franconnect

Springboard to Success

Activities Book – Secure Your Data

In these times of ransomware and data attacks, you want your important data to be as safe as you can make it. In this session, we'll discuss simple steps you can take to prevent unauthorized access of your proprietary data – both user data and your hub library of procedures.

This book gives you the steps to:

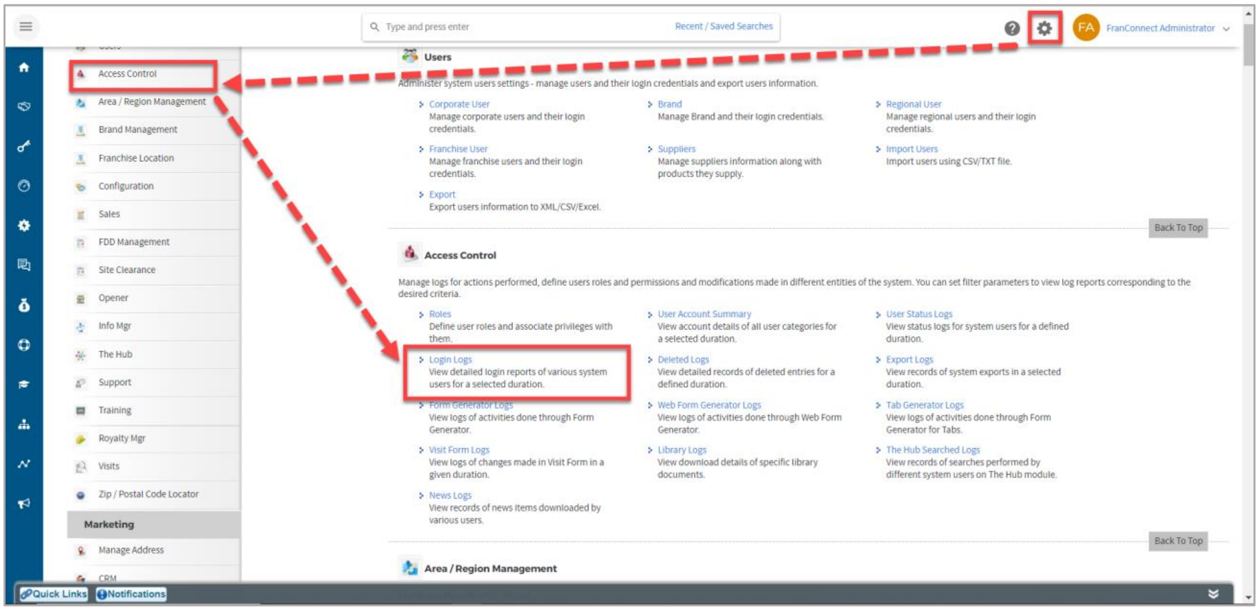
- Run login logs to identify inactive users, and follow up to see if they need deactivation
- Review Roles and who is in each one
- Review your password security, and update if desired
- Determine if you choose to password protect personally identifiable information

We invite you to use these instructions, to submit questions to training@franconnect.com, and if you're really really stuck, we invite you to schedule a 1:1 session with us to help you through these processes. You can schedule that time using this link: https://tinyurl.com/677y7tz8.

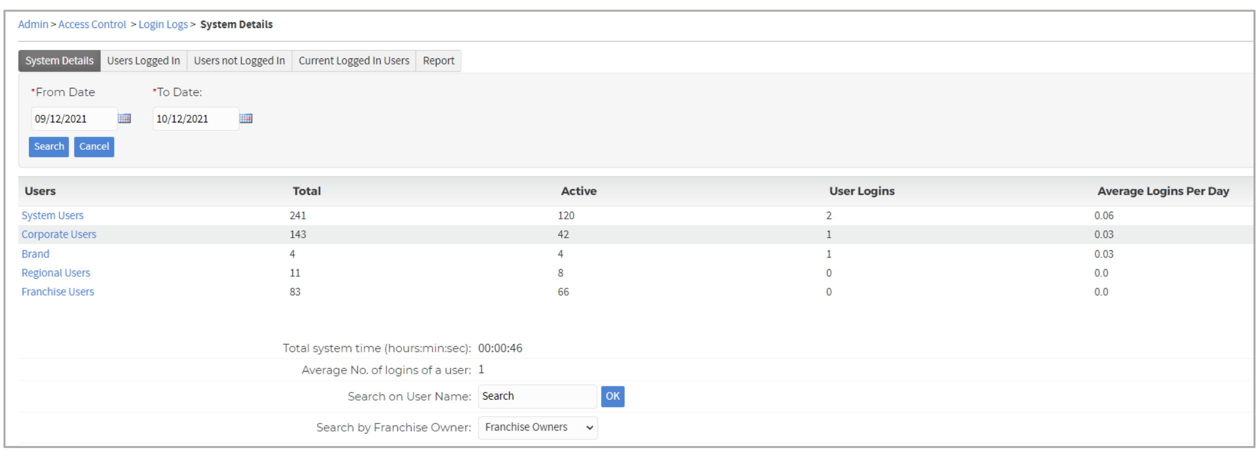
Contents

Run Logs to Idenfity Inactive Users

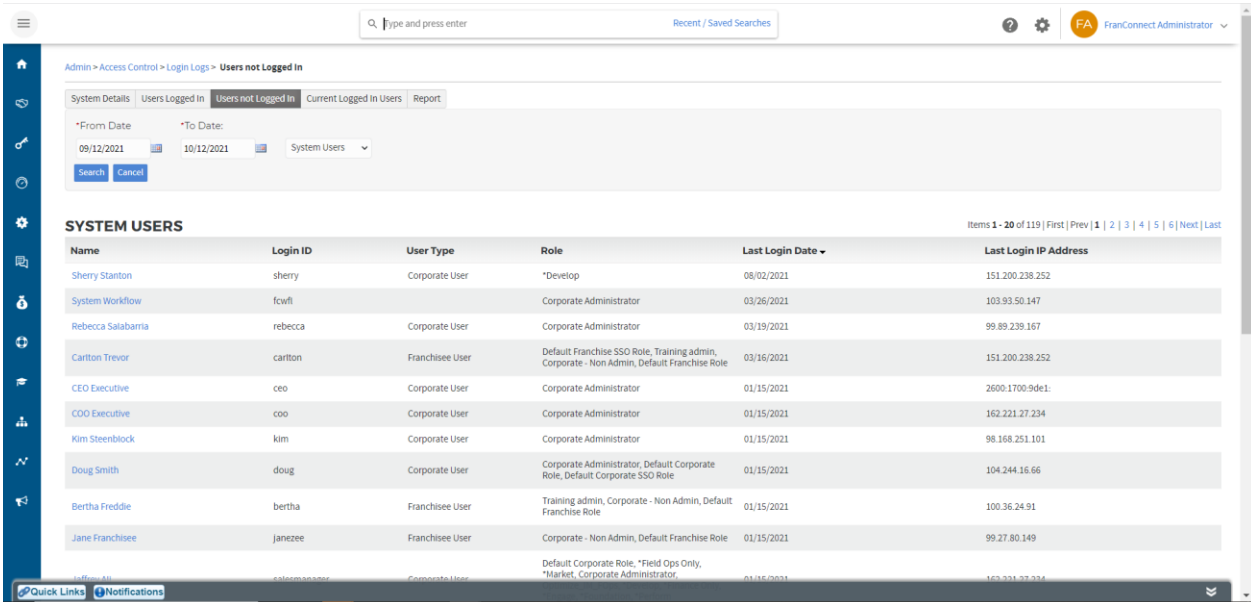
To view the number of users in the system, and identify inactive users, go to Admin > Access Control, and choose the Login Logs section.



You'll be taken to the Login Logs interface. The main page is a listing of all users, called the "System Details" tab. You can click on any blue user listing to see the details for that subset, for example, just Franchise Users. The tabs across the top will allow you to sort them by their login status.



For our purposes, we're looking for users who have not logged in recently. Click the "Users not Logged In" tab, and select a reasonable time range for inactivity. The default will be the past month.



Name	Login ID	User Type	Role	Last Login Date	Last Login IP Address
Sherry Stanton	sherry	Corporate User	*Develop	08/02/2021	151.200.238.252
System Workflow	fcwfl		Corporate Administrator	03/26/2021	103.93.50.147
Rebecca Salabarria	rebecca	Corporate User	Corporate Administrator	03/19/2021	99.89.239.167
Carlton Trevor	carlton	Franchisee User	Default Franchise SSO Role, Training admin, Corporate - Non Admin, Default Franchise Role	03/16/2021	151.200.238.252
CEO Executive	ceo	Corporate User	Corporate Administrator	01/15/2021	2600:1700:9de1:
COO Executive	coo	Corporate User	Corporate Administrator	01/15/2021	162.221.27.234
Kim Steenblock	kim	Corporate User	Corporate Administrator	01/15/2021	98.168.251.101
Doug Smith	doug	Corporate User	Corporate Administrator, Default Corporate Role, Default Corporate SSO Role	01/15/2021	104.244.16.66
Bertha Freddie	bertha	Franchisee User	Training admin, Corporate - Non Admin, Default Franchise Role	01/15/2021	100.36.24.91
Jane Franchisee	janezee	Franchisee User	Corporate - Non Admin, Default Franchise Role	01/15/2021	99.27.80.149

You can sort by login date to see the most recent logins at the top, or the least recent. Least recent will float to the top those users who have never logged in, which is a good place to start deactivating users.

SYSTEM USERS

Name	Login ID	User Type	Role	Last Login Date ▲
NathanS One	c01	Corporate User	Default Corporate Role	Never Logged In
CCO Executive	cco	Corporate User	Corporate without access all leads	Never Logged In
Fran Two	f02	Franchisee User	Corporate - Non Admin, Default Franchise Role	Never Logged In

You can export this list to an Excel sheet to share with non-FranConnect users in determining users who should or should not still have access. Click **Export as Excel** at the bottom of th listing.

Sania Tutie	sania	Franchisee User	Corporate - Non Admin, Default Franchise Role	Never Logged In
Tetra King	tetra	Franchisee User	Corporate - Non Admin, Default Franchise Role	Never Logged In

Print | Export As Excel | Back

Deactivating Inactive Users

Considerations in Removing Users from FranConnect

Users in FranConnect remain active indefinitely unless you've made them a guest user or unless you **deactivate** them. When a user is deactivated, the user can no longer log into FranConnect.

There are two methods for removing users from FranConnect – you can deactivate them, or you can delete the user record. Typically, the only reason to delete a user is in the case of a test user added that you want to “disappear” from the system. Actual users will have history and relationships that you may want preserved, at least for historical records.

Clicking **Deactivate** next to a user’s name will remove their access from the system and move their record to the Deactivated Users tab. Deactivated users can be reactivated.

Clicking **Delete** next to a user’s name will remove the user from the system. ***This is a non-reversible action.***

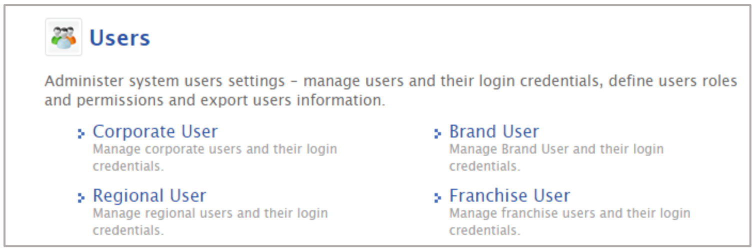
For this reason, the best practice is to deactivate users rather than delete.

These are the considerations for deactivating or deleting users. Detailed steps are given after this chart.

Corporate, Divisional or Regional Users	**Franchise Users**
Will this person’s duties be assumed by someone who does not yet have a user ID for FranConnect?	
1. Add a new user of the appropriate type from the Admin interface.	1. Add another owner or employee to the franchise record in Info Manager, owner or employee tab. 2. Add a user ID for the new owner or employee in the Admin interface.
Is this user a Default Owner of incoming CRM leads?	
1. Reassign default ownership at **Admin** > **CRM** > **Setup Default Owner >Default Owner**	1. Reassign default ownership at **Admin** > **CRM** > **Setup Default Owner > Default Location Owner**
Is this user a Default Owner of incoming franchise development (Sales) leads?	
1. Reassign default ownership at **Admin** > **Sales** > **Assign Lead Owners**	(not applicable)
Is this user associated with tasks in various areas of the system?	
1. Choose to deactivate user in **Admin** > **Users** > **Manage [Corporate/Divisional/Regional] Users** 2. Choose the user to delete/deactivate and choose that action on the Action Wheel 3. Choose “Reassign” in the dialog box and choose the user who will assume each type of role	1. Choose to deactivate user in **Admin** > **Users** > **Manage Franchisee Users** 2. Choose the user to delete/deactivate and choose that action on the Action Wheel 3. Choose “Reassign” in the dialog box and choose the user who will assume each type of role

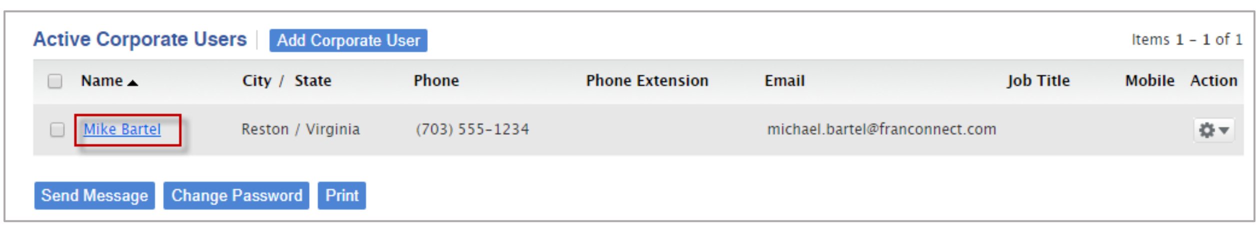
Navigating the Admin > Users interface

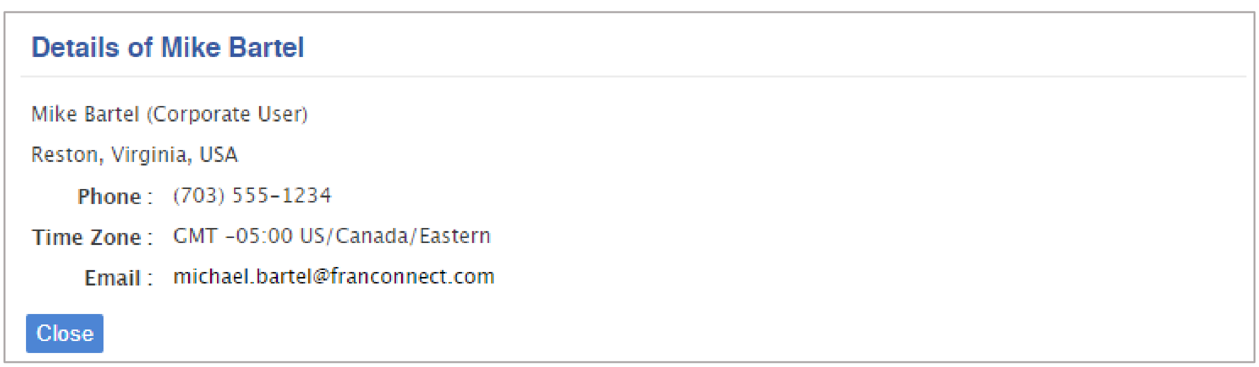
To manage user accounts, go to the corresponding user page where you will find the list of users.



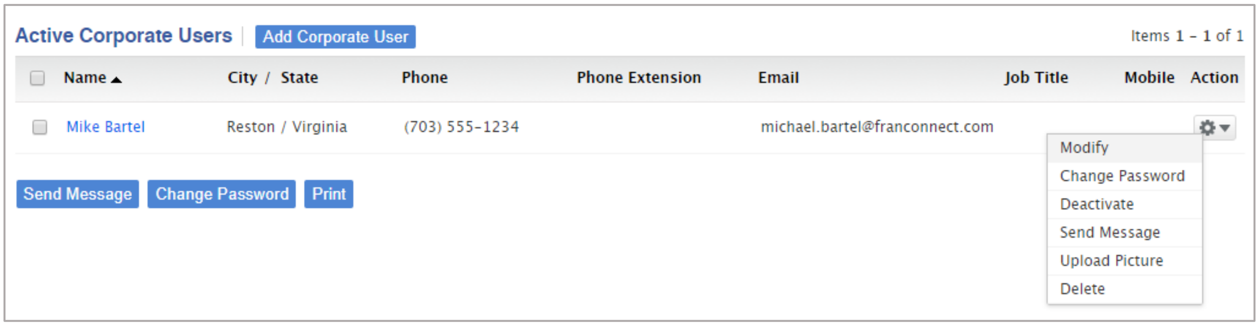
You can use the **Search** option at the top to search for different users.

To view information for a specific user, click the account hyperlink to open the information about that user account.



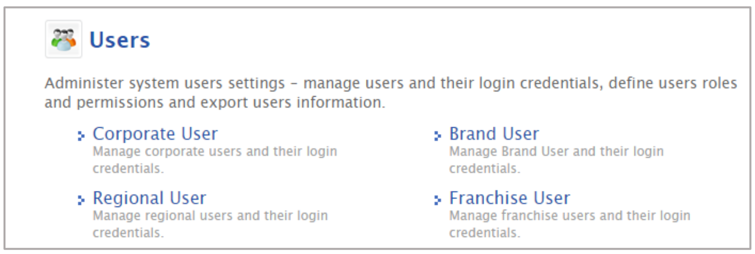


To modify a user account, use the **action wheel** for a variety of functions, such as **modify**, **change password**, **deactivate** and **delete**.

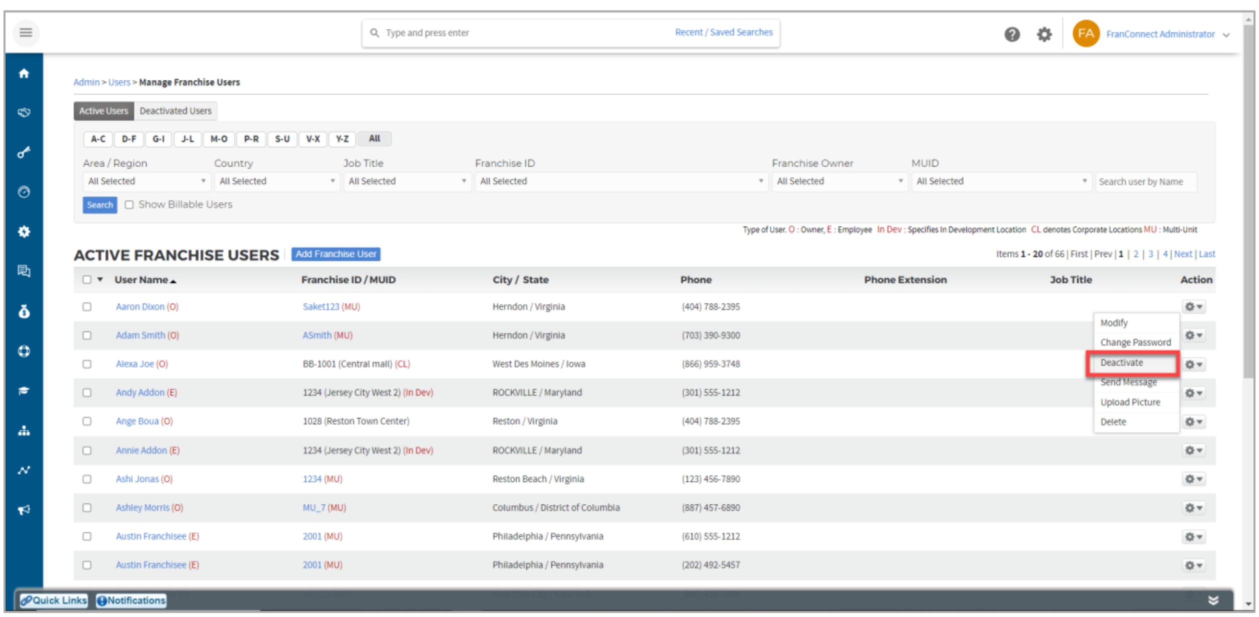


Deactivating Corporate, Divisional or Regional Users

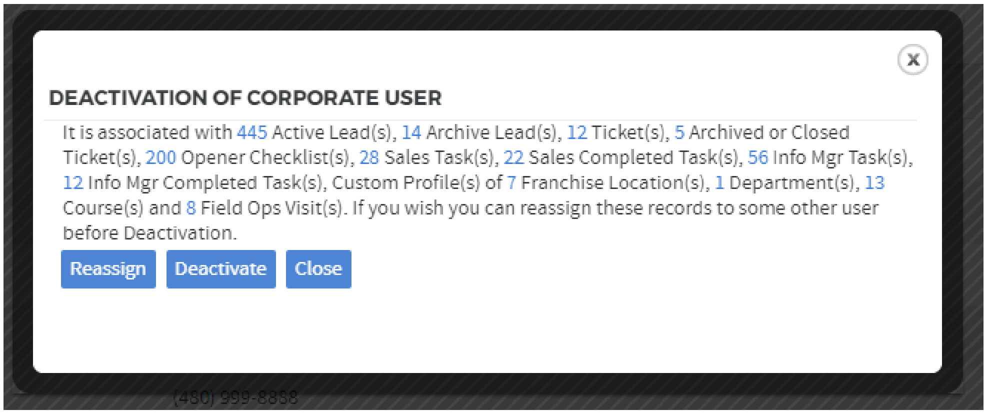
Go to the appropriate user type in the Admin > Users menu.



Navigate to the user to deactivate and click the action wheel to the right of the user's record.



If the user was attached to any records in the FranConnect system, you'll see a dialog box like the following, indicating what records were related to the user. You'll be offered the opportunity to reassign those items to a current user before deactivating the departing user.

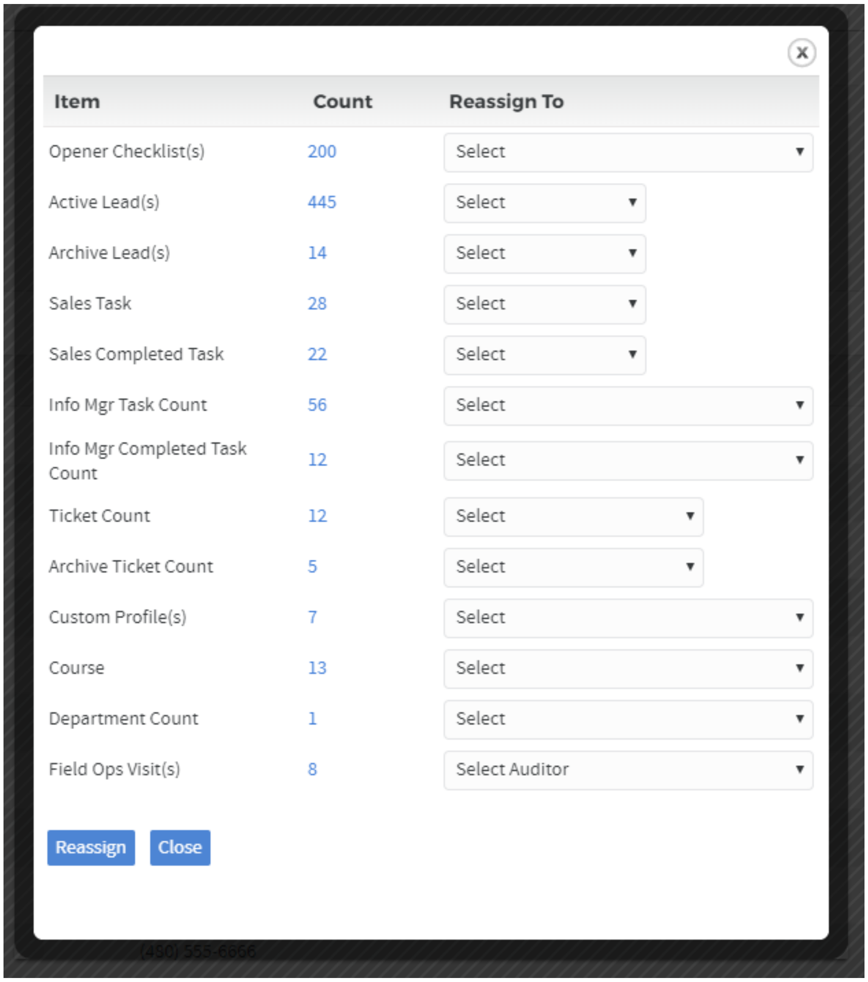


It is strongly recommended that you reassign everything, to avoid ongoing work falling through the cracks of assignment and reminders. The only exception to this is Courses, which are training course items that the departing user was taking, and don't need to be reassigned to someone else to take.

If you choose to **Deactivate** or **Delete** without reassigning, the user's name remains associated with the items, and will be reported, etc. The user will not receive reminders or alerts, so the items can potentially be ignored. The next time a record is opened, for example a lead record, that record may not be saved with the deactivated user associated, and you'll need to reassign before you can save the record.

If you **deactivate** without reassigning, you can choose to reactivate the user to see what remains assigned to them, and choose to deactivate again, this time reassigning the items. If you **delete**, you will have no easy way of seeing what items are still associated with the deleted user.

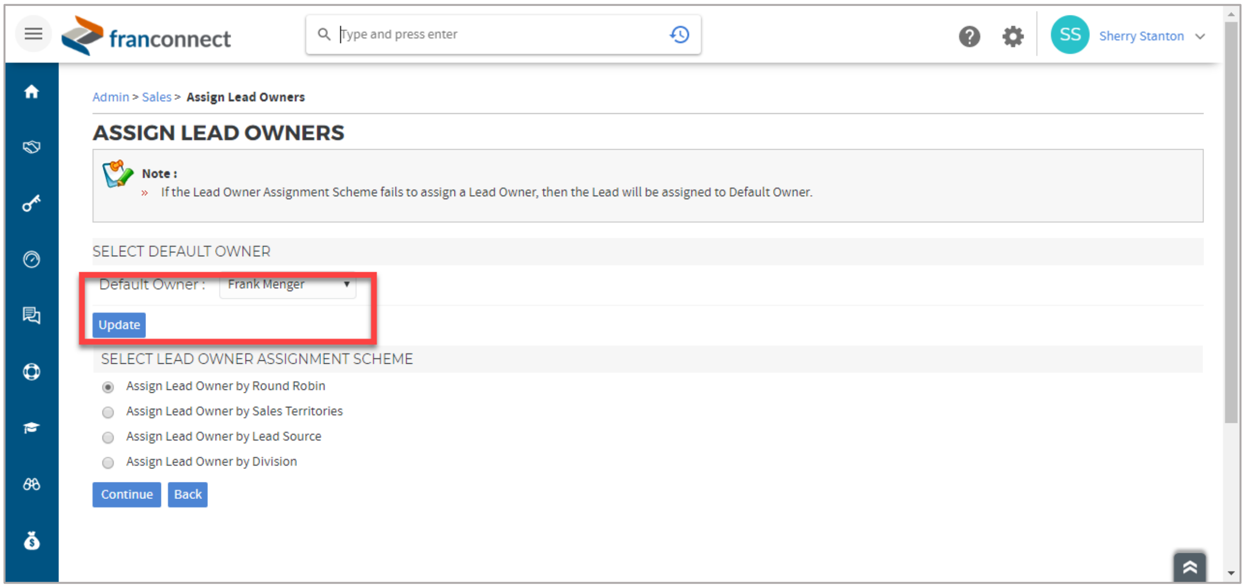
If you choose to **Reassign**, you'll see a dialog listing the records associated with the user, and you'll be able to choose an active user to assign the items to.



You can click on the Count of any item type to see the associated items, but it is not possible to reassign individual items. You are not required to fill out all the reassignment fields. Any you leave blank will remain associated with the deactivated user.

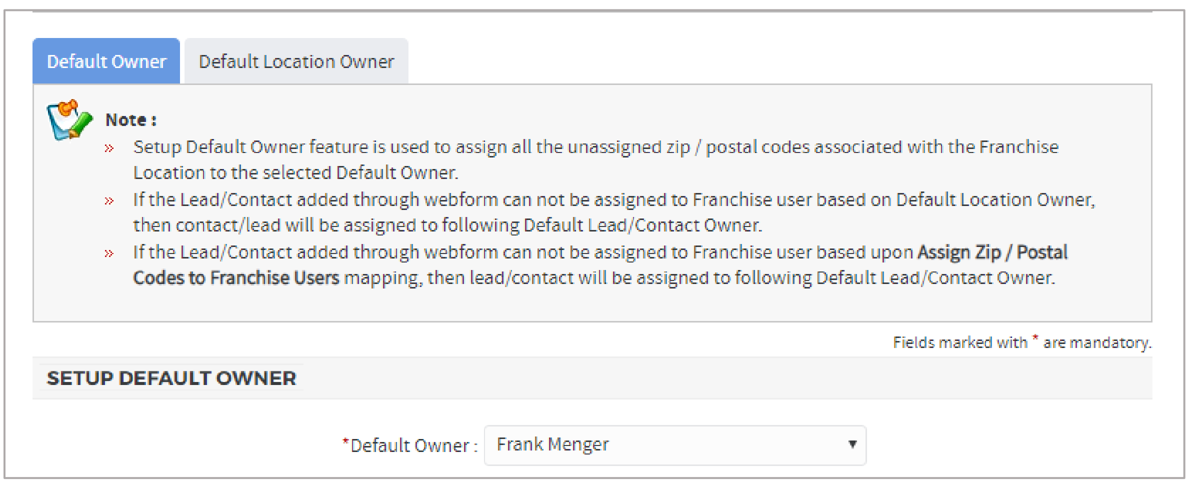
Reassigning Default Sales Owner

Go to **Admin > Sales > Assign Lead Owners**. If the desired user is the default Owner for unassigned leads, change the default owner to another user and choose “Update”.



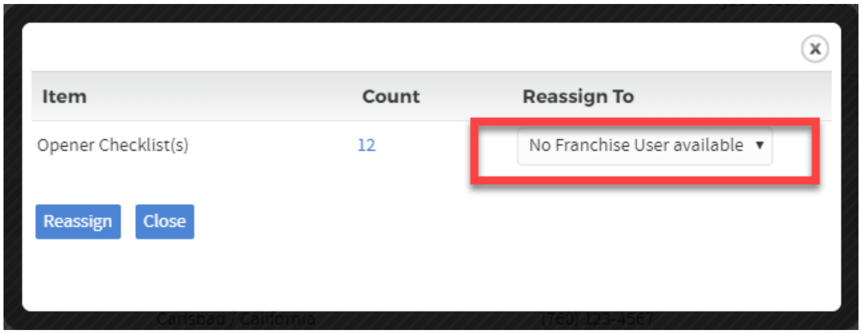
Reassigning the Default CRM Lead Owner

For Corporate Users, go to **Admin > CRM > Setup Default Owner**. If the desired user is the default Owner for unassigned leads, change the default owner to another user and choose “Update”.

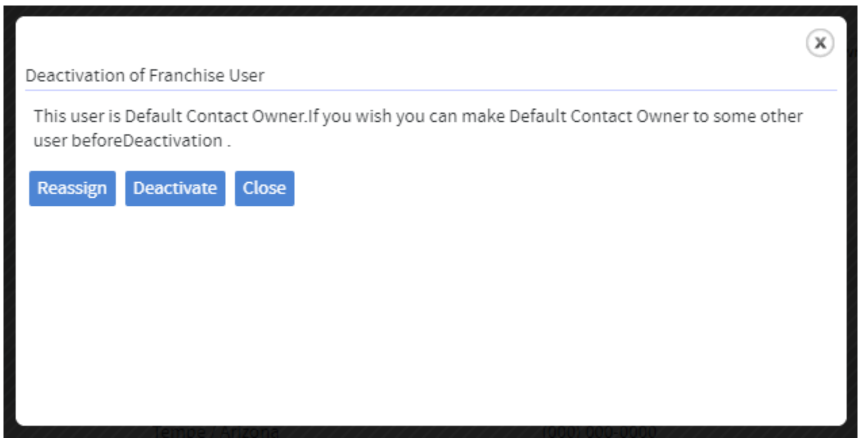


Deactivating Franchise Users

The procedure is exactly as described above for Corporate, Divisional and Regional users, with one additional consideration. If this user is the only user associated with the Franchise ID, you’ll need to enter another franchise user before you can reassign. If this is the case, you’ll see this message when you try to re-assign.



When deactivating or deleting a user, you may see the following error: “This user is Default Contact Owner. If you wish you can make Default Contact owner to some other user before Deactivation.”

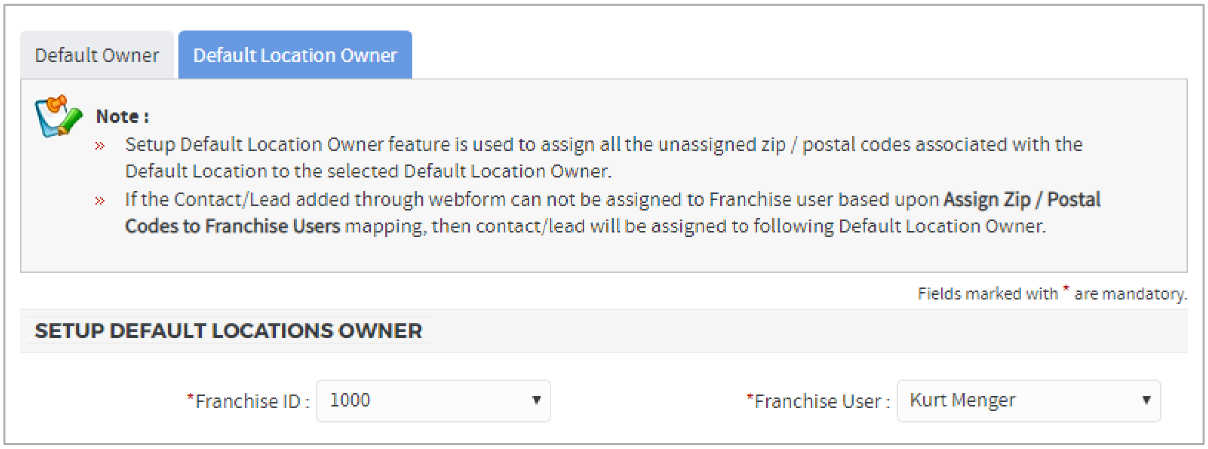


This item can’t be done on the “Reassign” screen. A user may be a Default Owner of incoming franchise development leads (Sales Module), if they are a corporate user, and/or of incoming franchisee business leads (CRM Module) if they are a franchisee user. You’ll need to check both places if you get the error message shown above. To correct this error, close this dialog box and follow the appropriate steps for the user type you’re deactivating. Close this dialog box and take the steps below to reassign Default Location CRM Lead Owner.

Reassigning the Default Location CRM Lead Owner

Go to **Admin > CRM > Setup Default Owner**.

If the user is a default owner for a specific service area, choose the **Default Location Owner** tab and select the Franchise ID that the user belongs to. Reassign the franchise ID to the new owner and choose "Update".



Review User Roles and Permissions

To avoid unnecessary data mistakes, it's best to limit user roles to just the data or screens that each user needs to see. This is done in the **Access Control > Roles** interface.

Introduction to Managing Users

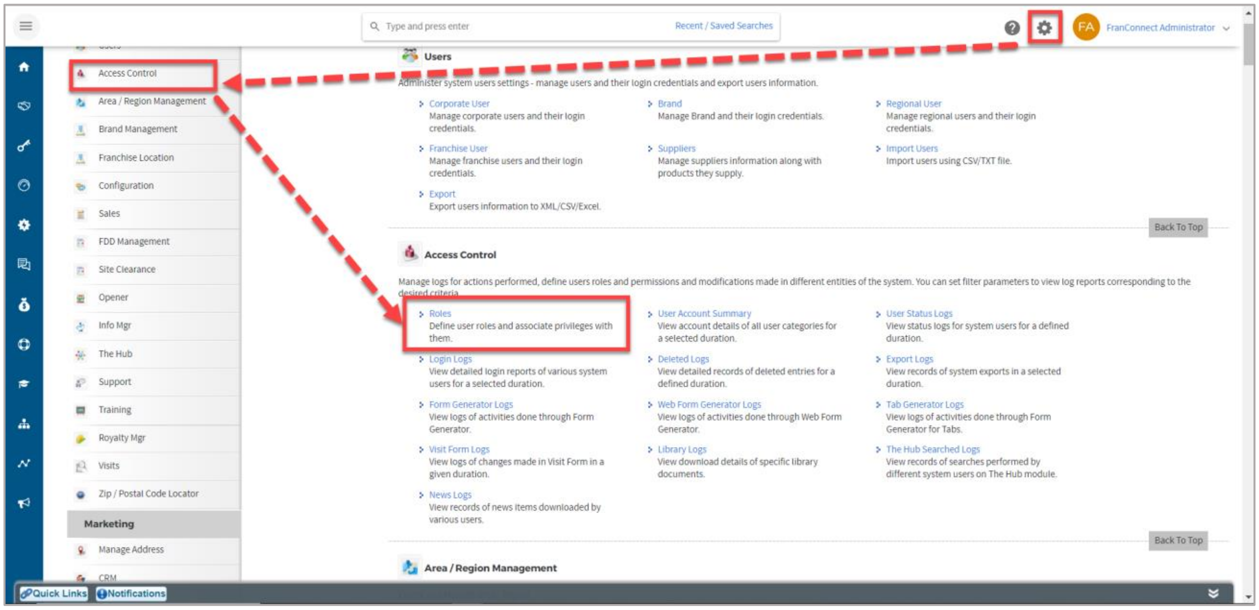
There are different user types, based on the roles performed in FranConnect. They are outlined in the chart below.

User Types	What records they can see	What software they can access
Corporate Users	Information for all records	See all licensed modules. If assigned an administrator role, also see setup gear next to login ID, which allows access to the Administration Page for setup and modification of licensed modules.
Divisional Users	Information for the brand or other divisional entity that they are associated with, if the system hosts multiple brands across a franchisor	See all licensed modules.
Regional Users	Information for the geographical region that they are assigned to	See all licensed modules.
Franchise Users	Information for franchises that they are associated with. Single-unit owners see only one unit; multi-unit owners can see all units they are associated with.	No access to Sales or Info Manager modules. If assigned as a unit administrator, may administer other users only in their owned units.

In order to manage a user, you need to know what type of user they are, to navigate to their user record. If you are making many changes, you may wish to export a list of users first, to have an easy reference to the user types of the people you're deactivating. To export users, go to **Admin > Users > Export Users**. Choose **Export as Excel** without specifying any parameters to get a complete user list.

Viewing Roles and their users

To see what roles are available in your system, choose **Admin > Access Control > Roles.**



You'll see a list of Roles, divided by what kind of user they apply to. Click on the blue Role Name to see the list of privileges that role has, and change tabs to see the users assigned to that role.

Admin > Access Control > Roles > ***Develop**

Roles Profile | Assigned Users

Role Type: Corporate Level

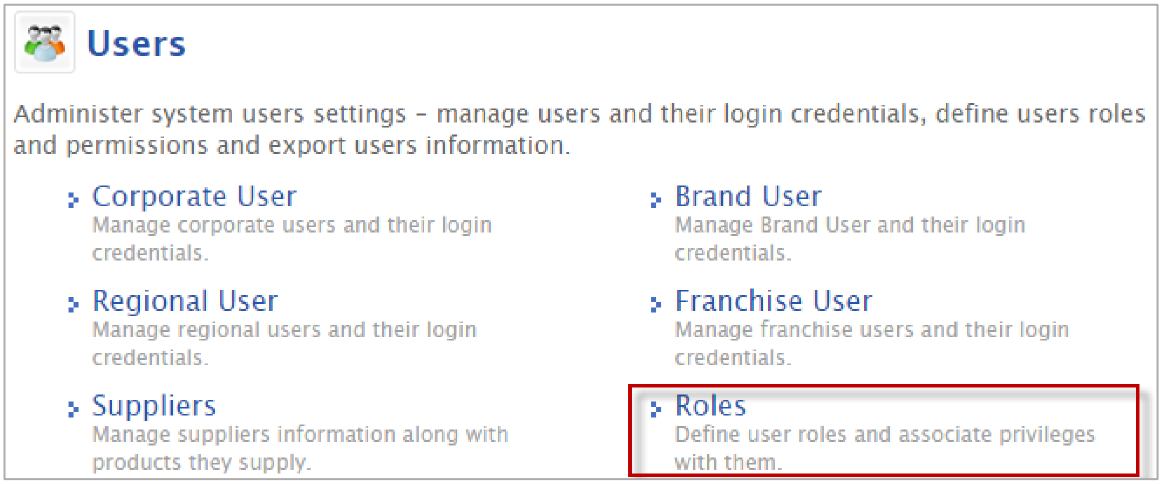
ROLES

No.	Privileges	Description
1	Can Manage Administer	Grants access to Administer module
	Can Administer Users	Grants access to Admin Users section
	Can Manage Corporate User	Grants access to Admin Corporate User
	Can Manage Brand	Grants access to Admin Brand
	Can Manage Regional User	Grants access to Admin Regional User
	Can Manage Franchise User	Grants access to Admin Franchise User
	Can Manage Supplier	Grants access to Admin Supplier
	Can Manage Export	Grants access to Admin Export
	Can Manage Users Import	Grants access to Users Import

Creating Roles

In FranConnect, Roles help you designate privileges (responsibilities) to users. This ensures that users only have access to those system functions that are necessary for the completion of their job.

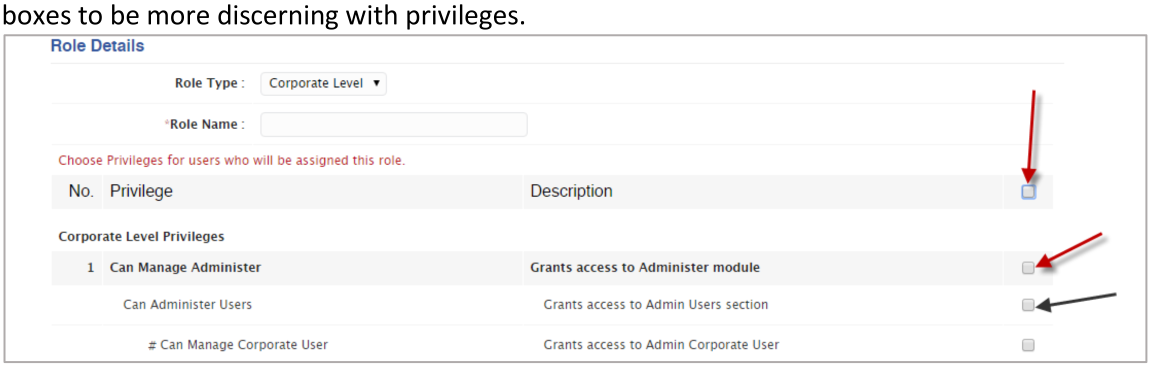
1. From Admin, select **Roles.**



2. Click **Add New Role**.

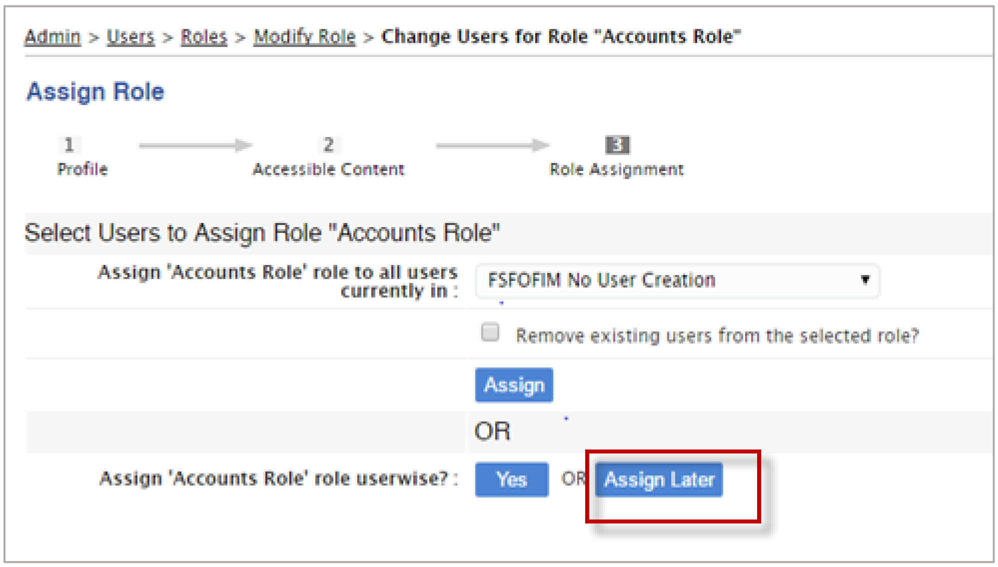
3. Click on the drop down to select the Role type: **Corporate**, **Brand**, **Regional**, **Franchise** Level and then input the Role Name.

4. Click on the master check box to select all the privileges in that section or select the individual boxes to be more discerning with privileges.



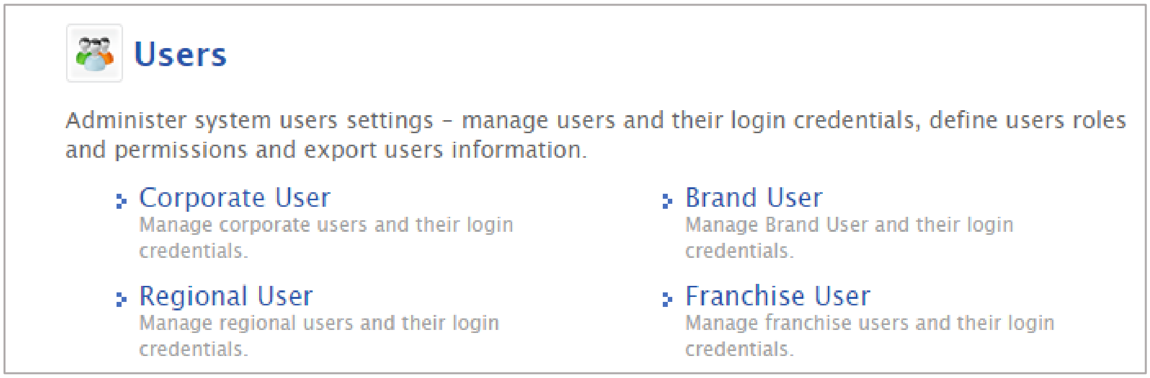
5. Lastly, select **Yes** or **No** to grant access to Documents and News then click **Submit**.

6. After clicking **Submit** you can assign the role to a user who is already in another role, you can select who you want to assign the role to, or select assign later to postpone placing a user into this role.

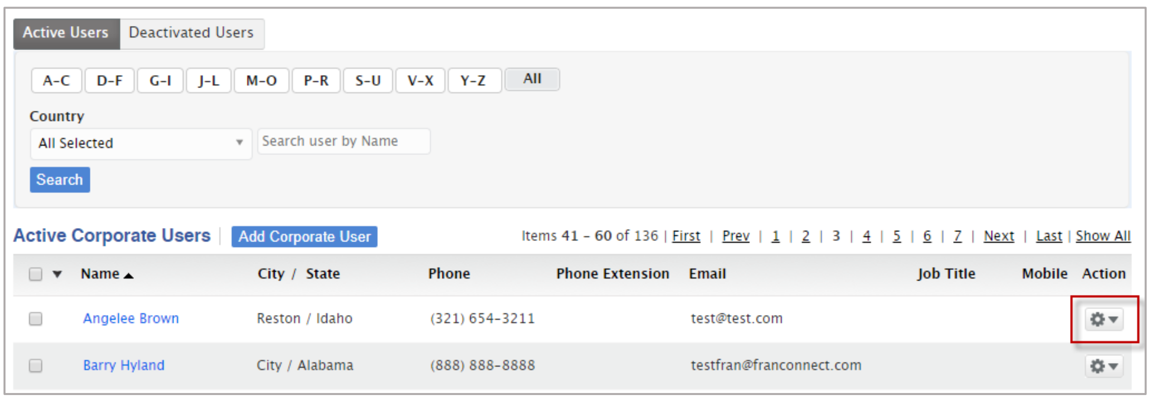


Associating Roles with Users

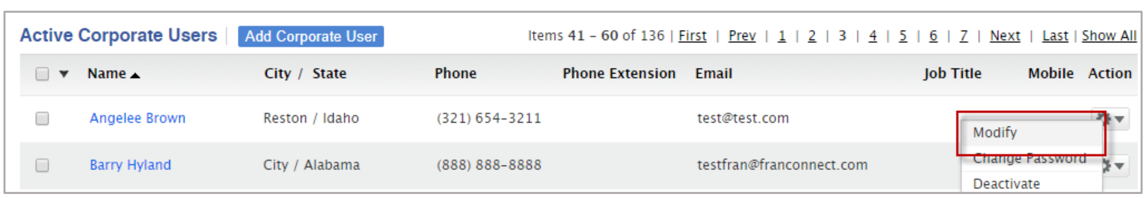
1. From the Users section in Admin choose the user type, **Corporate**, **Brand**, **Regional** or **Franchise.**



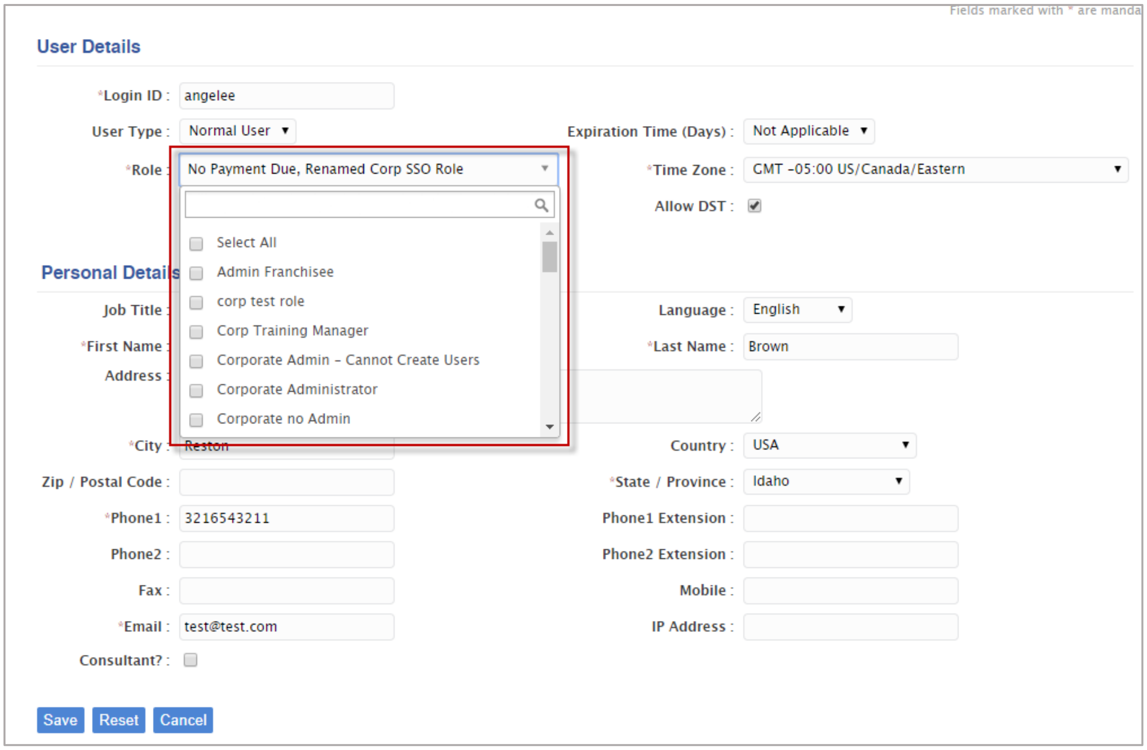
2. Click the action wheel beside the user you want to associate with a Role.



3. Click **Modify**.



4. From the Role Dropdown, select the role(s) you want to give the user.

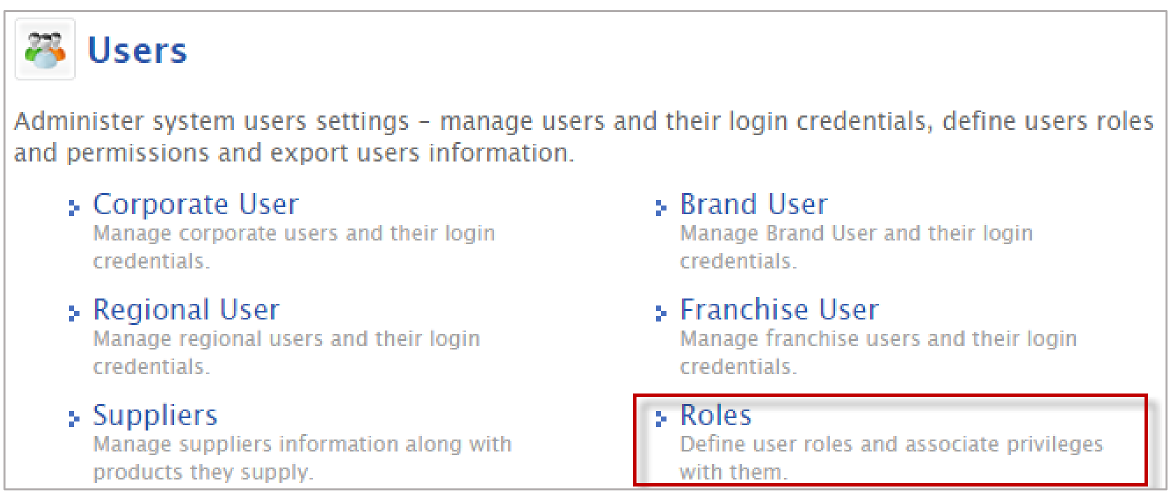


5. Click **Save**.

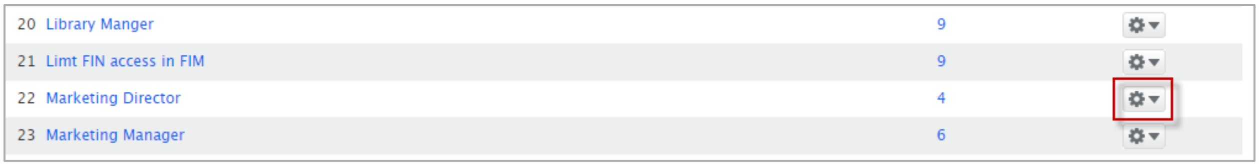
Changing Role Permissions

If you find that you need to adjust privileges, you can make edits to the Roles you've already created.

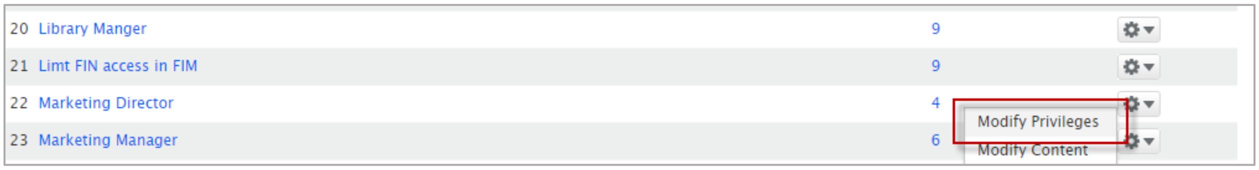
1. From Admin, select **Roles**.



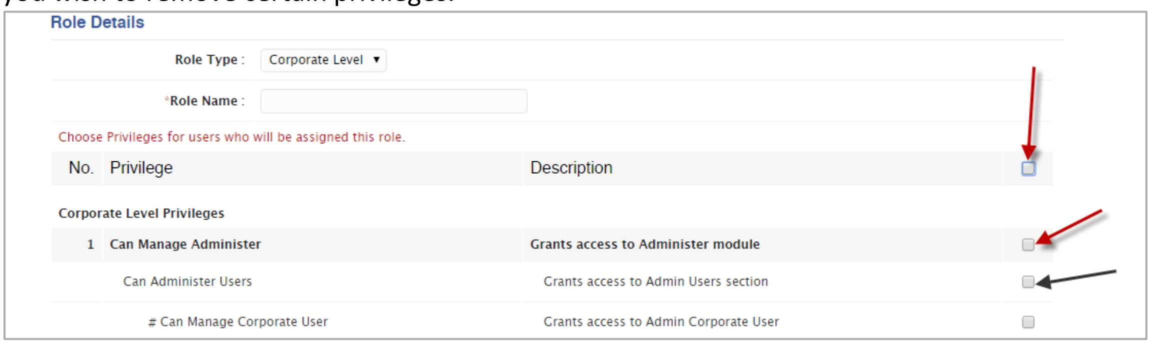
2. Select the action wheel for the Role you want to adjust.



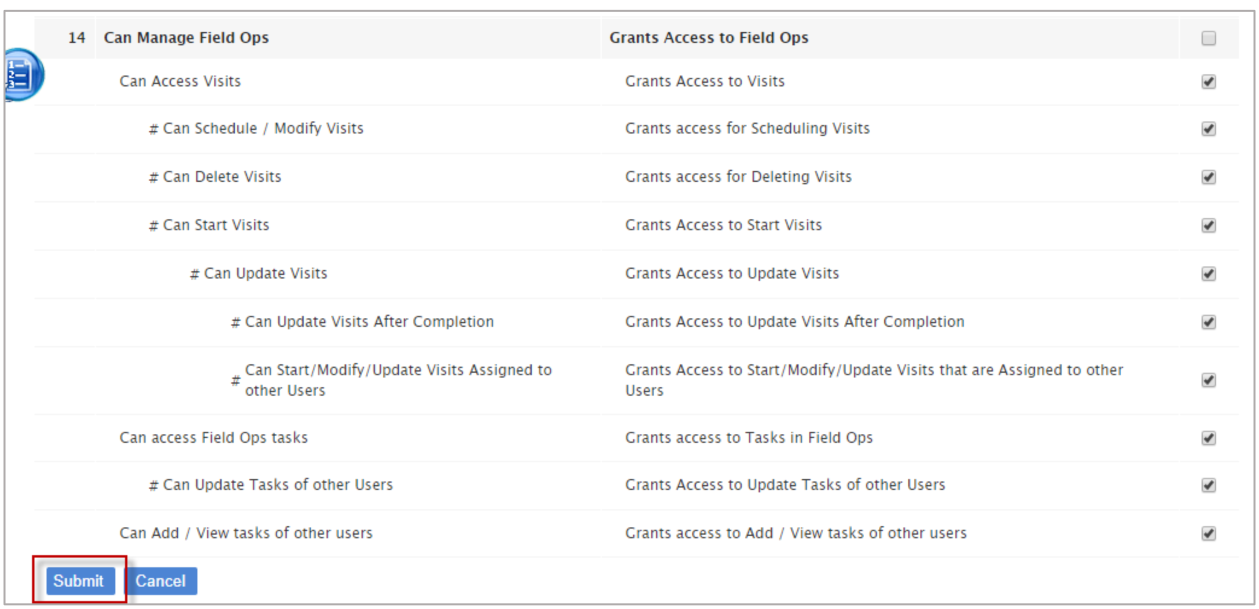
3. Select **Modify Privileges**.



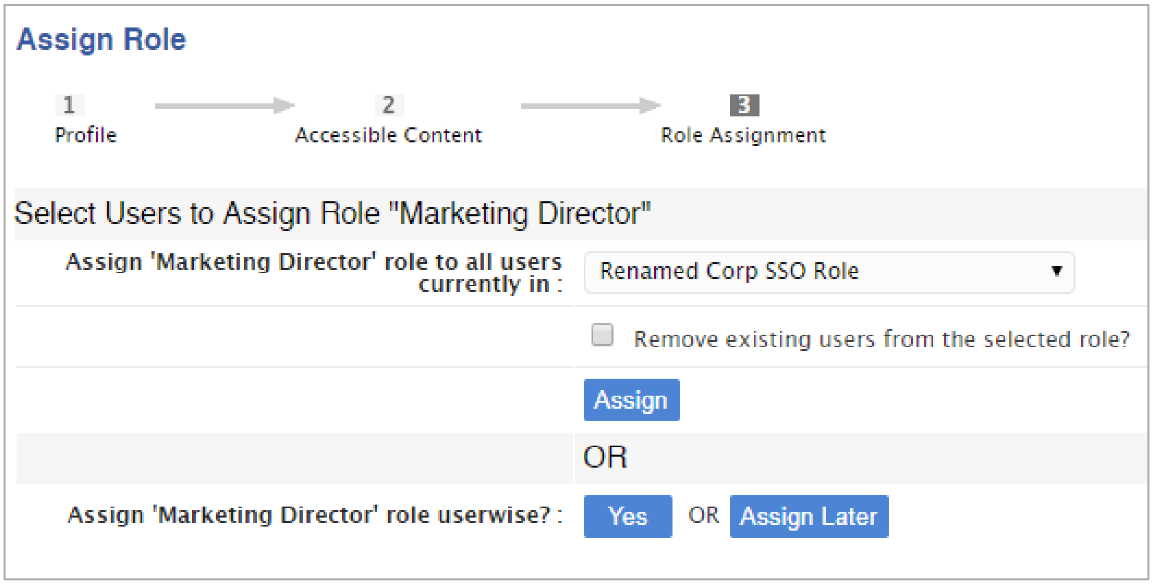
4. Click on the master check box to select all the privileges in that section or select the individual boxes to be more discerning with privileges. Boxes granting privileges can also be unchecked if you wish to remove certain privileges.



5. Click **Submit**.



6. After clicking **Submit** you can assign the role to a user who is already in another role, you can select who you want to assign the role to, or select assign later to postpone placing a user into this role.

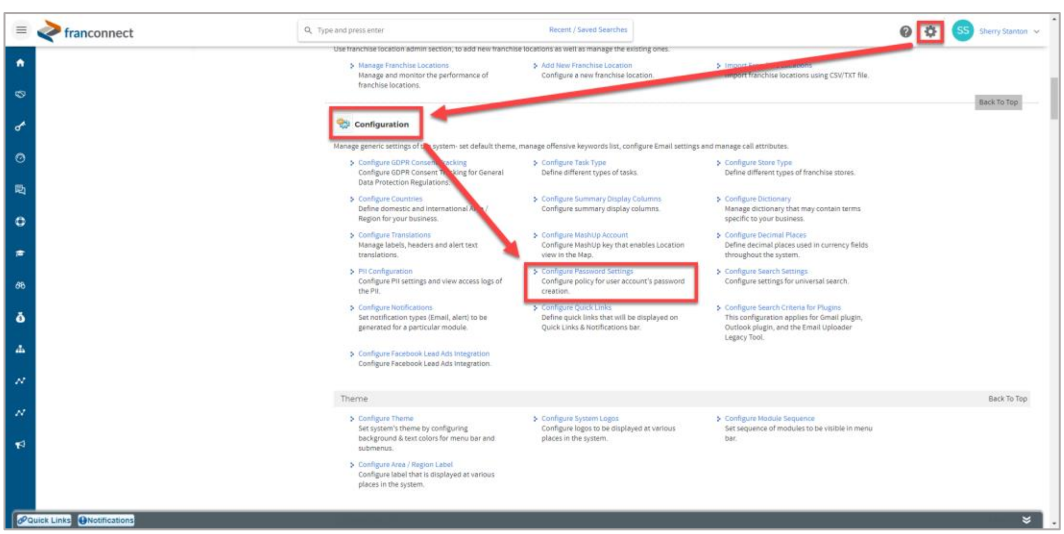


Review Your Password Security

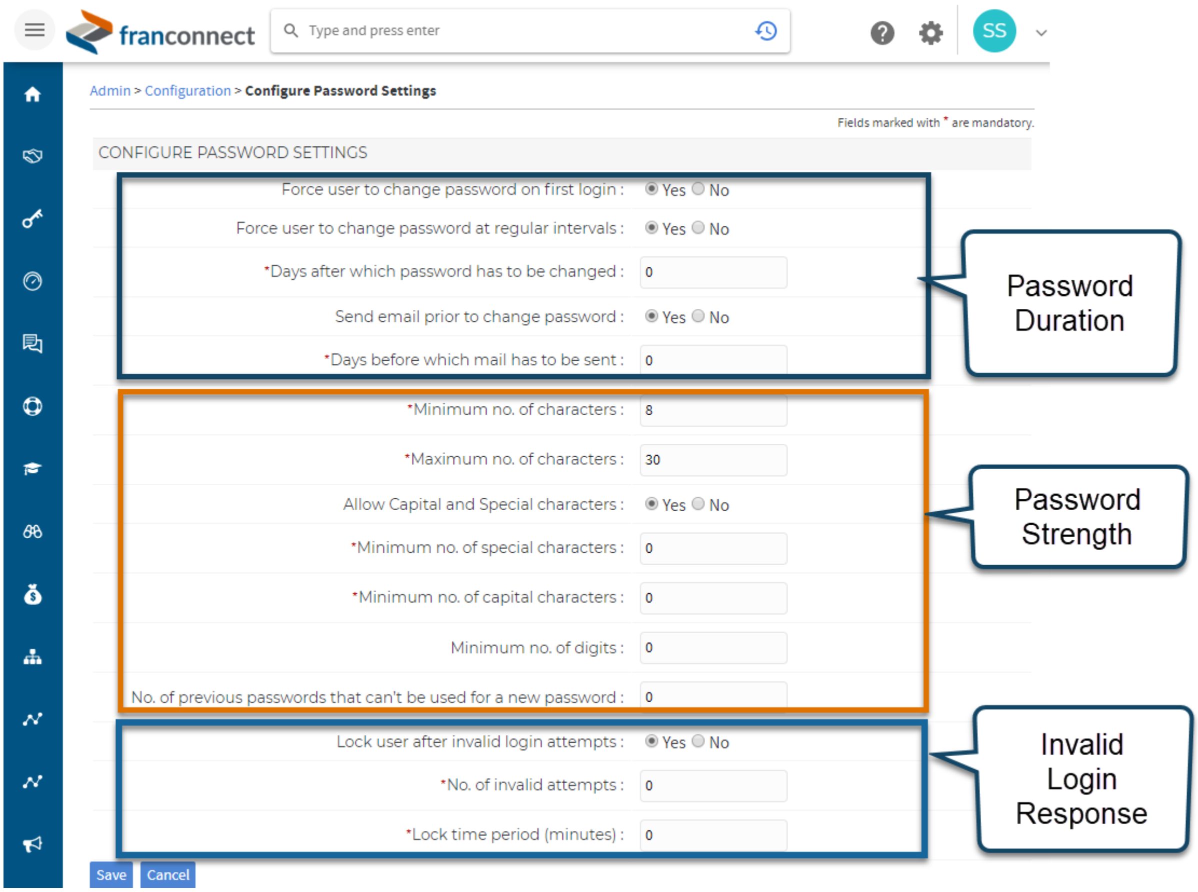
When you set up a user in FranConnect, they will need a user ID and a password to access the system. Their user ID will be associated with one or more Roles, which determine what portions of FranConnect that they see and which functions they can use. To prevent unauthorized use of FranConnect, a password is associated with each user ID.

Specifying Password Requirements

You can set up several parameters for passwords, in the Admin > Configure >



You can define the requirements for passwords in this screen.



Defining Password Security Parameters

There are three criteria that FranConnect lets you control to keep your data safe, described here.

Password Duration – changing passwords frequently is one defense against malicious parties who try to guess passwords using automated methods. There's a balance between discouraging outsiders, and changing passwords so often that legitimate users need password help frequently. It's advisable to force users to change their password on the first login, so that even the person who set them up does not know their password once they have logged on. If you choose this option, it's not necessary to set a strong password when you set the user up initially, since they will be changing it immediately anyway.

Forcing users to change their passwords at regular intervals is desirable but not required; your decision will be balanced between the sensitivity of your data and the technical acuity of your user community. If you have no PII concerns, and a low-experience community, you may choose not to force password changes routinely. If you choose intervals to change the password, you will choose the number of days of the interval – for example, every six months is an interval of 182 days. It's convenient for users if you advise them before their password expires, and you can choose the number of days ahead, typically from 1 to 7 days. In addition, you can strengthen password security by preventing users from using previous passwords, for example jumping back and forth between two passwords, to keep security higher.

Password Strength – the harder a password is to guess, the more secure it is. In this section of the screen you can set a minimum number of characters – the default is 8 – and a maximum number of characters. You can set this quite long, for more security, but typically the default of 30 characters exceeds what most users are willing to type to enter the system. Requiring special characters such as capital (upper-case) letters, symbols such as **#, $, !,** etc, and numbers makes passwords harder to guess through automated methods, and is recommended.

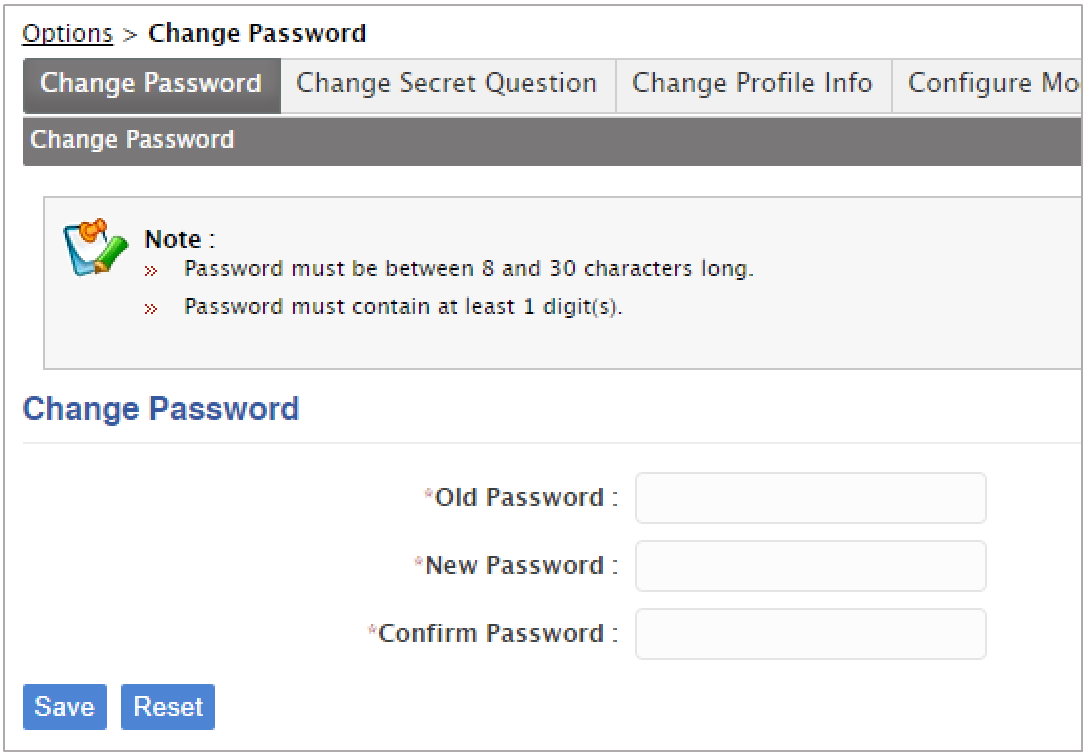
Response to Invalid Logins – another way to make it harder for malicious parties to guess passwords is to lock users out after a limited number of login attempts. In this section, you can specify the number of attempts before a user is locked out, and the period of time for which they are locked out before they may attempt login again.

CHANGING PARAMETERS FOR EXISTING USERS

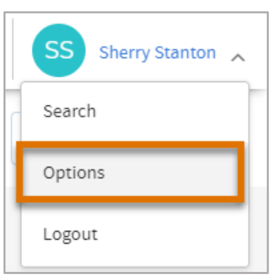
If you change your password parameters and users are in the system, you'll be asked if you want to have your users change their passwords to conform to the new guidelines on the next login. You can choose "Yes" to bring everyone into conformance, or "No" to grandfather existing passwords until the next scheduled reset time.

Administering Passwords

Users are assigned passwords when their user records are made initially, and you have the opportunity to force them to change their passwords, both on first receiving login credentials, and periodically. Users changing their passwords see this screen. It displays the parameters for password strength, and requires their old password, to ensure that they have the right to change the password, and then a correct entry of the same new password twice in a row to prevent mistyping the new password.



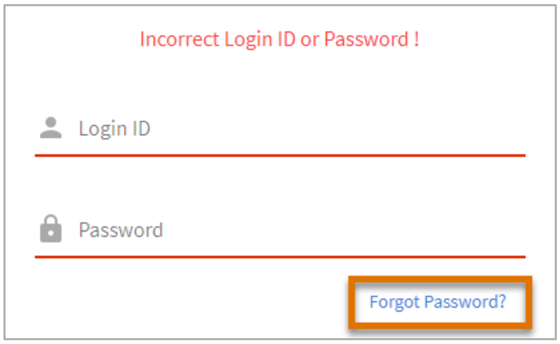
Users can additionally change their password at their discretion from their own Options screen, accessed by clicking the drop-down next to their login ID at the upper right of the interface.



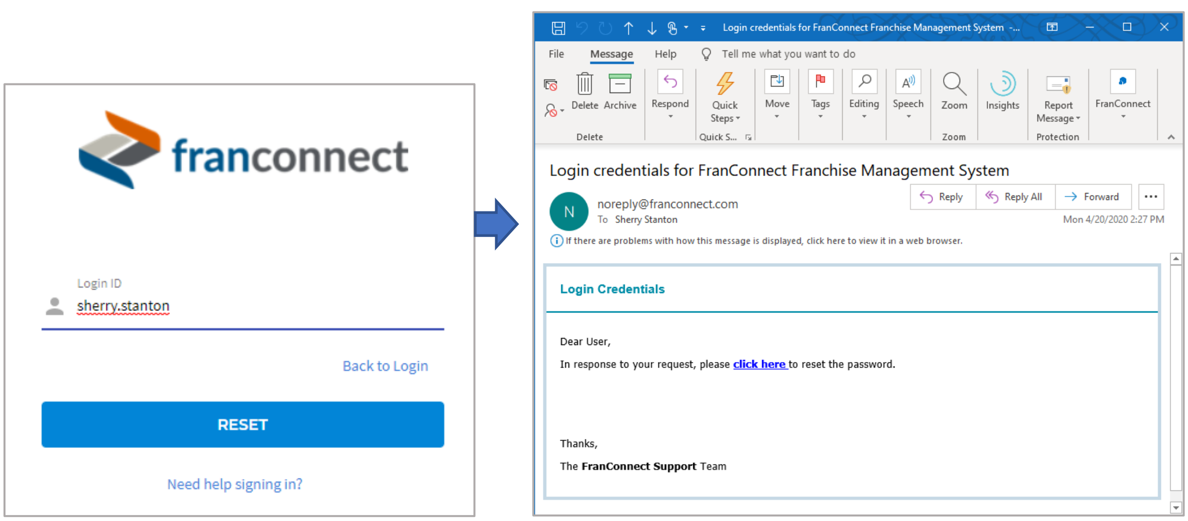
Resetting Passwords

Users resetting their own passwords

If a user logs in with the wrong username/password combination, a dialog is displayed that lets them know that they have entered the wrong combination and gives them the option to reset their password by having a link sent to their email address.

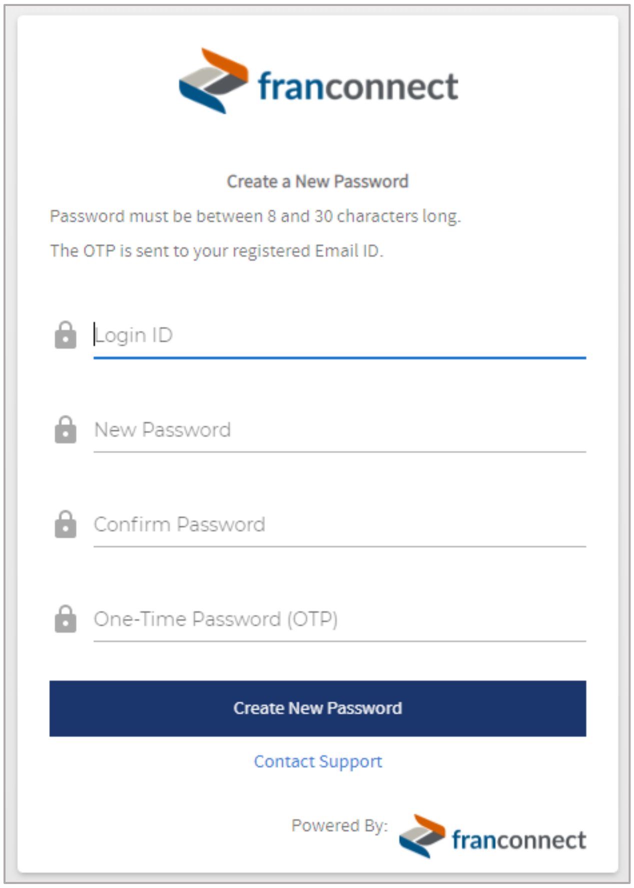


Clicking on the “Forgot Password” link takes the user to a screen that asks for their login ID and to press a “Reset” button, which will send an email to the address associated with the account. If the Login ID entered isn’t in the system, the error message “This Login ID does not exist” will be displayed, indicating that it’s the ID and possibly not the password that is the problem.



When the user clicks the link in the invitation email, two things happen.

- They will be sent another email with a One-Time password, to use in the reset screen. One-time passwords are an important feature to prevent malicious re-use of the password reset screen link.
- They will be taken to the password reset screen, which will show them the password parameters and ask for their login ID, and for them to type their new password twice (to avoid mis-types). This is the time when they will be asked for their One-Time Password from the second email, as well.

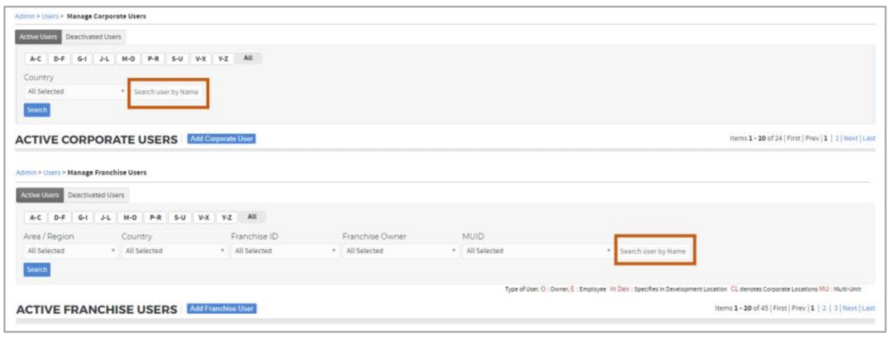

franconnect
Create a New Password
Password must be between 8 and 30 characters long.
The OTP is sent to your registered Email ID.
Login ID
New Password
Confirm Password
One-Time Password (OTP)
Create New Password
Contact Support
Powered By:
franconnect

Administrators resetting passwords

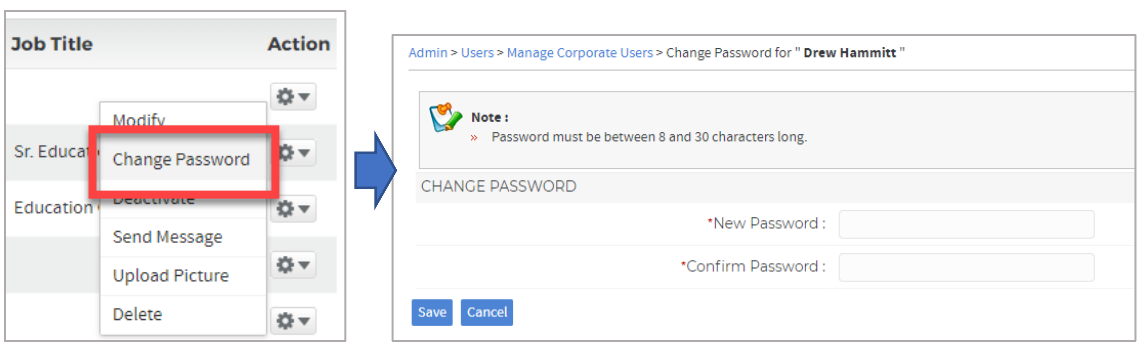
Occasionally a user needs help in getting into their system and requires help from the system administrator. When a user needs help, determine the following:

- Is the user a corporate, divisional, regional or franchise user? You will administer each type in a different place.
- What is the user's login ID?

Go to **Admin > User Administration** and choose the appropriate user type, and search for your user by name. Note, if the user is not found, they may be a different user type, for example a franchisee instead of a regional user. Try each user type before adding a new user.



When you have located the user, you can change their password directly from the action wheel.

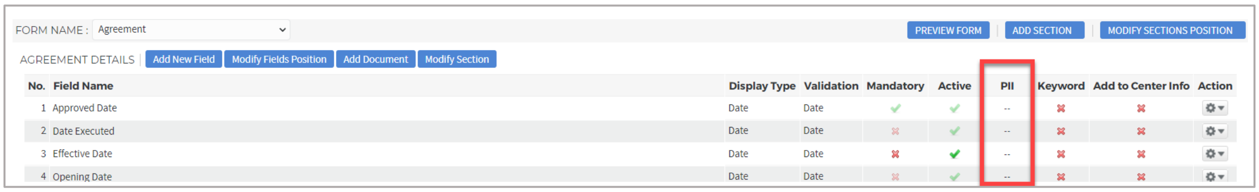


The new password you choose must conform to the rules you have set up in the system, but when you change it, the user will not be challenged for a one-time password or asked to change it on login; it is as though the user had changed it from their Options screen.

If, after a password reset, a user still has a problem, it may be that they are not typing their User ID into the system the way it has been assigned. To check for this, choose "Modify" from the action wheel for the user's record, and check the User ID against what they are entering. If they wish to change their User ID, for example to match other IDs they use, you can do this in this screen.

Determine if you choose to password-protect Personally Identifiable Information (PII)

Some information inside FranConnect, such as financial data, shouldn't be in plain sight for any user who has credentials. For this reason, you can flag fields which contain this information, and then users will need to know the password to retrieve this information. You can see whether fields are flagged this way in the Form Generator tab. They'll be flagged in the PII column.



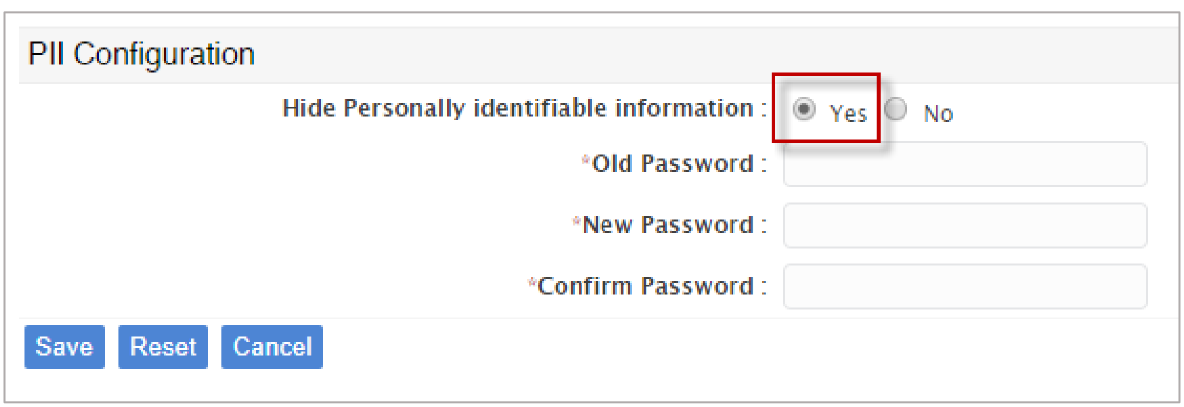
Using PII Configuration

PII allows you to hide information in fields that contain Personally Identifiable Information like SSN. From PII Configuration in Admin you can create a password that will show the PII details.

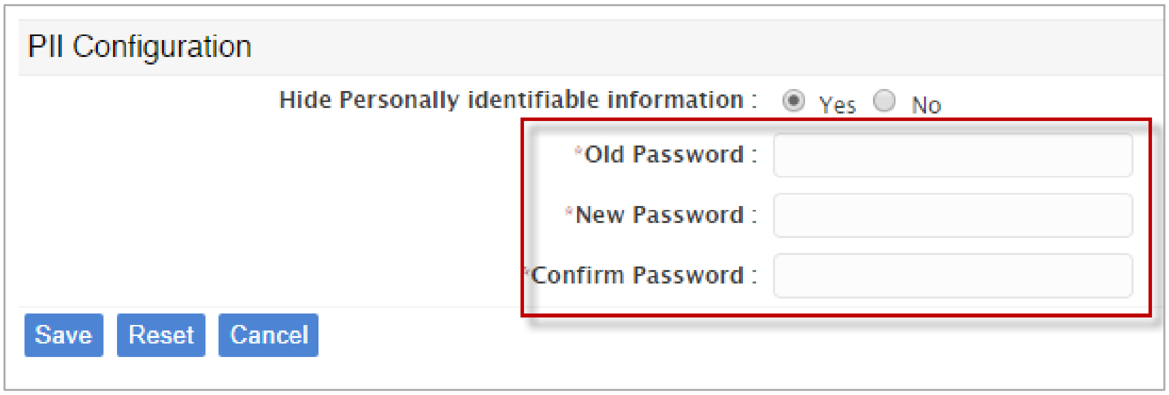
To add a password for PII fields

1. Under Configuration select **PII Configuration.**

2. Click the **Yes** radio button to Hide Personally Identifiable Information.



3. Assign a password.

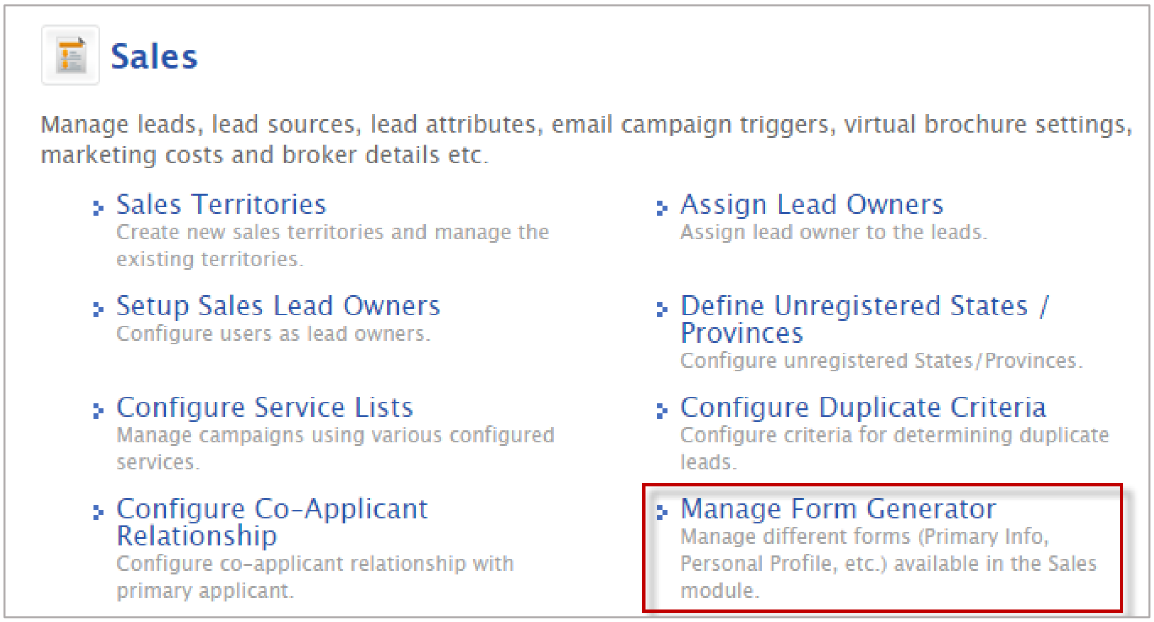


4. Click **Save.**

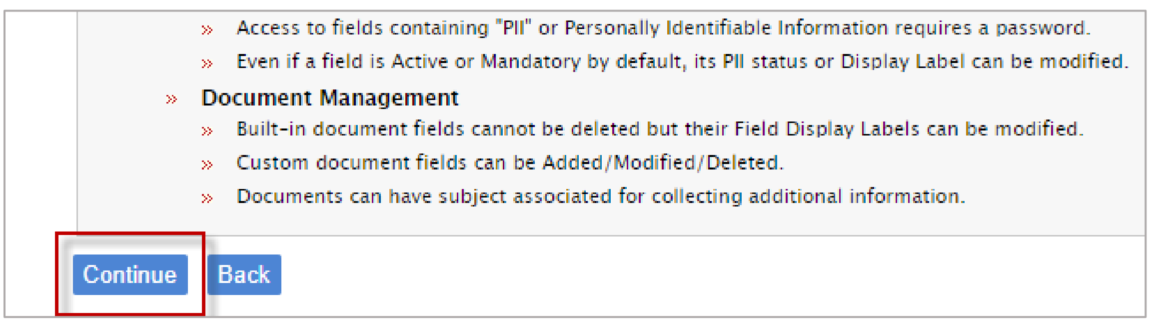
To create PII fields

Enabling the PII password is just the first step to ensuring PII fields are protected. Once you have enabled the password you will want to select the fields that should be protected. This can be done from the Form Generator in Sales or Information Manager.

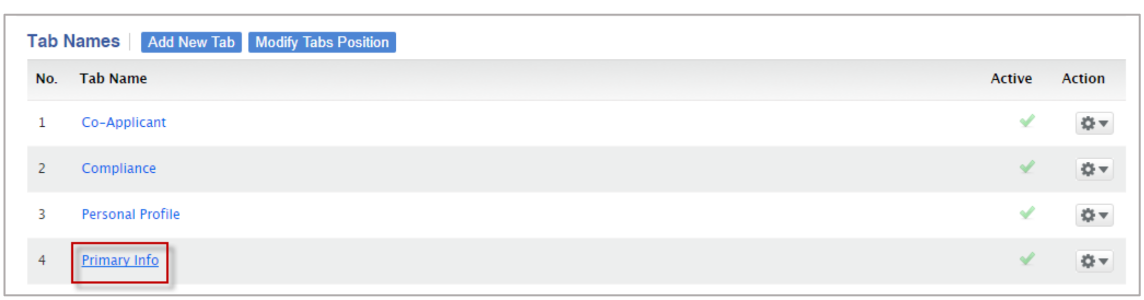
1. From Admin, Under Sales or Information Manager select **Manage Form Generator.**



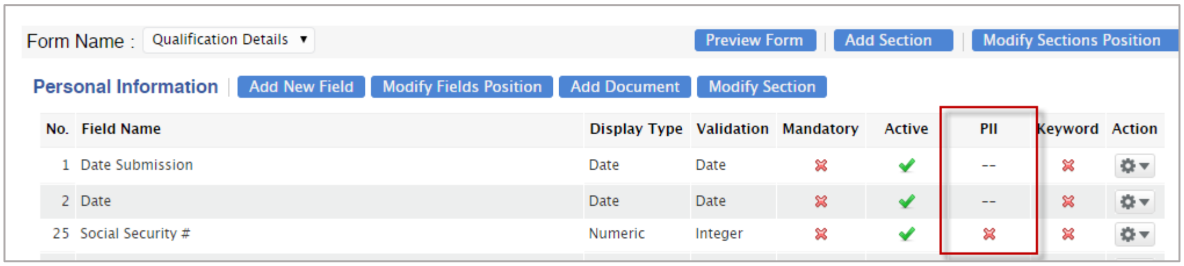
2. Click **Continue**.

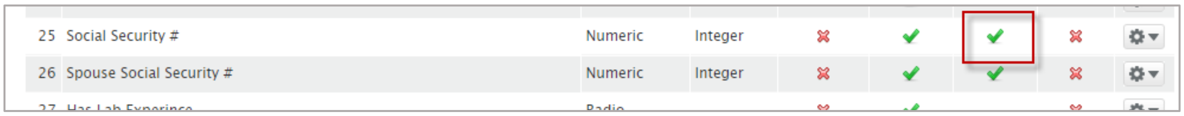


3. Click the tab you want to update.



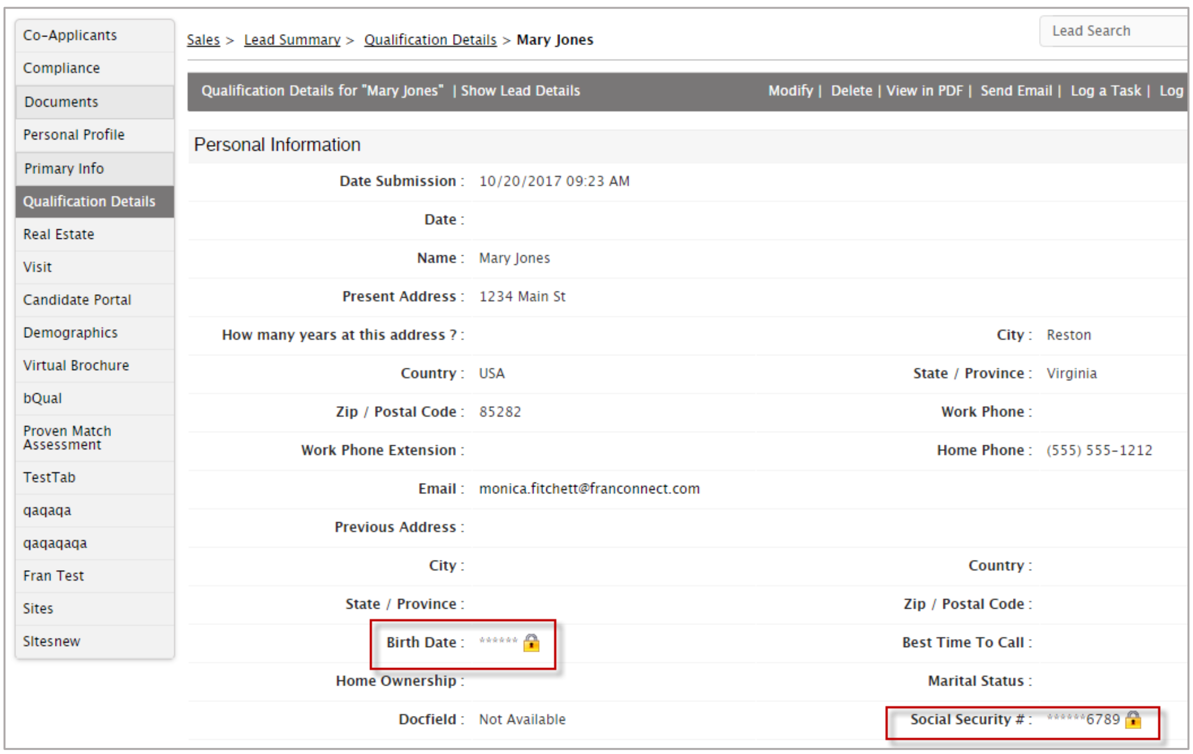
4. Click the "**X**" under the PII column to enable protection for that field.



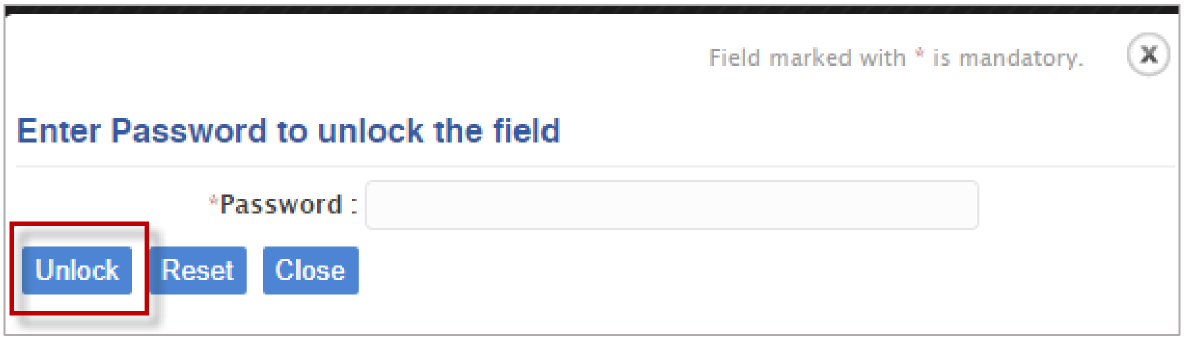


To view data in PII fields

1. From the record you want to view, click on the lock icon.



2. Input the PII password then click **Unlock**


Field marked with * is mandatory.
Enter Password to unlock the field
*Password :
Unlock
Reset
Close