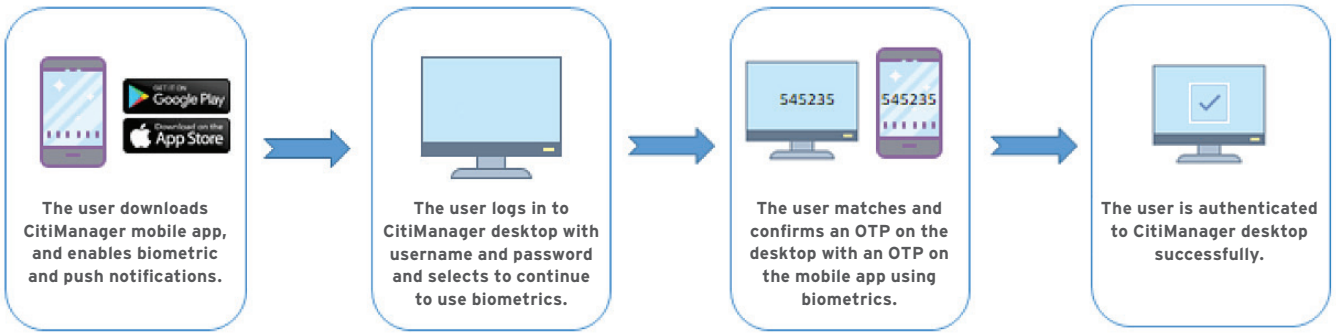
New Multi-Factor Authentication Using the CitiManager® Mobile App

Frequently Asked Questions

Effective August 15, 2020, Citi launched an upgraded version of its Multi-Factor Authentication (MFA) login capability to meet the most current National Institute of Standards and Technology (NIST) standards, as required under the GSA SmartPay® 3 master contract. This new NIST compliant MFA login capability will require CitiManager desktop users to use the CitiManager mobile application to access their One-Time Password (OTP). Below is a diagram that illustrates the new NIST compliant process for generating the OTP using the CitiManager Mobile app.



1. What is Multi-factor Authentication (MFA)?

MFA is an authentication method where a user must present two or more pieces of evidence before granted an access to the system. The principles for deploying both a secure and intuitive MFA capability are as follows:

1. Knowledge (something the user and only the user knows) e.g. User ID, password
2. Possession (something the user and only the user has) e.g. mobile device, security token
3. Inherence (something the user and only the user is) e.g. biometrics

2. Why is MFA important?

MFA drastically reduces the occurrences of online identity theft and online fraud. It is harder for bad actors to gain access to the system because it requires two or more pieces of evidence.

3. Why must Citi use MFA for login?

The GSA SmartPay® 3 Master Contract requires card issuers to follow NIST system security standards. Citi is required to offer a NIST compliant login capability via MFA that meets the NIST standards.

4. What is the new MFA solution for CitiManager desktop?

The new MFA solution will use the CitiManager mobile application and push notifications to deliver OTP. The user will match the OTP displayed on a mobile app with the OTP on the desktop screen to complete authentication.

5. Is the new MFA solution NIST compliant?

Yes, the new MFA solution is NIST compliant. It uses strong device binding, biometric authentication and time bound code to generate the OTP.

There is no change to the CitiManager process for logging in using the standard User ID and password.

6. Why change to new MFA solution?

The OTP via email and voice are not NIST compliant. Recently, NIST declared OTP via SMS is also not compliant. Two primary risks associated with SMS OTP are: 1) SIM swapping, and 2) Exposed OTP on the lock screen of users' mobile phones. The CitiManager mobile application protects against these risks when using MFA to generate the OTP.

7. Is the new MFA specific to GSA SmartPay® 3 clients?

The GSA SmartPay® 3 contract requires the use of NIST login standards, which includes 100% of user logins conducted through MFA and OTP, and excludes options such as SMS and email. Citi is meeting this requirement using the CitiManager mobile application, which will also be the commercial standard option for our Corporate and Public Sector clients in North America.

8. How can the new MFA be turned on for each agency?

The new MFA can be turned on at the company level in CitiManager. If the agency is setup as different companies for each program, then it can be turned on/off at a program level. Please note that turning off new MFA solution will make an agency non-NIST compliant.

9. Will the users receive an OTP via the new MFA each time they login to CitiManager when adopting to NIST standards?

Yes, every time a user, an A/OPC or a cardholder logs in to CitiManager, they will receive an OTP via new MFA in accordance with the NIST standard.

10. When will a user receive an OTP via email/voice/SMS?

Email, Voice and SMS are not NIST compliant. Email and SMS are considered high risk in accordance with Citi's security policies and will not be commercially available after August 15th, 2021. Agencies that are currently using email OTP as their NIST exception will have this capability for 1 year to allow for change management. Agencies currently using SMS as the prior NIST compliant MFA, will also be given until August 15th, 2021.

11. Why is email OTP considered a high risk and not NIST compliant?

The email OTP is not a NIST compliant solution because the method does not prove possession of a specific device. The user could use the same desktop to login to CitiManager website and their emails. In case of the user's desktop is compromised, the hacker might have access to CitiManager and an email OTP. The email OTP solution could indirectly jeopardize the security of a user's email messages.

12. During the transition to CitiManager mobile application for MFA/ OTP, can my agency also keep the current OTP delivery methods?

To assist agencies in their campaign to cardholders and non-cardholders to adopt the CitiManager mobile application, agencies choosing the NIST compliant CitiManager mobile application will also be able to continue to receive OTP via voice message and if currently configured, email OTP. The SMS OTP will not be supported if an agency wishes to use the CitiManager mobile application.

13. Will the new MFA via the CitiManager Mobile App have the capability to work with phone extension numbers?

The new MFA via CitiManager mobile app does not require a phone number for use. If an agency requests an exception to NIST Standards, phone numbers with an extension are not supported.

14. I already use CitiManager mobile app today. Does this affect the way I login to CitiManager mobile app?

The new MFA solution will be required for only CitiManager desktop login. The user must download CitiManager mobile app, and enable biometrics and push notifications.

If an agency requests an exception to NIST standard, then there will be no change in the way you login to the CitiManager mobile app.

The user should update the CitiManager mobile app periodically to make sure it is up to date.

15. How long does a user have to validate OTP before it times out?

The OTP can be used for 100 seconds from the time it is generated. After expiration, the user will need to request a new OTP. When the user receives an OTP, the automated message will advise the user the validity period for that OTP.

New MFA solution uses the 100-second timeout that matches with the existing non-NIST compliant SMS OTP solution.

16. Will Citi consider extending the 100-second timeout to 120-second timeout for CitiManager mobile application OTP?

100 seconds is Citi's security standard and cannot be extended. Please note the CitiManager mobile application authentication takes less time than voice, SMS, and email. The users will not have to enter the OTP they receive via the CitiManager mobile application. The users will need to pick up their phone, login to the CitiManager mobile application with fingerprint and confirm the OTP number shown on their phone matches with what is displayed on the CitiManager desktop screen. No data entry is required.

17. Is the new MFA solution applicable to A/OPC?

Yes, the new MFA solution is applicable to all cardholders and A/OPCs who want to login to CitiManager desktop using NIST compliant solution.

A/OPCs need to download the CitiManager mobile app to use the new MFA solution. Please keep in mind that currently CitiManager mobile app does not offer any functionality for A/OPCs. The A/OPCs will use the mobile app to retrieve the OTP. They will also be able to perform "Forgot Username" and "Forgot Password" functionality via the mobile app.

18. Can you summarize the NIST compliant vs non-compliant MFA solution?

NIST Compliant	NIST Non-compliant
OTP received through CitiManager mobile app with biometric and push notification enabled.	Voice call to phone numbers on file. SMS. Email to government domain.

19. What is the impact for Non-Cardholders with multiple roles (A/OPC and AO) with multiple CitiManager Non-Cardholder logins?

CitiManager and the CitiManager mobile app look at usernames to confirm the OTP, allowing users to have multiple Non-Cardholder IDs and have a seamless OTP experience. Whatever username is being used on CitiManager desktop will need to be the same username used to log in to the app for OTP to work. Users can log in as an AO in CitiManager desktop and then as an AO in the app and it will work. A minute later, the same user can log in to CitiManager desktop as an A/OPC and then as an A/OPC in the app and it will work.

2062308 11/21