

Allow users to reset their password with Microsoft Entra self-service password reset

1. Introduction

<https://learn.microsoft.com/en-us/training/modules/allow-users-reset-their-password/1-introduction>

Introduction

Completed

Suppose you're an IT administrator for a large retail organization. Your organization starts using Microsoft Entra ID to allow employees to securely sign in and use software as a service (SaaS) apps. It also allows access to the organization's resources in Microsoft 365. You're overwhelmed with password-reset requests because you currently reset employees' passwords manually. To get these employees back to being productive quickly and reduce your workload, you decide to evaluate and set up self-service password reset in Microsoft Entra ID.

In this module, you learn how Azure supports this feature and how to set it up. Only paid subscriptions can leverage this, while free and pay-as-you-go can't.

By the end of this module, you'll be able to configure self-service password reset in Microsoft Entra ID.

Learning objectives

In this module, you:

- Decide whether to implement self-service password reset.
- Implement self-service password reset to meet your requirements.
- Configure self-service password reset to customize the experience.

Prerequisites

- Basic understanding of Microsoft Entra ID
- A working Microsoft Entra tenant with a subscription package that includes Microsoft Entra ID P1

- An account with at least the Authentication Policy Administrator role

2. What is self-service password reset in Microsoft Entra ID?

<https://learn.microsoft.com/en-us/training/modules/allow-users-reset-their-password/2-self-service-password-reset>

What is self-service password reset in Microsoft Entra ID?

Completed

3. Implement Microsoft Entra self-service password reset

<https://learn.microsoft.com/en-us/training/modules/allow-users-reset-their-password/3-implement-azure-ad-self-service-password-reset>

Implement Microsoft Entra self-service password reset

Completed

You've decided to implement self-service password reset (SSPR) in Microsoft Entra ID for your organization. You want to start using SSPR for a group of 20 users in the marketing department as a trial deployment. If everything works well, you'll enable SSPR for your whole organization.

In this unit, you'll learn how to enable SSPR in Microsoft Entra ID.

Prerequisites

Before you start to configure SSPR, you need a:

- **Microsoft Entra organization:** This organization must have at least a P1 or P2 trial license enabled.

- **Microsoft Entra account with Authentication Policy Administrator role:** You'll use this account to set up SSPR.
- **Non-administrative user account:** You'll use this account to test SSPR. It's important that this account isn't an administrator, because Microsoft Entra imposes extra requirements on administrative accounts for SSPR. This user, and all user accounts, must have a valid license to use SSPR.
- **Security group with which to test the configuration:** The non-administrative user account must be a member of this group. You'll use this security group to limit who you roll SSPR out to.

Scope of SSPR rollout

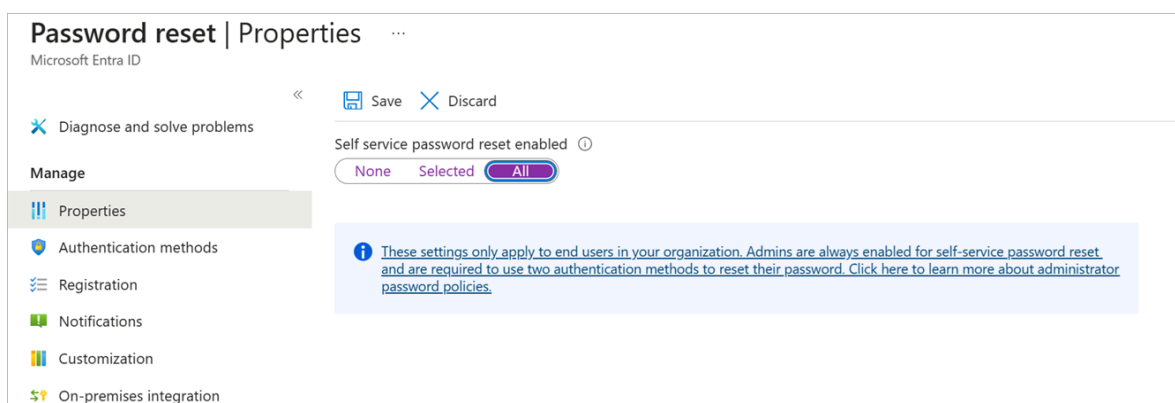
There are three settings for the **Self-service password reset enabled** property:

- **None:** No users in the Microsoft Entra organization can use SSPR. This value is the default.
- **Selected:** Only the members of the specified security group can use SSPR. You can use this option to enable SSPR for a targeted group of users who can test it and verify that it works as expected. When you're ready to roll it out broadly, set the property to **Enabled** so that all users have access to SSPR.
- **All:** All users in the Microsoft Entra organization can use SSPR.

Configure SSPR

Here are the high-level steps to configure SSPR:

1. Go to the [Azure portal](#), then to **Microsoft Entra ID > Manage > Password reset**.
2. **Properties:**
 - Enable SSPR.
 - You can enable it for all users in the Microsoft Entra organization or for selected users.
 - To enable for selected users, you must specify the security group. Members of this group can use SSPR.



3. **Authentication methods:**

- Choose whether to require one or two authentication methods.
- Choose the authentication methods that the users can use.

Password reset | Authentication methods ...

Microsoft Entra ID

<< Save Discard

Diagnose and solve problems

Manage

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

Activity

- Audit logs
- Usage & insights

Troubleshooting + Support

- New support request

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 (SMS only)
- ☐ Office phone ⓘ
- ☐ Security questions

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.](#)

4. **Registration:**

- Specify whether users are required to register for SSPR when they next sign in.
- Specify how often users are asked to reconfirm their authentication information.

Password reset | Registration ...

Microsoft Entra ID

<< Save Discard

Diagnose and solve problems

Manage

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

Require users to register when signing in? ⓘ

Yes No

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

180

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.](#)

5. **Notifications:** Choose whether to notify users and administrators of password resets.

Password reset | Notifications ...

Microsoft Entra ID

<< Save Discard

✖ Diagnose and solve problems

Manage

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

Notify users on password resets? ⓘ

☒ Yes ☐ No

Notify all admins when other admins reset their password? ⓘ

☐ Yes ☒ No

6. **Customization:** Provide an email address or web page URL where your users can get help.

Password reset | Customization ...

Microsoft Entra ID

<< Save Discard

✖ Diagnose and solve problems

Manage

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

Customize helpdesk link ⓘ

☒ Yes ☐ No

Custom helpdesk email or URL ⓘ

✓

4. Exercise - Set up self-service password reset

<https://learn.microsoft.com/en-us/training/modules/allow-users-reset-their-password/4-exercise-set-up-self-service-password-reset>

Exercise - Set up self-service password reset

Completed

In this unit, you'll configure and test self-service password reset (SSPR) by using your email. You'll need to use your email to complete the password-reset process in this exercise.

Create a group

You want to roll out SSPR to a limited set of users first to make sure your SSPR configuration works as expected. Let's begin by creating a security group for the limited rollout.

1. In the Microsoft Entra organization you created, under **Manage**, select **Groups**.
2. Select **New Group**.
3. Enter the following values:

Setting	Value
Group type	Security
Group name	SSPRTesters
Group description	Members are testing the rollout of SSPR
Membership type	Assigned

4. Select **Create**.

New Group

Got feedback?

Group type *

Security

Group name *

SSPRTesters

Group description

Members are testing the rollout of SSPR

Azure AD roles can be assigned to the group

Yes

No

Membership type *

Assigned

Owners

No owners selected

Members

No members selected

Create

Create a user account

To test your configuration, create an account that's not associated with an administrator role. You'll also assign the account to the group you created.

1. In your Microsoft Entra organization, under **Manage**, select **Users**.
2. Select **+ New user**, select **Create new user** in the drop-down, and use the following values:

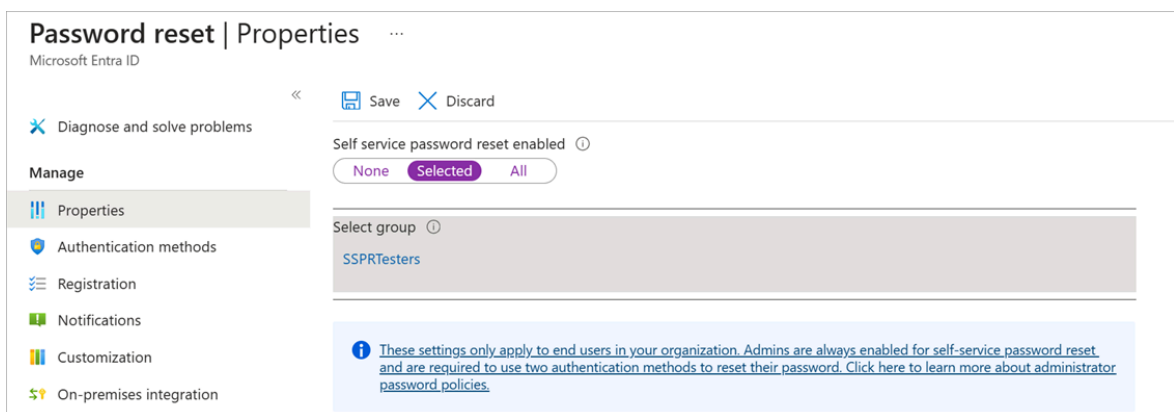
Setting	Value
User principal name	balas
Display name	Bala Sandhu
Password	Select the Copy icon next to the autogenerated password, then paste the password to a text editor like Notepad.

3. Select the **Assignments** tab.
4. Select **Add group**, check the box for the **SSPRTesters** group, and then the **Select** button.
5. Select **Review + create** and then select **Create**.

Enable SSPR

Now, you're ready to enable SSPR for the group.

1. In your Microsoft Entra organization, under **Manage**, select **Password reset**.
2. On the **Properties** page, select **Selected**. Select the link under **Select Group**, select the box next to the **SSPRTesters** group, and then the **Select** button.
3. Select **Save**.



4. Under **Manage**, select the **Authentication methods**, **Registration**, and **Notifications** pages to review the default values. Ensure **Authentication methods** has **Email** selected.

5. Select **Customization**.
6. Select **Yes**, and then in the **Custom helpdesk email or URL** text box, enter **admin@organization-domain-name.onmicrosoft.com**. Replace "organization-domain-name" with the domain name of the Microsoft Entra organization you created. If you've forgotten the domain name, hover over your profile in the Azure portal.
7. Select **Save**.

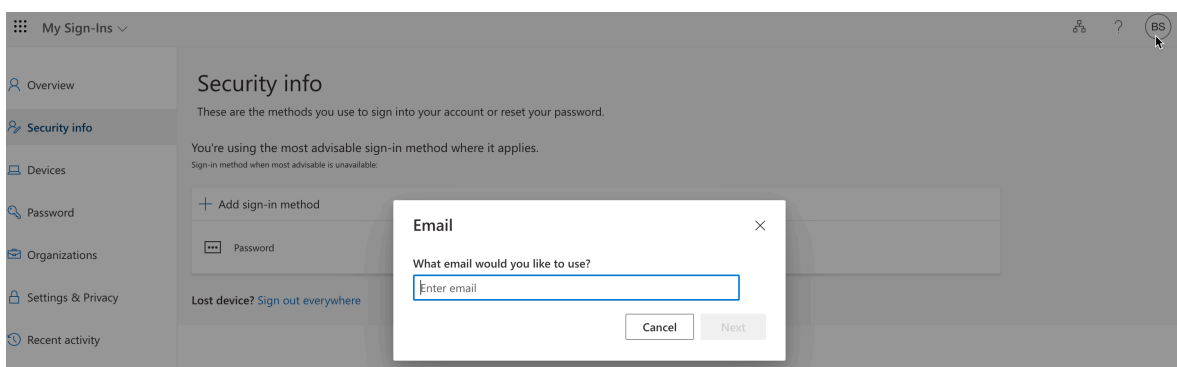
Register for SSPR

Now that the SSPR configuration is complete, register an email for the user you created.

Note

If you get a message that says "The administrator has not enabled this feature," use private/incognito mode in your web browser.

1. In a new browser window, go to <https://aka.ms/ssprsetup>.
2. Sign in with the user name **balas@organization-domain-name.onmicrosoft.com** and the password that you noted earlier. Remember to replace "organization-domain-name" with the domain name of the Microsoft Entra organization you created.
3. If you're asked to update your password, enter a new password of your choice. Make sure you note the new password.
4. Select the **Security info** tab, and then select **+ Add sign-in method**.
5. In the **Add a method** box, select **Email**.
6. Enter your email details.

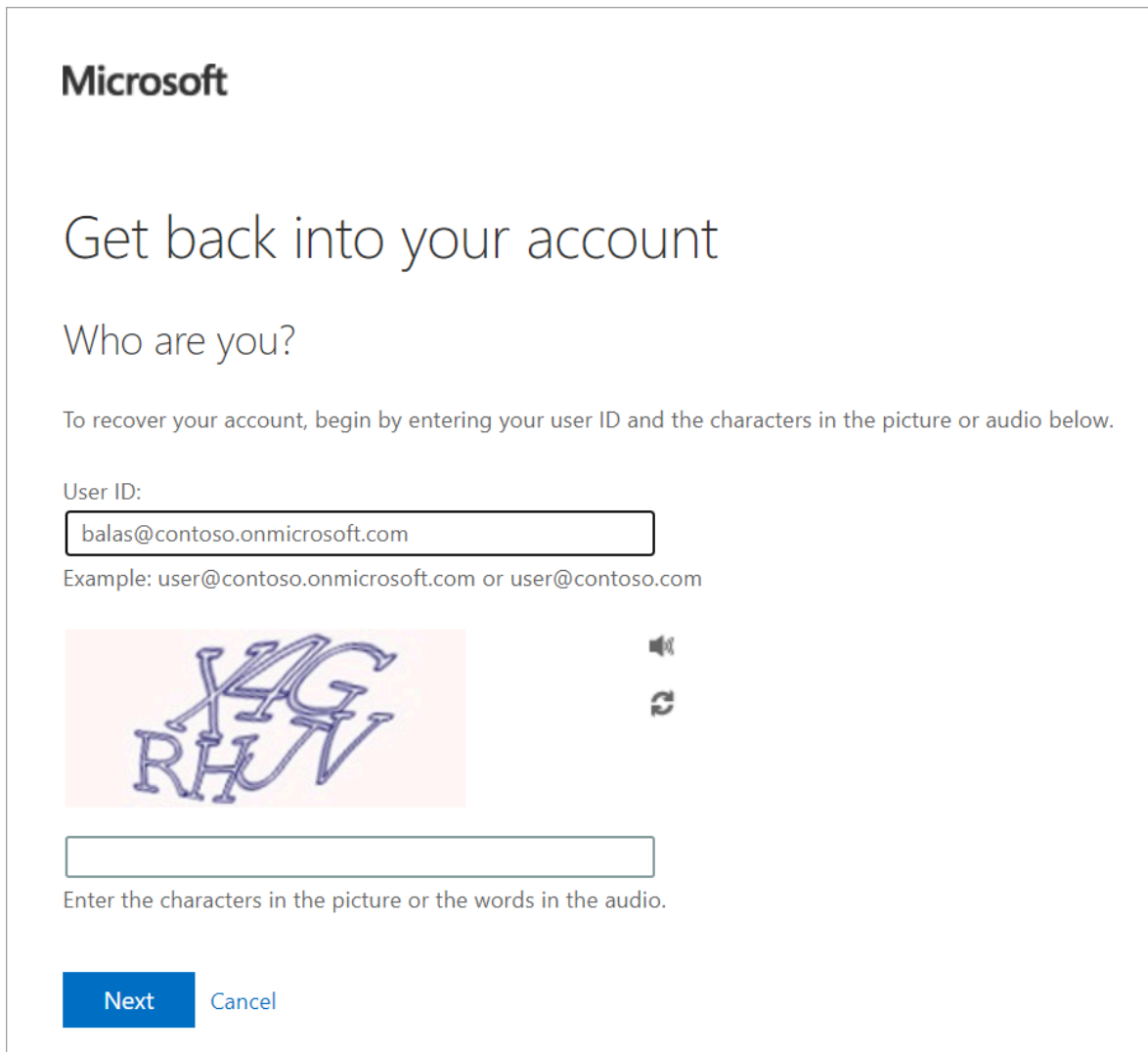


7. When you receive the code in your email, enter the code in the text box and select **Next**.

Test SSPR

Now, let's test whether the user can reset their password.

1. In a new browser window, go to <https://aka.ms/sspr>.
2. For **User ID**, type **balas@organization-domain-name.onmicrosoft.com**. Replace "organization-domain-name" with the domain you used for your Microsoft Entra organization.



3. Complete the CAPTCHA and select **Next**.
4. The **Email my alternate email** radio button is selected. Select **Email**.
5. When the email arrives, in the **Enter your verification code** text box, enter the code you were sent. Select **Next**.
6. Enter a new password, and then select **Finish**. Make sure you note the new password.
7. Close the browser window.

5. Exercise - Customize directory branding

Exercise - Customize directory branding

Completed

Suppose you've been asked to display your retail organization's branding on the Azure sign-in page to reassure users that they're passing credentials to a legitimate system. Here, you'll learn how to configure this custom branding.

To complete this exercise, you must have two image files:

- A page background image. This must be a PNG or JPG file, 1920 x 1080 pixels, and smaller than 300 KB.
- A company logo image. This must be a PNG or JPG file, 32 x 32 pixels, and smaller than 5 KB.

Customize Microsoft Entra organization branding

Let's use Microsoft Entra ID to set up the custom branding.

1. Sign in to the [Azure portal](#).
2. Go to your Microsoft Entra organization by selecting **Microsoft Entra ID**. If you're not in the right Microsoft Entra organization, go to your Azure profile, and select **Switch directory** to find your organization.
3. Under **Manage**, select **Company branding**. Then select the **Customize** button in the center of the screen.
4. Next to **Favicon**, select **Browse**. Select your logo image.
5. Next to **Background image**, select **Browse**. Select your page background image.
6. Select a **Page background color** or accept the default.

Customize default sign-in experience ...

Basics Layout Header Footer Sign-in form Review

Customize the default sign-in experience to personalize the sign-in page for anyone signing-in to your tenant.

Background

Upload background image, favicon or choose background color.

Favicon ⓘ

Background image ⓘ

Image size: 32x32px (resizable)
Max file size: 5KB
File Type: PNG (preferred), JPG, or JPEG

Image will appear darkened to improve contrast and legibility.

Image size: 1920x1080px
Max file size: 300KB
File Type: PNG, JPG, or JPEG

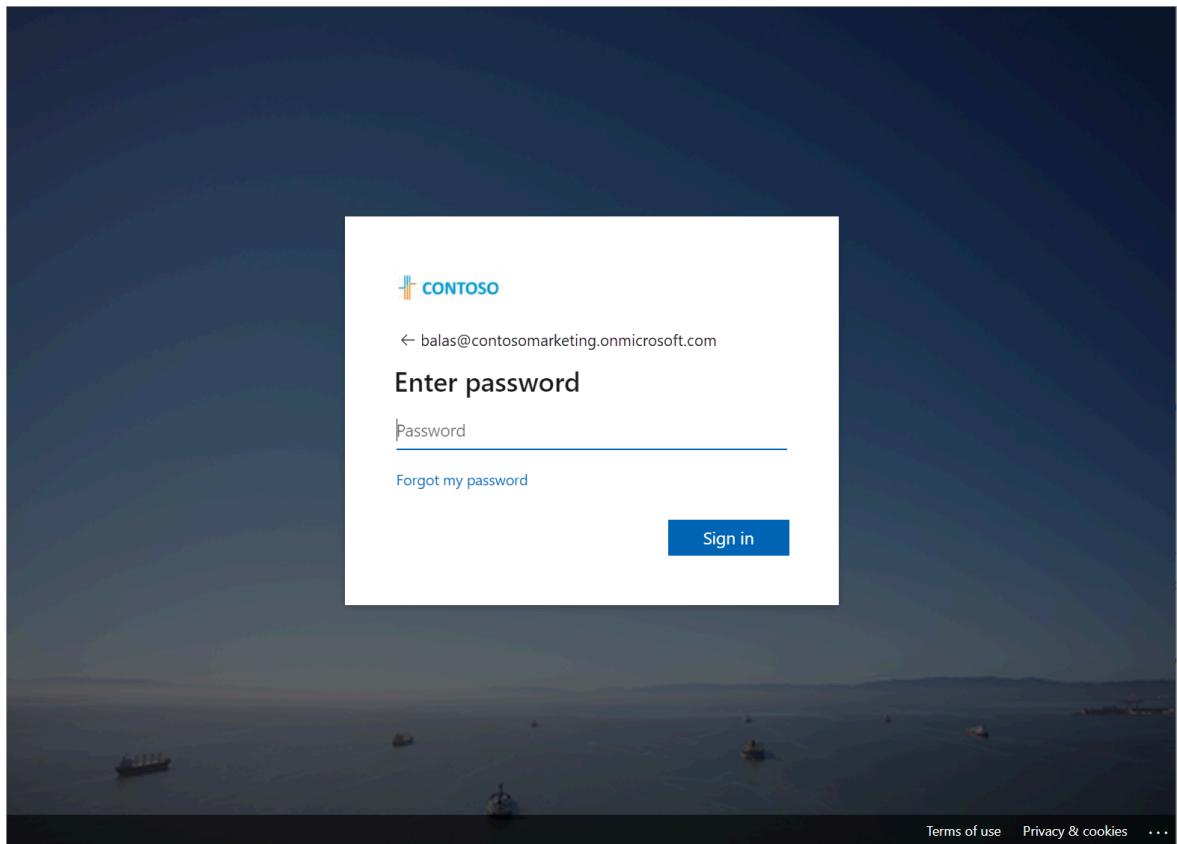
Page background color ⓘ

7. Select **Review + Create**, and then select **Create**.

Test the organization's branding

Now, let's use the account that we created in the last exercise to test the branding.

1. In a new browser window, go to <https://login.microsoft.com>.
2. Select the account for **Bala Sandhu**. Your custom branding is displayed.



3. Select **Forgot my password**.



Get back into your account

Who are you?

To recover your account, begin by entering your user ID and the characters in the picture or audio below.

User ID:

Example: user@contoso.onmicrosoft.com or user@contoso.com



Enter the characters in the picture or the words in the audio.

Next

Cancel

6. Summary

<https://learn.microsoft.com/en-us/training/modules/allow-users-reset-their-password/6-summary>

Summary

Completed

In this module, you've learned how you can use SSPR in Microsoft Entra ID to allow users to reset their forgotten or expired passwords. An administrator doesn't have to do the password reset. SSPR is secured by authentication methods of your choice. These methods can include a mobile authentication app, a code sent to you by an SMS text message, or security questions.

SSPR helps reduce the amount of work required from administrators. It also minimizes the productivity impact for users when they forget their password.

Clean up

Remember to clean up after you've finished.

- **Delete the user you created in Microsoft Entra ID:** Go to **Microsoft Entra ID** > **Manage** > **Users**. Check the box next to the user and select **Delete**. Select **OK**.
- **Delete the group you created in Microsoft Entra ID:** Go to **Microsoft Entra ID** > **Manage** > **Groups**. Check the box next to the group and select **Delete**. Select **OK**.
- **Turn off self-service password reset:** Go to **Microsoft Entra ID** > **Manage** > **Password reset**. Under **Self service password reset enabled**, select **None**. Select **Save**.

If you created a Premium trial Microsoft Entra tenant for this module, you can delete the tenant 30 days after the trial has expired.

Learn more

- [Tutorial: Enable users to unlock their account or reset passwords using Microsoft Entra self-service password reset](#)
- [How it works: Microsoft Entra self-service password reset](#)
- [Enable self-service password reset](#)