



ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

MFA (Multi-Factor Authentication) Management

Last update 10/12/2025

Multi-Factor authentication (MFA) enhances the security of institutional credentials by requiring an additional authentication method alongside your personal password. This second factor can be:

- a code received via SMS to the phone number provided during activation
- an automated phone call to the number provided during activation
- a notification sent by Microsoft via the Outlook Mobile app, if the app is installed on your smartphone and your @unibo.it mailbox has been configured.

Alternatively, you can configure the Microsoft Authenticator app and use it as a second factor (see [the vendor's documentation](#) for details).

The second factor is not requested at every login, but only periodically or when accessing services from a different device to your usual workstation.

Currently, MFA is only active for Microsoft applications (e.g., Outlook, Teams, OneDrive, OneNote...) and not for other university applications (e.g., AlmaEsami, Cedolini).

Examples of when the second factor is required:

- the first time you access each Microsoft application after activation (for each shared mailbox configured in Outlook, you may be asked for the second factor)
- the first time you access a Microsoft application from a new device
- the first time you access a Microsoft application in the web version (e.g., your mailbox or OneDrive). If you select 'No' when asked whether you want to 'stay signed in' after authentication, the second factor will also be required at the next login.

Summary

Activating MFA	2
Deactivating MFA	6
Activating Outlook as a second factor	8
Checking and editing Outlook settings	10

Activating MFA

Go to the page www.dsa.unibo.it and click **LOGIN**.
Log in using your SPID or CIE digital identity.





If you have both a @unibo.it account and a @studio.unibo.it account, click the **LOGIN** button next to your @unibo.it account.

DIRECTORY SERVICE D'ATENEEO

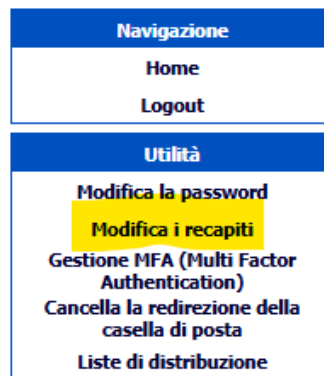
Portale utente del servizio Directory Service d'Ateneo (DSA)

Benvenuto Nome Cognome.

Sono stati trovati i seguenti account associati al codice fiscale *****944D
fornito da SPID/CIE.

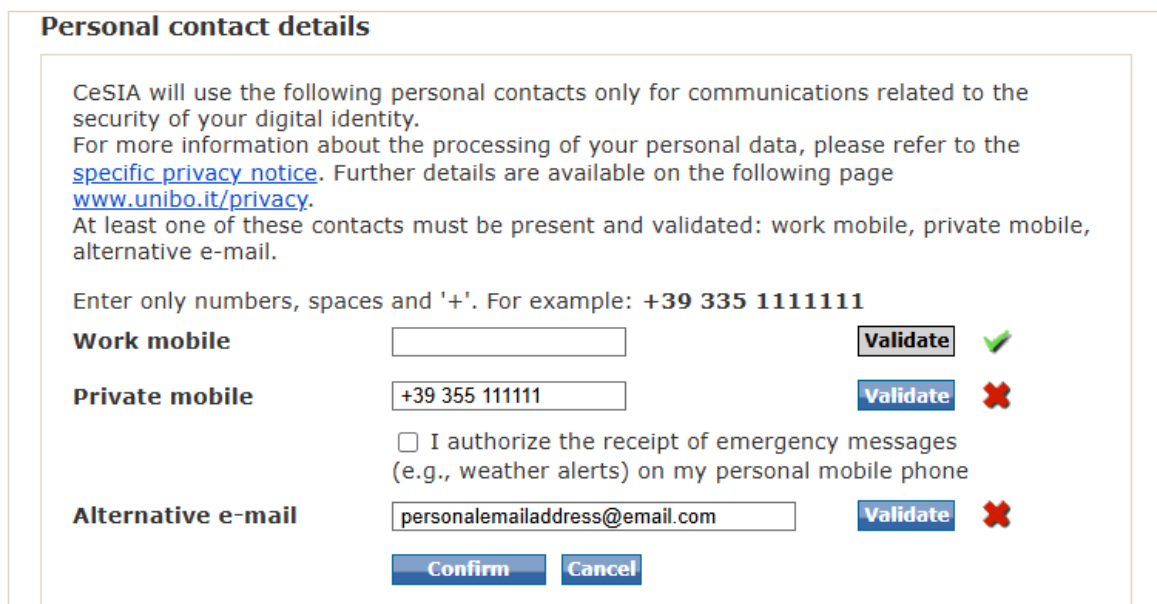
Tipo account	Username	Note	
PERSONALE	nome.cognome@unibo.it		 LOGIN
STUDENTE	nome.cognome@studio.unibo.it		 LOGIN

In the left-hand menu, click **Modify Contacts**.



The screenshot shows a vertical menu with two main sections: 'Navigazione' and 'Utilità'. Under 'Navigazione', there are links for 'Home' and 'Logout'. Under 'Utilità', there are links for 'Modifica la password', 'Modifica i recapiti' (which is highlighted with a yellow background), 'Gestione MFA (Multi Factor Authentication)', 'Cancella la redirectione della casella di posta', and 'Liste di distribuzione'.

Check that your personal mobile number is correct, update and validate it if necessary, then click **Confirm**.



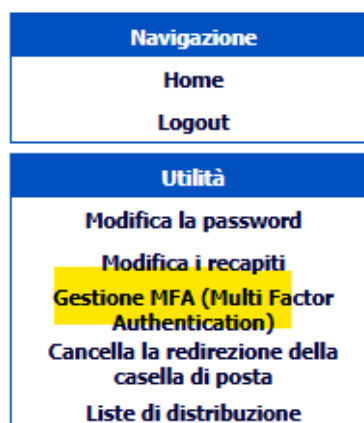
The screenshot shows a form titled 'Personal contact details'. It contains a paragraph of text explaining that CeSIA will use the provided contacts for communications related to the security of the user's digital identity, and that further details are available in the specific privacy notice at www.unibo.it/privacy. It also states that at least one of the contacts must be present and validated: work mobile, private mobile, or alternative e-mail.

Below the text, there are three input fields with corresponding 'Validate' buttons and status icons:

- Work mobile**: An empty input field. The 'Validate' button is greyed out, and there is a green checkmark icon.
- Private mobile**: An input field containing '+39 355 111111'. The 'Validate' button is blue, and there is a red 'X' icon.
- Alternative e-mail**: An input field containing 'personalemailaddress@email.com'. The 'Validate' button is blue, and there is a red 'X' icon.

At the bottom of the form, there are two buttons: 'Confirm' and 'Cancel'.

In the left-hand menu, click **MFA (Multi-Factor Authentication) Management**.



The screenshot shows the same vertical menu as before. In this instance, the 'Gestione MFA (Multi Factor Authentication)' link under the 'Utilità' section is highlighted with a yellow background.

MFA (Multi-Factor Authentication) Management

An information screen will appear.

Multi Factor Authentication (MFA) activation

1

2

3

General informations

Multi-Factor Authentication (MFA), which allows you to add an extra layer of protection to your institutional credentials, is **NOT ACTIVE** for your user **name.surname@unibo.it**

When the Microsoft systems receive the activation of MFA (usually within 30 minutes), you will be asked to enter your username, password, and an additional form of identification (second factor).

The second factor can be a code received via SMS, the response to an automated call to the phone number provided during the activation process, or the response to a notification sent by Microsoft through the Outlook mobile app.

Afterward, you will be able to configure the Microsoft Authenticator app to use it as an alternative second factor of authentication to SMS.

MFA is currently operational only for Microsoft applications (e.g., Outlook, Teams, OneDrive, OneNote...) and not for other university applications (e.g. Cedolini, PresenzeWeb, ...).

MFA can be deactivated at any time.

Do you want to proceed with the activation of MFA?

NEXT

Read the page carefully, then click **NEXT** if you wish to continue.

Check the telephone contacts shown on the page.

Multi Factor Authentication (MFA) activation

1

2

3

Your contacts

The MFA activation requires the use of at least one mobile phone number that must be present in the Microsoft systems.

The mobile phone numbers present in DSA for credential recovery will be transferred directly to Microsoft.

The following mobile numbers are registered with Microsoft.

no mobile number available.

Actions that will be performed for the numbers registered in DSA:

Personal mobile	+39 355 11111	It will be transferred to Microsoft.
-----------------	---------------	--------------------------------------

If you want to update your contact details DSA go to the page [change contacts](#).
The MFA activation will be interrupted, and you will be able to resume it later.

Do you want to complete the MFA activation?

BACK

NEXT

If you need to edit your contact information, you can do so by clicking the **change contacts** link on the page or the same item in the left-hand menu.

If you do this, the MFA activation process will stop.

If the information is correct, click **NEXT**.

Another information page will appear.

MFA (Multi-Factor Authentication) Management

Multi Factor Authentication (MFA) activation

1

2

3

Confirmation of activation

MFA ACTIVATION in progress.

You have been sent a confirmation email and SMS; the completion of the operation on the Microsoft systems may take approximately **30 minutes**.

When the Microsoft systems receive the MFA activation, you will be asked to enter your username, password, and the second factor.

The second factor can be a code received via SMS, the response to an automated call to the phone number provided during the activation process, or the response to a notification sent by Microsoft through the Outlook mobile app.

Afterward, you will be able to configure the Microsoft Authenticator app to use it as an alternative second factor of authentication to SMS ([instructions](#)).

You can edit the mobile numbers on Microsoft by connecting to the address mysignins.microsoft.com/security-info.

FINISH

Read it carefully, then click **FINISH**.

Your activation request has been completed, and you will receive a confirmation email and SMS from the system.

Updating the settings on Microsoft systems may take up to 30 minutes.

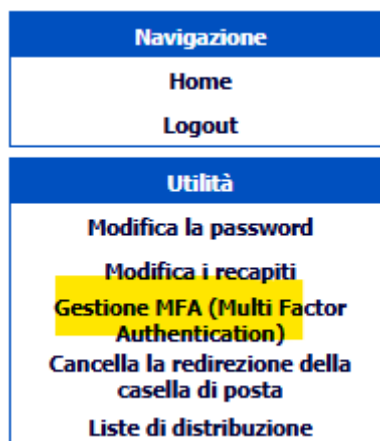
Once this is completed, if you are using applications that require MFA, you will be asked to enter your username, password, and second factor.

Deactivating MFA

Go to the page www.dsa.unibo.it and click **LOGIN**.
Log in using your SPID or CIE digital identity.



In the left-hand menu, click **MFA (Multi-Factor Authentication) Management**.



An information screen will appear.

Multi Factor Authentication (MFA) deactivation

Deactivation request

Multi-Factor Authentication (MFA), which allows you to add an extra layer of protection to your institutional credentials, is **ACTIVE** for your user **nome.cognome@unibo.it**

MFA is currently operational only for Microsoft applications (e.g., Outlook, Teams, OneDrive, OneNote...) and not for other university applications (e.g., AlmaEsami Cedolini, PresenzeWeb, ...).

If you wish, you can deactivate MFA for this account.

Do you want to proceed with the deactivation of MFA?

NEXT

MFA (Multi-Factor Authentication) Management

Read the content carefully.

If you wish to proceed, click **NEXT**.

Multi Factor Authentication (MFA) deactivation

1

2

Deactivation confirmation

MFA DEACTIVATION in progress.

You have been sent a confirmation email and SMS; the completion of the operation on the Microsoft systems may take approximately **30 minutes**.

MFA can be reactivated at any time using "*Gestione MFA (Multi Factor Authentication)*".

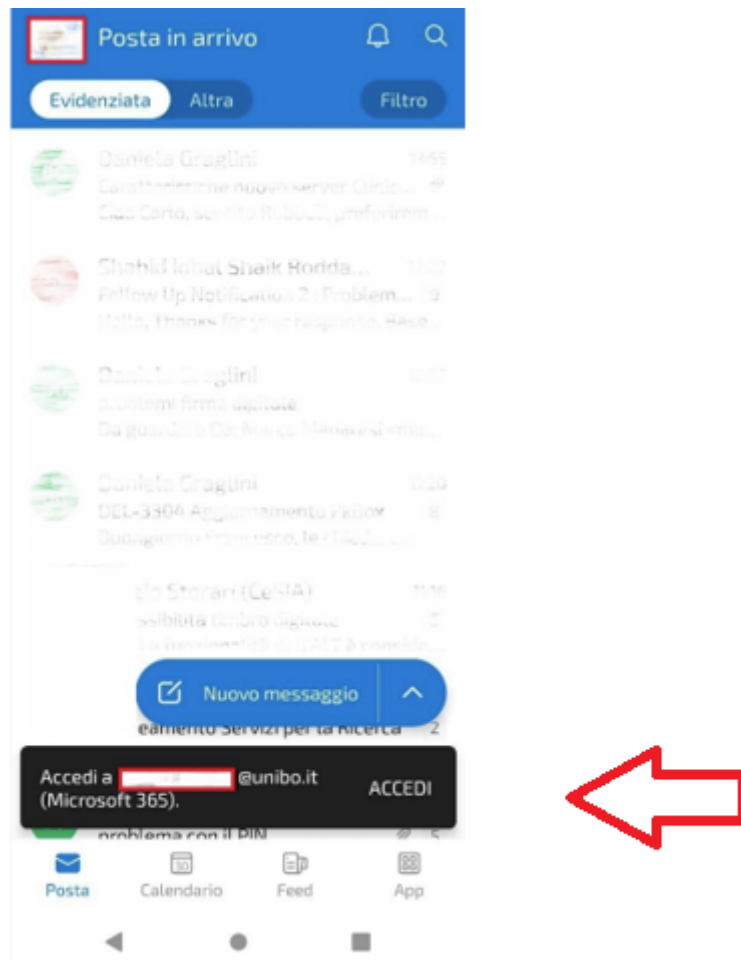
FINISH

Your deactivation request has been completed, and you will receive a confirmation email and SMS from the system.

Activating Outlook as a second factor

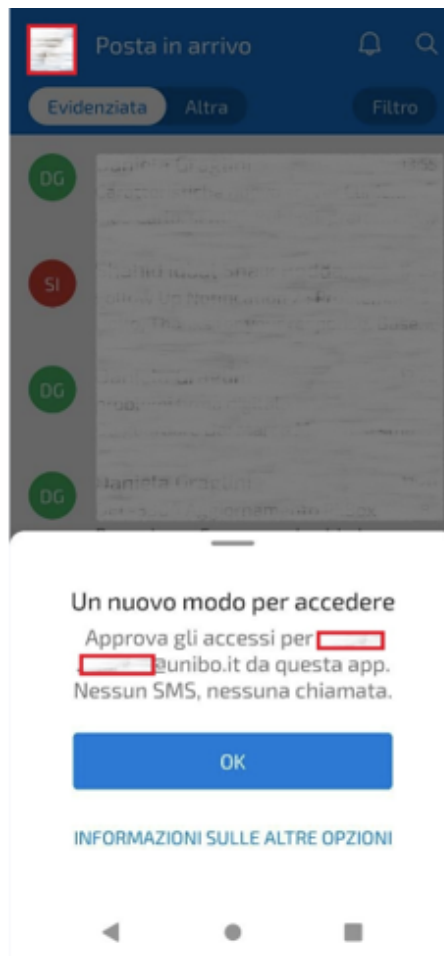
If you have the Outlook Mobile app installed on your phone and your @unibo.it email account is set up, you will be asked to sign in about 30 minutes after submitting the MFA activation request on www.dsa.unibo.it.

Tap **SIGN IN**.



Log in using your username in the format name.surname@unibo.it and your password, then enter the code sent to the phone number you provided during the MFA activation process.

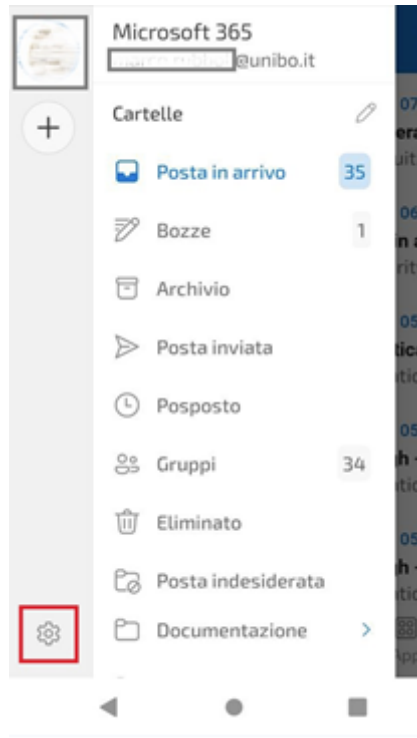
To set Outlook as your second authentication factor, tap **GOT IT**, then **OK** in the two pop-up windows that appear.



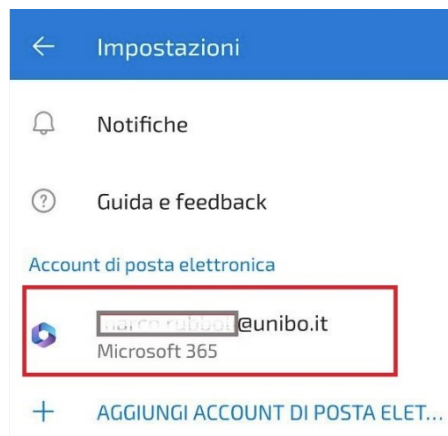
From this moment on, Outlook will be used as your second authentication factor (Authenticator Lite), replacing SMS authentication.

Checking and editing Outlook settings

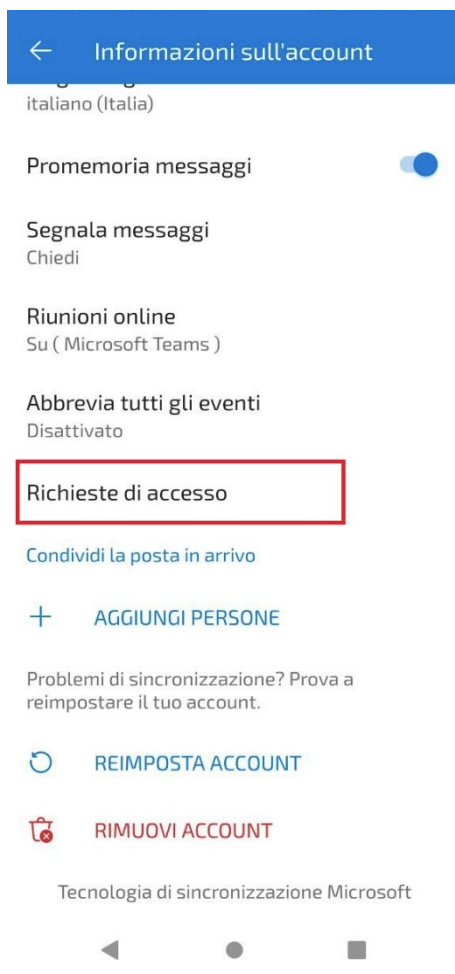
To verify or change your Outlook Mobile settings for MFA, open the **Settings** section by tapping the icon in the bottom left-hand corner.



Tap your email account.



Scroll to the bottom of the page and tap **Sign-in Requests**.



Use the **Allow sign-in requests** switch to enable or disable Outlook Mobile as the second authentication factor.

