ManageEngine
ADSelfService Plus

ADSelfService Plus

Security Measures Guide

Security measures in ADSelfService Plus

This guide provides a list of the various security measures available in ADSelfService Plus and walks you through what they do and when to use them. These security measures can be split into three categories based on when they are used and what they protect:

- Security features to prevent common cyberattacks
- Post-deployment security measures for connections to the ADSelfService Plus server
- Security measures to protect access to ADSelfService Plus and its features

Security measures to prevent **Common Cyberattacks**

ADSelfService Plus offers the following security features that help protect Active Directory (AD) domains and their user accounts from attacks like brute-force, password spraying, and credential stuffing.

Endpoint MFA

MFA can be a boon to organizations, as it strengthens the existing username and password-based authentication by adding extra levels of security. This helps secure users' accounts and the AD environment they belong to.

ADSelfService Plus' MFA feature can be used to secure the following enterprise endpoints:

- Workstations and servers
- Remote access points like RDP and VPN
- Internal Windows access points such as machine unlocks and elevated User Account Control prompts
- Enterprise cloud applications

Learn more about Endpoint MFA in ADSelfService Plus.

Types of MFA for machines

Windows logins can be secured by MFA in two ways:

Online MFA: The online MFA process in ADSelfService Plus verifies the user identity using registered authenticator data and a network connection between the product server and user machines.

Offline MFA: Offline MFA verifies the identity during Windows machine access without ADSelfService Plus communication by using secure authenticator data stored in the user's device by the Windows login agent.

You can apply MFA for Windows, macOS, and Linux machines in two ways:

User-based MFA: Each login attempt by a specific user will be secured through MFA. Machine-based MFA: Attempts by any user to log in or unlock a specific machine will be protected by MFA. This method also protects elevated UAC prompt.

Passwordless authentication for enterprise applications

Single-sign on to enterprise applications can be protected by passwordless authentication. The authentication system uses advanced methods such as biometrics and software and hardware TOTP authentication to secure logins.

Password Policy Enforcer

ADSelfService Plus' Password Policy Enforcer feature allows admins to create custom password policies in addition to the existing domain password policy offered by Microsoft. To create a password policy, admins simply have to select a self-service policy (this assigns the password policy only to users in the OUs and groups that come under this self-service policy) and choose the required password complexity rules from the list available. The rules offered help control the:

1. Characters used in the password.
2. Repetition of characters in the password and the usage of old passwords.
3. Usage of patterns, dictionary words, and palindromes.
4. Length of the password.

This ensures users create strong, complex domain passwords that are resistant to hacks. Learn how to enable the Password Policy Enforcer.

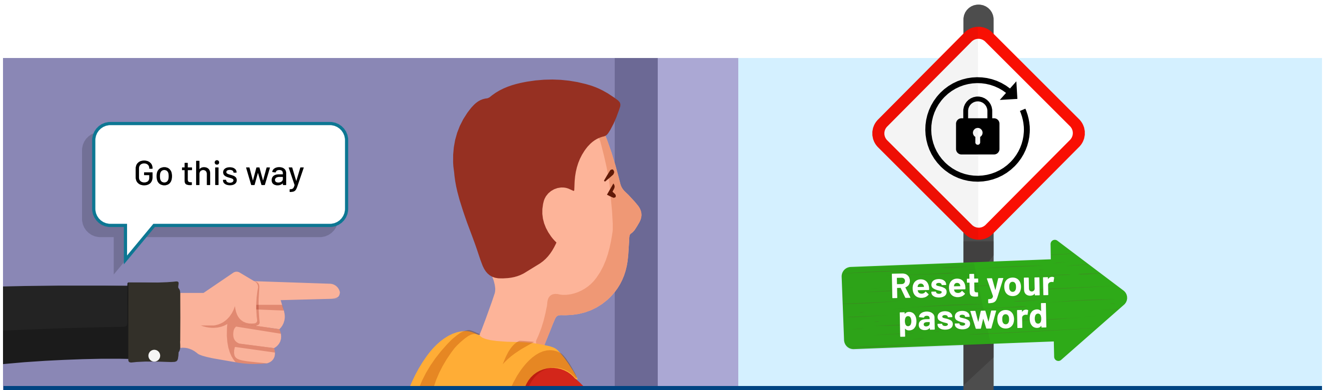
Integration with Have I Been Pwned

Have I Been Pwned is a service that informs users whether the passwords they use have been exposed during past data breaches. ADSelfService Plus can be integrated with Have I Been Pwned to prevent users from employing leaked passwords while resetting or changing their password. Here are the steps to configure this integration.

Password Expiration Notification

Another feature that ensures users maintain good password hygiene is the Password Expiration Notification. Microsoft offers the Password Age setting that imposes password expiration to ensure users change their passwords regularly. With the Password Expiry Notification feature, users are alerted about the impending expiration of their passwords through email, SMS, and push notifications. This encourages them to change their passwords before expiration. Learn how to enable password expiration notifications.

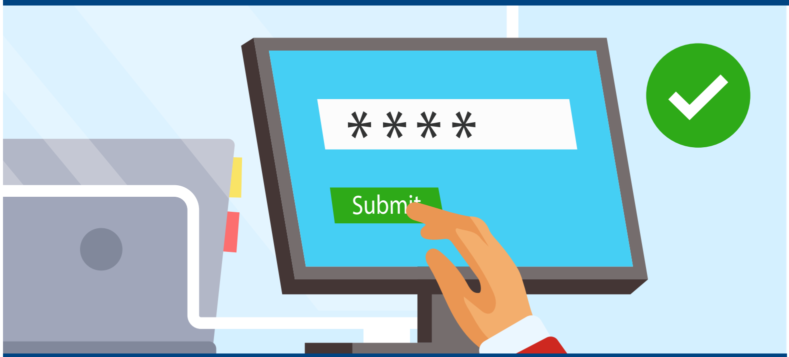
How ADSelfService Plus secures the self-service password reset action.



ADSelfService Plus provides users the option to reset their passwords from the login screen of their machines.

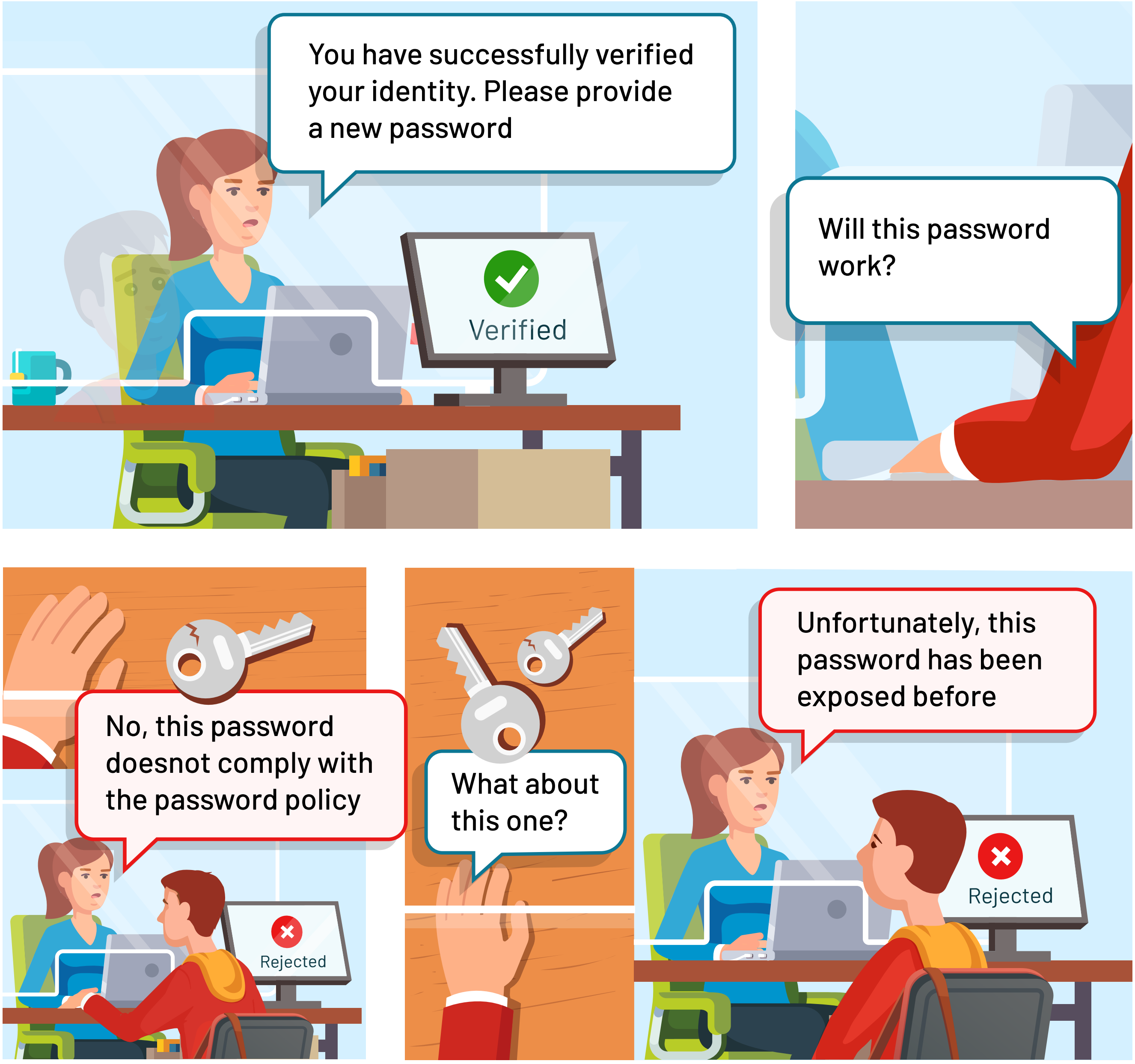
Reset your password
Username, please
Testuser1
Okay, you are a part of the Active Directory domain. Please verify your identity

Multi-factor authentication protects the password reset process through any of the 15 authentication methods supported.



Google Authenticator OTP

Fingerprint


You have successfully verified your identity. Please provide a new password
Verified
Will this password work?
No, this password doesnot comply with the password policy
Rejected
What about this one?
Unfortunately, this password has been exposed before
Rejected

Yes this works! It complies with the password policy and hasn't been exposed
This one?
Updated
******

The Password Policy Enforcer mandates users to comply with a custom password policy, and integration with Have I Been Pwned? prevents the usage of already exposed passwords.

Post-deployment **Security Measures**

Once ADSelfService Plus is deployed in an organization, the measures mentioned below need to be performed:

- Secure the data stored in the ADSelfService Plus installation directory.
- Secure inbound connections between the ADSelfService Plus server, the user's web browser, or the ADSelfService app. This is done by:
  - Configuring SSL.
  - Adding ciphers and protocols.
  - Applying security parameters.
- Secure outbound connections between the ADSelfService Plus server, the mail server, and the external database server. This is done by:
  - Enabling LDAPS.
  - Configuring an SSL/TLS connection with the email server.
  - Configuring an SSL connection with MS SQL Server.

Check out the post-deployment security measures guide for more information and detailed instructions on how to implement these security measures.

Security measures to protect access to ADSelfService Plus and its Features

ADSelfService Plus offers certain features and settings that protect access to the solution and its various features by:

- Securing ADSelfService Plus logins and self-service actions.
- Controlling access to the ADSelfService Plus portal.
- Monitoring users' domain status and actions.

Secure ADSelfService Plus logins and self-service actions

The following features and settings help protect access to the self-service actions as well as logins into the ADSelfService Plus portal:

Multi-factor authentication

ADSelfService Plus supports multi-factor authentication (MFA) to protect the self-service password reset and account unlock process. MFA also helps in securing ADSelfService Plus logins. The authentication methods listed above are employed here as well. Check out this guide for steps to enable MFA for self-service actions and ADSelfService portal logins.

Conditional access

ADSelfService Plus offers the Conditional Access feature that helps manage users' access to self-service features and enterprise applications based on their risk factors. With this feature, admins can create multiple self-service policies for a set of users and create conditions for each self-service policy based on these factors:

- IP address
- Type of device
- Working hours
- Geolocation

During an access attempt, the user's risk factors are analyzed, and if the conditions are satisfied, a specific policy is applied. With this feature, admins can seamlessly tighten or slacken login security through MFA, alter the accessibility to self-service features, and enable or disable SSO for enterprise apps without affecting the user experience.

Block users who have failed at identity verification

Admins can block access to self-service password reset and account unlock from the ADSelfService portal, login agent, or mobile app for a certain period after a specific number of failed authentication attempts. The maximum number of failed attempts after which users are blocked, and the time period for which they are blocked, can be set by the admin. Learn how to enable this setting.

CAPTCHA

Admins can enable CAPTCHA to prevent a bot-based brute-force attack. CAPTCHA can be implemented during:

- Self-service password resets and account unlocks.
- ADSelfService Plus logins.

ADSelfService Plus also offers the option of audio CAPTCHA to make identity verification accessible to all users. Learn how to enable CAPTCHA in ADSelfService Plus.

Restrict self-service actions

Admins can restrict the number of self-service password resets and account unlocks a user can perform within a specific period so that users don't abuse the self-service option to circumvent the password history requirement. Learn how to enable this feature.

Deny concurrent logins

Once the Deny Concurrent Logins setting is enabled, a user can only have one active ADSelfService Plus session at a time. They are prevented from having multiple active sessions simultaneously. Learn how to enable this setting.

ADSelfService Plus is also equipped with built-in safety measures that thwart the following security issues:

Bypassing client-side validations

Here, an attacker bypasses the client-side input validation for targeted content, say, password fields. Attackers usually bypass a web application's input validations by either removing JavaScript using a web developer tool or by handling the HTTP request (using a proxy tool) in a way that it does not go through the browser. ADSelfService Plus practices both client-side and server-side validation to defend against this type of attack.

SQL injection through framework builds

SQL injection occurs when an attacker adds or injects malicious code into a SQL statement executed by the web application. A SQL injection can let a hacker misappropriate or destroy existing data and even gain complete control over the web application's server and network. Database operations for ADSelfService Plus are handled through our internal framework to prevent SQL injections and other similar attacks.

Cross-site request forgery (CSRF) vulnerability

In a CSRF attack, the attacker causes the user to carry out an action unintentionally when they are logged in to an application. This sends an HTTP request the user did not intend to raise, which includes a cookie header that contains the user's session ID. Depending on the nature of the action, the attacker might be able to gain full control over the user's account. If the compromised user has a privileged role within the application, the attacker might be able to take full control of all the application's data and functionality.

ADSelfService Plus sends out every HTTP request with a token. This prevents the execution of actions that do not provide necessary authentication tokens.

All the product-related data, such as domain details, details of accounts that use ADSelfService Plus authentication, and user enrollment details, are stored in the product using strong encryption methods for maximum security. The encryption methods used in ADSelfService Plus are some of the most secure and are considered logically unbreakable.

Control access to the ADSelfService Plus portal

ADSelfService Plus offers the below settings that scrutinize access to the ADSelfService Plus portal.

Role-based access

ADSelfService offers an option for providing role-based access to the portal for non-admin users (technicians) too. Once a technician is created, they can be assigned one of two roles: Operator or Super Admin.

- **Operator:** The Operator role allows technicians to access the Dashboard tab and view statistics on password expiration, locked accounts, users' enrollment status, and self-service actions. They can also view built-in reports in the Reports tab that audit users' actions and provide information on users' accounts, passwords, and enrollment.
- **Super Admin:** The Super Admin role provides the technician with complete access to the admin portal.

Here are the steps to create technicians and provide them with role-based access to the ADSelfService Plus admin portal.

IP-based admin access restriction

Access to the ADSelfService Plus admin portal can also be restricted based on IP address. With the Allow/Restrict Application Access option, admins can specify selective IP addresses that can be either allowed to or denied from accessing the ADSelfService Plus admin portal. This ensures that the admin portal is being accessed only from the machines of admins or technicians with the necessary privileges. Learn how to enable this setting.

Session expiration

Admins can also set the maximum idle time beyond which any ADSelfService Plus session expires using the Session Expiration Time setting. This ensures that the ADSelfService portal is not left open and unattended. Learn how to enable this setting.

Monitor users' domain status and actions

ADSelfService Plus has security measures in place to help admins monitor domain user accounts' status and actions. By staying informed, admins can notice suspicious activity in real time and take immediate measures to alleviate or even hinder security issues.

Audit Reports

Real-time audit reports help admins monitor users' activities and spring into action if they notice anything out of the ordinary. ADSelfService Plus offers built-in reports that audit the following:

- Password resets
- Account unlocks
- Directory self-updates
- Password changes
- Notification delivery
- Identity verification failures
- Users' authentication attempts
- Blocked users

These extensive reports provide information such as when the action was performed, the machine from which it was attempted, the status of the action, and the number of attempts. The reports can be filtered for specific entries; exported in various formats like CSV, CSVDE, HTML, PDF, and XLS; and sent to the desired email addresses. Learn how to view, filter, and export audit reports in ADSelfService Plus.

Approval workflow

Once an approval workflow is enabled in ADSelfService Plus, when users attempt to perform self-service actions like password resets, account unlocks, or directory self-updates, requests are raised in the help desk. Only when the requests are approved can users proceed with the actions.

In order to configure an approval workflow, ADSelfService needs to be integrated with ManageEngine ADManager Plus—AD management, reporting, delegation, and workflow management software. Learn how to configure an approval workflow for self-service actions.

User action notifications

Users can be apprised through email, SMS, and push notifications when self-service password resets and account unlocks, directory self-updates, and password changes are performed from their user accounts. Admins can also be notified about the users' actions. Alerts are also sent when user accounts are blocked from ADSelfService Plus. Learn how to enable these notifications.