Visa IntelliLink Spend Management

Two-Factor Authentication Guide & FAQs

July 2019

Important Information on Confidentiality and Copyright

Notice: This information is proprietary and CONFIDENTIAL to Visa. It is distributed to Visa participants for use exclusively in managing their Visa programs.

The trademarks, logos, trade names and service marks, whether registered or unregistered (collectively the "Trademarks") are Trademarks owned by Visa. All other trademarks not attributed to Visa are the property of their respective owners.

Note: This document is not part of the Visa Rules. In the event of any conflict between any content in this document, any document referenced herein, any exhibit to this document, or any communications concerning this document, and any content in the Visa Rules, the Visa Rules shall govern and control.

Contents

About this Guide

The purpose of this guide is to help *Visa IntelliLink Spend Management* (VISM) users understand how to access the platform using Two-Factor Authentication in the login process. For additional details, please see the Online Help pages within *Visa IntelliLink Spend Management*.

If you need more information or assistance with any of the concepts or procedures described, please get in touch with your Administrator.

Note: The content and screen shots included in this guide may differ from what is seen within the *Visa IntelliLink Spend Management* application due to your company's settings.

Two-Factor Authentication Overview

Two-Factor Authentication (2FA) is a method of verifying a user's identity by requiring them to authenticate using two components (i.e. factors), each of which must be from a different authentication category, as summarized below:

Category	Description	Example
Knowledge	Something only the user knows	Username & password
Possession	Something only the user has	A verification code generated by a pre-registered device
Inherence	Something the user is	Biometrics (e.g. fingerprint, facial recognition)

The two factors must be independent from each other such that if one of the factors is compromised, the reliability of the other factor is not.

Prior to the July 2019 enhancement release, as directed by Visa's Key Controls and Technical Security Requirements for Customer Identity & Access, *Visa IntelliLink Spend Management* used a multi-layer authentication process, by initiating a second knowledge challenge (Memorable Word) after the Username & Password was entered. In the July 2019 enhancement release, the two-layer Memorable Word authentication was replaced by a Two-Factor Authentication process in which users are required to login to the system using a Possession factor (an authentication code) in conjunction with their existing Knowledge factor (their password).

The authentication code is generated via any of the following channels:

- The *Visa IntelliLink Spend Management* mobile app
- An email sent to the Email Address specified in the user's profile
- A third-party authentication application of the user's choice that supports the Time-based One-Time Password algorithm (TOTP), such as Google Authenticator, Authy, Duo Mobile, LastPass Authenticator, and others.

Enabling Two-Factor Authentication

Two-Factor Authentication is enabled at the Bank ID level in VISM. Once activated it applies to all companies in the Bank instance.

The supported methods for authentication code generation, as well as a default preferred method, are also configured at the Bank ID level. For example, a Bank may support the Visa IntelliLink Spend Management mobile app as the default preferred method, as well as Email, but not third-party authentication apps. If a Bank supports more than one method, the user may choose their own preferred method from among those supported.

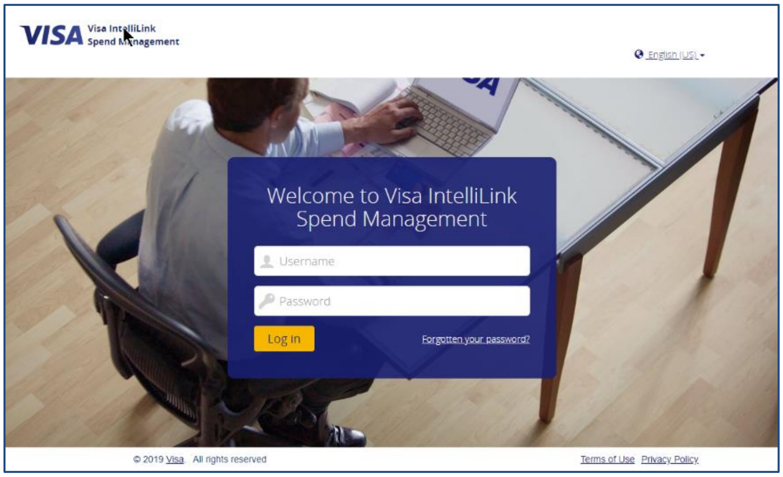
Note:

- 2FA was enabled for banks and companies in Europe and North America in the July 2019 enhancement release.
- 2FA will be enabled for banks and companies in other regions in the September 2019 enhancement release.
- 2FA will apply to users who login directly at https://intellilink.spendmanagement.visa.com. Users who access the application via Single Sign On from Visa Online or the Visa Business Solutions Experience portal may not be required to authenticate using 2FA.
- 2FA will not be required for Bank Administrators in the July release.

First-time Registration for Two-Factor Authentication

Step 1: Enter Your Username and Password

1. Open a web browser and navigate to: https://intellilink.spendmanagement.visa.com



VISA Visa IntelliLink Spend Management
English (US)
Username
Password
Log in
Forgotten your password?
© 2019 Visa. All rights reserved
Terms of Use Privacy Policy

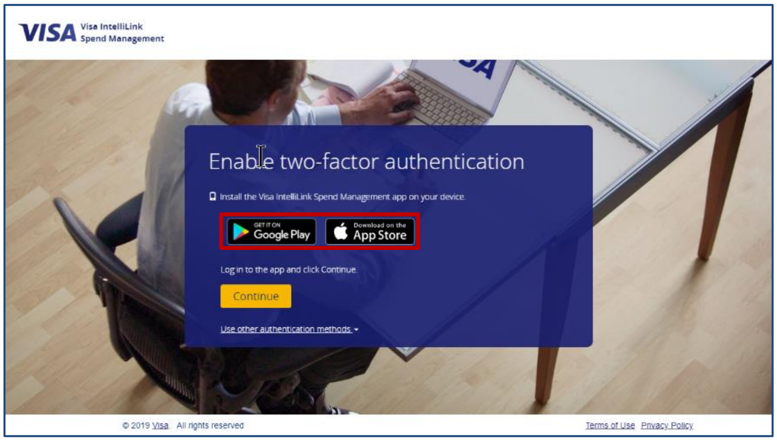
Welcome to Visa IntelliLink Spend Management

2. On the *Welcome to Visa IntelliLink Spend Management* page, enter your Username and Password. Then click **Log in**.
3. If this is your first login after the July 21, 2019 release you will be prompted to enter your **Memorable Word** prior to proceeding to register for Two-Factor Authentication.

Note: Users with profiles created after the July 21, 2019 release, who have not previously set a Memorable Word will proceed directly to the 2FA registration flow.

Step 2a: Set Up Two-Factor Authentication – Visa IntelliLink Spend Management Mobile App

4. After your username and password are accepted, the *Enable two-factor authentication* window displays. This is where you choose the authentication method to use when accessing the application. In this case, it suggests the *Visa IntelliLink Spend Management* mobile app. If you have not done so already, **download and install** the mobile app.

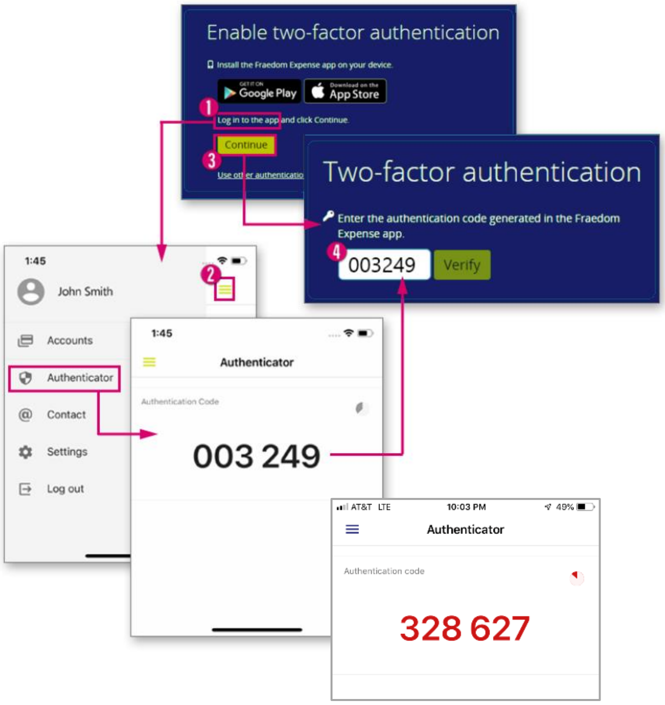


VISA Visa IntelliLink Spend Management
GET IT ON Google Play
Download on the App Store
Continue
Use other authentication methods
© 2019 Visa. All rights reserved
Terms of Use Privacy Policy

Enable two-factor authentication

Install the Visa IntelliLink Spend Management app on your device.

Log in to the app and click Continue.



Enable two-factor authentication

Install the Fraedom Expense app on your device.

Log in to the app and click Continue.

Two-factor authentication

Enter the authentication code generated in the Fraedom Expense app.

5. **Open and log in** to the *Visa IntelliLink Spend Management* app on your mobile device.

6. From within the *mobile app*:

   - Tap the **Options** menu.
   - Tap **Authenticator**.
     An *Authentication Code* displays in the mobile app for thirty seconds, then a new one is automatically generated.

   Tip: A small stopwatch icon in the upper-right corner of the Authenticator screen shows how long the code is still valid. The authentication code will turn **red** when it is nearing expiration.

7. From within the *desktop* application:

   - Click **Continue**.
   - Enter the **Authentication Code** currently displayed in the *mobile app*.
   - Click **Verify**.

8. Your registration with the *Visa IntelliLink Spend Management* mobile app is now complete. For all future log ins to the *Visa IntelliLink Spend Management* deskop application you will be asked to enter your username and password, and repeat **Steps 6 & 7**, above.

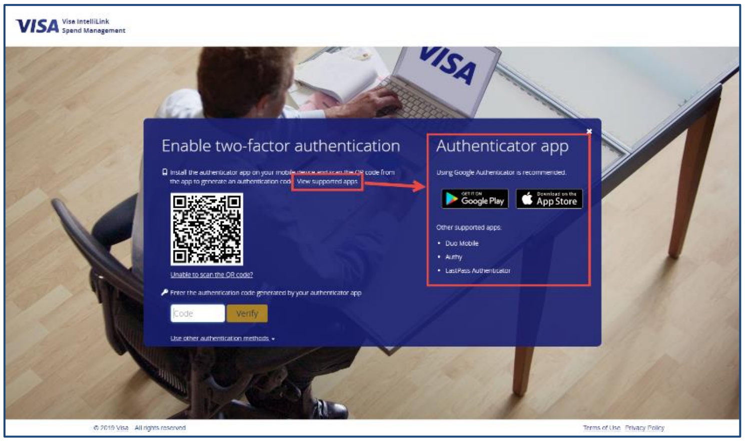
Note:

- For more information about installing and setting up the mobile app, ask your Administrator for the *Visa IntelliLink Spend Management Mobile App Guide*.
- If you prefer not to use the *Visa IntelliLink Spend Management* mobile app to authenticate, click **Use other authentication methods** to select *Email* or *Authenticator app* (as supported by your Bank) then follow the onscreen instructions. Whichever method you register with will be used every time you log in to the desktop application in the future.
- If you want to change your method, see *Change Your Two-Factor Authentication Method*, below for instructions to reset and re-register.

Step 2b: Set Up Two-Factor Authentication – Third-Party Authenticator App

2FA is also supported for *Visa IntelliLink Spend Management* using third-party authenticator apps that use the Time-Based One-Time Password (TOTP) protocol. Examples are: Google Authenticator, Authy, Duo Mobile, LastPass Authenticator, and others. The steps below are generalized from the Google Authenticator experience.

4. After your username and password are accepted, the *Enable two-factor authentication* window displays. This is where you choose the authentication method to use when accessing the application. If you have not done so already, **download and install** a TOTP-based Authenticator app from the relevant app store for your device.



Enable two-factor authentication

Install the authenticator app on your mobile device and scan the QR code from the app to generate an authentication code. View supported apps

Unable to scan the QR code?

Enter the authentication code generated by your authenticator app

Authenticator app

Using Google Authenticator is recommended.

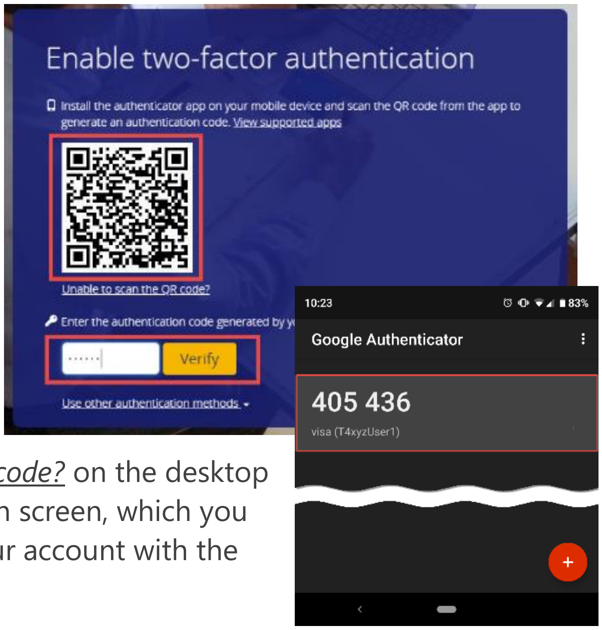
Other supported apps:

- Duo Mobile
- Authy
- LastPass Authenticator

© 2019 Visa All rights reserved

VISA Visa IntelliLink Spend Management
Code
Verify
Use other authentication methods
GET IT ON Google Play
Download on the App Store
Terms of Use Privacy Policy

5. **Open** the app on your mobile device.
6. From within the *mobile app*:
   - Add your *Visa IntelliLink Spend Management* account.
     - If the app supports it, scan the QR code on the login screen.
       An *Authentication Code* displays in the mobile app for 30 seconds, then a new one is automatically generated.
     - If the app does not support QR code scanning, or you are otherwise unable to scan the QR code, click *Unable to scan the QR code?* on the desktop login scren. An encryption key will be shown on screen, which you can enter into the app manually to register your account with the authenticator app.



Enable two-factor authentication

Install the authenticator app on your mobile device and scan the QR code from the app to generate an authentication code. View supported apps

Unable to scan the QR code?

Enter the authentication code generated by y

Google Authenticator

405 436

visa (T4xyzUser1)

7. From within the *desktop* application:
   - Enter the **Authentication Code** currently displayed in the *mobile app*.
   - Click **Verify**.

8. Your registration with the third-party authenticator app is now complete. For all future log ins to the *Visa IntelliLink Spend Management* deskop application you will be asked to enter your username and password, and repeat **Steps 5 & 7**, above.

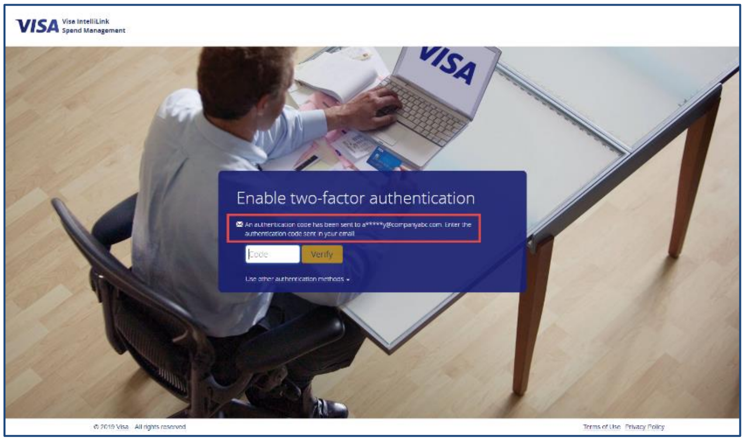
Note:

- If you prefer not to use a third-party authenticator app to authenticate, click **Use other authentication methods** to select *Email* or the *Visa IntelliLink Spend Management* app (as supported by your Bank), then follow the onscreen instructions. Whichever method you register with will be used every time you log in to the desktop application in the future.
- If you want to change your method, see *Change Your Two-Factor Authentication Method*, below for instructions to reset and re-register.

Step 2c: Set Up Two-Factor Authentication – Email

Email delivery of authentication codes is also a supported option for 2FA into *Visa IntelliLink Spend Management*

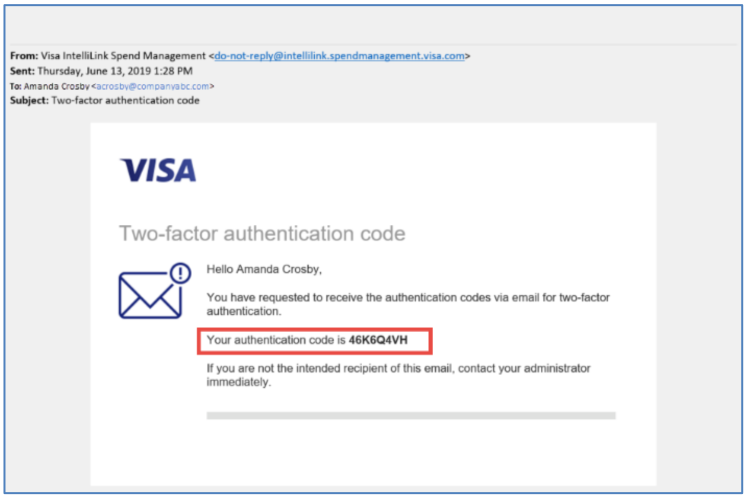
4. If your bank has configured Email as the default method for retrieving authentication codes, after your username and password are accepted, the *Enable two-factor authentication* window displays, informing you that an authentication code has been sent to the email address in your profile.


VISA Visa IntelliLink Spend Management
VISA
Code
Verify
Use other authentication methods
© 2019 Visa All rights reserved
Terms of Use Privacy Policy

Enable two-factor authentication

An authentication code has been sent to a*****y@companyabc.com. Enter the authentication code sent in your email

5. **Open** your email and copy-paste or type the authentication code into the text box on the login screen



From: Visa IntelliLink Spend Management <do-not-reply@intellilink.spendmanagement.visa.com>
Sent: Thursday, June 13, 2019 1:28 PM
To: Amanda Crosby <acrosby@companyabc.com>
Subject: Two-factor authentication code

Two-factor authentication code

Hello Amanda Crosby,

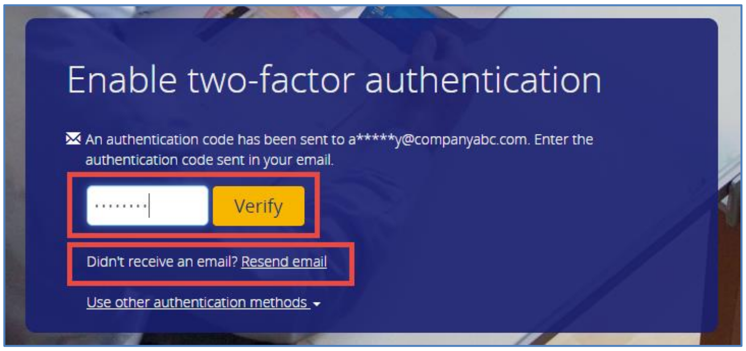
You have requested to receive the authentication codes via email for two-factor authentication.

Your authentication code is **46K6Q4VH**

If you are not the intended recipient of this email, contact your administrator immediately.

6. Click **Verify**.

7. Your registration with email is now complete. For all future log ins to the *Visa IntelliLink Spend Management* deskop application you will be asked to enter your username and password, and repeat **Steps 5 & 6**, above.



Enable two-factor authentication

An authentication code has been sent to a*****y@companyabc.com. Enter the authentication code sent in your email.

Didn't receive an email? Resend email

Tip: If you haven't verified a code after 1 minute, the *Didn't receive an email? <u>Resend email</u>* link displays. Click the link to re-send the email with a new authentication code..

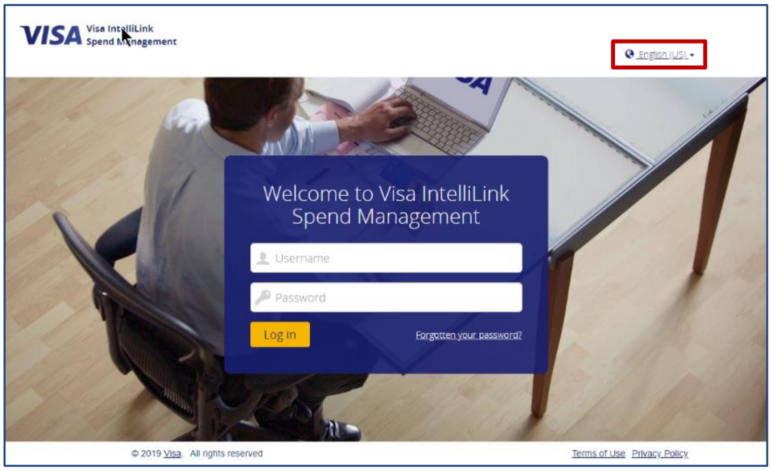
Note:

- A different logic is used to generate the codes sent via email than those generated in the mobile apps. The authentication code delivered via email will always be mix of characters and numbers rather than a six-digit numeric code.
- If you prefer not to use email to authenticate, click **Use other authentication methods** to select the *Visa IntelliLink Spend Management* app or a Third-Party Authenticator app (as supported by your Bank), then follow the onscreen instructions. Whichever method you register with will be used every time you log into the desktop application in the future.
- If you want to change how you authenticate, see *Change Your Two-Factor Authentication Method*, below for instructions to reset and re-register.

Ongoing Usage of Two-Factor Authentication for Log in

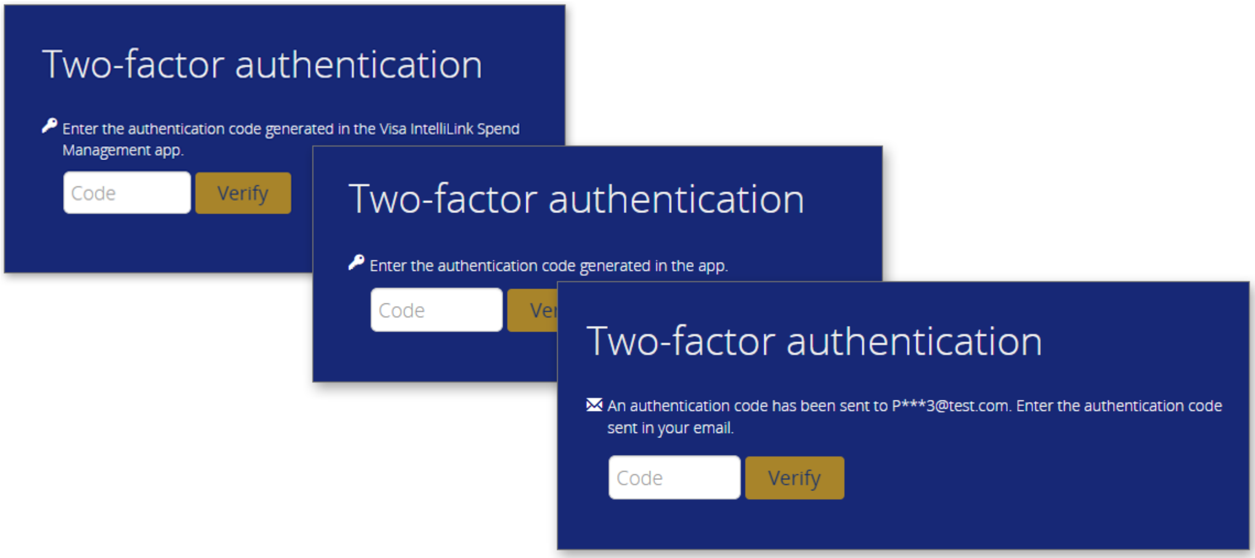
Step 1: Enter Your Username and Password

1. Open a web browser and navigate to: https://intellilink.spendmanagement.visa.com
2. On the *Welcome to Visa IntelliLink Spend Management* page, enter your Username and Password. Then click **Log in**.


VISA Visa IntelliLink Spend Management
English (US)
Welcome to Visa IntelliLink Spend Management
Username
Password
Log in
Forgotten your password?
© 2019 Visa All rights reserved
Terms of Use Privacy Policy

Step 2: Enter Your Two-Factor Authentication Code

3. After entering your Username and Password, you will be presented with the code verification screen for your chosen authentication method.


Two-factor authentication

Enter the authentication code generated in the Visa IntelliLink Spend Management app.

Two-factor authentication

Enter the authentication code generated in the app.

Two-factor authentication

An authentication code has been sent to P***3@test.com. Enter the authentication code sent in your email.

4. Open the chosen method to retrieve the authentication code and enter it into the *Code* text box on the *desktop application* log in screen.
5. Click **Verify**.

Note:

- You will be required to enter a 2FA code each time you log in to *Visa IntelliLink Spend Management*.
- 2FA will apply to users who login directly at https://intellilink.spendmanagement.visa.com. Users who access the application via Single Sign On from Visa Online or the Visa Business Solutions Experience portal may not be required to authenticate using 2FA.
- Your account will be temporarily locked following 4 unsuccessful log in attempts. You may try again later or contact your Administrator to unlock your account.

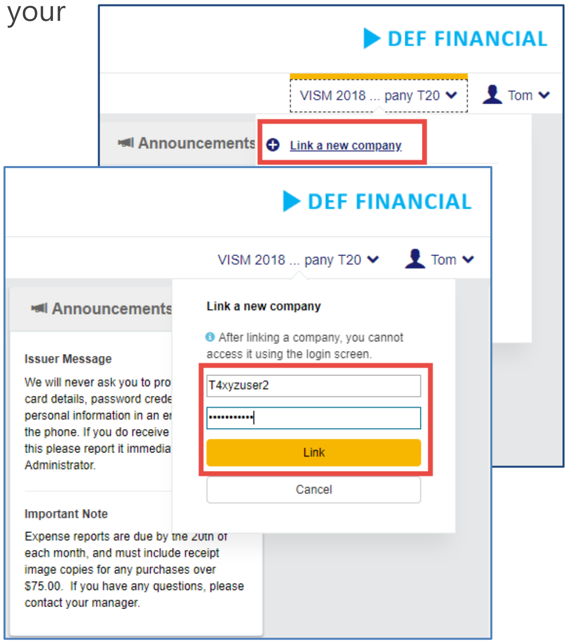
Usage of Two-Factor Authentication in Multi-Instance Access

If you are self-linking a company to your primary user profile via Multi-Instance Access you will be required to authenticate using a 2FA code if you have registered for 2FA in the company you are linking. If you have not yet registered for 2FA in the company you are linking, you will only be required to enter your username and password for the company being linked.

Step 1: Link a Company to Your Primary Profile

1. From the Multi-Instance Access drop-down menu within your primary company click **Link a new company**

2. Enter the Username and Password associated with the profile in the company you are linking to. Then click the **Link** button.



After linking a company, you cannot access it using the login screen.

T4xyzuser2

•••••••••••

Issuer Message

We will never ask you to pro card details, password crede personal information in an e the phone. If you do receive this please report it immedia Administrator.

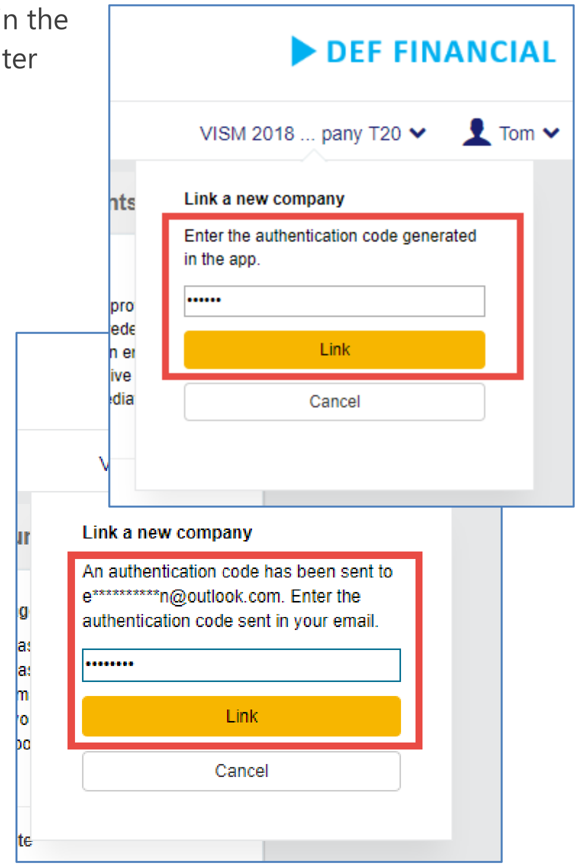
Important Note

Expense reports are due by the 20th of each month, and must include receipt image copies for any purchases over $75.00. If you have any questions, please contact your manager.

3. If you have previously registered for 2FA on the profile in the company you are linking to, you will be prompted to enter the authentication code generated via the method you registered for.

4. After entering the authentication code, click **Link**.

5. If the code is correct, the company will appear in your Multi-Instance Access drop-down menu, along with a **Success** message at the bottom of the screen.



Link a new company

Enter the authentication code generated in the app.

Link a new company

An authentication code has been sent to e**********n@outlook.com. Enter the authentication code sent in your email.

Note:

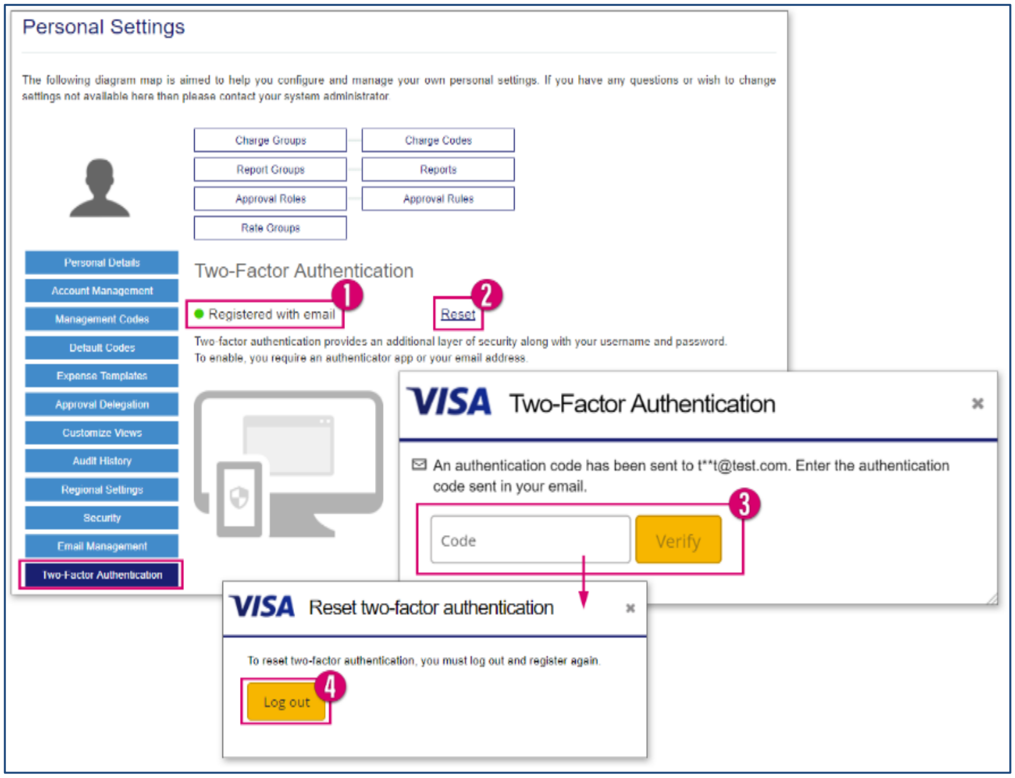
- You will not be prompted for a 2FA code when accessing companies that have already been linked to your primary profile.
- If you have not yet registered for 2FA in the company you are linking, you will only be required to enter your username and password for the company being linked.

Managing Two-Factor Authentication

Change Your Two-Factor Authentication Method

You can change the way you receive authentication codes by resetting two-factor authentication. This deletes your current registration method and allows you to choose a different method.

1. Click 👤 **Profile menu > Personal Settings > Two-Factor Authentication**. On the *Two-Factor Authentication* screen, you will see displayed your current two-factor authentication method.
2. Click **Reset**.
3. You will be required to confirm the reset by entering an authentication code from your currently registered method. Click **Verify**.
4. When the authentication code is confirmed, click **Log out**.



Personal Settings

The following diagram map is aimed to help you configure and manage your own personal settings. If you have any questions or wish to change settings not available here then please contact your system administrator

Two-Factor Authentication

● Registered with email

Two-factor authentication provides an additional layer of security along with your username and password. To enable, you require an authenticator app or your email address.

VISA Two-Factor Authentication

An authentication code has been sent to t**t@test.com. Enter the authentication code sent in your email.

VISA Reset two-factor authentication

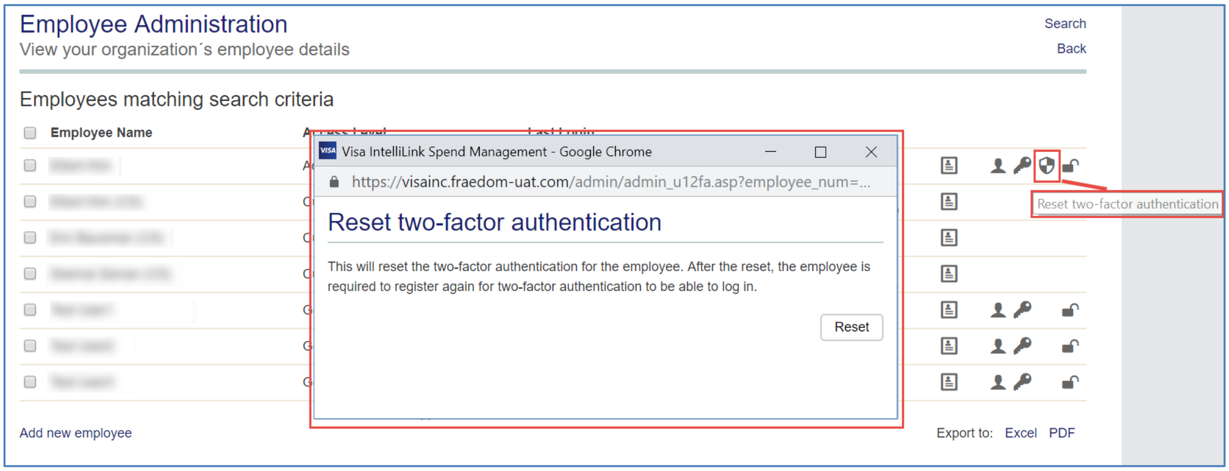
To reset two-factor authentication, you must log out and register again.

5. You may then re-register for an alternate method by following the instructions above.

Administrator Reset of a User’s Two-Factor Authentication

Administrators may reset a user’s method of Two-Factor Authentication as needed. This can prove useful in the event a user has lost his or her currently registered mobile device, or in multiple other circumstances.

1. Access the **Employee Administration** section of **Administration Overview**.
2. In the Employee search results, find the relevant employee and click the shield 🛡 icon.



Employee Administration

View your organization´s employee details

Employees matching search criteria

Visa IntelliLink Spend Management - Google Chrome

https://visainc.fraedom-uat.com/admin/admin_u12fa.asp?employee_num=...

Reset two-factor authentication

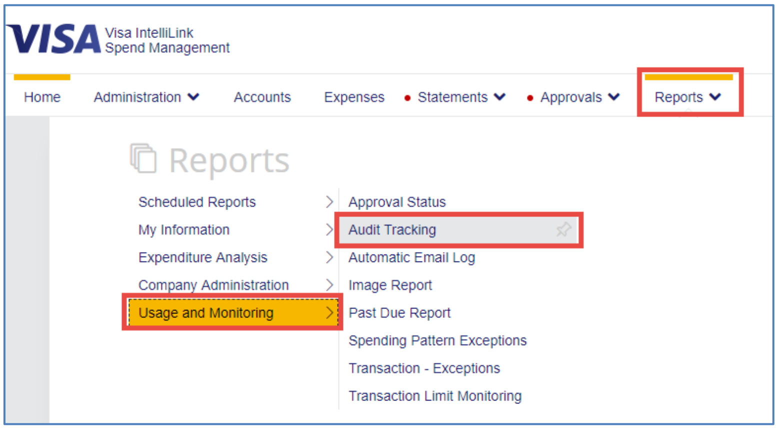
This will reset the two-factor authentication for the employee. After the reset, the employee is required to register again for two-factor authentication to be able to log in.

3. Click **Reset**.
4. The user can now re-register for an alternate method by following the instructions above.

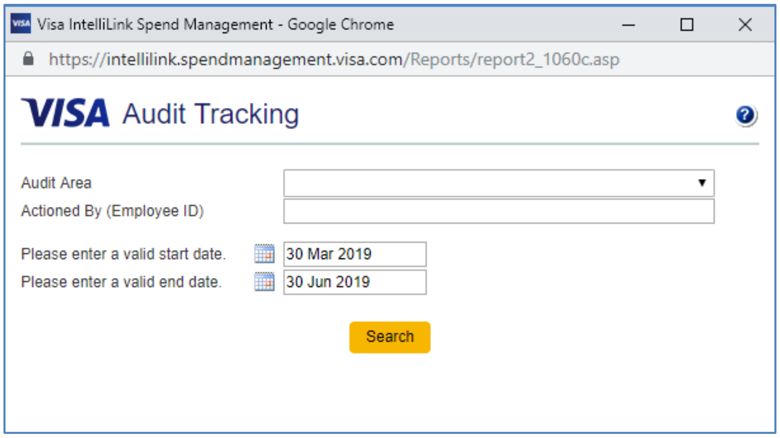
Audit Tracking for Two-Factor Authentication

Administrators can track authentication-related changes in the system using the **Audit Tracking** reports. The **Two-Factor Authentication** audit area in the **Audit Tracking** reports provide visibility to registered 2FA methods and resets.

1. Access the **Audit Tracking** option from the **Usage and Monitoring** section of the **Reports** menu.



2. In the **Audit Area**, select **Two-Factor Authentication**. Enter a date range, if desired.
3. Click **Search**.


Visa IntelliLink Spend Management - Google Chrome
https://intellilink.spendmanagement.visa.com/Reports/report2_1060c.asp
VISA Audit Tracking
Search

Audit Area
Actioned By (Employee ID)
Please enter a valid start date. 30 Mar 2019
Please enter a valid end date. 30 Jun 2019

4. Possible values in the **Action** column are:

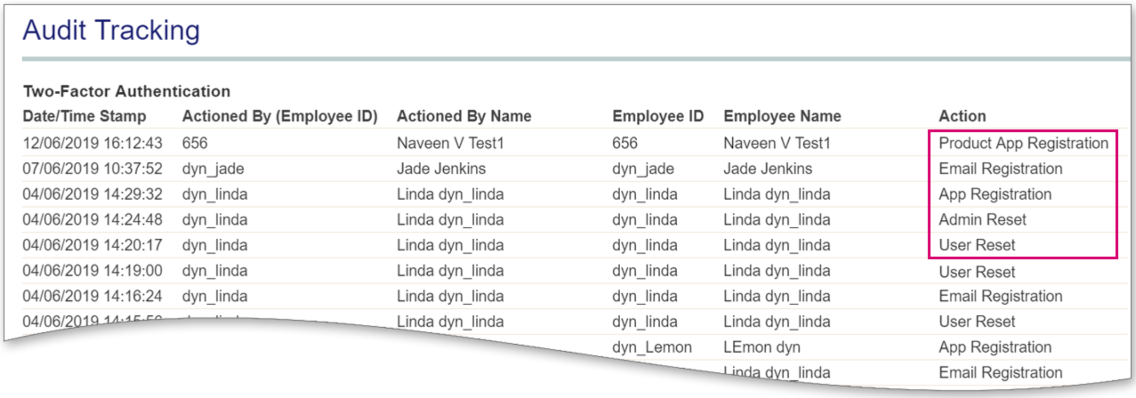
   Product App Registration – the user registered for 2FA using the *Visa IntelliLink Spend Management* mobile app

   App Registration – the user registered using a third-party authenticator app

   Email Registration – the user registered using email

   Admin Reset – the Administrator reset another user's 2FA method

   User Reset – the User reset his or her own 2FA method



Audit Tracking

Two-Factor Authentication

Date/Time Stamp	Actioned By (Employee ID)	Actioned By Name	Employee ID	Employee Name	Action
12/06/2019 16:12:43	656	Naveen V Test1	656	Naveen V Test1	Product App Registration
07/06/2019 10:37:52	dyn_jade	Jade Jenkins	dyn_jade	Jade Jenkins	Email Registration
04/06/2019 14:29:32	dyn_linda	Linda dyn_linda	dyn_linda	Linda dyn_linda	App Registration
04/06/2019 14:24:48	dyn_linda	Linda dyn_linda	dyn_linda	Linda dyn_linda	Admin Reset
04/06/2019 14:20:17	dyn_linda	Linda dyn_linda	dyn_linda	Linda dyn_linda	User Reset
04/06/2019 14:19:00	dyn_linda	Linda dyn_linda	dyn_linda	Linda dyn_linda	User Reset
04/06/2019 14:16:24	dyn_linda	Linda dyn_linda	dyn_linda	Linda dyn_linda	Email Registration
04/06/2019 14:15:5		Linda dyn_linda	dyn_linda	Linda dyn_linda	User Reset
			dyn_Lemon	LEmon dyn	App Registration
				Linda dyn_linda	Email Registration

5. The **Audit Tracking** report also gives Administrators visibility into what caused an authentication failure.

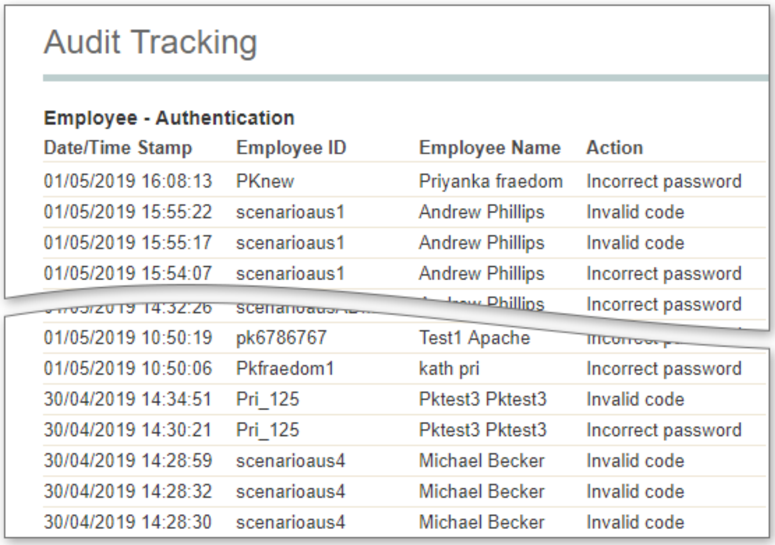
6. In the **Audit Area** of the Audit Tracking report, select **Employee – Authentication**. Enter a date range if desired.

7. Click **Search**.

8. Possible values in the **Action** column are:

   Incorrect password – the user entered an incorrect password

   Invalid code – the user entered an invalid authentication code



Audit Tracking

Employee - Authentication

Date/Time Stamp	Employee ID	Employee Name	Action
01/05/2019 16:08:13	PKnew	Priyanka fraedom	Incorrect password
01/05/2019 15:55:22	scenarioaus1	Andrew Phillips	Invalid code
01/05/2019 15:55:17	scenarioaus1	Andrew Phillips	Invalid code
01/05/2019 15:54:07	scenarioaus1	Andrew Phillips	Incorrect password
2019 14:32:26	scenarioaus	Phillips	Incorrect password
01/05/2019 10:50:19	pk6786767	Test1 Apache	Incorrect p
01/05/2019 10:50:06	Pkfraedom1	kath pri	Incorrect password
30/04/2019 14:34:51	Pri_125	Pktest3 Pktest3	Invalid code
30/04/2019 14:30:21	Pri_125	Pktest3 Pktest3	Incorrect password
30/04/2019 14:28:59	scenarioaus4	Michael Becker	Invalid code
30/04/2019 14:28:32	scenarioaus4	Michael Becker	Invalid code
30/04/2019 14:28:30	scenarioaus4	Michael Becker	Invalid code

Frequently Asked Questions

This list of Frequently Asked Questions is intended to be a living document. Additional questions may be added based on support inquiries to the Visa Business Solutions Account Management support teams.

What is Two-Factor Authentication?

Two-Factor Authentication (2FA) is a best-practice method of verifying a user's identity by requiring them to authenticate using two components (i.e. factors), each of which must be from a different authentication category, as summarized below:

Category	Description	Example
Knowledge	Something only the user knows	Username & password
Possession	Something only the user has	A verification code generated by a pre-registered device
Inherence	Something the user is	Biometrics (e.g. fingerprint, facial recognition)

The two factors must be independent from each other such that if one of the factors is compromised, the reliability of the other factor is not.

Why is Visa requiring Two-Factor Authentication?

Data breaches and identity theft are serious concerns in today's hyper-connected world. With this growing connectivity come millions of new potential opportunities for cybercriminals. Following the guidance of Visa's Key Controls and Technical Security Requirements for Customer Identity & Access we have decided to implement this enhanced layer of security and protection against fraudulent logins. With this approach we have strived to set the correct balance between convenience and risk reduction.

Can I bypass Two-Factor Authentication and continue using my Memorable Word?

The first time a user logs in after 2FA is enabled, they will be prompted to enter their username & password, then memorable word. They will immediately be prompted to register for 2FA using one of the supported methods. There will not be an opportunity to bypass and register later.

I don't see Email (or, third-party app or *Visa IntelliLink Spend Management* app) when I try to use other authentication methods. Why?

The supported methods for authentication code generation, as well as a default preferred method, were determined by your Bank. For information about why a specific method is not supported, please contact your Administrator.

Which third-party authenticator apps work with VISM? Why is Authenticator App X not supported?

Visa IntelliLink Spend Management supports the time-based one-time password (TOTP) protocol for authentication code generation. TOTP is a more secure method as it ensures there is only one valid OTP at any given time.

While any third-party authentication app that supports (TOTP) *should* work, due to the sheer number of them available in the various app stores we are only able to test against, and confirm support for, Google Authenticator, Authy, Duo Mobile, and LastPass Authenticator.

Can I retrieve my authentication code via SMS/Text Message?

Following the guidance of the National Institute of Standards and Technology's Digital Identity Guidelines, we do not support the use of SMS for authentication code delivery due to Social Engineering and Endpoint Compromise insecurities.

Is RSA SecurID supported?

RSA SecurID uses a proprietary algorithm to generate its one-time passwords. They do not support third-party products such as *Visa IntelliLink Spend Management*.

https://community.rsa.com/thread/193170

Can one user profile be associated with multiple authentication methods?

Each user profile can only be associated with one authentication method at any moment in time. If you wish to use an alternate method from your current registered one you must reset your 2FA and re-register with a new method. See *Change Your Two-Factor Authentication Method* above.

Can a single 2FA method be used for multiple user profiles?

A third-party app or Email may be used as the authentication method for multiple user profiles. In the case of third-party apps, you may be able to add as many accounts as necessary. In the case of Email, if yours is the Email Address 1 in multiple user profiles, you may receive the authentication codes for each profile at that email address. These are the most practical 2FA options for users with multiple profiles.

If you use the *Visa IntelliLink Spend Management* mobile app as the authenticator method, you will be prevented from changing users as the mobile app enforces a "one-at-a-time" relationship to the user profiles for 2FA. We do not currently support multiple authentication codes for different users in the VISM app.

How can I access another profile in the VISM mobile app after registering it as the 2FA method?

The *Visa IntelliLink Spend Management* mobile app authenticator enforces a "one-at-a-time" relationship to the user profiles for 2FA. Once the app is established as the 2FA method, you will be prevented from switching users in the app.

If you wish to use the app to access another profile, you will need to reset and re-register your 2FA method to an alternate method (i.e. email or third party app) and log-in to the mobile app using the new method. See *Change Your Two-Factor Authentication Method* above. This will deactivate the "one-at-a-time" relationship and allow you to 'Change Users' via the side menu bar in the app.

How can multiple users access a single shared account?

It is a best-practice for each person who needs access to *Visa IntelliLink Spend Management* to have his or her own unique profile and login credential. If multiple people support a single user/account, each of them can be delegated to the user/account from their own profile.

Is Two-Factor Authentication required to access the *Visa IntelliLink Spend Management* mobile app?

Log in to the *Visa IntelliLink Spend Management* mobile app generally won't require 2FA, but it is dependent on whether or not the user had downloaded the app and linked it to their profile prior to 2FA being enabled.

- If a device is already linked to the profile, users will not be prompted to enter 2FA when logging in to the app. The linkage between the device and the profile serves as a second factor via 'something the user has'. The user will only be required to enter their username and password – or, 5-digit PIN – to log-in.

- If the device was unlinked and the user has not yet registered a 2FA method, the user will be prompted with a message to notify them that the App is now the mechanism to use for 2FA. They will not be required to use 2FA for future logins to the mobile app.
- If the device was unlinked and the user has already registered another 2FA method, the user will be prompted to enter an authentication code as they would to log-in to the website. e.g. if a user registered email as their 2FA method, they will enter the authentication code sent to their email.

Help! I lost my phone and I am now unable to log in because I cannot retrieve my 2FA code.

Contact your Administrator. He or she may be able to reset your 2FA method for you.

If you had registered to use the VISM mobile app as your 2FA method, your Administrator will also need to remove your device from the ‘Mobile Devices’ tab in your profile after resetting your 2FA method. If this step is missed, you may still be prevented from using a 2FA code from your newly registered method.