ManageEngine
ADSelfService Plus

Buyer's guide

Your all-in-one ADSelfService Plus handbook

www.adselfserviceplus.com

Index

01 **Introduction** 2
- Password security today 2
- The need for better password management solutions 2

02 **What is ADSelfService Plus?** 3

03 **Why should I consider ADSelfService Plus?** 3
- What ADSelfService Plus offers 3

04 **How will ADSelfService Plus benefit me?** 5

05 **What do I get with each edition of ADSelfService Plus?** 8

06 **What do people say about ADSelfService Plus?** 9

07 **What is the architecture of ADSelfService Plus?** 10
- ADSelfService Plus' components 10
- Optional components 11

08 **Where can I get more information?** 13

Introduction

Password security today

The world has quickly adopted the hybrid working model and moved to cloud-based services. This is great for establishing a flexible work environment. However, this also brings a host of password management hurdles, and password security loopholes that are being exploited by threat actors because many people use weak and compromised passwords. Since passwords are the first line of defense against threat actors, an organization's security is only as strong as its weakest password. It is imperative for an organization to take its password security seriously.



The need for better password management solutions

Native password management tools are not capable of handling the demands of today's world. We now need more granular control, easier access to our services, and security hardening on a case-by-case basis. This is why organizations rely on password management and security solutions to oversee their passwords. These solutions help organizations not only harden their password security measures, but also allow for easy password management with functionalities such as remote password self-service and single sign-on (SSO) for applications. These functionalities help an organization build a strong and hassle-free password framework.



What is ADSelfService Plus?

ManageEngine ADSelfService Plus is an integrated self-service password management and SSO for on-premises and cloud applications. It bolsters an organization's password framework with self-service password reset (SSPR) and account unlock, endpoint and VPN multi-factor authentication (MFA), SSO to enterprise applications, Active Directory (AD)-based multi-platform password synchronization, password expiration notification, and password policy enforcer.

Why should I consider ADSelfService Plus?

What ADSelfService Plus offers

Implementing key password security processes is vital for an organization's defense strategy. Here's how ADSelfService Plus helps meet the demands of your organization:

You're on the lookout for	How ADSelfService Plus can help
Secure authentication	Secure access to machine (Windows, macOS, and Linux OS), VPN, and OWA logins with MFA. Regulate enterprise application access via SSO with advanced authenticators including biometrics, or RSA SecurID.
Remote password self-service	Enable users to perform SSPR, and self-service account unlock only after they prove their identity via the enforced authenticators. Secure cached credential updates via VPN during remote password resets.
Strong password policy enforcement	Enforce strong user passwords by requiring special characters and blacklisting dictionary words and patterns. Prevent users from using previous passwords during password resets.

With ADSelfService Plus, you can implement five capabilities that Gartner considers critical for an IAM framework.

Gartner recommended critical IAM capabilities in ADSelfService Plus

1. **User authentication methods:**
   Avoid impersonation attacks using biometrics and other advanced authentication methods. Step up your security by implementing MFA to access endpoints and applications.

2. **Adaptive authentication:**
   Enforce risk-based adaptive authentication using factors such as user location, IP address, time of previous logon, and device footprint.

3. **SaaS application enablement:**
   Set up SAML 2.0-based SSO for hundreds of enterprise SaaS applications, like Salesforce, ServiceNow, and Slack.

4. **Approval-based workflows*:**
   Build purpose-oriented business workflows. Create the required levels of approval by including the rights of the stakeholders. Define the approval flows for business processes, such as user account creation, modification, or permissions management.

*Approval-based workflow functionality requires ADManager Plus, ManageEngine's unified Active Directory, Exchange, and Microsoft 365 management and reporting solution.

How will ADSelfService Plus benefit my organization?

ADSelfService Plus comes packed with functionalities that go beyond native capabilities. Here's a list of what the solution can do, and what you get with each features:

SSPR and account unlock

Enables users to perform AD domain password resets and perform account unlocks 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.

What you receive

Empowers users to reset their passwords and unlock their accounts. This reduces the number of help desk tickets and unburdens help desk personnel. It also improves user productivity as passwords can be reset and accounts can be unlocked promptly and efficiently.

Enterprise SSO

Reduces the number of logins performed by the user through enabling enterprise SSO for Security Assertion Markup Language (SAML) application collections like Google Workspace, Microsoft 365, and Salesforce.

What you receive

With a single password, users can access multiple enterprise applications and accounts easily and efficiently.

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, Microsoft 365, Google Workspace, and Salesforce.

What you receive

Any changes to the domain password result in the changes being reflected across the integrated applications as well.

MFA

By implementing additional layers of identity verification and enhancing the existing credential-based authentication, MFA improves security. ADSelfService Plus implements additional identity verification steps for:

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

This solution supports up to 18 authentication techniques including biometrics, Google Authenticator, Microsoft Authenticator, time-based one-time password (TOTP), and Security Question and Answer.

What you receive

Even if attackers misappropriate users' credentials, they still need to complete the successive stages of authentication to gain access. Utilizing MFA, an organization is safeguarded because even exposed passwords are useless to attackers.

Password expiration notification

Sent through email and SMS, or as push notifications, password expiration notifications enable sending multiple reminder notifications on specific days prior to the expiration date.

What you receive

Notifies users about their impending domain password expiration and reminds 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-grained 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 use of weak passwords, dictionary words, and palindromes.

What you receive

Users can be required to adhere to these policies strictly, preventing them from setting weak passwords that might jeopardize the security of the organization.

Conditional access

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

What you receive

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

Self-service directory update

Enables 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 provided attribute values.

What you receive

Helps decrease the help desk workload while improving user productivity.

Employee directory search and organization chart

Enables users to search for information on other users, contacts, and groups in the organization, and view the organization chart that displays all the employees in the organizational hierarchy.

What you receive

Helps users discover details about other users from a single portal.

Mail group subscription

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

What you receive

Lets users gain access to the email groups they need without help desk assistance.

What do I get with each edition of ADSelfService Plus?

ADSelfService Plus is available in three editions: Free, Standard, and Professional. Here's what is included with each edition:

Standard	Professional	Free (for up to 50 domain users)
Web-based Self-Service Password Reset and Account Unlock	Includes everything in the Standard edition, and:	Supports all functionalities in the Professional edition
Password Expiry Notifier	Password Reset from Windows, macOS, and Linux login screens	Password Self-Service
Password Policy Enforcer	MFA for Windows, macOS, and Linux machine logons	Directory Self-Service
Real-time Password Synchronizer	MFA for VPN logons	Cloud Applications SSO & Password Sync
Password Reset Using iOS and Android App as well as Mobile Browser	MFA for OWA logons	
Self-Service Directory Update, Employee Search, Organization Chart, and Mail Group Subscription	Cached Credentials Update for Remote Password Reset Password Policy	
	Enforcement in Windows Change Password Screen and ADUC	
Starts at $595 for 500 domain users	Starts at $1195 for 500 domain users	

What do people say about ADSelfService Plus?

“

Now users do not have to travel to the office to perform Active Directory password resets. Our help desk calls related to password resets have been reduced by 100%.

Piergiuseppe Delfino

CIO at AUBAY SpA, Italy

“

Other options were requiring a modification of the Active Directory schema. I liked that ADSelfService Plus did not. The ability to ‘brand’ the tool to our school was also important.

Robert Peterson

Technical Support Manger, The Principia

“

The deployment is very simple, which makes it nearly fun. We didn’t find any other software which is as fast to deploy as ADSelfService Plus. The instructions are clear and straightforward; the support is working great.

Matthias Ziolek

Manager, Landratsamt Schwarzwald-Baar-Kreis

What is the architecture of AD360?

ADSelfService Plus components

These are the four components required to run ADSelfService Plus:

- Server
- Database
- AD integration
- ADSelfService Plus web portal

Server

The server is where ADSelfService Plus is installed, and it can be a member server or a domain controller. If you are configuring a high-availability environment, you will need a primary server and a secondary server. Both servers need to have ADSelfService Plus installed.

To enable load balancing, a primary server and one or more secondary servers have to be configured. All the servers need to have ADSelfService Plus installed.

Database

ADSelfService Plus uses a database to store information like AD attribute details, audit data, product configuration data, and enrollment data. The product comes with a built-in PostgreSQL database. You can also use a standalone Microsoft SQL database or PostgreSQL database.

Integration with AD

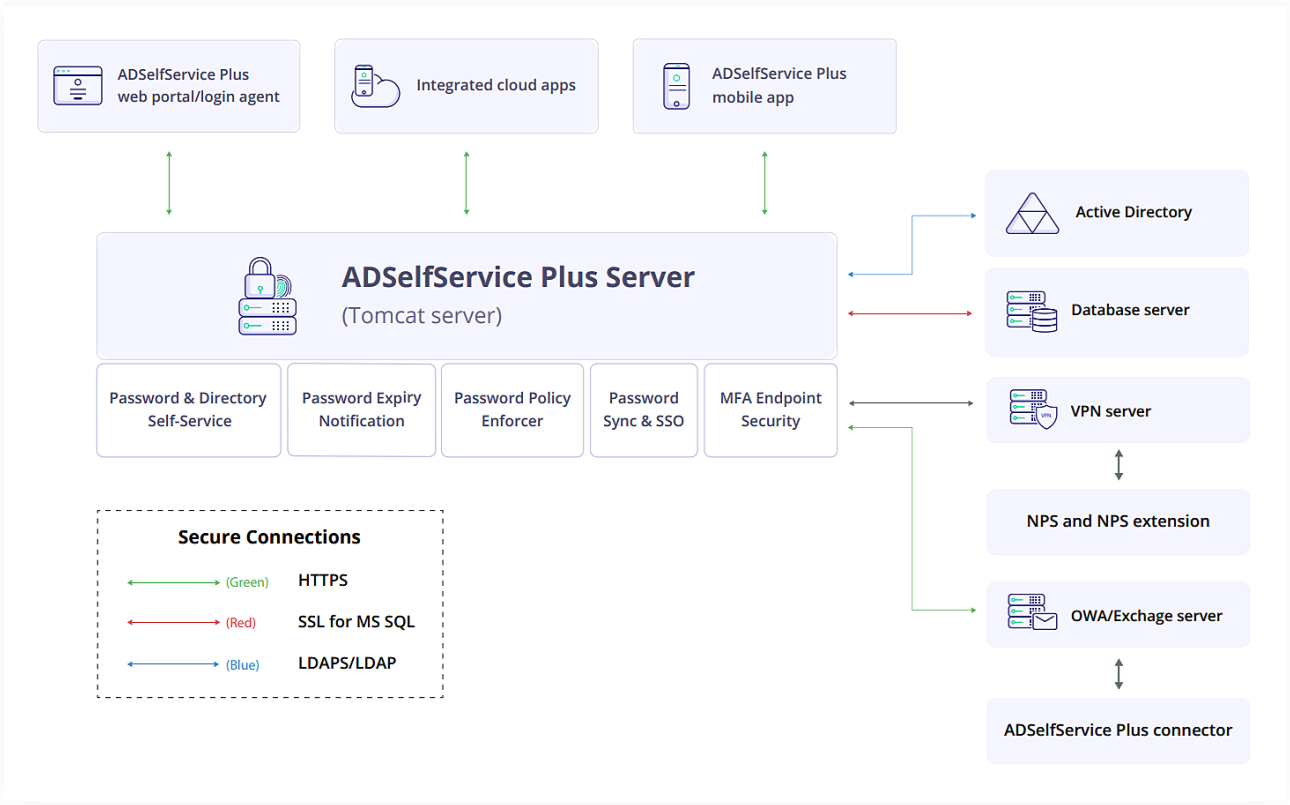
Scheduled synchronization of data between ADSelfService Plus and AD is necessary to allow the IT administrators to create various self-service policies and apply them to OUs and groups, install the login agent on domain computers, and configure various features and settings from within the product's portal. Synchronization with AD is also necessary for end users to perform various self-service actions.

ADSelfService Plus web portal

There are two kinds of ADSelfService Plus web portals:

Admin portal: The admin portal lets the IT administrator of the solution configure domain and connection settings (SSL, proxy server, etc.), create and apply various policies, deploy MFA, integrate on-premises and cloud applications with password sync and SSO, and more.

User portal: The user portal lets the users enroll themselves in ADSelfService Plus, perform the various self-service actions, search for employees, view the organization chart, etc.



ADSelfService Plus architecture

Optional components

ADAudit Plus helps you identify signs of a threat by monitoring for and alerting you about any suspicious behavior. By upgrading to AD360, you can also manage critical aspects of AD in the event of a breach. With the upgrade, you can:

ADSelfService Plus login agent

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

The login agent can either be pushed onto the client computers using the admin portal, Active Directory GPOs, Microsoft System Center Configuration Manager, third-party endpoint management solutions like ManageEngine Desktop Central, or be installed manually.

ADSelfService Plus password sync agent

The ADSelfService Plus password sync agent synchronizes native password changes across all enterprise applications integrated with ADSelfService Plus. It accomplishes this through password changes using the Ctrl+Alt+Del option, and password resets using the Active Directory Users and Computers console. It also enforces customized password policies created in ADSelfService Plus during native password changes. The Password Sync Agent must be installed on all the domain controllers in a configured domain.

ADSelfService Plus mobile application

The ADSelfService Plus mobile app lets domain users perform AD password resets and account unlocks using their mobile device. It enables users to 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
- Informing users of impending password and account expiration
- Distributing enrollment reminders

With the app, users can also authenticate themselves using a MFA method like TOTP passcode, push notifications, fingerprint-based, and QR codes. The mobile app can be either manually installed by users or pushed to mobile devices by the IT administrator.

Integration with enterprise applications

Through password synchronization and SSO, ADSelfService Plus integrates with various enterprise applications such as Google Workspace, Salesforce, Microsoft 365, and Dropbox. When password synchronization is enabled, any change to the users' domain passwords is synchronized across all the integrated applications, enabling the user to access all of them with a single password. In the case of SSO, if the user has logged into their ADSelfService Plus account, they are automatically logged into these cloud applications without having to furnish their user credentials.

VPN server and Network Policy Server (NPS)

To secure your VPNs using ADSelfService Plus' MFA feature, the VPN server should use a Windows NPS to configure RADIUS authentication, and the ADSelfService Plus NPS extension has to be installed in the NPS. This extension mediates between the NPS and ADSelfService Plus to enable MFA during VPN connections.

Where can I get more information?

Resource	Description
Admin guide	A comprehensive, one-stop guide that provides information for IT administrators on setting up and running ADSelfService Plus.
User guide	A detailed explanation for users on getting started and working ADSelfService Plus.
Detailed architecture	An in-depth resource about ADSelfService Plus components and deployment scenarios.
Privileges and permissions requirement guide	An elaboration of all the necessary roles and permissions required for ADSelfService Plus.

To get a personalized demo of ADSelfService Plus.

Click here to request a demo

To get a customized quote for ADSelfService Plus.

Click here to get a quote

For more details or speak to someone:

ad360-support@adselfserviceplus.com +1-408-916-9890 (toll-free)