ManageEngine
ADSelfService Plus

Zero password reset tickets: Fact or fiction?

www.adselfserviceplus.com

Table of Contents

Why do organizations need a password reset solution?

Password reset tickets are tiresome. Nobody knows this more than IT administrators who are forced to push more critical IT issues to the back of the queue to handle password reset tickets. Due to the time needed to verify user identities and reset passwords, password reset calls can severely reduce help desk productivity. According to a 2018 Forrester report, several large businesses have spent over $1 million trying to resolve password-related help desk calls.

How does ADSelfService Plus help?

ADSelfService Plus offers self-service password management as a solution for password reset ticket issues. With ADSelfService Plus' self-service password management capability in place, users can securely reset passwords and unlock accounts on their own, without any assistance from the IT team.

With ADSelfService Plus, users can reset Active Directory (AD) and cloud application passwords from multiple access points.

Users will be able to reset their passwords regardless of whether they are:

- ✓ **In the office:** Supports password resets via the login screen of the users' workstations (Windows, macOS, and Linux).
- ✓ **On the move:** Empowers users to perform password resets from mobile devices.
- ✓ **At home:** Enables users to update cached credentials in their workstation.

Simply put, ADSelfService Plus brings the help desk password reset tickets backlog to zero by helping users reset passwords anywhere, at any time.

Self-service password management portal registration

Before users can self-reset their passwords, they must complete the registration process in ADSelfService Plus. Enrollment is a one-time process; users enter their mobile number and email address, answer security questions, or provide other details in ADSelfService Plus to register for self-service password management.

Based on enforced multi-factor authentication (MFA) techniques, users need to provide certain information. For example, if admins have enforced security questions and answers as the method for authenticating users' identities, users will need to provide appropriate answers to the displayed questions. ADSelfService Plus verifies user identities during self-service password resets using the information users provide during the enrollment process. You can also choose to auto-enroll users by importing their enrollment data, and make the self-service password management option available to end users as soon as ADSelfService Plus is installed. Learn more about the enrollment process.

The self-service password reset process in action

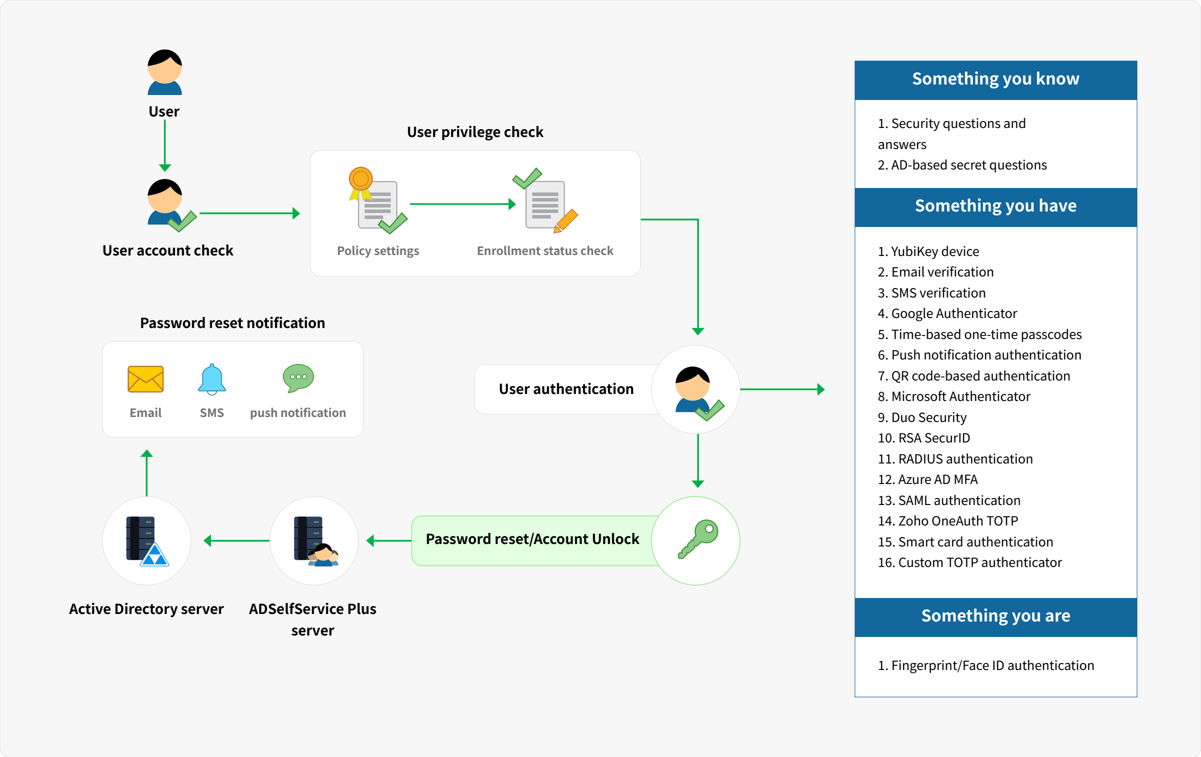
Every time a user attempts to access the password self-service portal, ADSelfService Plus initiates the following workflow:

1. User domain check

2. User authentication

3. Resetting the user password

4. Notifying the user


User
User account check
User privilege check
Policy settings
Enrollment status check
Password reset notification
Email
SMS
push notification
User authentication
Password reset/Account Unlock
Active Directory server
ADSelfService Plus server
Something you know
1. Security questions and answers
2. AD-based secret questions
Something you have
1. YubiKey device
2. Email verification
3. SMS verification
4. Google Authenticator
5. Time-based one-time passcodes
6. Push notification authentication
7. QR code-based authentication
8. Microsoft Authenticator
9. Duo Security
10. RSA SecurID
11. RADIUS authentication
12. Azure AD MFA
13. SAML authentication
14. Zoho OneAuth TOTP
15. Smart card authentication
16. Custom TOTP authenticator
Something you are
1. Fingerprint/Face ID authentication

1

User domain check

In the first step of the self-service password reset process, end users are requested to provide their domain username.

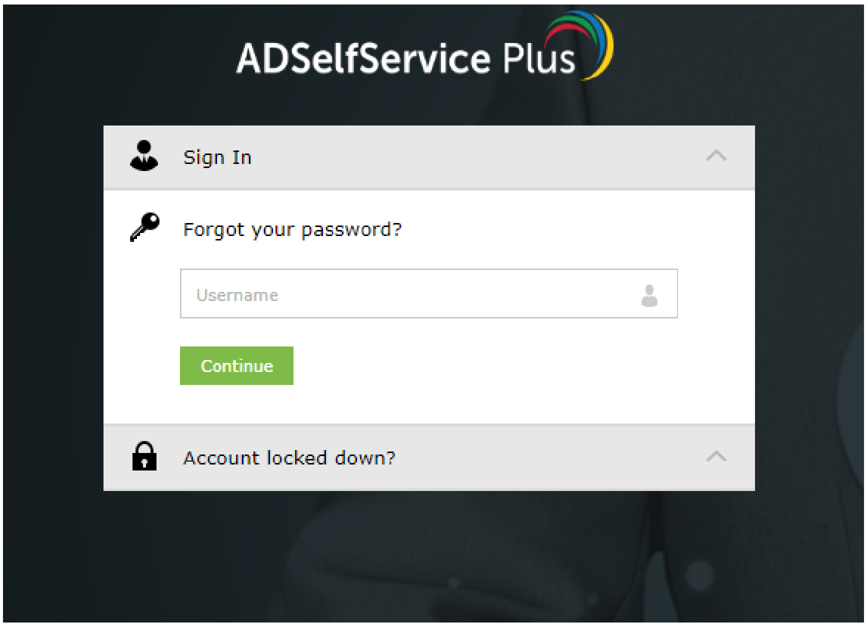
ADSelfService Plus then checks whether:

a. The user has a valid AD domain account (not restricted by ADSelfService Plus).

b. The user belongs to a self-service policy that enables them to reset their password.

c. The user has enrolled with ADSelfService Plus using any of the enforced authentication techniques for identity verification.

If the user satisfies all the above conditions, they will be allowed to proceed to the next step.



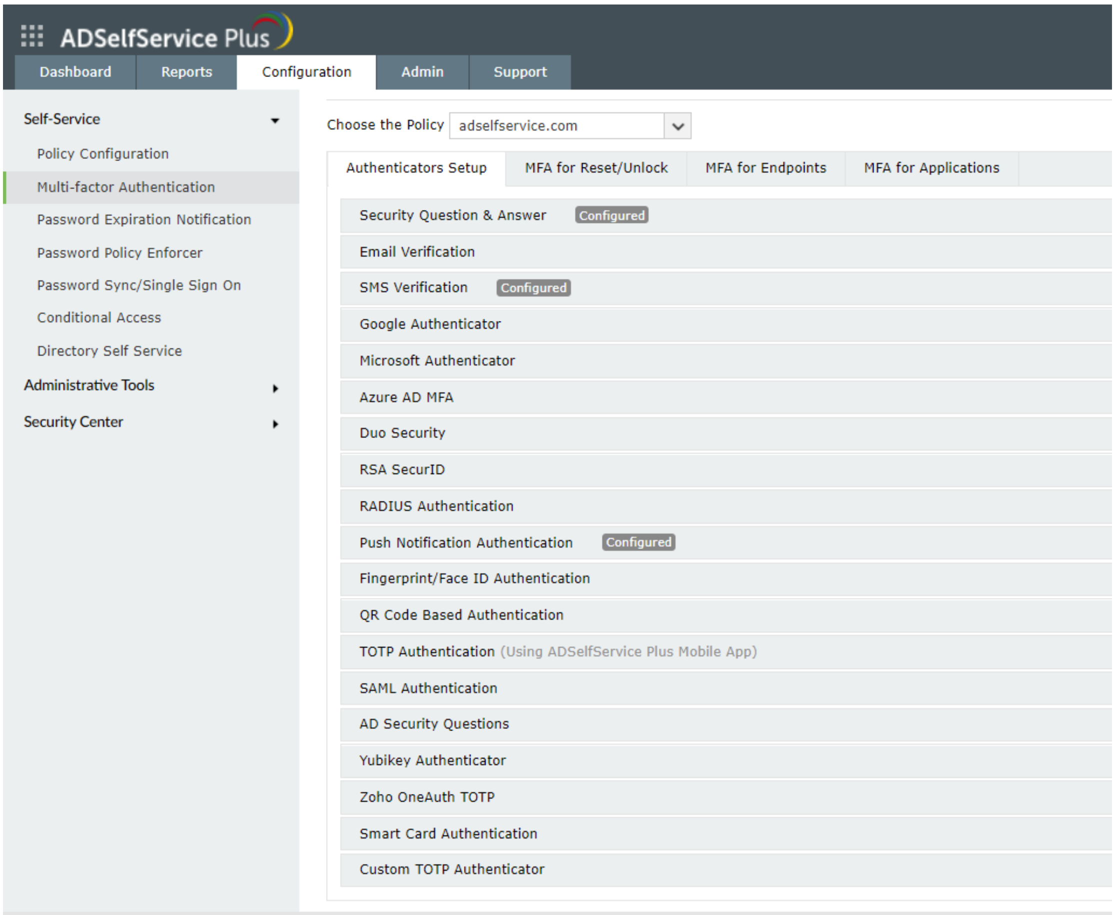
2

User authentication

Once successful, ADSelfService Plus triggers a preconfigured MFA workflow. Authentication techniques including SMS and email-based one-time-passcodes (OTPs), Yubikey, RSA SecurID, and biometrics ensure that the user is the owner of the account. Once the user identity is successfully verified, they will be able to reset passwords.

Complete list of supported authenticators:

1. Security Questions & Answers
2. Email Verification
3. SMS Verification
4. Google Authenticator
5. Azure AD MFA
6. Duo Security
7. RSA SecurID
8. RADIUS Authentication
9. YubiKey device
10. Push Notification Authentication
11. Fingerprint/Face ID Authentication
12. QR (quick response) Code Based Authentication
13. Microsoft Authenticator
14. TOTP Authentication (time-based one-time passcodes)
15. AD Secret (or) Security Questions
16. SAML Authentication
17. Zoho OneAuth TOTP
18. Smart Card Authentication
19. Custom TOTP Authenticator



Choose the Policy: adselfservice.com

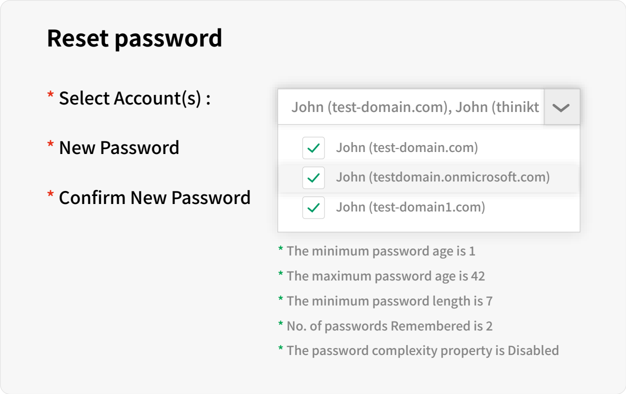
Security Question & Answer Configured
Email Verification
SMS Verification Configured
Google Authenticator
Microsoft Authenticator
Azure AD MFA
Duo Security
RSA SecurID
RADIUS Authentication
Push Notification Authentication Configured
Fingerprint/Face ID Authentication
QR Code Based Authentication
TOTP Authentication (Using ADSelfService Plus Mobile App)
SAML Authentication
AD Security Questions
Yubikey Authenticator
Zoho OneAuth TOTP
Smart Card Authentication
Custom TOTP Authenticator

3 Reset password

Once users have proved their identity through the authenticators, they will be able to reset passwords for their AD domain account, or other supported enterprise accounts including G Suite, Salesforce, and Office 365. While entering the new password, users must ensure that it complies with the default AD password policy and the ADSelfService Plus' advanced password policy settings.

Additionally, ADSelfService Plus' Password Strength Meter gives users instant visual feedback on password strength based on the enforced password policy.

Users can also choose to synchronize AD password resets across all enterprise application accounts by selecting *All Accounts* on the *Password Reset* page.



Reset password

* Select Account(s) : John (test-domain.com), John (thinikt

☑ John (test-domain.com)
☑ John (testdomain.onmicrosoft.com)
☑ John (test-domain1.com)

* New Password

* Confirm New Password

* The minimum password age is 1
* The maximum password age is 42
* The minimum password length is 7
* No. of passwords Remembered is 2
* The password complexity property is Disabled

Supported platforms

ADSelfService Plus supports password self-service for:

1. AD
2. Active Directory Lightweight Directory Services (AD LDS)
3. 389 Directory Server
4. Microsoft Dynamics CRM
5. HP-UX Directory Server
6. IBM i/AS400 system
7. MS SQL
8. Microsoft 365/Azure
9. Oracle DB
10. Oracle EBS
11. SAP NetWeaver
12. ServiceNow
13. OpenLDAP
14. G Suite (or) Google Workspace
15. Salesforce
16. PostgreSQL
17. Zendesk
18. Zoho

4 Password reset notification

Once the self-service password reset process is successfully completed, ADSelfService Plus triggers an SMS, email, or push notification to the user as a security measure. Though stringent authentication techniques thwart credential-based attacks, in case of any uninformed password reset by hackers, users should inform the admin immediately.

Why choose ADSelfService Plus?

1. **Self-service password reset and account unlock:** Enable users to securely reset passwords and unlock accounts for Windows AD, Microsoft 365, and other applications in a matter of seconds.

2. **Granular password policy enforcer:** Enforce password policies across Windows and enterprise cloud apps with advanced filters to blacklist dictionary words, patterns, etc.

3. **Password expiration notifier:** Warn users about their imminent password expiration via SMS, email, and push notifications.

4. **Real-time password synchronizer:** Enable users to use one password for multiple enterprise applications.

5. **Enterprise SSO:** Offer seamless access to any SAML-based cloud application via AD-based SSO.

6. **Endpoint MFA:** Add an additional layer of authentication for Windows, macOS, and Linux logins.

A shift in power

Empowering users to manage their passwords on their own introduces a new era in IT management. Try ADSelfService Plus free for 30 days to see how self-service password management brings a positive change to your organization.