ManageEngine
ADSelfService Plus

ADSelfService Plus

Evaluator's guide

Table of Contents

Document overview 3

ADSelfService Plus overview 3

Features and benefits 3

- Multi-factor authentication 3
- Conditional access 4
- Enterprise single sign-on 4
- Just-in-time user provisioning 4
- Self-service password reset and account unlock 4
- Password synchronization 4
- Password expiration notification 5
- Password policy enforcer 5
- Self-service directory update 5
- Employee directory search and organization chart 5
- Mail group subscription 5

ADSelfService Plus architecture 6

Roll out ADSelfService Plus 6

1. Password self-service deployment 6
2. Password and endpoint security 10
3. One-identity configuration 21
4. Directory self-service deployment 26
5. Supplementary features 29

Configure security settings in ADSelfService Plus 37

1. Implement failover and secure gateway features: 37
2. Configure SSL and LDAPS 37
3. Allow or restrict admin portal access based on IP addresses 38
4. Set the session expiration time 39
5. Manage product licenses 39

Other important settings 41

1. Configure the dashboard updater 41

2. Configure email and SMS servers for notifications 41
3. Enable auto-backup of the database 41
4. Configure technicians for product administration 42
5. Rebrand and personalize the portal 44

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

ADSelfService Plus is an identity security solution to ensure secure and seamless access to enterprise resources and establish a Zero Trust environment. With capabilities such as adaptive multi-factor authentication, single sign-on, self-service password management, a password policy enhancer, remote work enablement and workforce self-service, ADSelfService Plus provides your employees with secure, simple access to the resources they need. ADSelfService Plus helps keep identity-based threats out, fast-tracks application onboarding, improves password security, reduces help desk tickets and empowers remote workforces. For more information about ADSelfService Plus, visit https://www.manageengine.com/products/self-service-password.

Features and benefits

- ## 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:

- Workstations, servers, Windows, Linux, and macOS machines
- VPN and RADIUS-based access points
- OWA and IIS-based applications
- Internal Windows access points like RDP, machine unlocks, and User Account Control prompts
- Enterprise cloud application logins (via SSO)

The product supports up to 20 authentication techniques including FIDO passkeys, 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.

- ## 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.

- ## Enterprise single sign-on

Reduce the number of logins performed by the user by enabling enterprise SSO for SAML, OAuth, and OIDC 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.

- ## Just-in-time user provisioning

Streamline the user onboarding process by using SCIM-based JIT provisioning for supported enterprise applications.

Benefit: Saves time and eliminates the errors possible in manual and bulk user provisioning by automatically provisioning user accounts during the time of access.

- ## 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.

- ## 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.

- ## 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.

- ## 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.

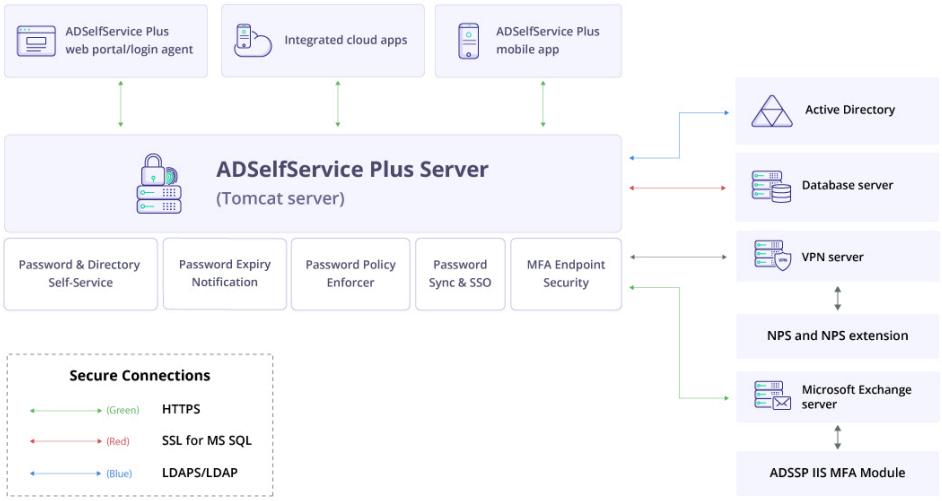
- ## Employee directory search and organization chart

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

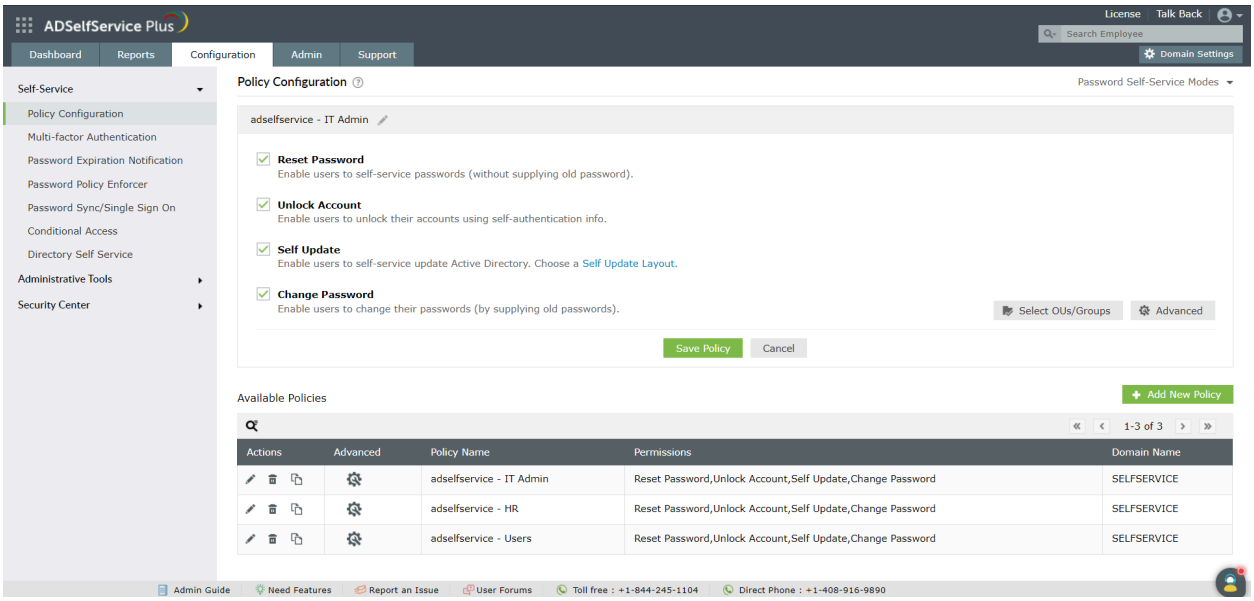
1. Password self-service deployment

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.



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 machine (Windows, macOS, and Linux) login screens. ADSelfService Plus also offers identity verification by MFA for local and remote logins into machines, VPN, OWA, and cloud applications. The MFA process relies on the information provided by users during enrollment with ADSelfService Plus. Here are the authentications methods supported by ADSelfService

Plus for MFA:

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

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.
- **Forced 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). Additionally, you can enable the cached credentials update to ensure that remote users can also reset their passwords from their login screens and regain access to their systems.
- **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 machines (Windows, macOS and Linux), VPN, OWA logins using 18 authentication methods.

Note: Endpoint MFA is required to access these features. Visit the store to purchase the feature.

MFA for machines

ADSelfService Plus' MFA for machines feature can be enabled in two ways:

- User-based MFA: Login attempts into any integrated machine by the specific user will be secured using MFA.
- Machine-based MFA: Logins and other access attempts like machine unlocks by any user into the specific machine will be protected by MFA.

Windows machines can be secured by:

- Online MFA: The default or online MFA process in ADSelfService Plus uses a network connection between the ADSelfService Plus server and user machines to verify the identity of users based on the authenticator data registered in the ADSelfService Plus server.
- Offline MFA: To ensure identity security even in the absence of a proper network connection or communication with the ADSelfService Plus server, offline MFA verifies the user identity with the authenticator data securely stored in the user machine by the Windows login agent. Offline MFA can be used to secure Windows and macOS logins, and other peripheral actions related to

Windows (UAC prompts, RDP server authentication, and machine unlocks).

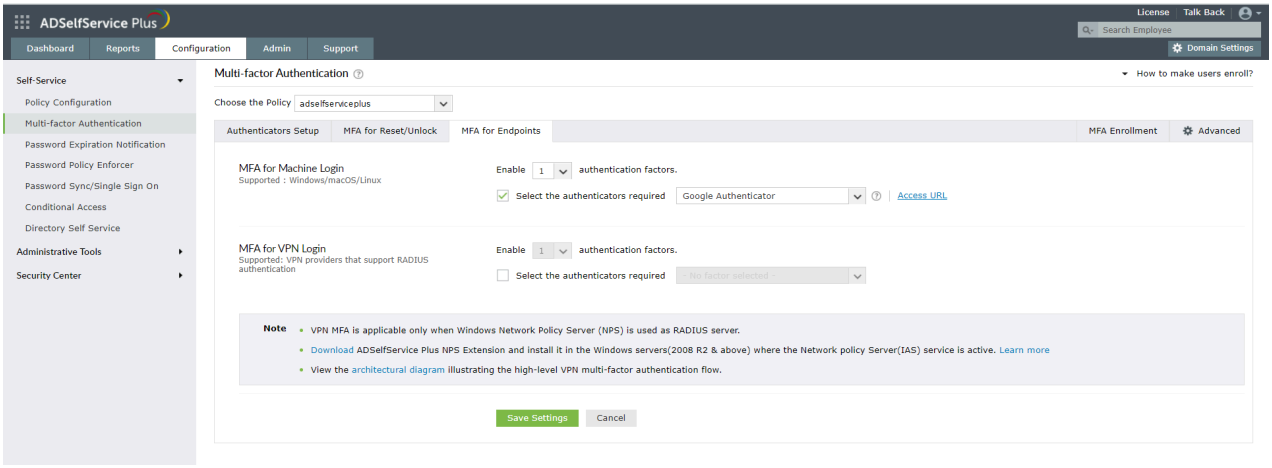
Prerequisites

- Endpoint MFA for ADSelfService Plus is required to enable the MFA for machine logins feature. Professional edition of ADSelfService Plus with Endpoint MFA is required to enable offline MFA.. Visit the store to purchase Endpoint MFA.
- **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.
- The access URL must be set to **HTTPS**. Navigate to **Admin** > **Product Settings** > **Connection** > **Connection Settings** > **Configure Access URL** and set the **Protocol** option to **HTTPS**.
- **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.
- Offline MFA is supported for Windows machines (except Windows 10 version 1803) and macOS logins. For remote logins, offline MFA is not supported for RDP client authentication.
- Please make sure that the login agent installed on your machines meets the required version: version 6.3 or above for Windows, and version 3.0 or above for macOS. If not, update the agent to the latest version by following these steps. If you have not installed the login agent yet, please configure offline MFA before doing so to ensure that the changes are updated.

Steps to enforce user-based MFA:

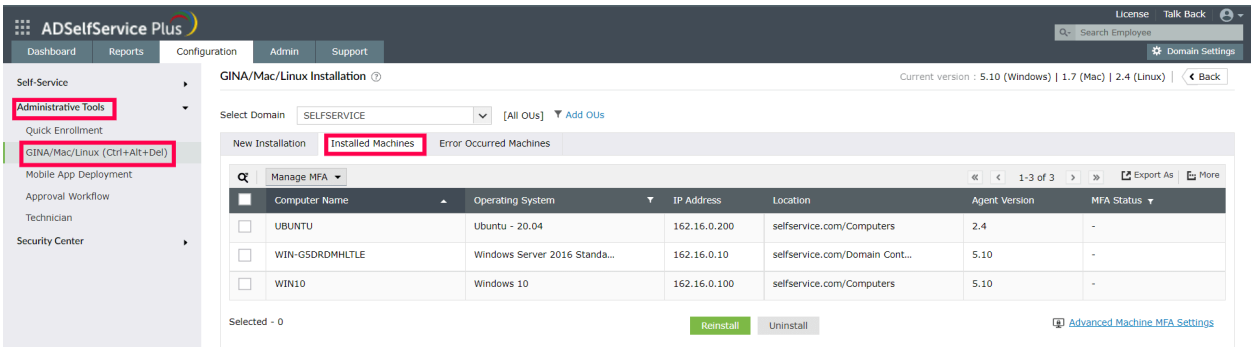
1. Go to **Configuration > Self-Service > Multi-factor Authentication > MFA for Endpoints**.
2. Select a policy from the **Choose the Policy** drop-down. This will determine which authentication methods are enabled for which sets of users.
3. In the **MFA for Machine Login** section, check the box next to **Enable authenticators**, enter the number of authentication methods to be enforced and select the authentication methods from the drop-down.
4. Select the **Choose Authenticators for Offline Machine Login MFA** option and select the authentication methods you prefer for offline MFA from the drop-down. The following authenticators are supported:
    a. Google Authenticator
    b. Microsoft Authenticator
    c. Custom TOTP
    d. Zoho OneAuth TOTP

5. Click **Save Settings**.

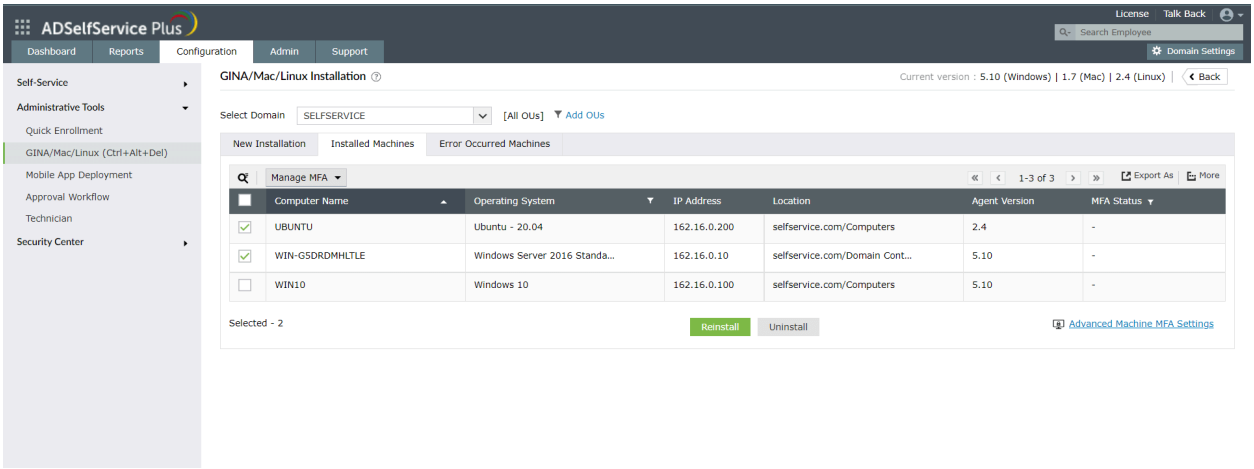


<u>Steps to enable machine-based MFA:</u>

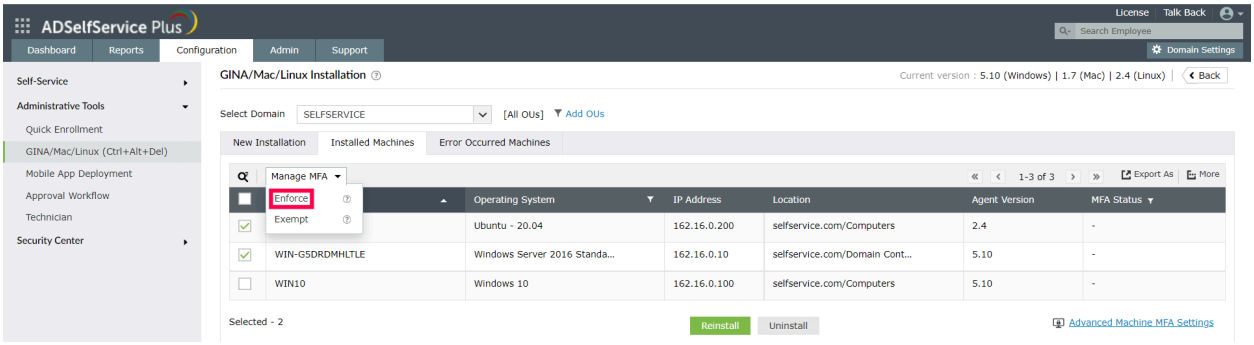
1. Complete steps 1 to 4 under Steps to enable user-based MFA
2. Navigate to **Configuration** > **Administrative Tools** > **GINA/Mac/Linux (Ctrl+Alt+Del)** > **GINA/Mac/Linux Installation** > **Installed Machines**.



3. Select the required domain from the drop-down list.
4. Select the machines for which you want to enforce Machine-based MFA.



5. Click **Manage MFA** and select **Enforce**.



To enable MFA for other peripheral access points, go to **Advanced Machine MFA Settings** and select the required options from the following:

- **Enable MFA for User Account Control**: When this setting is enabled, MFA will be prompted for all UAC credential prompts and the user will be able to perform the action only upon successful identity verification.
- **Enable MFA for RDP**: The admin can configure MFA to be prompted while establishing connections with machines through the RDP. The feature has the following options:
    - RDP server authentication: When this setting is enabled, all incoming remote desktop connections to Windows machines where the ADSelfService Plus login agent is installed will be authenticated and protected using MFA.
    - RDP client authentication: This setting can be enabled to prompt MFA for all outgoing remote desktop connections via the Windows Remote Desktop application (mstsc.exe) in machines where the ADSelfService Plus login agent is installed.
- **Enable MFA when unlocking Windows machine**: This setting will prompt MFA while unlocking a Windows machine.

MFA for VPN

Prerequisites:

- 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

Firstly, you need to decide which MFA mode you wish to use to configure VPN MFA. You can select either **VPN Client Verification** or **SecureLink Email Verification**, depending on the authenticators and type of MFA prompts you want to use:

a. VPN Client Verification
   - Select **VPN Client Verification** to present users with MFA prompts directly from the VPN client during the login process.
   - If your VPN supports the RADIUS challenge prompts, then ADSelfService Plus authenticators like TOTP Authentication, Microsoft Authenticator, YubiKey Authenticator, Zoho OneAuth TOTP, and one-way authenticators like Push Notification Authentication or Biometric Authentication can be selected for VPN MFA.
   - If your VPN does not support RADIUS challenge prompts, one-way authenticators like Push Notification Authentication or Biometric Authentication can be selected for VPN MFA.

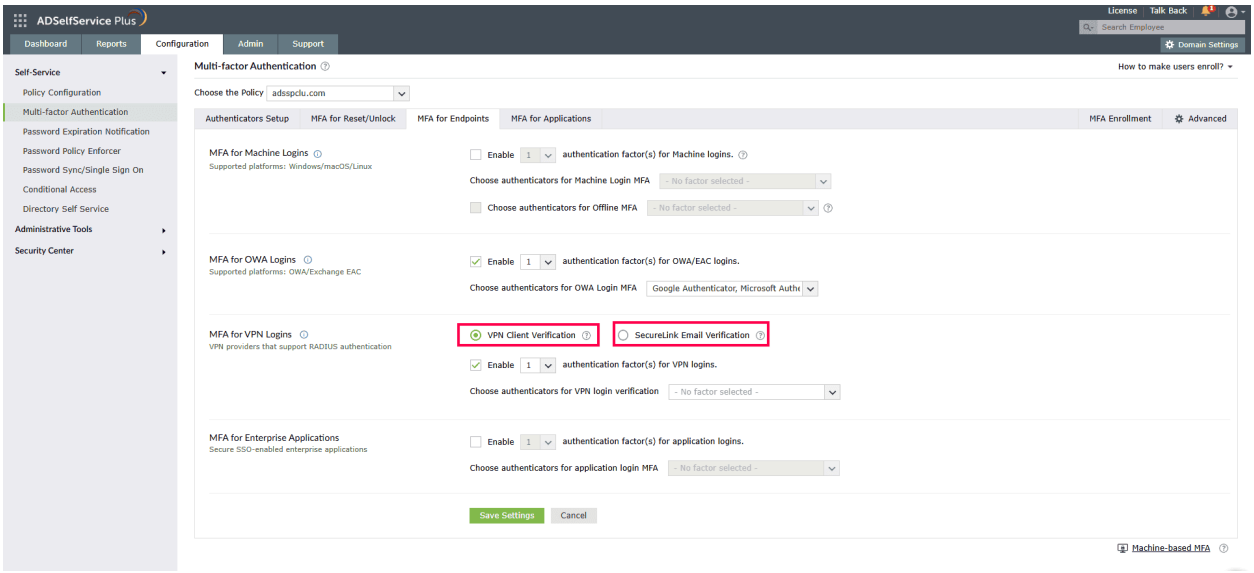
b. SecureLink Email Verification
   - Select **SecureLink Email Verification** to secure VPNs using any authenticator supported by ADSelfService Plus, including authenticators that are not supported by the VPN client, such as FIDO Passkeys or Smart Card Authentication.
   - When this method is selected, the user will receive a verification link in their mailbox that they need to click to verify their identity.

Step 2: Enable MFA for VPN and RADIUS-supporting endpoints 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 determines the users for whom MFA for VPN and endpoint logins are enabled. To learn more about creating an OU- or group-based policy, click here.
4. In the **MFA for VPN Logins** section, select **VPN Client Verification** or **SecureLink Email**

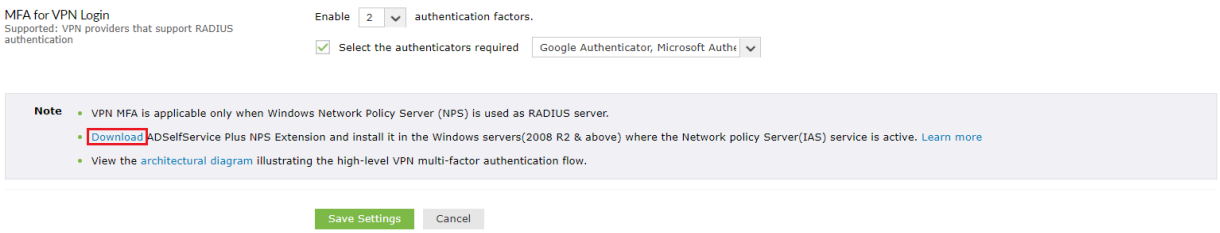
Verification, depending on the MFA mode decided upon previously.

5. Click the check box next to **Select the authenticators required**.
6. Choose the number of authentication factors to be enforced.
7. Select the authentication methods to be used. The authentication methods listed can also be rearranged by dragging and dropping them in the necessary positions.
8. Click **Save Settings**.



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.



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, <operation> can be 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.

MFA for OWA

Prerequisites:

- Ensure that the product is using only HTTPS protocol.
- The ADSelfService Plus SSL certificate should be installed in the Exchange Server.

Step 1: Configuring MFA for OWA

1. Go to **Configuration** > **Self-Service** > **Multi-factor Authentication** > **MFA for OWA Login**.
2. Click the **Choose the Policy** drop-down and select a policy. This will determine which authentication methods are enabled for which sets of users. To learn more about creating an OU or a group-based policy, click here.
3. In the **MFA for OWA Login** section, check the **Enable __ authentication factor** box, select the number of authentication methods, and specify which ones you'd like to use from the drop-down. **Note**: SAML authenticator is not supported in MFA for OWA.
4. Click **Save Settings**.

Step 2: Install ADSelfService Plus MFA Connector

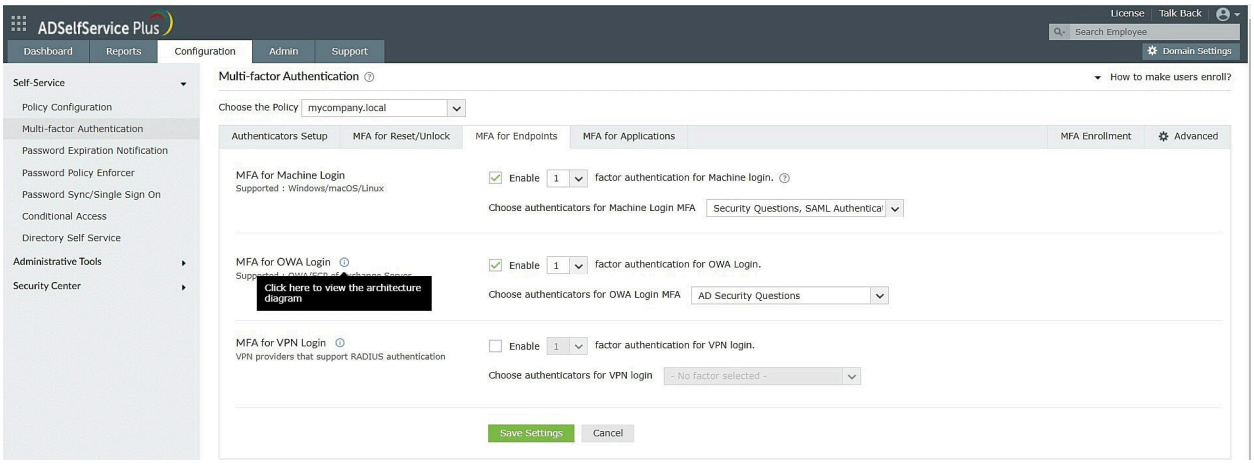
The IIS MFA extension must be installed in Exchanger Server to enable MFA for OWA and Exchange admin center logins. It triggers the request for the completion of other authentication factors after the primary password authentication is successful.

1. Go to **Configuration** > **Self-Service** > **Multi-factor Authentication** > **MFA for Endpoints**.
2. Navigate to **MFA for OWA** and click on the **help** icon.
3. Download the ADSelfService Plus MFA Connector from the pop-up that appears.
4. Copy the extension file (**AdsspOWAIISModule.zip**) to the Windows server that you have configured as the Exchange server. Extract the ZIP file's content and save it in a location.
5. Open PowerShell (x64) as an administrator and navigate to the folder where the content of the extension files is located.
6. Execute the following command:

   PS C:\> .\setupIISMFAModule.ps1 Install

Uninstall and update ADSelfService Plus MFA Connector

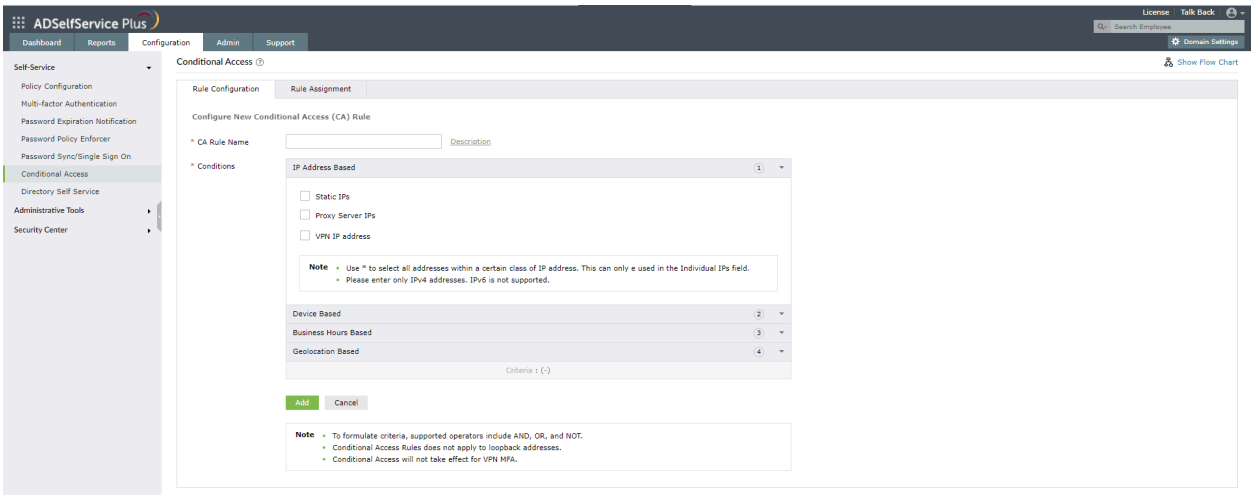
1. Open PowerShell (x64) as an administrator and navigate to the folder where the content of the extension files content is located (by default, it is stored in ***C:\Program Files\ManageEngine\ADSelfService Plus MFA Connector***).
2. To uninstall the extension, execute the following command:
   PS C:\> .\setupIISMFAModule.ps1 Uninstall
3. To update the extension, execute the following command:
   PS C:\> .\setupIISMFAModule.ps1 Update



ii. Configure conditional access

Rule configuration

1. Log in to ADSelfService Plus as an admin.
2. Navigate to **Configuration > Self-Service > Conditional Access > Rule configuration**.
3. Click **Configure New Conditional Access (CA) Rule**.
4. Enter the **CA Rule Name** and **Description**.
5. Select the **Conditions** from **IP Address**, **Device**, **Business hours, Geolocation** based on your requirement.
6. A **Criteria** is automatically created with the conditions you have enabled. If the created criteria matches your requirements, you do not have to make any changes to it. Modify them only if you are sure that they still do not satisfy your requirements. 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. Click **Configure**.



Rule assignment

1. Go to **Configuration > Self-Service > Conditional Access > Rule assignment**.
2. Select the rule that you want to assign from the drop-down.
3. Select the policy to which you want to assign this rule.

   Note: This refers to the self-service policy that you can configure by going to Configuration > Self-Service > Policy Configuration. To learn more, refer to this page.

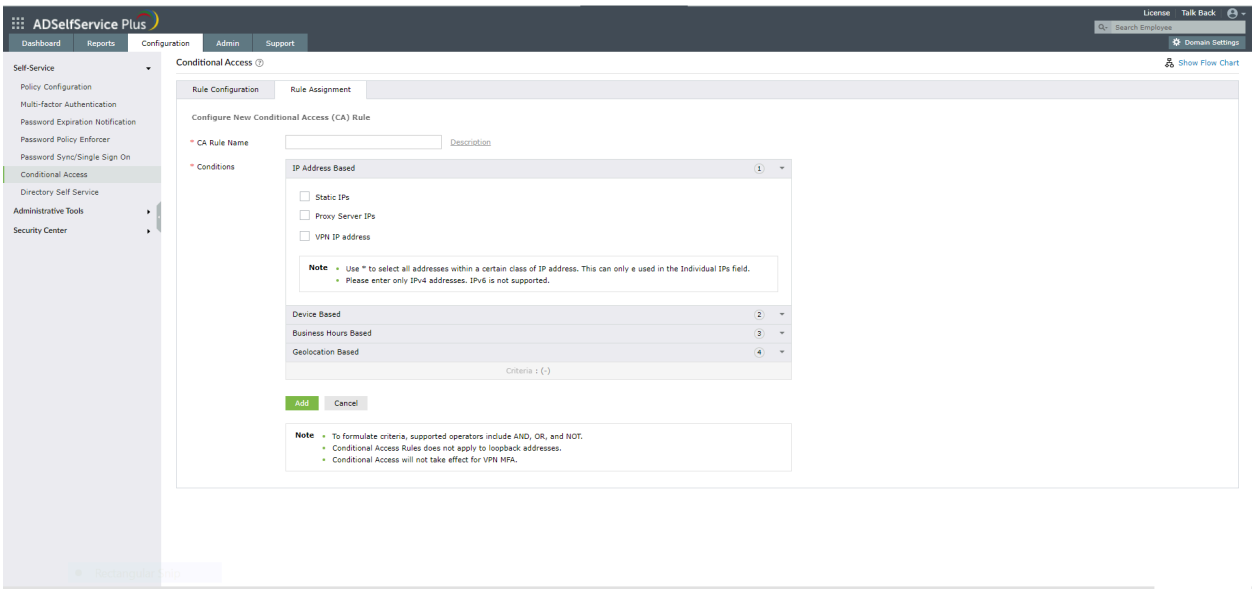
   It is important to note that the selected policy will be applicable to a user only if:

   i. The user satisfies the rule.

   ii. The user is included in the selected policy.

   Example: Consider three self-service policies, A, B, and C, and two conditional access rules, 1 and 2. Assume a user belongs to policies A and B. Let's say both policies A and C are assigned to rule 1. If a user satisfies rule 1, then only policy A will be assigned to the user as he belongs only to policy A.
4. Next, allow or block NTLM single sign-on and ADSelfService Plus portal access. These settings will be applicable wherever the selected rule is satisfied.

   Note: The option to allow or block NTLM single sign-on will be enabled only if NTLM authentication is configured in logon settings.

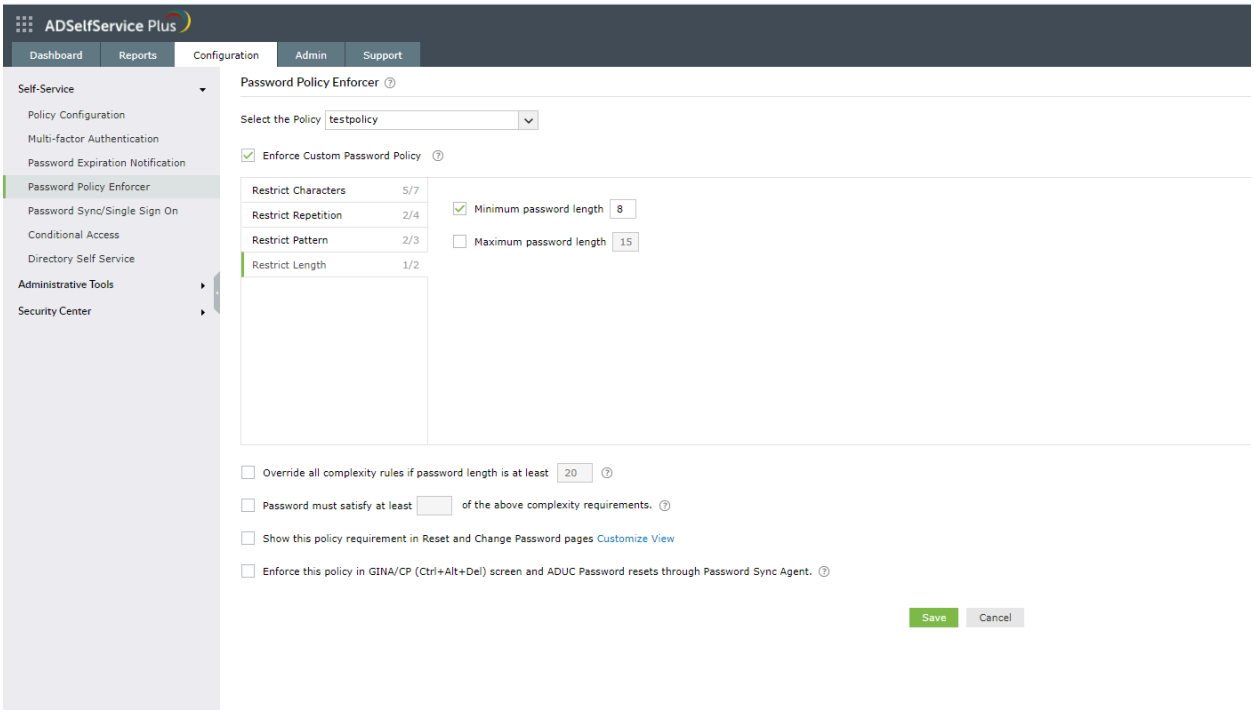


iii. Configure password policies

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. Use Regular Expressions (regex) to enforce advanced password policies tailored to your organization's needs. Select **Password should meet the given regex pattern**, enter a suitable regex in the text box, and align it with your password policy. Learn more about structuring regex patterns
    - **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**.

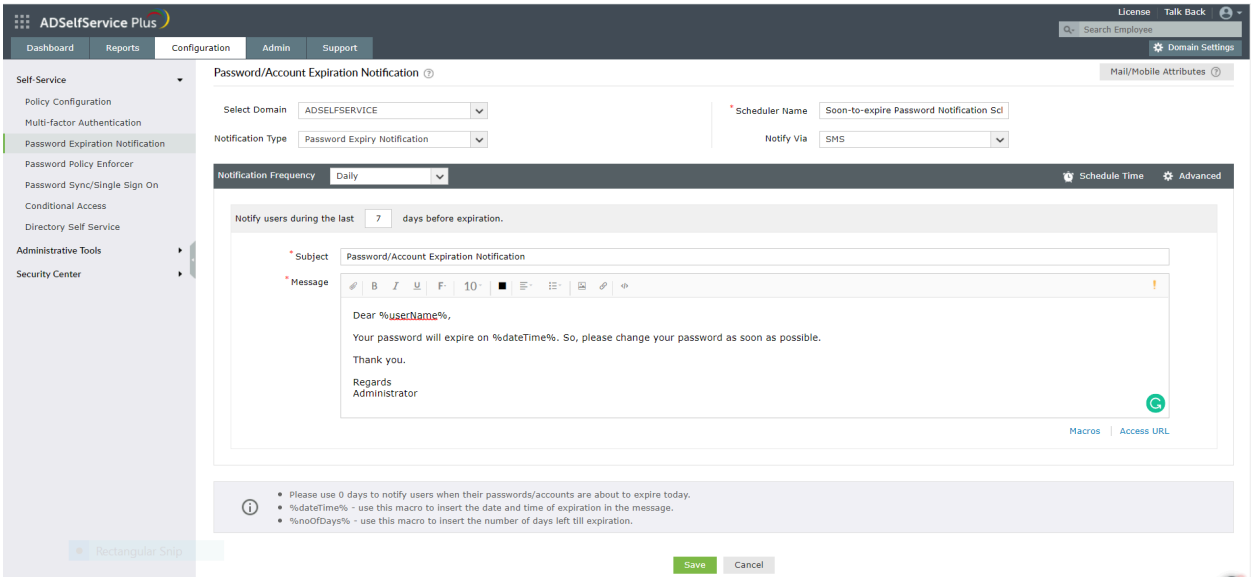


iv. Implement password expiration notifications

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



3. One-identity configuration

i. Implement enterprise single sign-on

ADSelfService Plus provides out-of-the-box SSO support for more than 100 enterprise applications based on SAML, OAuth, and OIDC protocols. It can also be used to enable SSO for custom applications. To configure SSO for applications:

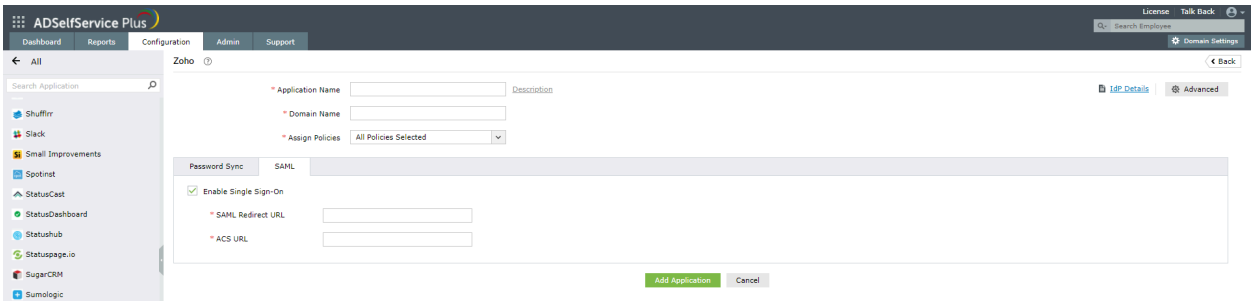
1. Navigate to **Configuration > Self-Service > Password Sync/Single Sign On > Add Application**, and select the desired application.
2. Click **IdP details** in the top-right corner of the screen.
3. In the pop-up that appears, copy the required URLs displayed and download the certificate or metadata 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.

From here depending on the type of application the steps vary as shown below:

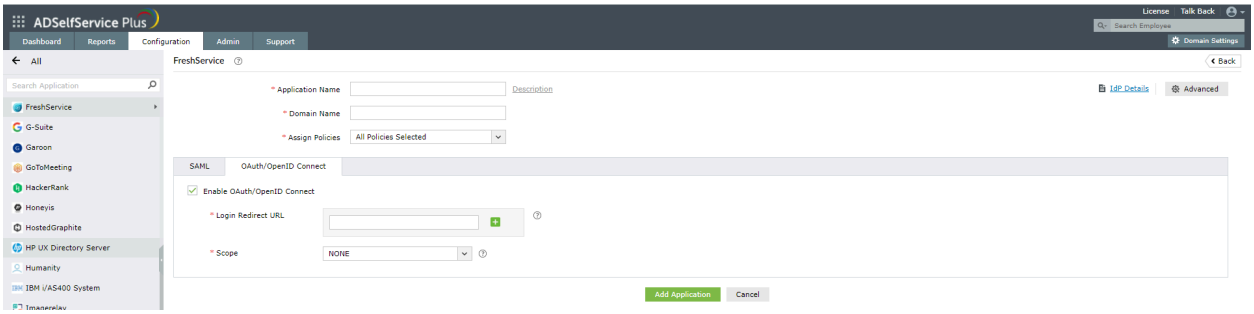
For SAML applications:

1. Go to **SAML.** Select **Enable Single Sign-On.**
2. Provide other information as required and click **Add Application.**



For OAuth/OpenID Connect applications:

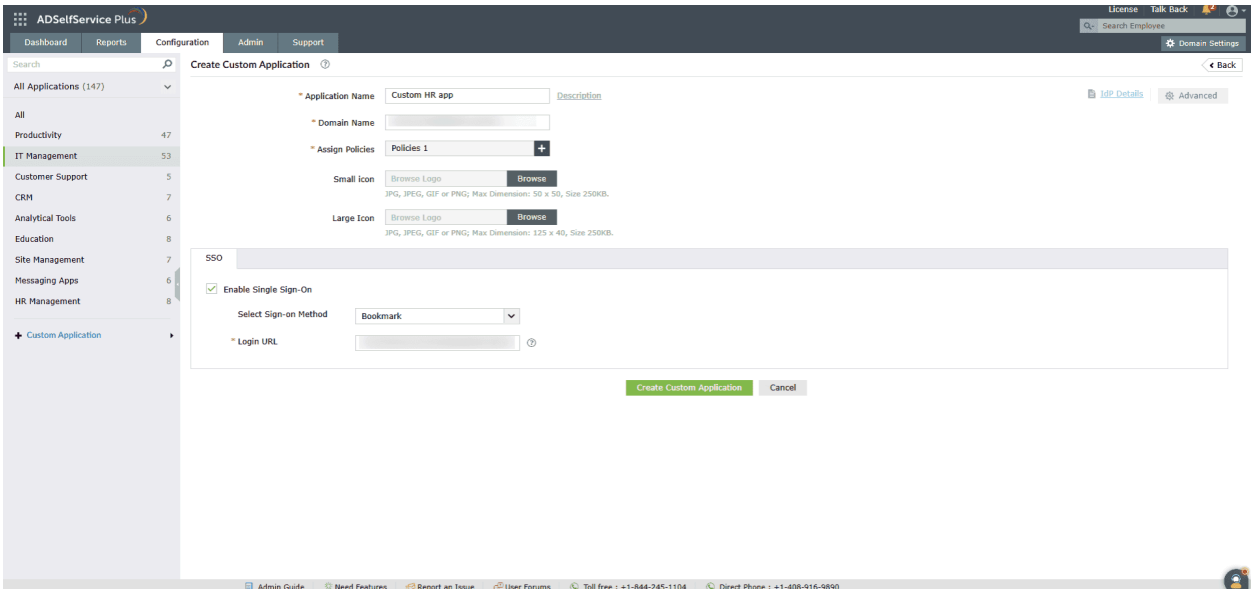
1. Go to **OAuth/OpenID Connect.** Select **Enable OAuth/OpenID Connect**.
2. Provide other information as required and click **Add Application.**



Bookmarking applications:

The Bookmark functionality allows admins to bookmark an application that does not support SSO, providing a convenient way to integrate their in-house or third party applications which do not support protocols—like SAML, OAuth, or OIDC—into the user portal.

1. Log in to ADSelfService Plus as an administrator.



2. Navigate to **Password Sync/Single Sign On** > **Add Application** > **Custom Application**.
3. Enter your **Application Name** and **Description**.
4. Upload an image for the app icon in both sizes.
5. From the *Select Sign-on Method* drop-down, select **Bookmark**.
6. Enter the app's login URL in the **Login URL** field.

Once the bookmark is configured, users can just click the application in the user portal, and it will lead them to the login page of the app. They must then authenticate using the credentials with which they registered on the app.

ii. Enable passwordless authentication for cloud applications

Prerequisites**:**

Enable HTTPS in ADSelfService Plus (go to Admin > Product Settings > Connection).

Step 1: Enable MFA for cloud applications

1. Go to **Configuration** > **Self-Service** > **Multi-Factor Authentication** > **MFA for Endpoints**.
2. 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.
3. In the **MFA for Cloud Applications Login** section, check the box next to **Enable authenticators**, enter the number of authentication methods to be enforced and select the authentication methods from the drop-down.

4. Click the asterisk (*) symbol next to the authentication method to set it as mandatory. You can also reorder the authenticators.

Note: When a user attempts to access an SSO-enabled application directly, this MFA process is triggered.

5. Click **Save Settings**.

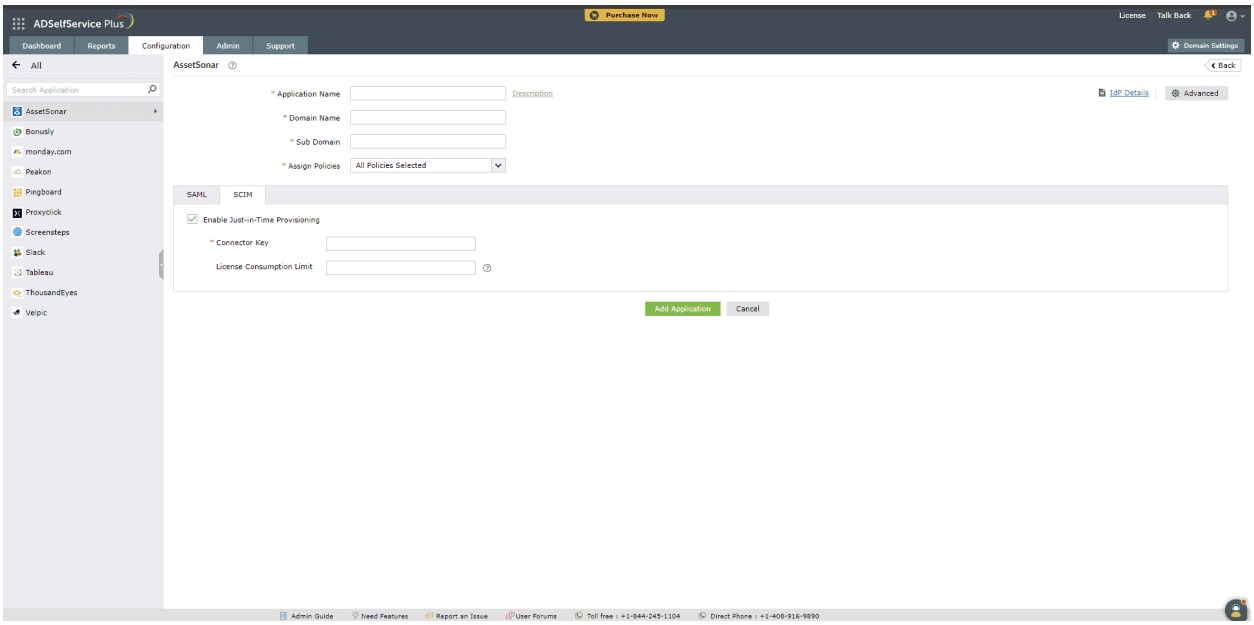
Step 2: Enable passwordless login

1. Go to **Configuration** > **Self-Service** > **Multi-Factor Authentication** > **Advanced** > **Applications MFA**.
2. Check the box next to **Enable Passwordless Login** under ADSelfService Plus login MFA.
3. Click **Save Settings**.

iii. Configure JIT user provisioning

ADSelfService Plus supports SCIM-based JIT user provisioning for more than 10 enterprise applications. To configure the feature:

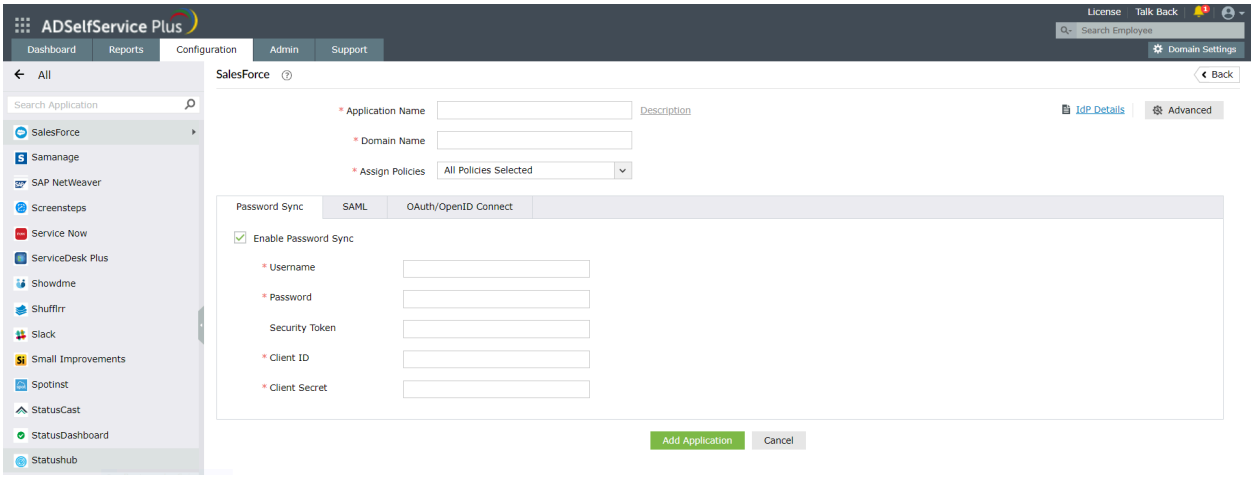
1. Navigate to **Configuration** > **Self-Service** > **Password Sync/Single Sign On/JIT Provisioning** > **Add Application**, and select the enterprise application required.
2. Enter the **Application Name** and **Description**.
3. Enter the **Domain Name** used in the enterprise application.
4. In the **Assign Policies** field, choose the self-service policies for which you want the application to be assigned.
5. Click **SCIM** and select **Enable Just-in-Time Provisioning**.
6. Enter the information required.
7. Set the maximum number of licenses you want to be consumed in this application using the **License Consumption** field.
8. Click **Add Application**.



iv. 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**.

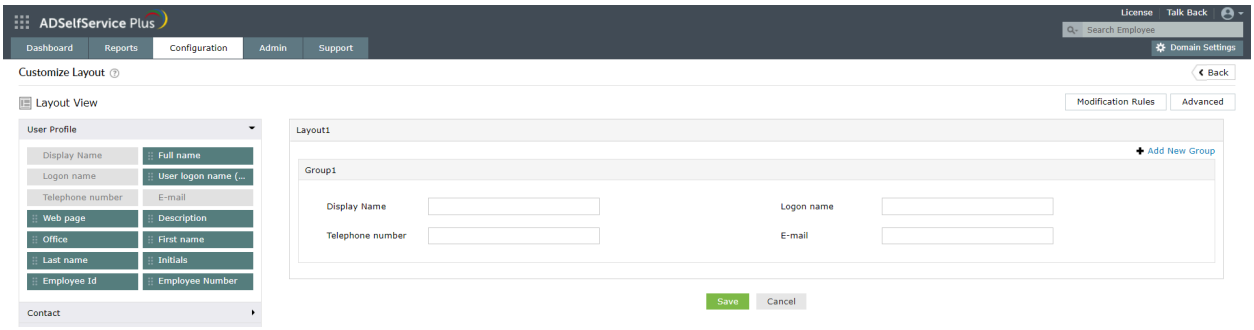


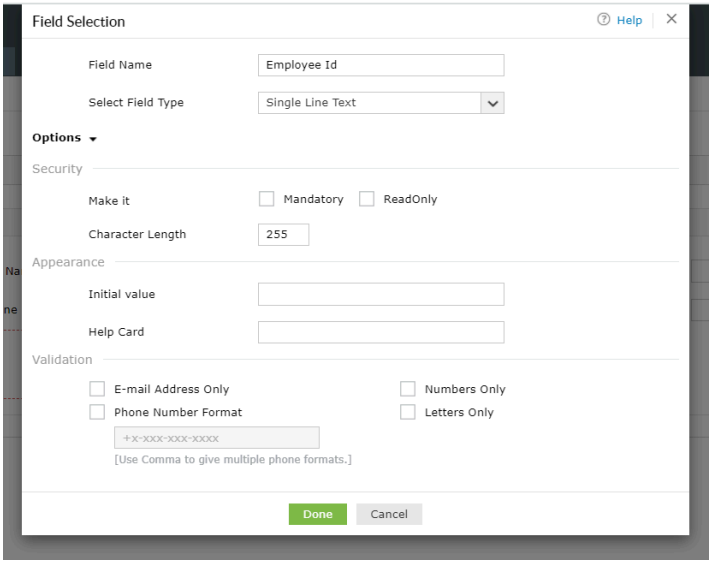
4. Directory self-service deployment

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.





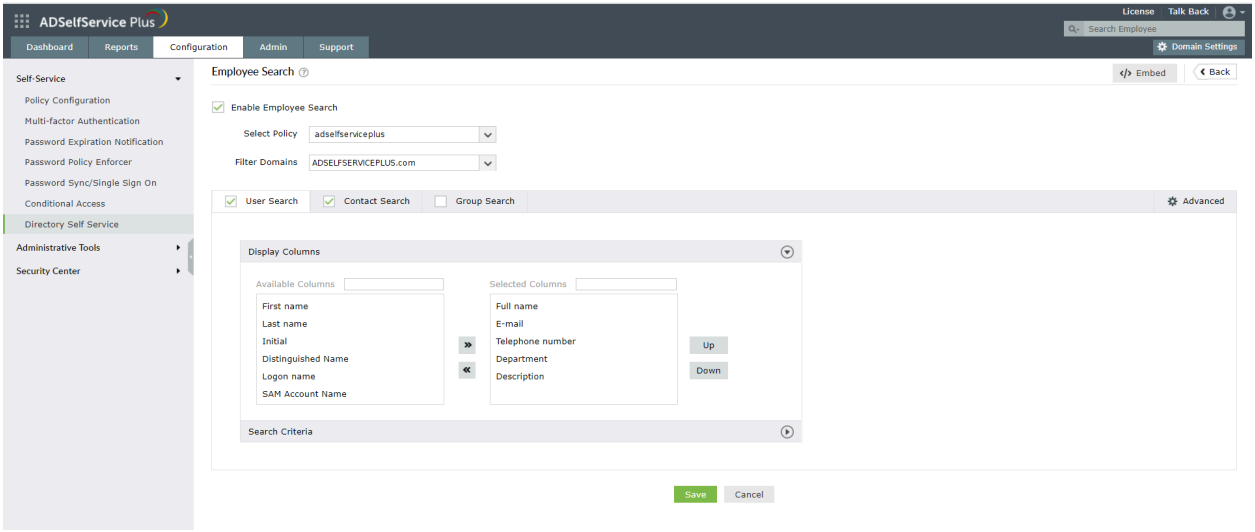
Configure user modification rules

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

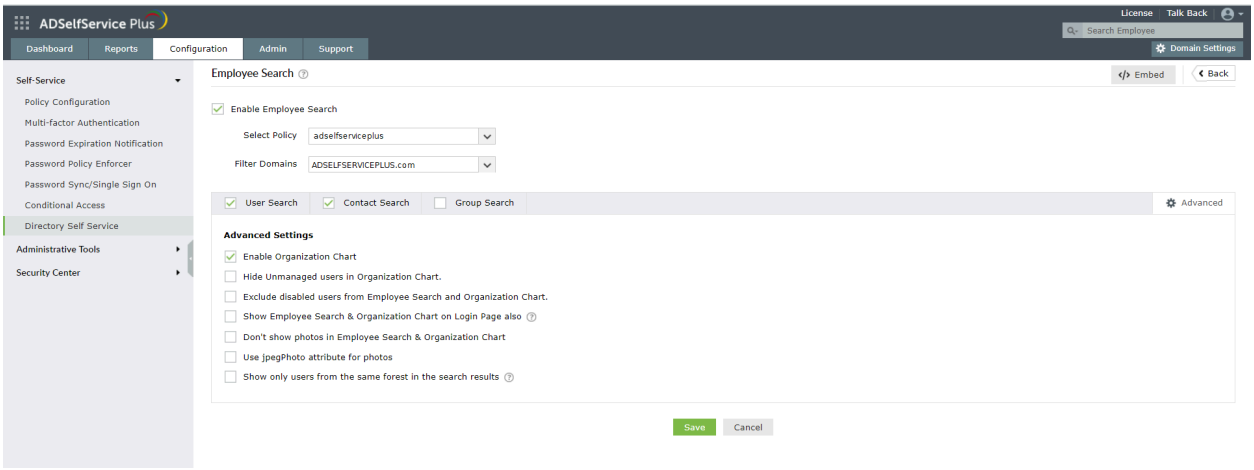
Employee search

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 will 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

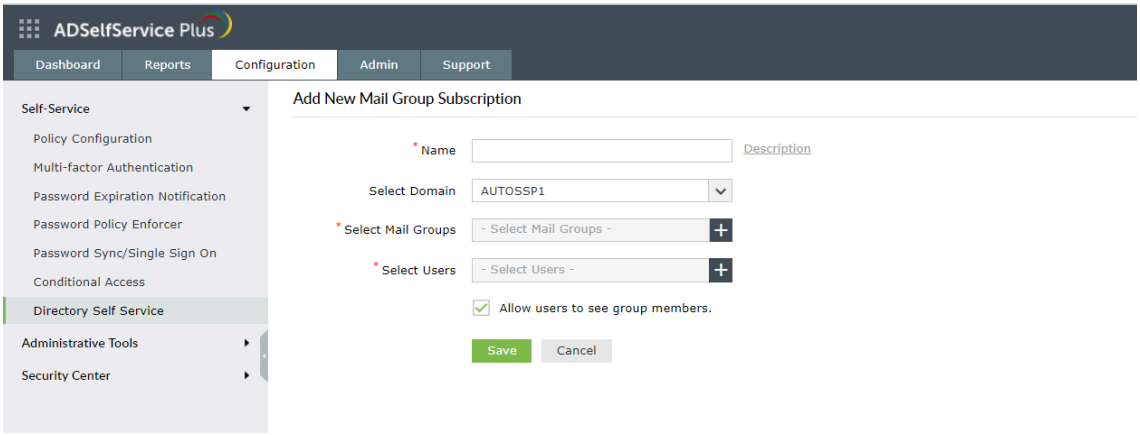
1. Under Employee Search, click **Advanced.**
2. Select **Enable Organization Chart** checkbox to allow employees to view the searched account's position in the organizational hierarchy.



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.**



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.

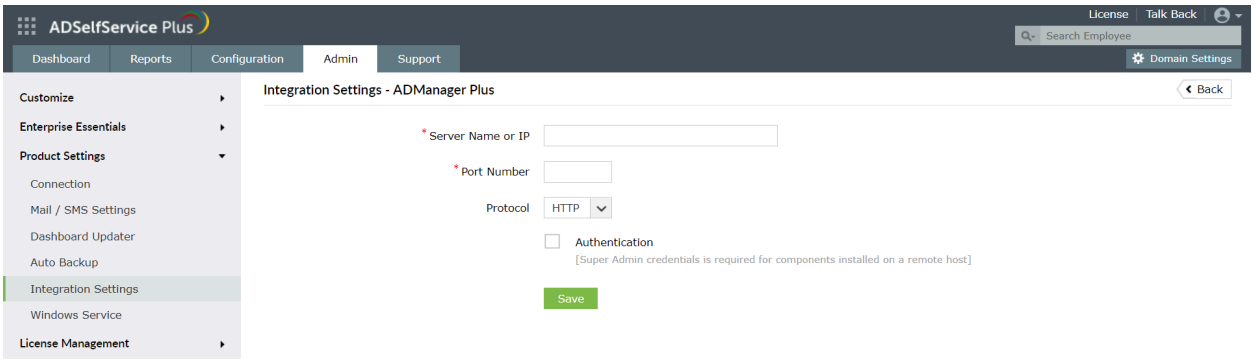
iii. Enterprise application integration

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.



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**.

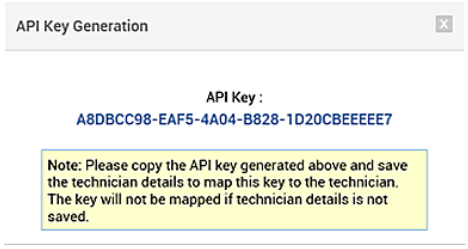
2. **ServiceDesk Plus and ServiceDesk Plus Cloud**: These are IT request tracking, and asset and change management solutions. When they are integrated with ADSelfService Plus, IT requests are automatically created in the solutions when self-service actions are performed by the user. This helps admins track users' self-service actions and follow up on them if needed. Moreover, end users can utilize passwordless login and SSO to access the ServiceDesk Plus Cloud console to raise IT tickets in one click from the ADSelfService Plus console. To integrate:

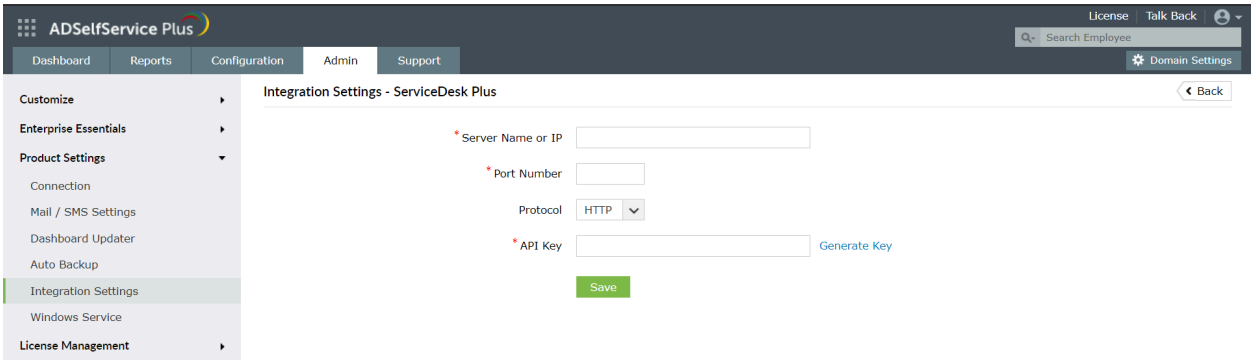
ServiceDesk Plus

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.

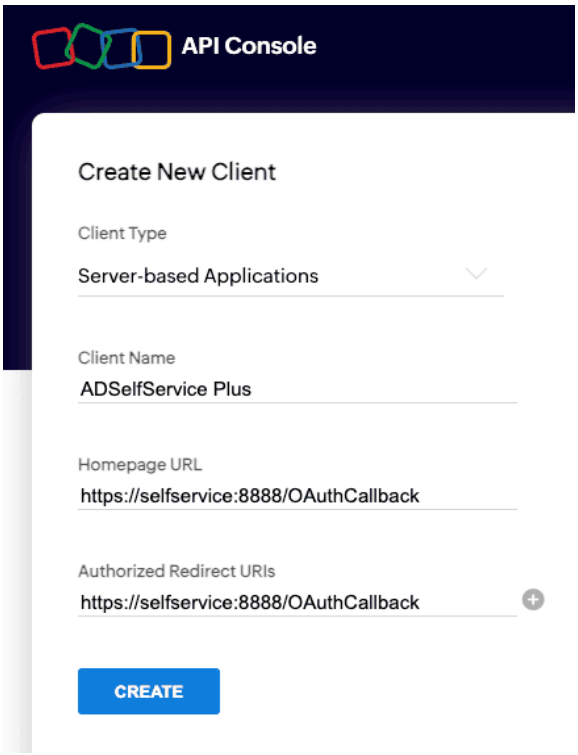
vii. Click **Save**.





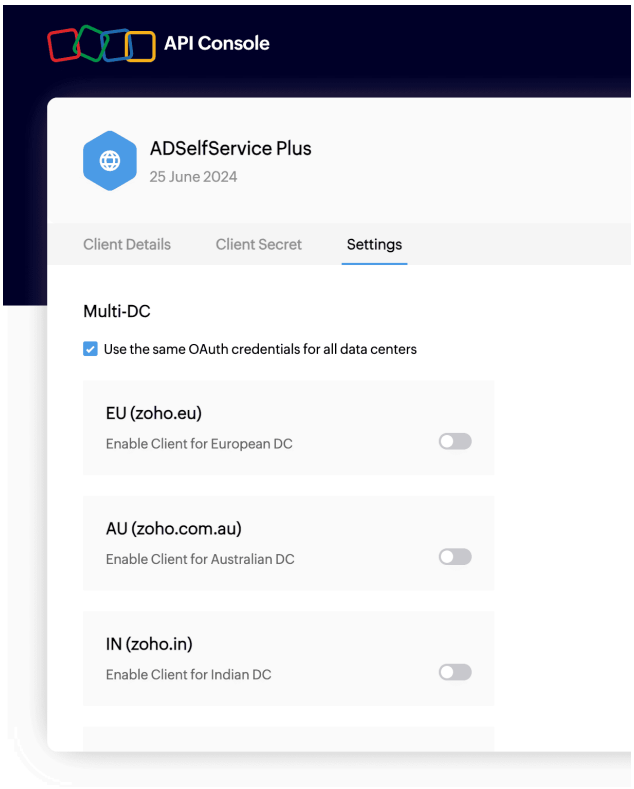
ServiceDesk Plus Cloud

1. Go to the Zoho API console and log in using your Zoho account.
2. After logging in, in the *Choose a Client Type* window, select the **Server-based Applications** tile.
3. In the *Create New Client* window, enter a **Client Name**.
4. In the **Homepage URL** and **Authorized Redirect URIs** fields, enter the URL value in the format given below:
   <product_access_url>/OAuthCallback. Sample URL: https://selfservice:8888/OAuthCallback.

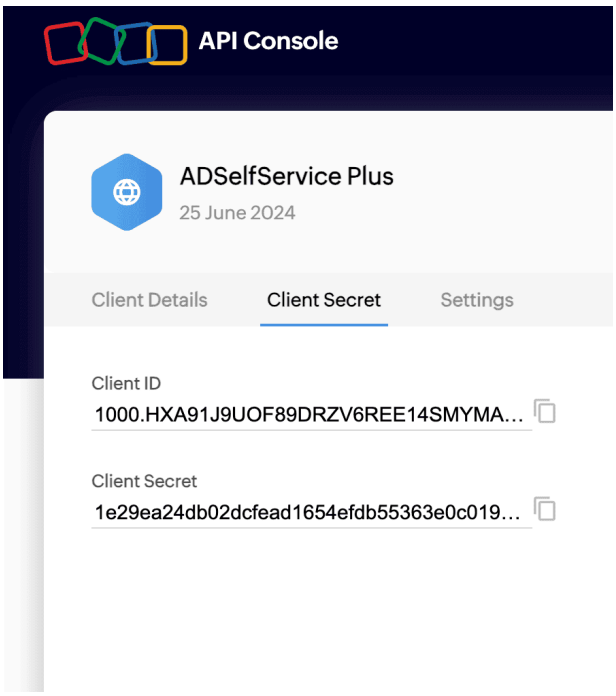


5. Enable multi-data center (DC) support (optional) by selecting the **Use the same OAuth credentials for all data centers** option in the **Settings** section. By default, the client ID remains the same, and the client secret differs from one DC to another. Enabling the **Use the same OAuth credentials for all data centers** setting allows you to have the same client secret across multiple domains based on your business needs. Additionally, you can allow users from specific domains to access the client using the same client secret by toggling the settings for those regions.

Note: The above option is not applicable for user accounts based in Chinese DCs.

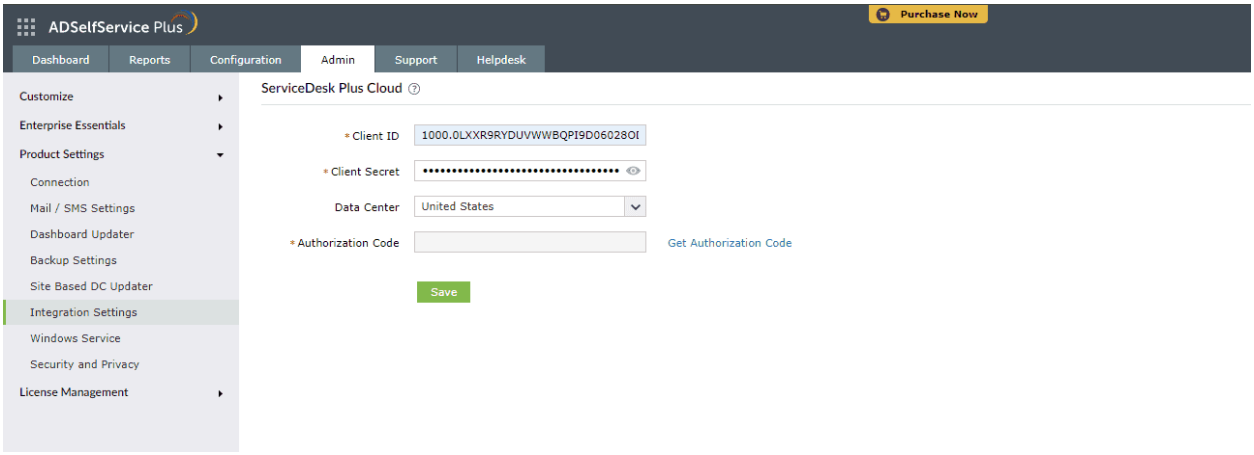


6. Copy the values of the **Client ID** and the **Client Secret** from the **Client Secret** section.

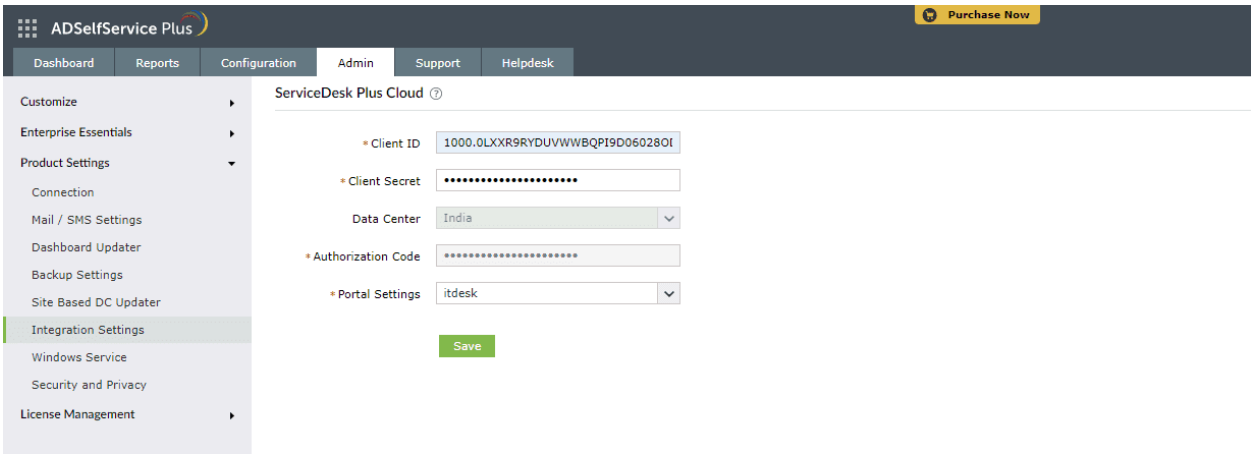


7. Next, log in to the ADSelfService Plus console with admin credentials.
8. Navigate to **Admin** > **Product Settings** > **Integration Settings**.
9. Click the **ServiceDesk Plus Cloud** tile.

10. In the **Client ID** and **Client Secret** fields, paste the values copied in step six.
11. Click the **Get Authorization Code** link. You will be redirected to the Zoho Account login page.



12. Authenticate using your ServiceDesk Plus Cloud technician account. Upon successful authentication, the **Authorization Code** will be filled automatically.
13. The default portal will be selected in the Portal field. If you wish to change the portal in which the tickets should be created, choose your preferred portal from the **Portal Settings** drop-down.
14. Click **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:

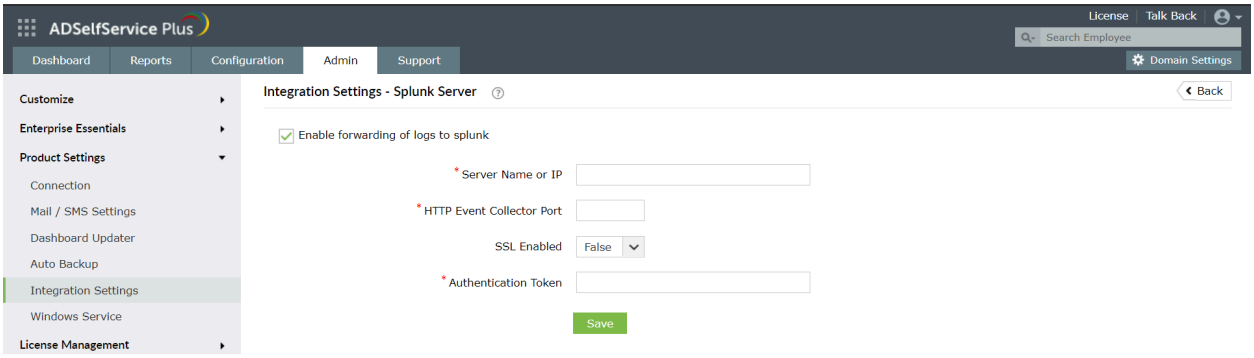
Prerequisite:

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.

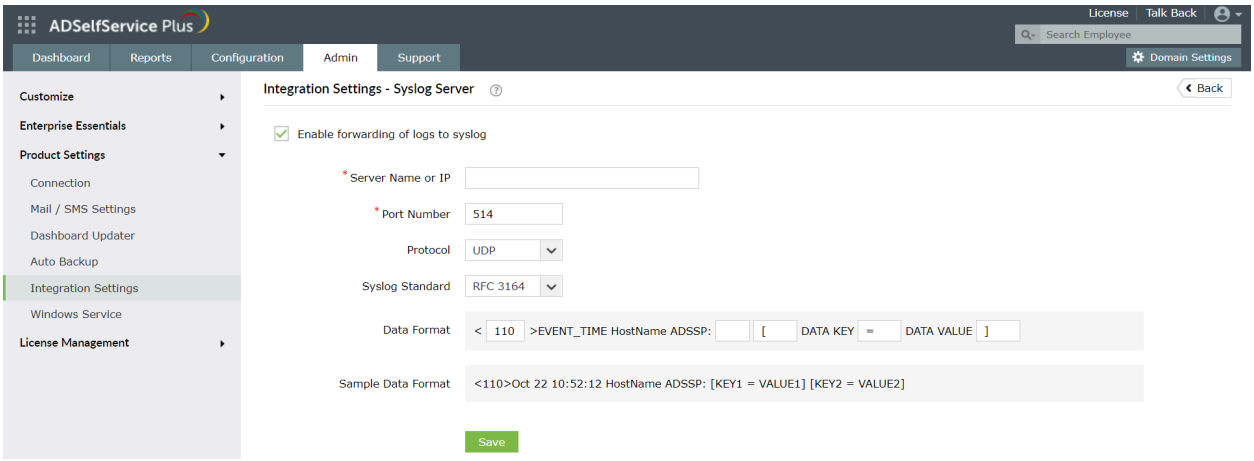
Once the HTTP event collector token is generated:

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**.



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.



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**

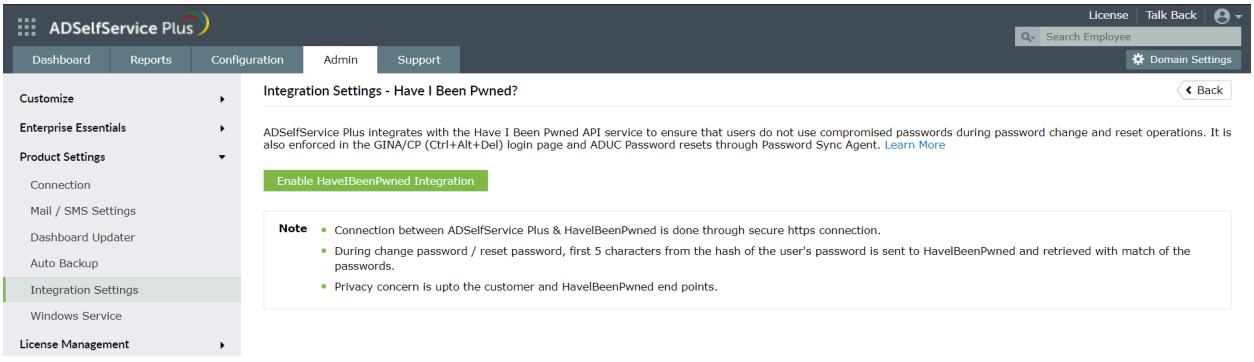
Steps to integrate:

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**



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.

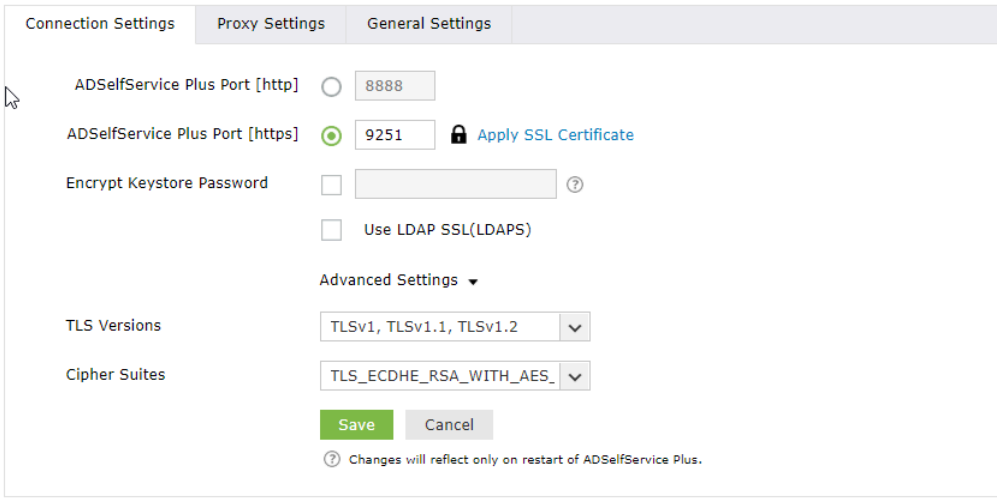
iii. High availability

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.



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.

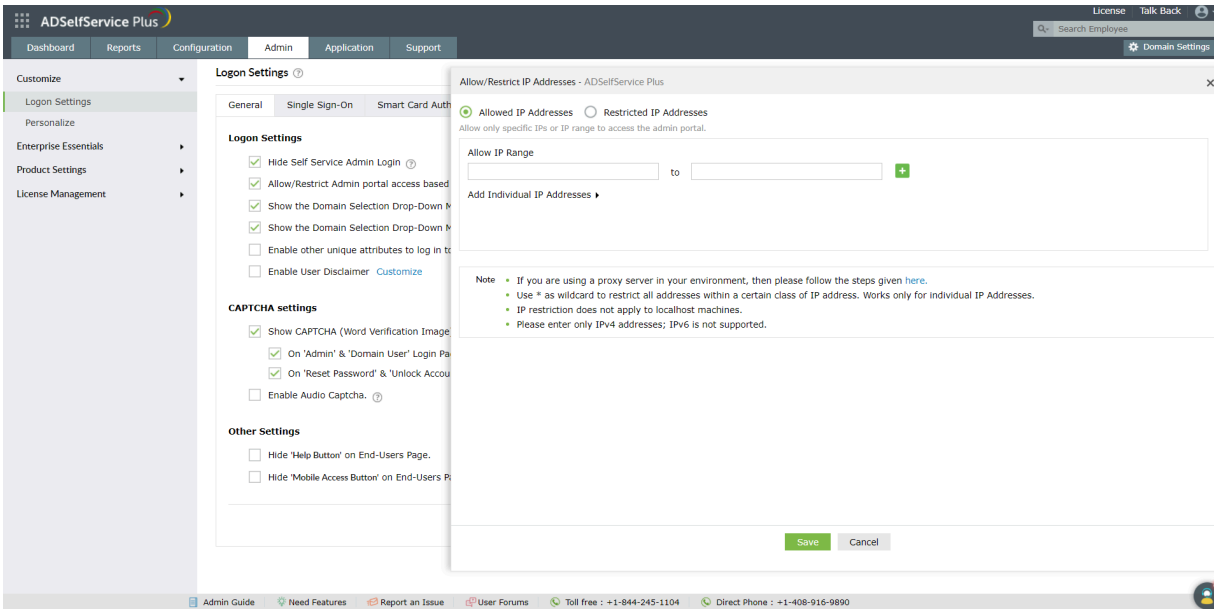
ix. Click **Save**.

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.**



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.

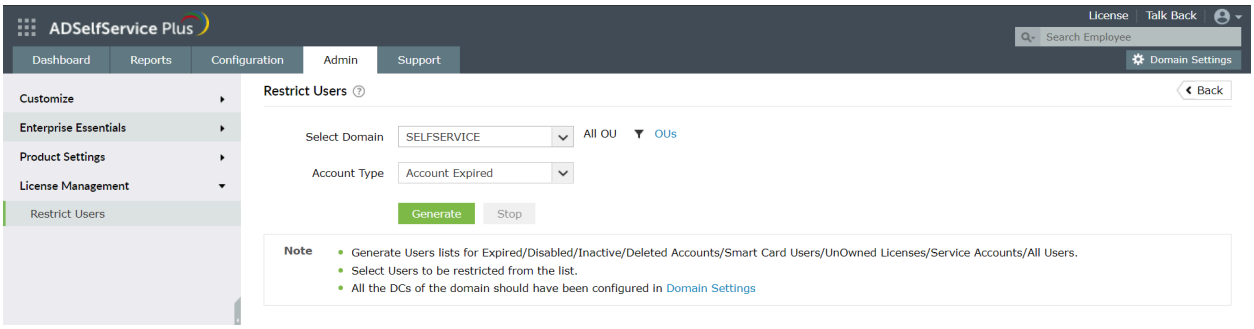
Steps to configure the Restrict Users option:

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

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

iii. Select the required **Domain.**

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



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.

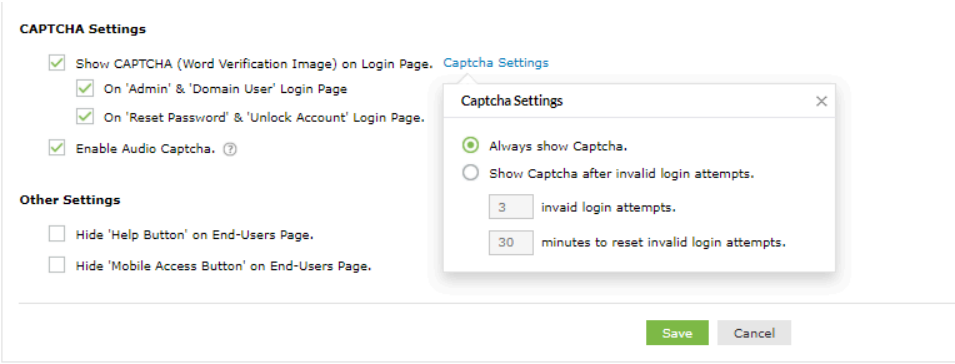
viii. Click **Restrict.**

Note: 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**.



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:

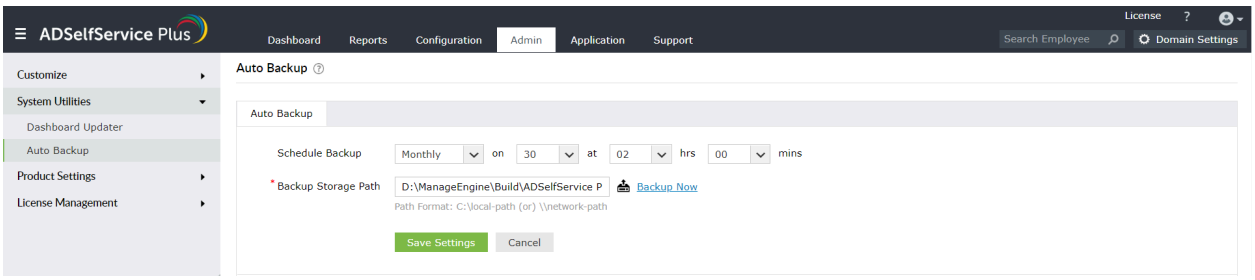
i. Go to **Admin** > **Product Settings** > **Dashboard Updater**.

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.



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:

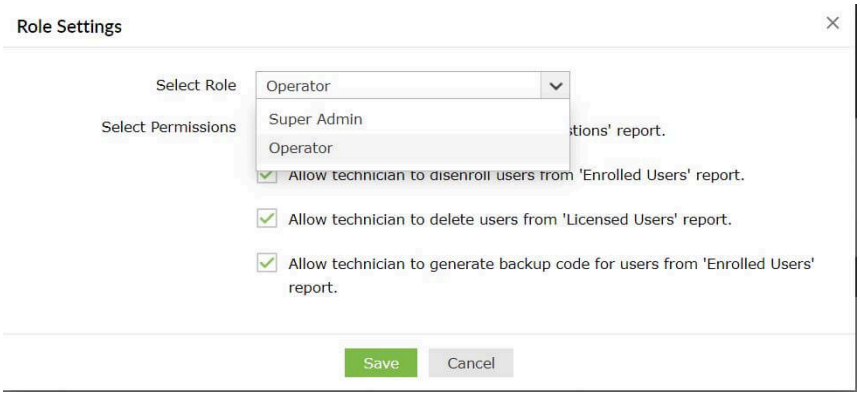
- Super Admin: Up to full control over the entire application by default.
- Operator: Can audit the various operations taking place in the application.

How to assign permissions to Technician roles

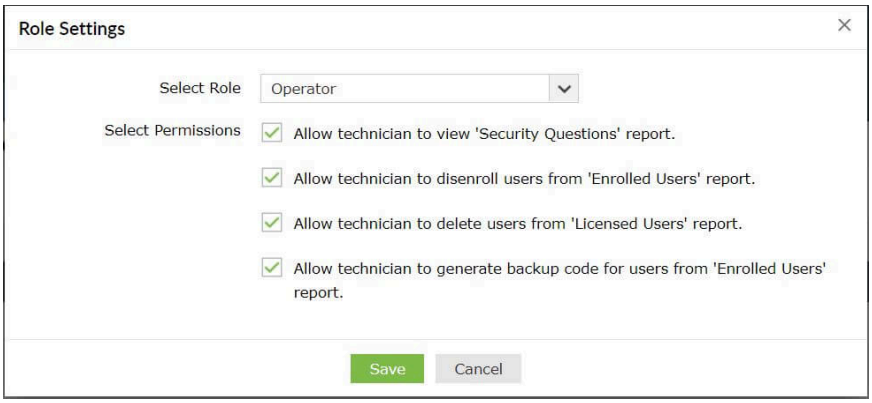
i. Go to **Configuration > Administrative Tools > Technician.**

ii. Select **Role Settings.**

iii. Select the required role from the drop-down.



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

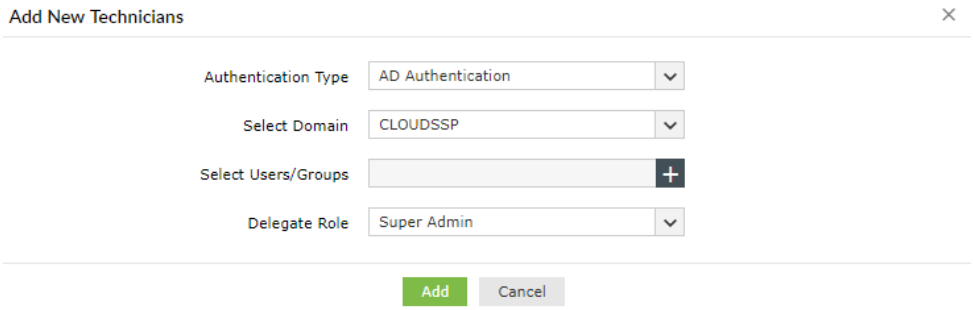


How to create a Technician

i. Go to **Configuration > Administrative Tools > Technician.**

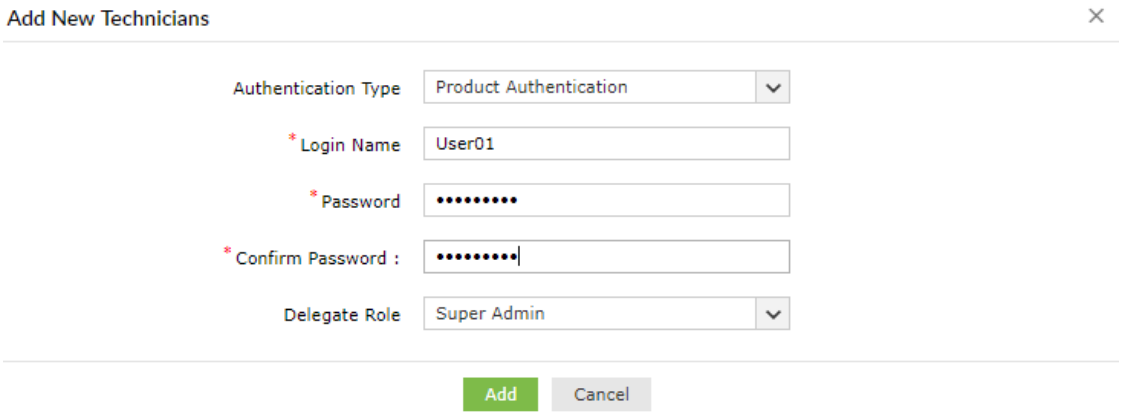
ii. Click the **Add new Technician button.**

iii. Select the **Authentication Type, Domain, Users/Groups,** and the **Role** from the respective drop-downs.



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.



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.

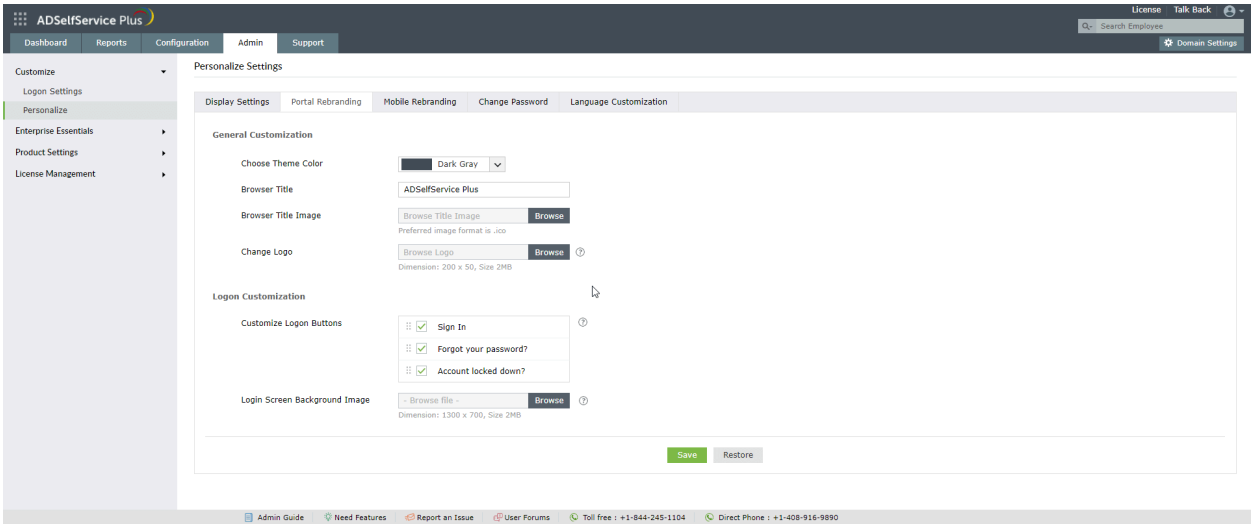
iv. Enter the desired **Browser Title**.

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.**



Our Products

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

About ADSelfService Plus

ADSelfService Plus is an identity security solution to ensure secure and seamless access to enterprise resources and establish a Zero Trust environment. With capabilities such as adaptive multi-factor authentication, single sign-on, self-service password management, a password policy enhancer, remote work enablement and workforce self-service, ADSelfService Plus provides your employees with secure, simple access to the resources they need. ADSelfService Plus helps keep identity-based threats out, fast-tracks application onboarding, improves password security, reduces help desk tickets and empowers remote workforces.

For more information about ADSelfService Plus, visit
www.manageengine.com/products/self-service-password.

$ Get Quote Download