Azure Active Directory Self-Service Password Reset-Adoption Kit

Version: 3.0

For the latest version, please check https://aka.ms/aadadoptionkits

Contents

Azure Active Directory Self-Service Password Reset- Adoption Kit	1
Awareness	2
Business overview	2
Pricing and licensing requirements	2
Key benefits	3
Announcements	3
Training and learning resources	4
Level 100 concepts	4
Training	4
Videos	4
Books	5
Online courses	5
Whitepaper	6
Planning and change management	7
Deployment Plan	7
Quickstarts	7
End-user readiness and communication	7
Combined registration with Multi-Factor Authentication	7
Customer stories/case studies	
Support and foodback	0

Awareness

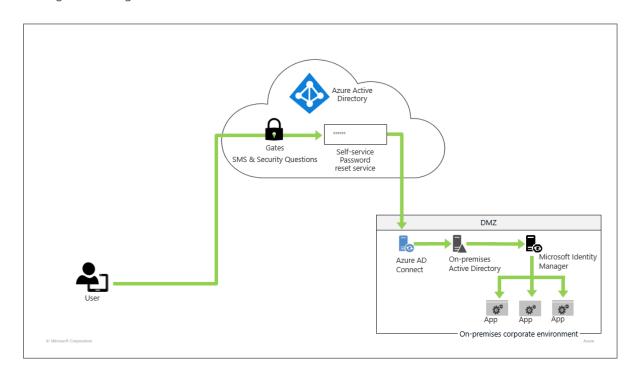
This section helps you to analyze the benefits of Azure Active Directory Self-Service Password Reset. You will learn about the ease of use, pricing, and licensing model. You can also access up-to-date announcements and blogs that discuss ongoing improvements.

Business overview

<u>Self-Service Password Reset (SSPR)</u> is an Azure Active Directory (Azure AD) feature that empowers the users to reset their passwords without the need to contact IT staff for help. The users can quickly unblock themselves and continue working no matter where they are or time of day. By allowing the employees to unblock themselves, your organization can reduce the non-productive time and high support costs for most common password-related issues.

SSPR has the following capabilities:

- **Self-service** allows end-users to reset their expired or non-expired passwords without contacting an administrator or helpdesk for support.
- **Password writeback** allows management of on-premises passwords and resolution of account lockout though the cloud.
- **Password management activity reports** give administrators insights into password reset and registration activity occurring in their organization.



Pricing and licensing requirements

SSPR is licensed per user. To maintain compliance, organizations are required to assign the appropriate license to their users. There are different features that make up SSPR including: change, reset, unlock, and writeback. Refer to <u>licensing</u> requirements for Azure AD SSPR for a comparative study to make the right licensing decision.

For more information on pricing, refer to Azure AD pricing.

Key benefits

Using SSPR give you the following benefits:



Manage cost

SSPR reduces IT support costs by enabling users to reset passwords on their own. It also reduc.es the cost of time lost due to lost passwords and lockouts.



Intuitive user experience

It provides an intuitive one-time user registration process that allows users to reset passwords and unblock accounts on-demand from any device or location. This allows users to get back to work faster and be more productive.



Flexibility and security

SSPR enables enterprises to access the security and flexibility that a cloud platform provides. Administrators can change settings to accommodate new security requirements and roll these changes out to users without disrupting their sign-in.



Robust auditing and usage tracking

Your organization can ensure that the business systems remain secure while its users reset their own passwords. Robust audit logs include information of each step of the password reset process. These logs are available from an API and enable the user to import the data into a Security Incident and Event Monitoring (SIEM) system of choice.

Announcements

Azure AD receives improvements on an ongoing basis. To stay up-to-date with the most recent developments, refer to What's new in Azure AD?

Training and learning resources

The following resources would be a good start to learn about SSPR. They include level 100 concepts, videos by our experts, link to online courses, and useful whitepapers for reference.

Level 100 concepts

Microsoft understands that some organizations have unique environment requirements or complexities. If yours is one of these organizations, use these recommendations as a starting point. However, most organizations can implement these recommendations as suggested.

- Find what is the identity secure score in Azure AD?
- Know the five steps to securing your identity infrastructure
- Understand identity and device access configurations

Refer to the following links to get started with SSPR:

- Understand how Azure AD SSPR works
- Know about the <u>authentication methods</u>
- Learn to customize the Azure AD functionality for SSPR
- Understand password writeback
- Learn about password policies and account restrictions in Azure AD
- Learn to register for SSPR
- Learn to <u>reset your work or school password</u>
- Understand <u>combined security information registration</u> so that users can register once and get the benefits of both Microsoft Azure Multi-Factor Authentication and SSPR
- Follow Password management frequently asked questions

For more information, deep-dive into Authentication documentation.

Training

Videos

Video	Description
How to get started with identity security	Learn about identity security, why is it important, and what you can do to get it more secure
How to improve your identity security posture with Secure Score	Get a walk-through about the identity secure score in the Azure AD portal.
What is self-service password reset?	Get the SSPR overview
Deploying self-service password reset	Learn to configure and deploy SSPR in the Azure AD portal.
How to roll out self-service password reset	Get a walkthrough of the SSPR implementation process from pilot to roll out.

Identity Architecture: Self-Service Password Reset	Learn about SSPR and the benefits for IT staff and employees.
How to register your security information in Azure Active Directory	Learn how to register security information through Azure AD for security features like Multi-Factor Authentication and SSPR. End users will also learn how to view and manage their security methods in Azure AD.

Books

Source: Microsoft Press - <u>Modern Authentication with Azure Active Directory for Web Applications (Developer Reference)</u>
<u>1st Edition.</u>

Learn the essentials of authentication protocols and get started with Azure AD. Refer to examples of applications that use Azure AD for their authentication and authorization, including how they work in hybrid scenarios with Active Directory Federation Services (ADFS).

Online courses

Refer to the_following courses on SSPR at_pluralsight.com:

Course	Description
Managing Identities in Microsoft Azure Active Directory	Learn the basics of Azure AD environment, including users, groups, devices, and applications. You will also examine how to leverage SSPR to give your users a modern, protected experience. Refer to Managing Azure Active Directory Users and Groups module.
The Issues of Identity and Access Management	Learn how to look at IAM in the proper perspective, as well as security issues to be aware of in your organization. Refer to Other Authentication Methods module.
Getting Started with the Microsoft Enterprise Mobility Suite	This course provides you with best practices that you need to know for extending on-premises assets to the cloud that allows for authentication, authorization, encryption, and a secured mobile experience. Refer to Configuring Advanced Features of Microsoft Azure Active Directory Premium module.

Whitepaper

Whitepaper	Description
How hybrid identity allows digital transformation	Learn more about hybrid identity framework that recommends deploying Azure AD SSPR.
Azure Active Directory Data Security Considerations	This whitepaper outlines data security considerations.
Zero Trust Deployment Guide for Microsoft Azure Active Directory	This guidance is to assist you if you are engaging in Microsoft's Zero <u>Trust security strategy</u> .

Planning and change management

In this section, you deep-dive into planning and deploying SSPR in your organization. You can leverage quickstarts on SSPR scenarios and end-user readiness material. You can also visit recommendations on how to register SSPR in your environment.

Deployment Plan

Refer to <u>SSPR deployment plan -</u> a comprehensive guide to plan and implement SSPR in your organization. It includes the following sections:

Sections	Description
Prerequisites	Get prepared for the deployment
Solution architecture	Understand the password reset solution architecture and workflow for hybrid environments
Best practices	To register SSPR successfully in your organization
Plan the deployment project	Determine the strategy for this deployment in your environment
Plan configuration	Settings required to enable SSPR along with recommended values
Plan testing, support and rollback	Prepare for test results, FAQs for support staff, and rollback considerations
Deploy SSPR	At each stage of your deployment from initial pilot groups through organization-wide, ensure that results are as expected.
Manage SSPR	Follow audits and view reports
Troubleshoot	Collect information to ease troubleshooting and follow the instructions

Quickstarts

Follow the step-by-step guidance to:

- Enable self-service password reset
- Enable password writeback to an on-premises environment
- Enable password reset from the Windows login screen

End-user readiness and communication

You can distribute the readiness material to your users during Azure AD SSPR rollout, educate them about the feature, and remind them to register. Download <u>Self-service password reset rollout materials</u> and customize them with your organization's branding.

Combined registration with Multi-Factor Authentication

We recommend that you enable the <u>enable combined security information registration in Azure AD</u> for SSPR and Multi-Factor Authentication.

Before enabling the new experience, review the article <u>combined security information registration</u> to ensure you understand the functionality and effects of this feature. In case of issues, refer to <u>Troubleshooting combined security information registration</u>.

Customer stories/case studies

Discover how most organizations use SSPR to set policies that extend rich admin capabilities to all the users in their directory.

The following featured stories demonstrate these needs:



<u>Aramex delivery limited:</u> Global logistics and transportation company creates cloud – connected office with identity and access management solution.

Aramex needed an identity and access management solution that would provide a better experience, tighten security, and make their identity and access processes more efficient. Azure AD was able to achieve all three of these goals with its SSO, Multi-Factor Authentication, and SSPR capabilities.



<u>HCL Technologies uses Enterprise Mobility + Security to deliver highly secure digital workplace</u>

HCL wanted to enhance an already mobile and agile corporate culture by boosting employees' productivity, so it chose Microsoft 365. Today, HCL employees have a simpler way to reset their passwords through self-service password management. HCL deployed a solution where employees can unlock and reset their passwords through interactive voice response, thereby reducing help-desk calls by approximately 15 percent.



Construction giant gains competitive edge with zero-trust approach to security.

When the Walsh Group moved to the cloud, it realized it needed better ways to manage who accesses its systems. The company set up identity as the control plane—with Microsoft Azure Active Directory at the center and a zero-trust security stance to better protect access to all its resources.

Working with Microsoft on the self-service password reset project revealed several areas where it could improve security across its hybrid infrastructure and plug the gaps to make sure that the expected user is the one using the identity.

To learn more about customer and partner experiences on SSPR, visit: See the amazing things people are doing with Azure.

Support and feedback

How can we improve SSPR? This section provides links to discussion forums and technical community support email IDs.

We encourage you to join our <u>Technical Community</u>, a platform to Microsoft Azure AD users and Microsoft to interact. It is a central destination for education and thought leadership on best practices, product news, live events, and roadmap.

If you have technical questions or need help with Azure, please try StackOverflow or visit the MSDN Azure AD forums.

Tell us what you think of Azure and what you want to see in the future. If you have suggestions, please submit an idea or vote up an idea at our User Voice Channel - <u>feedback.azure.com</u>.