

MULTI-FACTOR AUTHENTICATION (MFA) FOR ACCESSING REPLY EMAIL & CORPORATE APPLICATIONS

User Manual

written by:	ICT	approved by:	ICT Security
unit:	ICT	doc ID:	
review:	1.1	issue date:	April 2024 doc. model MDE_GEN_TEC_001 1.2

Privacy notes: *Internal Use*

REPLY

C.so Francia, 110 - 10143 Torino - Italia
tel +39 011 7711594 - fax +39 011 7495416
info@reply.com

www.reply.com



STATE OF THE DOCUMENT

Review	Date	Changes	(Approved by)
1.0	05-2022	MFA for Accessing Reply Email & Corporate Applications – User Manual	ICT Security
1.1	04/2024	Removed obsolete sections (e.g., from the FAQ), inserted info on YubiKeys/WebAuth and reviewed the guide in general	ICT Security
1.2	10/2024	Removed referrals to SMS and removed info on YubiKeys/WebAuth	

CHANGES SUMMARY

Main changes list compared to the previous version:	
---	--

ATTACHMENTS:

- N/A

written by:	ICT	approved by:	ICT Security	review:	1.1
unit:	ICT	issue date:	April 2024	page:	2/22

privacy note: Internal Use



CONTENT

1	INTRODUCTION	4
2	OPERATIVE INSTRUCTIONS	5
2.1	STEP 1 – DOWNLOAD CISCO DUO MOBILE APP	5
2.2	STEP 2 – ENROLL & LOGIN YOUR DEVICE	5
2.2.1	ENROLLMENT	6
2.2.2	LOGIN	16
3	F.A.Q.	19
3.1	DOES CHANGING MY PASSWORD AFFECT MFA ON MY OUTLOOK/TEAMS ACCOUNT?	19
3.2	DO I HAVE TO REINSERT MY CREDENTIALS EVERY TIME I LOG IN TO MY EMAIL, TAMTAMY, ETC.?	21
3.3	WHAT DO I HAVE TO DO, IF I NEED TO SWITCH MY AUTHENTICATION DEVICE?	22

written by:	ICT	approved by:	ICT Security	review:	1.1
unit:	ICT	issue date:	April 2024	page:	3/22

privacy note: *Internal Use*



1 INTRODUCTION

In order to access Reply's corporate services (Email, Tamtamy, Service Desk, VPN, etc.), the usage of Multi-Factor Authentication (MFA) is required as an additional step to providing your username and password.



Configuring the Multi-Factor Authentication (MFA) to connect securely to Reply's services, you only need to follow two basic steps:

- **STEP 1:** Download and install the latest version of the Cisco DUO application on your smartphone (*see section 2.1*)
- **STEP 2:** Log in to one of Reply's email/corporate applications of your choice and perform the first enrollment on DUO

Please make sure to carefully read and follow the operative instructions. If there are any doubts, try to take a look at the F.A.Q. section.

written by:	ICT	approved by:	ICT Security	review:	1.1
unit:	ICT	issue date:	April 2024	page:	4/22

privacy note: *Internal Use*



2 OPERATIVE INSTRUCTIONS

2.1 STEP 1 – DOWNLOAD CISCO DUO MOBILE APP

In order to activate MFA for your account, you have to download and install the Cisco Duo Mobile app on your smartphone.

The app can be downloaded for:

- Android - from the Google Play Store, search for **DUO Mobile** (<https://play.google.com/store/apps/details?id=com.duosecurity.duomobile>)
- iOS - from the App Store, search for **DUO Mobile** (<https://apps.apple.com/it/app/duo-mobile/id422663827>)

If the Cisco Duo App is not appearing in the app store for download, ensure that your mobile device is updated to the most recent version of its operating system. This update is necessary to accommodate the newest version of the app.

2.2 STEP 2 – ENROLL & LOGIN YOUR DEVICE

Enrollment to the MFA solution can be performed using any browser for your first access (both for laptop and mobile) that detects the MFA activation for the first time.

If you have already activated the Cisco DUO MFA on your Reply account (e.g., for accessing the Reply VPN) you can directly go on the Login section, by skipping the Enrollment section.

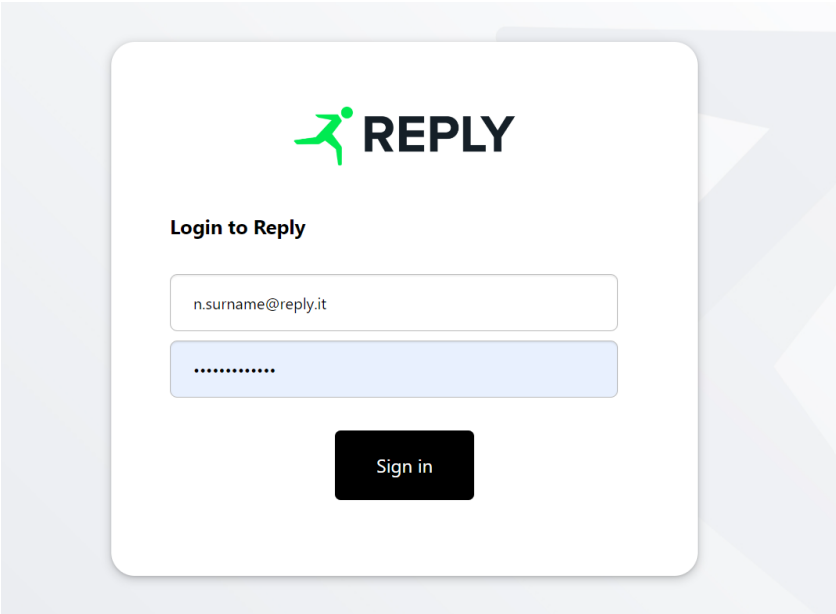
written by:	ICT	approved by:	ICT Security	review:	1.1
unit:	ICT	issue date:	April 2024	page:	5/22

privacy note: *Internal Use*

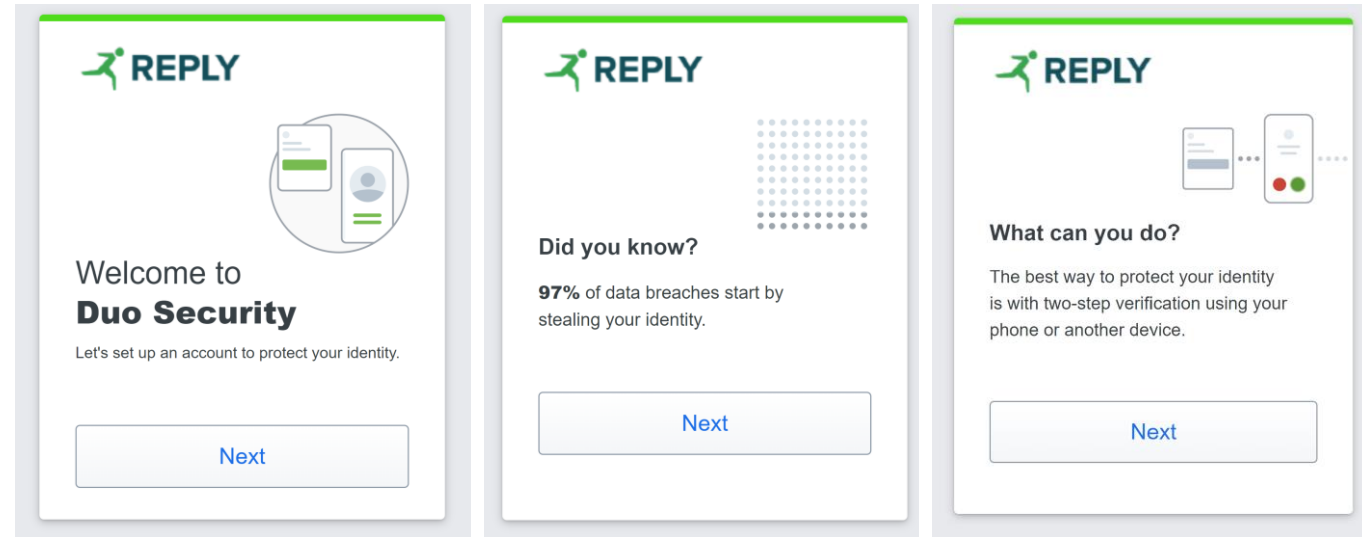


2.2.1 ENROLLMENT

[On your laptop] Open the browser and access the web version of the mail client or a corporate application (e.g., Tamtamy). Insert your Reply credentials when prompted.

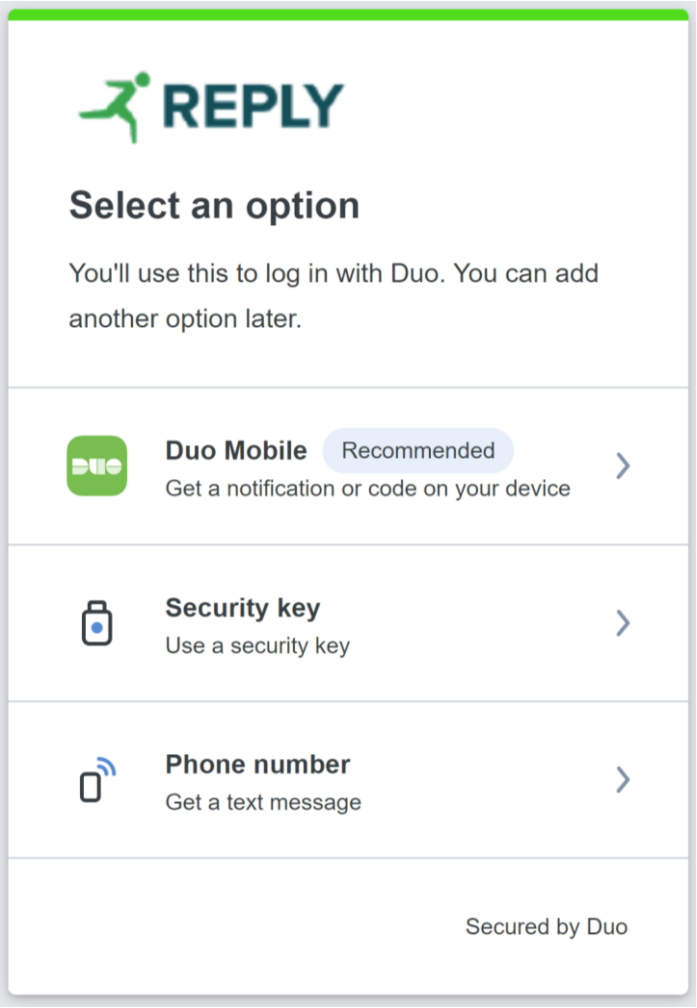


Signing in will cause the following screen to appear. Click on the “Next” button to start the enrollment. You will be presented with several informative screens. You can continue clicking “Next” until you reach the screen that prompts you to select your preferred authentication option.





It is recommended to select the “Duo Mobile” option as your preferred authentication method.





When enrolling your device for the first time, it is not necessary to enter your phone number to associate it with the app. Instead, select the “I have a tablet” option, which does not require you to input a phone number (you can select this if you do not have a corporate phone).

[< Back](#)

Enter your phone number

You'll have the option to log in with Duo Mobile.

Country code

+1 ▾

Phone number

Example: "201-555-5555"

Add phone number

[I have a tablet](#)

Secured by Duo

Now, if you already have the DUO Mobile app installed on your mobile device, you can scroll down and click on “Next” and move forward. Otherwise follow the required steps outlined in chapter 2.1 to install the app on your mobile device and then click on the “Next” button.

[< Back](#)

Now download the Duo app

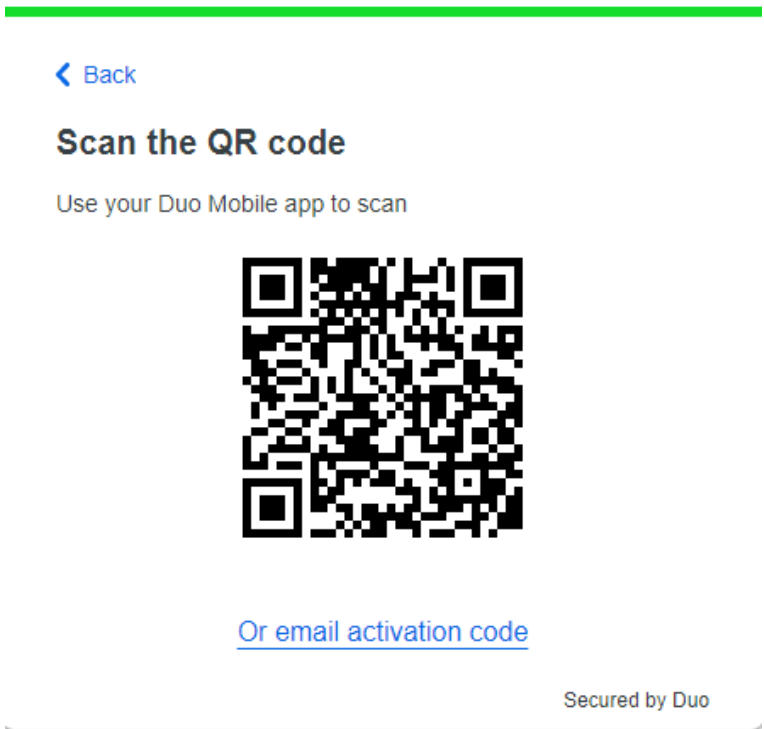
Available on iOS and Android

Next

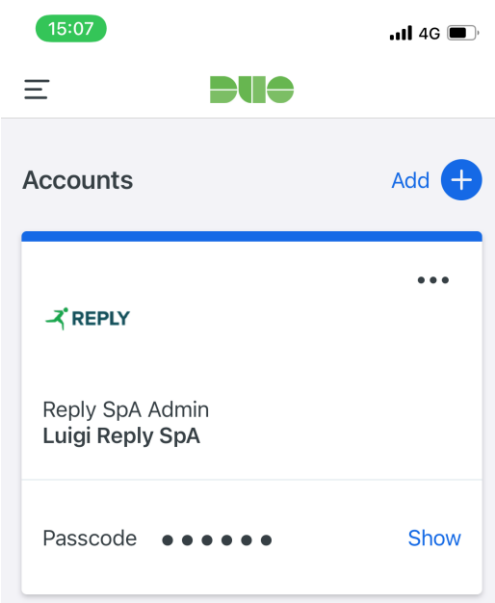
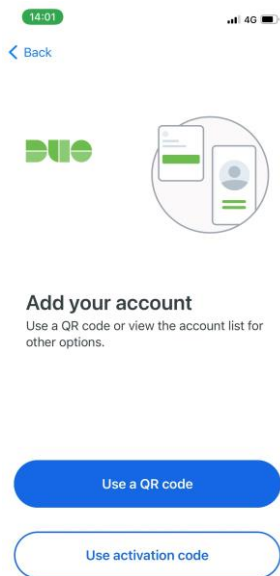
Secured by Duo



Now you will be presented with a QR-Code. The next steps will require you to take out your mobile device (the one on which you have installed the DUO app).



[On your mobile device] Open the Cisco DUO mobile app, click the “Use a QR code” button, if this is your first enrollment on the Cisco DUO app. Otherwise, click the “Add” or “+” button in the upper-right corner to add a new configuration.



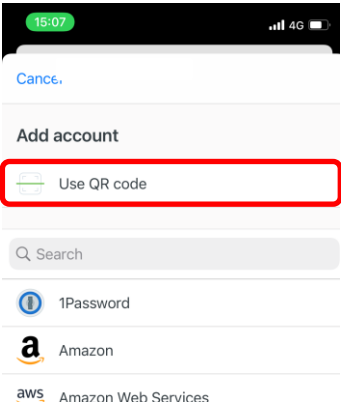
written by:	ICT	approved by:	ICT Security	review:	1.1
unit:	ICT	issue date:	April 2024	page:	9/22

privacy note: Internal Use




[On your mobile device] If you selected the “Add” or “+” button, next choose “**Use QR Code**” to activate the camera. It is located at the very top of the list, above the search bar.

Then, for either case, proceed to scan the QR Code displayed on your laptop.



[On your mobile device] Insert your Reply account name and finalize the configuration.

Name account



Account test

Account name

n.surname

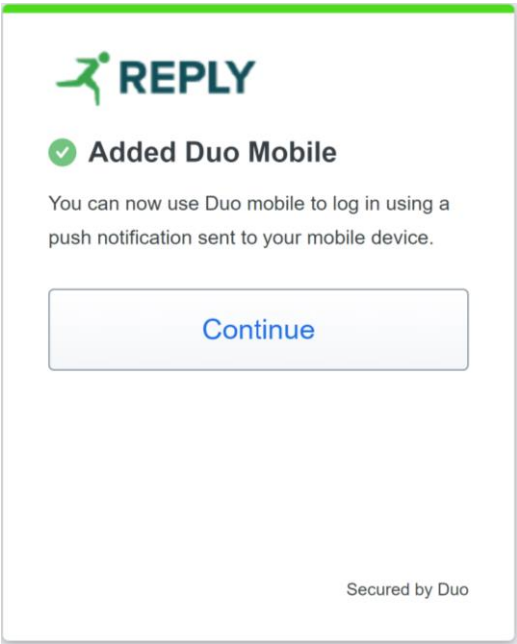
Username or email to be displayed for this account.

written by:	ICT	approved by:	ICT Security	review:	1.1
unit:	ICT	issue date:	April 2024	page:	10/22

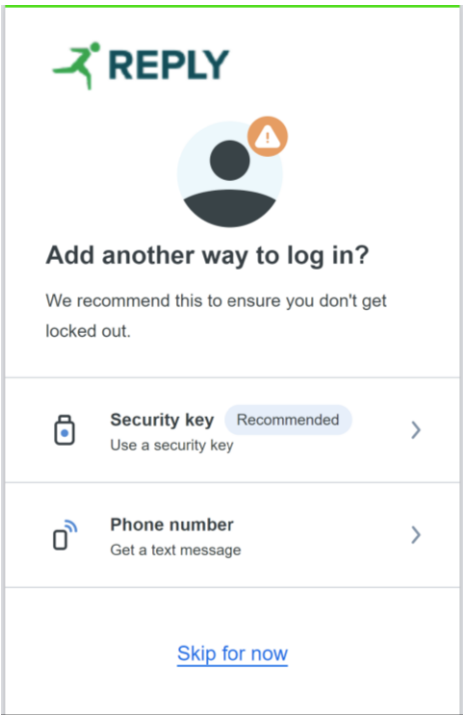
privacy note: Internal Use



[On your web access] Your account has been successfully added to the DUO mobile app, if you see the below screen. Click on the “Continue” button to finalize the process.



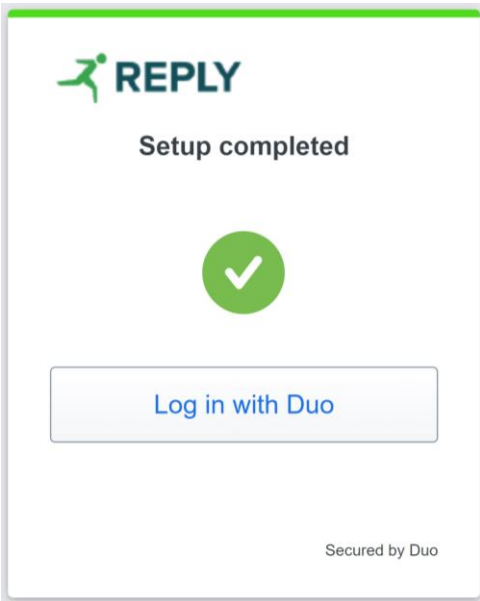
[On your web access] In the screen that appeared, click on “Skip for Now” to conclude the enrollment.



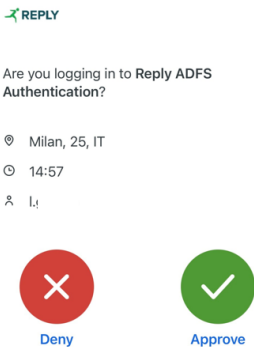
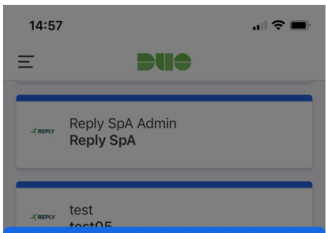
written by:	ICT	approved by:	ICT Security	review:	1.1
unit:	ICT	issue date:	April 2024	page:	11/22
privacy note: <i>Internal Use</i>					



[On your web access] Hang in there, enrollment is almost over! Just click on “Log in with DUO” and accept the push notification on your mobile device to complete the enrollment and login.




[On your mobile device] You will receive a notification on your mobile device via the second authentication method you chose (e.g., a push notification, if you previously selected DUO Mobile, as suggested). After you have approved the sign in **on your mobile device**, you will be able to access the relative Reply service.



written by:	ICT	approved by:	ICT Security	review:	ICT
unit:	ICT	issue date:	April 2024	page:	12/22
privacy note: <i>Internal Use</i>					



On your first access, you will be asked whether you trust the browser you are using. Only click “Approve” if you are using your corporate laptop or a secure workstation (i.e., not if you are using a personal or public device). If you click on “Yes, trust browser”, logging in to Reply’s corporate services on the same browser will let you skip the MFA authentication for the next 7 days!

 **REPLY**

Trust this browser?

You won't need to log in as often from this browser.

Yes, trust browser

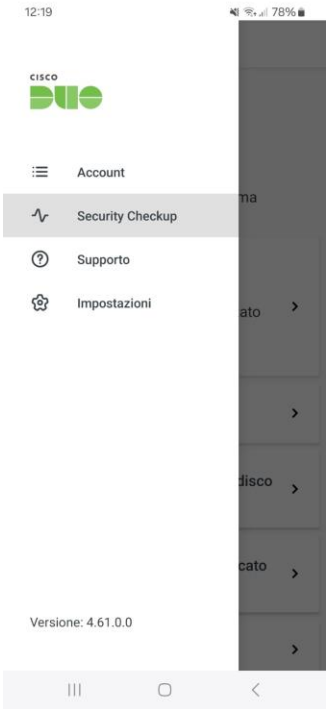
[No, do not trust browser](#)

Do you still need help? [Open a Ticket!](#)



IMPORTANT SECURITY CHECK

Finally, please regularly check that your smartphone is properly configured. This can be done by clicking on the icon in the top-left corner (three parallel vertical lines) and selecting the “Security Checkup” item.

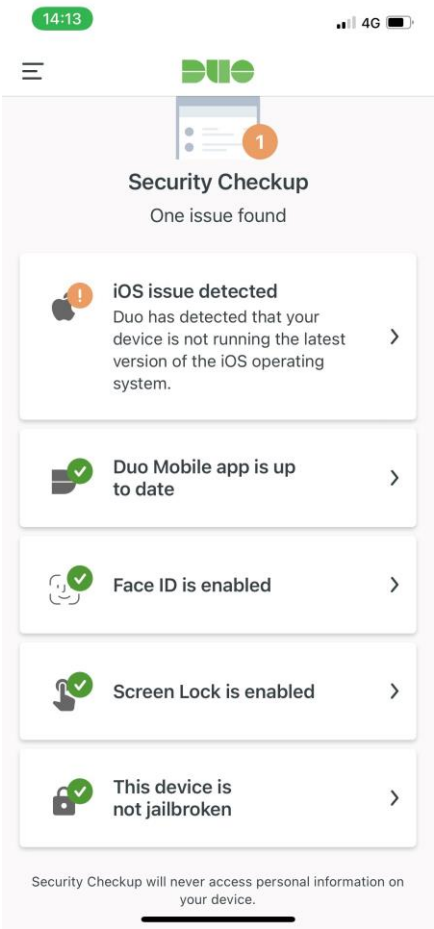


written by:	ICT	approved by:	ICT Security	review:	1.1
unit:	ICT	issue date:	April 2024	page:	14/22

privacy note: *Internal Use*



On this screen you will be able to see any relevant security weaknesses detected on your mobile device. If any issues were detected, please follow the present instructions to improve your device's (and app's) security.



Congratulations!

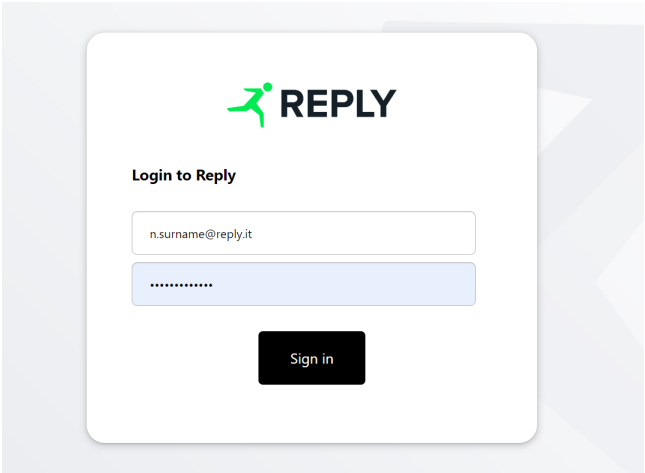
You have completed setting up the MFA.

written by:	ICT	approved by:	ICT Security	review:	1.1
unit:	ICT	issue date:	April 2024	page:	15/22
privacy note: <i>Internal Use</i>					

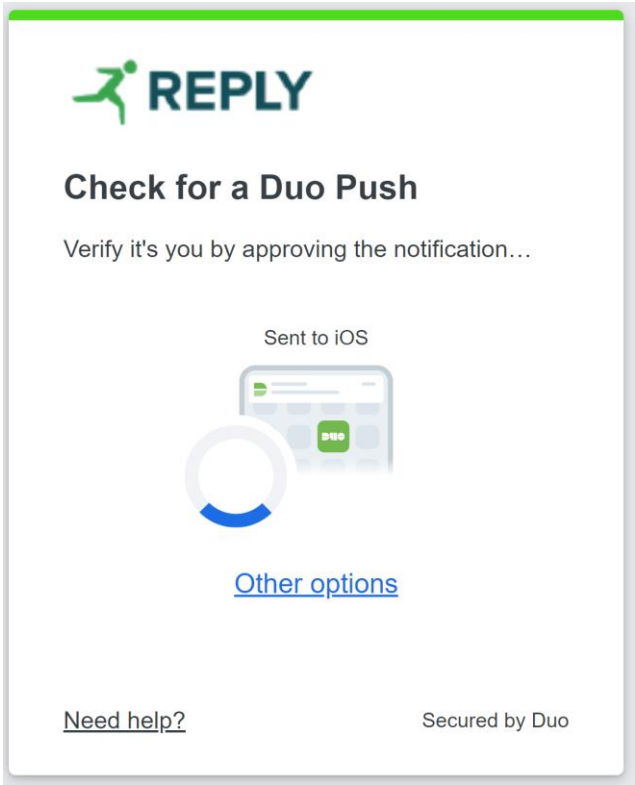


2.2.2 LOGIN

After having enrolled your device, you can log in on the web version of the mail client or a corporate application (e.g., Tamtamy). As usual, you will be asked to input your username and password.



Then, you will see the prompt related to the second authentication factor.

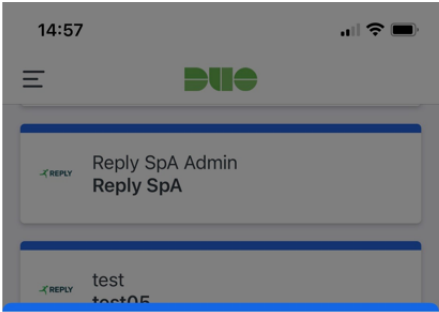


written by:	ICT	approved by:	ICT Security	review:	1.1
unit:	ICT	issue date:	April 2024	page:	16/22

privacy note: *Internal Use*



Following this, you will receive a notification on your mobile device, depending on the authentication method you chose (e.g., push notification). After approving the notification on the DUO app **on your mobile device**, you will be able to access the relative Reply service (e.g., mail or corporate application).



Are you logging in to Reply ADFS
Authentication?

Milan, 25, IT

14:57

l.i



Deny




Approve

written by:	ICT	approved by:	ICT Security	review:	1.1
unit:	ICT	issue date:	April 2024	page:	17/22

privacy note: Internal Use



Upon your first access (or after 7 days have passed since you last approved via MFA), you will be asked whether the used browser can be trusted. Only click “Approve” if you are using your corporate laptop or a secure workstation (i.e., not if you are using a personal or public device). If you click on “Yes, trust browser”, logging in to Reply’s corporate services on the same browser will let you skip the MFA authentication for the next 7 days!

 **REPLY**

Trust this browser?

You won't need to log in as often from this browser.

Yes, trust browser

[No, do not trust browser](#)

Any doubts left? Let us know by [Opening a Ticket!](#)

written by:	ICT	approved by:	ICT Security	review:	1.1
unit:	ICT	issue date:	April 2024	page:	18/22

privacy note: *Internal Use*



3 F.A.Q.

This section will provide answers to some of the most common questions related to enforcing MFA on Reply's email client or other corporate systems.

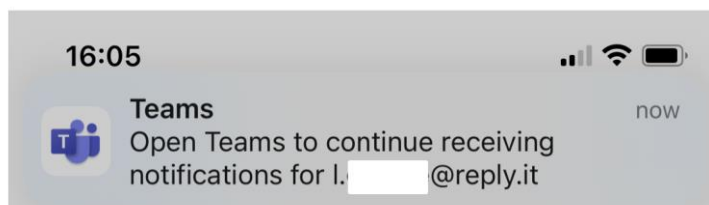
3.1 DOES CHANGING MY PASSWORD AFFECT MFA ON MY OUTLOOK/TEAMS ACCOUNT?

Since Outlook/Teams is linked to your Reply account, MFA will apply when logging in to either of them for the first time as well. This is especially relevant after you have changed your password, as this will cause you to receive a prompt from your client to reinsert your Reply credentials and subsequently to approve the MFA request using the DUO app.

Keep in mind that it is possible that it might take a while for this request to come through, meaning that it might not arrive immediately after you have changed your password (it might even take up to about half an hour) due to the account configuration synchronization needing some time.

Below please find some examples of such a request prompt from different clients:

Microsoft Teams

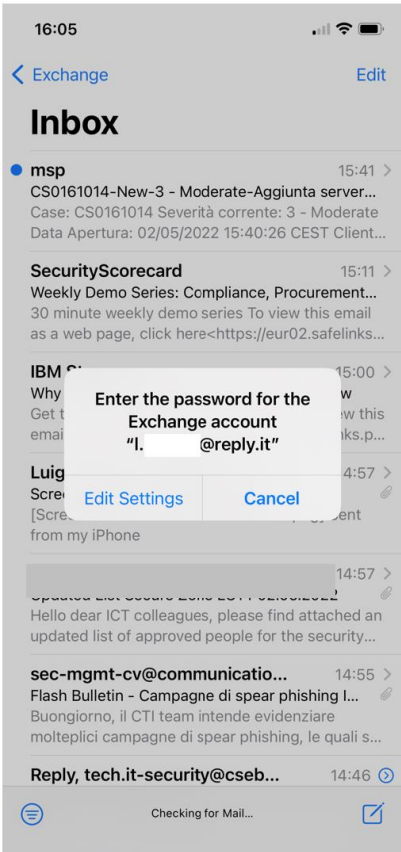


written by:	ICT	approved by:	ICT Security	review:	1.1
unit:	ICT	issue date:	April 2024	page:	19/22

privacy note: *Internal Use*



IOS email client



Just re-insert your Reply credentials on the new page that gets displayed and then approve the MFA request using your DUO app.

16:06

◀ Mail

Cancel

sts3.reply.eu

AA

↺

Login to Reply

l. @reply.it

Password

Sign in

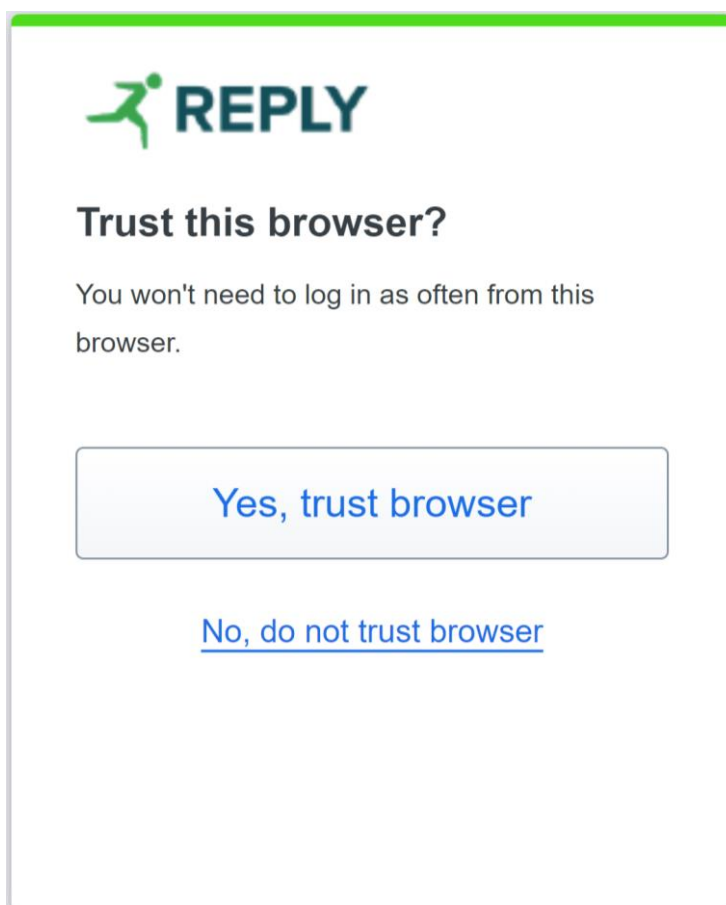


After having thus updated your credentials, no further action should be required from you until your next password change, as MFA approval on the client lasts for 90 days.

3.2 DO I HAVE TO REINSERT MY CREDENTIALS EVERY TIME I LOG IN TO MY EMAIL, TAMTAMY, ETC.?

No, after you have logged in for the first time that day and approved the related MFA request, you will not be required to reinsert your Reply credentials during your next access on other web corporate services or approve any more MFA requests.

Furthermore, you can save your “MFA access” on your browser for 7 days, by clicking on the “Yes, trust Browser” button when approving the MFA request on your browser.



This way, you will not be required to perform MFA when logging in to Reply's web services for the next 7 days!

written by:	ICT	approved by:	ICT Security	review:	1.1
unit:	ICT	issue date:	April 2024	page:	21/22

privacy note: *Internal Use*



3.3 WHAT DO I HAVE TO DO, IF I NEED TO SWITCH MY AUTHENTICATION DEVICE?

Please find a dedicated guide for this topic on Service Desk under the section titled "MFA: Switching/Adding Devices".

written by:	ICT	approved by:	ICT Security	review:	1.1
unit:	ICT	issue date:	April 2024	page:	22/22

privacy note: *Internal Use*