Dual Factor Authentication Manual

eSupplierConnect

Version 1.0

April 4th, 2022

Table of contents:

1 Introduction

This document is the **Dual Factor Authentication User Manual** and provides all the required information to configure and use the Two-Step verification on the eSupplierConnect Portal.

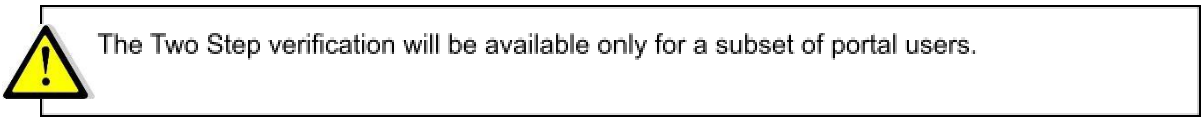
The next paragraphs will explain:

1) How the Dual Factor Authentication has been implemented in the eSupplierConnect Portal

2) How to install the Authenticator that is used to generate the verification codes for the login after the Two-Step verification has been activated

3) How to setup the Two-Step verification

4) How to login to the system after the activation of the Two Step verification



⚠ The Two Step verification will be available only for a subset of portal users.

2 Dual Factor Authentication

To enforce the authentication for the eSupplierConnect portal has been implemented the Time-Based Two-Step verification (following referenced as TOTP). After the activation the login to the portal will use the following authentication methods:

- User ID and Password (**currently used**)
- TOTP managed through an authenticator (**the new implementation described in the present manual**)

The solution implemented will be scalable allowing the management of different combinations of applications and functional roles.

The advantage of the implementation of a Two-Step verification using the TOTP is that no server-to-server connection is required, TOTP requires that the system that generates the code and the one that receives it both use a shared key and have their clocks synchronized. Once this is done, they each calculate a matched pair of one-time codes that are valid for the duration of the set time-period before they expire. The user is then asked to type the code from their authenticator app into the system they are attempting to log into. The system compares this code to the one it’s generated and if they match the user is allowed to proceed.

2.1 Who should use the Two-step verification for the eSupplierConnect portal?

The supplier portal users enrolled for the Two-step verification for the eSupplierConnect portal are the users having MyDocs application with authority to manage the financial bank details.

2.2 *Configuration of the portal to manage the Two-step verification*

The portal will be configured to manage two different states of implementation of the Two-step verification:

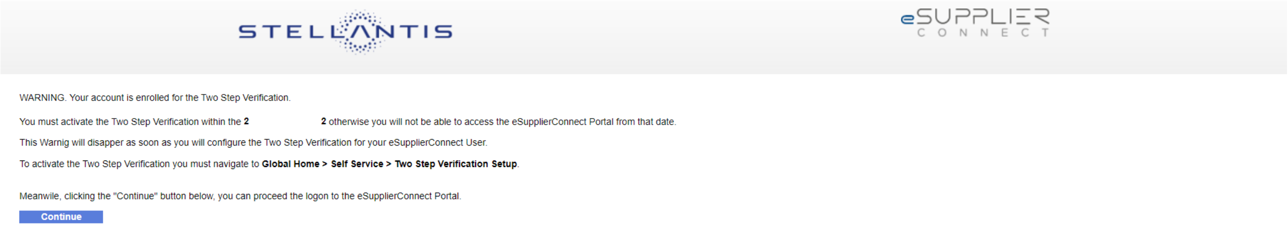
1. Grace Period

2. Active

2.2.1 Grace Period state

During the **Grace Period** state, the Two-step verification is configured and active but a user, that is enrolled to the Two-step verification, can proceed to the portal home page even if the Two-step verification has not been configured. A warning message, that must be acknowledge before proceeding, will be displayed until the user will complete the Two-step verification setup. All the users that are not enrolled for the Two-step verification can access the portal and will not display any warning message before the portal Homepage.

The image shows an example of the message displayed after the login into the eSupplierConnect portal when the Two-step verification is configured in Garce Period state.



WARNING. Your account is enrolled for the Two Step Verification.

You must activate the Two Step Verification within the **2** **2** otherwise you will not be able to access the eSupplierConnect Portal from that date.

This Warnig will disapper as soon as you will configure the Two Step Verification for your eSupplierConnect User.

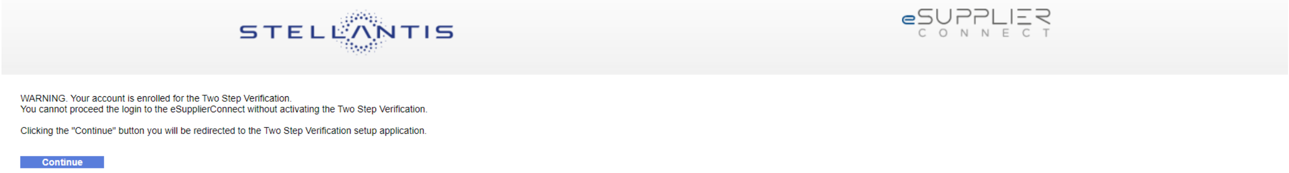
To activate the Two Step Verification you must navigate to **Global Home > Self Service > Two Step Verification Setup**.

Meanwile, clicking the "Continue" button below, you can proceed the logon to the eSupplierConnect Portal.

2.2.2 Active state

During the **Active** state, the Two-step verification is active and the user that is enrolled to the Two-step verification cannot proceed if the Two-step verification has not been configured. A message will be displayed, and the user, **acknowledging the message, will be redirected to the Two-step verification setup application**. All the users that are not enrolled for the Two-step verification can access the portal and will not display any message before the portal Homepage.

The image below shows an example of the message displayed after the login into the eSupplierConnect portal when the Two-step verification is configured in Active state.



WARNING. Your account is enrolled for the Two Step Verification.
You cannot proceed the login to the eSupplierConnect without activating the Two Step Verification.

Clicking the "Continue" button you will be redirected to the Two Step Verification setup application.

When the Two-step verification is in active state, a user enrolled for the Two-step verification, cannot access the eSupplierConnect authenticated Homepage until the completion of the setup and a subsequent logoff/login action.

3 Two-step verification configuration

The configuration and the activation of the Two-step verification for a user of the eSupplirConnect portal consists of the following steps

1. Installation of the authenticator (if not already present on the device chosen for the verification)
2. Setup of the Two Step Verification
3. Logout from the portal
4. Login into the Portal

3.1 Install the authenticator

The first step to setup the Two Step Verification for the esupplierConnect Portal is to install the Authenticator that is the application that will generate the code for the login verification. Ensure you choose a device that you will have access to the next time you need to log into eSupplierConnect Portal.

It is possible to choose between three possible authenticator that have been tested with the eSupplierConnect portal

A. For IOS and Android Mobile devices
   1. Google Authenticator
   2. Microsoft Authenticator

B. For Chrome Browser
   1. Authenticator extension by authenticator.cc

3.1.1 Install the Google Authenticator

The Google Authenticator app helps you sign into your accounts when you're using two-step verification. Two-step verification helps you to use your accounts more securely because passwords can be forgotten, stolen, or compromised. Two-step verification uses a second factor like your phone to make it harder for other people to break into your account.

In the following chapters you will find the instructions to install the Google Authenticator on IOS or Android devices.

3.1.1.1 IOS

If you have not already installed the Google authenticator on your IOS device, follow the steps below:

1. Tap the App Store icon on your device and tap to open
2. Using the search function simply type in 'Google Authenticator' and tap the search icon
3. The Google Authenticator app will display
4. Verify that the publisher is “**Google LLC**”
5. If the app is not already on your phone the button will read 'FREE' and you can tap on it
6. You will be prompted to enter your Apple ID or touch the home button if you have Touch ID, or double click the power button if you have the Face ID.

7. Once you have entered your Apple ID correctly or used the Touch ID or the Face ID, the app will start to install on your device

8. You now have the Google Authenticator app on your iOS device, and you can activate your code

3.1.1.2 Android

If you have not already installed the Google authenticator on your Android device, follow the steps below:

3. Find the Google Play icon on your device and tap to open

4. Using the search function simply type in 'Google Authenticator' and tap the search icon

5. The Google Authenticator app will display

6. Verify that the publisher is “Google LLC”

7. Tap on the app icon and then the 'install' button.

8. You now have the Google Authenticator app on your Android device, and you can activate your code

3.1.2 Install the Microsoft Authenticator

The Microsoft Authenticator app helps you sign into your accounts when you're using two-step verification. Two-step verification helps you to use your accounts more securely because passwords can be forgotten, stolen, or compromised. Two-step verification uses a second factor like your phone to make it harder for other people to break into your account.
In the following chapters you will find the instructions to install the Microsoft Authenticator on IOS or Android devices.

3.1.2.1 IOS

If you have not already installed the Microsoft Authenticator on your IOS device, follow the steps below:

1. Tap the App Store icon on your device and tap to open

2. Using the search function simply type in 'Microsoft Authenticator' and tap the search icon

3. The Microsoft Authenticator app will display

4. Verify that the publisher is “**Microsoft Corporation**”

5. If the app is not already on your phone the button will read 'FREE' and you can tap on it

6. You will be prompted to enter your Apple ID or touch the home button if you have Touch ID, or double click the power button if you have the Face ID.

7. Once you have entered your Apple ID correctly or used the Touch ID or the Face ID, the app will start to install on your device

8. You now have the 'Microsoft Authenticator app on your iOS device, and you can activate your code

3.1.2.2 Android

If you have not already installed the Microsoft Authenticator on your Android device, follow the steps below:

1. Find the Google Play icon on your device and tap to open

2. Using the search function simply type in 'Microsoft Authenticator' and tap the search icon
3. The Microsoft Authenticator app will display
4. Verify that the publisher is “**Microsoft Corporation**”
5. Tap on the app icon and then the 'install' button.
6. You now have the Microsoft Authenticator app on your Android device, and you can activate your code

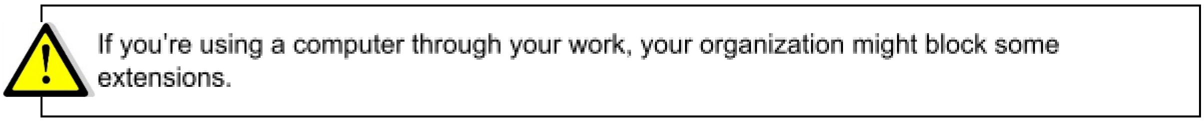
3.1.3 Install the Authenticator extension

The Authenticator extension helps you sign into your accounts when you're using two-step verification. Two-step verification helps you to use your accounts more securely because passwords can be forgotten, stolen, or compromised. Two-step verification uses a second factor like your phone to make it harder for other people to break into your account.
In the following chapters you will find the instructions to install the Authenticator extensions on your browsers.

3.1.3.1 Chrome Browser

If you have not already installed the Authenticator extension on your Chrome browser, follow the steps below:

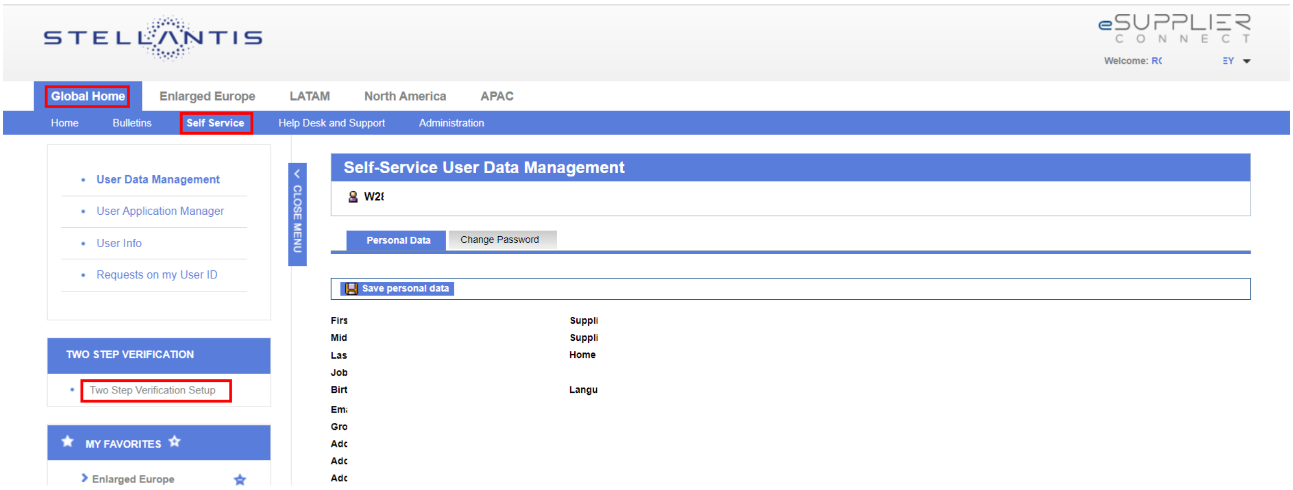
1. Open the Chrome Web Store.
2. Find and select the extension you want.
3. Verify that the publisher is **authenticator.cc**
4. Click Add to Chrome.
5. Some extensions will let you know if they need certain permissions or data. To approve, click Add extension. Important: Make sure you only approve extensions that you trust. To use the extension, click the icon to the right of the address bar.



If you're using a computer through your work, your organization might block some extensions.

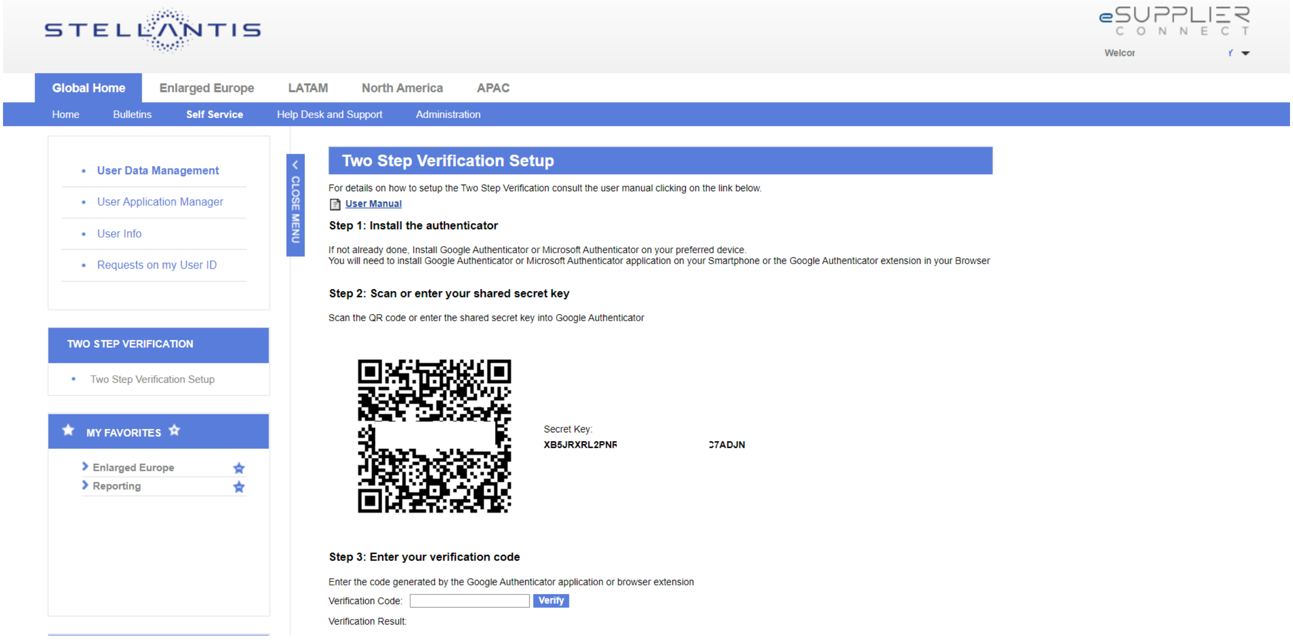
3.2 *Setup the Two-step Verification*

To setup the Two-step verification you need to navigate in the portal to **Global Home > Self Service** and click on the link **Two-step Verification Setup** placed in the box **TWO STEP VERIFICATION**.



The setup is divided in three steps (see image below)

1. Install the authenticator (if not already done)
2. Scan or entry your shared secret key
3. Enter your verification code



Two Step Verification Setup

For details on how to setup the Two Step Verification consult the user manual clicking on the link below.

User Manual

Step 1: Install the authenticator

If not already done, Install Google Authenticator or Microsoft Authenticator on your preferred device.
You will need to install Google Authenticator or Microsoft Authenticator application on your Smartphone or the Google Authenticator extension in your Browser

Step 2: Scan or enter your shared secret key

Scan the QR code or enter the shared secret key into Google Authenticator

Secret Key:
XB5JRXRL2PNF 37ADJN

Step 3: Enter your verification code

Enter the code generated by the Google Authenticator application or browser extension

Verification Code:

Verification Result:

3.2.1 Step 1 – Install the authenticator

If not already done, install the authenticator. To complete the operation, follow the instructions provided in the chapter "Install the Authenticator" above in this manual.

3.2.2 Step 2 – Scan or enter your shared secret key

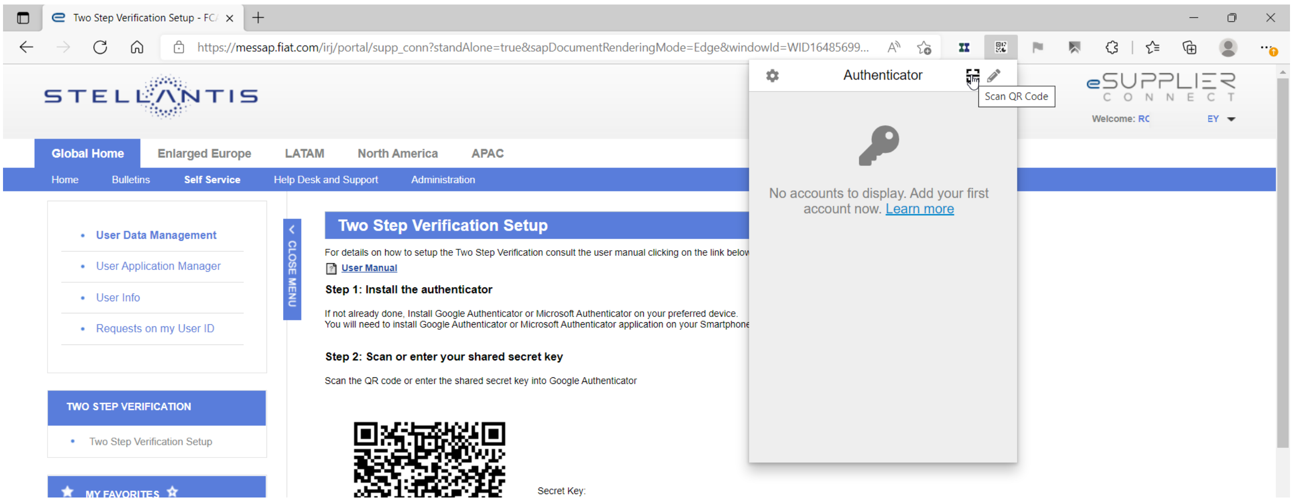
Depending on the device you've chosen for the verification you've to scan the QR Code displayed by the Two-Step verification application.

3.2.2.1 Scan the QR Code using a phone or a tablet

If you've chosen a phone or a tablet, start the Authenticator application and select the option to add a new account and scan the QR Code, the new account will be saved into the application.

3.2.2.2 Scan the QR Code using the Authenticator extension

If you've chosen the Authenticator extension for the browser, you must select the "Scan QR Code" option in the extension



No accounts to display. Add your first account now. Learn more

Two Step Verification Setup

For details on how to setup the Two Step Verification consult the user manual clicking on the link below

User Manual

Step 1: Install the authenticator

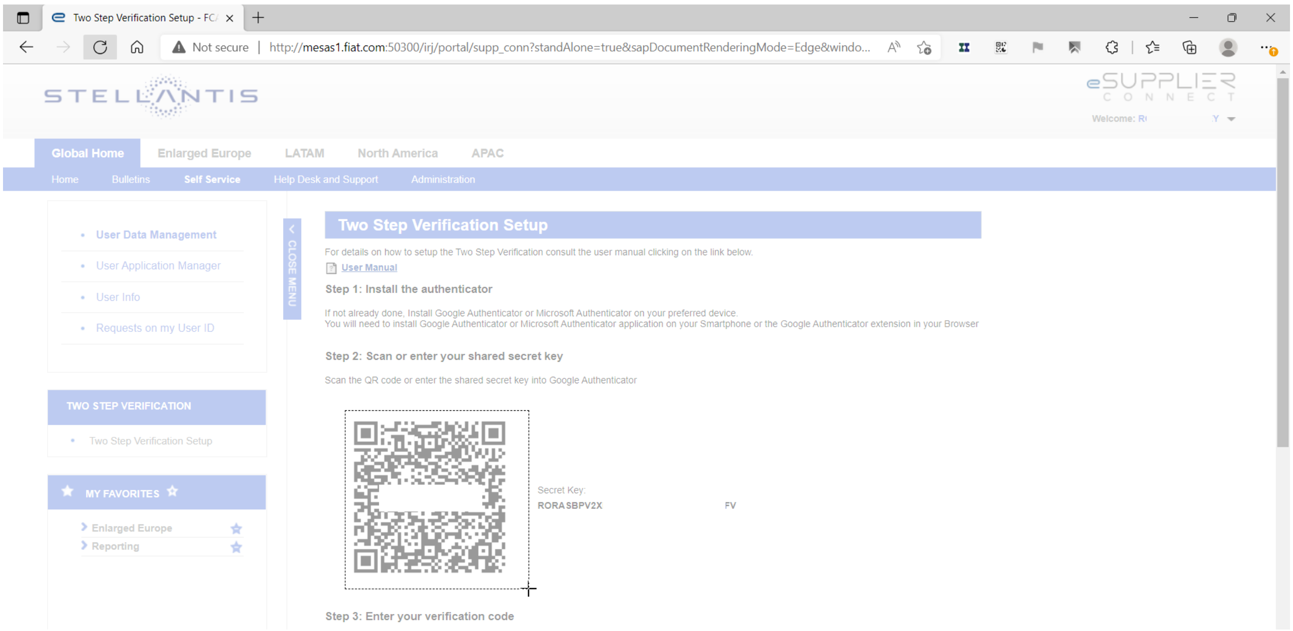
If not already done, Install Google Authenticator or Microsoft Authenticator on your preferred device.
You will need to install Google Authenticator or Microsoft Authenticator application on your Smartphone

Step 2: Scan or enter your shared secret key

Scan the QR code or enter the shared secret key into Google Authenticator

Secret Key:

And using the mouse you must select the QR Code displayed by the Two-step setup application (see image below). The account will be saved automatically into the Authenticator extension.



Two Step Verification Setup

For details on how to setup the Two Step Verification consult the user manual clicking on the link below.

User Manual

Step 1: Install the authenticator

If not already done, Install Google Authenticator or Microsoft Authenticator on your preferred device.
You will need to install Google Authenticator or Microsoft Authenticator application on your Smartphone or the Google Authenticator extension in your Browser

Step 2: Scan or enter your shared secret key

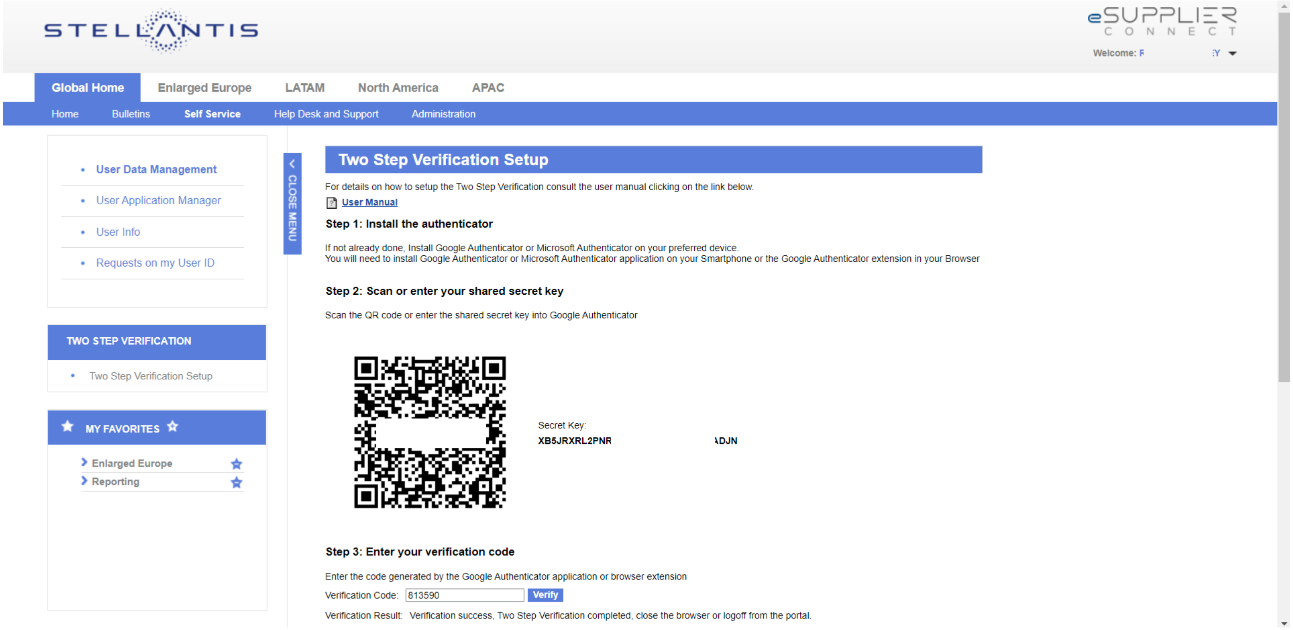
Scan the QR code or enter the shared secret key into Google Authenticator

Secret Key:
RORASBPV2X FV

Step 3: Enter your verification code

3.2.3 Step 3 – Enter your verification code

To complete the setup, you've to enter the verification code generated by the Authenticator application used to store the account in Step 2. The setup process is not completed until you've completed Step 3.



Two Step Verification Setup

For details on how to setup the Two Step Verification consult the user manual clicking on the link below.

User Manual

Step 1: Install the authenticator

If not already done, Install Google Authenticator or Microsoft Authenticator on your preferred device.
You will need to install Google Authenticator or Microsoft Authenticator application on your Smartphone or the Google Authenticator extension in your Browser

Step 2: Scan or enter your shared secret key

Scan the QR code or enter the shared secret key into Google Authenticator

Secret Key:
XB5JRXRL2PNR ADJN

Step 3: Enter your verification code

Enter the code generated by the Google Authenticator application or browser extension

Verification Code: 813590 Verify

Verification Result: Verification success, Two Step Verification completed, close the browser or logoff from the portal.

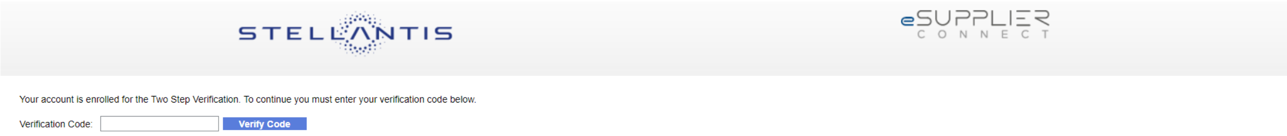
3.3 *Logout from the eSupplierConnect portal*

Once completed all the steps for the setup of the Two-step verification you must logout from the portal and close all the browser tabs.

3.4 *Login to the Portal after the activation of the Two Step Verification*

The next time you login into the eSupplierConnect Portal, after entering your username and password you will be prompted to enter the six-digit verification code (as shown below).

You simply need to open the authentication application you've used for the Two-step verification setup and retrieve the current six-digit number presented. You do not need to scan a QR Barcode or enter a Shared Secret as the device is already associated with your eSupplierConnect account.



Your account is enrolled for the Two Step Verification. To continue you must enter your verification code below.

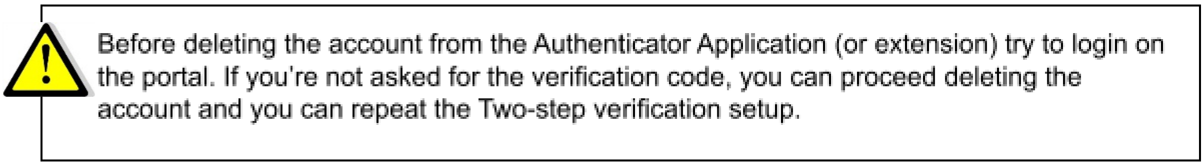
Verification Code: Verify Code

4 Troubleshooting

In the following paragraphs you can find some of the most common problems you can encounter using the Two-Step verification with the eSupplierConnect portal.

4.1 What to do if you’ve not completed the Step 3 of the setup

If for any reason, after saving the account on Step 2 of the Two-step verification setup, you were not able to complete Step 3 you must repeat the configuration again and you must delete from the Authenticator application (or extension) the account that you have created in Step 2.



Before deleting the account from the Authenticator Application (or extension) try to login on the portal. If you're not asked for the verification code, you can proceed deleting the account and you can repeat the Two-step verification setup.

4.2 Change of the authentication device

If you must change the authentication device, you can use the procedures of the Authentication application (or extension) you have chosen to move the accounts from the old device to the new one.

4.2.1 Google Authenticator

If you are using Google authenticator and you need to change the authenticator device, you must select the Export option from the Authenticator menu of the old device and follow the instructions on the screen.
You must have both the old and the new device to complete the operation.

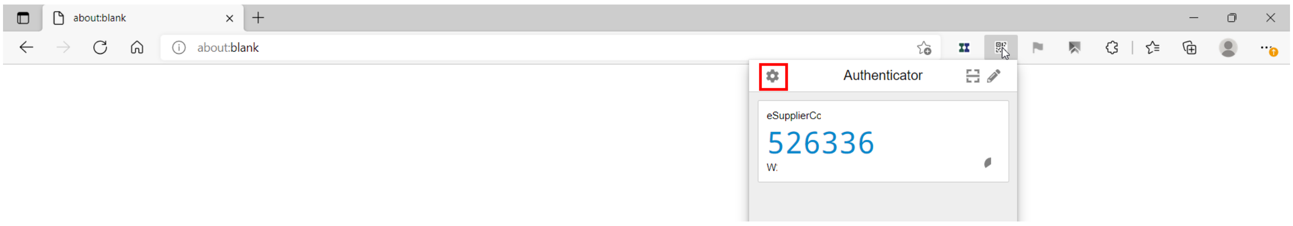
4.2.2 Microsoft Authenticator

If you are using Microsoft authenticator and you need to change the authenticator device, follow these steps:

- Open the Microsoft authenticator application on your old phone
- Tap the three dots at the top right
- Tap “Settings”
- Enable “Cloud backup” if you are using an android phone or ”iCloud Backup” if you are using a IOS phone.
- On your new phone, install the Microsoft Authenticator app and log in to your account
- Select “Begin Recovery”
- Your account and its settings will be added to your new phone

4.2.3 Authenticator extension for the Chrome browser

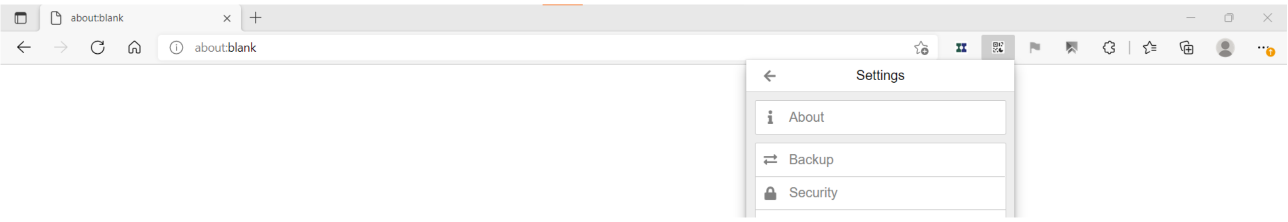
The Authenticator extension allows a Backup and Restore operation accessible through the settings menu. These functionalities can be used to move the configuration from the old device to the new one.



As the backup of the accounts is unencrypted you must store it in a safe place, or you must delete it as soon as the moving from the old device to the new one has been completed.

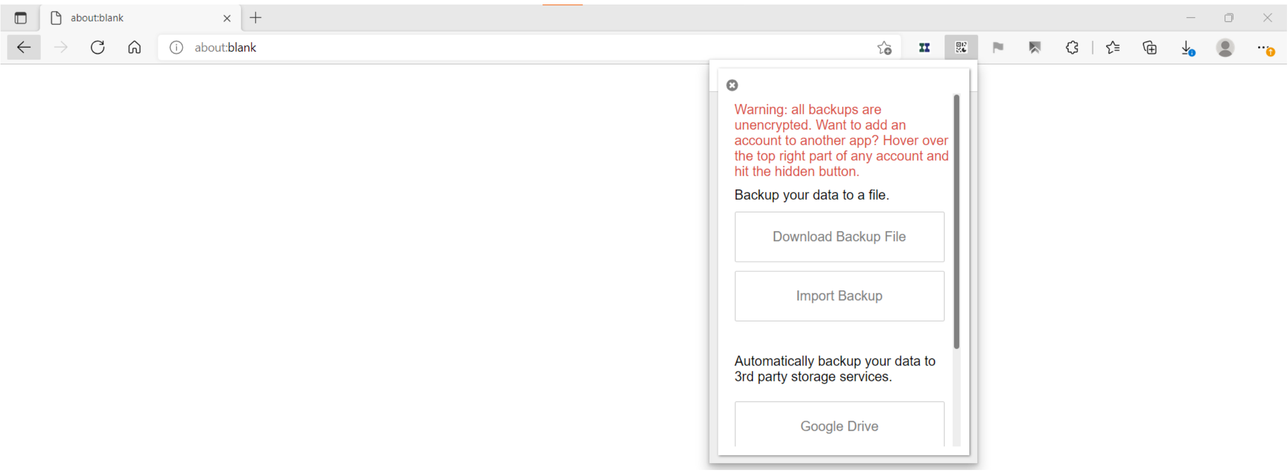
4.2.3.1 Backup

In the Settings menu select the Backup option. You can choose to save the backup locally using the Download Backup File option, or in the cloud for which Google Drive, OneDrive and Dropbox are the available options.



4.2.3.2 Restore

You can import a previously created backup using the Import Backup option. The file must be saved/moved locally before executing the operation.



Warning: all backups are unencrypted. Want to add an account to another app? Hover over the top right part of any account and hit the hidden button.

Backup your data to a file.

Automatically backup your data to 3rd party storage services.

4.3 How to reset the Two-Step verification

If for any reason you no longer have access to the Authenticator device (or extension) and you cannot move the configuration form the original device (or extension) to a new one, you must execute the reset the Two-step verification configuration.

To reset the Two-step verification, you have to open a DriveIT ticket.