ManageEngine
ADSelfService Plus

ADSelfService Plus

Deployment

Best Practices Guide

Table of Contents

1. Installation

i. Hardware requirements

Below are the system requirements for installing ADSelfService Plus.

Hardware	Minimum requirements	Recommended requirements
Processor	P4 - 1.6GHz	Core i3
RAM	1GB	4GB
Disk space	10GB	20GB

ii. Software requirements

Supported platforms

ADSelfService Plus can be installed on the following Windows operating systems:

Servers

1. Windows Server 2022
2. Windows Server 2019
3. Windows Server 2016
4. Windows Server 2012 R2
5. Windows Server 2012
6. Windows Server 2008 R2
7. Windows Server 2008
8. Windows Server 2003 R2
9. Windows Server 2003

Clients

1. Windows 11
2. Windows 10
3. Windows 8.1
4. Windows 8
5. Windows 7
6. Windows Vista

Supported browsers

ADSelfService Plus requires one of the following browsers to be used as a client to access the product's server:

1. Internet Explorer 9 or above
2. Firefox 4 or above
3. Chrome 10 or above
4. Microsoft Edge

Preferred screen resolution: 1,024x768 pixels or higher

Supported platforms for login agent installation

ADSelfService Plus' self-service password reset and account unlock operations can be performed from the login screens of the following platforms:

Windows

Servers

1. Windows Server 2022
2. Windows Server 2019
3. Windows Server 2016
4. Windows Server 2012 R2
5. Windows Server 2012
6. Windows Server 2008 R2
7. Windows Server 2008

Clients

1. Windows 11
2. Windows 10
3. Windows 8.1
4. Windows 8
5. Windows 7
6. Windows Vista

macOS

1. macOS 11 Big Sur
2. macOS 10.15 Catalina
3. macOS 10.14 Mojave
4. macOS 10.13 High Sierra
5. macOS 10.12 Sierra
6. OS X 10.11 El Capitan
7. OS X 10.10 Yosemite
8. OS X 10.9 Mavericks
9. OS X 10.8 Mountain Lion
10. Mac OS X 10.7 Lion
11. Mac OS X 10.6 Snow Leopard

Linux

1. Ubuntu 16.x-20.x
2. Fedora 27.x-31.x
3. CentOS 7.X

Note: While the ADSelfService Plus login agent has been officially tested and confirmed to run seamlessly on these three Linux distributions, it may support other Linux distributions as well. Please contact the support team (support@adselfserviceplus.com) to check if the Linux distribution used in your organization is supported.

iii. Choosing where to install the product

ADSelfService Plus can be installed on both servers and client machines.

- **64-bit version vs. 32-bit version**

  ADSelfService Plus offers two versions: a 64-bit version and a 32-bit version. Admins can choose to use either of these versions according to their organization's requirements.

  Once ADSelfService Plus has been deployed, admins should follow the security measures in this guide.

- **Supported databases**

  ADSelfService Plus offers a built-in PostgreSQL database to store user enrollment information, audit logs, domain configuration information, and some Active Directory (AD) attribute values. Organizations can also use external databases, like MS SQL and PostgreSQL, for the same purpose.

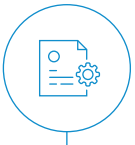
2. Domain Settings Configuration

- We recommend that admins place the primary domain controller at the top of the list of domain controllers that are configured. This ensures that ADSelfService Plus is synced with the latest AD information without any delays. Learn more about domain configuration.

- During domain configuration, admins must provide the credentials of a service account that possesses Domain Admin permissions in AD. If admins do not want to grant Domain Admin permissions to the service account for security reasons, they can selectively provide the required permissions by following the steps in this guide.

3. Password Self-service Features

Before enabling features, admins must configure self-service policies. These policies allow admins to select certain groups, OUs, and domains and assign specific self-service actions and other features only to them. Only users in these groups, OUs, and domains can use the selected features. Another prerequisite is configuring the authentication methods required for MFA.



OU- and group-based self-service policies:

During self-service policy configuration, admins are advised to create and configure self-service policies for OUs and groups as opposed to domains. This allows for the creation of fine-grained self-service policies that are applied only to the necessary users. In case an OU or group falls under multiple self-service policies, admins can prioritize the policies in the order of precedence.

Setting up multi-factor authentication for self-service features:

ADSelfService Plus' MFA feature must be configured for self-service password actions. Before resetting their passwords or unlocking their accounts, users are required to prove their identities using any of the following authentication methods:

1. Fingerprint or Face ID
2. YubiKey
3. Google Authenticator
4. Microsoft Authenticator
5. Azure AD MFA
6. Duo Security
7. RSA SecurID
8. RADIUS
9. Zoho OneAuth TOTP
10. TOTP
11. Push notification
12. QR code
13. Custom TOTP authenticator
14. SAML
15. Security questions and answers
16. Email verification
17. SMS verification
18. AD security questions
19. Smart card

Password and account expiration notifications:

Admins can enable email, SMS, or push notifications to inform end users about impending password and account expiration. This ensures users change their passwords well in advance and have constant access to domain accounts.

Learn more about configuring password and account expiration notifications.

Password Policy Enforcer:

Admins are recommended to configure the Password Policy Enforcer and enable the Password Strength Analyzer. The Password Policy Enforcer allows admins to create a custom password policy and force users to comply with it while creating passwords.

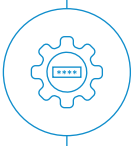
When the Enable Password Strength Analyzer option is selected, the password's strength level is displayed during change or reset, encouraging users to create strong passwords.

Learn more about the Password Policy Enforcer and Password Strength Analyzer.

Configure password reset and account unlock from login screens:

The GINA/macOS/Linux login agent allows domain users to reset their passwords and unlock their accounts from their Windows, macOS, and Linux login screens without depending on other users' machines to access the Reset Password/Unlock Account portal.

Learn more about the GINA/macOS/Linux login agent.



Configure password self-service actions on the go:

ADSelfService Plus' Mobile App Deployment feature helps admins push the ADSelfService Plus mobile app to domain users' mobile devices directly from the admin portal. It even spares users the difficulty of configuring their mobile apps. When users are met with a ready-to-use ADSelfService Plus mobile app, the change is much easier.

Learn more about Mobile App Deployment.

Enable cached credentials update

ADSelfService Plus' cached credentials update feature helps ensure remote domain password resets made by employees are updated in the local cache of their machines via VPN for streamlined authentication. This helps remote users who forget their passwords regain access to their machines. Learn how to enable cached credentials update.

4. User Enrollment

Force enrollment using logon scripts

Users need to enroll themselves with ADSelfService Plus in order to perform self-service actions. Forcing users to enroll after they have logged in to the domain ensures that they are enrolled in advance and can perform self-service actions and log in to the ADSelfService Plus portal without any delay. Learn how to force enrollment using logon scripts.

Send enrollment notifications

Another option is to send enrollment notifications to inform employees about the product and encourage them to enroll. When the Send Enrollment Notification via Email/Push feature is enabled, email or push notifications are sent to all users who have not yet enrolled with ADSelfService Plus. A scheduler can also be set up to automatically send notifications to non-enrolled users on a regular basis. Learn more about enrollment notifications.

Import enrollment data from CSV files

Users' enrollment information for email verification, authentication based on security questions and answers, and SMS verification methods can be imported in the form of a CSV file to enroll users automatically. Learn more.

Import enrollment data from an external database

ADSelfService Plus can be connected with an organization's data sources that store user information, like MS SQL, PostgreSQL, Oracle Database, and MySQL. The user information can then be used to automatically enroll users in the product. A scheduler can also be set to periodically search for newly added users in the connected external data sources and enroll them in ADSelfService Plus. Learn more.

5. Security

i. Endpoint Security

Enable MFA for machine logins

ADSelfService Plus' Endpoint MFA feature can be used to secure endpoint (Windows, macOS, and Linux) logins in the domain. This strengthens the existing username and password-based authentication by adding extra levels of security. Learn more.

Enable MFA for VPN logins

ADSelfService Plus provides the option to secure VPN logins using MFA. This helps secure remote access to the organization's domain network. The solution supports the following authenticators:

1. One-way authenticators
   - Push notification
   - Fingerprint or Face ID
2. Challenge-based authenticators
   - ADSelfService Plus TOTP
   - Google Authenticator
   - Microsoft Authenticator
   - Yubico OTP (hardware key authentication)

Enable MFA for Outlook Web Access logins

MFA can also be enabled to protect Outlook Web Access and Exchange admin center logins. This secures enterprise emails and other sensitive organizational information.

ii. Password Self-service Security

Configure conditional access

ADSelfService Plus' conditional access feature provides users with contextual access to self-service features, single sign-on, and password synchronization depending on risk factors like IP address, device type, time of access, and location. This helps automate access control decisions without affecting the user experience. Learn how to configure conditional access.

Configure CAPTCHA for password resets and account unlocks

We recommend that admins enable CAPTCHA to prevent bots from attempting to log in to the self-service password reset and account unlock portal. Admins have the option of enabling audio CAPTCHA as well. To enable CAPTCHA:

1. Navigate to **Admin → Customize → Logon Settings.**
2. Select **Show CAPTCHA (Word Verification Image) on Login Page.**
3. Select **On 'Reset Password' & 'Unlock Account' Login Page.**
4. Click **Save.**

Enable user and admin notifications for password self-service operations

Admins can enable notifications that send users an acknowledgement when they enroll with the product, as well as every time they perform actions like reset or change their password or unlock their account. These notifications can also be sent to the admin when users perform such actions. Learn how to enable these notifications.

Block users who have failed at identity verification

We recommend that admins enable the Block User setting to block users who have made consecutive failed identity verification attempts in the ADSelfService login or self-service portal.

1. Go to **Configuration > Self-Service > Policy Configuration > Advanced.**
2. Click on the **Block User** tab.
3. Specify the maximum number of invalid attempts and the time limit.
4. Specify the duration for which the user will be blocked.
5. Click **Save.**

Restrict the number of self-service actions that can be performed

We recommend that admins set the maximum number of times users can perform a self-service password reset within a given number of days. To do this:

1. Go to **Configuration > Self-Service > Policy Configuration > Advanced.**
2. Click on the **Block User** tab.
3. Under the *Restrict Self-service Actions* tab, select **Allow user to reset their password _ times in days.** Specify the maximum number of times users can reset their passwords as well as the number of days for which this limit applies.
4. Click **Save.**

Set limitations on the ADSelfService Plus portal's idle time

ADSelfService Plus' Session Expiration Time setting allows admins to select the maximum time span an ADSelfService Plus session can be idle for before the session automatically ends. To enable this setting:

1. Go to **Admin → Product Settings → Connections → General Settings.**
2. Select the **Deny Concurrent Logins** checkbox, then select the **Click here** link to reset the session status of all users.
3. In the *Confirm Action* pop-up, click **Yes.**

6. Single Sign-on and Password Synchronization

Configure single sign-on for cloud and on-premises applications

The single sign-on feature of ADSelfService Plus allows users to sign in to ADSelfService Plus and access their enterprise applications without having to log in to each application. This makes it easier to look after multiple accounts and allows users to retain one identity across multiple business applications that support SAML, OAuth, and OpenID Connect protocols. Organizations can also require SSO to be used for custom SAML or OAuth-based applications. Read more.

Password synchronization for in-house AD and enterprise applications

The single sign-on process can be protected by passwordless authentication based on MFA. Users don't have to authenticate using their AD credentials and can directly perform MFA using the configured methods. Once authenticated, they can access multiple SSO-enabled enterprise applications without further authentication Learn more.

Password synchronization for in-house AD and enterprise applications

The Password Synchronization feature in ADSelfService Plus allows users to synchronize their AD account password with their user accounts in integrated enterprise applications. If the Password Sync Agent is enabled, any native password changes (password changes using the Ctrl+Alt+Del option in Windows, and password resets using the ADUC console) may also be synchronized. Learn more.

7. Employee Directory Update and Search

Configure Directory Self-update

We recommend that admins configure the Self-update feature to provide users with the option to update their AD profile information without depending on the help desk. Admins can select specific attributes that can be updated and allow users to update custom attribute values. Learn more.

Enable Employee Search

The Employee Search feature allows users to search for information on other users in the organization. Employees can search for information on users, contacts, and groups. Learn more.

Enable the Organization Chart

The Organization Chart feature displays information about all employees in the organizational hierarchy. Learn how to enable the Organization Chart.

Configure mail group subscription

This feature allows domain users to subscribe themselves to mail groups, reducing their dependency on the help desk. Learn how to configure mail group subscription.

8. Portal Security and Other Recommended Settings

i. Security Settings

Configure SSL and LDAPS

Admins must apply a Secure Sockets Layer (SSL) certificate and configure an HTTPS connection to protect the data transferred between the ADSelfService Plus server, the user's web browser, and the ADSelfService Plus app, and to secure data during API access. Secure Lightweight Active Directory Application Protocol (LDAPS) can also be configured to secure the connection between the product and AD. Learn more about SSL and LDAPS configuration.

Restrict admin portal access

ADSelfService Plus offers the option to hide the admin login section in the product login page and permit admins to log in only from specific IP addresses. To configure the list of IP addresses to be allowed to or restricted from accessing the login page:

1. Go to **Admin** > **Customize** > **Logon Settings** > **General.**
2. Select the **Hide Self Service Admin Login** checkbox.
3. Select the **Allow/Restrict Application access based on IP Addresses** checkbox.
4. In the *Allow/Restrict IP Addresses* section that appears, select **Allowed IP addresses** or **Restricted IP addresses.**
5. Enter the appropriate IP address range in the available fields.
6. Restrict or allow specific IPs by selecting **Add Individual IPs.**
7. Click **Save.**

Deny concurrent logins

The Deny Concurrent Logins option restricts users from having multiple active ADSelfService Plus sessions at once. To enable this option:

1. Go to **Admin** > **Product Settings** > **Connection** > **General Settings.**
2. Under the *Session Settings* section, select the **Deny Concurrent Logins** checkbox.

Enable ADSelfService Plus login MFA

The MFA feature can be used to protect ADSelfService Plus portal logins. This, in turn, secures actions like directory self-update, employee search, and mail group subscription. Configuring MFA for ADSelfService Plus logins also protects access to cloud and on-premises applications through SSO.

Enable CAPTCHA for portal logins

We recommend that admins enable CAPTCHA for ADSelfService Plus portal logins as well.

Configure a reverse proxy server when the product is hosted on the internet

If ADSelfService Plus will be hosted on the internet, admins are recommended to configure a reverse proxy server, a type of proxy server that retrieves resources on behalf of a client from a server. These resources are then returned to the client, appearing as if they originated from the reverse proxy itself. Thus, the website or service never needs to reveal the IP address of its origin server. By configuring a reverse proxy, the ADSelfService Plus server, othe components, and the LAN they are located in are concealed from third-party attacks. Learn about reverse proxy configuration using ManageEngine AD360, Apache HTTP Server, and IIS.

Remove ADSelfService Plus licenses from stale users

Admins can revoke the ADSelfService Plus licenses assigned to stale AD accounts, like expired, deleted, and inactive accounts, using the Restrict Users option. This frees up the unused licenses that are assigned to these accounts and prevents such accounts from getting assigned licenses in the future. Learn how to restrict users.

Configure notifications on application downtime

Admins can enable notifications that inform them every time their ADSelfService Plus license expires, the product shuts down unexpectedly, the product gets updated, or any event or workshop is announced. To enable these notifications:

1. Go to **Admin > Product Settings > Mail/SMS Settings > Mail Settings.**
2. Under *Notification Settings*, enable:
   - **License Expiration Notification**
   - **Enable Downtime Notification**
   - **Enable Product Update Notification**
   - **Enable Events and Workshop Notification**
3. Click **Save Settings.**

i. Other Recommended Settings

Schedule DB backups

Using the Auto Backup feature, admins can create a schedule to regularly update the built-in PostgreSQL database as a measure against data loss. To enable automatic DB backups:

1. Go to **Admin** > **System Utilities** > **Auto Backup.**
2. Enter the time and frequency at which the scheduler should run.
3. Enter a custom **Backup Storage Path** or keep the default path, *D:\new flat ui\ADSelfService Plus\Backup.*
4. Click **Backup Now** to back up the database at that instant.
5. Click **Save Settings.**

Configure High Availability

ADSelfService Plus employs automated failover to support high availability of the product in case of system failure. This is done by creating two instances of the product in two machines so that if one instance fails, the other instance takes over and provides admins and end users with uninterrupted access to the product. Learn more about High Availability configuration.

Configure Load Balancing

Admins are also recommended to configure the Load Balancing feature that helps split incoming requests among multiple servers. This improves the product's availability and reliability. By enabling Load Balancing, admins can ensure users have fast and uninterrupted access to the product at all times. Learn more about Load Balancing configuration.