Important Information on Confidentiality and Copyright

© 2019 Visa. All Rights Reserved.

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 .......................................................................................................................... 3

Two-Factor Authentication Overview ....................................................................................... 3

Enabling Two-Factor Authentication ......................................................................................... 4

First-time Registration for Two-Factor Authentication ............................................................... 4
  Step 1: Enter Your Username and Password ......................................................................... 4
  Step 2a: Set Up Two-Factor Authentication – Email ............................................................... 4
  Step 2b: Set Up Two-Factor Authentication – Visa IntelliLink Spend Management Mobile App... 6

Ongoing Usage of Two-Factor Authentication for Log in .......................................................... 8
  Step 1: Enter Your Username and Password ......................................................................... 8
  Step 2: Enter Your Two-Factor Authentication Code ............................................................. 8

Managing Two-Factor Authentication ......................................................................................... 10
  Change Your Two-Factor Authentication Method ................................................................ 10

Invalid Login Credentials ........................................................................................................... 10
  User entering correct username with incorrect password or authentication code .......... 11
  User entering incorrect username ....................................................................................... 13

Frequently Asked Questions ..................................................................................................... 15
  What is Two-Factor Authentication? .................................................................................. 15
  Why is Visa requiring Two-Factor Authentication? .............................................................. 15
  Can I bypass Two-Factor Authentication and continue using my Memorable Word? .......... 15
  Can I retrieve my authentication code via SMS/Text Message? ......................................... 16
  Is RSA SecurID supported? ............................................................................................... 16
  Do the authentication codes expire? .................................................................................... 16
  What if I don’t receive the email with my authentication code, or the authentication code expires before I receive the email and use the code? ................................................................. 16
  What does it mean if I receive the message “Login failed. Try again or contact your administrator?” ................................................................. 17
What does it mean if I receive the message “The Resend email link is unavailable due to multiple attempts. Please try after some time once the Resend email link appears or contact your administrator for assistance?” ................................................................. 17

Can one user profile be associated with multiple authentication methods? ................................................................. 17

Can a single 2FA method be used for multiple user profiles? .................................................................................. 17

How can I access another user profile (Change user) in the VISM mobile app after registering it as the 2FA method? .................................................................................................................. 18

How can multiple users access a single shared account? .................................................................................. 18

Is Two-Factor Authentication required to access the Visa IntelliLink Spend Management mobile app? .................................................................................................................. 19

Help! I lost my phone and I am now unable to log in because I cannot retrieve my 2FA code. ... 19
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.

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 organization’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:

<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.

Prior to the July 2019 enhancement release, 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 either of the following channels:

- An email sent to the Email Address specified in the user’s profile
- The Visa IntelliLink Spend Management mobile app
Enabling Two-Factor Authentication

The default preferred authentication code generation method is Email, however, the user may change their preferred method to the Visa IntelliLink Spend Management mobile app.

First-time Registration for Two-Factor Authentication

Step 1: Enter Your Username and Password

1. Open a web browser and navigate to: https://identity.intellilink.spendmanagement.visa.com
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 20, 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 20, 2019 release, who have not previously set a Memorable Word will proceed directly to the 2FA registration flow. Those users will not be prompted to enter a Memorable Word.

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

4. 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.
5. **Open** your email and copy-paste or type the authentication code into the text box on the login screen.

![Two-factor authentication code](image)

6. **Click** Verify.

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

**Tip:** If you haven't verified a code after 1 minute, the *Didn't receive an email? Resend email* 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 app. The authentication codes delivered via email may differ in length and/or be comprised of different types of characters than the authentication codes generated via the mobile app.
- If you prefer not to use email to authenticate, click **Use other authentication methods** to select the Visa IntelliLink Spend Management app, 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.
Step 2b: Set Up Two-Factor Authentication – Visa IntelliLink Spend Management Mobile App

Obtaining authentication codes from the Visa IntelliLink Spend Management mobile app is also a supported option for 2FA into Visa IntelliLink Spend Management.

4. 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. *Please note that you should disregard / delete this email since you want to generate the authentication code via the mobile app.

5. To register to use the Visa IntelliLink Spend Management mobile app as the authentication code generator, select Use other authentication methods. From the drop-down, select Visa IntelliLink Spend Management app.

6. If you have not done so already, download and install the mobile app.
7. **Open and log in** to the *Visa IntelliLink Spend Management* app on your mobile device.

8. 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.

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

10. Your registration with the *Visa IntelliLink Spend Management* mobile app is now complete. For all future log ins to the *Visa IntelliLink Spend Management* desktop application you will be asked to enter your username and password, and repeat **Steps 7-9** above.

**Note:**

- A different logic is used to generate the codes sent via email than those generated in the mobile app. The authentication codes delivered via email may differ in length and/or be comprised of different types of characters than the authentication codes generated via the mobile app.

- If you want to change your authentication method, 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://identity.intellilink.spendmanagement.visa.com
2. On the Welcome to Visa IntelliLink Spend Management page, enter your Username and Password. Then click Log in.

![Login Page](image)

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.

![Code Verification](image)
4. Open the chosen method (either the email you received containing the code, or the Visa IntelliLink Spend Management mobile app) 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.
- Your account will be temporarily locked following 4 unsuccessful log in attempts. Your account will automatically unlock after 2 hours. You may wait 2 hours and try again, or contact your Administrator to unlock your account prior to that.
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.

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

Invalid Login Credentials

Following the guidance of the National Institute of Standards and Technology’s Digital Identity Guidelines, Visa’s Technical Security Requirements for Customer Identity & Access require proper handling of, and messaging about, failed login attempts.

Specifically, during unsuccessful login attempts the application must not disclose which component of the login process failed – username & password or authentication code. Additionally, the on-screen messaging should not indicate whether a username was not found, a password was entered
incorrectly, or an authentication code was invalid. The messaging must be generic, such as “Login failed.”

To comply with these requirements, Visa IntelliLink Spend Management employs specific login flows for the various invalid login credentials scenarios.

**Note:**
An account will be temporarily locked following four unsuccessful login attempts.

### User entering correct username with incorrect password or authentication code

The login flow will vary for users entering their correct username with an incorrect password, depending on whether they have previously registered for 2FA.

If they have **not** registered for 2FA, users entering their correct username with an incorrect password will be immediately returned to the *Welcome to Visa IntelliLink Spend Management* page and presented with a “Login failed” message prompting them to try again or contact their administrator.
If they have registered for 2FA, users entering their correct username with an incorrect password will be allowed to continue to the Two-factor authentication screen and prompted to enter the code retrieved from their registered method. Even if they enter the authentication code correctly, they will not be logged in as they failed to enter the correct password. Likewise, if the user enters a correct password, but an inaccurate authentication code, they will then be returned to the Welcome to Visa IntelliLink Spend Management page and presented with a “Login failed” message prompting them to try again or contact their administrator.
User entering incorrect username

In case of an incorrectly entered username, there are two possibilities:

1. The username cannot be identified as a valid user in any company instance.
2. The username may coincidentally match a valid user in another company instance. The matched username may or may not be registered for 2FA.

Users may be shown the Welcome to Visa IntelliLink Spend Management page and presented with a “Login failed” message prompting them to try again or contact their administrator.

Users may be shown the Two-factor authentication screen – even if they have not registered for 2FA. This screen will prompt them to try logging in again, if they believe they have reached this screen in error, or to contact their administrator. If they retry their login and enter the same incorrect username, they will be shown the same screen they saw the first time. If they retry and enter the correct username, password, and (if applicable) authentication code they will be authenticated and see their Home screen.
Note:

- The prompt may not match the registered method (if the user has already registered). Because they have incorrectly entered their username, the application has not accurately identified them and can only show a randomly generated prompt.

- Whatever authentication code is entered at this step will not pass as the Username has been entered incorrectly. After clicking **Verify** the user will be redirected to the *Welcome to Visa IntelliLink Spend Management* page and presented with a “Login failed” message.
Frequently Asked Questions

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 Visa has 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 July 20, 2019, 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.
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

Do the authentication codes expire?

Every authentication code sent by email expires after 10 minutes. You can generate/resend a new code 3 times per 1 minute. If none of those codes are used, you must then wait for 15 minutes to start generating codes again. The authentication codes retrieved from the VISM mobile app are valid for 30 seconds. After 30 seconds, a new code is displayed on the app screen and then you must enter that new code.

What if I don’t receive the email with my authentication code, or the authentication code expires before I receive the email and use the code?

VISM employs a micro-service that sends the email virtually instantaneously after the credentials have been presented. It may take some small time for your email to show up depending upon your email client, email server and network settings. If more than ten minutes has elapsed without an email, the code will no longer be valid. If this happens, click the Didn’t receive an email? Resend email link on the VISM login page to re-send the email with a new authentication code.

If you consistently receive the emails with the authentication codes after the ten minute expiration, you may choose to use the VISM mobile app to generate the codes instead. Please refer to Change Your Two-Factor Authentication Method above for more details.
What does it mean if I receive the message “Login failed. Try again or contact your administrator?”

If you receive this message, you likely entered an incorrect username, password, or authentication code. Try logging in again. If you receive the same message, incorrect password and authentication code attempts can be viewed by a VISM administrator by navigating to Reports > Usage and Monitoring > Audit Tracking, select Employee – Administration from the “Audit Area” drop-down list, enter the date range and click Search. Administrators can confirm the Username for an employee by navigating to Administration > Overview > Administration Overview > Employees.

What does it mean if I receive the message “The Resend email link is unavailable due to multiple attempts. Please try after some time once the Resend email link appears or contact your administrator for assistance?”

In order to deter fraudsters, the system will initiate a delay if repeated incorrect login credentials are presented. If you are seeing the message above, it likely indicates that either the Username or Password you entered are inaccurate. Incorrect password and authentication code attempts can be viewed by your VISM administrator. Administrators can also confirm your Username.

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?

Yes if the 2FA method is Email. An Email may be used as the authentication method for multiple user profiles. If yours is the Email Address 1 in multiple user profiles, you may receive the authentication codes for each profile at that email address.

No if the 2FA method is the Visa IntelliLink Spend Management mobile app. If you use the Visa IntelliLink Spend Management mobile app as the authenticator method, you will be prevented from changing users in the mobile app because 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 user profile (Change user) 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.

Example of VISM mobile app menu on a device that has more than one VISM user registered, and has not registered the VISM mobile app as the 2FA method for logging into the desktop website.

Example of VISM mobile app menu on that same device after the user has registered the VISM mobile app as the 2FA method for logging into the desktop website.

If you wish to use the mobile app to access more than one user profile, you will need to reset and re-register your 2FA method to Email. See Change Your Two-Factor Authentication Method above. This will deactivate the “one-at-a-time” relationship and allow you to ‘Change user’ 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 prior to the July 20 release (e.g. the user has already installed and logged into the mobile app on a device prior to the July 20 release), the user 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 to the mobile app.

- If the device was unlinked (e.g. the user has not installed and logged into the mobile app on a device prior to the July 20 release) and the user has not yet registered a 2FA method (e.g. the user has not yet logged into the desktop website after the July 20 release), the user will not be required to use 2FA when logging in to the mobile app. However, during the first login to the mobile app, the authentication method for logging into the desktop website will be defaulted to the VISM mobile app, and the user will see a message to notify them that the App is now the mechanism to use for 2FA. This means the next time the user logs into the desktop website, they will be prompted to generate their authentication code via the mobile app.

- If the device was unlinked (e.g. the user has not installed and logged into the mobile app on a device prior to the July 20 release) and the user has already registered Email as their 2FA method for logging into the desktop website, the user will receive an authentication code via email the first time they attempt to log into the mobile app, and will need to enter that code during their first login to the mobile app. *Please note that the authentication code will only need to be entered during the first login to the mobile app. All subsequent logins to the mobile app will not require an authentication code to be entered.

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 will 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.