

Self-service Password Reset

Self-service password reset (SSPR) in Azure Active Directory (AAD) allows users to reset their passwords without needing to involve IT support. It enhances security and user productivity by providing a streamlined process for password recovery. With SSPR, users can reset their passwords via methods like email, SMS, or security questions, reducing reliance on manual password resets and improving overall efficiency. Administrators can configure SSPR policies to align with security requirements, ensuring a balance between convenience and security.

In this guide, we're setting up self-service password reset (SSPR) in Azure Active Directory (AAD) with Microsoft Entra ID P2 licenses. The end goal is to empower users to reset their passwords independently, utilizing various authentication methods such as email, phone, or authenticator app. This enhances security, reduces reliance on IT support for password resets, and improves overall user productivity.

To begin with the Lab:

1. The Prerequisite for this lab is that you should have Microsoft Entra ID P2 license in place.

Basic information

Name	CloudFreaks	Users	3
Tenant ID	bc45c375-f8b5-420b-9bae-325d48b59d33	Groups	1
Primary domain	CloudFreaks.onmicrosoft.com	Applications	0
License	Microsoft Entra ID P2	Devices	0

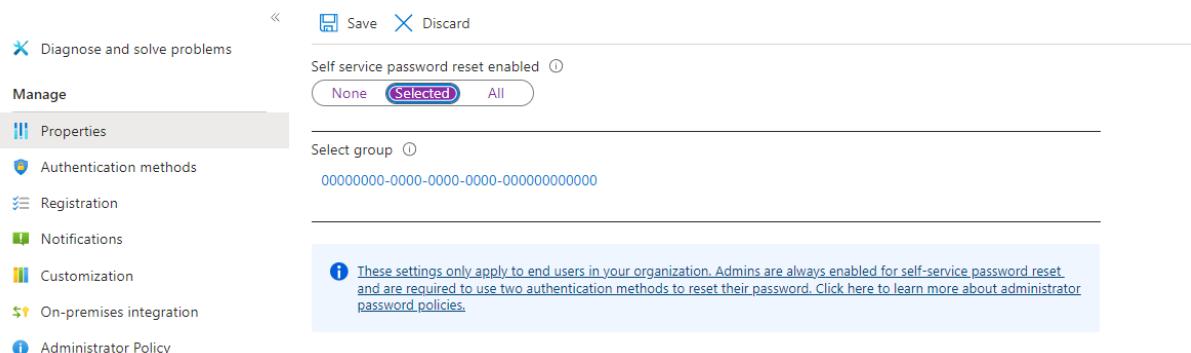
Alerts

2. In your Azure Portal navigate to Microsoft Entra ID. Then you need to expand the Manage tab from left pane.
3. After that scroll down to the Password reset option. Then in there, you need to choose Selected and you will see that it is asking you to select a group click on it.

Home > CloudFreaks | Password reset > Password reset

Password reset | Properties ...

CloudFreaks



Save Discard

Diagnose and solve problems

Manage

Properties

Authentication methods

Registration

Notifications

Customization

On-premises integration

Administrator Policy

Self service password reset enabled

Select group

00000000-0000-0000-0000-000000000000

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. Choose the group and click on save.

Default password reset policy

The screenshot shows the 'Default password reset policy' page in the Microsoft Entra admin center. At the top, there is a search bar and a message: 'Try changing or adding filters if you don't see what you're looking for.' Below the search bar, it says '1 result found'. There are two filter buttons: 'All' and 'Groups', with 'Groups' being selected. A table follows, with columns 'Name', 'Type', and 'Details'. One row is shown, representing 'GroupA' which is a 'Group'. A blue checkmark icon is next to the row. At the bottom of the table are 'Save' and 'Discard' buttons.

Name	Type	Details
GroupA	Group	

5. Now you can see your group here. Just click on save.

The screenshot shows the 'Self-service password reset enabled' section for 'GroupA'. It has three buttons: 'None', 'Selected' (which is highlighted in purple), and 'All'. Below this, there is a 'Select group' dropdown menu with 'GroupA' selected. At the bottom, there is a note: '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.'

6. After that you need to ensure that the members in your group have the Microsoft Entra ID P2 license with them.
7. So, you are going to assign licenses to both of the users. For that, you need to go to the Users tab and open one of your user.
8. Choose your user then click on Edit properties.

Home > CloudFreaks | Users > Users >

The screenshot shows the Azure portal's user management interface. At the top, there's a navigation bar with 'Search', 'Edit properties', 'Delete', 'Refresh', and 'Reset password' buttons. Below the navigation bar, there are three tabs: 'Overview' (selected), 'Monitoring' (disabled), and 'Properties'. On the left, a sidebar lists 'Overview', 'Audit logs', 'Sign-in logs', and 'Diagnose and solve problems'. Under 'Manage', there are 'Custom security attributes' and a large circular profile picture of 'UserA' with a blue 'U' and a small camera icon. To the right, the user details are displayed: 'UserA', 'UserA@CloudFreaks.onmicrosoft.com', and 'Member'.

9. Now you need to make sure that you provide the Usage location in the settings tab.

The screenshot shows the 'Properties' page for 'UserA'. The 'Settings' tab is selected. A note says 'This view only contains properties that can be updated.' Below is a search bar for 'Settings' properties. Under 'Usage location', there is a dropdown menu with a downward arrow. The 'Account enabled' checkbox is checked.

10. After that you need to go to Licenses from the left pane and click on Assignments.

The screenshot shows the 'Licenses' page for 'UserA'. The 'Assignments' button in the top navigation bar is highlighted with a red box. The main table shows 'Products', 'State', 'Enabled Services', and 'Assignment Paths' columns, with a note 'No license assignments found.' The left sidebar includes 'Overview', 'Audit logs', 'Sign-in logs', and 'Diagnose and solve problems'.

11. Then you need to select the license and click on the save button. Then in some time your license will be assigned.

Update license assignments

i When a user has both direct and inherited licenses, only the direct license assignment is removed w

Select licenses

Microsoft Entra ID P2

Review license options

Select



Microsoft Entra ID P2

- Microsoft Defender for Cloud Apps Discovery
- Microsoft Azure Multi-Factor Authentication
- Microsoft Entra ID P1
- Microsoft Entra ID P2

12. Now go back to Password reset option and then go to authentication methods. Here you can set the authentication method of your choice.

Password reset | Authentication methods ...

CloudFreaks

«  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

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.

13. Now we have made the setup for User A to reset their password.
14. Now you need to log in with User A then you will see that it is saying that action required for my organization to keep our account secure.
15. If you remember in the authentication method we had two options email and phone which means that we need to add either our email or our mobile number with it. Click on next.



usera@cloudfreeks.onmicrosoft.com

Action Required

Your organization requires additional security information. Follow the prompts to download and set up the Microsoft Authenticator app.

[Use a different account](#)

[Learn more about the Microsoft Authenticator app](#)

You have 14 days until this is required.

[Ask later](#)

[Next](#)

16. Below you can see that it is asking you to download the Microsoft authenticator app in your mobile phone.

Keep your account secure

Method 1 of 2: App	
App	2
Phone	

Microsoft Authenticator

 [Start by getting the app](#)

On your phone, install the Microsoft Authenticator app. [Download now](#)

After you install the Microsoft Authenticator app on your device, choose "Next".

[I want to use a different authenticator app](#)

[Next](#)

17. Then it will ask you to set up your account in your mobile phone. Just click on next.

Keep your account secure

Method 1 of 2: App



App

2

Phone

Microsoft Authenticator



Set up your account

If prompted, allow notifications. Then add an account, and select "Work or school".

Back

Next

18. Scan the QR code with your phone. Then click on next, afterwards it will give to a number to enter in your mobile phone do that.

Keep your account secure

Method 1 of 2: App



App

2

Phone

Microsoft Authenticator

Scan the QR code

Use the Microsoft Authenticator app to scan the QR code. This will connect the Microsoft Authenticator app with your account.

After you scan the QR code, choose "Next".



[Can't scan image?](#)

[Back](#)

[Next](#)

19. Then you need to complete the second method which is via phone number.

20. Enter your phone number then the OTP or the six digit code.

Keep your account secure

Method 2 of 2: Phone



App



Phone

Phone

You can prove who you are by receiving a code on your phone.

What phone number would you like to use?

Greenland (+299)

Enter phone number

Receive a code

Message and data rates may apply. Choosing Next means that you agree to the [Terms of service](#) and [Privacy and cookies statement](#).

Next

[I want to set up a different method](#)

21. Then it will give you the successful message.

Keep your account secure

Method 2 of 2: Phone



App



Phone

Phone

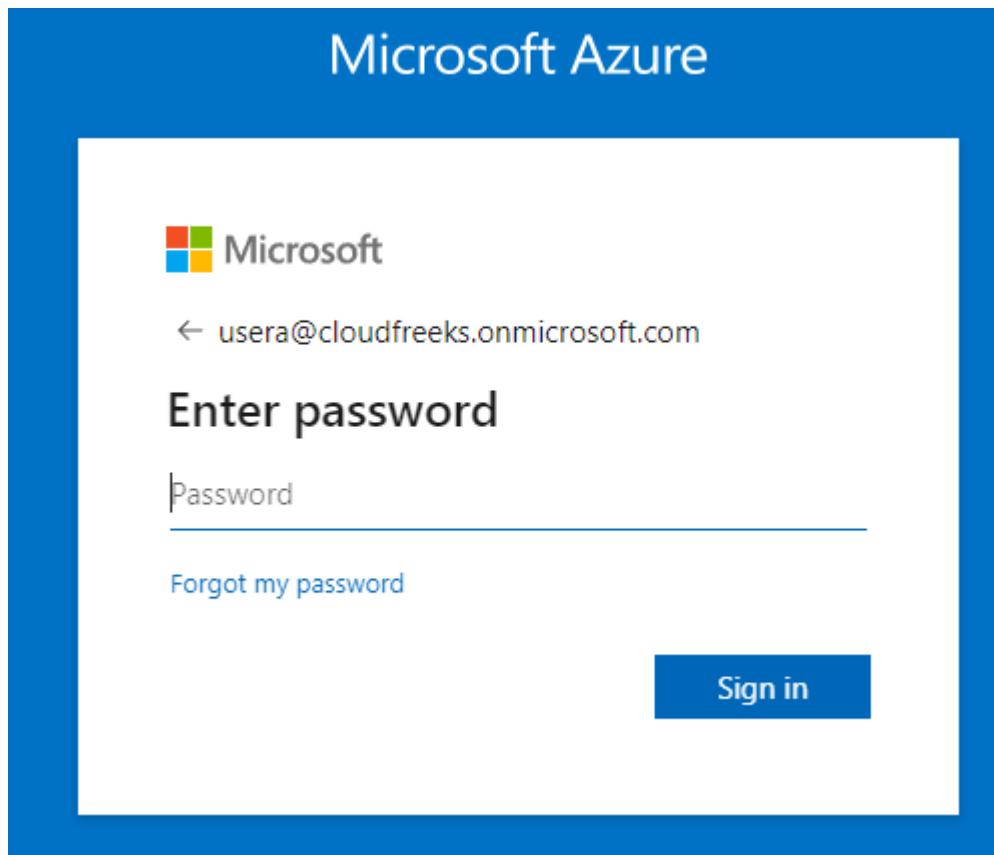
Verification complete. Your phone has been registered.

Next

22. After that you need to Re-login. Once you have logged in then you need to log out.

23. Now let's suppose you forgot your password and you want to change it. Then logout of your account.

24. Choose forgot your password.



25. Here you need to enter your mobile number then a six-digit code will be texted over to your phone you need to enter.
26. After that choose a new password for your user.



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 (*****59) 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](#)

27. Enter the code and click on next.

Get back into your account

verification step 1 > choose a new password

Please choose the contact method we should use for verification:

<input checked="" type="radio"/> Text my mobile phone	We've sent you a text message containing a verification code to your phone.
<input type="text" value="018622"/>	
Next	Try again Contact your administrator

28. After that enter the new password.



Get back into your account

verification step 1 ✓ > **choose a new password**

* Enter new password:

A text input field containing six dots, representing a password.

strong

* Confirm new password:

A text input field containing six dots, representing a password.

Finish

[Cancel](#)

29. Then try to login with your new password.