Connecting to and Managing RAMP

Table of Contents

CONNECTING TO AND MANAGING RAMP 1
Downloading Citrix Receiver 1
Logging In to RAMP 5
FileSaver 7
FileMover 8
TESSITURA SELF-SERVICE TOOL 10
Account Page 12
Manage Organization 14
Users *14*
Assigning and Unassigning RAMP User Accounts *17*
Assigning , Unassigning, and Unlocking Tokens *20*
URL Endpoints *22*
Sync Token 23
MOBILE RAMP TOKENS 25
Mobile Token Installation for iOS 26
Mobile Token Installation for Android 28
Using Mobile Tokens 31

NOTICES

Connecting to and Managing RAMP

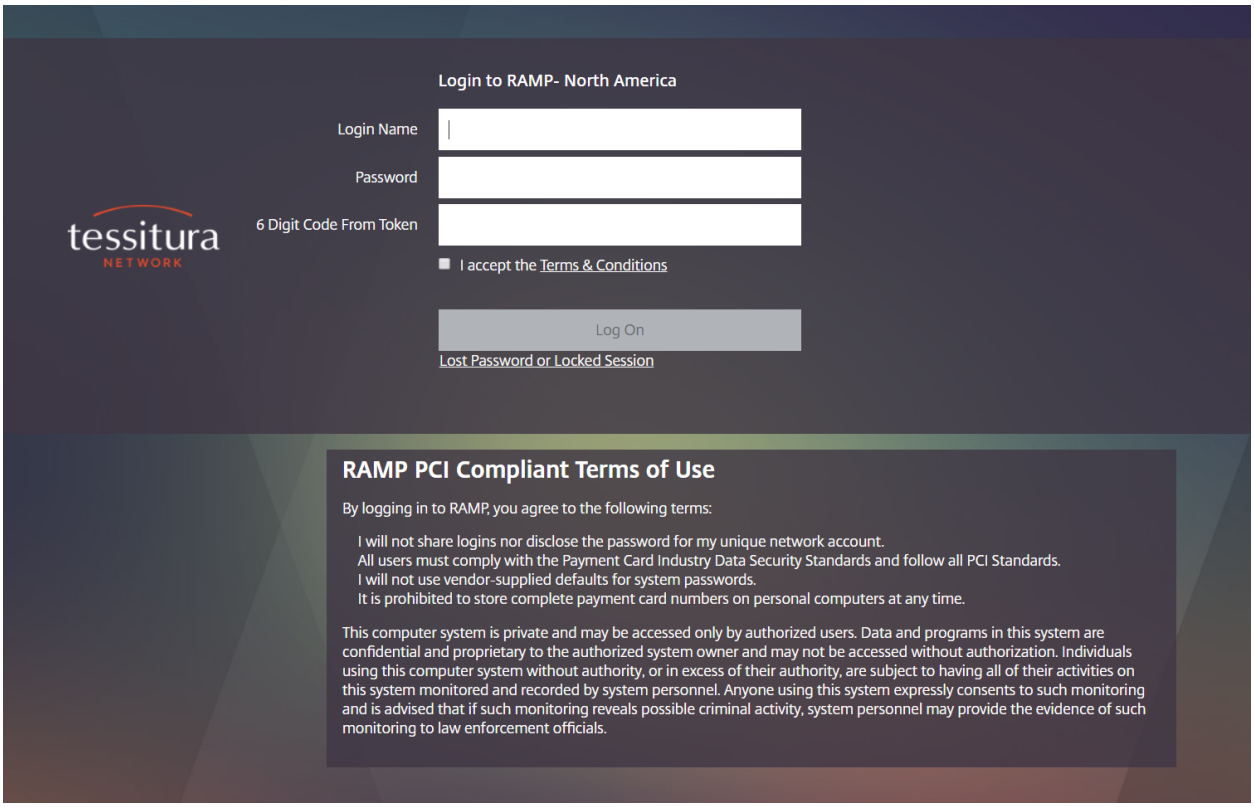
Tessitura's Remote Access Managed Plan (**RAMP**) service deploys Tessitura via the cloud. This document details how to connect to your RAMP instance, how to use the Tessitura Self Service Tool for managing RAMP logins, and how to configure mobile RAMP tokens.

Downloading Citrix Receiver

The first time you connect to RAMP from a particular workstation, Citrix Receiver will need to be downloaded and installed. The installation steps vary slight depending on which internet browser you use.

Installing Citrix Receiver Using Chrome

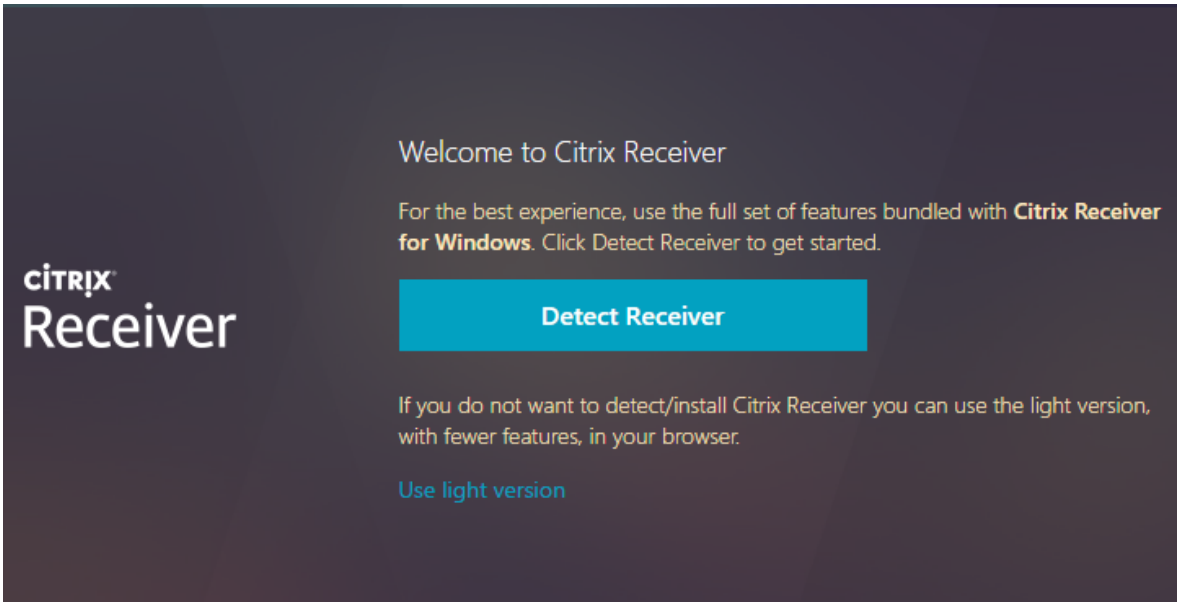
1. Open a new Chrome browser window or tab and navigate to naramp.tessituranetwork.com for licensees housed in the North American region, euramp.tessituranetwork.com for licensees housed in the European region, or apramp.tessituranetwork.com for licensees housed in the Asia Pacific region.



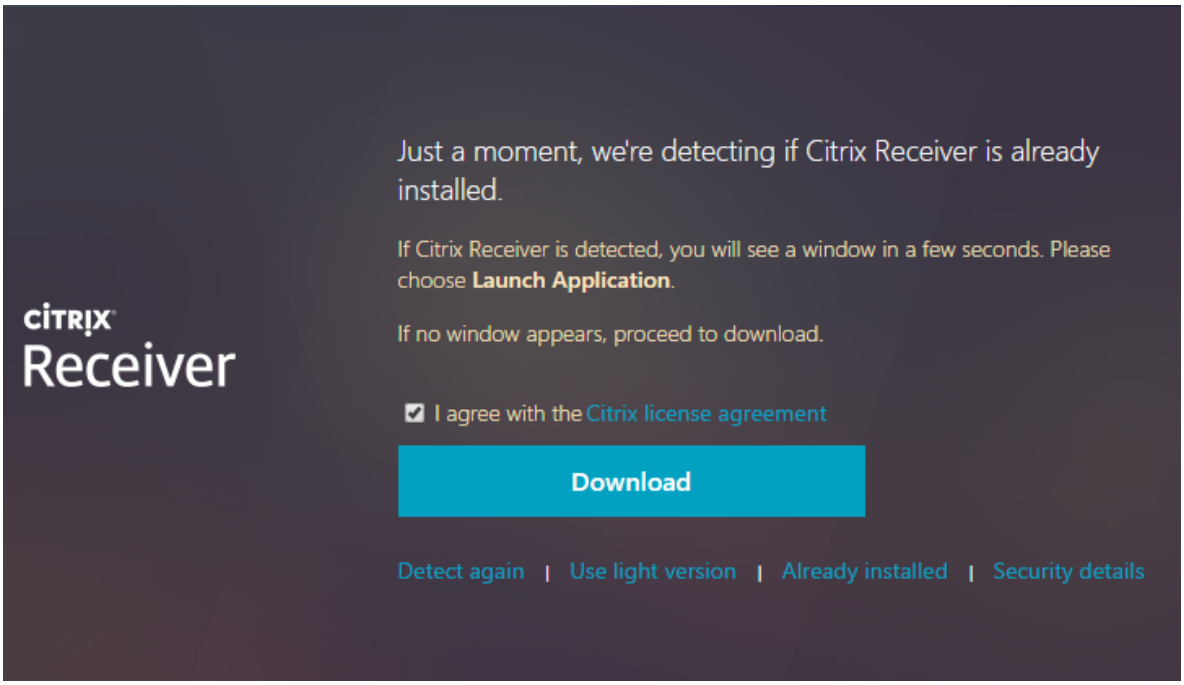
2. Log in using your RAMP user name, password, and token.

Note: Do not allow the browser to save your RAMP login information, as this the login information will not be saved properly and will cause your login to be locked.

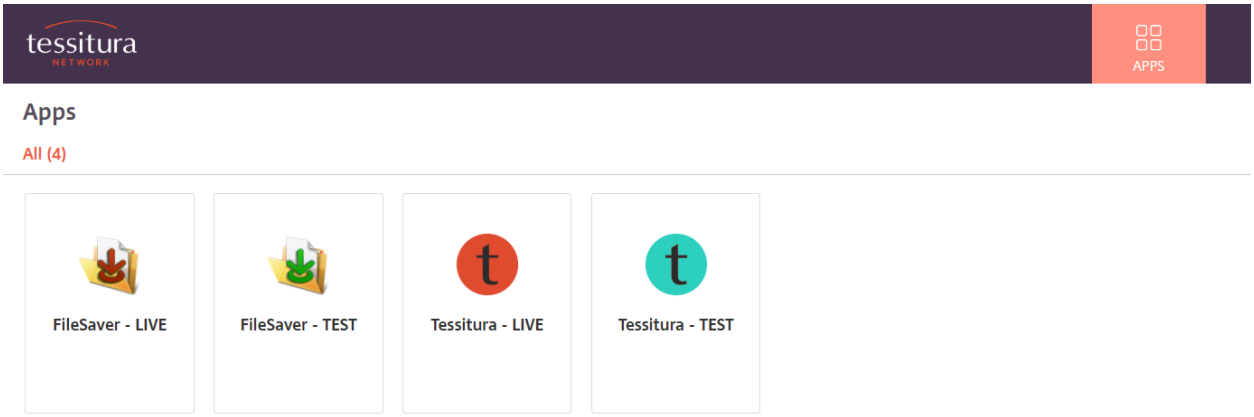
3. Upon successfully logging in, you will be prompted to download and install Citrix Receiver.



4. Click **Detect Receiver**



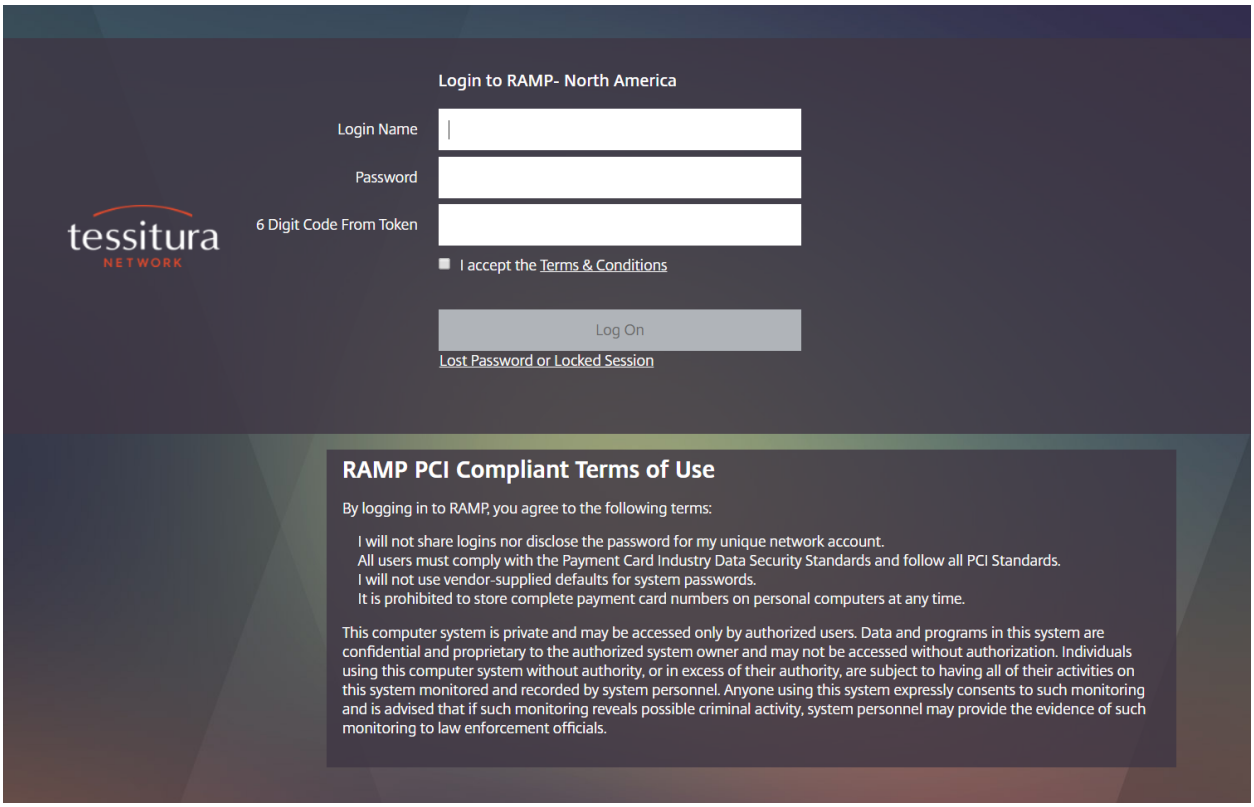
5. Check the license agreement box, click **Download**, and then run the installation file when the download is complete.
6. When the installer opens, click **Start**, check the license agreement box, and then click **Next**.
7. Choose whether or not to participate in the Citrix Customer Experience Improvement Program then click **Install**.
8. When the installation is complete, click **Finish**and then in your browser window click **Continue**.
9. When Chrome asks permission to run the application, check **Remember my choice...**box and then click **Launch Application**.
10. The browser will return to the Citrix Receiver detection screen. Click **Already Installed** to complete your connection to RAMP and be taken to your list of applications.



The first time you launch an application an ica file will download. Right-click on the file and click **Always open files of this type** so that the next time you click to open an application it will open as usual. When the application opens you may also be prompted that the application is attempting access your computer; click **Permit Use** and then log in to the application as usual.

Installing Citrix Receiver Using Edge

1. Open a new Chrome browser window or tab and navigate to naramp.tessituranetwork.com for licensees housed in the North American region or euramp.tessituranetwork.com for licensees housed in the European region, or apramp.tessituranetwork.com for licensees housed in the Asia Pacific region.

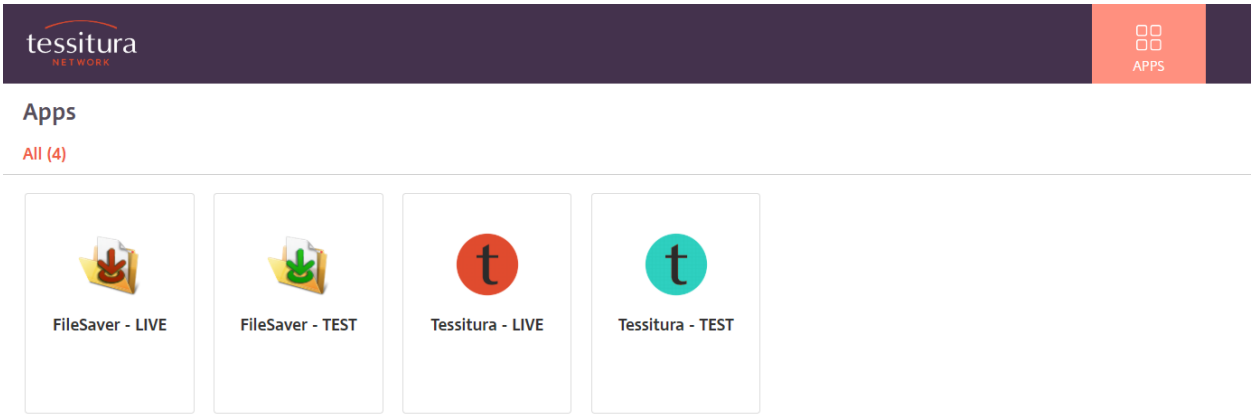


2. Log in using your RAMP user name, password, and token.

> **Note**: Do not allow the browser to save your RAMP login information, as this the login information will not be saved properly and will cause your login to be locked.

3. Upon successfully logging in, you will be taken to a list of your available applications. If prompted to allow the site to open pop-ups, click **OK** and **Always Allow**. Before attempting to launch any of the listed applications, you must manually download Receiver.
4. Click on the arrow next to your user name then select **Download Citrix Receiver**.
5. Check the license agreement box, click **Download**, and then run the installation file when the download is complete.
6. When prompted, click **Run** to run the installer file.
7. When the installer opens, click **Start**, check the license agreement box, and then click **Next**.
8. Choose whether or not to participate in the Citrix Customer Experience Improvement Program then click **Install**.
9. When the installation is complete, click **Finish**.

10. When the installer window closes, click the arrow next to your user name and select Change **Citrix Receiver**.
11. On the next page, click **Use full version** and then you will be returned to your list of applications.



The first time you launch an application an ica file will download. Once the download is complete, click **Open Folder** to go to the file location, then right-click on the .ica file and select **Open with**.

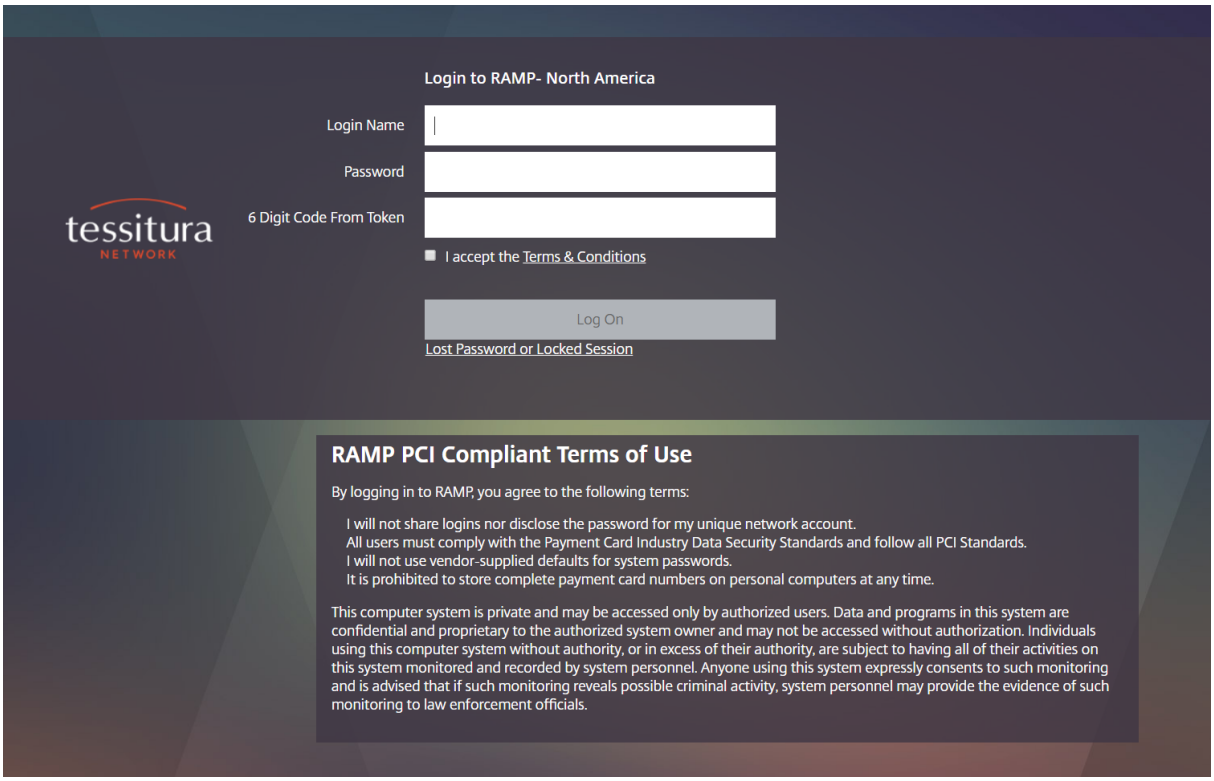
Citrix Connection Manager should be selected as default program, check **Always use this app to open .ica files**, and then click **OK**.

When the application opens you may also be prompted that the application is attempting access your computer; click **Permit Use** and then log in to the application as usual.

Logging In to RAMP

To log in to RAMP:

1. Open a browser window or tab and navigate to naramp.tessituranetwork.com for licensees housed in the North American region, euramp.tessituranetwork.com for licensees housed in the European region, or apramp.tessituranetwork.com for licensees housed in the Asia Pacific region.



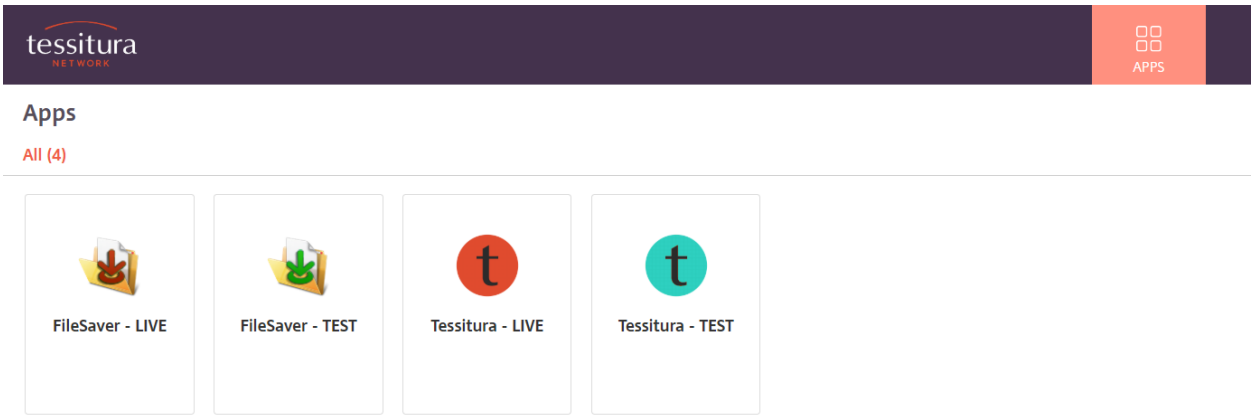
2. Enter your RAMP login name and password.
3. Generate a one-time password (OTP) on your physical or mobile token then enter the code into the **6 Digit Code From Token** field.
4. Check the box to accept the terms and conditions and click **Log On**.

> **Note**: If you have not connected to RAMP on a particular workstation before you will be prompted to download Citrix Receiver upon successful log in.

> **Note**: If your password has expired, you will be prompted to enter a new password after successfully entering your current password.

> **Note**: If you enter an incorrect password or token code, you will need to reenter all three fields after the failed login attempt.

5. If your credentials are valid you will be connected to RAMP and taken to your list of applications.



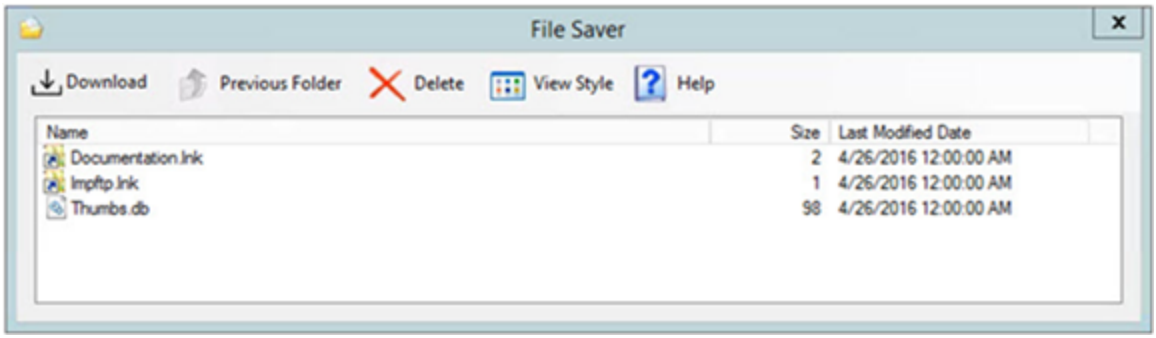
FileSaver

The **FileSaver** application is used to download files from RAMP to your local computer.

> **Note**: Users with rights to upload files to the RAMP server will have access to the FileMover application instead of the FileSaver application.

You will have two versions of the application, one for your Live system (mapped to the L drive) and one for the Test system (mapped to the T drive)

When you open the application it will display shortcuts to the Documentation and Impftp folders on either the L (Live) drive or T (Test) drive:



The **Impftp** folder is where extraction output is saved when extracting to a file from Tessitura, and is the most common location from which you will be downloading files. The Documentation folder is used to hold local documentation your organization has

included in the Tessitura Help System and is a less common location from which to download files.

Note: The Thumbs.db file is a FileSaver configuration file.

To download a file:

1. Navigate to the desired file using the FileSaver links.
2. Select the file, and then click the **Download** button. The Windows Select File window opens.
3. Navigate to the location where you want save the downloaded file and click **Save**.

   Note: To navigate to your local computer, select the **Local Disk** option in the file tree. All other locations in the file tree are on the RAMP servers.

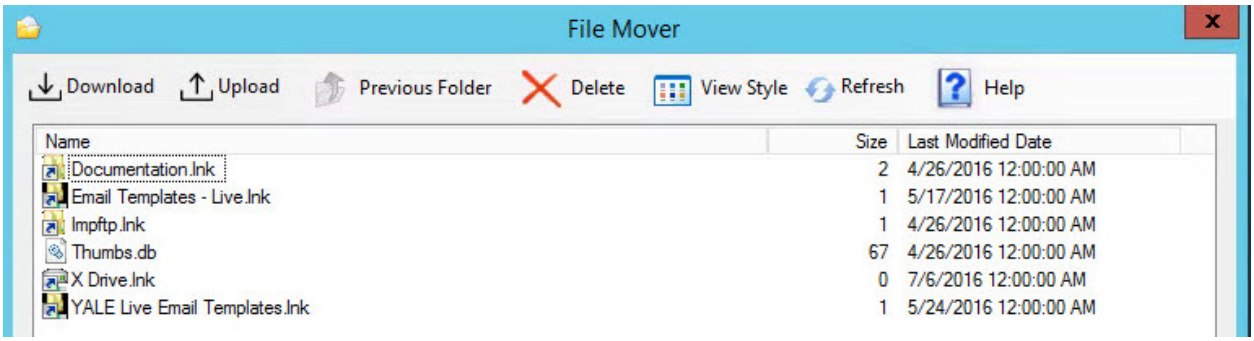
FileMover

The **FileMover** application is used to upload and download files to and from RAMP to your local computer.

Note: Users without rights to upload files to the RAMP server will have access to the FileSaver application instead of the FileMover application.

You will have two versions of the application, one for your Live system (mapped to the L drive) and one for the Test system (mapped to the T drive).

When you open the application it will display shortcuts to the Documentation, Impftp, and User Reports folders on either the L (Live) drive or T (Test) drive. The **Impftp** folder is where extraction output is saved when extracting to a file from Tessitura, and is also the location where the files for the various import utilities are placed. The **Documentation** folder is used to hold local documentation your organization has included in the Tessitura Help System. You may also have shortcuts to your email templates folder, your PAH templates folder, and your PAH logs.



Note: The Thumbs.db file is a FileMover configuration file.

To download a file:

1. Navigate to the desired file using the FileMover links,
2. Select the file, and then click the **Download** button. The Windows Select File window opens.
3. Navigate to the location where you want save the downloaded file and click **Save**.

   Note: To navigate to your local computer, select the **Local Disk** option in the file tree. All other locations in the file tree are on the RAMP servers.

To upload a file:

1. Navigate to the folder where you want to place the uploaded file using the FileMover links. Do not begin the upload from the home of the FileMover application.
2. Click the **Upload** button. The Windows Select File Window opens.
3. Navigate to the location of the file you are uploading, select the file, and click **Upload**.

   Note: To navigate to your local computer, select the **Local Disk** option in the file tree. All other locations in the file tree are on the RAMP servers.

Tessitura Self-Service Tool

The **Tessitura Self-Service Tool** allows RAMP users to:

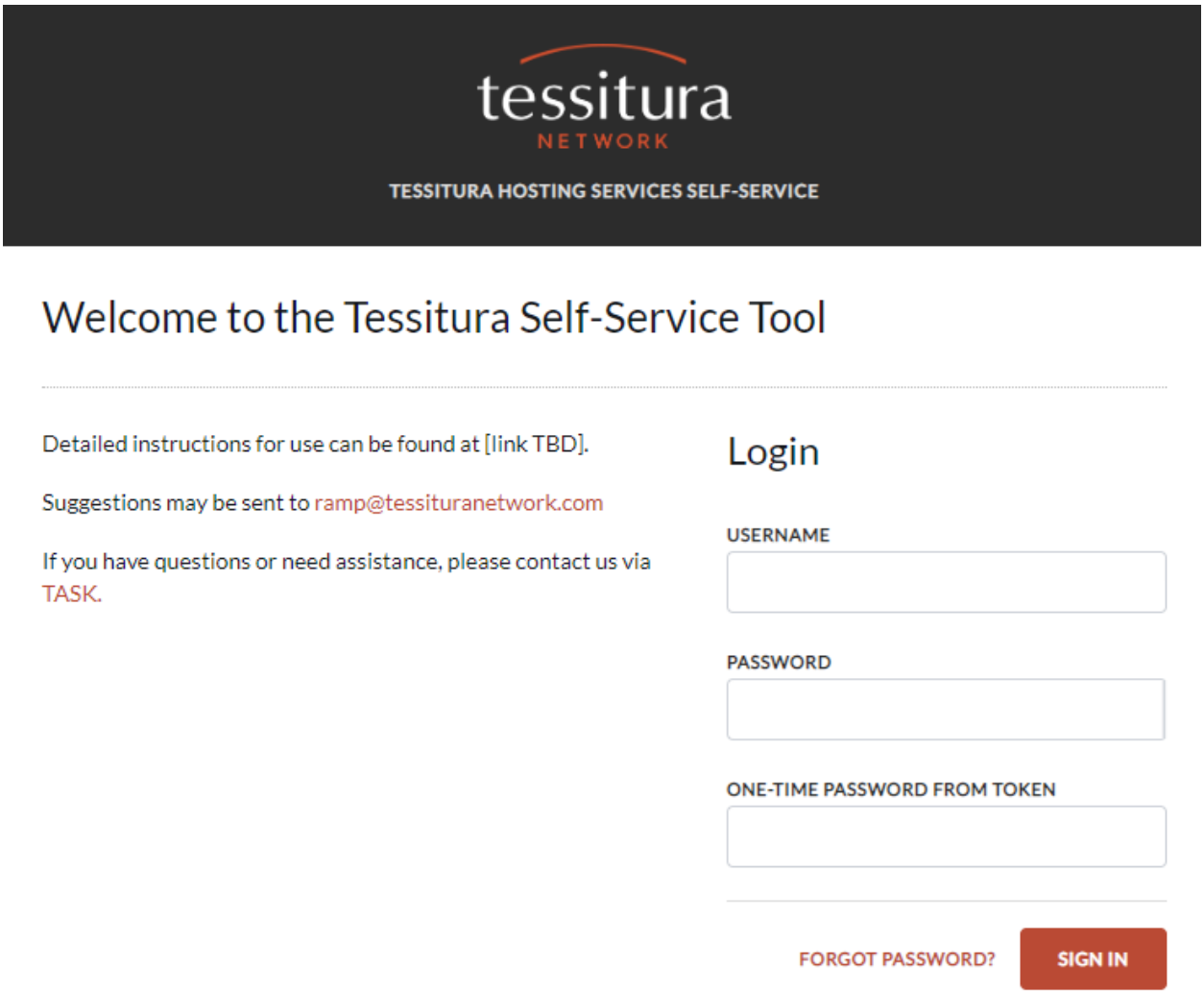
- Change their passwords
- Synchronize their tokens
- End hung Citrix sessions

Additionally, users with security management rights can also:

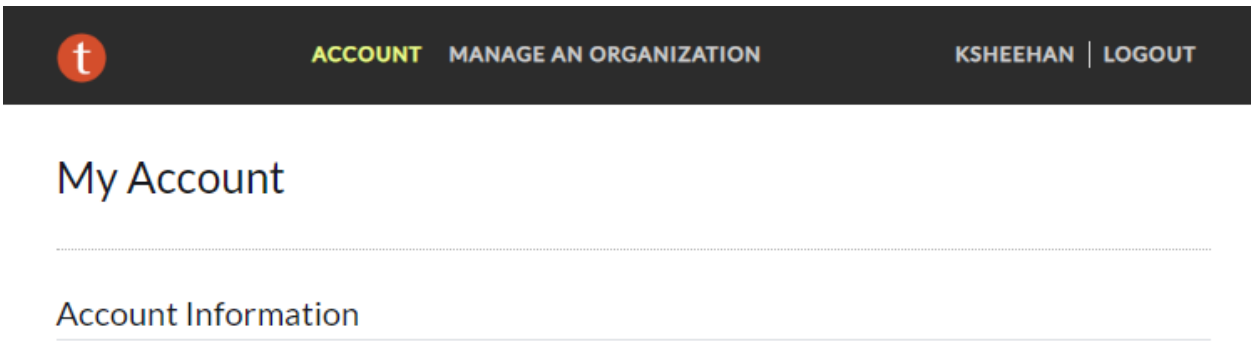
- Send reset password links to RAMP users
- Assign and unassign RAMP user accounts
- Assign, unassign, and unlock tokens
- View their endpoint URLs and corresponding whitelisted IP addresses

To log in to the Tessitura Self-Service Tool:

1. Go to https://selfservice.tessituranetworkramp.com.



2. Enter your RAMP **Username**, **Password**, and **One-Time Password** generated from your RAMP token, then click **Sign In**. If the entered login details are valid, the Tessitura Self-Service Tool loads

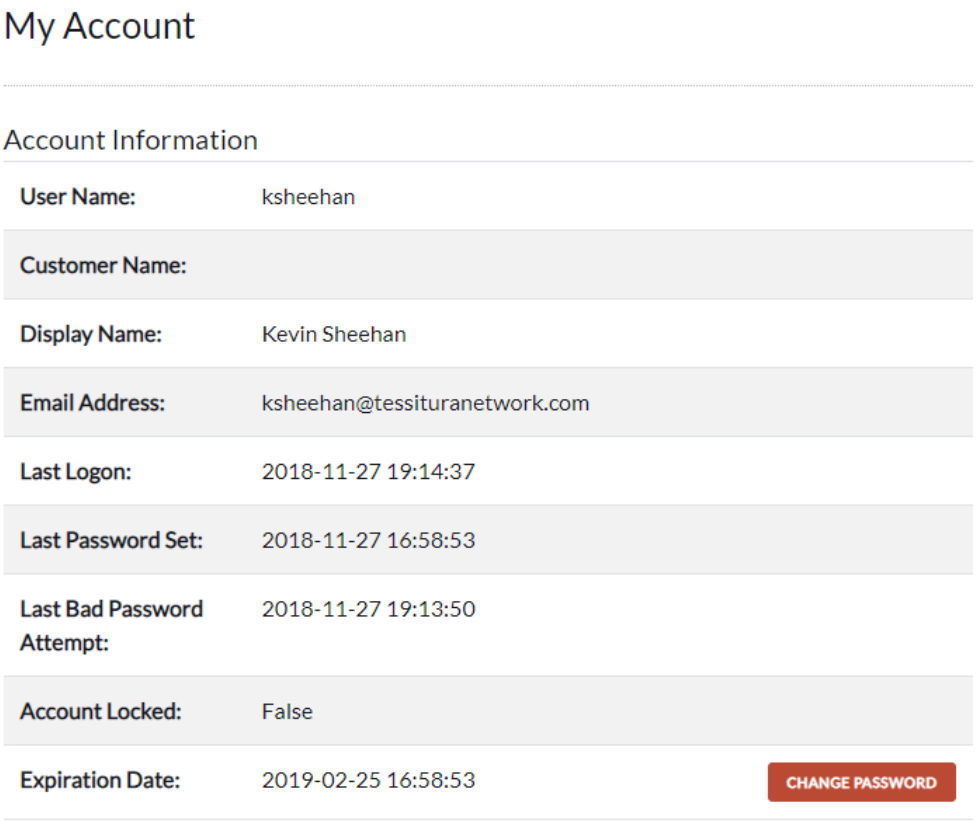


Regular users will have access to the Account page only. Users with management rights will also have access to the Manage Organization section

Account Page

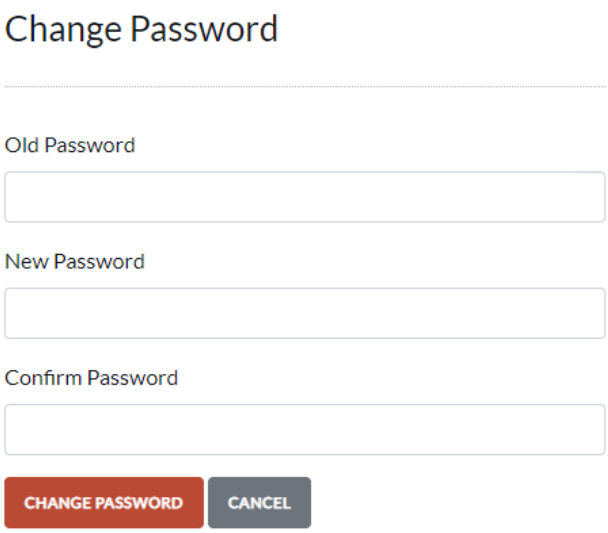
The **Account** page of the Tessitura Self-Service Tool displays information about the current user's account, tokens, and Citrix sessions.

My Account



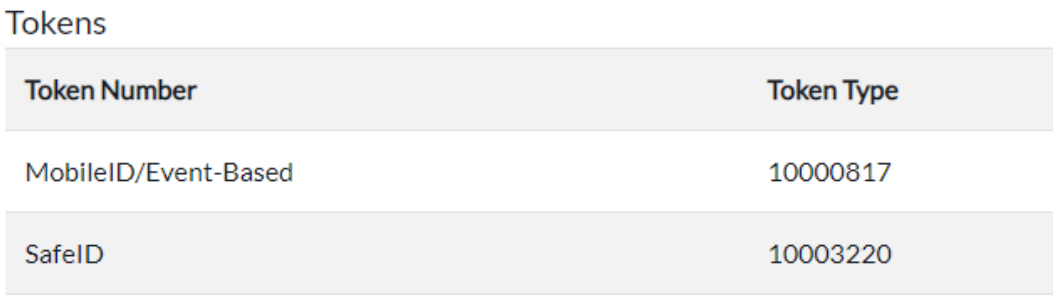
The **My Account** section displays audit information about the current user's account.

Click the **Change Password** button opens the Change Password page:



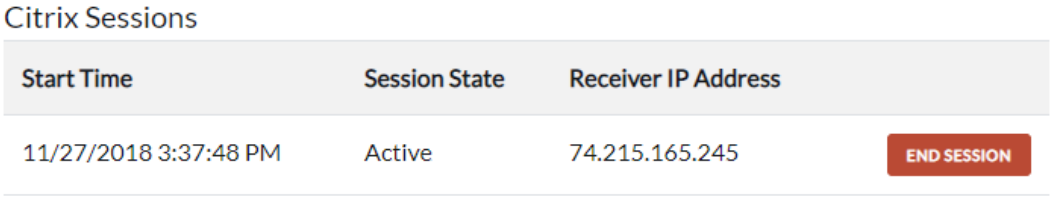
Enter the current password in the **Old Password** field and a new password in the **New Password** and **Confirm Password** fields. Click **Change Password** to save the change.

Tokens



The **Tokens** section lists all RAMP tokens that have been assigned to the current user and holds the Sync Token button.

Citrix Sessions

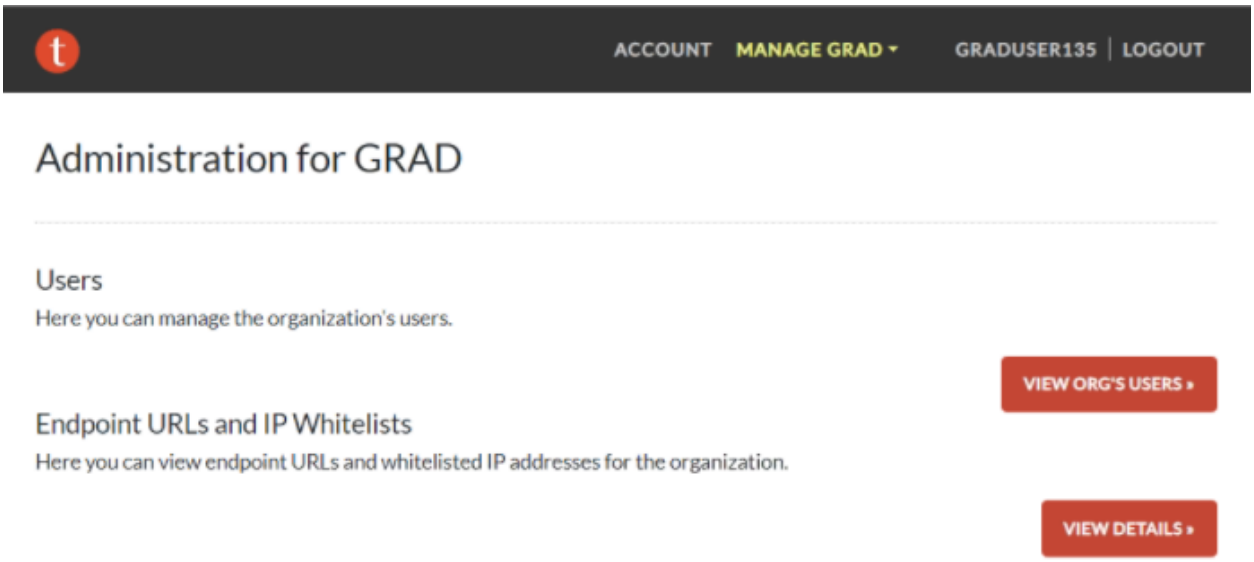


The **Citrix Sessions** section lists all open Citrix sessions for the current user. Click the **End Session** button to terminate a session. This can be used to resolve a "Cannot Start App" error received when attempting to start Tessitura.

Manage Organization

The **Manage Organization** section of the Tessitura Self-Service Tool is used to manage your organization's RAMP user accounts and review the endpoint URLs and whitelisted IP addresses for your organization.

Note: Only users with security management rights have access to this section.

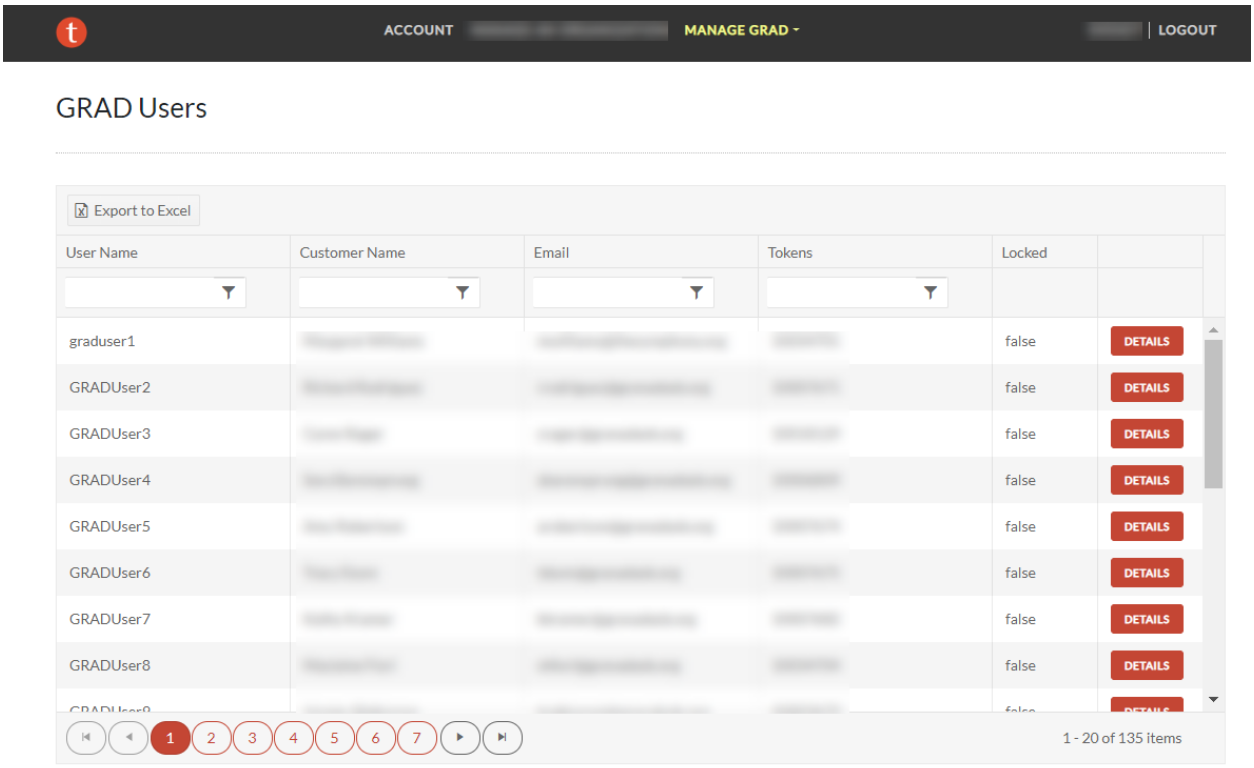


The Users page is used to assign and unassign RAMP user accounts, sync tokens, and reset passwords.

The Endpoint URLs and IP Whitelists page is used to view your organization's endpoint URLs, including REST and SOAP API, Tessitura on the Go, and NScan. It will also display the IP addresses currently whitelisted for these endpoints.

Users

The **Users** page is used to assign and unassign RAMP user accounts, manage tokens, and reset passwords.

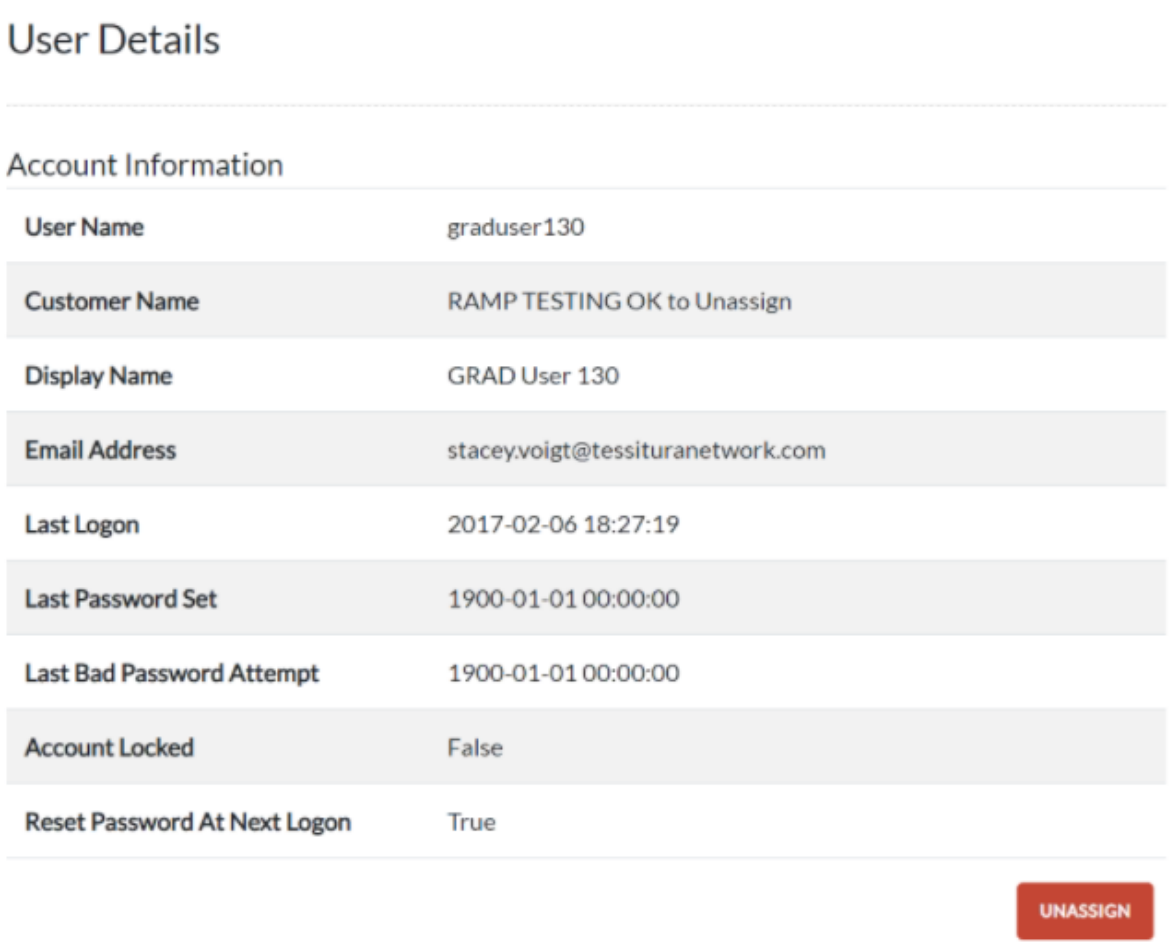


All RAMP user accounts for your organization are listed with the User Name, Customer Name (the person to whom the account is assigned), Email (the email address for the person to whom the account is assigned), Tokens (the ID numbers of all tokens associated with the account), the Locked status (whether or not the account has been locked). You can search for specific user accounts by typing in any of the column header filter fields.

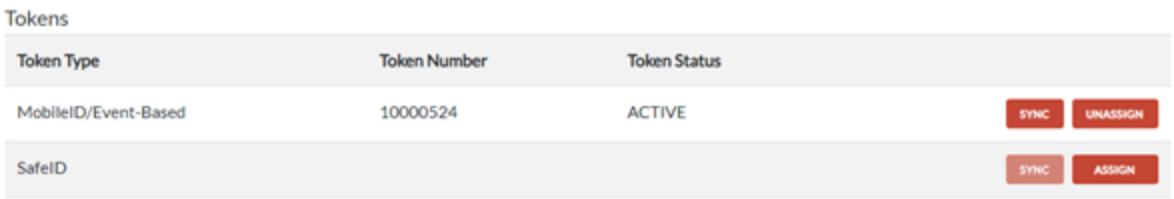
Click the **Export to Excel** button to download a list of all users and their tokens.

User Details

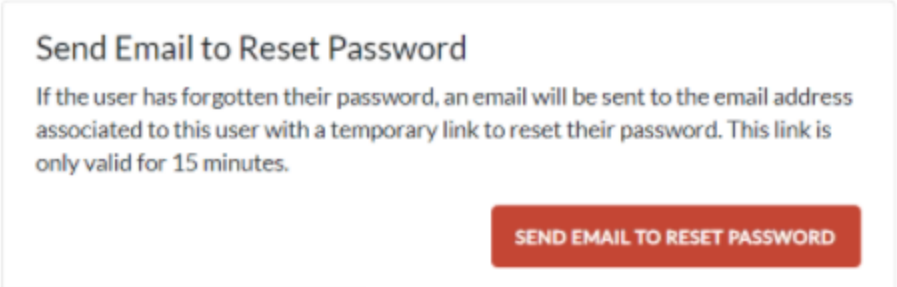
Click the **Details** button on an account row opens the **User Details** page for that account, from which actions can be taken on the account.



The **Account Information** section displays audit information about the user account and holds the Assign/Unassign button.



The **Tokens** section lists the tokens associated with the account. From here tokens can be assigned, unassigned, and unlocked as well as re-synced.



Clicking the **Send Email to Reset Password** button at the bottom of the page will send a password reset link to the email address on file for the account that can be used to reset the password.

Locked Users

When a user has exceeded the maximum number of incorrect log in attempts, their account will be locked. The user can wait 20 minutes for the lock to clear, or may reset their password to immediately clear the lock.

Assigning and Unassigning RAMP User Accounts

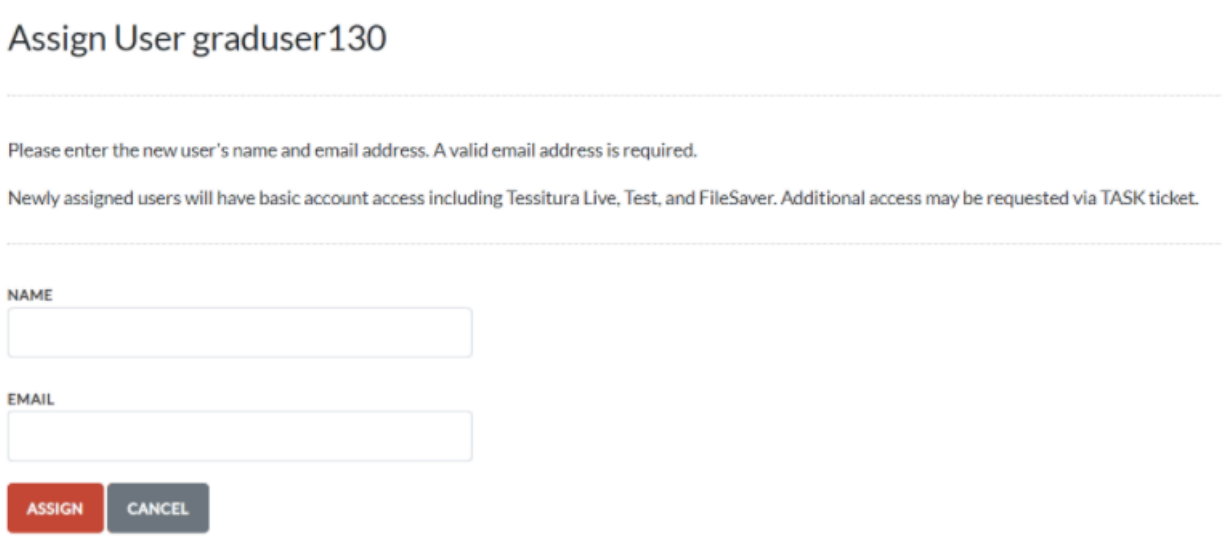
RAMP user accounts can be assigned to or unassigned from a person on the User Details page for the account.

Assigning a User Account

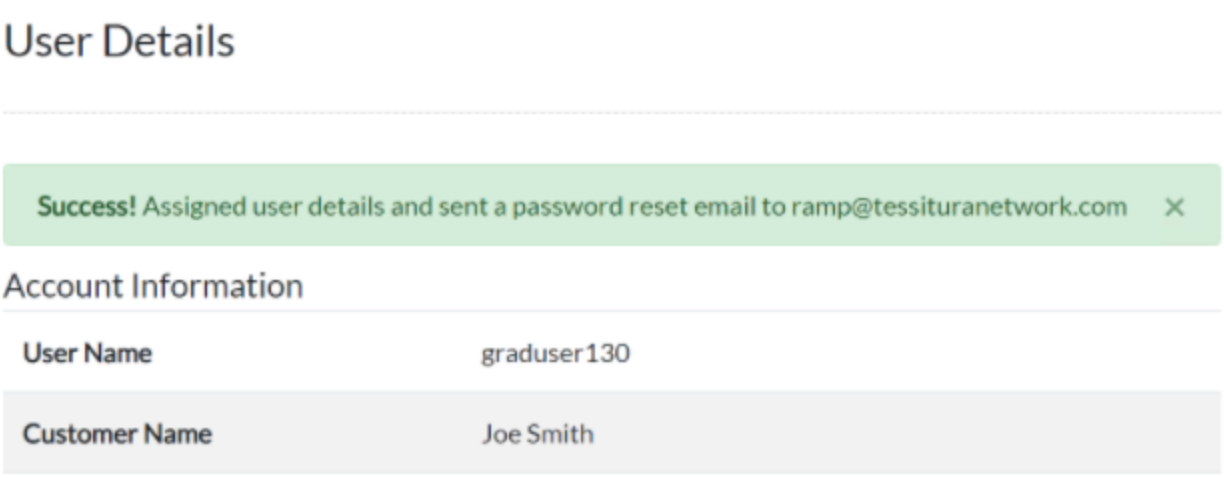
When a RAMP account is assigned, the account is granted basic RAMP access (Tessitura Live, Tessitura Test, and FileSaver). To request additional access contact support via a help ticket.

To assign an unassigned account:

1. Click the **Assign** button in the Account Information section. The **Assign User** dialog opens:



2. Enter the **Name** of the person to whom the account is being assigned.
3. Enter the **Email** address of the person to whom the account is being assigned.
4. Click the **Assign** button. A success message is displayed when the assignment is complete:



An email is sent to the person assigned to the account with a password reset link.

Note: If you make a mistake when assigning a user, such as entering the email address incorrectly, you may unassign and reassign again, or you may contact support via a help ticket to request corrections.

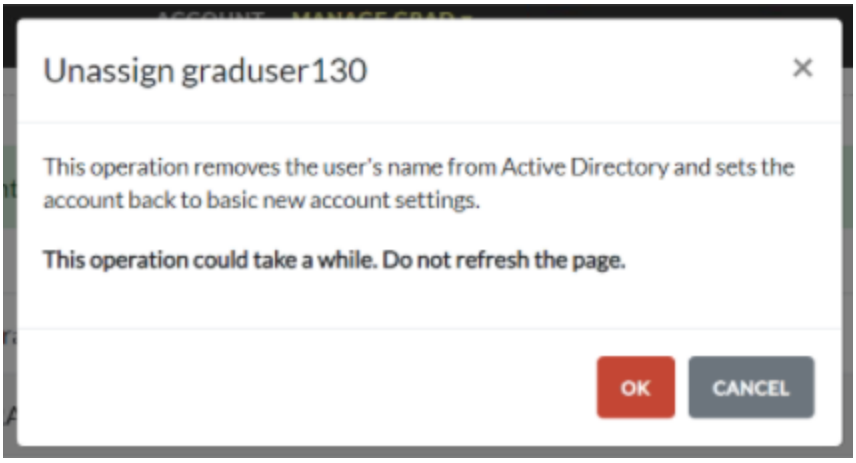
Unassigning a User Account

If a person with RAMP access leaves your organization, you can unassign the RAMP

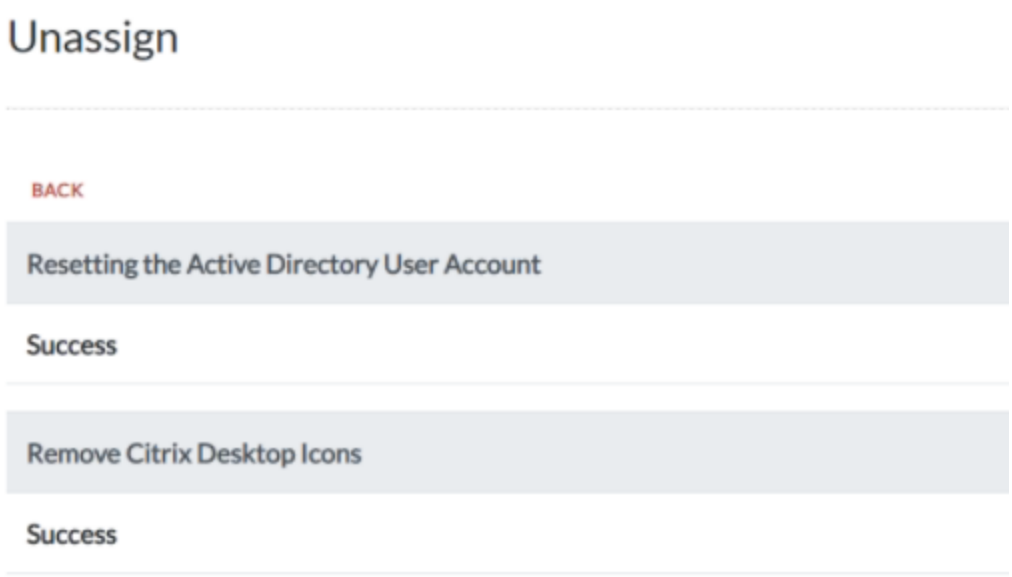
user account that they used, making the account available for assignment to a new person. When an account is unassigned, all non-standard access (such as SQL Server Management Studio, T-Stats, and Infomaker) is removed from the account and it is reset to basic access (Tessitura Live, Tessitura Test, and FileSaver).

To unassign an assigned account:

1. Click the **Unassign** button in the Account Information section. A confirmation dialog opens:



2. Click **OK** to continue with the unassignment (the dialog will remain open while the unassignment is processed) or **Cancel** to cancel. A success message is displayed when the unassignment is complete:



Assigning , Unassigning, and Unlocking Tokens

Tokens can be assigned, unassigned, and unlocked on the User Details page for the account.

A user account can have one physical token (SafeID) and one mobile token (MobileID) assigned.

Note: RAMP user accounts must be assigned to a person before tokens can be assigned to the account.

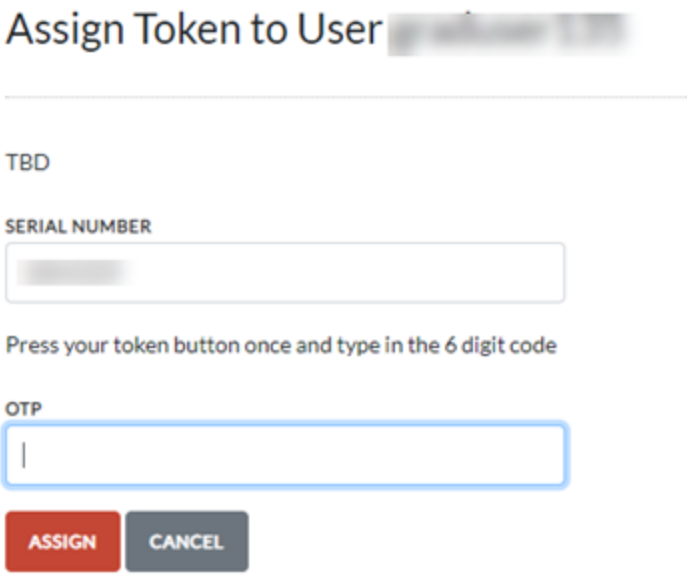
If a token becomes locked an **Unlock** button is displayed; click the button to return the status to Active.

Assigning a Physical Token

Note: The physical token being assigned must be accessible in order to complete its assignment to a user.

To assign a physical token to a user account:

1. Click the **Assign** button on the **SafeID** row. The **Assign Token to User** dialog opens.



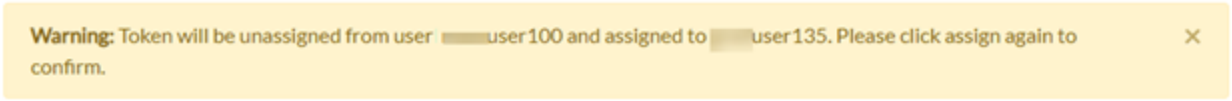
2. Enter the serial number printed on the back of the physical token into the **Serial Number** field in the dialog.

   Note: If the serial number sticker is no longer on the token, hold down the button on the token for appropriately six seconds to display the serial number.

3. Press the button on the token and then enter the code generated into the **OTP** field in the dialog.

4. Click **Assign** to save the assignment.

   If the token is currently assigned to another user a warning message is displayed.

   Click Assign again if you want to complete moving the assignment from one user to the other.

Assigning a Mobile Token

To assign a mobile token to a user account:

1. Click the **Assign** button on the **MobileID** row.

2. The token credential details are generated, and they are then displayed and emailed to the email address on file for the user. The Serial Number and Seed

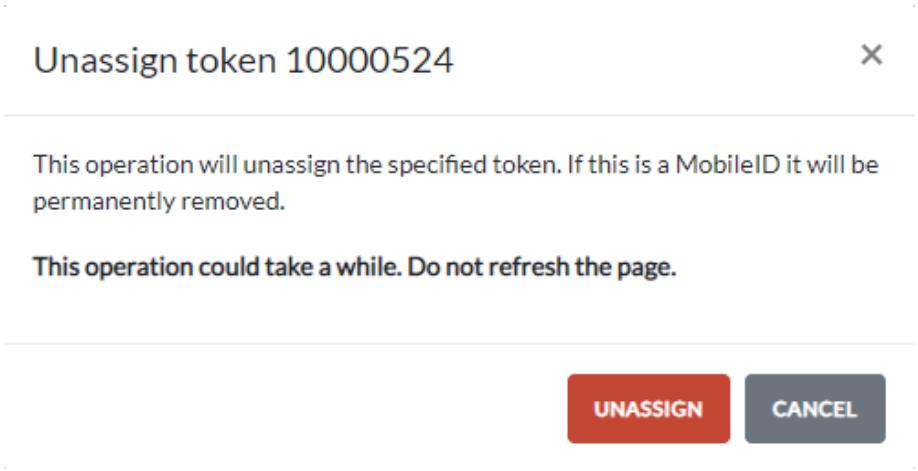
Data values will need to be entered into the **DeepNet MobileID** app on the user's mobile device.

> **Note**: After the mobile token credentials are closed they cannot be retrieved again. If they are lost before being entered into the DeepNet MobileID app, you must unassign and then reassign the MobileID row for the user to generate new mobile token credentials.

Unassigning a Token

To unassign a token from a RAMP user account:

1. Click the **Unassign** button on the token's row. A confirmation dialog opens:

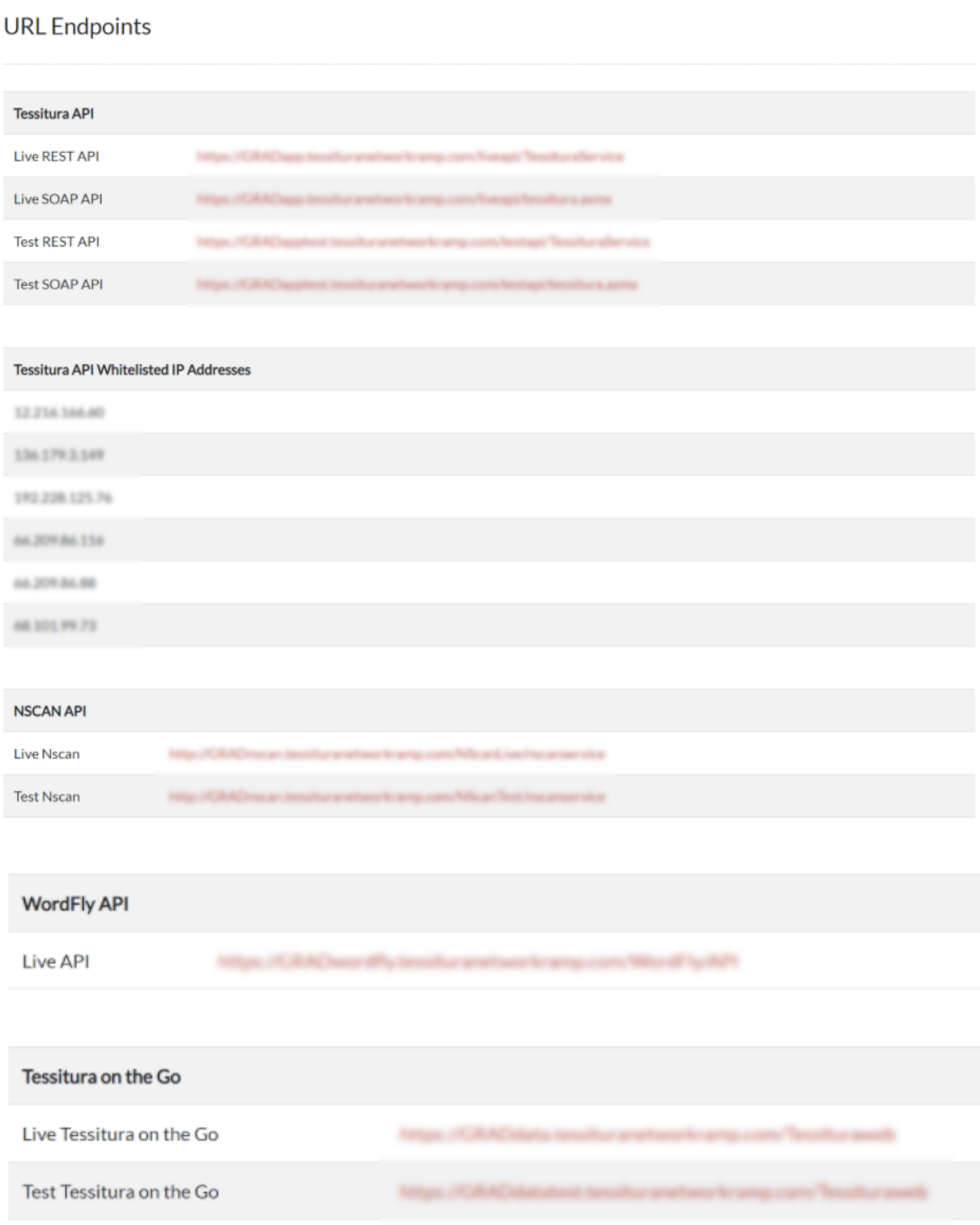


2. Click **Unassign** to continue with the unassignment (the dialog will remain open while the unassignment is processed) or **Cancel** to cancel. A success message is displayed when the unassignment is complete.

URL Endpoints

The **Endpoint URLs and IP Whitelists** page is used to view your organization's endpoint URLs, including REST and SOAP API, Tessitura on the Go, and NScan. It will also display the IP addresses currently whitelisted for these endpoints.

> **Note**: This page is for reference only. Any changes must be requested by contacting Support via a help ticket



URL Endpoints

Tessitura API	
Live REST API	
Live SOAP API	
Test REST API	
Test SOAP API	

Tessitura API Whitelisted IP Addresses

NSCAN API	
Live Nscan	
Test Nscan	

WordFly API	
Live API	

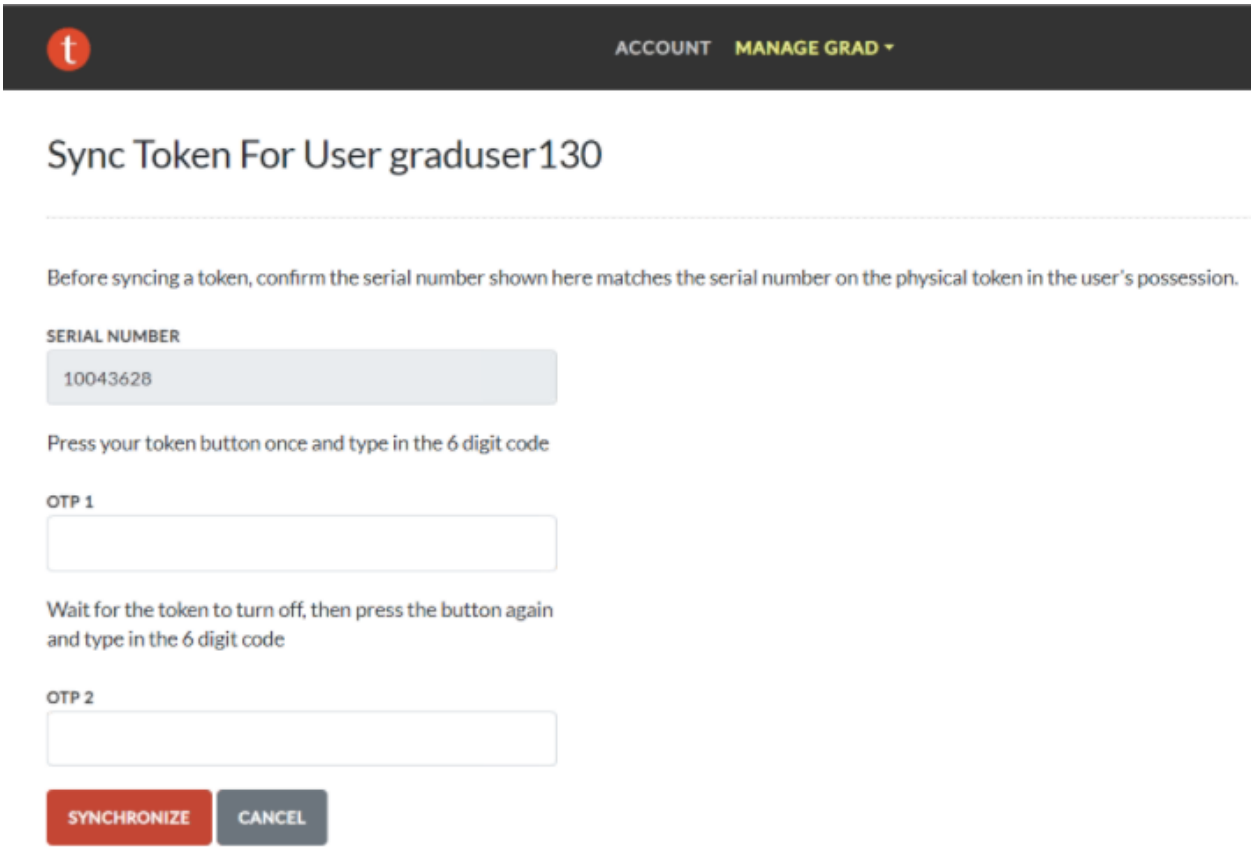
Tessitura on the Go	
Live Tessitura on the Go	
Test Tessitura on the Go	

Sync Token

Tokens can be re-synced using the **Sync Token** function on the Account or User Details page.

To sync a token:

1. Click the **Sync Token** button in the Tokens section. The Sync Token dialog opens:



2. Confirm that the **Serial Number** displayed matches the serial number of the token.
3. Generate a code on the token and enter it into the **OTP1** field.
4. Wait for the token to turn off (physical) or code to expire (mobile) then generate a new code and enter it into the **OTP2** field.
5. Click **Synchronize** to complete the synchronization.

> **Note**: If you receive a "failed to sync" message, open a help ticket. This is normally a sign that the token has failed, but support can research further.

Mobile RAMP Tokens

Mobile RAMP tokens use the **DeepNet MobileID** app to generate the token codes required for logging in to RAMP as part of two-factor authentication. The DeepNet MobileID app can be installed on both Android and iOS devices. Mobile tokens can be used instead of or in conjunction with physical RAMP tokens.

Mobile tokens are assigned to users through the Tessitura Self-Service Tool.

> **Note**: Mobile tokens should also be unassigned through the Tessitura Self-Service Tool when an employee leaves your organization.

Mobile Token FAQ

Can a user have both a mobile token and a physical token?

Yes, this is allowed.

Is there a cost associated with mobile tokens?

Our token licensing is based on users rather than tokens. Adding a mobile token to an existing named user (example: ABCDUser10) will not incur a charge, as it's occupying an existing license. If you increase the number of named users (and thus the number of licenses), each new named user will incur a charge for mobile token.

Likewise, the annual token maintenance fee will still apply on a per-named-user basis for extra users beyond concurrent user limit.

What happens when an employee leaves?

When an employee leaves, you should unassign their mobile token through the Tessitura Self-Service Tool.

Can I move my token from one device to another?

No, mobile tokens cannot be transferred from one device to another. If you have recently changed devices, please reach out to your local administrator to receive a new mobile token assignment or open a help ticket to request new token details.

Can I use my mobile token on multiple devices at once?

While it is possible to successfully install your mobile token on more than one device, you will receive errors when logging in if using the same token on multiple devices.

Can I install my MobileID on a PC rather than a mobile device?

Yes, however this can lead to complications if a PC is used by more than one user, and is not recommended. Likewise, since a user has only one mobile ID, they will not be

able to "carry" it from PC to PC without potential issues such as the token becoming out of sync.

Can we opt out of using mobile tokens for some of our users?

Yes, simply do not assign a mobile token to their accounts.

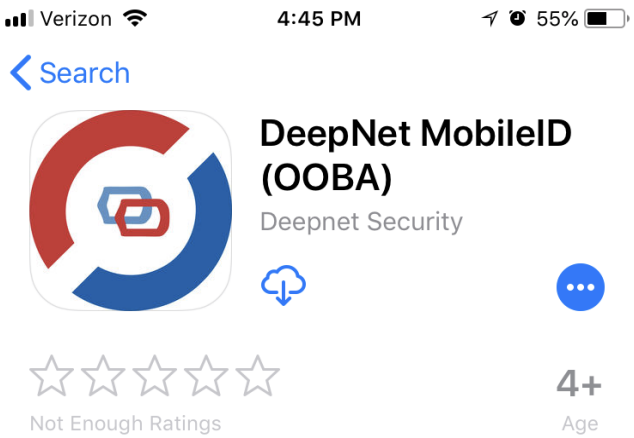
What should we do with our old/unused physical tokens?

Our recommendation is to keep them as spares for any users who may still be assigned to physical tokens. If this is not applicable, you may recycle them through any electronic recycling program.

Mobile Token Installation for iOS

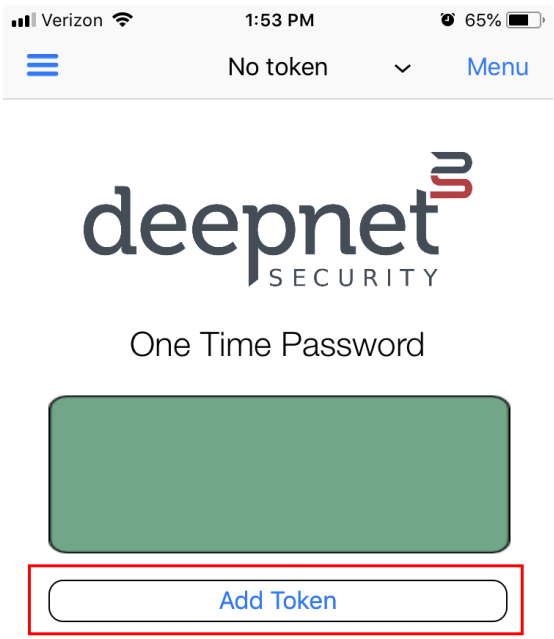
To install and configure a mobile token on an iOS device:

1. Go to the App Store and find and install the **DeepNet MobileID** app:

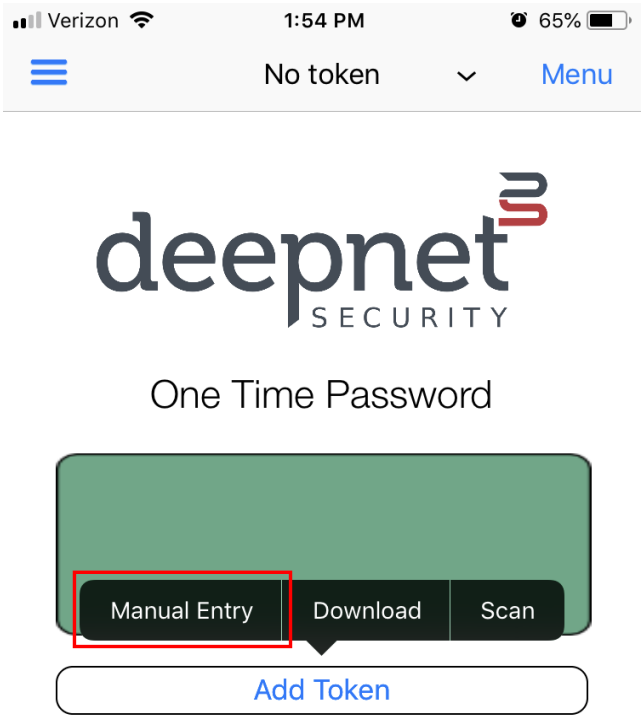


> **Note**: Each set of MobileID credentials can be installed on one device. For this reason, we recommend installing on a mobile phone rather than on a PC, particularly for staff who often work at multiple workstations.

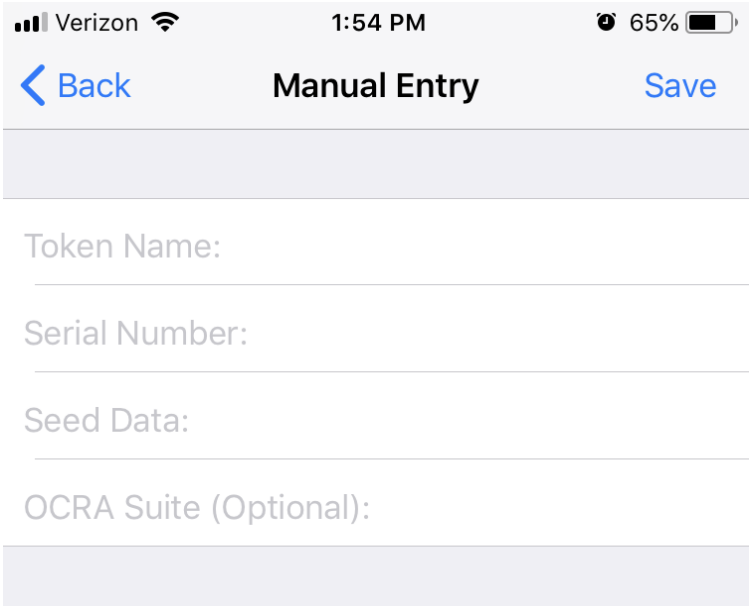
2. Launch **MobileID** on the device and press **Add Token**.



3. Select **Manual Entry** from the menu.



The token details open:



4. In the **Name** field enter a name used to identify the token on the device. Any name can be used.
5. In the **Serial Number** field enter the serial number generated when assigning the token in the Tessitura Self-Service Tool.
6. In the **Seed Data** field enter the seed value generated when assigning the token in the Tessitura Self-Service Tool.
7. Press **Save** to save the token details.

Adding a PIN

You can optionally set a PIN to secure your MobileID app.

Warning: If you set a PIN and forget it, Tessitura Support is not able to recover it for you.

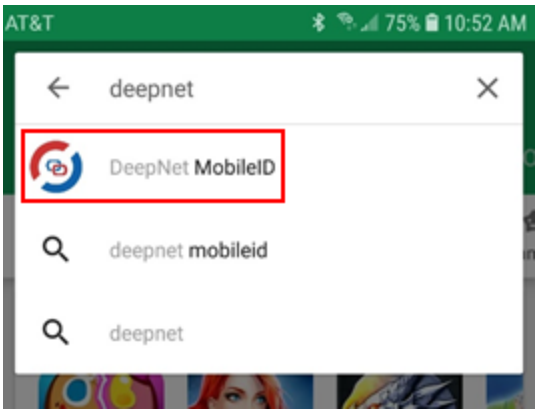
To set up a PIN:

1. Open the top left app menu and select **Settings**.
2. Select **PIN Setting**.
3. Press the **Enable PIN** switch.
4. Enter a PIN in the **New PIN** field and renter the PIN in the **Confirm PIN** field.
5. Press **Save** to save the changes.

Mobile Token Installation for Android

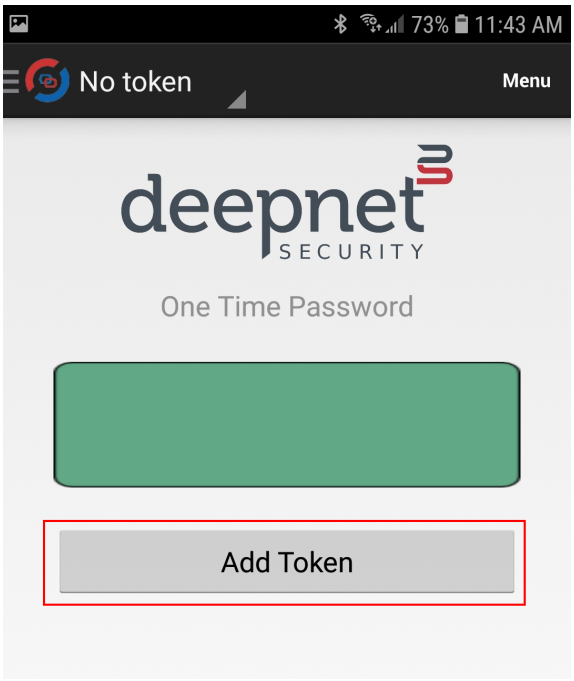
To install and configure a mobile token for an Android device:

1. Go to the Google Play store and find and install the **DeepNet MobileID** app:

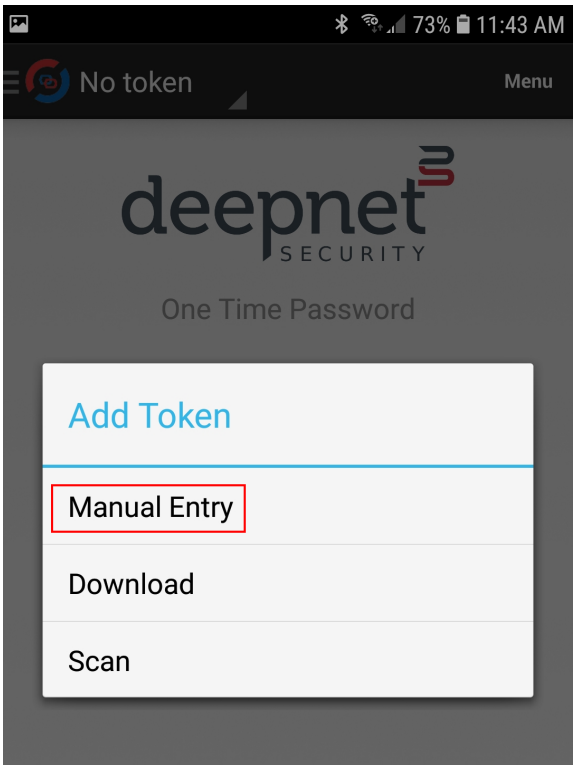


> **Note**: Each set of MobileID credentials can be installed on one device. For this reason, we recommend installing on a mobile phone rather than on a PC, particularly for staff who often work at multiple workstations.

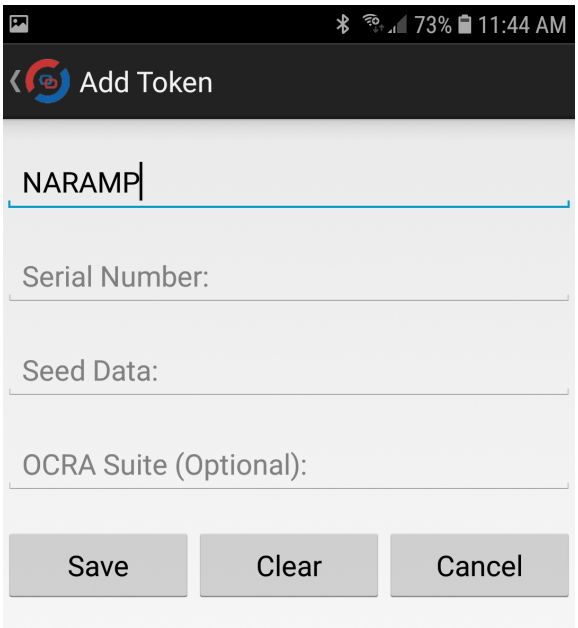
2. Launch **MobileID** on the device and press **Add Token**.



3. Select **Manual Entry** from the menu.



The token details open:



4. In the **Name** field enter a name used to identify the token on the device. Any name can be used.
5. In the **Serial Number** field enter the serial number generated when assigning the token in the Tessitura Self-Service Tool.

6. In the **Seed Data** field enter the seed value generated when assigning the token in the Tessitura Self-Service Tool.
7. Press **Save** to save the token details.

Adding a PIN

You can optionally set a PIN to secure your MobileID app.

> **Warning**: If you set a PIN and forget it, Tessitura Support is not able to recover it for you.

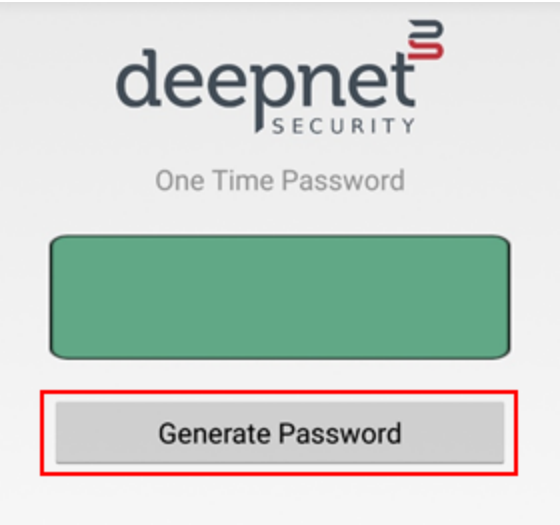
To set up a PIN:

1. Open the top left app menu and select **Settings**.
2. Select **PIN Setting**.
3. Press the **Enable PIN** switch.
4. Enter a PIN in the **New PIN** field and renter the PIN in the **Confirm PIN** field.
5. Press **Save** to save the changes.

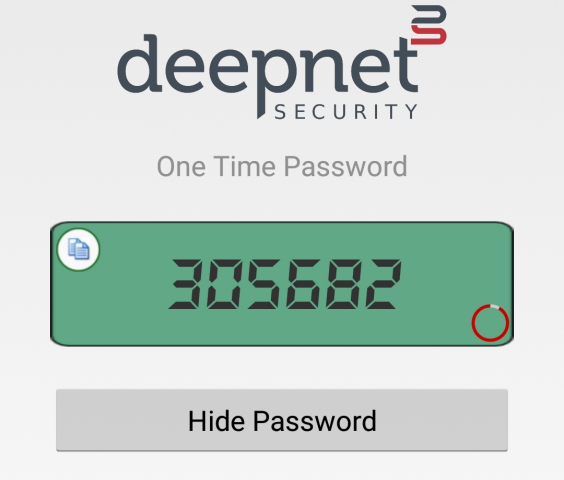
Using Mobile Tokens

To generate a token code for logging in to RAMP:

1. Open the MobileID app on your mobile device. If a PIN has been enabled you will be prompted to enter the PIN.
2. Press **Generate Password** to generate a token code.



3. The token code is displayed in the center of the screen.



Enter the displayed code into the RAMP login page; the red circle is a countdown timer that indicates how much time remains before the token code expires.