200 XP

What is self-service password reset in Azure Active Directory?

7 minutes

You've been asked to assess ways to reduce help-desk costs in your retail organization. You've noticed that support staff spend much of their time resetting passwords for users. Users often complain about delays with this process. The delay impacts their productivity. You want to understand how you can configure Azure to enable users to manage their own passwords.

In this unit, you'll learn how self-service password reset (SSPR) works in Azure Active Directory (Azure AD).

Why use SSPR?

In Azure AD, any user can change their password if they're already signed in. But if they're not signed in and forgot their password or it's expired, they'll need to reset their password. With SSPR, users can reset their passwords in a web browser or from a Windows sign-in screen to regain access to Azure, Microsoft 365, and any other application that uses Azure AD for authentication.

SSPR reduces the load on administrators, because users can fix password problems themselves, without having to call the help desk. Also, it minimizes the productivity impact of a forgotten or expired password. Users don't have to wait until an administrator is available to reset their password.

How SSPR works

The user initiates a password reset either by going directly to the password reset portal or by selecting the **Can't access your account** link on a sign-in page. The reset portal takes these steps:

1. **Localization**: The portal checks the browser's locale setting and renders the SSPR page in the appropriate language.
2. **Verification**: The user enters their username and passes a captcha to ensure that it's a user and not a bot.
3. **Authentication**: The user enters the required data to authenticate their identity. They might, for example, enter a code or answer security questions.

4. **Password reset**: If the user passes the authentication tests, they can enter a new password and confirm it.
5. **Notification**: A message is usually sent to the user to confirm the reset.

There are several ways you can customize the SSPR user experience. For example, you can add your company logo to the sign-in page so users know that they're in the right place to reset their password.

Authenticate a password reset

It's critical to verify the identity of a user before you allow a password reset. Malicious users might exploit any weakness in the system to impersonate that user. Azure supports six different ways to authenticate reset requests.

As an administrator, you choose the methods to use when you configure SSPR. Enable two or more of these methods so that users can choose the ones that they can use easily. The methods are:

Authentication method	How to register	How to authenticate for a password reset
Mobile app notification	Install the Microsoft Authenticator app on your mobile device, and then register it on the multifactor authentication setup page.	Azure sends a notification to the app, which you can either verify or deny.
Mobile app code	This method also uses the Authenticator app, and you install and register it in the same way.	Enter the code from the app.
Email	Provide an email address that's external to Azure and Microsoft 365.	Azure sends a code to the address, which you enter in the reset wizard.
Mobile phone	Provide a mobile phone number.	Azure sends a code to the phone in an SMS message, which you enter in the reset wizard. Or, you can choose to get an automated call.
Office phone	Provide a nonmobile phone number.	You receive an automated call to this number and press #.
Security questions	Select questions such as "In what city was your mother born?" and save responses to them.	Answer the questions.

In free and trial Azure AD organizations, phone call options aren't supported.

Require the minimum number of authentication methods

You can specify the minimum number of methods that the user must set up: one or two. For example, you might enable the mobile app code, email, office phone, and security questions methods and specify a minimum of two methods. Then users can choose the two methods they prefer, like mobile app code and email.

For the security question method, you can specify a minimum number of questions that the user must set up to register for this method. You also can specify a minimum number of questions that they must answer correctly to reset their password.

After your users register the required information for the minimum number of methods you've specified, they're considered registered for SSPR.

Recommendations

- Enable two or more of the authentication reset request methods.
- Use the mobile app notification or code as the primary method, but also enable the email or office phone methods to support users without mobile devices.
- The mobile phone method isn't a recommended method because it's possible to send fraudulent SMS messages.
- The security question option is the least recommended method because the answers to the security questions might be known to other people. Only use the security question method in combination with at least one other method.

Accounts associated with administrator roles

- A strong, two-method authentication policy is always applied to accounts with an administrator role, regardless of your configuration for other users.
- The security questions method isn't available to accounts that are associated with an administrator role.

Configure notifications

Administrators can choose how users are notified of password changes. There are two options that you can enable:

- **Notify users on password resets**: The user who resets their own password is notified to their primary and secondary email addresses. If the reset was done by a malicious user,

this notification alerts the user, who can take mitigation steps.
- **Notify all admins when other admins reset their password**: All administrators are notified when another administrator resets their password.

License requirements

The editions of Azure AD are free, Premium P1, and Premium P2. The password reset functionality you can use depends on your edition.

Any user who is signed in can change their password, regardless of the edition of Azure AD.

If you're not signed in and you've forgotten your password or your password has expired, you can use SSPR in Azure AD Premium P1 or P2. It's also available with Microsoft 365 Apps for business or Microsoft 365. SSPR isn't available in the free edition of Azure AD.

In a hybrid situation, where you have Active Directory on-premises and Azure AD in the cloud, any password change in the cloud must be written back to the on-premises directory. This writeback support is available in Azure AD Premium P1 or P2. It's also available with Microsoft 365 Apps for business.

Check your knowledge

1. When is a user considered registered for SSPR?

- ○ When they've registered at least one of the permitted authentication methods.
- ○ When they've registered at least the number of methods that you've required to reset a password.
- ○ When they've set up the minimum number of security questions.

2. When you enable SSPR for your Azure AD organization...

- ○ Users can change their password when they're signed in.
- ○ Admins can reset their password by using one authentication method.
- ○ Users can reset their passwords when they can't sign in.

Check your answers