



User Guide – M7 2FA

Two-Factor Authentication (2FA)

1 User summary

Contents

1	User summary.....	3
2	How do I log in with the 2FA?	4
3	How to enable 2FA in 6.15 and get a user QR Code/TOTP Key?	5
4	if I lose it?	7
5	How to get a new TOTP Key or QR code FAQ.....	9
6	Glossary.....	12

1 User summary

In compliance with the industry security standards, **the Two-Factor Authentication (2FA)**, will be introduced ^{to} **add one layer of security to your user account:**

- optional with M7 6.15,
- **mandatory as of M7 6.16.**

This ***Time-based One-Time Password*** (TOTP) 2FA consists in asking users to **provide when logging in:**

1. **their usual username (CX...) and password** (today's M7 6.14 situation),
 - this password can be considered as "static" (if we exclude its potential automatic expiry every 90 days, please see the FAQ section for more details).
2. **a NEW 6-digits "authentication code"**, time-based,
 - meaning it **will change every 30 seconds**,
 - and will be given by an **Authenticator App** on your smartphone or for API automated applications calculated by an **algorithm** (the public "TOTP" algorithm).

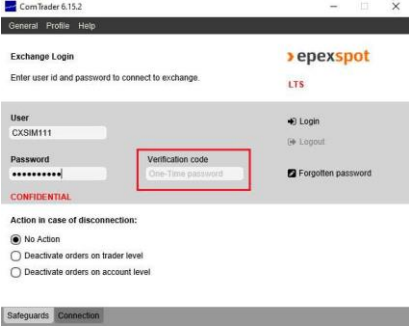


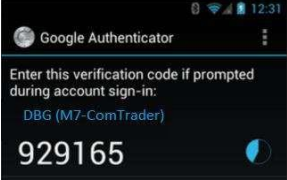
This guide describes the 2FA principles and the related procedures you need to follow to be able to:

- enable this 2FA for each desired user (since optional with M7 6.15),
- generate the required elements (*QR code* for smartphone and *TOTP Key* for automated API apps) for you to generate this new *Authentication Code* that will change every 30 seconds and be able to log in with your user:
 - in ComTrader;
 - in the WebGUI with a report user;
 - in the M7 API.
- re-generate them in needed, for instance if lost.

The last FAQ section covers related M7 topics (*Password Policy, API certificates*) **and specific 2FA questions** (e.g.

What is the validity of my QR code or TOTP Key?, Which application or API library should I use to generate TOTP codes?, etc.).

2 How do I log in with 2FA?

User Type	New Login Interface	How to get this new code?
<p>ComTrader users</p>		<ol style="list-style-type: none"> Download a TOTP Authentication app on your smartphone (e.g. Google Authenticator, Microsoft Auth)  <ol style="list-style-type: none"> Enable TOTP in ComTrader 6.15 Scan the ComTrader QR Code with your app <p>→ 4. The app will generate a TOTP Verification Code, changing every 30 seconds.</p>
<p>Report users</p> <p>(XML reports; TC540, TC810, etc.)</p>		 <p>users: below the</p> <p>For report please check</p>
<p>API users</p>	<p>Login Request with a new authVerificationCode attribute. AMQP connections are not affected.</p> <p>Example for an API user for which TOTP has been enabled in ComTrader 6.15:</p> <pre><LoginReq xmlns="http://www.deutsche-boerse.com/m7/v6" user="CXSIMXXX" force="true" disconnectAction="NO" authVerificationCode="84498"></pre> <p>Manual API apps with a GUI showing a Login panel can</p>	<p>Automated API apps will have to implement the public TOTP algorithm (or use public libraries).</p> <p>ComTrader will give you a TOTP Key (see below), required as an input of the TOTP algo to generate this new 6-digit verification code in real time.</p>

mimic the ComTrader login panel (users can then

follow the ComTrader process above, while the app sends


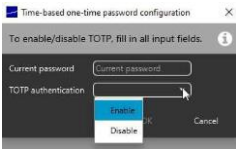
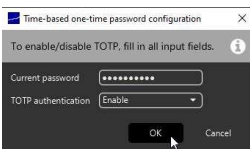


the enriched Login Request with the new code).

Optional in 6.15, mandatory in 6.16.

3 How to enable 2FA in 6.15 and get a user QR Code/TOTP Key?

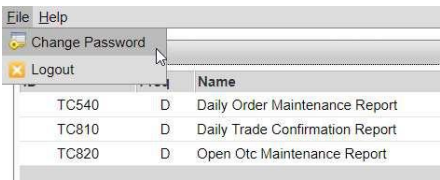
Once M7 6.15 is delivered, 2FA is by default disabled for all users.

Though still optional in 6.15, we encourage you to activate it by following the below procedure.

User Type	How do I activate/enable 2FA for my user in ASIM? (or later in PROD)
<p>ComTrader and API users</p>	<ul style="list-style-type: none"> Once logged in ComTrader, go to the menu >Profile>TOTP Password:  A new panel pops-up: <ul style="list-style-type: none"> select "Enable" after having input your current user password (the one you used to log in), and click on "OK":   After having clicked on "OK", ComTrader displays: <ul style="list-style-type: none"> A secret "TOTP Key" = C3L6YOITYKQH4PHX6GKK3OD4TAI6H3EN (to be copied for a later use by API apps for this user), a QR Code (that contains this TOTP Key).  If using ComTrader, or a manual API app with a GUI user: <ul style="list-style-type: none"> scan this QR code with your phone authenticator app: it will generate a new 6-digit code every 30 seconds.  If using an automated API app: <ul style="list-style-type: none"> store the TOTP key string for a later usage by your API app. This will be one input of the TOTP algo, the 2nd being the current timestamp. Note: This TOTP Key works exclusively for this very user.

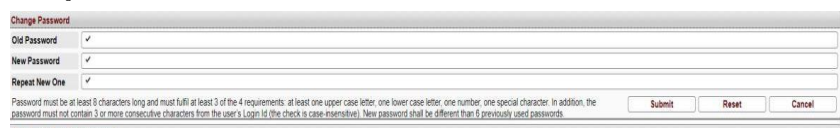
TC report users

For Report user, log in the Web GUI, and select the >File>Change password menu:



	Name	Report Name
TC540	D	Daily Order Maintenance Report
TC810	D	Daily Trade Confirmation Report
TC820	D	Open Otc Maintenance Report

- This leads you to a page that in its lower part gives you the possibility to **Enable the 2FA** for the logged in report user:
 - Input your user current password
 - Click on *Enable*



Change Password

Old Password ✓

New Password ✓

Repeat New One ✓

Submit Reset Cancel

Time-Based One-Time password


Current status: Disabled

Password: [REDACTED]

For any operation affecting TOTP, you need to enter your normal password. Please save the generated key, it will only be displayed once.

Enable Regenerate key Disable

- **A new TOTP Key gets generated.**
- The page gives you as well the possibility to **generate a new QR code:**



Time-Based One-Time password

Current status: Enabled

Password: ✓

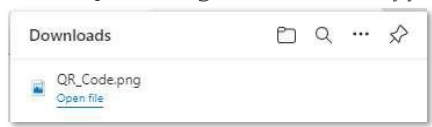
For any operation affecting TOTP, you need to enter your normal password. Please save the generated key, it will only be displayed once.

TOTP Key: 3C1V7OP8BDUJ2A0HEJIP3PF0BEYCUA

QR code

Enable Regenerate key Disable

- If you click on "QR code" a **new QR code image file** is downloaded by your browser:



Downloads

QR_Code.png

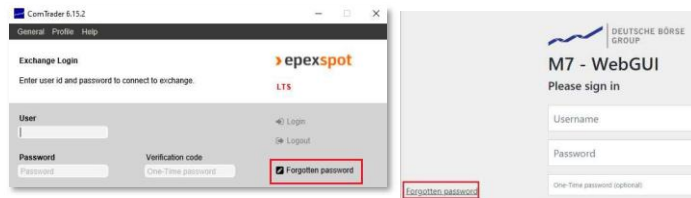
Open file

- **Then please use the TOTP key or scan the QR code as explained above**, depending on how you connect retrieve your TC reports (manual GUI log in versus automated app).

The below **Forgotten Password procedure** is applicable for all users : ComTrader, Report users and API users.

By the TOTP security standard, the secret “TOTP key” is:

- Personal: unique for each User
- only retrievable by the intended user when enabling 2 FA.
 - Neither EPEX/DBAG nor the user will be able to retrieve it afterwards in case the TOTP Key or QR code has not been not noted down or was lost / forgotten)
 - The “forgotten password” procedure will need to be followed
- **Launch ComTrader (for ComTrader or API users), OR open the Web GUI (for report users) and click on the “Forgotten password” link (without filling anything):**



- The “Forgotten password webGUI” now contains a new option to **request a new TOTP Key/QR Code:**



- When clicking on “Request Password Reset”, M7 sends to the e-mail address a link, valid for 1 hour. Clicking on it leads you to a new page where you can **regenerate your user TOTP Key** :
 - Enter your current user password
 - Click on “Regenerate key”



- **A new TOTP Key gets generated.** The page gives you as well the possibility to generate a new QR code:



- If you click on “QR code” a **new QR code image file** is downloaded by your browser:

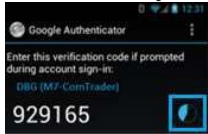
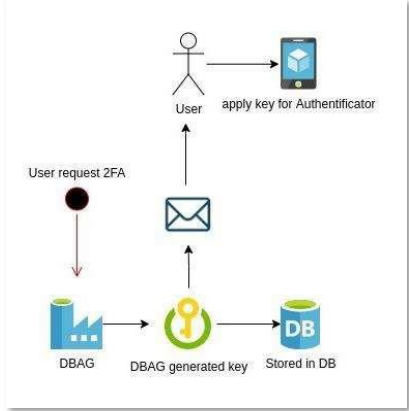


Note for the testing period in ASIM:
please make sure that your email is registered in ASIM for your tested user so you can receive the required link :
 do not hesitate to contact our Market Operation team at powerspot@epexspot.com to adjust your user setup if required, so you can receive all emails sent by M7.



5 FAQ

QUESTION	ANSWER
<ul style="list-style-type: none"> • How does this 2FA fit with the password policy, currently deactivated in PROD? 	<ul style="list-style-type: none"> • This 2FA security policy will not replace the password policy (constraints on new password + automatic expiration after 90 days). • This policy is now deactivated in production and will be reactivated in Q2 2023. A further communication will follow.
<ul style="list-style-type: none"> • Will API certificates still be required once 2FA is mandatory with M7 6.16? 	<ul style="list-style-type: none"> • Yes, API certificates per API application will still be required.
<ul style="list-style-type: none"> • What is the difference between these codes: between a TOTP Key (or a QR code) and a TOTP verification code? 	<ul style="list-style-type: none"> • The TOTP Key or the QR code must be requested only once (though then can be generated again if lost). • They are used to generate a real time TOTP code, required when logging in, on top of your usual user/password. • Manual users who need to type their TOTP code when logging in will use an authenticator app: they will scan once the QR Code and then only use the app. <ul style="list-style-type: none"> ○ QR code -> scan it once -> then use the app to get your TOTP code to log in • Automated API apps will be fed with the TOTP key, so they can use it as a TOTP algo input, combined with the current timestamp. <ul style="list-style-type: none"> ○ TOTP Code = function (TOTP secret key, current time)
<ul style="list-style-type: none"> • Which application or API library should I use to generate TOTP codes? 	<ul style="list-style-type: none"> • The TOTP code can be generated using the known and public TOTP algorithm. • For app with a manual log in panel, either one of the industry-standard authentication applications (authenticators like <i>Google Authenticator</i>, <i>Microsoft Auth</i>) can be used. • For automated API apps: customers can implement their own algorithm based on the TOTP "norm", or use public libraries.
<ul style="list-style-type: none"> • With M7 6.15, can I enable 2FA for all my users at once? 	<ul style="list-style-type: none"> • No, the activation (enabling 2FA) is personal, and thus must be done user per user. • No mass activation is possible with M7 6.15.
<ul style="list-style-type: none"> • What is the validity of the TOTP Key and the QR code? 	<ul style="list-style-type: none"> • Neither the TOTP Key nor the QR Code (which contains as well the TOTP Key) expires automatically. • They become invalid only if you generate a new one.
<ul style="list-style-type: none"> • What is the validity of each TOTP verification code? 	<ul style="list-style-type: none"> • The validity of the 6-digit code generated by the Authenticator (i.e. length of the window in which the code, in combination with the correct User Password and User Name is accepted by M7) is valid for a maximum of 30 seconds. • Once logged in, the User will not be asked anymore to provide the TOTP code. This is also valid for API connections – if the

<p>5 FAQ</p>	<p>connection drops and the User is considered disconnected, then a new login with a TOTP code is required.</p>
<ul style="list-style-type: none"> With M7 6.14, my user becomes invalid/revoked when I enter a wrong password 5 times in a row. Is this rule affected by 2FA? 	<ul style="list-style-type: none"> With M7 6.15, wrong 2FA TOTP verification codes are not counted as part of these 5 trials. As of M6.16, 2FA each wrong verification codes is counted.
<ul style="list-style-type: none"> If I experience an AMQP disconnection, or if I am logged out, do I need to enter again a TOTP code when I re-log in? 	<ul style="list-style-type: none"> Yes, each time a new login is required, a new TOTP code must be input. This code changes every 30 seconds : if you log in twice during the same 30 second interval during which a code is valid, then the code works again for your 2nd login. Your authenticator app will display code changes on your phone screen and usually gives a rough indication of the remaining number of seconds (framed in blue below): you see when the TOTP code is about to expire:  <ul style="list-style-type: none"> Reminder: in case an API app experiences an AMQP disconnection without having been able to send a Logout Request, M7 detects this loss within the next 20 to 40 seconds and logs your user out for "INACTIVITY" : please refer to the M7 API FAQ for more details.
<ul style="list-style-type: none"> How does it work on M7 side? 	<ul style="list-style-type: none"> M7 stores the generated TOTP Key in its database:  <ul style="list-style-type: none"> When a user logs in with its user/password and the new TOTP verification code, M7 generates as well a TOTP code (based on the same TOTP Key and its current timestamp) and

	<p>compares it with the one provided : if they match, the user is authenticated and gets logged in:</p> <pre> graph LR A[Login page User name & password auth +2FA] --> B[LDAP verification 2FA generation and verification base on key from DB] B -- valid match --> C[Permit user to login] </pre>
<ul style="list-style-type: none"> • Is it possible that my TOTP code gets refused while correct at the moment it was generated? 	<ul style="list-style-type: none"> • Indeed, the TOTP algorithm divides the time elapsed since 00:00:00 UTC on 1 January 1970 into 30 seconds interval. • If your app generates a TOTP code at the very end of a 30 seconds interval, it can have become obsolete by the time your Login Request reaches M7 and M7 generates its own code (using the next 30 seconds interval): the two codes do not match and you cannot log in. • As a result, your API app must be ready to try to relog in with a new TOTP code.

6 Glossary

Term	Description
2FA	Two-Factor Authentication. Also referred to as multi-factor authentication. Instead of just using a password, one other mean of user authentication is required to add another layer of security, in order to prevent unauthorized users from gaining access to a user account with nothing more than a stolen password.
TOTP	Time-based One-Time Password. Sometimes referred to as "OTP". "Time-based" means that the password is valid for a short time (in our case 30 seconds), when usual user passwords can be considered as "static" (though they have their own life cycle with a potential
TOTP Algorithm	Public cryptographic algorithm that generates a one-time password (OTP): <ul style="list-style-type: none"> • that uses the current time as a source of uniqueness in combination with a static secret key,
TOTP Key	Or "OTP Key" or "Secret Key". <ul style="list-style-type: none"> • used as a standard in many industries 2FA systems.
TOTP Verification Code	The static "secret" key given by ComTrader/webGUI, required to be able to generate a TOTP Or "OTP Verification Code" Or "TOTP code" Or "TOTP authentication code" Or "2nc password" verification code.
Code	The new code changing every 30 seconds, that users need to be able to log in M7, on top of their usual user/password combination, when 2FA is enabled for this user.

This code is a function of a secret Key and current time.

TOTP Code = function (TOTP secret key, current time)