ManageEngine
ADSelfService Plus

ADSelfService Plus

Deployment

Best Practices Guide

Table of Contents

1. Installation

i. Hardware requirements

Hardware	Minimum requirements	Recommended requirements
Processor	2.4 GHz	3 GHz
RAM	8 GB	16 GB
Disk space	100 GB (SSD preferred)	200 GB (SSD preferred)

ii. Software requirements

Supported platforms

ManageEngine ADSelfService Plus can be installed in the following Windows operating system versions:

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

Clients

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

Supported browsers

ADSelfService Plus requires one of the following browsers to be used as a client to access its server.

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

Supported Databases

ADSelfService Plus comes with a built-in PostgreSQL database for storing user enrollment information, domain configuration information, certain AD attribute values, ADSelfService Plus reports data, etc. Organizations can also use an external Microsoft SQL or PostgreSQL database to store this data.

PostgreSQL

ADSelfService Plus build number	Supported database versions
6513 and above	PostgreSQL 14 and 15
6500 to 6512	PostgreSQL 12, 13 and 14
6100 to 6410	PostgreSQL 9.4-9.6, 10.0-10.15, and 11.0-11.7
5500 to 6013	PostgreSQL 9.2-9.6

Microsoft SQL

ADSelfService Plus build number	Supported database versions
6500 and above	Microsoft SQL Server 2012 and above
5500 to 6410	Microsoft SQL Server 2005 and above

Preferred screen resolution: 1024 x 768 pixels or higher.

Note: If your ADSelfService Plus server is using a MySQL database, we recommend migrating to PostgreSQL. Contact the support team at support@adselfserviceplus.com to know more.

Supported platforms for login agent installation

The ADSelfService Plus login agent enables end users to securely log into their machines and perform self-service password resets and unlocks directly from the machine login screen.

You can install the login agent on 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

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

macOS clients
1. macOS 15 Sequoia
2. macOS 14 Sonoma
3. macOS 13 Ventura
4. macOS 12 Monterey
5. macOS 11 Big Sur
6. macOS 10.15 Catalina
7. macOS 10.14 Mojave
8. macOS 10.13 High Sierra
9. macOS 10.12 Sierra
10. OS X 10.11 El Capitan
11. OS X 10.10 Yosemite

Linux clients
1. Red Hat Enterprise Linux 8.x-9.x *
2. Rocky Linux 8.x-9.x *
3. Ubuntu-16.x-20.04.4
4. Fedora - 27.x-31.x
5. CentOS - 7.X

*Machines running Red Hat Enterprise Linux and Rocky Linux can be secured with machine login MFA. Self-service password resets and unlocks from the login screen are currently not supported for these platforms.

Note: While the ADSelfService Plus login agent has been officially tested and confirmed to run seamlessly on the three Linux distributions mentioned, 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. Prerequisites

Before enabling features, admins must configure self-service policies, enable authenticators, and set up user enrollment methods.

Configure OU- and group-based self-service policies:

Self-service policies enable admins to select certain groups, OUs, and domains, and assign specific self-service actions, authenticators, and other features to them. Only users in these groups, OUs, and domains can use the selected feature. In case an OU or group falls under multiple self-service policies, admins can prioritize the policies in the order of precedence. Learn more here.

Enable authenticators for MFA:

Admins must configure necessary authenticators for the MFA features. The authenticators can be used to verify users' identities when accessing machines, enterprise applications, VPN, OWA, and other supported endpoints. They are also used to authenticate users during self-service password resets and account unlocks. Below are the authenticators supported by ADSelfService Plus:

1. FIDO Passkeys
2. Biometric Authentication
3. YubiKey
4. Google Authenticator
5. Microsoft Authenticator
6. Azure AD MFA
7. Duo Security
8. RSA SecurID
9. RADIUS
10. Zoho OneAuth TOTP
11. ADSelfService Plus TOTP
12. Push notification
13. QR code
14. Custom TOTP authenticator
15. SAML
16. Security questions and answers
17. Email verification
18. SMS verification
19. AD security questions
20. Smartcard

User enrollment

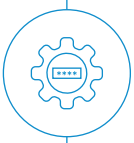
Users need to enroll themselves with ADSelfService Plus using the assigned authenticators. This provides them access to the product's features and ensures they complete identity verification when accessing MFA-enabled endpoints. Users can voluntarily enroll to start using the features, or one of the following methods can be used to enroll them.

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.

4. Identity 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 offline MFA

To ensure identity security even without 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 or macOS login agent. Offline MFA can secure Windows and macOS logins, Windows RDP server authentication, and Windows UAC prompts. Click here to 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. To configure VPN MFA, you must first select the appropriate MFA mode based on the type of authenticators and MFA prompts you wish to use. ADSelfService Plus supports the following two modes:

VPN Client Verification: In this mode, MFA prompts are displayed directly within the VPN client.

SecureLink Email Verification: This mode enables MFA via all ADSelfService Plus authenticators, with users authenticating via an email verification link.

With these configurations, MFA will be enabled for VPN logins, ensuring secure access to your network. Learn more.

Enable MFA for Outlook Web Access logins

MFA can also be enabled to protect Outlook Web Access (OWA) and Exchange admin center logins. This secures enterprise emails and other sensitive organizational information. Learn how to enable MFA for OWA.

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.

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.**

Enable user enumeration to avoid revealing valid user accounts

During brute-force attacks, hackers may employ user enumeration by observing the application's response to the credentials entered. By observing whether MFA is invoked or not, hackers can identify if the credentials entered belong to a valid user. To prevent this, a mock MFA process can be enabled to run even when incorrect credentials are entered. For this:

1. Navigate to **Admin > Customize > Login Settings.**
2. Select **Prevent hackers from finding out valid users.**
3. Click **Configure** to enable the authenticators to be displayed during the mock MFA process. If you enable the **Random security questions** option, two random security questions will be displayed. By clicking **Modify**, you can customize the security questions. If you enable the **Email verification link** option, a message reading Email verification link sent will be displayed to the user. This is a false message, and no email will be sent to the user.
4. Click **Save.**

5. Single sign-on and just-in-time provisioning

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

The single sign-on (SSO) feature in ADSelfService Plus enables users to sign in once and access multiple enterprise applications without repeated logins, simplifying account management and ensuring a unified identity across applications supporting SAML, OAuth, and OpenID Connect protocols. Organizations can also enforce SSO for custom SAML or OAuth-based applications. Additionally, the bookmark functionality allows admins to integrate applications that do not support SSO by bookmarking them in the user portal. Users can then access these applications with a single click, redirecting them to the login page where they authenticate using their registered credentials.. Read more.

Enable passwordless authentication for enterprise applications

MFA-based passwordless authentication can secure single sign-on. 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 single-sign-on-enabled enterprise applications without further authentication. Learn more.

Set up 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.

Enable just-in-time provisioning for enterprise applications

Just-in-time provisioning provides seamless access to enterprise applications by automatically creating a user account upon a user's first login. This helps reduce the IT admin's workload and enhance the user experience. Learn more.

6. Self-service password management and password security

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. FIDO passkeys
2. Biometric Authentication
3. YubiKey
4. Google Authenticator
5. Microsoft Authenticator
6. Azure AD MFA
7. Duo Security
8. RSA SecurID
9. RADIUS
10. Zoho OneAuth TOTP
11. ADSelfService Plus TOTP
12. Push notification
13. QR code
14. Custom TOTP authenticator
15. SAML
16. Security questions and answers
17. Email verification
18. SMS verification
19. AD security questions
20. Smartcard authentication

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 encouraged to configure the Password Policy Enforcer and enable the Password Strength Analyzer in ADSelfService Plus to enhance password security. The Password Policy Enforcer enables the creation of custom password policies, ensuring users adhere to defined rules when setting or resetting their passwords. Additionally, organizations can enforce custom regex patterns, allowing precise control over password structure to align with internal security requirements. When the Password Strength Analyzer is enabled, users receive real-time feedback on password strength during changes or resets, motivating them to choose more secure credentials.

Learn more about the Password Policy Enforcer, Regex patterns, 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 for streamlined authentication. This helps remote users who forget their passwords regain access to their machines. Learn how to enable this.

Configure CAPTCHA for password changes and account unlocks

We recommend that admins enable CAPTCHA to prevent bots from complete authentication during self-service password reset, self-service account unlock, and password change.
To enable CAPTCHA:

1. Go to **Configuration > Self-Service > Policy Configuration.**
2. In the *Policy Configuration* section, select **Advanced.**
3. Select the **General** tab in the Advanced pop-up.
4. In the **Hide CAPTCHA** in drop-down, select the actions you want to be protected by CAPTCHA.
5. Select **OK**.

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.

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.**

Advanced password policies for product technicians

It is recommended that advanced password policies are enabled for product-authenticated technicians, especially Super Admins. For this:

1. Go to **Configuration > Administrative Tools > Technician.**
2. Click **Advanced** in the bottom-right corner and click the **Password Policy** tab.
3. **Restrict Characters:** Specify how many special characters, numbers, and Unicode characters should be used in a password.
4. The **Password Policy** tab will display all the password policy settings. Enable the settings you prefer to enforce the creation of complex passwords.
5. **Restrict Repetition:** Limit the use of:

Consecutive characters (e.g., aaaa).

A string of consecutive characters from the username and old password (e.g., user01).

6. **Restrict Pattern:** Restrict technicians from using palindromes, dictionary words, and other custom patterns in their passwords.
7. **Restrict Length:** Specify the maximum and minimum password length.
8. **Enable Password Strength Analyzer:** Enable this setting to provide a visual representation of the strength of the password, encouraging technicians to create complex passwords.
9. You can configure the settings to override all the complexity rules if the password meets a predefined password length. You can also specify the number of complexity rules a password must satisfy.

Ban breached passwords during change and reset

The solution can be integrated with Have I Been Pwned?, a leaked password database. This resource detects the use of any breached passwords from the database during password reset or change and bans it. To integrate:

1. Navigate to **Admin > Product Settings > Integration Settings.**
2. Click the **Have I Been Pwned?** tile.
3. Click **Enable HaveIBeenPwned Integration.**

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

Enable MFA for ADSelfService Plus logins

It is just as crucial to enable MFA for ADSelfService Plus logins as it is for other network endpoints like machines, VPN, and OWA. ADSelfService Plus' admin portal provides a myriad of sensitive security features including configuring MFA and SSO, setting password policies, enabling HTTPS, etc. The user portal enables users to perform actions like password change, directory update, employee search, and more. To secure the ADSelfService Plus portal with MFA, follow these steps:

1. Go to **Configuration > Self-Service > Multi-Factor Authentication > Advanced > Applications MFA.**

2. In the *MFA for ADSelfService Plus 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.

Note: The Professional edition of ADSelfService Plus is required to utilize advanced authenticators for MFA.

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

Note: This MFA process will be triggered when a user attempts to access an SSO-enabled application directly

4. Click **Save Settings.**

Enable CAPTCHA for portal logins

It is recommended that admins enable CAPTCHA for ADSelfService Plus portal logins as well. This includes logins into the ADSelfService Plus web portal, self-service password reset web browser portal, and self-service account unlock web portal. To enable CAPTCHA:

1. Go to **Admin > Customize > Login Settings.**
2. Select **Show CAPTCHA (word verification image) on login page.**
3. Enable CAPTCHA for the login pages of admin, domain user, and during password reset and account unlock.
4. Click the CAPTCHA settings link to configure whether to show CAPTCHA every time, or only after a certain number of invalid login attempts.
   i. Select **Show CAPTCHA every time** to always display CAPTCHA whenever someone tries to login to the product.
   ii. 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.
5. Select **Enable audio CAPTCHA** to offer CAPTCHA for visually impaired users.
6. Click **Save.**

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.**

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. They can choose to receive mail alerts for license expiration, product updates, and upcoming events or workshops. For product startup and downtime events, admins can enable both mail and SMS notifications—with SMS alerts sent to a specified mobile number. These settings ensure timely updates and help minimize disruptions by keeping admins informed of all critical system activities. Learn more about notification settings.

9. 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.**

Set a complex password for the ADSelfService Plus database backup file

The ADSelfService Plus database backup files' default password is the reverse string of the filename. We recommend changing this to a different, complex password of at least eight characters. To do this:

1. Go to **Admin > Connection > General Settings.**
2. Under *Privacy settings*, enter the new password in the **Change Password For Database Backup Files.**
3. 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.

ManageEngine
ADSelfService Plus

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