ManageEngine
ADSelfService Plus

ADSelfService Plus

Evaluator's guide

www.adselfserviceplus.com

Table of Contents

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.

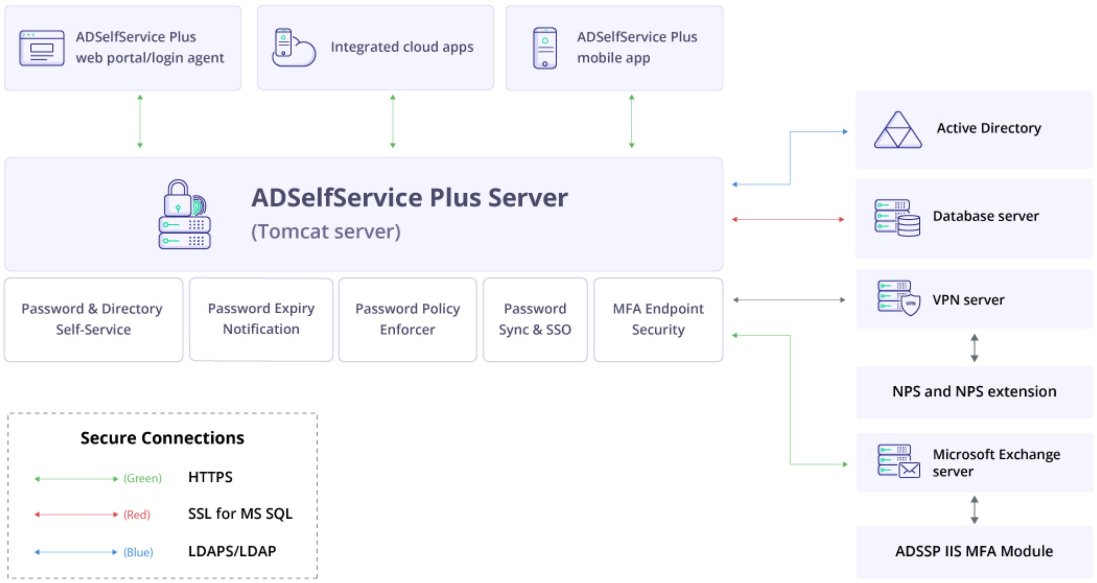
Benefit: This helps users discover details about other users from a single portal.

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

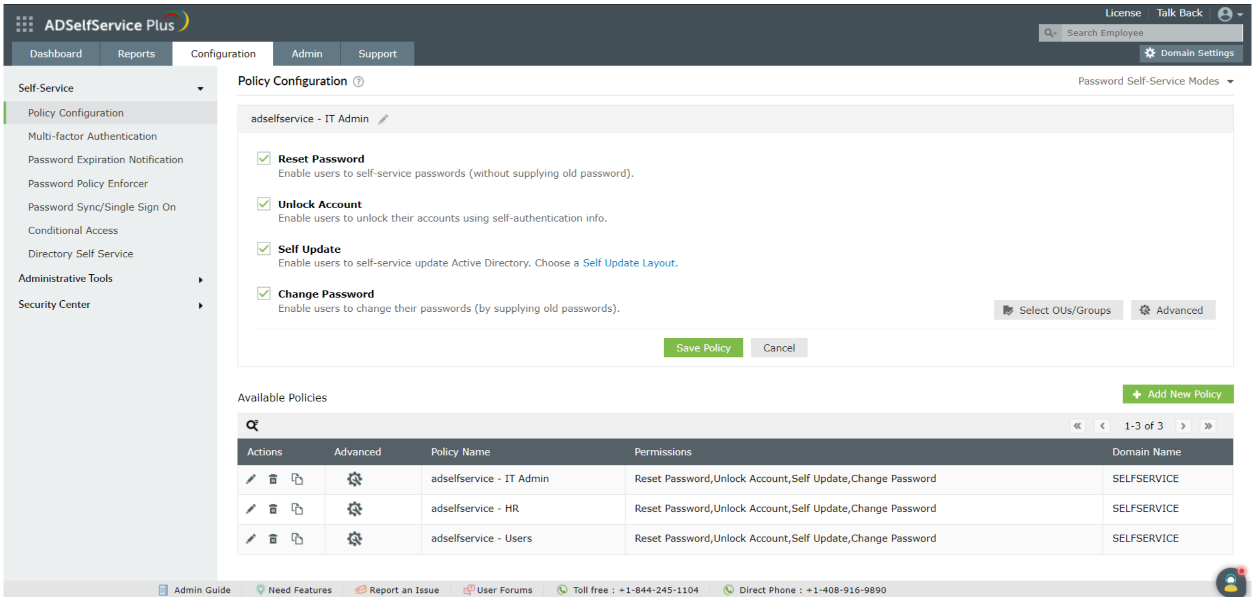
1. Password self-service deployment

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.



Policy Configuration

adselfservice - IT Admin

☑ **Reset Password**
Enable users to self-service passwords (without supplying old password).

☑ **Unlock Account**
Enable users to unlock their accounts using self-authentication info.

☑ **Self Update**
Enable users to self-service update Active Directory. Choose a Self Update Layout.

☑ **Change Password**
Enable users to change their passwords (by supplying old passwords).

Available Policies

Actions	Advanced	Policy Name	Permissions	Domain Name
		adselfservice - IT Admin	Reset Password,Unlock Account,Self Update,Change Password	SELFSERVICE
		adselfservice - HR	Reset Password,Unlock Account,Self Update,Change Password	SELFSERVICE
		adselfservice - Users	Reset Password,Unlock Account,Self Update,Change Password	SELFSERVICE

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**.

Learn how the ADSelfService Plus login agent can be configured and self-service features can be enabled for users' Windows, macOS, and Linux login screens. Click here 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. Learn 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. Bookmarked here 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. **Click here** 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 deployed onto users' machines from the ADSelfService Plus admin portal, installed manually, and installed via GPO or Microsoft System Center Configuration Manager (SCCM).
- **Mobile devices**: Deploy 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

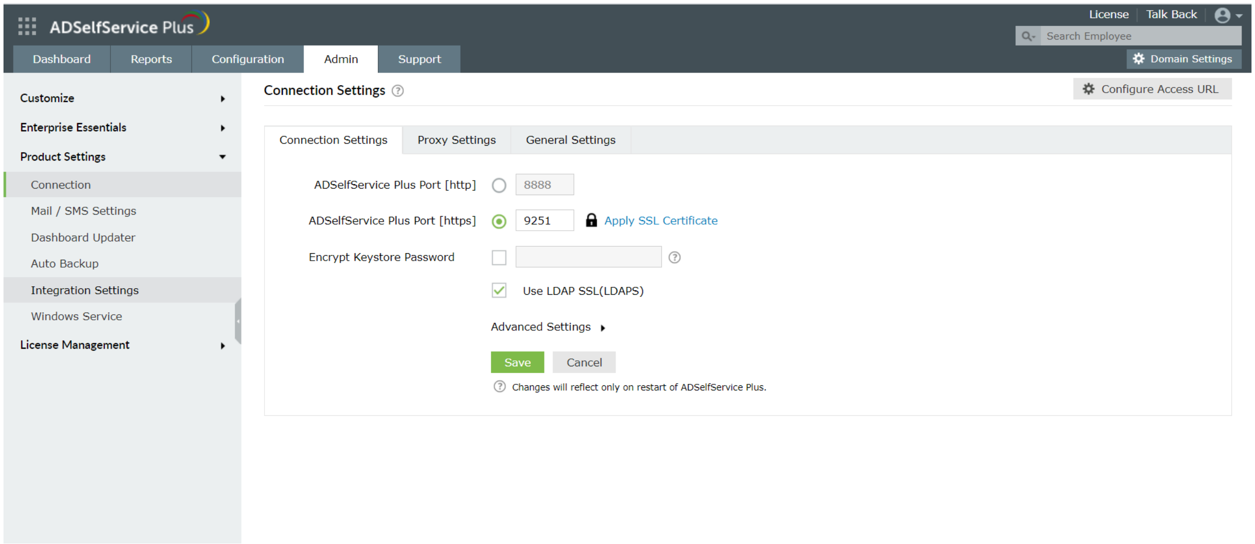
i. Enforce endpoint MFA:

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.



Connection Settings

ADSelfService Plus Port [http] ○ 8888

ADSelfService Plus Port [https] ● 9251 Apply SSL Certificate

Encrypt Keystore Password □

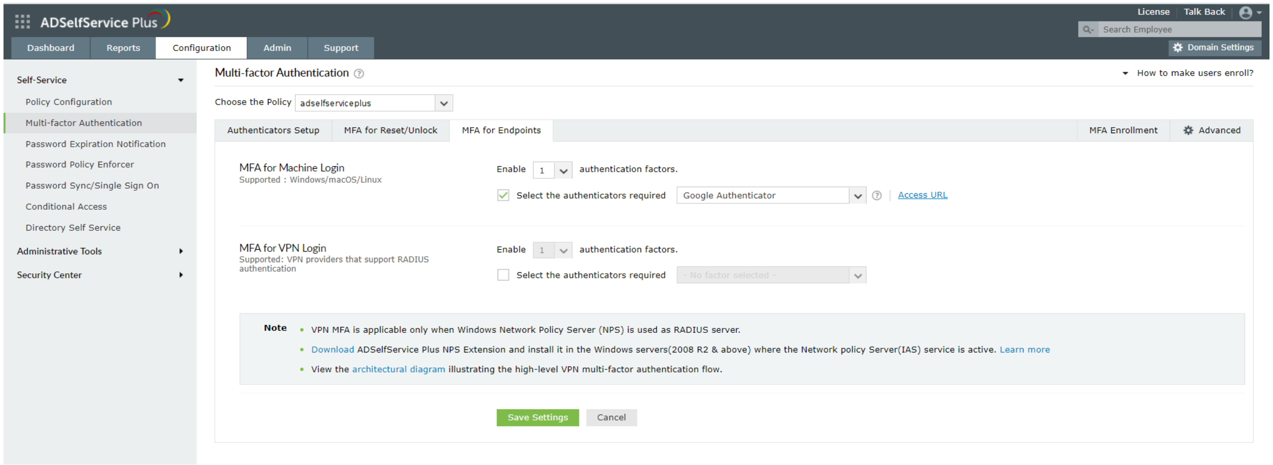
☑ Use LDAP SSL(LDAPS)

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**.



Multi-factor Authentication

Choose the Policy adselfserviceplus

MFA for Machine Login
Supported : Windows/macOS/Linux

Enable 1 authentication factors.

☑ Select the authenticators required Google Authenticator

MFA for VPN Login
Supported: VPN providers that support RADIUS authentication

Enable 1 authentication factors.

□ Select the authenticators required - No factor selected -

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.

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:

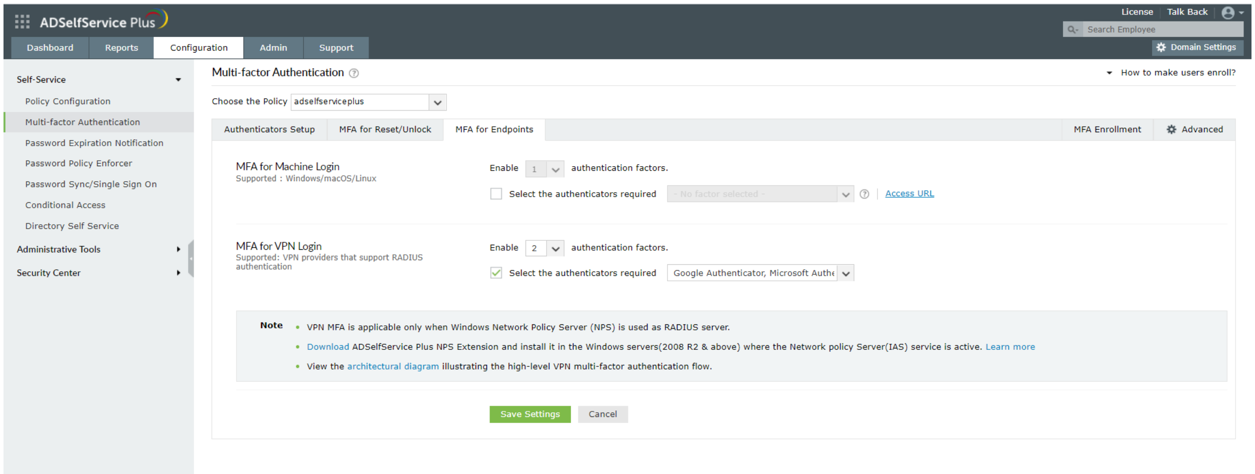
- When you enable **Push Notification** or **Fingerprint/Face ID Authentication**, make sure the ADSelfService Plus server is reachable by the users (through the internet) from their mobile devices.
- **RADIUS authentication** timeout should be set to at least 60 seconds in the VPN server's RADIUS authentication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



Multi-factor Authentication

Choose the Policy: adselfserviceplus

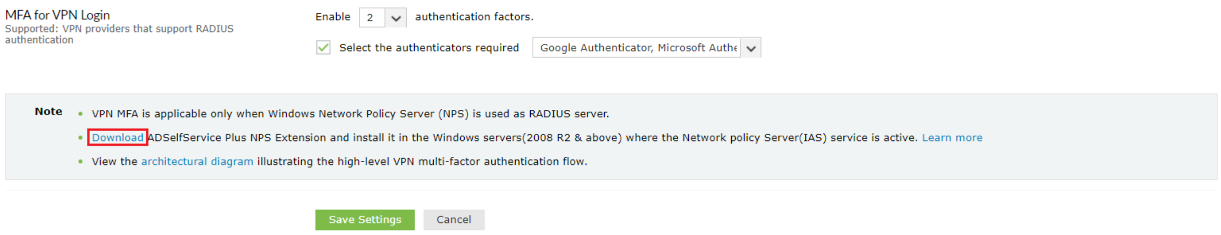
MFA for Machine Login
Supported : Windows/macOS/Linux
Enable 1 authentication factors.
□ Select the authenticators required: - No factor selected -

MFA for VPN Login
Supported: VPN providers that support RADIUS authentication
Enable 2 authentication factors.
☑ Select the authenticators required: Google Authenticator, Microsoft Authe

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.

Step 3: Install the NPS extension

1. 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
Supported: VPN providers that support RADIUS authentication

Enable 2 authentication factors.

☑ Select the authenticators required: Google Authenticator, Microsoft Authe

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.

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.

3. 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**.

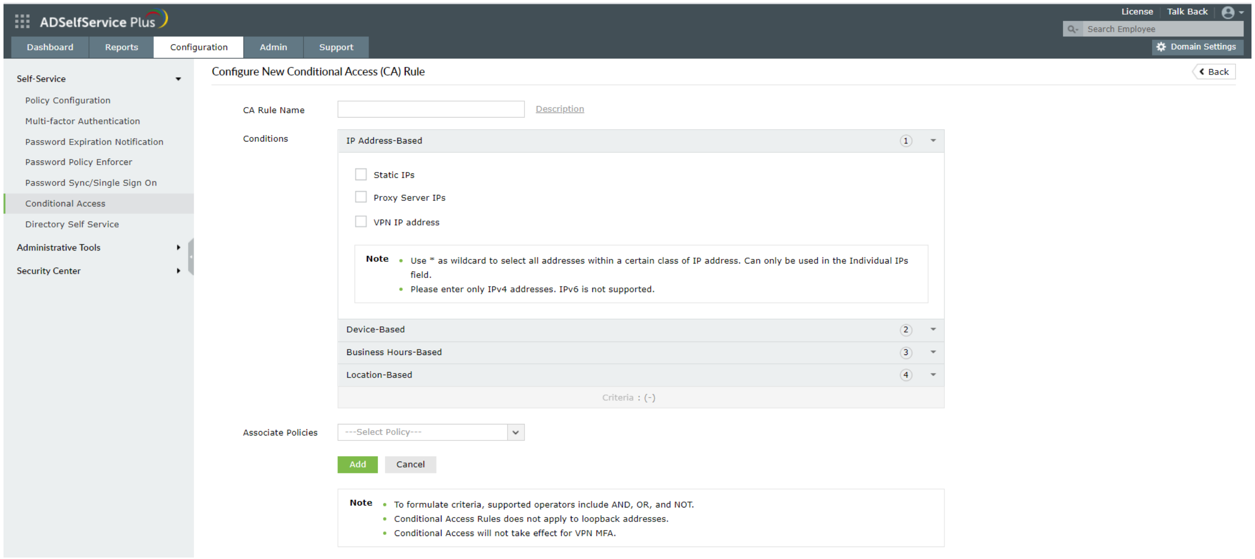
4. Enter a **CA Rule Name** and **Description**.

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**.



Configure New Conditional Access (CA) Rule

CA Rule Name

Conditions

IP Address-Based 1

□ Static IPs

□ Proxy Server IPs

□ VPN IP address

Note
- Use * as wildcard to select all addresses within a certain class of IP address. Can only be used in the Individual IPs field.
- Please enter only IPv4 addresses. IPv6 is not supported.

Device-Based 2

Business Hours-Based 3

Location-Based 4

Criteria : (-)

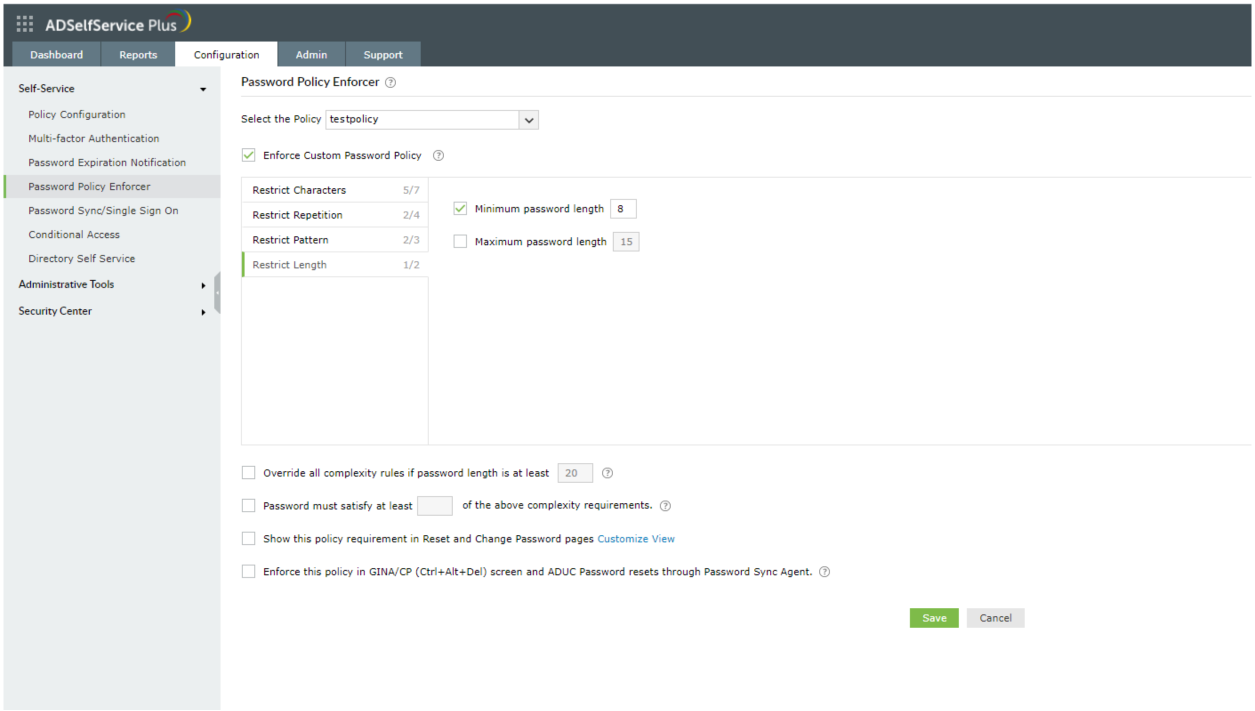
Associate Policies ---Select Policy---

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”).
   - **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**.



Password Policy Enforcer

Select the Policy: testpolicy

☑ Enforce Custom Password Policy

☑ Minimum password length 8

☐ Maximum password length 15

☐ Override all complexity rules if password length is at least 20

☐ Password must satisfy at least ___ of the above complexity requirements.

☐ Show this policy requirement in Reset and Change Password pages

☐ Enforce this policy in GINA/CP (Ctrl+Alt+Del) screen and ADUC Password resets through Password Sync Agent.

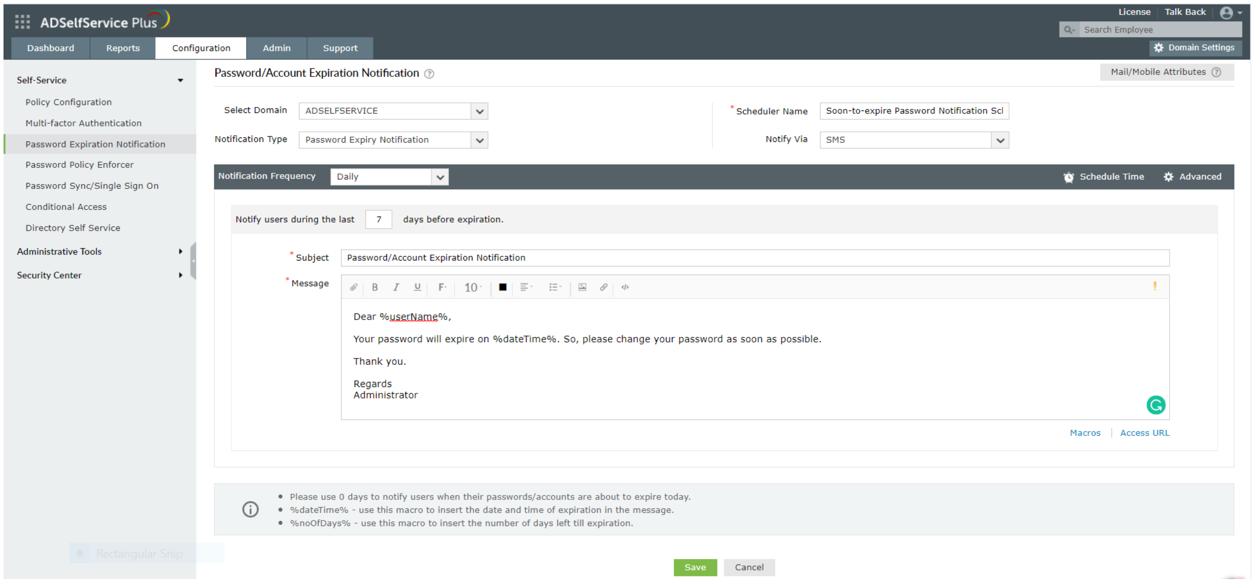
iv. Implement password expiration notifications

1. The email and SMS server must be configured for password expiration notification can be configured. (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.

8. 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.



Password/Account Expiration Notification

Select Domain: ADSELFSERVICE

Notification Type: Password Expiry Notification

* Scheduler Name: Soon-to-expire Password Notification Scl

Notify Via: SMS

Notification Frequency: Daily

Notify users during the last 7 days before expiration.

* Subject: Password/Account Expiration Notification

* Message:

Dear %userName%,

Your password will expire on %dateTime%. So, please change your password as soon as possible.

Thank you.

Regards
Administrator

- Please use 0 days to notify users when their passwords/accounts are about to expire today.
- %dateTime% - use this macro to insert the date and time of expiration in the message.
- %noOfDays% - use this macro to insert the number of days left till expiration.

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:

1. 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.

3. 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.

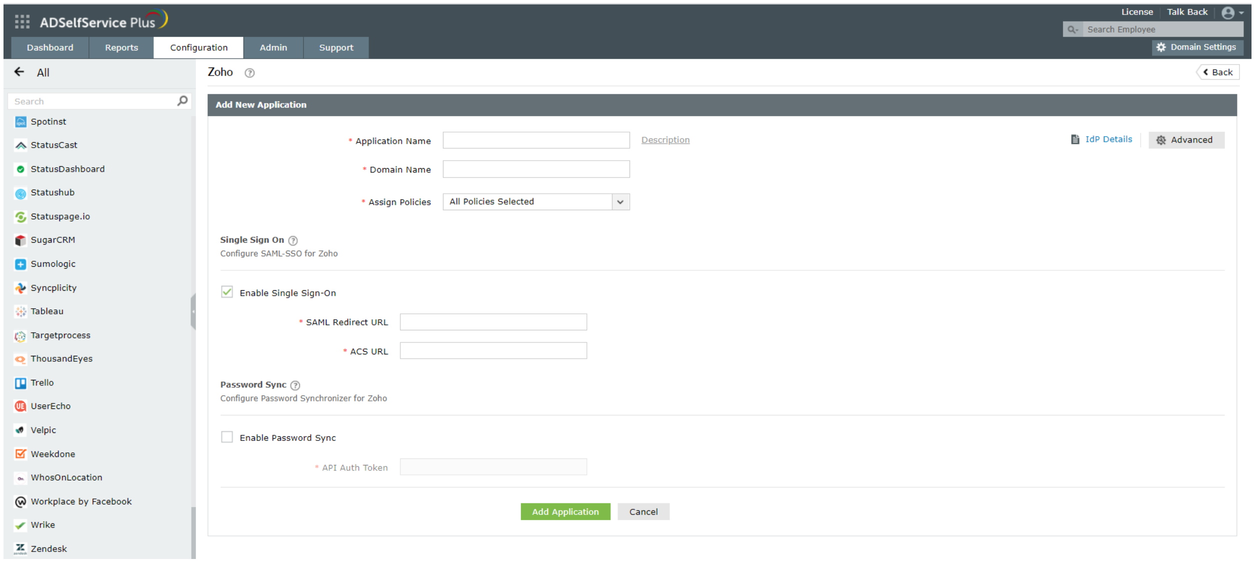
5. Switch back to ADSelfService Plus.

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.**



Add New Application

* Application Name Description

* Domain Name

* Assign Policies: All Policies Selected

Single Sign On
Configure SAML-SSO for Zoho

☑ Enable Single Sign-On

* SAML Redirect URL

* ACS URL

Password Sync
Configure Password Synchronizer for Zoho

□ Enable Password Sync

* API Auth Token

Add Application Cancel

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 automated or done manually. 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 password sync agent 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.

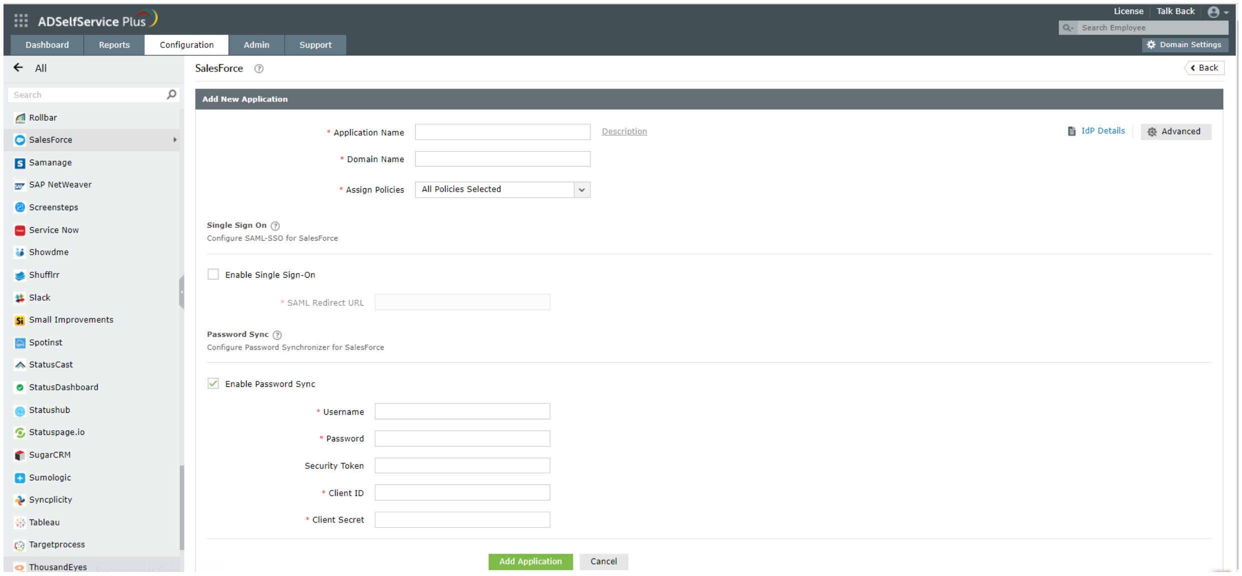
3. Enter the **Application Name** and **Description**.

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 admin guide for further details.

7. Click **Add Application**.



SalesForce

Add New Application

* Application Name

* Domain Name

* Assign Policies: All Policies Selected

Single Sign On

Configure SAML-SSO for SalesForce

□ Enable Single Sign-On

* SAML Redirect URL

Password Sync

Configure Password Synchronizer for SalesForce

☑ Enable Password Sync

* Username

* Password

Security Token

* Client ID

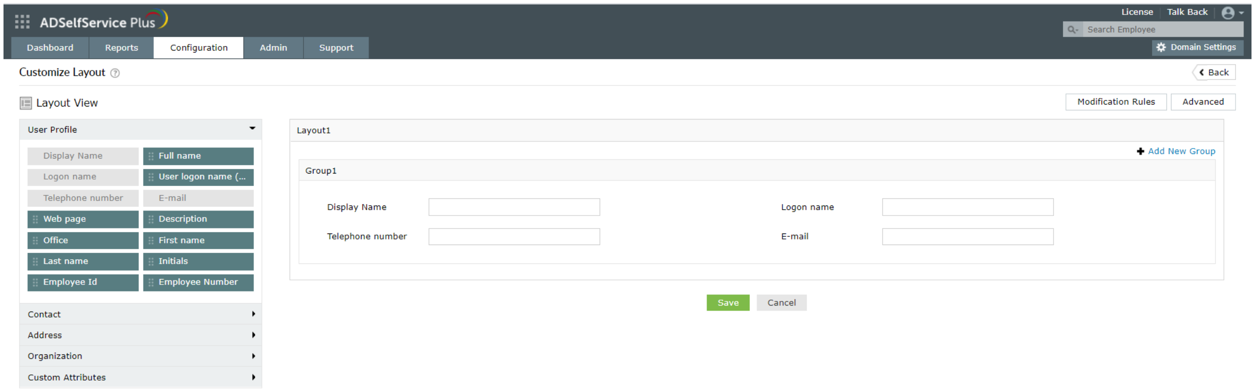
* Client Secret

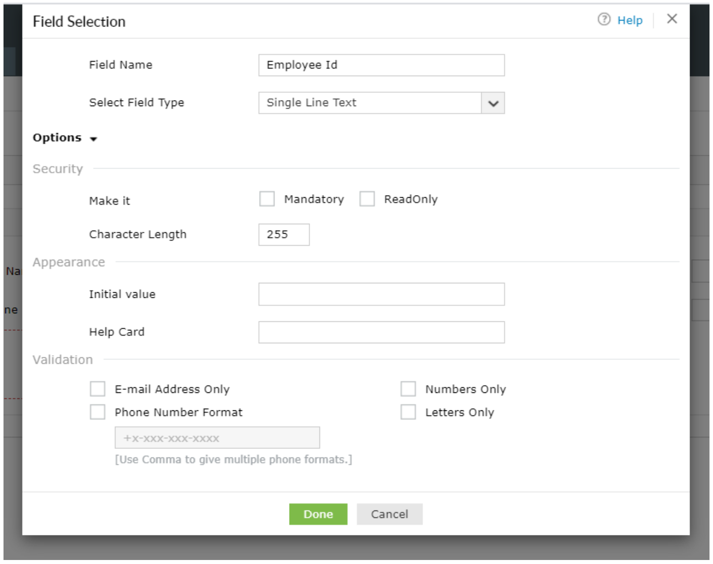
4. Directory self-service deployment

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.





Field Name: Employee Id

Select Field Type: Single Line Text

Make it: □ Mandatory □ ReadOnly

Character Length: 255

Initial value:

Help Card:

□ E-mail Address Only
□ Numbers Only
□ Phone Number Format
□ Letters Only

+x-xxx-xxx-xxxx

[Use Comma to give multiple phone formats.]

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. Learn 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**.

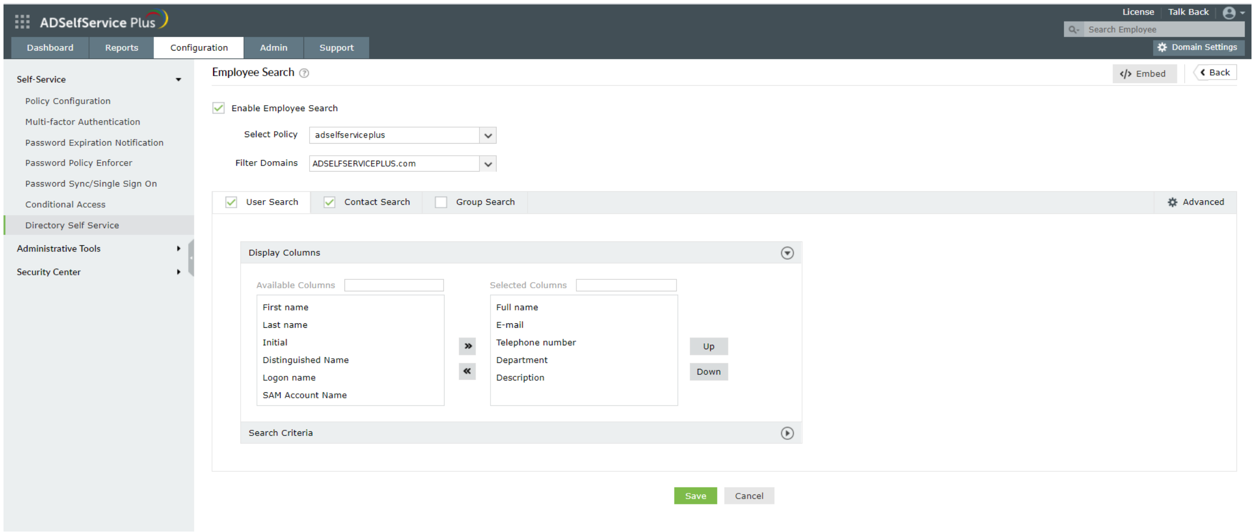
5. Enable the **Users/Contacts/Groups** checkboxes:

   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.



Employee Search

☑ Enable Employee Search

Select Policy: adselfserviceplus

Filter Domains: ADSELFSERVICEPLUS.com

☑ User Search ☑ Contact Search □ Group Search

Display Columns

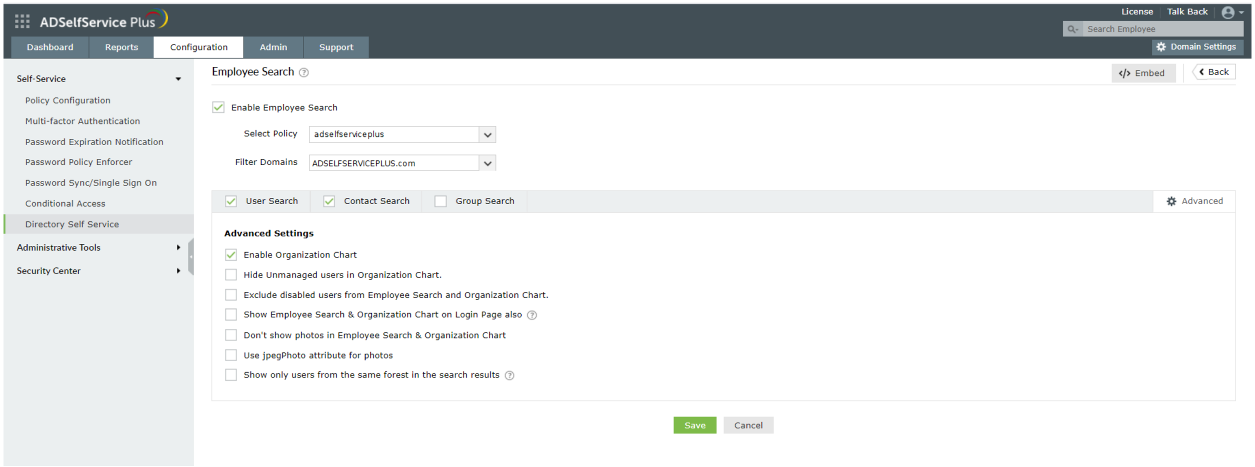
Available Columns	Selected Columns
First name	Full name
Last name	E-mail
Initial	Telephone number
Distinguished Name	Department
Logon name	Description
SAM Account Name	

Search Criteria

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.



Employee Search

☑ Enable Employee Search

Select Policy: adselfserviceplus

Filter Domains: ADSELFSERVICEPLUS.com

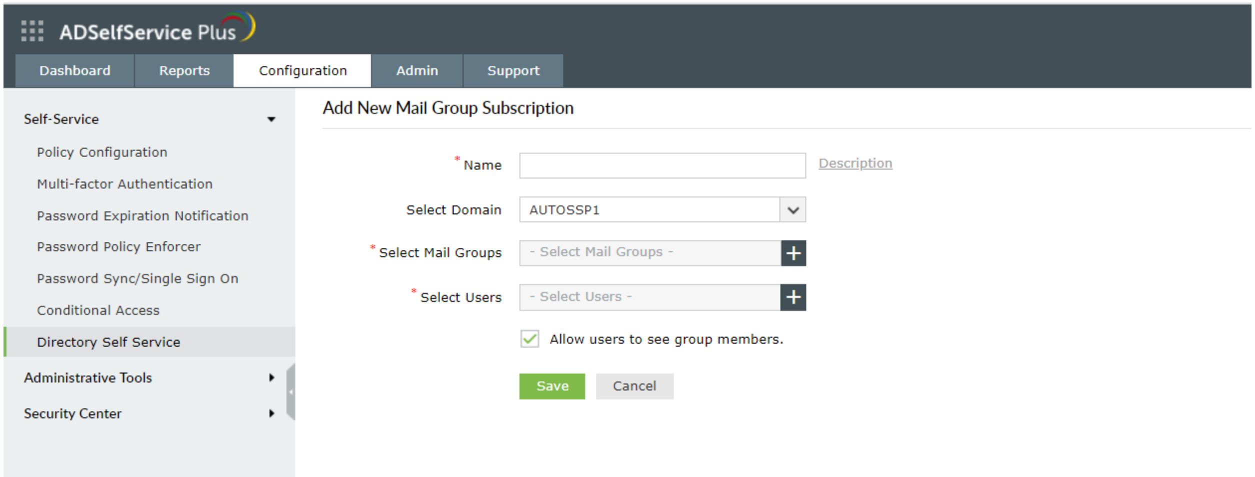
☑ User Search ☑ Contact Search □ Group Search

Advanced Settings

☑ Enable Organization Chart
□ Hide Unmanaged users in Organization Chart.
□ Exclude disabled users from Employee Search and Organization Chart.
□ Show Employee Search & Organization Chart on Login Page also
□ Don't show photos in Employee Search & Organization Chart
□ Use jpegPhoto attribute for photos
□ Show only users from the same forest in the search results

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.**



Add New Mail Group Subscription

*Name:

Select Domain: AUTOSSP1

*Select Mail Groups: - Select Mail Groups -

*Select Users: - Select Users -

☑ Allow users to see group members.

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 admin portal, GPOs, SCCM, third-party endpoint management solutions like ManageEngine Desktop Central, 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 pushed onto the mobile devices by the administrator.

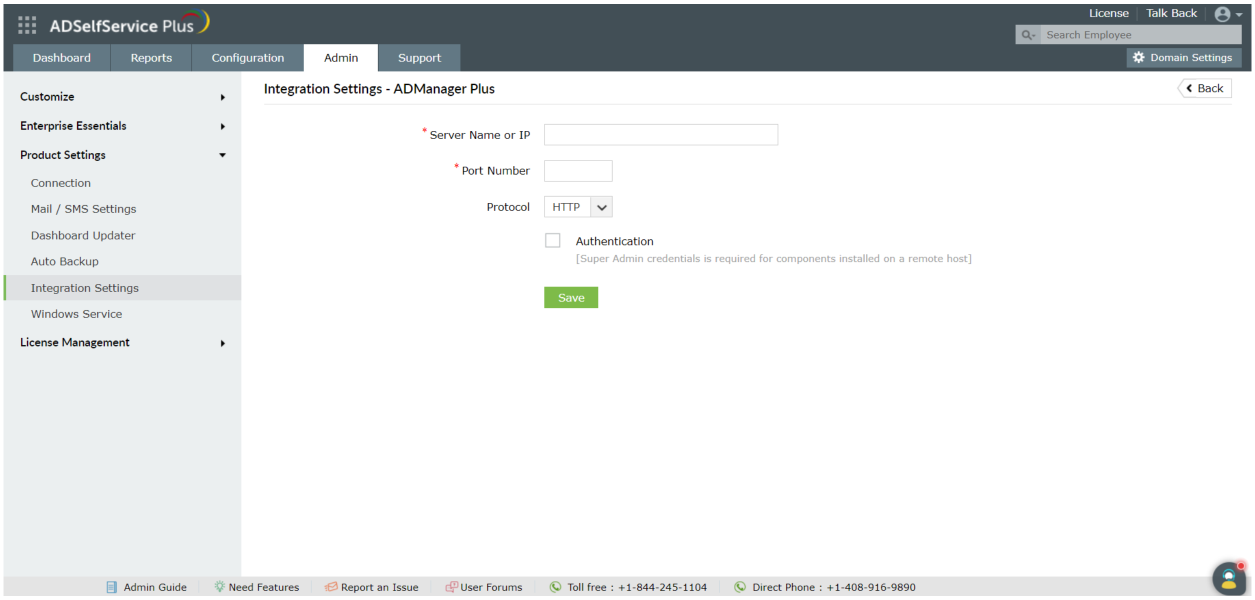
iii. Enterprise application integration

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.



Integration Settings - ADManager Plus

* Server Name or IP

* Port Number

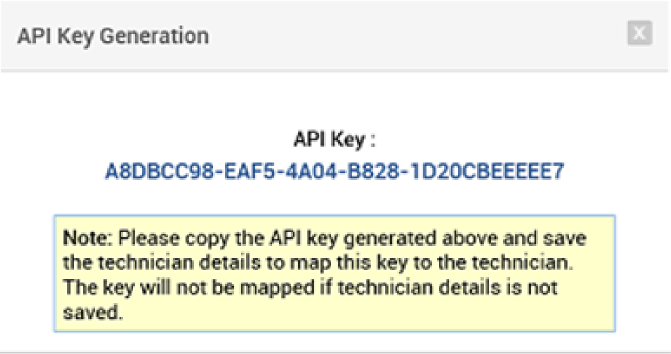
Protocol HTTP

□ Authentication
[Super Admin credentials is required for components installed on a remote host]

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:

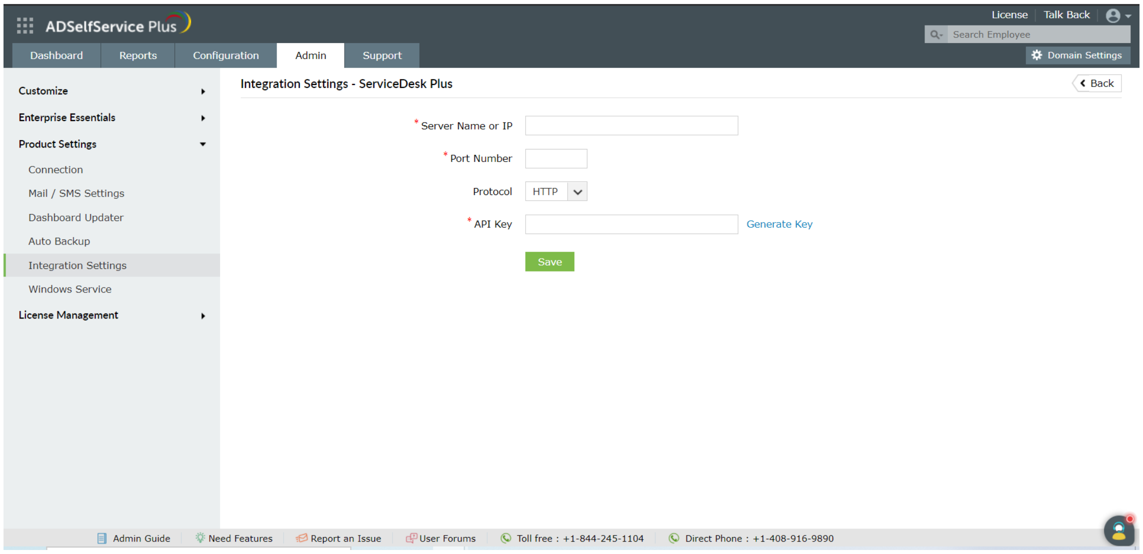
i. Navigate to **Admin** > **Product Settings** > **Integration Settings**.
ii. Click the **ServiceDesk Plus** tile.
iii. In the **Server Name or IP** field, enter the name of the server in which ServiceDesk Plus is installed.
iv. Enter the **Port Number** used by ServiceDesk Plus.
v. Select the **Protocol** (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

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.



Integration Settings - ServiceDesk Plus

* Server Name or IP

* Port Number

Protocol HTTP

* API Key Generate Key

Save

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.

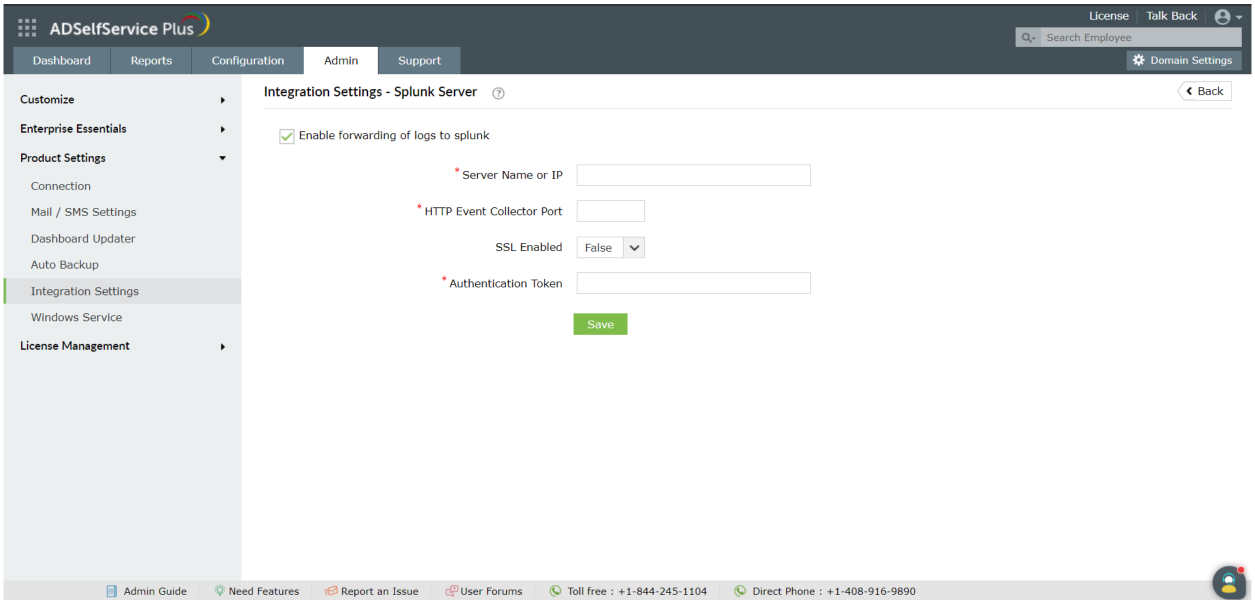
iii. Click **Enable forwarding of logs to splunk**

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**.



Integration Settings - Splunk Server

☑ Enable forwarding of logs to splunk

* Server Name or IP

* HTTP Event Collector Port

SSL Enabled: False

* Authentication Token

Save

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:

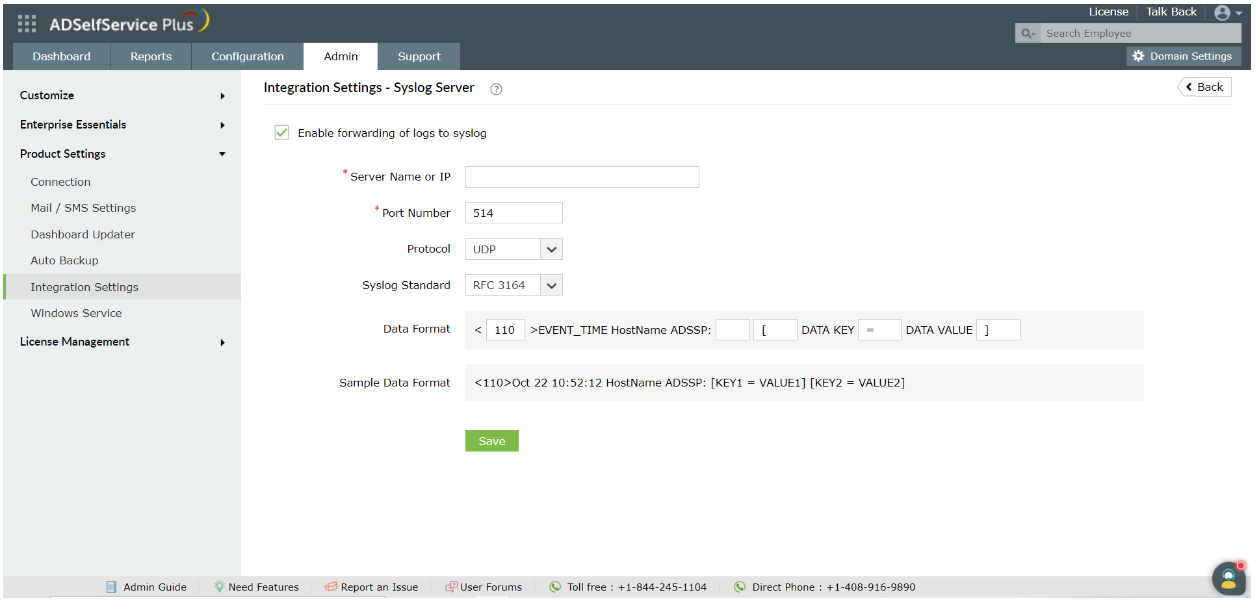
i. Log in to ADSelfService Plus as default Admin.

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.



Integration Settings - Syslog Server

☑ Enable forwarding of logs to syslog

* Server Name or IP	
* Port Number	514
Protocol	UDP
Syslog Standard	RFC 3164
Data Format	< 110 >EVENT_TIME HostName ADSSP: [DATA KEY = DATA VALUE]
Sample Data Format	<110>Oct 22 10:52:12 HostName ADSSP: [KEY1 = VALUE1] [KEY2 = VALUE2]

Save

vi. Click **Save.**

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**

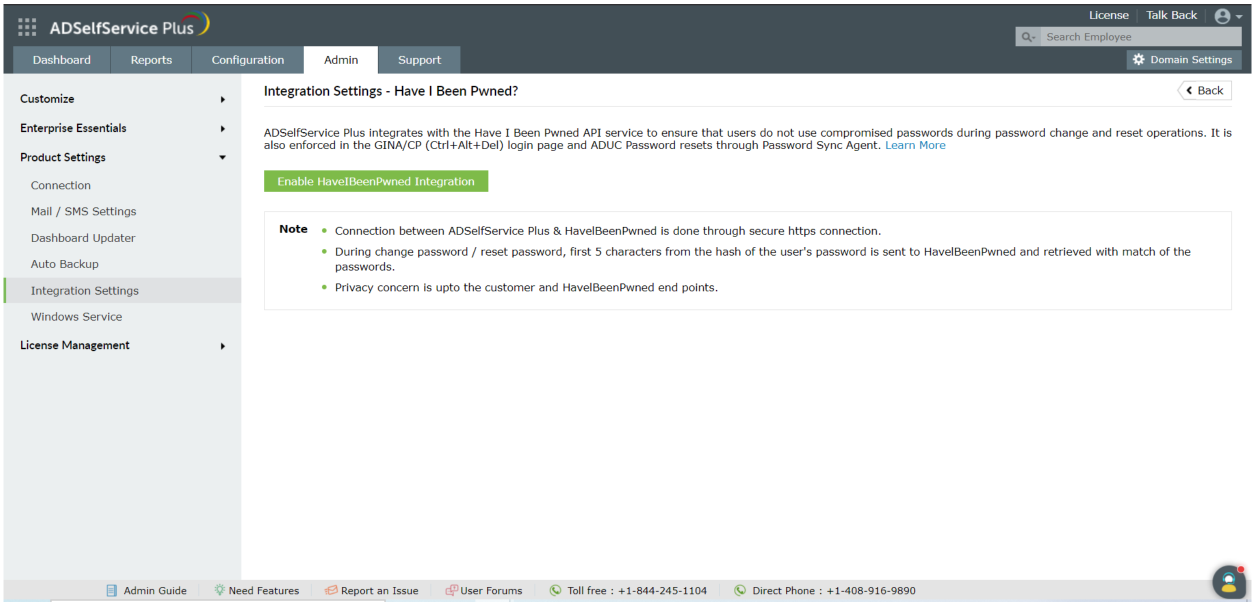
Steps to integrate:

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 HaveIBeenPwned Integration**



Integration Settings - Have I Been Pwned?

ADSelfService Plus integrates with the Have I Been Pwned API service to ensure that users do not use compromised passwords during password change and reset operations. It is also enforced in the GINA/CP (Ctrl+Alt+Del) login page and ADUC Password resets through Password Sync Agent. Learn More

Enable HaveIBeenPwned Integration

Note
- Connection between ADSelfService Plus & HaveIBeenPwned is done through secure https connection.
- During change password / reset password, first 5 characters from the hash of the user's password is sent to HaveIBeenPwned and retrieved with match of the passwords.
- Privacy concern is upto the customer and HaveIBeenPwned end points.

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.

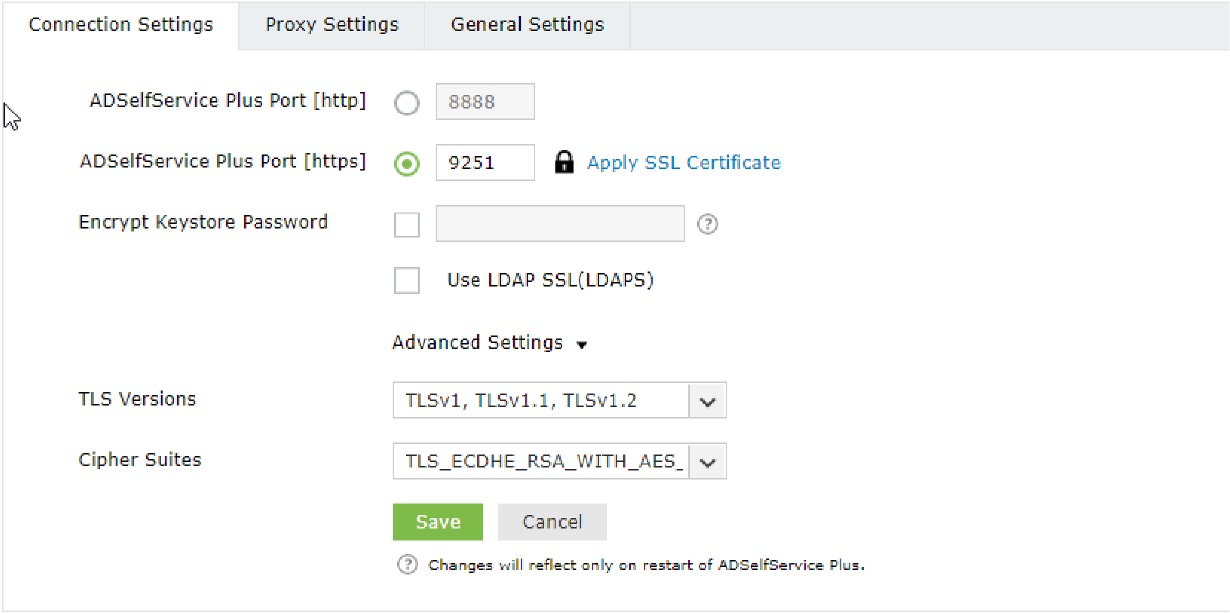
iii. High availability

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 here 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.



ADSelfService Plus Port [http] ○ 8888

ADSelfService Plus Port [https] ● 9251

Encrypt Keystore Password □

□ Use LDAP SSL(LDAPS)

TLS Versions: TLSv1, TLSv1.1, TLSv1.2

Cipher Suites: TLS_ECDHE_RSA_WITH_AES_

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 follow these steps.

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.

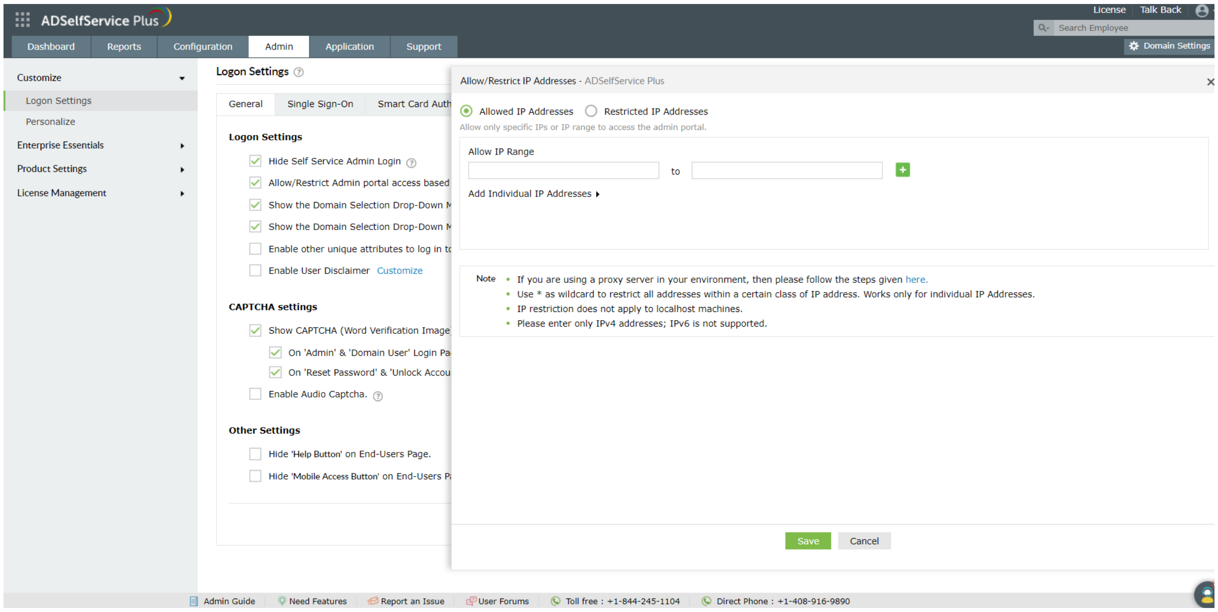
ix. Click **Save**.

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.**



Logon Settings

☑ Hide Self Service Admin Login

☑ Allow/Restrict Admin portal access based

☑ Show the Domain Selection Drop-Down M

☑ Show the Domain Selection Drop-Down M

□ Enable other unique attributes to log in to

□ Enable User Disclaimer Customize

CAPTCHA settings

☑ Show CAPTCHA (Word Verification Image

☑ On 'Admin' & 'Domain User' Login Pa

☑ On 'Reset Password' & 'Unlock Accou

□ Enable Audio Captcha.

Other Settings

□ Hide 'Help Button' on End-Users Page.

□ Hide 'Mobile Access Button' on End-Users Pa

Allow/Restrict IP Addresses - ADSelfService Plus

● Allowed IP Addresses ○ Restricted IP Addresses

Allow only specific IPs or IP range to access the admin portal.

Allow IP Range

to

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 certain 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.

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.

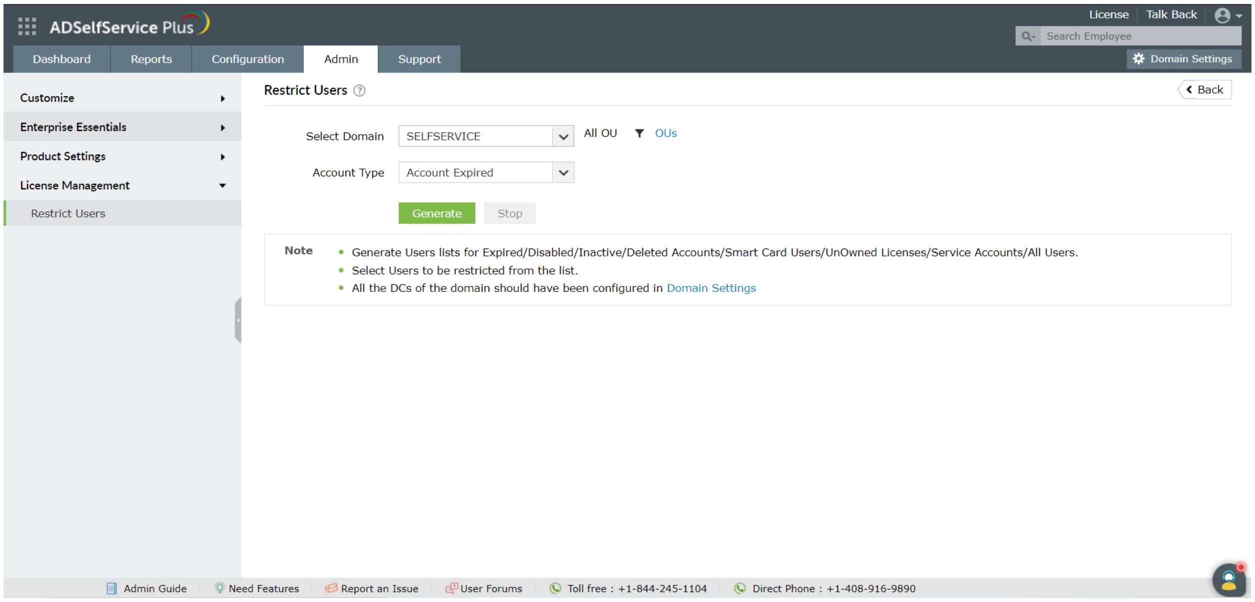
<u>Steps to configure the Restrict Users option:</u>

i. Navigate to **Admin > License Management > Restrict Users.**

ii. Click **Restrict Users** from the right corner of the page.

iii. Select the required **Domain.**

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



Restrict Users

Select Domain: SELFSERVICE — All OU — OUs

Account Type: Account Expired

Generate | Stop

Note

- Generate Users lists for Expired/Disabled/Inactive/Deleted Accounts/Smart Card Users/UnOwned Licenses/Service Accounts/All Users.
- Select Users to be restricted from the list.
- All the DCs of the domain should have been configured in Domain Settings

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.

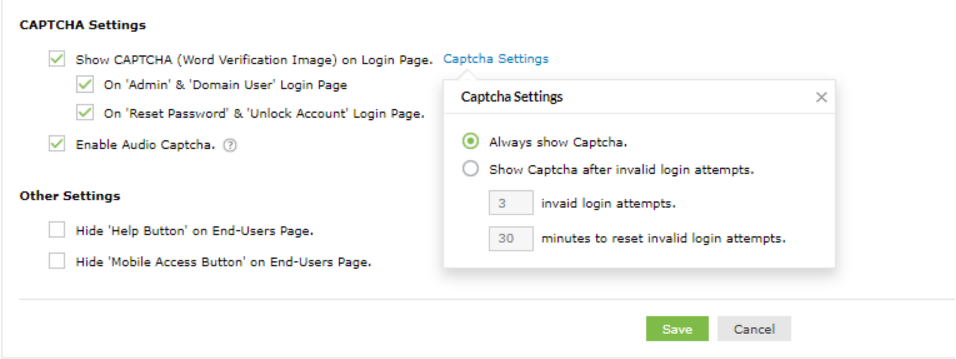
viii. Click **Restrict.**

> 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** → **Customize** → **Logon Settings.**

ii. Select **Show CAPTCHA (Word Verification Image) on Login Page**.



CAPTCHA Settings

☑ Show CAPTCHA (Word Verification Image) on Login Page. Captcha Settings

☑ On 'Admin' & 'Domain User' Login Page

☑ On 'Reset Password' & 'Unlock Account' Login Page.

☑ Enable Audio Captcha.

Other Settings

□ Hide 'Help Button' on End-Users Page.

□ Hide 'Mobile Access Button' on End-Users Page.

Captcha Settings

● Always show Captcha.

○ Show Captcha after invalid login attempts.

3 invaid login attempts.

30 minutes to reset invalid login attempts.

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

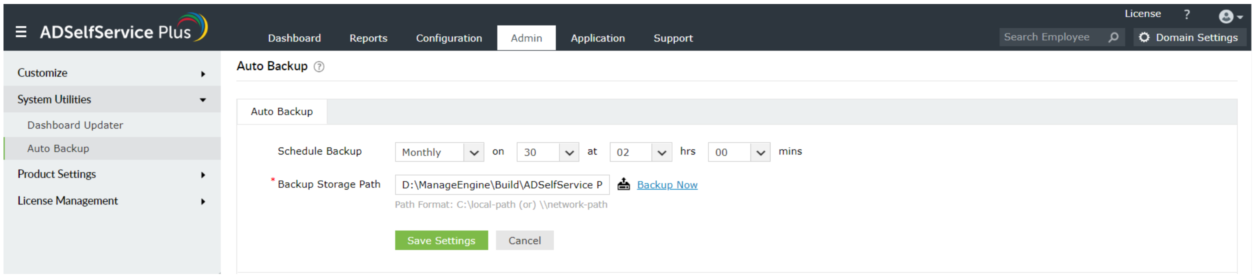
To enable email and SMS notifications for email, or SMS-based verification codes, password expiration notifications, and other product notifications, email and SMS servers need to be configured in ADSelfService Plus. Learn how to configure email and SMS servers.

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**.



Schedule Backup: Monthly on 30 at 02 hrs 00 mins

* Backup Storage Path: D:\ManageEngine\Build\ADSelfService P

Path Format: C:\local-path (or) \\network-path

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:

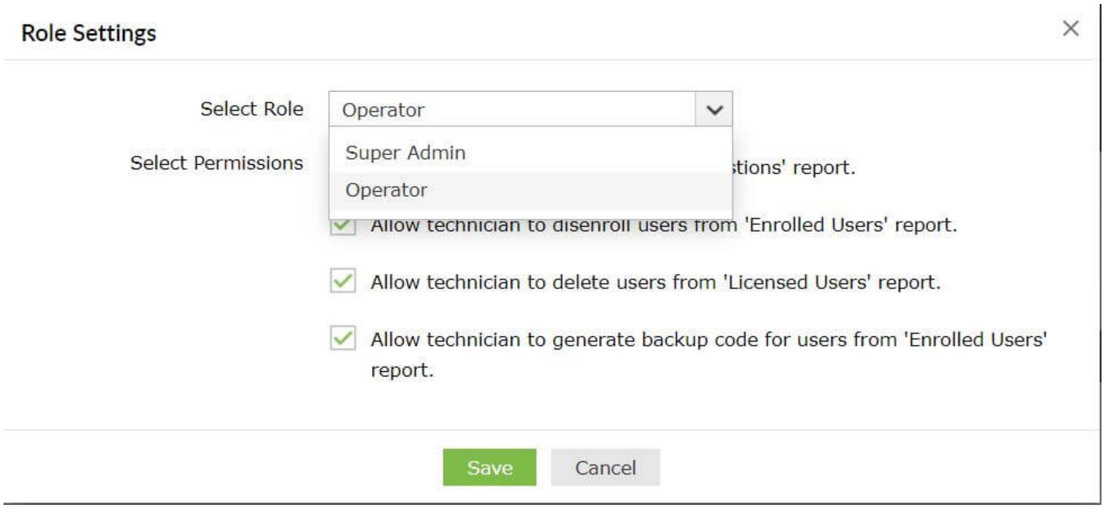
- Super Admin: Up to full control over the entire application by default.
- Operator: Can audit the various operations taking place in the application.

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

Super Admin
Operator

Select Permissions

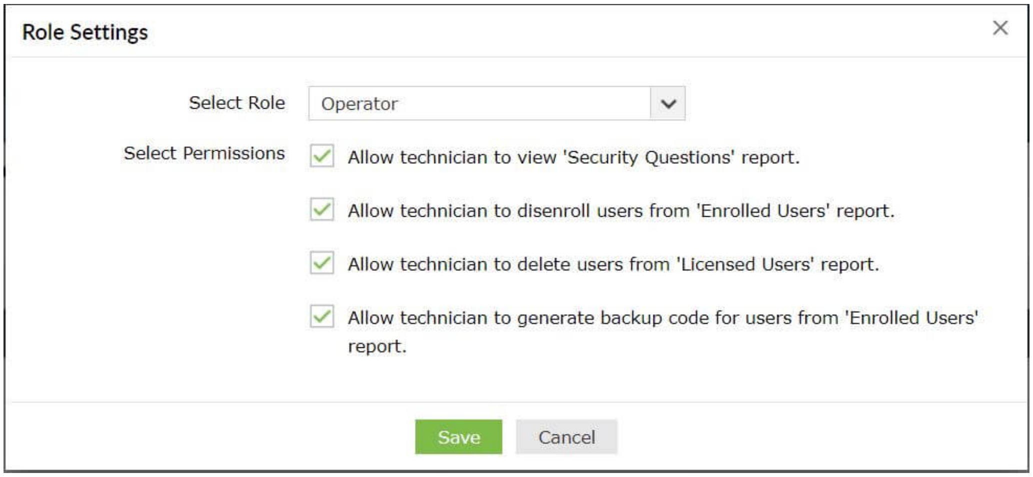
…tions' report.

☑ Allow technician to disenroll users from 'Enrolled Users' report.

☑ Allow technician to delete users from 'Licensed Users' report.

☑ Allow technician to generate backup code for users from 'Enrolled Users' report.

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



Role Settings

Select Role: Operator

Select Permissions

☑ Allow technician to view 'Security Questions' report.

☑ Allow technician to disenroll users from 'Enrolled Users' report.

☑ Allow technician to delete users from 'Licensed Users' report.

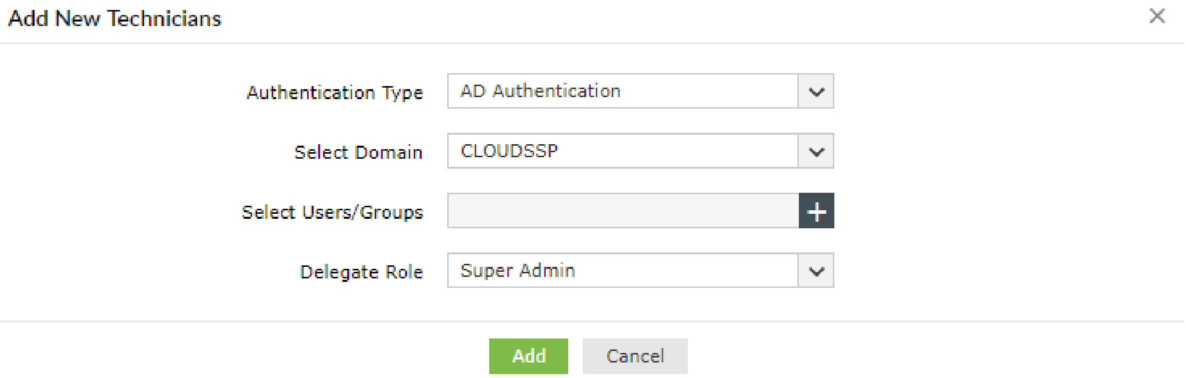
☑ Allow technician to generate backup code for users from 'Enrolled Users' report.

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.

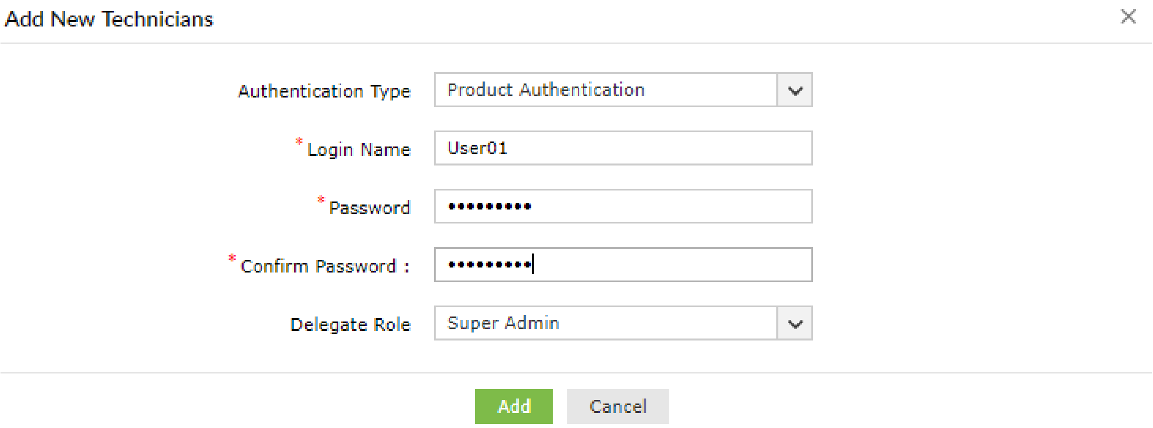


Add New Technicians

Authentication Type	AD Authentication
Select Domain	CLOUDSSP
Select Users/Groups	
Delegate Role	Super Admin

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

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.

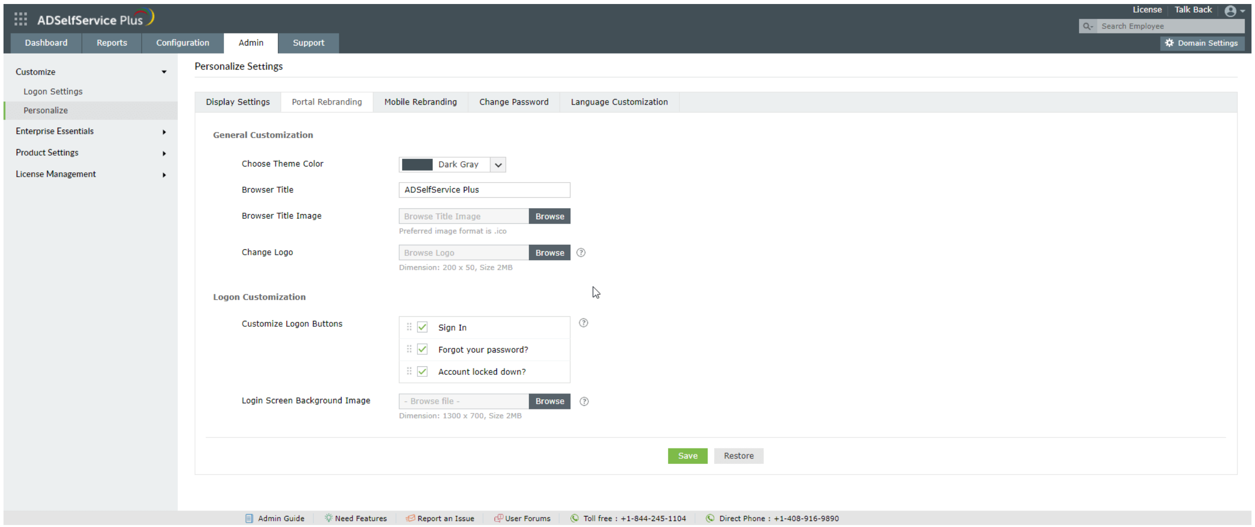
iv. Enter the desired **Browser Title**.

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.**



Personalize Settings

General Customization

Choose Theme Color: Dark Gray

Browser Title: ADSelfService Plus

Browser Title Image: Browse Title Image
Preferred image format is .ico

Change Logo: Browse Logo
Dimension: 200 x 50, Size 2MB

Logon Customization

Customize Logon Buttons:
☑ Sign In
☑ Forgot your password?
☑ Account locked down?

Login Screen Background Image: - Browse file -
Dimension: 1300 x 700, Size 2MB

Toll free : +1-844-245-1104 | Direct Phone : +1-408-916-9890

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/

$ Get Quote

⤓ Download