Allow users to reset password using self service

Why use SSPR(self service password reset)

* Reduce workload for administrators
* Users can fix password problems themselves
* Users do not have to wait for admin to fix

How SSPR works

Before the process begins users must first select **cant access your account**

1. Localization, checks browser locale setting and language
2. Verification, enters username and captcha check
3. Authentication, enter data for authenticity
4. Password reset, once authentication tests are passed user can change password
5. Notification, message sent to confirm password reset

Methods

There are different methods in which password resets can be done such as:

* Sms code, code sent to phone for reset
* Email, code sent to email for reset
* Office phone, automated call
* Security questions, reCAPTCHA or like online banking questions
* Mobile app notification, enter code from app

You can set the minimum number of methods above to use for resetting the password

Recommendations

* Enable two or more
* Mobile phone is not good as it can send fake messages
* Only use security method along with others

Configure notifications

* Users are notified for password resets if they have more than one email address
* All admins are notified when another resets their password

SSPR requirements

* Azure AD, minimum free trial
* AD account with global admin privileges, used for creation of SSPR
* Non admin account, used for testing
* A security group for testing as well

Scopes

* Disabled, default option. No one can use SSPR
* Enabled, all users in AD can use SSPR
* Selected, specified group only. Only use enabled when testing is done and can be used for all

How to enable password reset

1. Azure portal > active directory > password reset

Company Branding

* You can also customize directory branding for sign-in so you know that you’re in the right place

**Role Based Access Control RBAC**

Azure role and Azure AD Roles

* Azure roles are used to manage access to vms
* Azure AD roles are used to manage access to AD resources such as user accounts and passwords

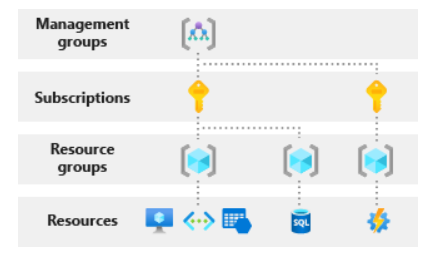
Azure Role

* Aka as a collection of permissions
* Allows control over who has access to resources

Custom roles

* Owner, full access and delegate
* Contributor, can create and manage
* Reader, read only access
* User account admin, manage access to resource

Scope



Azure AD Roles

* Global admin, admin features and can grant admin roles, user sign up as for directory is admin by default
* User admin, manage users, groups, monitoring, resetting passwords
* Billing admin, in charge of the subscription, monitor service health and detailed billing permissions

Difference between Azure AD and Azure roles is that Azure roles applies to resources whereas Azure AD is users, groups, and domains

As global admin you might need to elevate permissions to:

* Regain lost access
* Grant another user access to azure sub or management group
* View azure resources

To assign admin access to a subscription you must have **Microsoft.Authorization/roleAssignments/write** and **Microsoft.Authorization/roleAssignments/delete**

**Role Assignment**

* Role definition; collection of permissions, read, write, delete
* Security principal; users, groups
* Scope; access in levels, like subscriptions, single resource

RBAC allow model

* NotActions permission; create a set of not allowed permissions