2-Factor Authentication One-Time Pin (OTP)

Frequently Asked Questions

Table of Contents

2FA related questions 2

1. What is a 2-Factor Authentication (2FA) login process?
2. Why is there a need for a 2FA login?
3. How many channels of receiving OTP will I have?

General OTP Questions 2

1. How do I enable 2FA login process?
2. How do I add or change the number used for OTP delivery?
3. Are there any charges for receiving OTP via SMS and/or IVR?
4. What should I do if I do not receive the OTP after repeated attempts?

SMS OTP Specific Questions 2

1. How long will the SMS OTP take to be generated?
2. What is the format of the OTP delivered via SMS?
3. How many contact numbers can I register for SMS OTP?
4. Will I be able to get the IVR OTP if I am an overseas telecommunication user?

IVR OTP Specific Questions 3

1. Why is the IVR OTP implemented?
2. How long will the IVR OTP take to be generated?
3. What is the format of the OTP delivered via IVR?
4. How many contact numbers can I register for IVR OTP?
5. Will I be able to get the IVR OTP if I am an overseas telecommunication user?

Security Measures 4

1. My access to CitiManager has been disabled. How do I regain access?
2. What are the security measures that I should be aware of?

Appendix 5

1. Step by step guide for logging onto CitiManager using 2FA.
2FA Related Questions

1. What is a 2-Factor Authentication (2FA) login process?

   The 2FA login process consists of:
   1. What you know (Username, Password)
   2. What you have (One Time Pin tokens, Mobile Phones etc.)

   On top of the username and password, you will be required to input a One Time Pin (OTP) generated by the bank to log in to an online financial system.

2. Why is there a need for a 2FA login process?

   To ensure that you access sensitive information in a more secured environment, Citi implemented a 2FA login process for you to login to an online financial system using a second level of authentication. This is also in compliance with the Monetary Authority of Singapore (MAS) Technology Risk Management (TRM) guidelines to safeguard and protect sensitive information of our clients.

3. How many channels of receiving OTP will I have?

   There will be 2 channels for receiving OTP:
   1. SMS
   2. Interactive Voice Response (IVR)

General OTP Questions

1. How do I enable 2FA login process?

   No action is required on your part because the 2FA login process will automatically be implemented for you on the stipulated date as indicated in your communication letter.

2. How do I add or change the number used for OTP delivery?

   If your number is not updated, please call the customer service helpdesk at 800 181 1070 or (65) 6238 6367 to update your number.

3. Are there any charges for receiving OTP via SMS and/or IVR?

   Charges may vary according to the service provider you subscribe to and depending on the location where you are based in. Please check with your service providers for more details.

4. What should I do if I do not receive the OTP after repeated attempts?

   Your phone number might not have been updated or it can be due to other technical reasons. Please call the customer service helpdesk at 800 181 1070 or (65) 6238 6367 and they will assist you in resolving this matter.

SMS OTP Specific Questions

1. How long will the SMS OTP take to be generated?

   After selecting the 'text message' option, you will receive a SMS showing your OTP in approximately 10 seconds.

2. What is the format of the SMS OTP?

   The OTP received via SMS will take the form of 6 alphanumeric or numeric digits.

3. How many contact numbers can I register for SMS OTP?

   A maximum of 1 number can be registered for SMS OTP.

   1) A mobile phone number which will be reflected as ‘Call Mobile’ and ‘Text Message’ option.

   Refer to the appendix for more details.

4. Will I be able to get the SMS OTP if I am an overseas telecommunication user?

   Yes, you will be able to receive the SMS OTP even if you are an overseas telecommunication user.
**IVR OTP Specific Questions**

1. **Why is the IVR OTP implemented?**
   As part of Citi’s drive in continued innovation and process enhancements, IVR gives you more options to receive your OTP.

2. **How long will the IVR OTP take to be generated?**
   After selecting the ‘Call Office’ or ‘Call Mobile’ option, you will receive a phone call reading out the OTP in approximately 10 seconds.

3. **What is the format of the IVR OTP?**
   The OTP received via IVR will take the form of 8 numerical digits.

4. **How many contact numbers can I register for IVR OTP?**
   A maximum of 2 numbers can be registered for IVR OTP.
   - 1) An office number or residential number and will be reflected as ‘Call Office’ at the user selection page.
   - 2) A mobile phone number which will be reflected as ‘Call Mobile’ and ‘Text Message’ option.

   Refer to the appendix for more details.

5. **Will I be able to get the IVR OTP if I am an overseas telecommunication user?**
   Yes, you will be able to receive the IVR OTP even if you are an overseas telecommunication user.
Security Measures

1. My access to CitiManager has been disabled. How do I regain access?

If you have been logged out of CitiManager, please call the customer service helpdesk at 800 181 1070 or (65) 6238 6367 to reset your access.

2. What are the security measures I should be aware of?

Password Security
- Do not reveal the One Time Password (OTP) generated to anyone.
- Password should not be based on username, personal telephone number, birthday or other personal information.
- Password must be memorized, not recorded, kept confidential and not be divulged to anyone.
- The same password should not be used for different websites, applications or services, particularly when they relate to different entities.

Software Security
- Ensure that anti-virus, anti-spyware, and firewall software is deployed on your personal computers, especially when your personal computers are linked via broadband connections, digital subscriber lines, or cable modems.
- Update the anti-virus and firewall products with security patches or newer versions on a regular basis.
- Do not install software or run programs of unknown origin.

Usage Security
- You should check the authenticity of the CitiManager website by comparing the URL with its digital certificate or by observing the indicators provided by an extended validation certificate.
- Check that the CitiManager website address changes from http:// to https:// and a security icon that looks like a lock or key appears when authentication and encryption is expected.
- Terminate a login session if a SSL certificate does not belong to Citi and a warning is given to this effect.
- Log off the online session and turn off the computer when not in use.
- Do not select the browser option for storing or retaining user name and password.
- Check your commercial card accounts and transactions frequently and report any discrepancy.
- Do not disclose personal, financial or credit card information to little-known or suspected websites.
### Appendix

1. Step by step guide for logging onto CitiManager using 2FA.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>A)</strong> The landing page for CitiManager</td>
<td><strong>B)</strong> The options to receive your OTP. Note only the last 4 digits of your phone number will be shown for security reasons</td>
</tr>
<tr>
<td><img src="image1" alt="" /></td>
<td><img src="image2" alt="" /></td>
</tr>
</tbody>
</table>

**C)** Sample screenshot of the SMS OTP

**Ci)** Sample screenshot of the IVR OTP

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>D)</strong> Input your OTP here</td>
<td></td>
</tr>
<tr>
<td><img src="image3" alt="" /></td>
<td></td>
</tr>
</tbody>
</table>