

CitiDirect® Mobile Token Enablement Guide for Security Managers

The CitiDirect mobile token is a new, upgraded version of mobile token for CitiDirect desktop and mobile login. CitiDirect mobile token is embedded within the CitiDirect mobile app and offers an intuitive and quick activation process.

Note: The existing security procedures that are currently in place relating to mobile application based soft tokens will continue to apply with respect of the CitiDirect mobile token; nothing has changed in this regard.

To streamline access to CitiDirect, enabling the mobile token is now easier for you and your organization.

Navigation

The navigation has been simplified, making it easier to switch between functions. Clicking on **“Self Service”**, then **“Client Administration Service”**, followed by **“Users & Entitlements”** loads a left-hand navigation panel that can be used to access all CitiDirect security manager functions.

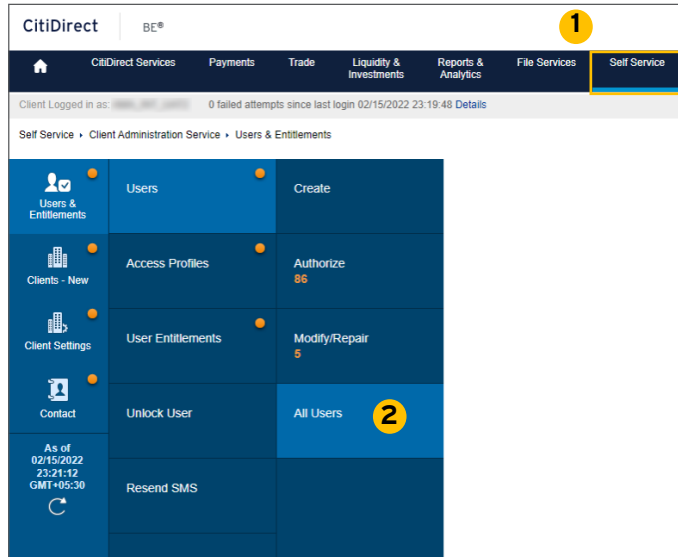
- To use the left-hand navigation panel, hover over a section (e.g. **“Users & Entitlements”**), and options for which you are entitled will be available. Hover over the next item (e.g. Users), and options such as **“Create”**, **“Authorize”**, **“All Users”** will appear (based on your entitlements). Orange indicators within each option box will let you know if you have any records pending authorization or repair or pending in draft status.

Table of Contents

- I. Steps for Enabling CitiDirect Mobile Token for Your Organization’s Users
- II. Steps for Enabling “Default Credential Type” & “Allow Users to Request Mobile Token”
- III. Steps for Reactivating the CitiDirect Mobile Token for Users
- IV. Steps to Enable/Disable CitiDirect Mobile Access

I. Steps for Enabling CitiDirect Mobile Token for Your Organization's Users

To make logging into CitiDirect easier, enable your users with the mobile token credentials by following the simple steps below:



1. Click on “Self Service”, then “Client Administration Service”, followed by “Users & Entitlements” from the mega menus at the top of the screen (see #1 above).
2. Select the “User & Entitlements/Users/All Users” from left hand menu (see #2 above).
3. Make sure that each user has the appropriate “Role” selected from the dropdown menu

All Users: Details ^ 38 of 50 v

Processed

Complete the sections below to define user information, assign credentials and associate entitlements. * = Required Field

<p>* First Name ⓘ</p> <input type="text"/>	<p>Middle Name ⓘ</p> <input type="text" value="Enter name from official documents"/>	<p>* Last Name ⓘ</p> <input type="text"/>
<p>Nickname ⓘ</p> <input type="text"/>	<p>Dept. / Division ⓘ</p> <input type="text"/>	<p>* User Role ⓘ</p> <div style="border: 2px solid orange; padding: 2px;"> <input type="text" value="Security Manager"/> </div>

4. Scroll to Section 1: "User Information", and ensure the mobile number is accurately entered.

1 - User Information This section is required

Enter general user information, address and contact details.

User Alias: Status: Active Inactive User Manager:

Initials: Alternate Login ID:

Employee ID:

Address Details

Click 'The above address is correct' check-box to confirm that address details are correct.
Click 'Create New Address' to enter new address details.

Building/Floor/Room: Street Address 1: City:

Country: State / Province / Territory: Postal Code / Zip Code:

Time Zone: Eastern Time (US & Canada) (EST)

The above address is correct

[Create New Address](#)

Contact Details

Telephone: Mobile Country Code/Telephone: Email:

Allow Access

Date: Time: Days of the week:

5. Scroll to Section 2: "Credentials", and add "Mobile Token" (see #5 below).

All Users: Details

Processed

Complete the sections below to define user information, assign credentials and entitlements.

First Name: CHARU Middle Name: (Enter name from official documents)

Nickname: Dept. / Division:

> 1 - User Information

< 2 - Credentials

The following credentials will be assigned to this user. Use Add Credentials to add more.

Credential Type	Action
Challenge/Response - Host 9	<input type="button" value="Link Existing Safeword Card"/>
Portal - Secure Password	

> 3 - User Entitlements

Expand All Collapse All

Reset User
Select the Reset User checkbox and Submit to unlock the User.

Subscription Status

Select Credential Type (28)

Search:

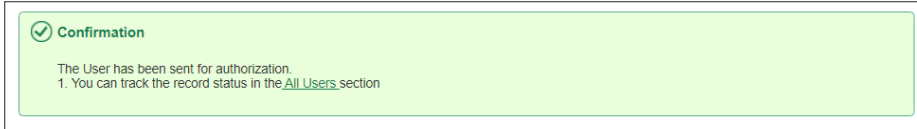
Credential Type:

List of Available Credential Types

Credential Type	Credential Description
<input checked="" type="checkbox"/> Mobile Token	QR Code Login
<input type="checkbox"/> IVR CIN	Interactive Voice Response Credential
<input type="checkbox"/> Secured Password ID	CitiDirect Services Secure Password ...
<input type="checkbox"/> Challenge/Response - Host 9	Safeword Card Login using Host 9
<input type="checkbox"/> CBII ID	CBII App Credential
<input type="checkbox"/> SpeedCollect ID	SpeedCollect App Credential
<input type="checkbox"/> Tax & Child Support Payment ID	US Tax & Child Support App Credential

6

6. Submit the record (see #6 above).



Note: Another security manager will need to AUTHORIZE the change before it goes into effect.

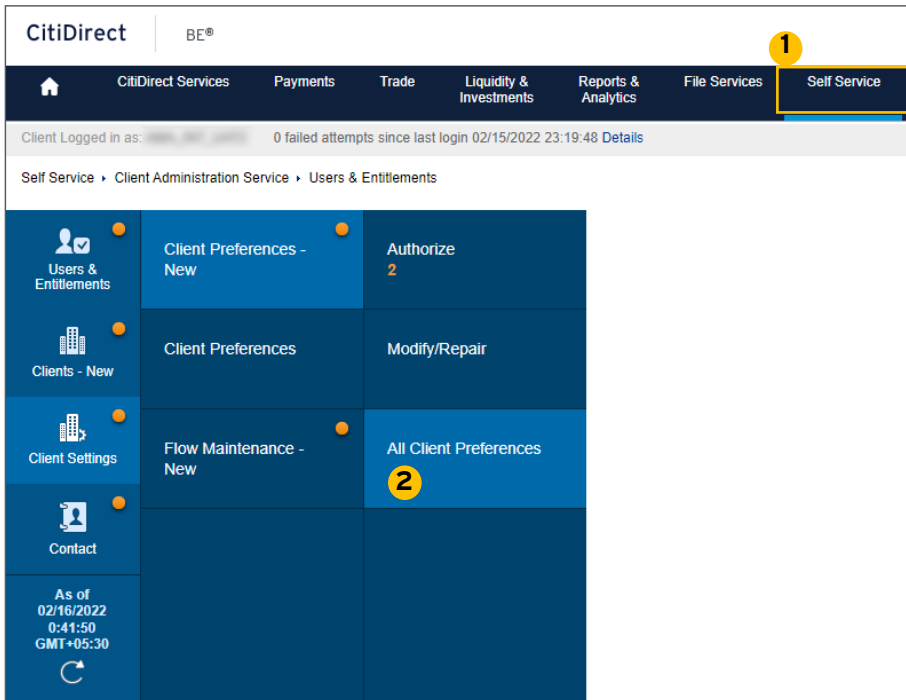
7. Once approved, an email will be sent to the USER with instructions on how to activate the mobile token.

Note: At this time, existing users can continue utilizing other credentials (e.g. MobilePASS, SafeWord) after the mobile token is added. Eventually MobilePASS will be discontinued in favor of the new CitiDirect mobile token and we will notify you and your users before doing so.

II. Steps for Enabling “Default Credential Type” & “Allow Users to Request Mobile Token”

Default Credential Type can be selected in Client Preferences to set the mobile token as the default credential at the time of new user creation:

1. Click on “Self Service”, then “Client Administration Service”, followed by “Client Settings” from the mega menus at the top of the screen (see #1 below).



2. Select the “Client Settings/Client Preferences – New/All Client Preferences” from left hand menu (see #2 above).

3. Select "Global" (see #3 below).

Self Service > Client Administration Service > Client Settings > Client Preferences: All

Save As Print

All Client Preferences (18)

Show Search Criteria

All (1 - 18 of 18) (As of 11/12/2020 15:31:51 GMT)

Service 1 ▲	Worklist Status 2 ▲
[Redacted]	Processed (Draft)
[Redacted]	Processed
[Redacted]	Processed
[Redacted]	Processed
[Redacted]	Processed (Draft)
[Redacted]	Processed
[Redacted]	Processed
[Redacted]	Processed (Draft)
[Redacted]	Processed
[Redacted]	Processed (Draft)
Global 3	Processed (Draft)

4. Select "Default Credential Type" (see #4 below).

All Client Preferences: Details 11 of 22

Customize system behaviour for client and user. * Required Field

Global
Processed

* Date Format: MM/DD/YYYY

* Amount Format: English(US,UK)- 12.345.53

Default Language: English

Email Domain: [Empty]

Default Credential Types 4: Mobile Token

Allow Users to Request Mobile Token 5

Allow Users to Request MobilePASS

Other

Certificate Authority Type: Entrust Certificate

Allow Mobile Access

Display Access Administrator List

Digital Signing Document Type: DocumentTypeLookup99DigitalS

Delete Public Report: [Empty]

6

Submit Save Delete Cancel

5. If your organization's "Default Credential Type" is set to "Mobile Token", the "Allow Users to Request Mobile Token" client preference will automatically be selected (see #5 above). Security Managers (maker/checker) can always uncheck the "Allow Users to Request Mobile Token" client preference to disable the user self-request option if it is no longer desired.

Note: In some cases, clients may have this option pre-selected by Citi Handlowy to help with the transition to the upgraded mobile token.

Once "Allow Users to Request Mobile Token" is enabled, existing users may benefit from multiple user-driven options:

If "Allow Users to Request Mobile Token" is selected, existing MobilePASS users can request the mobile token without further Security Managers' approval. An email notification will be sent to Security Managers when users request mobile token. This is available at:

1. CitiDirect > My Settings/Authentication
2. CitiDirect banner presented at logout
3. Mobile banner upon login

Existing SafeWord card and/or Biometric authentication users who are not also MobilePASS users will require a Security Manager's approval before enablement. This is available at:

1. CitiDirect > My Settings/Authentication
2. CitiDirect banner presented at logout
3. Mobile banner upon login

Existing Mobile Token users can request the reactivation of Mobile Token (i.e. to transfer it to a new device) without further Security Managers' approval. An email notification will be sent to Security Managers when users request reactivation. This is available at:

1. CitiDirect > My Settings/Authentication
2. Mobile > Settings > Switch to a New Phone

6. Submit the record as required (see #6 above).

Note: Another Security Manager will need to AUTHORIZE the change before it goes into effect.

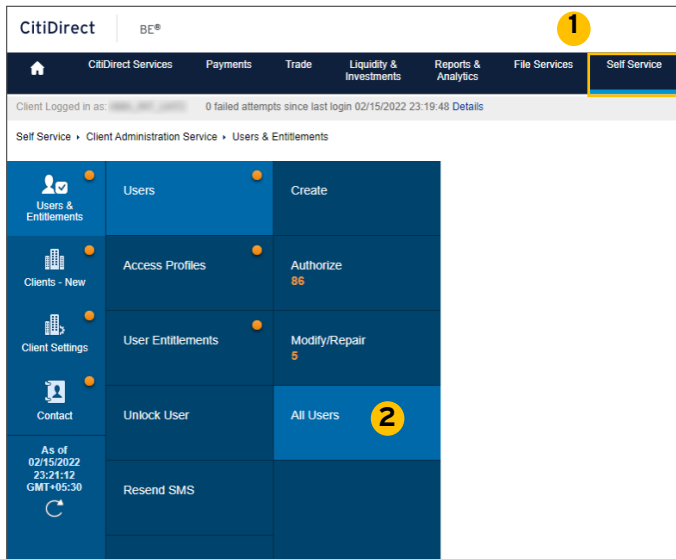
III. Steps for Reactivating the CitiDirect Mobile Token for Users

Reactivation might be required in the following scenarios:

- Activation code is expired (valid for 10 days)
- User forgot the mobile token Passcode
- User needs to re-install the CitiDirect Mobile Token on a new device
- User cannot locate the activation email
- User lost the device

Note: Users can now resend the activation email during the activation process by selecting **“Resend”** option and reactivate the mobile token from the Mobile app directly, by selecting **“Switch to a New Phone”** option in the Settings.

Reactivate mobile token credentials for logging into CitiDirect by following the simple steps below:



1. Click on **“Self Service”**, then **“Client Administration”** Service, followed by **“Users & Entitlements”** from the mega menus at the top of the screen (see #1 above).
2. Select the **“User & Entitlements/Users/All Users”** from left hand menu (see #2 above).

3. Select the user who requires re-activation by clicking on the user name (see #3 below).

User name	User Alias	Worklist status	Access Profiles	User Status	Credential Registration	Mobile Access
ACME, TES ...		Draft	1	Active		YES
ACME, TES ...		Draft	1	Active		YES
ACME, TES ...		Draft	1	Active		YES
ACME, TES ...		Draft	1	Active		YES
[Redacted]		Processed	15	Active		YES
[Redacted]		Pending Aut...	22	Active		YES
[Redacted]		Processed (...)	1	Active		YES
[Redacted]		Processed	84	Active		YES
[Redacted]		Processed	13	Active		YES
[Redacted]		Processed	14	Active		YES

4. Scroll to Section 1: "User Information", and ensure the Telephone and Mobile Country Code/Telephone are accurately entered (see #4 below).

1 - User Information This section is required

Enter general user information, address and contact details.

User Information

User Alias: [Text Field] * Status: Active Inactive User Manager: [Search Field]

Initials: [Text Field] Alternate Login ID: [Text Field] * Employee ID Type: [Dropdown Menu]

* Employee ID: [Text Field]

Address Details

Click 'The above address is correct' check-box to confirm that address details are correct.
Click 'Create New Address' to enter new address details.

Building/Floor/Room: [Text Field] Street Address 1: [Text Field] City: [Text Field]

* Country/Jurisdiction: [Dropdown Menu] State / Province / Territory: [Text Field] Postal Code / Zip Code: [Text Field]

* Time Zone: [Dropdown Menu]

* The above address is correct

[Create New Address](#)

Contact Details

* Telephone Code/* Subscriber no./ Ext.: [+91 Ind] [Text Field] [Text Field] * Mobile Country Code/Telephone: [+91 Ind] [Text Field] * Email: [Text Field]

5. Scroll to **Section 2: Credentials**, select “Action” and “Re-activate Mobile Token” (see #5 below).

6. Submit the record (see #6 above). **Note:** Another Security Manager will need to AUTHORIZE the change before it goes into effect.

7. Notification will be sent to the User via email. The User should follow the instructions in the email to activate mobile token.

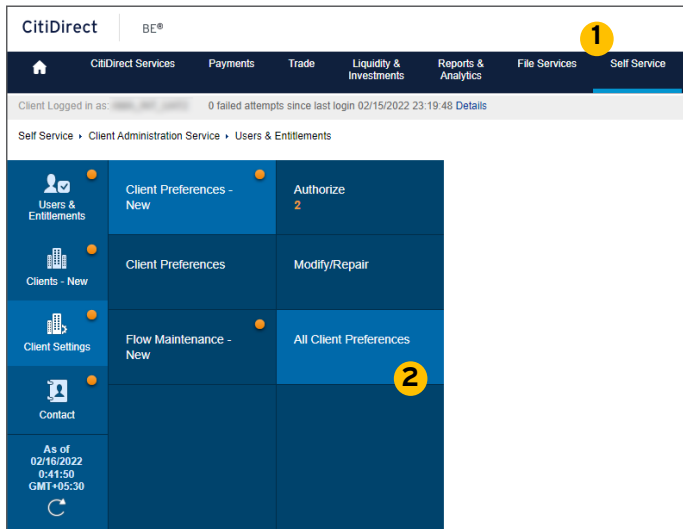
To support the transition for existing MobilePASS users, MobilePASS reactivation will no longer be available for clients enabled with Mobile Token. Users will be assigned with Mobile Token as a new login credential instead of reactivating MobilePASS.

IV. Steps to Enable/Disable CitiDirect Mobile Access

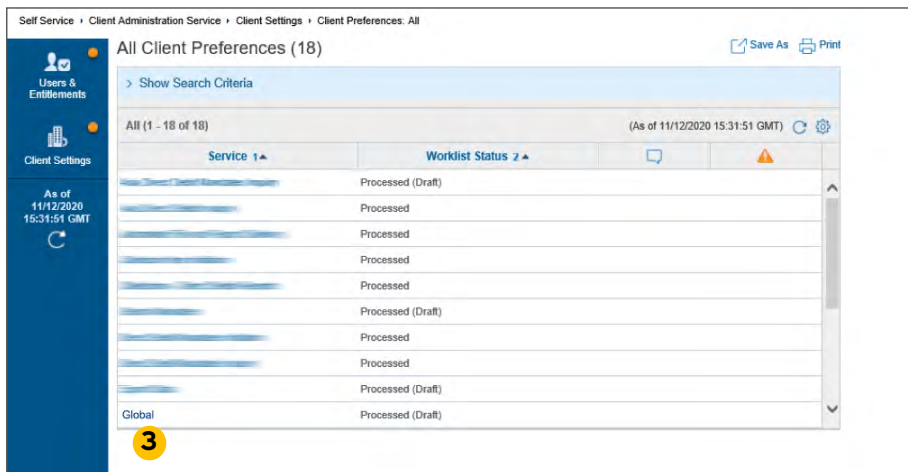
As a Security Manager you may enable/disable the option to login to CitiDirect Mobile for all or selected users in your organization.

A. Steps to Enable/Disable CitiDirect Mobile Access for All Users

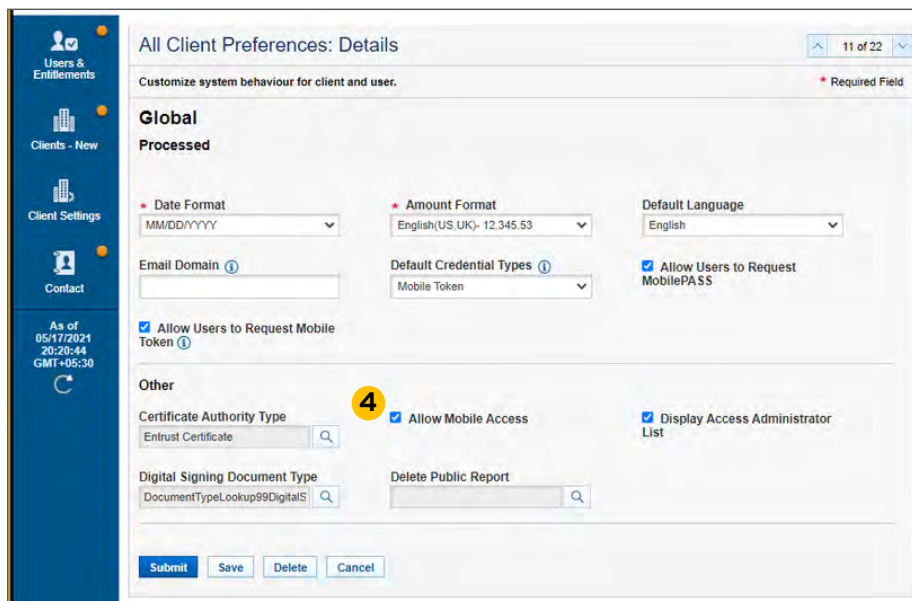
1. Click on "Self Service" (see #1 below), then "Client Administration Service", followed by "Client Settings" from the mega menus at the top of the screen.



2. Select the "Client Settings/Client Preferences – New/All Client Preferences" (see #2 above) from left hand menu.
3. Select "Global" (see #3 below).

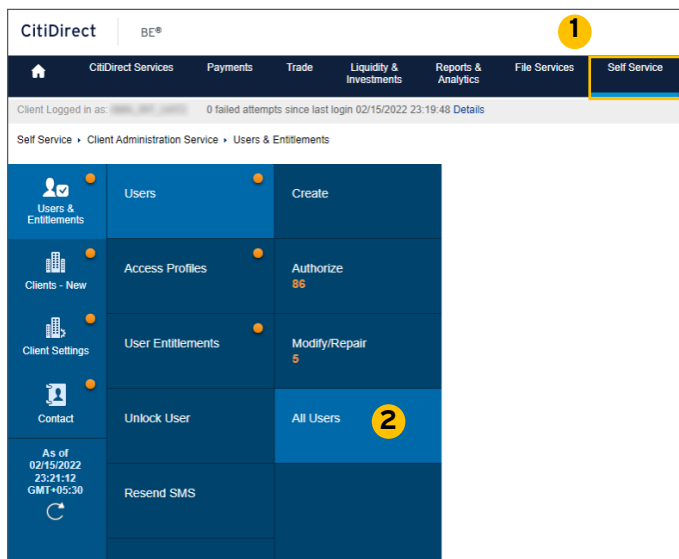


4. Select/deselect "Allow Mobile Access" (see #4 below) as required.



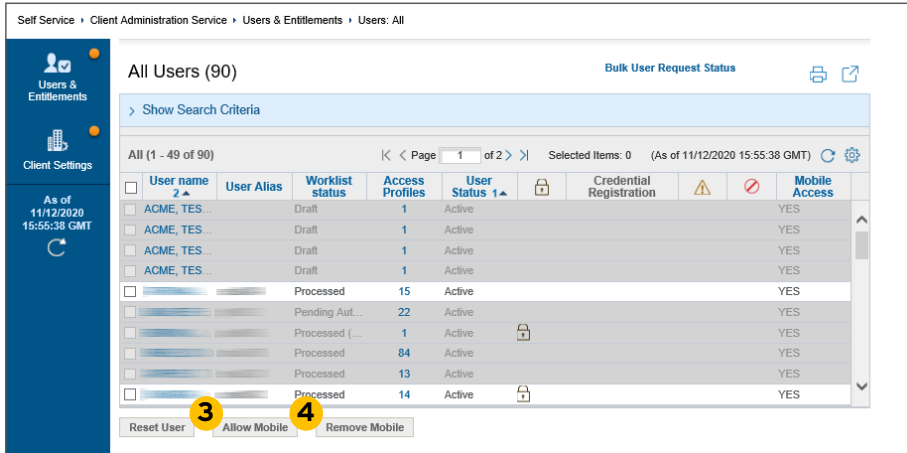
B. Steps to Enable/Disable CitiDirect Mobile Access for Selected Users

To be able to enable/disable CitiDirect Mobile Access for selected user, "Allow Mobile Access" must first be enabled in "Client Preferences" (see point A above).



1. Click on "Self Service", then "Client Administration Service", followed by "Users & Entitlements" from the mega menus at the top of the screen (see #1 above).
2. Select the "Users & Entitlements/Users/All Users" from left hand menu (see #2 above).

3. Select the user who requires changes on Mobile access and choose between “Allow Mobile” or “Remove Mobile” as required (see #3 and #4 below).



Mobile Access is no longer required for mobile token or biometrics to work on the CitiDirect mobile app as an authenticator. Security Managers may decide to enable/disable Mobile Access based on their preferences for the mobile services access for the users.

Click to learn more about the [CitiDirect mobile token](#) or [review FAQs](#).