

Turning on MFA

Video for Admins: <https://www.youtube.com/watch?v=vE09Sb326XM>

Start here: https://help.salesforce.com/articleView?id=sf.mfa_welcome_to_mfa.htm&type=5

Then go to Roll Out: https://help.salesforce.com/articleView?id=sf.mfa_rollout_phase.htm&type=5

To actually turn it on: https://help.salesforce.com/articleView?id=sf.mfa_enable_core.htm&type=5

Create a permission set:

The screenshot shows the Salesforce Setup interface for creating a new permission set. At the top, there is a 'SETUP' header with a user icon and the text 'Permission Sets'. Below this, the page title is 'Permission Set Create'. There are 'Save' and 'Cancel' buttons in the top right corner. The main section is titled 'Enter permission set information' and contains the following fields:




- Label:** Multi factor authentication
- API Name:** Multi_factor_authentication
- Description:** (Empty text area)
- Session Activation Required:** [i](#)

Below this section is another titled 'Select the type of users who will use this permission set'. It includes the question 'Who will use this permission set?' followed by three bullet points:

- Choose '--None--' if you plan to assign this permission set to multiple users with different user and permission licenses.
- Choose a specific user license if you want users with only one license type to use this permission set.
- Choose a specific permission set license if you want this permission set license auto-assigned with the permission set.

There is a link 'Learn more here.' and a 'License' dropdown menu currently set to '--None--'.

In the System Permissions Turn on "Multi-Factor Authentication for User Interface Logins:

SETUP		
Permission Sets		
Moderate Files in Experience Cloud Sites	<input type="checkbox"/>	Moderate Salesforce Files in Experience Cloud sites.
Modify All Data	<input type="checkbox"/> 	Create, edit, and delete all organization data, regardless of sharing set
Modify Data Classification	<input type="checkbox"/>	View and modify field-level data classification metadata.
Modify Metadata Through Metadata API Functions	<input type="checkbox"/> 	Create, read, edit, and delete org metadata. Users must have appropriate permission. Some metadata executes in system context, when object example, Apex executes in system context.
Multi-Factor Authentication for API Logins	<input type="checkbox"/> 	Require users to enter a code from a time-based one-time password (
Multi-Factor Authentication for User Interface Logins	<input checked="" type="checkbox"/>	Require users to provide an additional verification method in addition t

Save and assign the users to the permission set.

Alternatively, if you have custom profiles, you can turn this option on directly on the profiles (won't work for System Administrator)

For Office365, go to Admin, Azure Active Directory admin center, Azure Active Directory, Properties, Manage Security Defaults, and Enable Security Defaults:

- Dashboard
- All services
- FAVORITES
- Azure Active Directory
- Users
- Enterprise applications

Dashboard > Enclude

Enclude | Properties

Azure Active Directory

- Devices
- App registrations
- Identity Governance
- Application proxy
- Licenses
- Azure AD Connect
- Custom domain names
- Mobility (MDM and MAM)
- Password reset
- Company branding
- User settings
- Properties**
- Security
- Monitoring
- Sign-ins
- Audit logs
- Provisioning logs (Preview)
- Logs
- Diagnostic settings
- Workbooks
- Usage & insights

Save Discard

Tenant properties

Name *

Enclude

Country or region

Ireland

Location

EU Model Clause compliant d

Notification language

English

Tenant ID

Technical contact

eamon.kelly@enclude.ie

Global privacy contact

Privacy statement URL

Access management for

Eamon Kelly (eamon.kelly@er
management groups in this te

Yes No

Manage Security defaults

Enable Security d

Security defaults is a set of basic recommended by Microsoft. Wh will be automatically enforced in and users will be better protecte attacks.

[Learn more](#)

Enable Security defaults

Yes No

Save