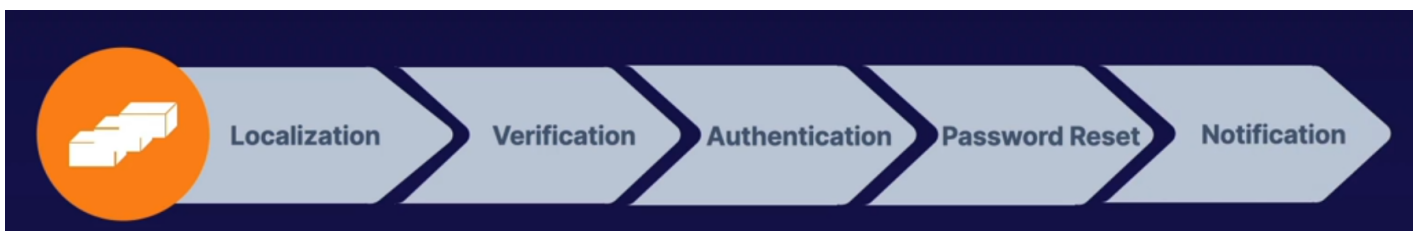


# AZ-104 Azure Identity - Configuring SSPR (self service password reset)

- Self Service Password Reset (SSPR)

- SSPR Process
- Authentication Methods
- SSPR Considerations



## Authentication methods

- Mobile app: Authentication via app notification. AN example is the Microsoft authentication application
- Mobile app code: Authentication via time-based codes, An example is the Microsoft authentication application
- Email: Authentication via an external to Microsoft using codes sent to that email address
- Mobile Phone: Authentication via a mobile number using a phone call or SMS provides a code. (less recommended method)
- Office Phone: Authentication via a non-mobile phone using a phone cal that prompts the user to press #
- Security Questions: Authentication via answering a set of security questions (Least recommended method).

## SSPR Considerations

Enable and manage SSPR via Azure AD Groups.

- Required methods: One or more of the available authentication methods is required for SSPR
- SSPR for Admins: Security questions not available by admins. By Default, admins must register for MFA methods
- Required Licenses: Azure AD P1 or P2, Microsoft apps for business, or Microsoft licensing is required for SSPR.

Navigate to Entra ID then password reset

The screenshot shows the Microsoft Entra ID console. The breadcrumb path is "Home > Default Directory". The main heading is "Default Directory | Password reset". The left-hand navigation pane is expanded to "manage", and "Password reset" is highlighted with a red arrow. A red arrow also points to the "Password reset" link in the breadcrumb path. The main content area displays the "Self-Service Password Reset" feature description and benefits.

**Self-Service Password Reset**

This feature includes a set of capabilities that allow your users to manage any password from any device, at any time, from any location, while remaining in compliance with the security policies you define.

**Why use self-service password reset?**

- REDUCE COST**  
Support-assisted password reset is typically 20% of organization's IT spend
- IMPROVE USER EXPERIENCES**  
Users don't want to call helpdesk and spend an hour on the phone every time they forget their passwords
- LOWER HELPDESK VOLUME**  
Password Management is the single largest helpdesk driver for most organizations
- ENABLE MOBILITY**  
Users can reset their passwords from wherever they are

The screenshot shows the "Password reset | Properties" page in the Microsoft Entra ID console. The breadcrumb path is "Home > Default Directory | Password reset > Password reset". The main heading is "Password reset | Properties". The page shows the "Self service password reset enabled" setting, which is currently set to "None". The "None" button is highlighted with a mouse cursor. The "Save" and "Discard" buttons are visible at the top right of the settings area.

**Self service password reset enabled**

None Selected All

These settings only apply to end users in your organizations ,admins are always enabled for SSPR and are required to use two authentication methods to reset their passwords

- None: no user can perform SSPR (except admins).
- Select: Here we can use groups to Enable SSPR.
- ALL - this will enable all users in the tenant with SSPR.

For this exercise we select all users and select which type of authentication method

Home > Default Directory | Password reset > Password reset

## Password reset | Authentication methods

Default Directory - Azure Active Directory

<< Save Discard

**Authentication Methods for SSPR and Signin can now be managed in one converged policy. [Learn more](#)**

Number of methods required to reset ⓘ

1 2

Methods available to users

- Mobile app notification
- Mobile app code
- Email
- Mobile phone
- Office phone
- Security questions

Diagnose and solve problems

Manage

- Properties
- Authentication methods**
- Registration
- Notifications
- Customization
- On-premises integration
- Administrator Policy

Activity

- Audit logs
- Usage & insights

Troubleshooting + Support

# Password reset | Registration

Default Directory - Azure Active Directory

- Diagnose and solve problems
- Manage
  - Properties
  - Authentication methods
  - Registration
  - Notifications
  - Customization
  - On-premises integration
  - Administrator Policy
- Activity
  - Audit logs
  - Usage & insights
- Troubleshooting + Support

<< Save Discard

Require users to register when signing in? ⓘ

Yes  No

Number of days before users are asked to re-confirm their authentication information ⓘ

180

**i** These settings only apply to end users in your organization. Admins are always enabled for self-service password reset and are required to use two authentication methods to reset their password. [Click here to learn more about administrator password policies.](#)

# Password reset | Notifications

Default Directory - Azure Active Directory

- Diagnose and solve problems
- Manage
  - Properties
  - Authentication methods
  - Registration
  - Notifications
  - Customization
  - On-premises integration
  - Administrator Policy
- Activity
  - Audit logs
  - Usage & insights
- Troubleshooting + Support

<< Save Discard

Notify users on password resets? ⓘ

Yes  No

Notify all admins when other admins reset their password? ⓘ

Yes  No

# Password reset | Administrator Policy ...

Default Directory - Azure Active Directory

- Diagnose and solve problems
- Manage**
- Properties
- Authentication methods
- Registration
- Notifications
- Customization
- On-premises integration
- Administrator Policy**
- Activity**
- Audit logs
- Usage & insights
- Troubleshooting + Support

<<

Is self-service password reset enabled?  
Yes

Number of methods required to reset:  
2

Methods available to administrators:

- Email
- Mobile phone (SMS only)
- Mobile phone
- Office phone
- Mobile app code

 [Click here to learn more about administrator password policies.](#)

Revision #2  
Created 19 February 2024 22:16:06 by Cesar Gzz  
Updated 19 February 2024 22:45:57 by Cesar Gzz