ManageEngine
ADSelfService Plus

PROOF OF CONCEPT

www.adselfserviceplus.com

Table of contents

Executive summary

This document evaluates the feasibility and success of implementing ADSelfService Plus within the organization's environment. The primary objective is to assess how the solution enhances identity security, optimizes operational efficiency, and improves user experience through self-service capabilities. The proof of concept (PoC) helps determine the product's suitability for the organization's identity security requirements.

Scope

The PoC focuses on validating key functionalities of ADSelfService Plus, including self-service password reset and account unlock, multi-factor authentication (MFA), single sign-on (SSO), password synchronization, and password policy enforcement. The evaluation will involve a set of users to demonstrate usability, integration with Active Directory, and the overall impact on help desk workload and access security.

Product overview

ADSelfService Plus is an identity security solution that ensures secure and seamless access to enterprise resources and establishes a Zero Trust environment. With capabilities such as adaptive MFA, SSO, 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. Key features include:

- MFA
- Conditional access
- Self-service password reset / account unlock
- Enterprise SSO
- Password synchronization
- Password policy enforcement
- Password expiration notification
- Directory self-update and corporate directory search

Goals and objectives

ADSelfService Plus aims to achieve the following goals and objectives:

- Evaluate the efficiency of self-service password management by enabling users to securely reset forgotten passwords and unlock their accounts without IT intervention, thereby reducing help desk workload and downtime.
- Assess the robustness of MFA in securing user logons across self-service portals, endpoints (Windows/macOS/Linux), VPN, and Outlook Web Access (OWA), ensuring protection against credential-based attacks.
- Examine the seamless operation of SSO across cloud and on-premises applications, providing a unified user experience when accessing enterprise resources.
- Validate password synchronization capabilities across multiple applications to deliver password updates in AD that are consistently propagated to all connected systems in real time.
- Evaluate how advanced password policy enforcement strengthens password security and ensures compliance with internal and external security standards.
- Assess the usability and adoption of directory self-update and group subscription features, focusing on how effectively users can manage their own profile information and group memberships without IT support.
- Determine the scalability of the solution.

Prerequisites

To facilitate a smooth deployment and evaluation of ADSelfService Plus, ensure that the following prerequisites are met:

- The test environment must meet the system requirements specified for deploying the application.
- A service account with Domain Admin permissions, or with the delegated privileges outlined in the required privileges and permissions document, must be available for configuration.

Methodology

ADSelfService Plus follows the methodology below:

- Determine the specific organizational scenarios that need to be tested.
- Configure and deploy ADSelfService Plus in the test environment.
- Set up the required test accounts for the testing scenario.
- Test the features of ADSelfService Plus and gather feedback on their functionality in the organization.
- Evaluate the results against the predefined success criteria.

Timeline

The installation and setup of ADSelfService Plus will take approximately **30 minutes,** followed by configuration and feature testing, which is expected to take around **one hour**. After successful configuration, a client walkthrough will be conducted to demonstrate the product's capabilities and gather feedback, lasting approximately **one hour**.

Activity	Duration
Installation and setup	30 minutes
Configuration and testing	1 hour
Client walkthrough	1 hour
Total	**2.5 hours**

Note: The duration can vary based on the complexity of the implementation.

Evaluation scenarios

SCENARIO 1

Empowering users with self-service password reset and account unlock through ADSelfService Plus

Forgotten passwords and account lockouts are among the most common reasons for IT help desk tickets. These incidents cause user downtime, increase administrative burden, and slow business productivity. Manual intervention for password resets or unlocks also increases the risk of delays and potential security issues.

ADSelfService Plus's role in enabling password self-service

ADSelfService Plus enables users to securely reset their passwords and unlock their accounts without IT assistance through multiple interfaces—web portal, login screen (Windows, macOS, Linux), and mobile app. Before performing these actions, users must verify their identity using MFA (such as email/SMS OTP, push notification, security questions, or biometric authentication). This self-service approach reduces password-related tickets, strengthens security, and improves user autonomy.

Success criteria

- The success rate of password resets and account unlocks completed without IT involvement.
- The average time taken for users to regain access to their accounts.
- The reduction in password-related help desk tickets within the pilot group.
- Positive feedback from users on ease of use and accessibility.

SCENARIO 2

Strengthening logon security through ADSelfService Plus' MFA capability

Single-factor authentication based solely on passwords exposes organizations to credential theft and brute-force attacks. Without additional verification layers, compromised credentials can easily lead to unauthorized access and data breaches.

ADSelfService Plus's role in secure authentication

ADSelfService Plus provides adaptive MFA for both self-service actions and logon access to endpoints such as Windows, macOS, Linux, VPN, and OWA. It supports a wide range of authenticators including push notifications, time-based one-time password (TOTP), biometrics, smart cards, and third-party authenticators. Conditional access rules can be applied based on login time, IP address, device or location to enforce contextual authentication. This helps strengthen security without compromising user convenience.

Success criteria

- The number of successful MFA verifications performed during endpoint logons.
- The enforcement of conditional access policies as per organizational requirements.

SCENARIO 3

Streamlining user authentication to multiple applications and providing unified access through ADSelfService Plus' SSO capability

Frequent logins across numerous business applications lead to credential fatigue, reduced productivity, and increased password reuse.

ADSelfService Plus's role in simplified user authentication

ADSelfService Plus provides SSO for cloud and on-premises applications through SAML, OAuth, and OpenID Connect. After authenticating once, users can securely access all assigned applications from a centralized portal using their AD credentials. Integrated MFA ensures that access to sensitive applications remains protected. This unified access experience boosts productivity and minimizes password-related help desk calls.

Success criteria

- Successful configuration of selected cloud and on-premises applications for SSO.
- Average time saved per user when accessing applications via the SSO portal.
- Reduction in password reset or account lockout tickets for integrated apps.

SCENARIO 4

Maintaining consistency across systems through ADSelfService Plus' password synchronization capability

Inconsistent passwords across multiple systems lead to synchronization issues, user frustration, and additional administrative work. Delays in updating credentials across connected apps can lock users out or create security risks.

ADSelfService Plus's role in synchronized password management

ADSelfService Plus includes a Password Sync Agent that synchronizes password changes in AD with supported cloud and on-premises applications. It ensures password consistency across environments, eliminating mismatched credentials and improving user experience.

Success criteria

- Successful synchronization of password changes between AD and connected applications.
- Absence of synchronization errors during the test period.
- Average latency observed between AD password change and target application update.
- Feedback from users on improved consistency and reduced login issues.

SCENARIO 5

Enforcing password security with ADSelfService Plus' password policy enforcer

Weak, repetitive, or compromised passwords pose a major threat to organizational security. Native AD password policies often lack the flexibility to enforce modern complexity rules or block predictable patterns.

ADSelfService Plus's role in enforcing secure password policies

ADSelfService Plus's Password Policy Enforcer enables administrators to define custom password rules that go beyond AD's native limitations. Organizations can block dictionary words, sequential or repeated characters, keyboard patterns, palindromes, and even known breached passwords (via integrations like Have I Been Pwned). This ensures users create strong, compliant passwords aligned with the organization's security and compliance standards.

Success criteria

- The number of weak passwords prevented during resets and password changes.
- User compliance rate with the new password policy.
- Reduction in password-related incidents.
- Validation that password policies are consistently applied across all OUs.

SCENARIO 6

Empowering users to manage directory information through ADSelfService Plus' self-update and group subscription features

Keeping user information and group memberships up to date is crucial for effective access management,communication, and compliance. Relying solely on IT staff to maintain these details can lead to delays, increased workload, and potential data inconsistencies.

ADSelfService Plus's role in directory self-management

ADSelfService Plus provides users with self-service capabilities to update their personal directory attributes (such as phone number, address, or department) and manage their group memberships in accordance with predefined policies. Administrators can configure customizable self-update layouts to specify which directory attributes users are allowed to modify. This delegation minimizes IT workload and ensures directory information remains accurate and up to date.

Success criteria

- The number of successful directory attribute updates and group membership changes performed by users.
- The reduction in help desk requests related to directory or group updates.

SCENARIO 7

Ensuring compliance through ADSelfService Plus' reporting and audit capabilities

Without comprehensive visibility into self-service activities, password changes, and MFA adoption, organizations can struggle to maintain compliance, detect anomalies, and assess the overall health of their identity and access management framework. Lack of centralized reports can make it difficult to identify security risks or demonstrate compliance with internal and external audit requirements.

ADSelfService Plus's role in compliance reporting

ADSelfService Plus provides built-in reports that provide administrators comprehensive insights into all self-service and authentication activities. These reports are organized into five categories—Active Directory Reports, Password Self-Service Reports, MFA Reports, GINA/macOS/Linux Agent Installation Reports, and Other Reports—covering details such as domain user accounts and passwords, self-service actions, identity verification, enrollment, and more.

Administrators can schedule and export reports in various formats (CSV, PDF, XLS).These insights help monitor user adoption, detect unusual activities, and ensure compliance with security and audit requirements like ISO 27001, SOX, HIPAA, and the GDPR.

By leveraging ADSelfService Plus's reporting features, organizations can proactively maintain accountability, gain deeper visibility into user activities, and improve audit readiness.

Success criteria

- The time taken to generate and export reports can be determined by the duration required by ADSelfService Plus to process data and convert it into comprehensible reports.
- The data accuracy of reports can be measured by verifying whether the data presented is correct, up-to-date, and free from errors or inconsistencies by comparing reported data with actual data sources.

Stakeholders

The list of key stakeholders involved in the PoC of ADSelfService Plus:

Solution sales executives:
Technical experts from ADSelfService Plus' support team or presales team.

Client representatives:
System admins, network engineers, database admins, or security analysts from the client's organization.

Conclusion

The PoC demonstrated that ADSelfService Plus effectively enhances identity security, reduces IT workload, and improves user experience through secure self-service capabilities. The solution validated core functionalities including password self-service, MFA, SSO, password synchronization, and reporting.

Users were able to reset passwords, unlock accounts, and access enterprise applications securely with minimal IT assistance. MFA and SSO improved authentication security and access efficiency, while password synchronization and policy enforcement supported consistent and compliant credential management.

Administrators benefited from comprehensive reporting, enabling better monitoring, compliance, and governance. The solution proved scalable, aligning with the organization's Zero Trust and identity management goals.

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