

**ManageEngine** 

**Comparison Document**

---

**ManageEngine  
ADSelfService Plus**

**Vs**

**Azure AD Self-Service Password  
Reset (SSPR)**

## **ManageEngine ADSelfService Plus**

**vs.**

## **Azure AD Self-Service Password Reset (SSPR)**

Password reset tickets constitute a significant source of bottleneck for IT admins and help desk staff. They affect productivity and increase help desk costs. That's why Microsoft has equipped Azure AD with self-service password reset (SSPR). This feature allows end users to reset their Azure AD password on their own without help desk intervention.

What about SSPR for on-premises AD? Microsoft's On-premises AD does not provide any option for SSPR. However, there is a workaround. There is an option called password writeback in AD Connect that allows password changes in the cloud to be written back to existing on-premises directory.

So, if users forget their passwords, they can use Azure AD portal to reset it and this new password will be synchronized with on-premises AD. For this to happen, you need to have a valid Azure AD subscription and integrate your Azure AD with on-premises AD using Azure AD connect. It's complicated and costly.

ManageEngine ADSelfService Plus is an integrated Active Directory self-service password management and single sign-on solution that helps eliminate password-related help desk tickets, improves password security, and enhances end-user experience. It features SSPR for both on-premises AD and Azure AD along with multiple other enterprise applications and directories including IBM iSeries, HP UX, G Suite, and Salesforce.

## Why choose ADSelfService Plus over Azure AD SSPR?

### Supports both on-premises and hybrid AD:

Using ADSelfService Plus, you can enable SSPR for on-premises AD and hybrid environment.

Microsoft only provides SSPR for Azure AD and not on-premises AD.

### Password reset from logon screen:

With ADSelfService Plus, you make the SSPR option accessible from the logon screens of both Windows and Mac machines.

Azure AD SSPR from login screen works only on machines running a certain version of Windows 10.

### Mobile apps:

ADSelfService Plus mobile apps for Android and iOS devices allow users to reset their password and unlock their account using their mobile devices.

Azure AD SSPR doesn't have an option to reset password through mobile devices.

### Cached credential update for remote users:

ADSelfService Plus can update the local cached credentials of remote users after a password reset, helping them to get access to their machines even when they are not connected to their corporate network.

Azure AD SSPR doesn't have any provision for this.

### Multiple and customizable multi-factor authentication:

ADSelfService Plus supports a wide range of multi-factor authentication methods—thirteen to be precise—including SAML providers, with powerful customization options. You can enforce any more than two authentication options, change the order of authentication, and much more.

Azure AD supports only 4 authentication methods and you can enforce only maximum of two authentication options for password reset.

### Maximum ROI through force and auto-enrollment

ADSelfService Plus provides multiple ways to ensure users enroll for password self-service including forced and auto-enrollment techniques.

Azure AD's enrollment techniques can be easily bypassed by users.

### Advanced auditing capabilities

ADSelfService Plus provides multiple audit reports with capabilities to export them in different file formats, schedule them to be automatically generated and delivered via email to admins and managers, and more.

Azure AD only provides audit reports on user activities concerning SSPR.

### Additional self-service features

In addition to self-service password reset, ADSelfService Plus supports additional self-service features such as directory self-update, employee search, and mail group subscription (for distribution groups). Moreover, with password policy enforcer, ADSelfService Plus allows you to create custom password policies and display them on the reset and change password pages.

Azure AD supports self-service for password reset and group management only.

## Detailed comparison

The following table compares the self-service password management capabilities of ManageEngine ADSelfService Plus and Microsoft Azure AD (Premium).

Feature	Description	ADSelfService Plus	Azure AD (Premium)
<b>Core Features</b>			
Self-Reset Password	Users can reset their passwords without depending on the helpdesk.	✓	✓
Self-Account Unlock	Users can unlock their accounts without calling the helpdesk.	✓	✓
Change Password	Users can change their password from anywhere, at any time.	✓	✓
Automate AD Password Reset	Create password reset scheduler to reset the expired passwords automatically.	✓	✗
Password Expiration Notifier	Notify users via email and SMS to inform them about their password expiry date, and ask them to change their password before it expires.	✓	✗ *Only as pop-ups in the task bar
Account Expiration Notification	Notify users via email and SMS notifications about their impending account expiration.	✓	✓







Ease of Access			
<p>Password Self-Service Login Agent for Windows and Mac</p>	<p>Users can access the self-service portal from the Windows and Mac login prompts.</p>		 <p>(Password self-service login is available only for machines running a certain version of Windows)</p>
<p>Web Interface</p>	<p>Users can access the self-service portal from a web browser.</p>		
<p>Native Android and iPhone Apps</p>	<p>Android and iPhone apps for password reset and account unlock on the go.</p>		
<p>Cached Credentials Update</p>	<p>Updates the local cache stored in the users' machine so that remote users can access their machine even if they forget their password.</p>		
<p>Enterprise Single Sign-On</p>	<p>Users will be able to access SAML -based 100+ enterprise applications like G suite, Office 365, and Salesforce by signing in just once to.</p>		
<p>Password Synchronizer</p>	<p>Synchronize password changes across various applications like G-suite, Office 365, and Salesforce.</p>		

Security

<p>Identity Verification Methods</p>	<p>Authentication techniques to verify users' identities.</p>	<p>✓</p> <ol style="list-style-type: none"> <li>1. Security Q &amp; A</li> <li>2. Verification code via email and SMS.</li> <li>3. Google Authenticator.</li> <li>4. DUO Security.</li> <li>5. RSA SecurID.</li> <li>6. RADIUS Authenticator.</li> <li>7. Mobile Authenticator.</li> <li>8. SAML Authentication.</li> <li>9. AD Security Questions.</li> </ol> <p>(You can enforce more than two methods of authentication depending on your organization's security stance.)</p>	<p>✓</p> <ol style="list-style-type: none"> <li>1. Call.</li> <li>2. Text.</li> <li>3. Notification through mobile app.</li> <li>4. Verification code from mobile app or hardware token.</li> </ol> <p>(You can only enforce any two of the above methods for password reset.)</p>
<p>Windows Logon TFA</p>	<p>For improved security of your network resources, users will be required to enter their password, and additionally authenticate via the selected authentication methods.</p>	<p>✓</p> <p>The second level of authentication can be through one of the following:</p> <ol style="list-style-type: none"> <li>1. SMS or email-based verification codes.</li> <li>2. DUO Security.</li> <li>3. RSA SecurID.</li> <li>4. RADIUS.</li> </ol>	<p>✓</p> <p>(Not available in on-premises AD)</p>
<p>SMS, Email, and Push Notifications on completion of Password Management Activities.</p>	<p>Acknowledgement will be sent to users and administrators when they perform any of these listed actions.</p>	<p>✓</p>	<p>✗</p>





	<ol style="list-style-type: none"> <li>1. Self-service password reset.</li> <li>2. Self-service account unlock.</li> <li>3. Change password.</li> <li>4. Self directory update.</li> <li>5. Enroll with ADSelfService Plus.</li> <li>6. Exceed their bad password threshold or account lockout threshold and are blocked out of their accounts.</li> </ol>		
<b>Enrollment Capabilities</b>			
Forced Enrollment of Users	Process which automatically locates and forces un-enrolled users to enroll when they log in to their machines.	✔	✘
Automatic Enrollment - Type 1	Reuse enrollment data from your in-house database.	✔	✘
Automatic Enrollment - Type 2	Import enrollment data from a CSV file and enroll users without their intervention.	✔	✘
Enrollment Reminders	Automatically remind unenrolled users via mail or push notifications to enroll.	✔	✘

## Reporting Capabilities

Audit Reports	Audit reports allow administrators to track the actions performed by users in a chosen time period.	 (Provides a variety of audit reports like unlock account audit, change password audit, identity verification audit, and much more)	 (Captures all activities in audit logs)
Report Scheduler	Automatically generate and email reports to multiple users at the specified times.		
Export Reports	Reports can be saved for later use in a target file format such as HTML, PDF, CSV, etc.		 (Only in CSV format)

## Additional Features

### Password Policy Enforcer

Password Complexity Requirements for all integrated applications.	Option to force any or all the below character group requirements in a password: <ul style="list-style-type: none"> <li>• Uppercase characters</li> <li>• Lowercase characters</li> <li>• Special characters</li> <li>• Numeric characters</li> </ul>		 (Only three are enforced)
History Rule	Password history enforcement for password resets to prevent users from reusing their old passwords.		



Pattern Rule, Dictionary Rule, and Unicode Rule	<p>1. Option to disallow the use of specific patterns (like abc, 123, etc. ), palindromes, and dictionary words.</p> <p>2. Option to force the use of unicode characters.</p>	✓	✗
Password Sync Agent	Synchronizes password changes and enforces the configured password policy across a range of cloud-based and on-premise applications in real-time.	✓	✓
<b>Self-Service Features</b>			
Directory Self-Update	Users can maintain their information up-to-date in AD.	✓	✗
Mail-group Subscription	Users can opt-in or opt-out of the selected distribution groups.	✓	✓
Employee Search and Organization Chart	Users can search for their colleagues' information and find their position in the organization's hierarchy.	✓	✗

**Licensing and pricing:**

ADSelfService Plus is licensed based on the number of domain users, and [priced](#) affordably at **1,195 USD for 500 domain users** annually.

Azure AD (premium) is licensed based on the number of users and is priced at **6 USD/user /month**. That is, you'd have to pay **3000 USD for 500 users every month** or **36,000 USD annually**.

## Conclusion:

Both ADSelfService Plus and Azure AD support SSPR capabilities and help reduce help desk costs. However, ADSelfService Plus offers SSPR capability extensively, at a much lesser cost, and also provides a variety of other features like cached credential update and better enrollment capabilities.

### ADSelfService Plus has the upper hand in the following categories:

1. Automated and forced enrollment capabilities.
2. Extensive audit reports.
3. Sending phased password expiration reminders through email and SMS.
4. Scheduling and sending reports via email.
5. Automate password reset for expired passwords.

If your organization requires a solution that reduces password-related help desk tickets by empowering end users, ADSelfService Plus is indisputably the better choice and would give you a better return on investment.

Note: This document is for comparative purposes only. All the information mentioned here is based on the documents and data available on the competitor's website. The information provided might vary in the actual product.

## Our Products

AD360 | Log360 | ADManager Plus | ADAudit Plus | RecoveryManager Plus | M365 Manager Plus

ManageEngine

### 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](http://www.manageengine.com/products/self-service-password).

\$ Get Quote

↓ Download