Wolters Kluwer
When you have to be right

Configure Staff

Quick Start Guide

January 2022

CCH Incorporated

2050 West 190th Street, Suite 300

Torrance, CA 90504

Contents

Chapter 1 - Introduction 1

Highlights of Configure Staff 1

Guide Conventions 2

Getting Help 2

Chapter 2 - Getting Started 3

Account Administrator 3

Logging In to Configure Staff for the First Time 4

Setting Up 2-Step Verification Options 6

FAQs about 2-Step Verification 7

Smartphone Authenticator Overview 9

Advantages of Using Smartphone Authenticator 9

Supported Authenticator Apps 10

Getting Started with Smartphone Authenticator 10

Enabling and Disabling the Smartphone Authenticator Feature 10

Completing 2-Step Verification Using Your Smartphone 11

Navigating Configure Staff 14

Link Menu 14

Navigation Bar 15

Context-Sensitive Help 15

Quick Links Menu 15

Product Access Rights and User Licenses 16

Overview of Licensing/Product Access 16

Overview of Functional Rights 16

Adding Staff Members 17

Chapter 3 - Customizing Configure Staff 22

Managing Product Access with Groups 22

Creating Groups 22

Assigning and Removing Group Members 24

Editing Groups 25

Deleting Groups 26

Setting Up Teams 26

Adding Teams 27

Adding and Removing Team Members 27

Editing Team Detail 28

Deleting Teams 28

Contents

Setting Up Departments 29
Creating Departments 29
Editing a Department's Name 29
Deleting Departments 29
Setting Up Titles 30
Adding Titles 30
Editing Titles 30
Deleting Titles 30
Copying Office Configurations 31

Chapter 4 - Managing Staff Members 33

Changing Profile Information 33
Unlocking Staff Members 34
Deleting Staff Members 34
Resetting Passwords 35
Modifying Individual Product Functional Rights 35
Modifying Licensing/Product Access Settings 37
Printing the Licensing/Product Access Report 38

Chapter 1

INTRODUCTION

Configure Staff provides an easy means of managing the users of the following CCH ProSystem *fx* Internet products and services:

- My1040Data Toolkit
- Electronic Filing Status
- support.cch.com

User information can be easily maintained with Configure Staff because user data for all of the Internet-based applications is stored in a centralized database.

Highlights of Configure Staff

Listed below are highlights of Configure Staff:

- **Managing Users**. Add, modify, unlock, or delete staff members, and change passwords.
- **Single Sign-On**. After logging in, staff members can access other CCH ProSystem *fx* Internet products without having to sign on again.
- **Create Teams**. Organize staff members into project teams.
- **Audit Licenses**. Track the distribution of product user licenses. Generate a report of currently assigned licenses.
- **Flexible Product Access Management**. Assign functional rights to staff members individually or in groups.
- **Multi-Office Firms**. Copy Configure Staff configurations between offices.

Guide Conventions

To help you locate and interpret information easily, this guide uses consistent visual cues and a few standard text formats as follows:

- Specific entries to be made by the user appear in bold lettering. For example: Enter **Setup**.
- Italics are used for references to chapters and sections. For example: See *Chapter 2 - Getting Started* on page 7 for details.
- A message beginning with **Note**, **Tip**, or **Warning!** contains important additional information about the preceding text.

Getting Help

Online help for Configure Staff is available.

- To access general help, click the **Help** link located at the top of every page.
- To receive page-specific help, click the **Question Mark** icon when present.

Chapter 2

GETTING STARTED

Procedures for accessing Configure Staff for the first time and creating staff members are described in this chapter. The topics that are covered include the following:

- Role of the configure staff administrator
- Setting up 2 - Step Verification options
- Overview of product access rights and user licenses
- Adding staff members

Account Administrator

In Configure Staff, the Account Administrator has the primary role of accessing the application and adding staff. This user is created when your firm first licenses a CCH ProSystem *fx* product and cannot be deleted.

Firms with multiple offices can have an Account Administrator from one of the offices upgraded to a Super Administrator. A Super Administrator can remotely access and manage Configure Staff settings for offices other than the firm's Home office.

Notes:

- Offices must be linked with a Group code in order to access information from other offices in their firm. Group codes may be obtained from Customer Service.
- When other staff are given access to Configure Staff, they will have access to all features except the ability to access data in other offices, unless they are given multi-office access.

Logging In to Configure Staff for the First Time

When you first log in to Configure Staff, use the Account Administrator login ID, password, and URL supplied by CCH ProSystem *fx* via email. You will be prompted to change your password during the initial login.

1. On admin.prosystemfx.com, enter your User ID and password.

   Notes:

   - After a successful login, the system checks for the presence of the required browser. If the required version is not detected, a page will display with a link to download it. The system also verifies that the browser is configured to accept Javascript and cookies.
   - Password history is maintained for five passwords. Therefore, you will not be able to reuse your last five passwords.
   - You can retrieve your user ID by clicking *Forgot your User ID* and entering your Account number and Email address.

2. Enter the text in the image provided to validate your identity. Alternatively, you can click **Audio** to hear the letters pronounced.

   Notes:

   - The text is not case sensitive.
   - The text expires after 60 seconds. Click **Reset** to obtain a new image.

3. Click **Login**.
4. Enter a new password in the *New Password* field. The password must be between 8 - 32 characters. The password must contain an upper case and lower case letter, a number, and a special character. Any combination of letters, numbers, or symbols may be used, but spaces are not allowed.

   Notes:

   - Your user ID will be locked if you enter an invalid password five times. The administrator within your firm can log into admin.prosystemfx.com to unlock your user ID or reset your password.
   - When entering your password, an indicator will appear if Caps Lock is on.
   - You can display the masked password you have entered to verify it by clicking the Eye icon in the field.
   - Passwords expire every 90 days. You will receive warning emails prior to the expiration date with a link to change your password.

5. Re-enter your new password in the *Verify Password* field and click **Submit**.
6. Click **OK** on the confirmation message.
7. Select a question from the *Your question is?* drop-down list.
8. Enter an answer in the following field and click **Submit**. A confirmation message displays.
9. Click **OK**. The *Terms of Use* page displays.

10. After reading the Terms of Use, click **I Accept**.
11. To verify your identity, select one of the following:
    - **Email**. Sends a verification code to your email address.
    - **Text message**. Sends a verification code to your verified phone number.
    - **Authenticator App**. Allows you to confirm your identity via a separate authenticator app installed on your smartphone. This option is only available if your firm has enabled this option and you have paired your device to your user account. See Completing 2-Step Verification Using Your Smartphone for more information.
    - **Voice message**. Sends a voice message with a verification code to your verified phone number.

    Notes:
    - The options available depend on what is configured in your staff profile in Global Staff Manager.
    - The code expires five minutes after it is sent.
12. Click **Send the Code**.

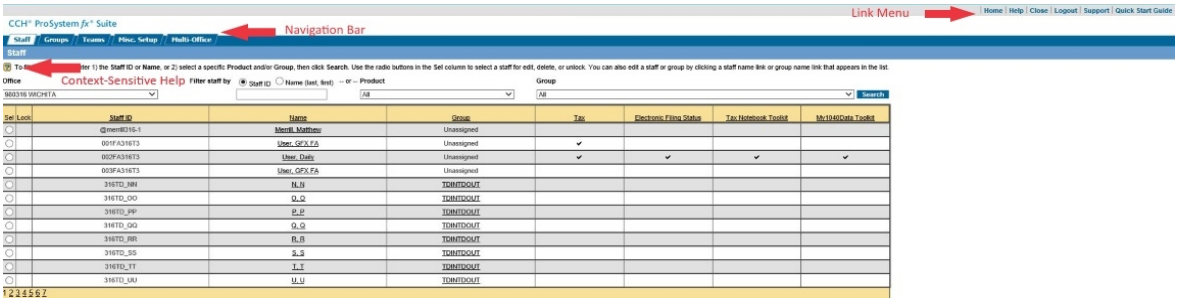
    Note: Codes sent by text or voice message expire five minutes after they are sent. Codes generated in the Google Authenticator™ app expire every 20 seconds.
13. Do one of the following depending on the verification option you selected:
    - If you selected the email, text, or voice option, enter the code on the *Verify Your Identity* window.
    - If you selected the Authenticator App option, do one of the following depending on which app you have installed.
        - **Wolters Kluwer Authenticator**. Tap **Approve** in the app on your phone or on the notification from the app. The login process completes automatically. No additional steps are necessary.
        - **Google Authenticator™**. Open the app on your phone. A unique and time-restricted code displays. Enter the currently displayed code on the *Verify Your Identity* window on your computer.
14. Select **Remember this device** if you are using a private and secure device and want to bypass 2-Step Verification for the number of days your firm has configured in Global Staff Manager.

    Notes:
    - Do not select this option if you are using a public device.
    - The verification process is specific to your user credentials, device, and browser. You can select to remember each device that you use to log in to the CCH® ProSystem *fx*® Suite.
15. Do one of the following:
    - If you used the email or text option, click **Submit**.
    - If you used the voice message option, click **Voice Message was Received**.

16. If your CCH® ProSystem *fx*® Suite profile does not include a phone number, you must set one now and complete the verification process.
    a. If your phone is already part of your user profile, you select a number or click the option to add a new phone number. If no phone number is included in your user profile or if you want to add another phone number to your profile, enter a phone number.
    b. Click **Continue**.
    c. Select whether you want to receive the account verification code by text or voice message, and then click **Send the Code**.
    d. When you receive the verification code, enter it in the *Account Verification* window, and then click **Submit**.
17. The Configure Staff home page displays.

Notes:

- There is a time-out period in Configure Staff. If the system does not detect any activity for a period of 30 minutes, your session will expire. “Activity” can be defined as clicking on a link or button on the page.
- If you open another browser session and log into another CCH ProSystem *fx* Internet product while logged into Configure Staff, you will be prompted for your ID and password.



Setting Up 2-Step Verification Options

The 2-Step Verification window allows default administrators to set login defaults for your firm. Note that the verification process is specific to the user, device, and browser. See FAQs about 2-Step Verification for more information.

To configure 2-Step Verification for your firm, do the following:

1. Go to admin.prosystemfx.com.
2. Log in with your Single Sign On (SSO) user ID and password.
3. Click **2-Step Verification**.
4. Select the verification method. By default, all staff members have the option to authenticate by receiving a verification code by text or voice message. In addition, you can select the **Smartphone authenticator** check box to allow staff to use an authenticator application supported by ProSystem *fx*.

- **Smartphone authenticator**. Select this option to use the WK Authenticator or Google Authenticator to verify your login. For more details, see SmartPhone Authenticator Overview.

5. Select an option to indicate the basis you want to use for determining when users must complete 2-Step Verification again on a trusted device.
   - **Never trust devices**. Select this option to require 2-Step Verification for every login on every device. Devices that are already trusted require 2-Step Verification after the existing trust expires.
   - **Require reauthentication of trusted devices every**. Select this option to trust a device but reauthenticate after a specified number of days.
     - Select the number of days before reauthentication is required. You can select from 7, 15, or 30 days.
       - **After the last 2-Step verification**. Select this option if you want all users to complete 2-Step Verification on a set schedule, such as every 15 days.
       - **After the last valid login**. Select this option if you want users to complete 2-Step Verification when they use a different computer, web browser, or have not logged in for a while, such as 15 days.

         Example: You have selected for users to reauthenticate 30 days from their last valid login on a trusted device. Harvey logs in and completes 2-Step Verification on his personal laptop for the first time on September 1. He continues logging in daily on this computer through September 10. Each day that he successfully logs in restarts the 30-day time frame. So, while on by September 1 his verification was valid until October 1, on September 10, the 30-day verification window has been extended until October 10.
6. Click **Submit** to save your changes.

FAQs about 2-Step Verification

Listed below are some of the most frequently asked questions about 2-Step verification in CCH ProSystem *fx*. Additional questions and answers can also be found in the Knowledge Base on our Support site.

Can my firm disable 2-Step Verification?

To provide maximum security and comply with pending IRS requirements, 2-Step Verification is now required for all firms that use the CCH® ProSystem *fx*® Suite. This option cannot be disabled. Your firm administrator can, however, configure how often you must complete verification.

How often must I complete the 2-Step Verification process?

You can reduce how frequently 2-Step verification is required by selecting the *Remember this device* during account verification. You should **not** select this option if you are logging in to a shared or public

computer.

If *Remember this device* is selected, you must complete 2-Step Verification:

- The first time you log in to the CCH® ProSystem *fx*® Suite using a unique device and browser combination.
- After you have cleared the cookies in your browser on a trusted device.
- After resetting your password.
- After a specific period of time that is set by your firm administrator in the 2-Step verification configuration options for your firm.

If you do not select *Remember this device*, you must complete verification each time you log in.

Why am I prompted to complete 2-Step Verification every time I log in, even after selecting *Remember this device*?

Your browser might be configured to delete cookies automatically. Disabling this option often solves the problem. Consult the documentation for your browser to learn how to change this option.

If you are not comfortable updating these settings, contact your firm's IT team for assistance.

What methods can I use to receive my verification code?

All users have the option to receive verification codes by text and voice message. If your firm has enabled the Smartphone Authenticator feature, you also can use a dedicated application on your iPhone® or Android™ phone to verify your identity. Consult your CCH ProSystem *fx* administrator to ask if this option is available in your firm.

Why is the option to receive a verification code through email being removed?

For security reasons, the IRS recommends that the ability to receive verification codes through email be disabled. Although this is not yet a mandate from the IRS, we anticipate that it will be in the near future.

To improve both security and convenience, we have replaced the email option with the ability to use authenticator apps for completing 2-Step Verification. You also can continue to receive verification codes via text messages or phone calls.

Will the phone number that I provide for 2-Step Verification be used by Wolters Kluwer for marketing or other purposes?

No. The phone numbers that you provide as part of the authentication process are used only to verify your identity when you log in to the CCH ProSystem *fx* Suite.

Which authenticator apps does CCH ProSystem *fx* support?

CCH ProSystem *fx* supports the use of two authenticator apps, Wolters Kluwer Authenticator and Google Authenticator™. These applications can be downloaded for free from the Apple® App Store® (for iPhones®) and Google Play™ (for phones on the Android™ platform). Use the links below to download and install the apps:

For iPhone®

Wolters Kluwer Authenticator

Google Authenticator™

For Android™

Wolters Kluwer Authenticator

Google Authenticator™

Which authenticator app should I use?

We recommend the Wolters Kluwer Authenticator app because it provides a more streamlined workflow, both during set up and verification. There is no need to retrieve and enter verification codes using Wolters Kluwer Authenticator. Instead, you complete verification with a single tap in the app. The CCH ProSystem *fx* Suite opens without any further action on your part once verification is completed.

While Google Authenticator™ does require a few more steps during setup and verification, this app might be preferred by users who are already use it for 2-Step Verification with other online services. During setup and verification, you will manually enter verification codes generated by the app.

Can I pair my phone to more than one authenticator app at a time?

No. To pair to a second authenticator app, you first must remove your pairing to the first authenticator app.

Smartphone Authenticator Overview

When you select to open the CCH® ProSystem *fx*® Suite you can also use the Smartphone Authenticator feature. Smartphone Authenticator is a type of 2-Step verification in which you pair your smartphone to your CCH ProSystem *fx* user account via a dedicated authenticator app. The app is used anytime you must complete 2-Step verification while logging in to the CCH ProSystem *fx* Suite. However, instead of receiving a verification code via text message or phone call, you verify your login or receive a code in the app on the paired device.

Advantages of Using Smartphone Authenticator

Verifying your identity through an authenticator app is more secure than receiving verification codes through text messages or phone calls. Text messages can be intercepted or redirected. Also, hackers who engage in SIM card swapping can steal a mobile phone number, and thus gain access to both your phone calls and text messages.

Authenticator apps avoid these risks by requiring that the person logging in have physical access to the paired device during login. If the device has a lock code or other security measure in place to prevent unauthorized use, that provides another level of security should the device be lost or stolen.

Another advantage of authenticator apps is that paired devices do not need Internet access or cell phone service to complete verification. If you use the Wolters Kluwer Authenticator app, you also can save time and steps. Instead of having to enter a verification code in CCH ProSystem *fx*, you simply tap **Approve** in the app to complete 2-Step verification.

Supported Authenticator Apps

CCH ProSystem *fx* supports the use of two authenticator apps, Wolters Kluwer Authenticator and Google Authenticator™. These applications can be downloaded for free from the Apple® App Store® (for iPhones®) and Google Play™ (for phones on the Android™ platform). Use the links below to download and install the apps:

For iPhone®	For Android™
Wolters Kluwer Authenticator	Wolters Kluwer Authenticator
Google Authenticator™	Google Authenticator™

Note: A staff member can only pair to a single authenticator app at a time.

Getting Started with Smartphone Authenticator

Smartphone Authenticator is disabled by default, but can be enabled by your firm's administrator. The recommended workflow for getting started with Smartphone Authenticator is as follows:

1. Decide if you want your users to use a specific authenticator app, or if both of the supported mobile apps are acceptable.
2. Enable Smartphone Authenticator in the firm's login options.
3. Communicate with your staff about this new feature. The following resources can help staff get started:
   - The topic Completing 2-Step Verification Using Your Smartphone provides the steps for pairing a device to your CCH ProSystem *fx* user account. It also includes the steps for completing 2-Step Verification using an authenticator app.
   - Short demonstrations on how to install and use the apps are available in the video library on our Support site.
   - The topic FAQs about 2-Step Verification addresses many of the common questions about 2-Step Verification.
   - Additional articles are available in the Knowledge Base on our Support site.

Enabling and Disabling the Smartphone Authenticator Feature

By default, the Smartphone Authenticator feature is disabled. A CCH ProSystem *fx* administrator can enable or disable this feature using the procedures below.

For more information about how Smartphone Authenticator works and why your firm should consider it, see Smartphone Authenticator Overview.

Important: Keep in mind the following when you're enabling or disabling Smartphone Authenticator:

- Once you enable Smartphone Authenticator, staff members will be able to pair devices to their CCH ProSystem *fx* user accounts. A paired device remains paired and can be used for authentication until the user unpairs it. This is true even if you later disable the Smartphone Authenticator firm option.
- Smartphone Authenticator must be enabled for users to unpair their devices. If you no longer want staff members to authenticate using this method, instruct staff members to unpair their devices before you disable the feature.

Enable Smartphone Authenticator

1. On the CCH® ProSystem *fx*® Suite login page, enter your credentials and the image text, then click **Login**.
2. Click **2-Step Verification**.
3. In the *Select method(s)* section of the 2 - Step Verification Configuration page, select the **Smartphone authenticator** check box.
4. Review the message which displays, and then click **OK**.
5. A save notification will display.

Tip: Once Smartphone authenticator is enabled, you can share the Help topic Completing 2-Step Verification Using Your Smartphone with your staff so that they can get started using the feature. They can also visit the video library on our Support site to view short demonstrations on installing and using the authenticator apps.

Disable Smartphone Authenticator

1. On the CCH® ProSystem *fx*® Suite login page, enter your credentials and the image text, then click **Login**.
2. Click **2-Step Verification**.
3. In the *Select method(s)* section of the 2 - Step Verification Configuration page, clear the **Smartphone authenticator** check box.
4. Review the message which displays, and then click **OK**.
5. A save notification will display.

Completing 2-Step Verification Using Your Smartphone

If your firm administrator has enabled the Smartphone Authenticator feature, you can use a dedicated authenticator app on your mobile device to complete 2-Step verification.

This verification method requires you to pair your mobile device to your CCH ProSystem *fx* user account using the authenticator app. After pairing is completed, any time you are prompted to complete 2-Step Verification, you may perform an action or retrieve a code in the app to complete authentication.

This verification method is more secure than receiving verification codes via phone calls or text messages. Also, unlike these other methods, your device does not need to be connected to the Internet or cell service. As long as your device remains paired to your CCH ProSystem *fx* user account, you can complete authentication.

See the sections below to learn more about how to setup and use this authentication method.

Install the Authenticator App

CCH ProSystem *fx* supports the use of two authenticator apps, Wolters Kluwer Authenticator and Google Authenticator™. These applications can be downloaded for free from the Apple® App Store® (for iPhones®) and Google Play™ (for phones on the Android™ platform). Use the links below to download and install the apps:

For iPhone®	For Android™
Wolters Kluwer Authenticator	Wolters Kluwer Authenticator
Google Authenticator™	Google Authenticator™

Your firm might provide guidance about which authenticator app to use. If your firm does not specify which application to use, the following information may be useful in helping you decide which app to use:

- **Wolters Kluwer Authenticator (recommended)**. This app provides the most streamlined approach to 2-Step Verification. There is no need to manually enter codes during setup or when completing verification. Once you've set up your account, you can complete verification and login with a single tap in the app.
- **Google Authenticator™**. This app generates random verification codes that expire every 20 seconds. To set up your user account and verify your identity with this app, you will enter the current verification code displayed in the app into the 2-Step Verification window.

See the documentation provided with your smartphone for instructions on installing apps.

Pair Your Device

1. Select **User Options** on the CCH® ProSystem *fx*® Suite login page.
2. Log in with your Single Sign On (SSO) user ID and password.
3. On the *User Options* page, click **2-step Verification Device Pairing**.
4. Select the authentication app you would like to use for 2-Step Verification.
5. Click **Pair device** beneath the selected app.
6. Select the type of phone you have.
7. Click **Continue**. The barcode that displays will be used to pair your device with the authenticator app.
8. Open the authenticator app on your smartphone.
9. Add your CCH ProSystem *fx* user account to the app. To view detailed instructions, click the link below that corresponds with the app you are using.

- **Wolters Kluwer Authenticator**
  i. Tap the plus sign (+) in the app.
  ii. Tap **Scan QR Code**.
  iii. Scan the barcode displayed on your computer.
  iv. Tap **OK** on the app. Your CCH ProSystem *fx* user account is now added to the app.
- **Google Authenticator™**
  i. Tap **Begin Setup**.
  ii. Tap **Scan Barcode**.
  iii. Scan the barcode displayed on the 2-Step Verification window with your phone. Your account is added to the app. The six-digit number that displays in the app is the current verification code. The number will expire after 20 seconds and be replaced by a new code.

10. Click **Continue** on the 2-Step Verification window on your computer.
11. If you are connecting to Google Authenticator™, enter the code displayed in the app in the 2-Step Verification window, and then click **Continue**. This step is not necessary for Wolters Kluwer Authenticator.
12. Click **Close** on the 2-Step Verification window on your computer.

Unpairing Your Device

1. Select **User Options** on the CCH® ProSystem *fx*® Suite login page.
2. Log in with your Single Sign On (SSO) user ID and password.
3. On the *User Options* page, click **2-step Verification Device Pairing**.
4. Click **Unpair device** beneath the paired app.
5. Click **OK**.
6. Click **Close**.

Changing and Restoring Your Pairing

You can change which app you use for 2-Step Verification at any time. However, you can only be paired with one app at a time. If you pair your device with one app, and then later pair with the other app, the pairing with the first app is disabled. If you later want to restore the original pairing, you can click **Pair again** to restore that connection. If you experience issues with your current pairing, you can also click **Pair again** to reset the pairing.

Complete 2-Step Verification with an Authenticator App

Once your device has been paired with the authenticator app, you can begin using the app for 2-Step Verification. The process for logging in and verifying your identity is as follows:

1. On the CCH® ProSystem *fx*® Suite login page, enter your credentials and the image text as you normally would, and then click **Login**.
2. When you are presented with the option to confirm your identity, select **Authenticator App**.

3. Click **Send the Code**.
4. Do one of the following, depending on which authenticator app you use:
   - **Wolters Kluwer Authenticator**. Click **Approve** in the app on your phone. You can also click **Approve** on the notification sent by the app. Once you click Approve, you are logged in to the CCH® ProSystem *fx*® Suite automatically.
   - **Google Authenticator™**. Open the app. A unique and time-restricted code displays. Enter the currently displayed code on the *Verify Your Identity* window on your computer. Then, click **Submit**.

     Note: Codes expire after 20 seconds. An animated circle below and to the right of the code indicates the amount of time left before the current code expires.

Navigating Configure Staff

This section provides an explanation of some of the navigational options and features available in Configure Staff.

Link Menu

At the top of every page is a link menu. The function of the links available on this menu are described below.

- Home. Click this link to return to the Configure Staff home page.
- Help. Click this link to access general online help.
- Close. Click this link to close the Configure Staff window.You will also be logged out of your single sign-on (SSO) session if Configure Staff is the only SSO application open.
- Logout. Click this link to log out of SSO. Logging out of your SSO session prohibits you from making updates to any open SSO applications until you have re-established a session. You will be prompted with a log in link should you want to continue updating.
- Support. Click this link to access the CCH ProSystem *fx* Support site.
- Quick Start Guide. Click this link to access a printable Quick Start guide in PDF format for Configure Staff.

Navigation Bar

Configure Staff provides a navigation bar, shown below, from which you can access its various administrative functions. Click one of the options displayed on the bar to access a specific feature or a sub-menu of options.

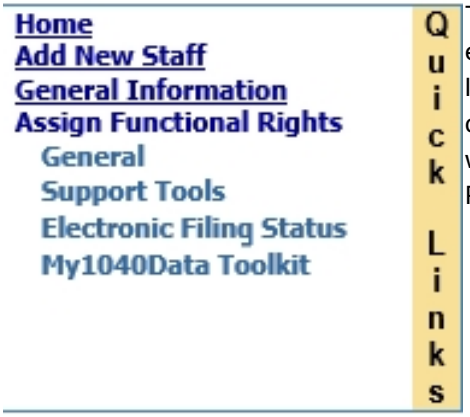
- **Staff**. Click this option to return to the Configure Staff home page.
- **Groups**. Click this option to access the *Groups* page. On this page, you can configure groups and assign staff members.
- **Teams**. Click this option to access the *Teams* page. On this page, you can configure teams and assign staff members.
- **Misc. Setup**. Position the mouse over this option to display a sub-menu for the following functions:
  - **Departments**. Select this option to add, edit, and delete departments.
  - **Titles**. Select this option to add, edit, and delete titles.
- **Multi-Office**. Click this option to access the *Multi-Office* page. On this page, you can copy configurations between offices.

  Note: The Multi-Office option only displays for users assigned multi-office access in Configure Staff on the *Functional Rights* page under General.

Context-Sensitive Help

To get page-specific help, click the **Question Mark** icon when present.

Quick Links Menu



The Quick Links menu is available on pages on which you edit staff profile information or configure staff product licenses or functional rights. It provides links allowing you to quickly navigate between pages. By default, the menu title will display as a tab in the upper-left corner of a page. Position your mouse over the title to display the full menu.

Product Access Rights and User Licenses

The primary function of Configure Staff is to provide your employees with access to CCH Internet products and services. The following sections describe the tasks involved in giving staff members access to products, such as assigning user licenses and basic product access, and granting additional functional rights for specific product features.

Overview of Licensing/Product Access

In Configure Staff, users are simultaneously assigned a user license, when required for a product, as well as given basic access.

Once users are granted product access, they will have limited access to product options until they are assigned additional functional rights. See the following section *Overview of Functional Rights* for details.

Note: The degree of product functionality available with basic access rights will vary by product or service.

You should select staff members for license assignment carefully. Once all licenses for a product have been distributed, no additional users will be able to access the product.

Note: Licenses can be re-assigned to other users.

For auditing purposes, Configure Staff tracks the total number of licenses purchased and assigned by product. A report is available to print detailed information for your records. The system also monitors for discrepancies between the number of licenses distributed versus those available.

If your firm reduces the number of user licenses for a product and the number of staff currently assigned licenses for that application is now greater than the total licenses available, a warning message will display when any staff member attempts to access the product. All staff will be locked out of the application until the licensing discrepancy is resolved. You will also be notified of this problem the next time you access Configure Staff.

Overview of Functional Rights

Configure Staff provides a great deal of flexibility in managing the level of access to Internet products. In addition to the basic functions staff can use when granted product access, they can be assigned additional functional rights to specific features within a CCH ProSystem *fx* Internet product or service.

This flexible approach of giving functional rights allows firms to define their own roles for staff members.

There are two methods that can be used to assign functional rights: individually or in groups.

Assigning Functional Rights Individually

Functional rights for staff can be configured on an individual basis. This user-specific approach is the most expedient and flexible manner to assign product access for small offices. For offices with large staff, this method may become inefficient.

Assigning Functional Rights with Groups

Configure Staff allows you to associate users into units, called groups, which share identical functional rights. The same rights can be defined for a group as for an individual. The main advantage of using groups is that when any user is assigned to a group they automatically inherit that group's rights. For many firms, groups can provide a time-saving alternative for assigning functional rights.

Staff members are not restricted to functional rights inherited from their designated group. They can be assigned additional rights on an individual basis.

Other benefits of groups include the following:

- Groups provide an excellent manner of enforcing standardization for functional rights within an organization.
- Multi-office firms can copy group configurations between offices.
- Groups can be used to divide staff by department and assign appropriate rights.
- Groups are useful for sorting the staff members into lists.

See *Creating Groups* on page 22 for instructions on adding groups to Configure Staff.

Adding Staff Members

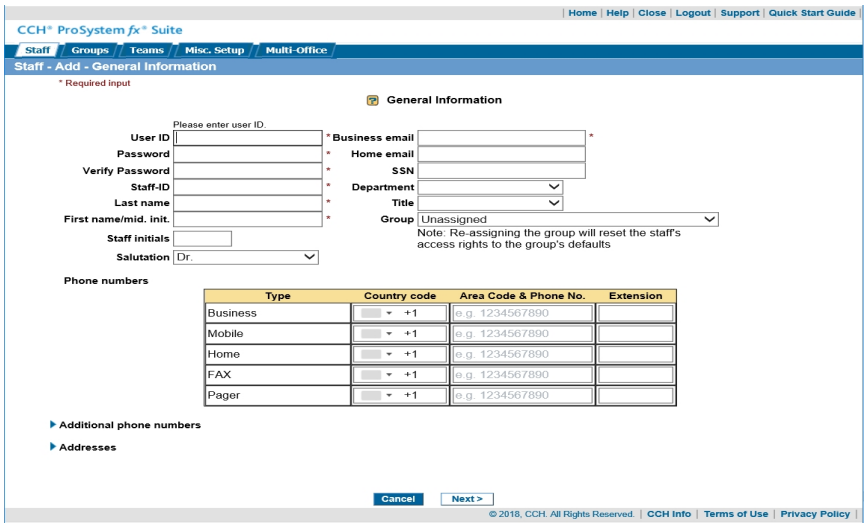
This section provides steps for creating staff members in Configure Staff.

If you want to use groups to assign functional rights, you will need to add them before proceeding with this procedure. See *Creating Groups* on page 22 for details.

The process of adding a user consists of the following tasks:

- Adding general/profile information
- Assigning user licenses and product access
- Assigning functional rights

1. Click **Add** on the Staff home page. The *General Information* page displays.



2. Enter the required information in the following fields.
   - **User ID**. The ID may consist of the following: letters, numbers, underscores, hyphens, periods, and the @ symbol. Spaces, colons, double quotes, and other special characters are not allowed. A minimum of six characters is required.

     Notes:

     - A six digit numerical User ID is not allowed. Such IDs are reserved for Account Administrators.
     - User IDs must be unique. If the User ID was previously used and deleted, it may not be added.
     - A User ID cannot end with a period.

   - **Password**. The password must be between 8 - 32 characters. The password must contain an upper case and lower case letter, a number, and a special character. Any combination of letters, numbers, or symbols may be used, but spaces are not allowed. Password history is maintained for five passwords. Therefore, you will not be able to reuse your last five passwords.
   - **Notes**:

     - Your user ID will be locked if you enter an invalid password five times. The administrator within your firm can log in to admin.prosystemfx.com to unlock your user ID or reset your password.
     - When entering your password, an indicator will appear if Caps Lock is on.
     - You can display the masked password you entered to verify it by clicking the Eye icon in the field.
     - Passwords expire every 90 days. You will receive warning emails prior to the expiration date with a link to change your password.

   - **Verify Password**. Enter the password again to confirm it.

- **Staff-ID**. The system populates this field with the same characters used for a member's User ID. Edit this field as needed. The staff ID must be unique within your account.
- **Last name**. Enter the user's last name.
- **First name/mid. Init**. Enter the user's first name and middle initial.

3. Enter a business email address. The email address may contain the following special characters: underscores, hyphens, periods, and the @ symbol. Spaces, colons, double quotes, and other special characters are not allowed. A minimum of seven alphanumeric characters is required for the email address.

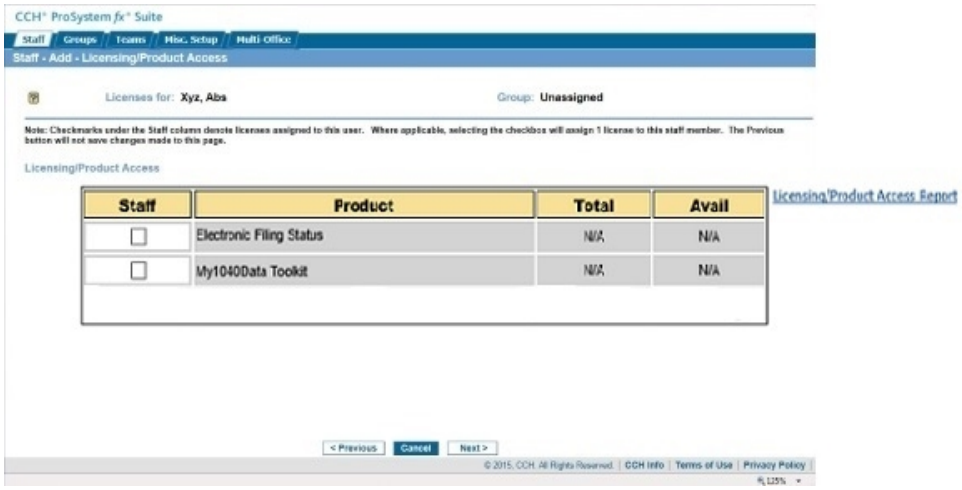
   Note: The email address does not need to be unique across all users. However, if you enter an email address that is currently assigned to an existing Tax and Accounting Destination Site user, a warning screen will appear. Click **Use selected user** if this is the same person and you want to use a single login for both destinations.

4. Enter further user contact information as needed.
5. If your firm is using customized groups, select one from the *Group* drop-down list.
6. Enter the staff member's phone numbers including area code for business, mobile, home, fax, and pager.

   In the *Country code* field, make a selection from the drop-down list next to the flag.

   Note: Phone numbers should only contain numbers. No special characters or spaces are allowed.

7. Click the **Expand/Collapse** arrows located at the bottom of the page to add additional phone numbers and address information for the staff member.
8. Click **Next**. The *Licensing/Product Access* page lists products for which your firm is licensed. It also lists the total number of user licenses available for each product.



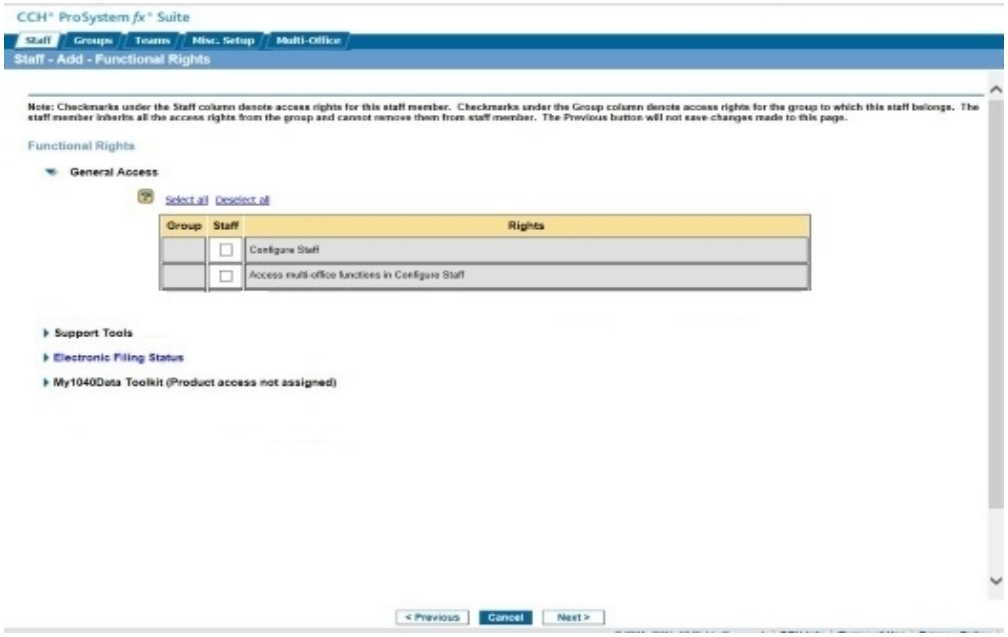
Note: "N/A" means "not applicable." If a product displays "N/A" in the *Avail* column, the number of users that may be assigned access to that product is unlimited.

9. Check the boxes to the left of each product for which you want to assign a user license, if applicable, and grant this user access.

   Notes:

   - User licenses do not apply to My1040Data Toolkit, but they must be checked to allow the user access.
   - The check boxes for products with zero available licenses will be disabled.

10. Click **Next**. The *Functional Rights* page displays a listing of licensed products.



11. Click the **Expand/Collapse** arrow located next to the listed products to display a list of product options for which you can grant functional rights.
12. Do one of the following:
    - **Select individual options**. Check the box in the *Staff* column adjacent to an option for which you want to grant this user access.
    - **Select all options**. Click the **Select all** link located above the listed options to give this staff member access to all of the product's features.
    - **Deselect all options**. Click the **Deselect all** link located above the listed options to remove all functional rights for this user.

Notes:

- For each functional right, a *Group* and *Staff* column are displayed. If a staff member is assigned to a group, check marks will display next to functional rights associated with that group in both the *Group* and *Staff* columns. These fields cannot be edited. You can only grant functional rights for product options this member has not acquired from their assigned group.
- For detailed information on the options listed for each product, click the Question mark icon located to the left of the product title.

13. Click **Next**. You will be returned to the *Staff* home page.

Chapter 3

CUSTOMIZING CONFIGURE STAFF

The advanced features of Configure Staff are covered in this chapter. These features allow you to customize Configure Staff to better meet your firm's unique needs. The following topics are discussed:

- Managing product functional rights with groups
- Organizing staff member into teams
- Adding department and title information to provide greater staff member profile detail
- Copying configure staff configurations between offices in a multi-office firm

Managing Product Access with Groups

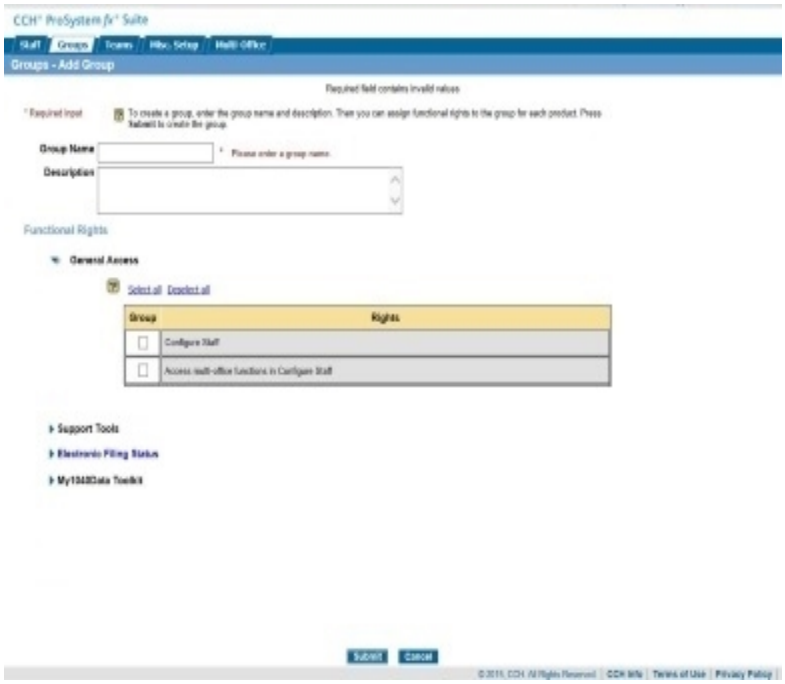
The following section covers procedures for adding, editing, and deleting groups. It also covers steps for adding or removing staff members from a group. For an overview of groups, see *Assigning Functional Rights with Groups* on page 17.

Creating Groups

To add Groups to Configure Staff, do the following:

1. Click **Groups** on the navigation bar. The *Groups* page displays.
2. Click **Add**. The *Add Group* page displays.
3. Enter a name in the *Group Name* field.
4. Enter descriptive detail in the *Description* field (optional).

5. Click the **Expand/Collapse** arrow located next to the product titles, listed below the *Description* field, for which you want to configure functional rights. The list of product options displays.



Note: Only products for which your firm is licensed display.

6. Do one of the following:
   - **Select individual options**. Select the check box adjacent to an option for which you want to grant this group access.
   - **Select all options**. Click the **Select all** link located above the listed options to give this group full access to all of the product's features.
   - **Deselect all options**. Click the **Deselect all** link located above the listed options to remove all product access rights for this group.

   Note: For detailed information on the options listed for each product, click the Question mark icon located to the left of the product, beneath the product name.

7. Once Group rights have been assigned, click **Submit**.

To assign multiple members to this group, use the procedure in the following section. To change group assignments individually, edit a specific staff member's profile. See *Changing Profile Information* on page 33 for details.

Assigning and Removing Group Members

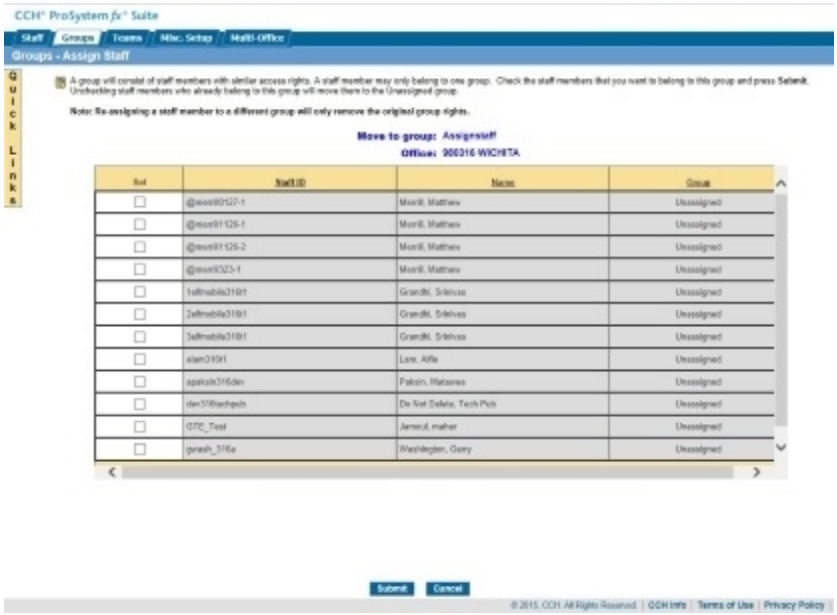
Review the following points before assigning group members:

- When staff are re-assigned to a new group, their current rights are reset and they inherit the defined rights of the new group. Additional rights can be granted to users on an individual basis. See *Modifying Individual Product Functional Rights* on page 35 for details.
- Staff members cannot be assigned to multiple groups.
- Staff members cannot be added to the Account Administrator group.

Use the following procedure to change a staff member's group assignment.

1. Click **Groups** on the navigation bar. The *Groups* page displays.
2. Select the radio button of the group to which you want to assign a staff member.

   Note: A Super Administrator or Multi-office administrator can assign staff members in other offices by making a selection from the *Office* drop-down list.
3. Click **Assign Staff**. The *Assign Staff* page displays a list of staff in your office.



4. Do one of the following:
   - **Assign staff members**. Check the boxes next to staff to be added to this group.
   - **Un-assign staff members**. Un-check the boxes next to staff to be removed from this group.

   Note: The user's current group assignment, displayed in the *Group* column, will change accordingly.
5. Click **Submit**. You will be returned to the *Groups* page.

Editing Groups

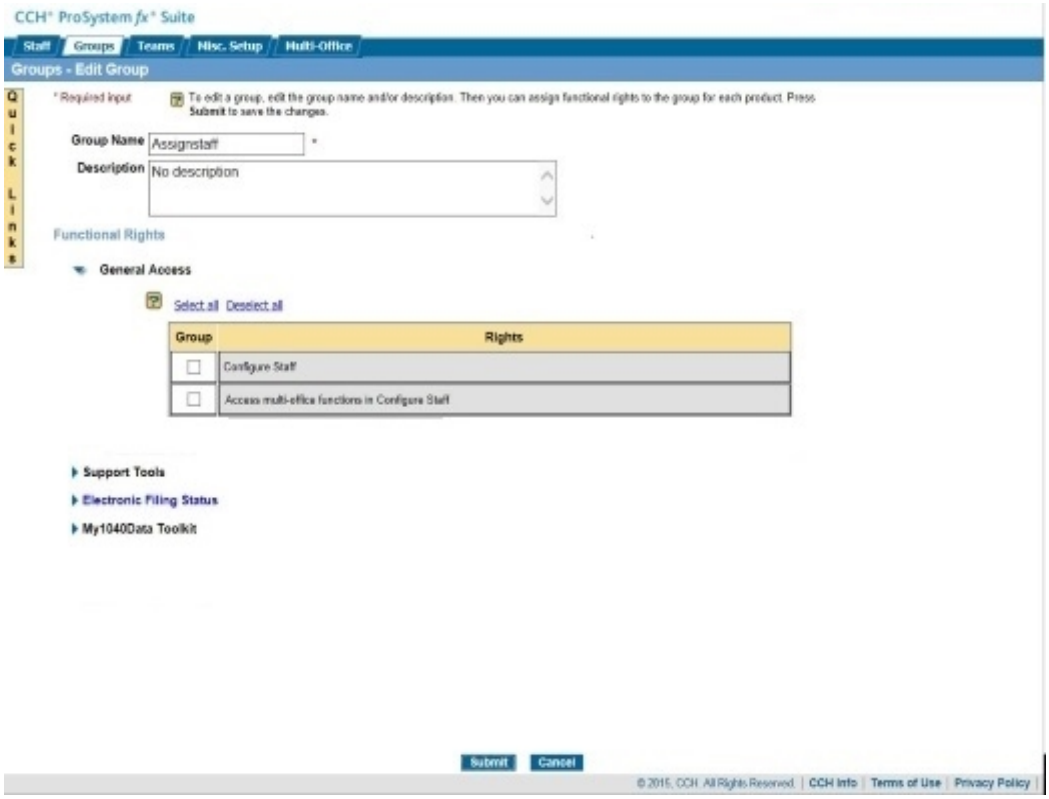
To make changes to a group's settings, (i.e., name, description, or functional rights) do the following:

1. Select **Groups** from the navigation bar. The *Groups* page displays.

   Notes:

   - If you are assigned multi-office access functions in Configure Staff, you can manage groups belonging to other offices. Select an office from the *Office* drop-down list. The Group list will display groups associated with the selected office.
   - The Unassigned group cannot be edited.

2. Click **Edit**. The *Edit Group* page displays.



3. Make the desired changes to the Group name and description.
4. To edit a Groups access rights, click the **Expand/Collapse** arrow located next to the listed products and do one of the following:
   - **Select individual options**. Check the box next to an option for which you want to grant this group functional rights.
   - **Deselect individual options**. Uncheck the box next to an option for which you want to remove functional rights.
   - **Select all options**. Click the **Select all** link located above the listed options to give this group full access to all of the product's functions.

- **Deselect all options**. Click the **Deselect all** link located above the listed options to remove all product functional rights for this group.

Notes:

- Only products for which your firm is licensed will display.

5. Click **Submit** to save your changes.

Deleting Groups

All staff currently assigned to this group will have a group status of Unassigned. These members will have no product functional rights.The unassigned group cannot be deleted.

To delete a group do the following:

1. Select **Groups** from the navigation bar. The *Groups* page displays.

   Note: If you are a Super Administrator or Multi-office Administrator, you can manage groups from other offices. Select an office from the *Office* drop-down list. The Group list will display groups associated with the selected office.

2. Select the radio button of the group to be deleted.
3. Click **Delete**. A confirmation dialog displays indicating that there are either staff members assigned, or not assigned, to the group.
4. Do one of the following:
   - Click **OK** to remove the group. Any members that were assigned to this group will be reassigned to the unassigned group and will have all functional rights of the new group.

     To reassign the members, select a new group, and click **Assign Staff** to move staff members to a new group. The *Assign Staff* page displays. See *Assigning and Removing Group Members* on page 24 for further details.
   - Click **Cancel** to terminate the deletion process.

Setting Up Teams

To aid in project management, you can organize staff members into teams for work assignment purposes.

Note: Multi-office firms can create teams composed of staff members located in different offices.

Adding Teams

Use the following steps to add a team to Configure Staff.

1. Click **Teams** on the navigation bar. The *Teams* page displays.

Note: A Super Administrator or Multi-office Administrator can add teams for other offices by selecting an office from the *Office* drop-down list.

2. Click **Add**.
3. Enter a name in the *Team Name* field.
4. Enter descriptive information in the *Description* field.
5. Click **Submit**.

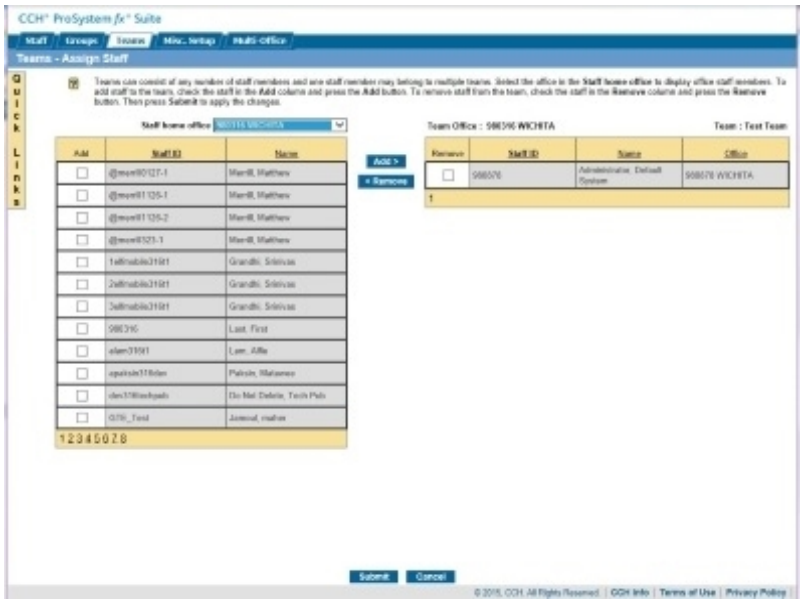
Adding and Removing Team Members

Use the following procedures to add or remove staff members from a team.

1. Click **Teams** on the navigation bar. The *Teams* page displays.

   Note: A Super Administrator or Multi-office Administrator can manage teams for other offices by selecting an office from the *Office* drop-down list.

2. Select the radio button of the team to which you want to assign or remove staff members and click **Assign Staff**. The *Assign Staff* page displays.



3. Do one of the following:
   - Add staff to a team. Check the box next to each user listed in the *Staff home office* list to be assigned and click **Add**.
   - Remove staff from a team. Check the box next to each user listed in the *Team* list and click **Remove**.
4. Click **Submit**. You will be returned to the *Teams* page.

Editing Team Detail

Use the following steps to change a team's name or description.

1. Click **Teams** on the navigation bar. The *Teams* page lists existing teams for your home office.

   Note: A Super Administrator or Multi-office Administrator can list teams from other offices by selecting an office from the *Office* drop-down list.
2. Click **Edit**.
3. Edit the information in either the *Team* or *Description* field.
4. Click **Submit**.

Deleting Teams

Do the following to remove a team from Configure Staff. Any associated staff will become unassigned.

1. Click **Teams** on the navigation bar. The *Teams* page lists existing teams for your home office.

   Note: A Super Administrator can list teams from other offices by selecting an office from the *Office* drop-down list.
2. Select the radio button of the team to be deleted.

3. Click **Delete**. If this team contains staff members, a confirmation dialog displays.
4. Click **OK**.

Setting Up Departments

For organizational purposes, you can create departments to reflect your organization's office structure. When staff members are added, you can designate the department they belong to in their user profile.

Creating Departments

Use the following steps to add departments to Configure Staff.

1. Select **Misc. Setup > Departments** from the navigation bar. The *Departments* page displays.
2. Click **Add**. A blank row will display at the end of the *Departments* list.
3. Enter a department name and click **Save**.

   Note: Click **Reset** to cancel your changes.

Editing a Department's Name

Use the following procedure to change the name of a department.

1. Select **Misc. Setup > Departments** from the navigation bar. The *Departments* page displays.
2. Select the radio button of a department and click **Edit**.

   Note: A Super Administrator can display departments from other offices by making a selection from the *Office* drop-down list.
3. Edit the department name.

   Note: Click **Reset** to cancel your changes.
4. Click **Save** when you have finished.

Deleting Departments

Use these steps to remove a department from Configure Staff.

1. Select **Misc. Setup > Departments** from the navigation bar. The *Departments* page displays.
2. Select the radio button of the department and click **Delete**.

   Note: A Super Administrator can display departments from other offices by making a selection from the *Office* drop-down list.
3. A confirmation dialog displays. Click **Yes**.

   Notes:

   - Click **Reset** to cancel your changes.
   - Click **Save** to apply changes to the database once changes have been made.

Setting Up Titles

To provide more descriptive profile detail for staff members, you can create Titles reflecting the various roles within your firm. Staff members can then be assigned an appropriate title.

The Titles option also provides another means for sorting and filtering lists of staff members for certain Configure Staff functions.

Adding Titles

Use the following steps to add Titles to Configure Staff.

1. Select **Misc. Setup > Titles** from the navigation bar. The *Titles* page displays.
2. Click **Add**. A blank row will display at the end of the *Titles* list.

   Note: A Super Administrator can add a title for an office other than the default, by making a selection from the *Office* drop- down list.

3. Enter a title name and click **Save**.

   Note: Click **Reset** to cancel your changes.

Editing Titles

To edit a title use the following steps.

1. Select **Misc. Setup > Titles** from the navigation bar. The *Titles* page displays.
2. Select the radio button next to a title and click **Edit**.

   Note: A Super Administrator can display titles from other offices by making a selection from the *Office* drop-down list.

3. Edit the contents of the field containing the name of the selected title.

   Note: Click **Reset** to cancel your changes.

4. Click **Save** when you have finished.

Deleting Titles

Use the following procedure to remove a title from the system.

1. Select **Misc. Setup > Titles** from the navigation bar. The *Titles* page displays.
2. Select the radio button next to a title.

   Note: A Super Administrator can display titles from other offices by making a selection from the *Office* drop-down list.

3. Click **Delete**.
4. A confirmation dialog displays. Click **Yes**.

Copying Office Configurations

Configure Staff provides an option that allows a Super Administrator to copy configurations between offices to ensure uniformity in staff profiles, group rights, and team assignments.

The following settings and detail can be copied:

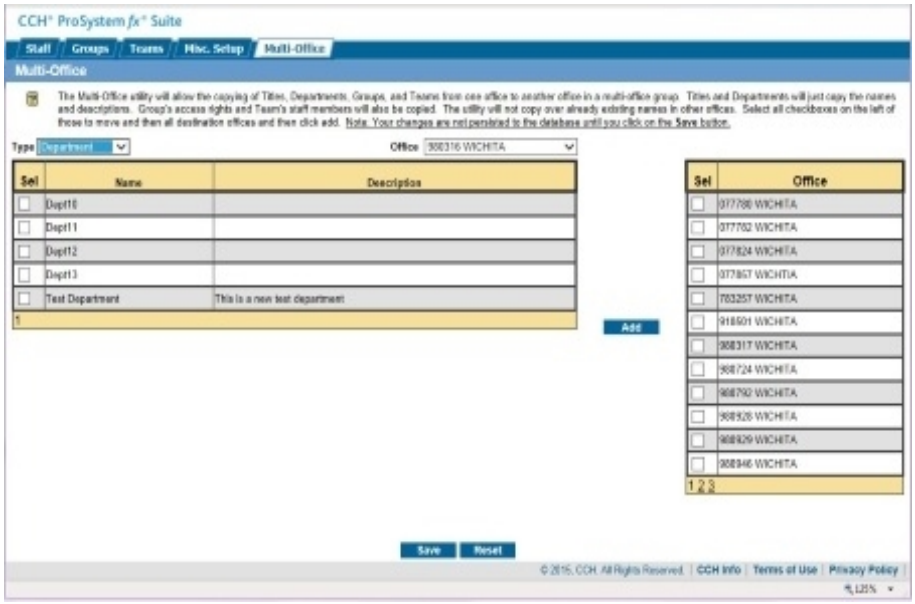
- **Groups**. Name, description, and functional rights settings.
- **Teams**. Name and list of assigned staff members.
- **Departments and Titles**. Name and description.

Notes:

- This task can only be implemented by a Super Administrator.
- When Teams are copied, profile information for assigned staff is not copied.

To copy office configurations, do the following:

1. Click **Multi-Office** from the navigation bar. The *Multi-Office* page displays.



2. Select an office setting type to copy from the *Type* drop-down list.
3. Select an office to copy from the *Office* drop-down list.
4. Do one of the following:
   - If you selected **Groups** from the *Type* list, select the check box next to groups to be copied.
   - If you selected **Teams** from the *Type* list, select the check box next to teams to be copied.
   - If you selected **Departments** from the *Type* list, select the check box next to departments

to be copied.

- If you selected **Titles** from the *Type* list, select the check box next to titles to be copied.

5. Check a box next to the offices listed in the *Destination Office* list to which you want to copy the items.
6. Click **Add**.
7. Click **Save**.

Chapter 4

MANAGING STAFF MEMBERS

Once Configure Staff is set up and staff members have been added, there are various administrative tasks that need to be carried out to make sure the users of CCH ProSystem *fx* Internet applications and services continue to have the access rights they require and have their profile information kept current.

The various administrative tasks required of users managing staff members consist of:

- Unlocking staff members
- Deleting staff members
- Printing licensing audit reports
- Editing staff member profile information
- Resetting passwords

Changing Profile Information

To edit a staff member's profile, do the following:

1. On the Staff Home page, do one of the following:
   - Display a specific staff member. Select either the **Staff ID** or **Name** radio button, enter the search information, and click **Search** to display a list of staff matching the search criteria entered.
   - Display members in a specific group. Select a group from the *Group* drop-down list and click **Search** to display staff assigned to a specific group.
   - Display members by office. Make a selection from the *Office* drop-down list and click **Search**.

     Notes:

     - Super Administrator or multi-office access is required to access staff information from other offices.
     - You can refine your search by combining Product and Group selections.
     - Any value in the *Staff ID/Name* field will override the other selections.
2. Select the radio button for a staff member and click **Edit**. The *General Information* page displays.

3. Make any changes.

   Note: If you change a staff members group assignment, their current rights are reset and they will inherit the defined rights of the new group. If a user requires additional rights, they can be granted on an individual basis. See *Modifying Individual Product Functional Rights* on the facing page for details.

4. Click **Return to Staff Home** to save your changes and exit this page.

Unlocking Staff Members

If a user fails to enter a correct password to a CCH ProSystem *fx* Internet product, after five attempts the user's ID becomes locked. A red lock icon will appear next to the user's ID on the *Staff Home* page.

Do the following to unlock the user:

1. On the Staff Home page, do one of the following:
   - **Display a specific staff member**. Select either the **Staff ID** or **Name** radio button, enter the search information, and click **Search** to display a list of staff matching the search criteria entered.
   - **Display members in a specific group**. Select a group from the *Group* drop-down list and click **Search** to display staff assigned to a specific group.
   - **Display members by office**. Make a selection from the *Office* drop-down list and click **Search**.

     Note: Only a Super Administrator or Multi-office Administrator can access staff information from other offices.

2. Select the radio button for a staff member and click **Unlock**.
3. A confirmation dialog displays, click **OK**.

Deleting Staff Members

To delete a staff member, do the following:

1. On the *Staff Home* page, do one of the following:
   - **Display all staff members**. Click **Search**.
   - **Display a specific staff member**. Select either the **Staff ID** or **Name** radio button, enter the search information, and click **Search** to display a list of staff matching the search criteria entered.
   - **Display a list of staff members with access to a specific product**. Select a product from the *Product* drop-down list and click **Search** to display staff assigned access to the selected product.

- **Display members in a specific group**. Select a group from the *Group* drop-down list and click **Search** to display staff assigned to a specific group.
- **Display members by office**. Make a selection from the *Office* drop-down list and click **Search**.

  Note: Only a Super Administrator or Multi-office Administrator can access staff information from other offices.

2. Select the radio button for a staff member and click **Delete**.
3. A confirmation window displays. Click **OK**.

   Note: Once deleted, a User ID cannot be reused.

Resetting Passwords

To reset a password for a staff member, do the following:

1. Select the staff member, and click **Edit**.
2. Enter a new password in the *Password* and *Verify Password* fields.

   Note: Password history is maintained for five passwords. Therefore, you will not be able to reuse your last five passwords.

3. Click **Return to Staff Home**, and your changes will be saved.

   Notes:

   - If you cannot remember your password, you can select the **Forgot Your Password?** link from the login page, and have the system email a temporary password to the email address in your profile. The **Forgot Your Password?** link will also unlock a locked account, once authenticated.
   - When a staff member is given a new password from the Administrator or Customer Support, it can be used only once. The first time the new password is used to access a CCH ProSystem *fx* Internet product, the staff member will be prompted to change it.

Modifying Individual Product Functional Rights

To make changes to a staff member's individual functional rights, use the following procedure.

Notes:

- Staff members will still retain rights inherited from their assigned group.
- A staff member can only be assigned to one group at a time.

1. On the *Staff Home* page, do one of the following:
   - **Display a specific staff member**. Select either the **Staff ID** or **Name** radio button, enter the search information, and click **Search** to display a list of staff matching the search criteria entered.

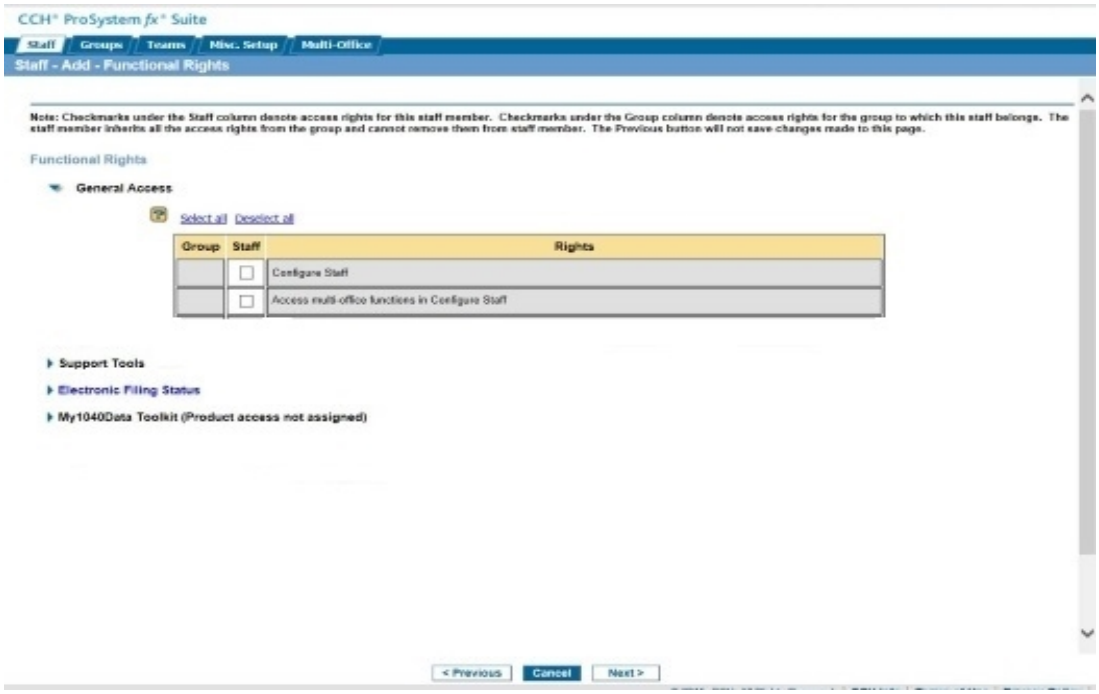
- **Display members in a specific group**. Select a group from the *Group* drop-down list and click **Search** to display staff assigned to a specific group.
- **Display members by office**. Make a selection from the *Office* drop-down list and click **Search**.

  Note: Only a Super Administrator or Multi-office Administrator can access staff information from other offices.

2. Select the radio button for a staff member and click **Edit**. The *General Information* page displays.
3. Click **Functional Rights**. The *Functional Rights* page shown on the following page displays a lists of products for which the staff member has been granted access.
4. Click the **Expand/Collapse** arrow located next to the listed products for which you want to configure access rights. The list of product options will display.

Notes:

- Download of software will allow those users who are licensed to download only CCH® ProSystem *fx*® Engagement and CCH® ProSystem *fx*® Knowledge Coach releases, as well as the permission key.
- Download of permission key will continue for users who are licensed for other Foundation products.



5. Do one of the following:
   - **Select individual options**. Check the box next to an option for which you want to grant this staff member functional rights.

- **Select all options**. Click the **Select all** link located above the listed options to give this staff member full access to all of the product's functions.
- **Deselect all options**. Click the **Deselect all** link located above the listed options to remove all product functional rights for this staff member.

Note: For detailed information on the options listed for each product, click the Question mark icon located to the left of the product.

6. Click **Return to Staff Home** to save your changes and return to the *Home* page.

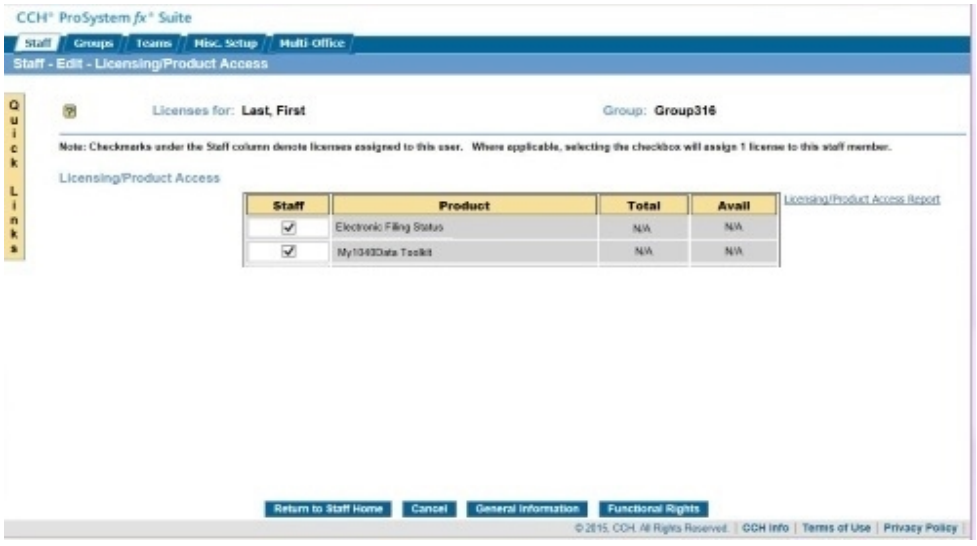
Modifying Licensing/Product Access Settings

To make changes to a staff member's Licensing/Product Access settings, use the following steps.

1. On the *Staff Home* page, do one of the following:
   - **Display a specific staff member**. Select either the **Staff ID** or **Name** radio button, enter the search information, and click **Search** to display a list of staff matching the search criteria entered.
   - **Display members in a specific group**. Select a group from the *Group* drop-down list and click **Search** to display staff assigned to a specific group.
   - **Display members by office**. Select from the *Office* drop-down list and click **Search**.

     Note: Only a Super Administrator or Multi-office Administrator can access staff information from other offices.

2. Select the radio button for a staff member and click **Edit**. The *General Information* page displays.
3. Click **Licensing/Product Access**. The *Licensing/Product Access* page lists products for which your firm is licensed. It also lists the total number of user licenses for each product.



4. Do one of the following:
   - Check the boxes to the left of each product for which you want to assign a user license, if applicable, and grant this staff member access.

     Notes:

     - User licenses do not apply to products such as Tax Notebook Toolkit and My1040Data Toolkit, but they must be checked to allow access.
     - Product access cannot be granted for products with zero licenses available.

   - To un-assign a staff member's user licenses and product access privileges, clear the check boxes next to the product.
5. Click **Return to Staff Home** to save your changes and return to the *Staff Home* page.

Printing the Licensing/Product Access Report

Use the following steps to generate a report displaying the total licenses purchased and the currently unassigned or available licenses by product.

To print the Licensing/Product Access Report, do the following:

1. On the *Staff Home* page, click **Report**. The report displays in a second window.
2. Click the **Print** icon located at the top of the report to print the report.

   Note: You may also print the report by selecting the Licensing/Product Access Report link from the *Licensing/Product Access* page.