Integration Settings.
- iii. Click the **Syslog Server** tile.
- iv. Click Enable forwarding of logs to Syslog
- v. Enter the details including **Syslog Server Name**, **Port number**, and **Protocol**. Choose the **Syslog Standard** and specify the **Data Format** needed for your SIEM parser.

ADSelfS	ervice Plus)			License Talk Back Q- Search Employee	8-
Dashboard	Reports	Config	uration Admin	Support	🛱 Domain Set	tings
Customize		•	Integration Settings -	Syslog Server 🛛 💿	< B/	ack
Enterprise Essenti	ials	•	Enable forwarding	of logs to syslog		
Product Settings Connection Mail / SMS Set	tings	·	* Server I * Po	ame or IP rt Number 514		
Dashboard Upc Auto Backup	dater			Protocol UDP	v	
Integration Set	ttings		Syslo	Standard RFC 316	54 🗸	
Windows Servio	nent	•	D	ta Format < 110	>EVENT_TIME HostName ADSSP: [DATA KEY = DATA VALUE]	
			Sample D	ta Format <110>0	Dct 22 10:52:12 HostName ADSSP: [KEY1 = VALUE1] [KEY2 = VALUE2]	
				Save		
E	Admin Guide	🕸 Ne	ed Features 🛛 🕫 Report an	ssue 🗗 User Forum	is 🔋 🖗 Toll free : +1-844-245-1104 👘 🖗 Direct Phone : +1-408-916-9890	2
vi. C	Click Sa	ve.				

5. Have I Been Pwned?: This website allows users to check whether the passwords they use have been compromised due to data breaches. By integrating ADSelfService Plus with the Have I Been Pwned? service, admins can ensure that users do not use weak passwords during enterprise password resets and changes. It is also enforced in the GINA/CP (Ctrl+Alt+Del) login page and ADUC Password resets through Password Sync Agent. To integrate ADSelfService Plus with Have I Been Pwned?:

Prerequisite :

i. The firewall should have the outbound connection to **api.pwnedpasswords.com**

Steps to integrate:

- i. Log in to ADSelfService Plus as default Admin.
- ii. Navigate to Admin > Product Settings > Integration Settings.
- iii. Click the Have I Been Pwned? tile.
- iv. Click Enable HavelBeenPwned Integration



Configure security settings in ADSelfService Plus

1. Implement failover and secure gateway features:

i. Reverse proxy

In computer networks, a reverse proxy is a type of proxy server that retrieves resources on behalf of a client (in this case the user) from one or more servers (in this case the ADSelfService Plus server). These resources are then returned to the client as though they originated from the reverse proxy itself. A reverse proxy is used as a strategic point in the network to enforce web application security. Learn how to enable reverse proxy for ADSelfService Plus.

ii. Load balancing

With load balancing, the incoming requests to ADSelfService Plus are split among multiple server nodes. To enable load balancing in ADSelfService Plus, a primary node and multiple secondary nodes have to be configured. When requests are made to ADSelfService Plus, the primary node splits the requests among the secondary nodes using the round-robin method. Load balancing helps alleviate performance degradation due to heavy traffic and improves the user experience. Learn how to enable load balancing.

iii. High availability

High availability is configured in ADSelfService Plus to provide failover in the case of system or application failures. High availability is achieved through automatic failover, that is, when the service running on one server fails, another instance of the service running on another server will take over. Setting up high availability involves configuring a primary and secondary server. When the primary server fails to function, the instance running in the secondary server takes over. Since the data in the primary server is cloned to the secondary server during configuration, the switchover is automatic and free of hiccups. High availability helps the administrators and end users have continued access to ADSelfService Plus. Click <u>here</u> to learn how to enable high availability.

2. Configure SSL and LDAPS

- i. Go to Admin > Product Settings > Connection.
- ii. Click the **Connection Settings** tab. You can choose a HTTP or HTTPS port.

C	onnection Settings	Proxy Settings	General Settings
23	ADSelfService P	lus Port [http]	8888
	ADSelfService Plu	us Port [https] 🧕 🧕	9251 Apply SSL Certificate
	Encrypt Keystore	Password	(?
			Use LDAP SSL(LDAPS)
		Ac	vanced Settings 👻
	TLS Versions	1	LSv1, TLSv1.1, TLSv1.2 🗸
	Cipher Suites	1	LS_ECDHE_RSA_WITH_AES_
		(Save Cancel Changes will reflect only on restart of ADSelfService Plus.

- iii. Select the **ADSelfService Plus Port [HTTP]** and enter the port number of your choice.
- iv. If you want to configure a HTTPS port, select the **ADSelfService Plus Port [HTTPS]** option and enter the port number.
- v. If you want to apply SSL certificate, click **Apply SSL Certificate** (optional) and <u>follow these steps</u>.

- vi. Select the **Enable LDAP SSL** to secure communication between AD and ADSelfService Plus.
- vii. Select the **Encrypt keystore password** and enter the keystore password. The password you enter will be encrypted for better security.

Note: The value of the keystorePass property in the server.xml file will be replaced with the macro \${adssp.keystorePass}.

- viii. Select the **TLS Versions** and the **Cipher Suites** from the drop-down.
- ix. Click Save.

3. Allow or restrict admin portal access based on IP addresses

- i. Go to Admin > Customize > Logon Settings
- ii. Select Allow/Restrict Application access based on IP Addresses
- iii. Click Configure Now.

ADSelfService Plus)			License Talk Back 😜
Dashboard Reports	Configuration Adr	nin Application		🔅 Domain Settings
Customize Logon Settings Personalize Enterprise Essentials Product Settings	General Logon Setting Logon Setting Hik Million Setting	gs ⑦ Single Sign-On Sr tings de Self Service Admin Lo ow/Restrict Admin porta	nart Card Auth gin ③	Allow Restrict IP Addresses - ADSelfService Plus × Allowed IP Addresses Addresses Autor ofly specific TPs or IP range to access the admin portal. Allow IP Range to
License Management	, Sh Sh En En CAPTCHA : Sh	ow the Domain Selection ow the Domain Selection able other unique attribu able User Disclaimer Q settings ow CAPTCHA (Word Veri	n Drop-Down M n Drop-Down M ites to log in to stomize	Add Individual IP Addresses > Note If you are using a proxy server in your environment, then please follow the steps given here. Use * as wildcard to restrict all addresses within a cottain class of IP address. Works only for individual IP Addresses. IP restriction does not apply to localhost machines. Please enter only IPv4 addresses; IPv6 is not supported.
	Other Sett) On Admin & Domain) On 'Reset Password' & able Audio Captcha. (7) ings de 'Help Button' on End-U de 'Mobile Access Button' o	'Unlock Accou sers Page. n End-Users Pi	Save

- iv. Select Allowed IP Addresses or Restrict IP Addresses.
- v. Enter the appropriate IP address range in the available fields.
- vi. Restrict or allow specific IPs by selecting Add Individual IPs.
- vii. Click Save.

4. Set the session expiration time

- i. Navigate to Admin > Product Settings> Connections > General Settings.
- ii. Select a Session Expiration Time limit from the drop-down.
- iii. Click Save Settings.

5. Manage product licenses

Administrators can free unused ADSelfService Plus licenses by using the Restrict Users feature in ADSelfService Plus. When configured, this feature not only frees the licenses assigned to the selected user accounts but also restricts them from accessing ADSelfService Plus in the future. Here are the types of stale user accounts that can be restricted using the Restrict Users feature:

- 1. Account Expired Accounts that are expired in AD.
- 2. Account Disabled Accounts that are disabled by the administrator.
- 3. Inactive users Accounts that have not logged in to the domain for a specific period.
- 4. Deleted users Accounts that were deleted from AD.
- 5. Service Accounts AD service accounts.
- 6. Smart Card Users User accounts that use a smart card for authenticating their workstations.

Steps to configure the Restrict Users option:

- i. Navigate to Admin > License Management > Restrict Users.
- ii. Click **Restrict Users** from the right corner of the page.

Restrict Users

- iii. Select the required **Domain**.
- iv. Select the desired **OUs** (if you want to restrict users from a particular OU).

ManageEngine ADSelfService Plus

ADSelfServ	ice Plus)									Q- Search B	License Talk Back	8-
Dashboard R	Reports	Config	uration Adm	nin Support								🌣 Domain Se	ettings
Customize		•	Restrict Users	3 (?)								< E	Back
Enterprise Essentials		•	Select [Domain SELFS	SELFSERVICE VII VII VII VII VII VII VII VII VII VI								
Product Settings		•	Accour	nt Type Accourt	t Expired	Expired V							
License Management		•											
Restrict Users				Gener	ate Stop								
			Note • •	Generate Users I Select Users to b All the DCs of the	sts for Expired/C e restricted from domain should	isabled/Inactive/ the list. nave been configu	Deleted Accoun	ts/Smart Card	Users/UnOwned I	Jcenses/Service A	ccounts/All Users.		Ő
Ad	dmin Guide	🔅 Nee	d Features 👘 🕫 R	Report an Issue	🖓 User Forums	🕓 Toll free : +	1-844-245-1104	🕓 Direct P	Phone : +1-408-910	-9890			

- v. From the **Account Type** drop-down menu select the type of users you want to restrict.
- vi. Click Generate. A list of users of the selected type will be generated.
- vii. Select the users you want to restrict. You can select all the users at once or a particular user.

viii. Click **Restrict**.

Once restricted, the user will not be able to log in or perform any actions using ADSelfService Plus. The enrollment data of the user will be deleted too.

6. Configure CAPTCHA:

- i. Go to Admin \rightarrow Customize \rightarrow Logon Settings.
- ii. Select Show CAPTCHA (Word Verification Image) on Login Page.

On 'Reset Password' & 'Unlock Account' Login Page	Captcha Settings ×
Enable Audio Captcha. (?)	Always show Captcha.
	 Show Captcha after invalid login attempts.
Settings	3 invaid login attempts.
Hide 'Help Button' on End-Users Page.	30 minutes to reset invalid login attempts.
Hide 'Mobile Access Button' on End-Users Page.	

- iii. Enable CAPTCHA for the login pages of admin, domain user, and during password reset and account unlock.
- iv. Click the **Captcha Settings** link to configure whether to show **CAPTCHA** every time or only after a certain number of invalid login attempts.
 - Select Show CAPTCHA after invalid login attempts to enable captcha only after a certain number of invalid login attempts. Enter the number of invalid login attempts allowed and the time (in minutes) that must pass before the invalid login count is reset.
 - Select Always show CAPTCHA to display CAPTCHA every time someone tries to log in to the product.
- v. Select Enable Audio CAPTCHA to offer CAPTCHA for visually impaired users.
- vi. Click Save.

Other important settings

1. Configure the dashboard updater

You can set up schedules to automatically update the Dashboard in the ADSelfService Plus admin portal. You can also synchronize ADSelfService Plus with your organization's AD. The feature offers schedulers for the following:

- AD Synchronizer.
- Locked Out Users.
- Soon-To-Expire User Passwords.
- Password Expired users.

To configure the dashboard updater:

- i. Go to Admin > Product Settings > Dashboard Updater.
- ii. Click the edit icon next to the desired scheduler.
- iii. Use **Select Duration** to schedule automatic updates at a set frequency.
 - Daily: The scheduler is run once every day.

- Hourly: The scheduler is run once every hour.
- Weekly: The scheduler is run once every week.
- Monthly: The scheduler is run once every month.
- iv. Click Save.

2. Configure email and SMS servers for notifications

To enable email and SMS notifications for email, or SMS-based verification codes, password expiration notifications, and other product notifications, email and SMS servers need to be configured in ADSelfService Plus. Learn how to configure <u>email</u> and <u>SMS</u> servers.

3. Enable auto-backup of the database

To enable auto-backup of the product database:

- i. Go to Admin > Product Settings > Dashboard Updater.
- ii. Set up a backup scheduler.
- iii. Enter the Backup Storage Path.
- iv. Click Save Settings.

Note: To save a backup immediately, click Backup Now.



4. Configure technicians for product administration

Technicians are users with elevated rights in the product. ADSelfService Plus Technicians consist of these roles and permission levels that allow customizable options:

- Super Admin: Up to full control over the entire application by default.
- Operator: Can audit the various operations taking place in the application.

How to assign permissions to Technician roles

- i. Go to **Configuration > Administrative Tools > Technician.**
- ii. Select Role Settings.
- iii. Select the required role from the drop-down.

Role Settings			×
Select Role	Operator	~	
Select Permissions	Super Admin		itions' report.
	Operator Allow technician to disenroll u	isers from	n 'Enrolled Users' report.
	Allow technician to delete use	ers from 'I	Licensed Users' report.
	Allow technician to generate b	backup co	ode for users from 'Enrolled Users'
	report.	6	
	Save Cancel		

iv. You can now choose to assign or remove the displayed permissions.

' report.
olled Users' report.
sed Users' report.
or users from 'Enrolled Users'
0

How to create a Technician

- i. Go to **Configuration > Administrative Tools > Technician.**
- ii. Click the Add new Technician button.
- iii. Select the **Authentication Type, Domain, Users/Groups,** and the **Role** from the respective drop-downs.

		>
AD Authentication	~	
CLOUDSSP	~	
	+	
Super Admin	~	
	AD Authentication CLOUDSSP Super Admin	AD Authentication CLOUDSSP

Important: When AD Authentication is selected, the created Technician can use their Windows logon credentials to log in to ADSelfService Plus.

iv. If you select **Product Authentication** in the Authentication Type field, you will be required to enter the login credentials of that Technician.

Add New Technicians		×
Authentication Type	Product Authentication	
* Login Name	User01	
* Password	•••••	
* Confirm Password :	••••••	
Delegate Role	Super Admin 🗸	
	Add Cancel	

v. Click Add.

5. Rebrand and personalize the portal

Using the rebranding settings, the product's theme color, logo, browser title and image, and the login screen's background image can be modified. The buttons displayed on the login screen can also be customized.

- i. Navigate to Admin > Customize > Personalize > Portal Rebranding.
- ii. Under General Customization, use the **Choose Theme Color** field to select the desired theme color.
- iii. Click Browse next to the Change Logo field and choose a logo of your choice. The image should be 200x50 pixels in dimensions.
- iv. Enter the desired Browser Title.
- v. Click Browse next to the Browser Title Image field to select a title image for your choice.
- vi. Under Logon Customization, use the Customize Logon Buttons to change the other order of and the text displayed in the Sign in, Reset Password, and Account Unlock buttons.
- vii. Select Choose next to the Login Screen Background Image to select the desired image.
- viii. Click Save.

ADSelfService Plus)					License Talk Back 🕒 🗸
Dashboard Reports	Config	uration Admin	Support			🌣 Domain Settings
Customize	•	Personalize Setting	ţs			
Logon Settings		Display Settings	Portal Rebranding	Mobile Rebranding Change Password Lan	guage Customization	
Enterprise Essentials	•	General Custor	mization			
Product Settings License Management		Choose T	heme Color	Dark Gray 🗸		
		Browser	Title	ADSelfService Plus		
		Browser	Title Image	Browse Title Image Browse Preferred image format is .ico		
		Change L	.ogo	Browse Logo Browse ⑦ Dimension: 200 x 50, Size 2MB		
		Logon Customi	ization		L2	
		Customiz	e Logon Buttons	🗄 🗹 Sign In 🔇	0	
				ii 🗹 Forgot your password?		
				Account locked down?		
		Login Scr	reen Background Image	- Browse file - Browse (7 Dimension: 1300 x 700, Size 2MB	D	
					Save Restore	

About ADSelfService Plus

ManageEngine ADSelfService Plus is an integrated self-service password management and single sign-on solution. It offers self-service password reset and account unlock, endpoint multi-factor authentication for machines and VPN logins, single sign-on to enterprise applications, Active Directory-based multi-platform password synchronization, password expiration notification, and password policy enforcer. It also provides Android and iOS mobile apps that facilitate self-service for end users anywhere, at any time. ADSelfService Plus helps reduce IT expenses associated with help desk calls, improves the security of user accounts, and spares end users the frustration due to computer downtime. For more information about ADSelfService Plus, visit: www.manageengine.com/products/self-service-password/