Enable per-user multifactor authentication - Microsoft Entra ID | Microsoft Learn - 03/11/2024 18:42 https://learn.microsoft.com/en-us/entra/identity/authentication/howto-mfa-userstates

Learn Discover Product documentation Development languages Topics Sign in

Microsoft Entra Microsoft Entra ID External ID Global Secure Access ID Governance Permissions Management More Admin center

Filter by title
Configure custom banned password lists
Enable risk-based sign-in protection
Enable security notifications
Concepts
Authentication methods
Conditional Access authentication strength
Self-service password reset
Multifactor authentication
Password protection
Security information registration
Resilient access controls
Web browser cookies
How-to guides
Manage authentication methods
Temporary Access Pass
Passwordless
Use SMS-based authentication
Use email address sign-in
Use Microsoft managed settings
Security info registration
Self-service password reset
Microsoft Entra multifactor authentication
Deployment guide
Configure settings
Configure users
Verify mandatory MFA
Find coverage gaps
Enable per-user MFA
Manage external authentication method
Configure authentication providers
Use app passwords
Directory Federation
RADIUS Integration
On-premises password protection
Microsoft Entra smart lockout
Reporting
MFA Server
Troubleshoot
Reference
Resources
Download PDF

… / Microsoft Entra / Microsoft Entra ID / Authentication /

Enable per-user Microsoft Entra multifactor authentication to secure sign-in events

Article • 10/31/2024 • 33 contributors

Feedback

In this article

To secure user sign-in events in Microsoft Entra ID, you can require Microsoft Entra multifactor authentication (MFA). The best way to protect users with Microsoft Entra MFA is to create a Conditional Access policy. Conditional Access is a Microsoft Entra ID P1 or P2 feature that lets you apply rules to require MFA as needed in certain scenarios. To get started using Conditional Access, see Tutorial: Secure user sign-in events with Microsoft Entra multifactor authentication.

For Microsoft Entra ID Free tenants without Conditional Access, you can use security defaults to protect users. Users are prompted for MFA as needed, but you can't define your own rules to control the behavior.

If needed, you can instead enable each account for per-user Microsoft Entra MFA. When you enable users individually, they perform MFA each time they sign in. You can enable exceptions, such as when they sign in from trusted IP addresses, or when the **remember MFA on trusted devices** feature is turned on.

Changing user states isn't recommended unless your Microsoft Entra ID licenses don't include Conditional Access and you don't want to use security defaults. For more information on the different ways to enable MFA, see Features and licenses for Microsoft Entra multifactor authentication.

> **Important**
>
> This article details how to view and change the status for per-user Microsoft Entra multifactor authentication. If you use Conditional Access or security defaults, you don't review or enable user accounts using these steps.
>
> Enabling Microsoft Entra multifactor authentication through a Conditional Access policy doesn't change the state of the user. Don't be alarmed if users appear disabled. Conditional Access doesn't change the state.
>
> **Don't enable or enforce per-user Microsoft Entra multifactor authentication if you use Conditional Access policies.**

Microsoft Entra multifactor authentication user states

A user's state reflects whether an Authentication Administrator enrolled them in per-user Microsoft Entra multifactor authentication. User accounts in Microsoft Entra multifactor authentication have the following three distinct states:

Expand table

State	Description	Legacy authentication affected	Browser apps affected	Modern authentication affected

Disabled	The default state for a user not enrolled in per-user Microsoft Entra multifactor authentication.	No	No	No
Enabled	The user is enrolled in per-user Microsoft Entra multifactor authentication, but can still use their password for legacy authentication. If the user has no registered MFA authentication methods, they receive a prompt to register the next time they sign in using modern authentication (such as when they sign in on a web browser).	No. Legacy authentication continues to work until the registration process is completed.	Yes. After the session expires, Microsoft Entra multifactor authentication registration is required.	Yes. After the access token expires, Microsoft Entra multifactor authentication registration is required.
Enforced	The user is enrolled per-user in Microsoft Entra multifactor authentication. If the user has no registered authentication methods, they receive a prompt to register the next time they sign in using modern authentication (such as when they sign in on a web browser). Users who complete registration while they're *Enabled* are automatically moved to the *Enforced* state.	Yes. Apps require app passwords.	Yes. Microsoft Entra multifactor authentication is required at sign-in.	Yes. Microsoft Entra multifactor authentication is required at sign-in.

All users start out *Disabled*. When you enroll users in per-user Microsoft Entra multifactor authentication, their state changes to *Enabled*. When enabled users sign in and complete the registration process, their state changes to *Enforced*. Administrators may move users between states, including from *Enforced* to *Enabled* or *Disabled*.

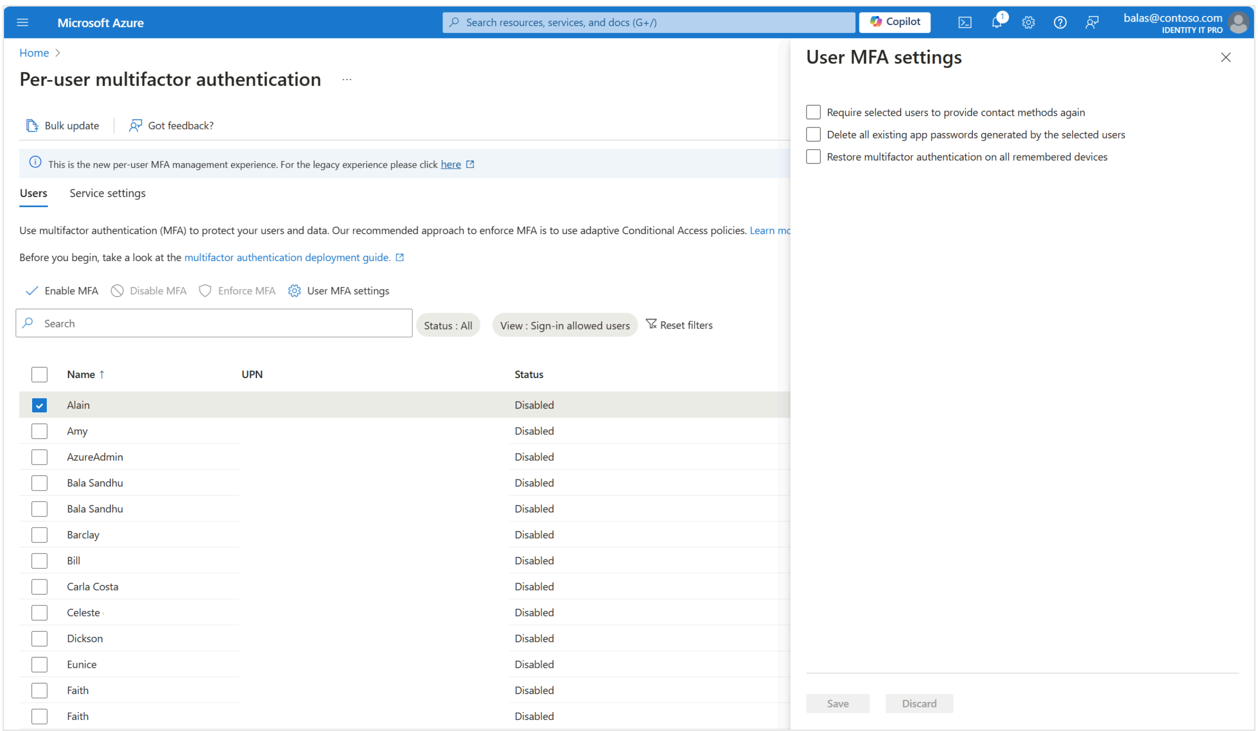
ⓘ Note

If per-user MFA is re-enabled on a user and the user doesn't re-register, their MFA state doesn't transition from *Enabled* to *Enforced* in MFA management UI. The administrator must move the user directly to *Enforced*.

View the status for a user

The per-user MFA administration experience in the Microsoft Entra admin center is recently improved. To view and manage user states, complete the following steps:

1. Sign in to the Microsoft Entra admin center as at least an Authentication Policy Administrator.
2. Browse to **Identity** > **Users** > **All users**.
3. Select a user account, and click **User MFA settings**.
4. After you make any changes, click **Save**.



Per-user multifactor authentication

This is the new per-user MFA management experience. For the legacy experience please click here

Use multifactor authentication (MFA) to protect your users and data. Our recommended approach to enforce MFA is to use adaptive Conditional Access policies. Learn mc

Before you begin, take a look at the multifactor authentication deployment guide.

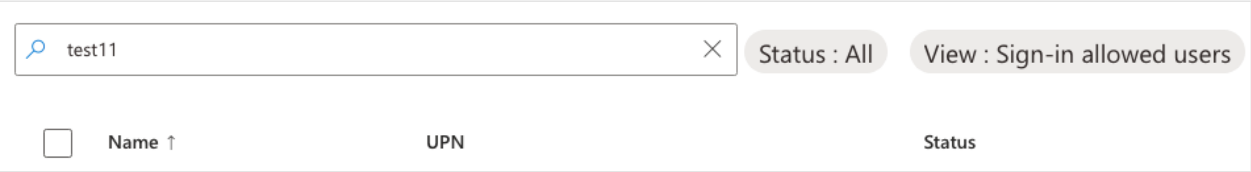
	Name ↑	UPN	Status
☑	Alain		Disabled
□	Amy		Disabled
□	AzureAdmin		Disabled
□	Bala Sandhu		Disabled
□	Bala Sandhu		Disabled
□	Barclay		Disabled
□	Bill		Disabled
□	Carla Costa		Disabled
□	Celeste		Disabled
□	Dickson		Disabled
□	Eunice		Disabled
□	Faith		Disabled
□	Faith		Disabled

User MFA settings

□ Require selected users to provide contact methods again
□ Delete all existing app passwords generated by the selected users
□ Restore multifactor authentication on all remembered devices

If you try to sort thousands of users, the result might gracefully return **There are no users to display**. Try to enter more specific search criteria to narrow the search, or apply specific **Status** or

View filters.



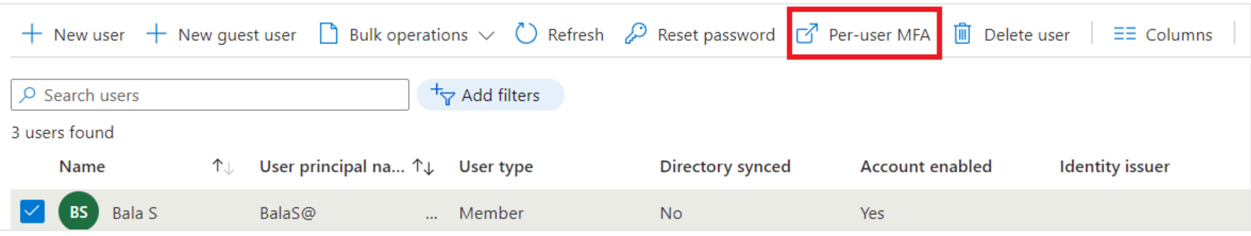
□	Name ↑	UPN	Status

During transition to the new per-user MFA experience, you can also access the legacy per-user MFA experience. The format is:

`https://account.activedirectory.windowsazure.com/usermanagement/multifactorverification.aspx?tenantId=${userTenantID}`

To get the `userTenantID`, copy the tenant ID on the **Overview** page in the Microsoft Entra admin center. Then follow these steps to view status for a user with the legacy experience:

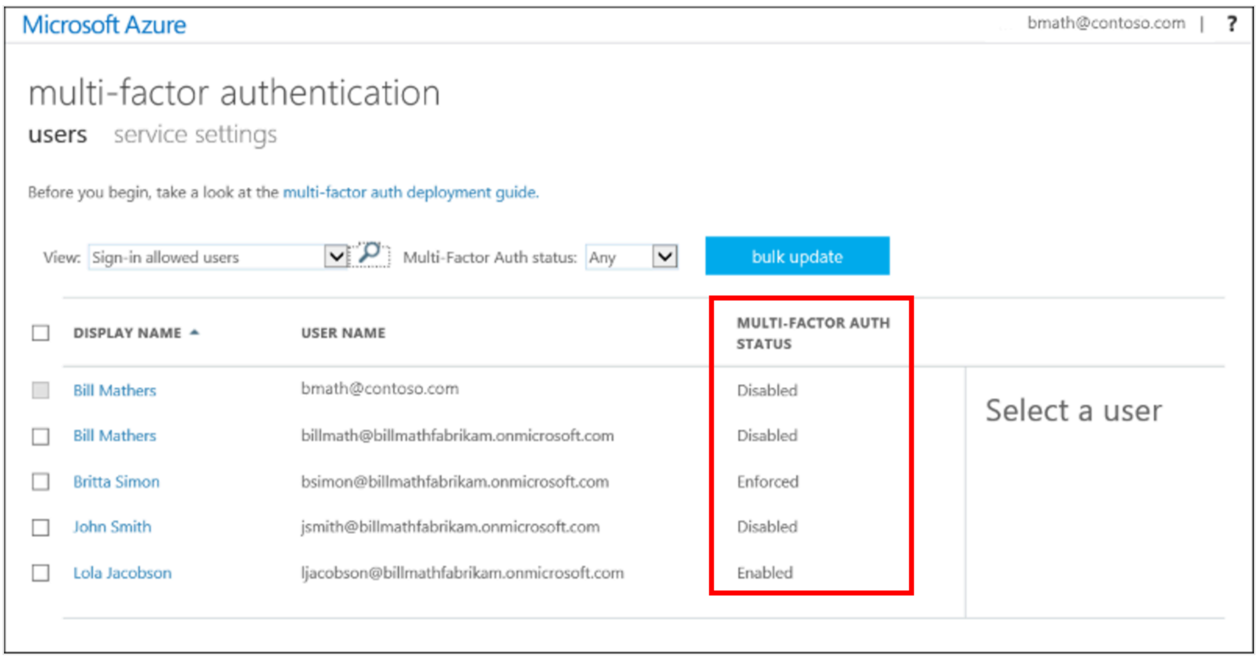
1. Sign in to the Microsoft Entra admin center as at least an Authentication Administrator.
2. Browse to **Identity** > **Users** > **All users**.
3. Select **Per-user MFA**.



3 users found

	Name	User principal na...	User type	Directory synced	Account enabled	Identity issuer
☑	BS Bala S	BalaS@ ...	Member	No	Yes	

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
View: Sign-in allowed users
Multi-Factor Auth status: Any
bulk update
Select a user

Before you begin, take a look at the multi-factor auth deployment guide.

□	DISPLAY NAME ▲	USER NAME	MULTI-FACTOR AUTH STATUS
□	Bill Mathers	bmath@contoso.com	Disabled
□	Bill Mathers	billmath@billmathfabrikam.onmicrosoft.com	Disabled
□	Britta Simon	bsimon@billmathfabrikam.onmicrosoft.com	Enforced
□	John Smith	jsmith@billmathfabrikam.onmicrosoft.com	Disabled
□	Lola Jacobson	ljacobson@billmathfabrikam.onmicrosoft.com	Enabled

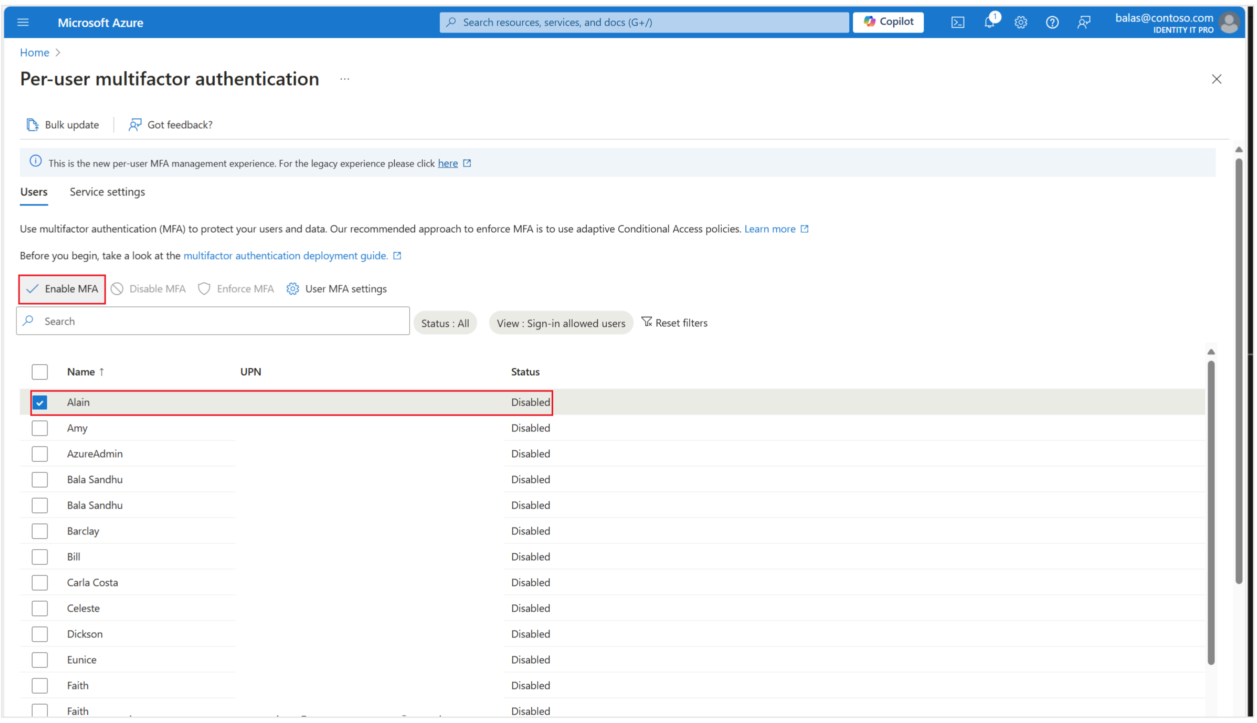
Change the status for a user

To change the per-user Microsoft Entra multifactor authentication state for a user, complete the following steps:

1. Sign in to the Microsoft Entra admin center as at least an Authentication Policy Administrator.

2. Browse to **Identity** > **Users** > **All users**.

3. Select a user account, and click **Enable MFA**.



This is the new per-user MFA management experience. For the legacy experience please click here

Use multifactor authentication (MFA) to protect your users and data. Our recommended approach to enforce MFA is to use adaptive Conditional Access policies. Learn more

Before you begin, take a look at the multifactor authentication deployment guide.

□	Name ↑	UPN	Status
☑	Alain		Disabled
□	Amy		Disabled
□	AzureAdmin		Disabled
□	Bala Sandhu		Disabled
□	Bala Sandhu		Disabled
□	Barclay		Disabled
□	Bill		Disabled
□	Carla Costa		Disabled
□	Celeste		Disabled
□	Dickson		Disabled
□	Eunice		Disabled
□	Faith		Disabled
□	Faith		Disabled

> **Tip**
>
> *Enabled* users are automatically switched to *Enforced* when they register for Microsoft Entra multifactor authentication. Don't manually change the user state to *Enforced* unless the user is already registered or if it is acceptable for the user to experience interruption in connections to legacy authentication protocols.

4. Confirm your selection in the pop-up window that opens.

After you enable users, notify them by email. Tell the users that a prompt is displayed to ask them to register the next time they sign in. If your organization uses applications that don't run in a browser or support modern authentication, you can create application passwords. For more information, see Enforce Microsoft Entra multifactor authentication with legacy applications using app passwords.

Use Microsoft Graph to manage per-user MFA

You can manage per-user MFA settings by using the Microsoft Graph REST API Beta. You can use the authentication resource type to expose authentication method states for users.

To manage per-user MFA, use the perUserMfaState property within users/id/authentication/requirements. For more information, see strongAuthenticationRequirements resource type.

View per-user MFA state

To retrieve the per-user multifactor authentication state for a user:

```
GET /users/{id | userPrincipalName}/authentication/requirements
```

For example:

```
GET https://graph.microsoft.com/beta/users/071cc716-8147-4397-a5ba-b2105951cc0b/authentic
```

If the user is enabled for per-user MFA, the response is:

```
HTTP/1.1 200 OK
Content-Type: application/json

{
  "perUserMfaState": "enforced"
}
```

For more information, see Get authentication method states.

Change MFA state for a user

To change multifactor authentication state for a user, use the user's strongAuthenticationRequirements. For example:

```
PATCH https://graph.microsoft.com/beta/users/071cc716-8147-4397-a5ba-b2105951cc0b/authent
Content-Type: application/json

{
  "perUserMfaState": "disabled"
}
```

If successful, the response is:

```
HTTP/1.1 204 No Content
```

For more information, see Update authentication method states.

Next steps

To configure Microsoft Entra multifactor authentication settings, see Configure Microsoft Entra multifactor authentication settings.

To manage user settings for Microsoft Entra multifactor authentication, see Manage user settings with Microsoft Entra multifactor authentication.

To understand why a user was prompted or not prompted to perform MFA, see Microsoft Entra multifactor authentication reports.

Feedback

Was this page helpful? Yes No

Provide product feedback

Additional resources

Training

Module

Secure Microsoft Entra users with multifactor authentication - Training

Learn how to use multifactor authentication with Microsoft Entra ID to harden your user accounts.

Certification

Microsoft Certified: Identity and Access Administrator Associate - Certifications

Demonstrate the features of Microsoft Entra ID to modernize identity solutions, implement hybrid solutions, and implement identity governance.