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:

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Knowledge</td>
<td>Something only the user knows</td>
<td>Username &amp; password</td>
</tr>
<tr>
<td>Possession</td>
<td>Something only the user has</td>
<td>A verification code generated by a pre-registered device</td>
</tr>
<tr>
<td>Inherence</td>
<td>Something the user is</td>
<td>Biometrics (e.g. fingerprint, facial recognition)</td>
</tr>
</tbody>
</table>

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.
Visa IntelliLink Spend Management – Two-Factor Authentication

- 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.