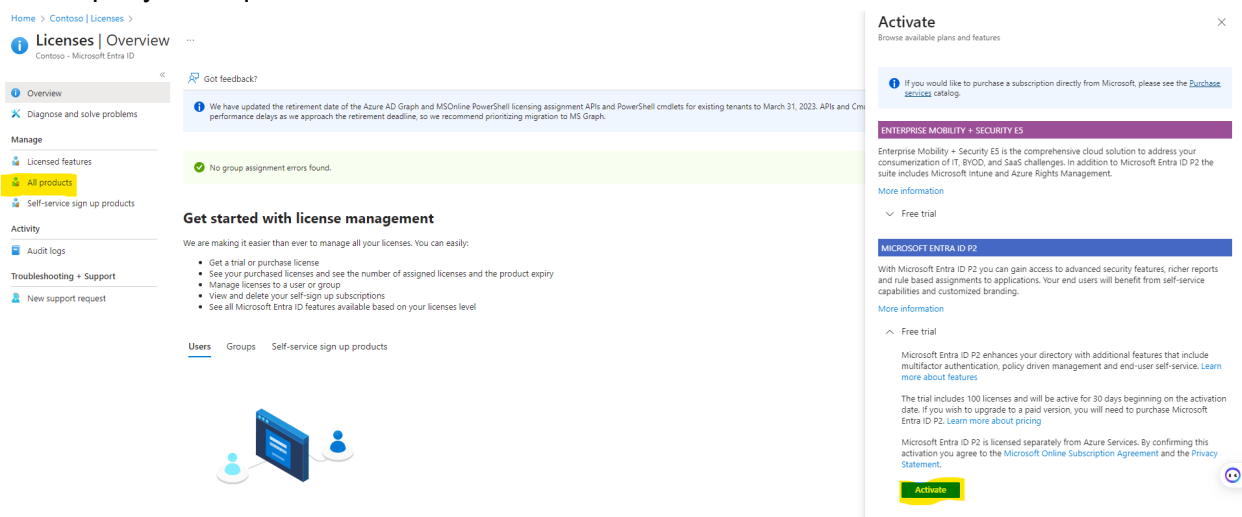


Manage users and groups

1. Under the Manage blade, click Users.
2. Review the different Sources such as Windows Server AD, Invited User, Microsoft Account, and External Microsoft Entra ID.
3. Notice the choice for New guest user.
4. Click New user.
5. Review the two ways to create a user: Create user and Invite user.
6. Create a new user. Review Identity, Groups and roles, Settings, and Job Info.
7. Navigate to Microsoft Entra ID, under Manage click Groups.
8. Review the Group types: Security and Microsoft 365.
9. Create a new group by clicking "New Group" with the Membership type as Assigned.
10. Add a user to the same group.
11. Create another new group with Membership type as Dynamic user.
12. Review the details to construct dynamic group membership rules.

Enable Microsoft Entra ID P2

1. Sign into Azure Portal in the search box Search for Microsoft Entra ID and select it from the results.
2. In the left pane select Licenses->Overview In the top right under "Quick tasks" select "Get a free trial." Select Microsoft Entra ID P2 and select Activate. On the same page under the "All products" tab, you see the list of licenses you have, and you can assign as per your requirements.



The image shows two screenshots from the Azure Portal. The left screenshot displays the 'Licenses | Overview' page for 'Contoso - Microsoft Entra ID'. The left-hand navigation pane is visible, with 'All products' highlighted under the 'Manage' section. The main content area shows a message about updated retirement dates for Azure AD Graph and MSOnline PowerShell licensing APIs, a green status bar indicating 'No group assignment errors found', and a 'Get started with license management' section with a list of tasks. The right screenshot shows the 'Activate' dialog for 'Microsoft Entra ID P2'. It provides information about the free trial (100 licenses, 30 days) and includes an 'Activate' button at the bottom.

Microsoft Entra ID P2 free trial are limited to one free trial per tenant, if you have already activated the Microsoft Entra ID P2 free trial in past it will not allow you activate again.

Configure MFA

1. In the Portal, search for and select Microsoft Entra ID.
2. Under Manage select Security.
3. Under Manage select MFA.
4. In the center pane, under Configure select Additional cloud-based MFA settings.
5. Select the Users tab.
6. Select AZ500User1. Make a note of their user name in the form user@domain.com.
7. On the far right click Enable.
8. Read the information about enabling multi factor authentication in Azure.
9. Click enable multi-factor auth.
10. Wait for update. AZ500User1 will now be required to provide two factor authentication.

Test MFA

1. Sign in to the Portal as AZ500User1. Use their user name from a previous step.
2. Provide the password, click Next.
3. More information is required. Click Next.
4. Review the Additional security verification page.
5. In Step 1, enter your phone number and ensure the send me a code by text message is selected.
6. Click Next.
7. In Step 2, enter the verification code from the text message.
8. Click Verify.
9. In Step 3, read about how to keep your existing applications working.
10. Click Get started with this app password.
11. If prompted, Allow access.
12. Click Done.
13. On the Update password screen, provide and confirm a new password.
14. Click Sign-in.
15. Confirm that you can now access the Portal.

View the status for a user

1. Sign in to the Microsoft Entra admin center as at least an Authentication Administrator.
2. Browse to Identity > Users > All users.

3. Select Per-user MFA.

Navigation bar: + New user + New guest user Bulk operations Refresh Reset password **Per-user MFA** Delete user Columns

Search users Add filters

3 users found

Name	User principal na...	User type	Directory synced	Account enabled	Identity issuer
<input checked="" type="checkbox"/> BS Bala Sandhu	BalaS@nwtraders1.on...	Member	No	Yes	nwtraders1.onmicrosoft.c

4. A new page opens that displays the user state, as shown in the following example.

Microsoft Azure bmath@contoso.com

multi-factor authentication

users service settings

Before you begin, take a look at the [multi-factor auth deployment guide](#).

View: Sign-in allowed users Multi-Factor Auth status: Any **bulk update**

DISPLAY NAME	USER NAME	MULTI-FACTOR AUTH STATUS
<input type="checkbox"/> Bill Mathers	bmath@contoso.com	Disabled
<input type="checkbox"/> Bill Mathers	billmath@billmathfabrikam.onmicrosoft.com	Disabled
<input type="checkbox"/> Britta Simon	bsimon@billmathfabrikam.onmicrosoft.com	Enforced
<input type="checkbox"/> John Smith	jsmith@billmathfabrikam.onmicrosoft.com	Disabled
<input type="checkbox"/> Lola Jacobson	ljacobson@billmathfabrikam.onmicrosoft.com	Enabled

Select a user

Configure conditional access (require MFA)

1. In the Portal, search for and select Microsoft Entra ID.
2. Under Manage, select Security.
3. Under Protect, select Conditional access.
4. Click New Policy.
 - a. Name: AZ500Policy1
 - b. Users and groups > Select users and groups > Users and Groups > Select: AZ500User1
 - c. Cloud apps or actions > Select apps > Select: Microsoft Azure Management
 - d. Review the warning that this policy impacts Portal access.
 - e. Conditions > Sign-in risk > Review the risk levels
 - f. Device platforms > Review the devices that can be included, such as Android and iOS.
 - g. Locations > Review the physical location selections.

- h. Under Access controls click Grant.
 - i. Review the Grant options such as MFA. You may require one or more of the controls.
 - j. Select Require multi-factor authentication.
 - k. For Enable policy, select On.
- 5. Click Create.

Test the policy

- 1. Sign in to the Portal as the AZ500User1.
- 2. Before you can sign in, a second authentication is required.
- 3. If you have a phone number associated with the user, provide and verify the text code. You should be able to sign in to the Portal successfully.
- 4. If you do not have a phone number associated with the user, this demonstrates that MFA is in effect.
- 5. You may want to return to the AZ500Policy1 and turn the policy Off.

Configure an access review

- 1. In the Portal, search for and select Identity Governance.
- 2. Under Access Reviews, select Access Reviews.
- 3. Click New Access Review.
- 4. We will create an access review to ensure we validate the AZ500Admin group membership.
- 5. Complete the required information and discuss each setting. Configuration settings are added as you make your selections. For example, if you select a weekly access review, you will be prompted for the duration.
 - a. Review name: AZ500Review
 - b. Start date: current date
 - c. Frequency: One-time
 - d. Users to review: Members of a group
 - e. Scope: Everyone
 - f. Select a group: AZ500Admins
 - g. Reviewers: Selected user
 - h. Select reviewers: add yourself as a reviewer
 - i. Review the Upon completion settings, specifically the action if a reviewer doesn't respond.
 - j. Review Advanced settings.
- 6. Start the access review.

7. On the Access review page, ensure the new access review is listed.
8. The Status will change from Not started to Initializing.

Conduct an access review

1. When the access review is complete, you will receive an email. This is the email associated with your reviewer account.
2. View the email and discuss the review instructions. Note when the review period will end.
3. In the email, click Start review.
4. On the Access reviews page, click the AZ500Review.
5. Notice you are reviewing the AZ500Admin group members. There are two members.
6. Use the Details link to view information about the user.
7. Select Approve for one user and Deny for the other. Be sure to provide a Reason.
8. Submit your reviews.

Review the access review results

1. Return to the Portal.
2. Click the AZ500Review.
3. From the Overview blade, review the results.
4. There should be one member approved and one member denied.
5. Click Results for more detailed information about the reviewer and their reasons.
6. From the Overview blade, click Stop and confirm you want to stop the review.
7. The Review status should now be Complete.

Apply the access review

1. In the Portal, search for and select Microsoft Entra ID.
2. Under Manage, select Groups.
3. Locate the AZ500Admins group.
4. Review the members of the group.
5. Confirm there are two members.

6. Return to the AZ500Review.
7. Click Apply.
8. Confirm that you want to remove the denied member.
9. The Review status will change from Applying to Result applied.
10. Verify the AZ500Admins group now only has one member.