

FREQUENTLY ASKED QUESTIONS

The following FAQs have been developed to help answer many of the common questions about mobile token from both Web or Security Administrators and users.

As a reminder, Web or Security Administrators can assign mobile tokens to users through the Administration Console of the MUFG Exchange landing page. We recommend that clients migrate to the mobile solution if possible as it is a more convenient and secure method of using a security token. It is also faster and more efficient to implement a mobile token.

If you need additional assistance, please contact Transaction Banking Technical Client Services at 844-544-0387, select Option 2, 8:00 a.m. to 7:00 p.m. ET, Monday through Friday, excluding federal holidays, or via email at TB-technicalsupport@us.mufg.jp

ALL USERS

Q: What is the difference between using a physical token and a mobile token?

A: Whether you are using a physical or a mobile token, you will use the information the same way. When prompted for your security token, you will need to enter your PIN plus the 6-digit number displayed on either the physical token or on the token app on your mobile device. In either case, to help ensure the highest level of security that a token can provide, we recommend that you commit your PIN to memory and do not write it down or save it on your phone.

The main difference in using a mobile token over a physical token is the added convenience and security. With the mobile token, it is available wherever you have your mobile device and you do not have to carry an additional piece of hardware for banking transactions.

With respect to security, the token vendor RSA, an industry leader, has included several features that help keep your token information private. For example:

- The RSA app will not provide a token code if the phone's operating system has been compromised i.e. Jailbroken for IOS or Rooted for Android.
- Once a token is activated on the app, it is protected with unique application data that cannot be migrated to another device.
- If an unauthorized user or malware attempts to copy the token database to another machine or device, the user cannot obtain a token codes or the app appears as not having an active token.
- If the user obtains a new device, the software token must be reissued.
- If a screenshot is taken of a code, the app will post a warning alert.
- When a user shares their mobile screen with apps like Quicktime, the app will hide the code from being seen.

(continued)

WEB OR SECURITY ADMINISTRATORS

Q: We received physical tokens but would like for some users to have mobile tokens, how do I get mobile tokens?

A: Simply go to the Administration Console of the MUFG Exchange and select the user profile. Then click on the Assign Security Token button and then select the mobile option. Once the mobile token is activated the user will receive a notice in their Action Items widget on the MUFG Exchange landing page. From there, they can click on the link and follow a few steps to activate the token. Please note that users cannot have both a physical and mobile token. For more information about assigning mobile tokens, please refer to the [online user guide](#).

Q: Can my organization have users that use physical tokens and users who use mobile tokens?

A: Yes. Your organization can have a blend of users who use physical and mobile tokens. But a single user ID can have only a physical OR mobile token—not both.

Q: I have multiple User IDs; can I use one token?

A: No. For security purposes, you must have a different token for each of your User ID profiles. If you use a mobile token, you can manage up to 10 tokens on the RSA SecurID Software Token app. The app allows you to assign a name or ID for each token, so it is easier to use and identify the appropriate token. If you use a physical token, you will need a separate token for each User ID.

MOBILE TOKEN USERS

Q: How do I activate a mobile token?

A: Once you have been assigned a mobile token, you will see a task in your Action items widget on the MUFG Exchange landing page. Click on the link and you will be taken to the activation page.

Please follow a few easy steps detailed on the screen and you should be able to activate your mobile token in 10 minutes or fewer. Please make sure you have your mobile device available before beginning the activation steps.

For more details, please refer to the [online user guide](#).

Q: I use tokens for wires initiated via telephone/Direct Access and the online wires service, can I get a mobile token?

A: Yes. A Web or Security Administrator for your organization can assign a mobile token to you through the MUFG Exchange.

Q: I have activated my mobile token, but the activation link is still live on my Action Items widget on the landing page. Why is that? Did I do something incorrectly?

A: No, you have not made a mistake. Once you have received the confirmation that your token has been activated correctly, you do not need to take any additional steps.

The link will remain live so you can conveniently activate a new token if you lose or replace your mobile device.

Q: Do I need to use data on my personal device when using the mobile token?

A: While you will need to use data in order to download the RSA SecurID app to your phone, you do not need to use any data for the app to generate a security code. The app will generate a code even if you have no internet connection.

Q: I am located outside of the U.S.; will I be able to download the app from the Apple App and Google Play stores here?

A: Yes. The RSA SecurID Software Token app is available globally on the Apple App and Google Play stores.

(continued)

Q: Can I use the same PIN as I have for my expiring Physical token?

A: Yes. You can use the same PIN, however, for added security we recommend that you change your mobile token password.

Q: I have already activated my mobile, but I really wanted my physical token what do I do?

A: Please contact your company's Web or Security Administrator. They can visit the MUFG Exchange and assign a physical token to you. You cannot have both a physical and a mobile token, therefore, once you activate your physical token, your mobile token will automatically become inactive.

Q: I activated my mobile token and received a physical token in the mail, what do I do now?

A: Your mobile token is still active, please return the token to your Web or Security Administrator so it can be reassigned as necessary. If you are not currently able to give it to the Web or Security Administrator, please hold on to it until such time that you are able to do so.

PHYSICAL TOKEN USERS

Q: The token was sent to the wrong address, what do we do?

A: Please send us a Secure Message for Technical Assistance from the MUFG Exchange landing page. In the body of the message please indicate the need for a replacement physical token with the following information:

- Username and User ID
- Phone number
- Correct mailing address where the token should be sent.

Note: Tokens are sent using an express mail service and require a street address.
We cannot deliver to a Post Office Box.

Q: My security token has expired; how do I get a new token?

A: For your convenience, a physical replacement token has been sent to your business address we have on file. The instructions for activating your token are included with the new token.

MUFG Bank is now able to offer mobile tokens for qualifying clients. If you prefer to use a mobile token instead of a physical token, please contact your Web or Security Administrator, who can enable one online for you.

Q: How do I activate my physical token?

A: Please refer to the token activation guide included with your replacement token. You will need to go to the MUFG Exchange to create a PIN.

Q: My token was shipped to the wrong address and I need to perform transactions now. What can I do?

A: is the benefit of our new mobile token option. You can activate a mobile token quickly and continue to use the mobile token in lieu of a physical token. Note that you cannot have both a mobile and physical token. Therefore, if you prefer a physical token, the mobile token will automatically be de-activated when you activate your physical token.

Q: If I activate my physical token now and I change my mind and want a mobile token later what do I do?

A: Please contact your company's Web or Security Administrator and they can go to the MUFG Exchange and assign a mobile token to you.

You cannot have both a physical and a mobile token, therefore, once you activate your mobile token, your physical token will automatically become inactive.

Return the token to your Web or Security Administrator so it can be reassigned as necessary. If you are not currently able to give it to the Web or Security Administrator, please hold on to it until such time that you are able to do so.