

# Implementing SSPR

## Step 1: Create the first group






- From the **Manage** tab, select **Groups**.
- Then, select **New group**.
- Create a **group** called "SSPR\_Enabled".

 Delete |  Got feedback?



### SSPR\_Enabled

This is a group for users with SSPR

Membership type	Assigned	
Source	Cloud	
Type	Security	
Object Id	35adc8a7-4611-4a60-b757-a669a7a41d1b	
Created at	6/2/2023, 12:59:50 PM	


## Step 2: Fill in the group details

Here, you should have added the following details about the first group:

- The name of the group is "SSPR\_Enabled".
- An appropriate description.
- The roles remain **Unassigned**.
- Membership type is toggled to **assigned**.
- A sample user is assigned to the group.

[Home](#) > [Groups | All groups](#) >

## New Group ...

 Got feedback?

Group type \* ⓘ

Security

Group name \* ⓘ

Enter the name of the group

Group description ⓘ

Enter a description for the group

Azure AD roles can be assigned to the group ⓘ

Yes

No

Membership type \* ⓘ

Assigned

Owners

No owners selected

Members

### Step 3: Enable SSPR

- In this step, SSPR is enabled by navigating from the Overview menu to the **Password reset tab**.
- Then, you should have selected the toggle button for the option called **Selected**.
- "SSPR\_Enabled Group" is added, followed by selecting the **Save** button.

 Save  Discard

Self service password reset enabled ⓘ


None

Selected

All

Select group ⓘ

SSPR\_Enabled

 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.](#)

## Step 4: Register a user

- You confirmed that the user cannot access SSPR.
- Therefore, navigate to the application website and register a **user** on the site.

## Step 5: Verify user access to Password reset

Access the SSPR portal. The test is complete and demonstrates that the user can access the Password reset.

### Get back into your account

verification step 1 > choose a new password

---

Please choose the contact method we should use for verification:

☒ Text my mobile phone

In order to protect your account, we need you to enter your complete mobile phone number (\*\*\*\*\*50) below. You will then receive a text message with a verification code which can be used to reset your password.

Enter your phone number

Text

[Cancel](#)

## Step 6: Create the second group






Steps two and three are repeated when creating the second group.

- This group is labeled as "SSPR\_not\_Enabled".
- Here, SSPR is not configured.
- A member is **Assigned**.



## Not\_SSPR\_ENABLED

This group is to showcase an inability to perform SSPR

Membership type	Assigned	
Source	Cloud	
Type	Security	
Object Id	0fef3ccd-9d01-4f03-b5f6-2827cf03b917	
Created at	6/2/2023, 2:14:52 PM	

## Step 7: Demonstrate non-SSPR availability

The image confirms that a member of the "SSPR\_not\_Enabled" group attempts to activate the SSPR functionality but is unsuccessful.

Get back into your account

We're sorry

You can't reset your own password because password reset isn't turned on for your account.

You must [contact your administrator](#) to turn on password reset for your account.

Show additional details

## Conclusion

In this exercise, you have demonstrated how groups can be used in conjunction with SSPR to limit the scope of a worker. You created two groups, of which the first accessed the system using SSPR, and the second group is without SSPR. Instead, you as the administrator must facilitate access privileges to the "SSPR\_not\_Enabled" group.