GOSYSTEM TAX™

RS ADMINISTRATOR GUIDE

FOR TAX YEAR 2021

Last Updated: October 06, 2021

THOMSON REUTERS®

TABLE OF CONTENTS

CHAPTER 1: SETTING FIRM CONFIGURATION

FIRM ADMINISTRATOR LOGIN

Only administrators can set the **Firm Configuration** in RS Browser. To log in as the firm administrator, enter:

- the login ID of the firm administrator
- the firm
- "***" in the location field
- the password for the firm administrator.

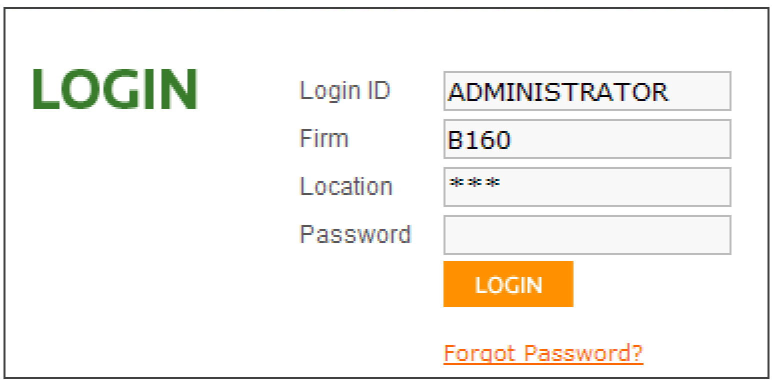


Figure 1:1

The figure above shows the screen where this information is entered. The firm administrator's initial login ID is *ADMINISTRATOR*. The firm and initial password are indicated in an email sent to the firm administrator. The firm administrator will be prompted to select a new password upon initial login.

Before setting up other user logins, the *** Firm Administrator should make selections in the **Firm Configuration** screens.

1. Select **Admin > Firm Configuration**. The following screen appears:

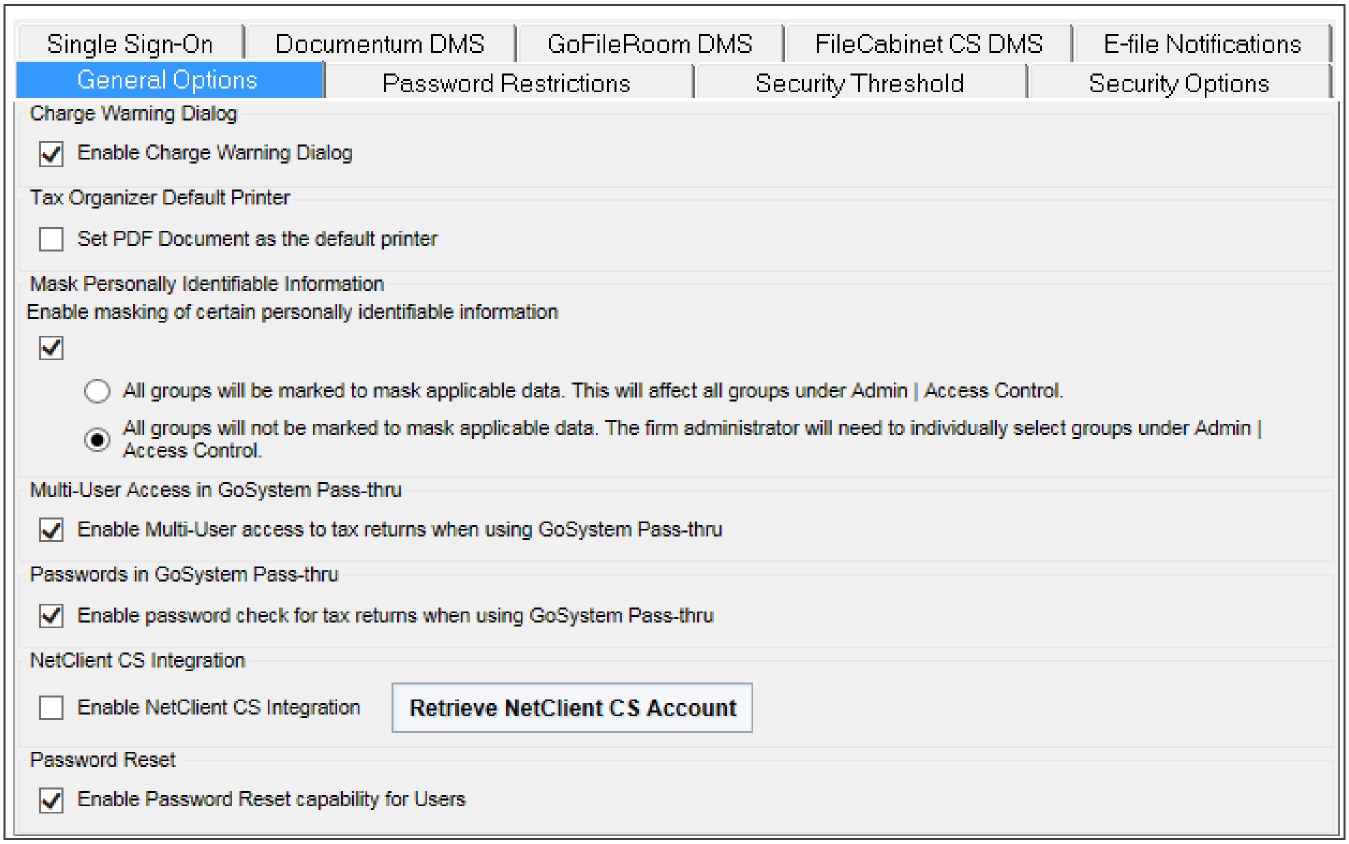


Figure 1:2

2. Select the applicable tab to make selections:
   - **General Options (page 3)**
   - **Password Restrictions (page 4)**
   - **Security Threshold (page 4)**
   - **Support and Other Options (page 4)**
   - **Single Sign-on (page 4)**
   - Documentum DMS
   - GoFileRoom DMS
   - FileCabinet CS DMS
   - **Setting Firm Configuration (page 1)**
3. After making your selections, select **Update** to change your options, or select **Restore Defaults** to return to the system options.
4. Select **History** to review the changes a given user made and the dates of those changes.

GENERAL OPTIONS

Use this tab to:

- enable the charge warning dialog
- set **PDF Document** as the default printer
- enable masking of personally identifiable information (see **Redacting Certain Personally Identifiable Information (page 27)**)
- enable multi-user access to tax returns when using pass-through
- enable password check for tax returns when using pass-through
- enable NetClient CS integration
- enable password reset capability for users (see **Password Reset Feature (page 12)**).

PASSWORD RESTRICTIONS

See **Password Restrictions (page 18)** for more information on password restrictions.

SECURITY THRESHOLD

See **Security Threshold (page 20)** for more information on setting security threshold options.

SUPPORT AND OTHER OPTIONS

See **Support and Other Options (page 22)** for more information on setting support and other options.

SINGLE SIGN-ON

Use this tab to:

- enable single sign on using SAML Authentication
- ***require*** SAML Authentication to login
- allow firm administrators [in *** Location] to login without SAML Authentication.

DOCUMENT MANAGEMENT SYSTEMS

Go to **https://www.riahelp.com/html/2021/grs/content/grs_procedures_dms/dms_intro.htm** for information on using Documentum and GoFileRoom.

Firms have multiple options available for e-file status notifications. These options provide firms a way to select statuses for notification and gives them the ability to set up the notifications at the firm, account, group, or locator level.

E-FILE NOTIFICATIONS TAB

The **E-file Notifications** tab appears on the **Firm Configuration** page. Any user who currently sees the **Firm Configuration** page will see this tab; it is not restricted by any additional user right.

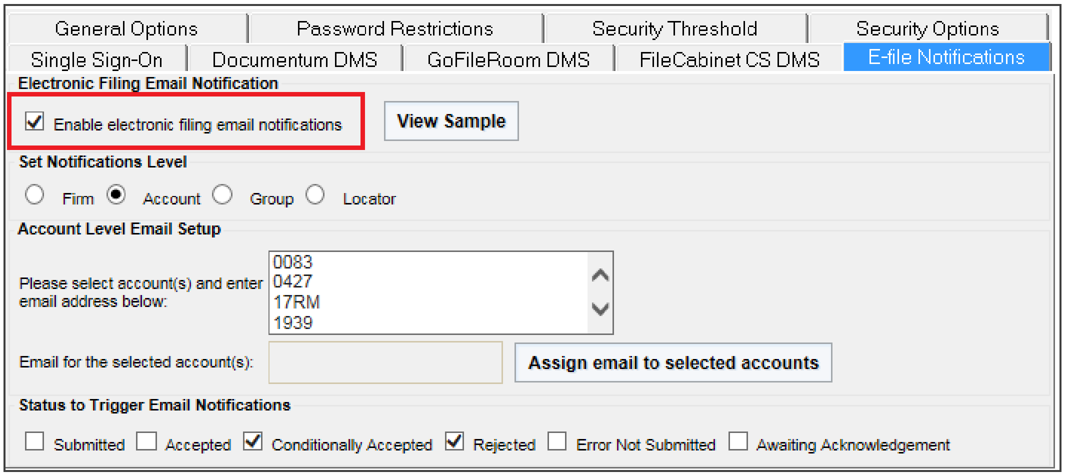


Figure 1:3

SETTING THE NOTIFICATION LEVEL

Four options are available for the notification level:

- Firm
- Account
- Group
- Locator

These options are mutually exclusive, so only one may be chosen per firm.

Firm Notification Level

This notification level allows the Administrator to select one email address to which all notifications will be sent. If more than one email address needs to receive the notifications, we suggest setting up a group email address. All e-file status notifications for returns within the firm will be sent to the email address entered.

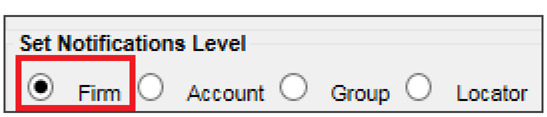


Figure 1:4

Account Notification Level

This notification level allows the Administrator to assign an email address to each account within the firm for which notifications will be sent. The accounts may be selected individually, or if the same email address is desired for more than one account, the accounts may also be multi-selected.

If more than one email address needs to receive notifications for an account, we suggest a group email address be set up and that email address can be entered here.

All e-file status notifications for returns within the account will be sent to the email address entered.

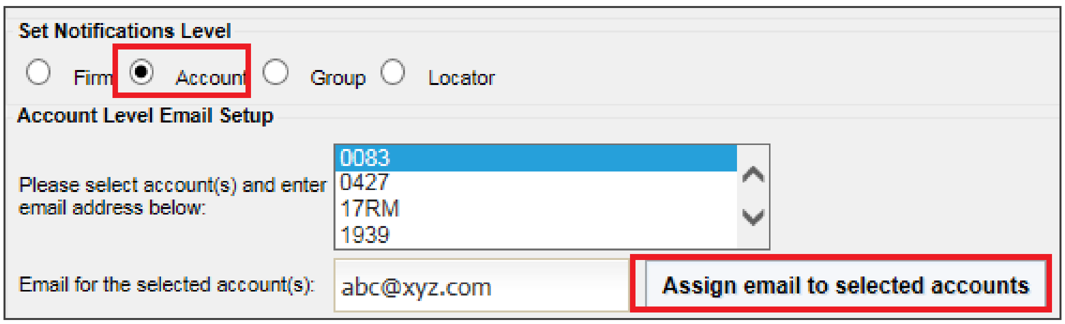


Figure 1:5

Group Notification Level

This notification level allows notifications to be sent at the group level. When this option is selected, e-file notifications for returns assigned to a group will be sent to the email address associated with that group.

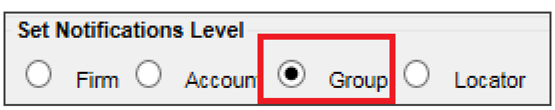


Figure 1:6

To enter the email address for each group:

1. Select **Admin > Access Control**.
2. Select the **Groups** tab.
3. Select the group.
4. Click the **Edit** button.

5. Enter an email address in the appropriate field.

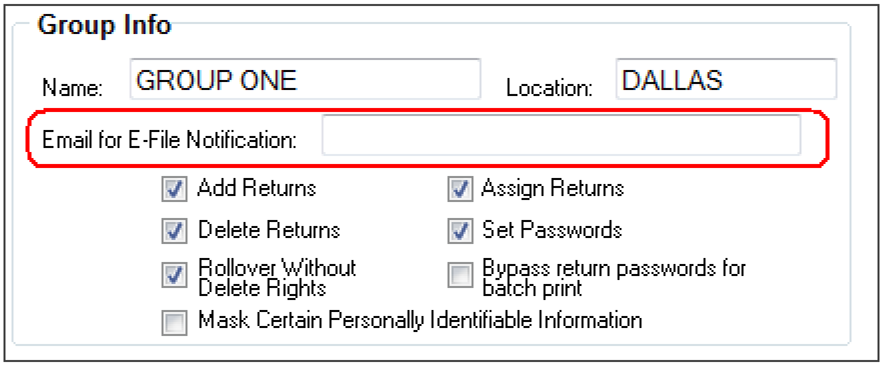


Figure 1:7

Locator Notification Level

This notification level allows email notifications to be sent at the locator level using the assignments selected. Each e-file status may have a different set of people notified. An option for another email address to be included in the notifications is available via the *Other* selection.

The locator level notification option requires that you make locator assignments and enter email addresses in **Access Control** for all of the assigned users.

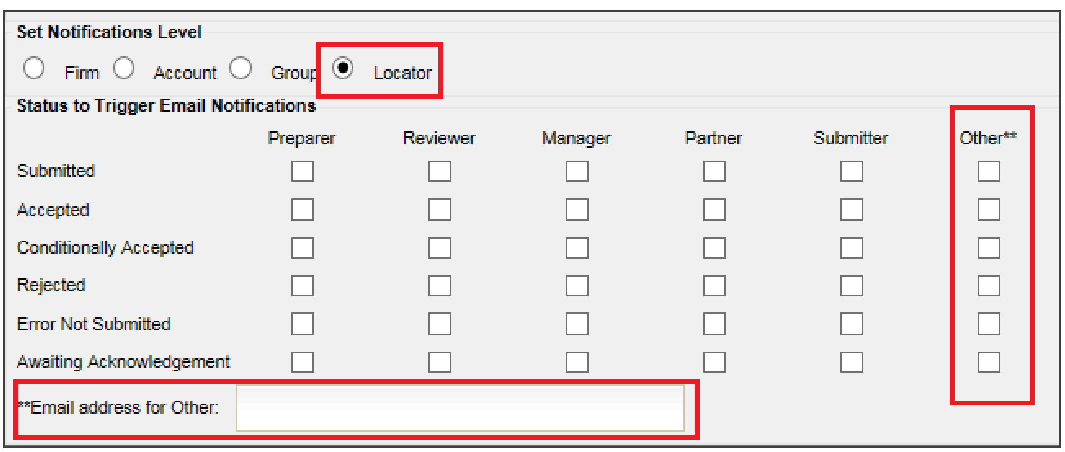


Figure 1:8

STATUS TO TRIGGER EMAIL NOTIFICATIONS

For each of the notification levels, with the exception of the *Locator Notification Level*, these statuses are available for email notifications:

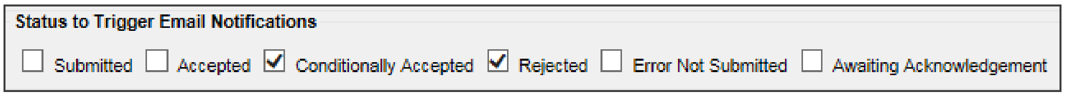


Figure 1:9

EMAIL NOTIFICATIONS

The email notifications are different for each e-file status. Each notification includes the jurisdiction, year, taxpayer name, tax type, and locator number for which the status is being sent.

To see a sample email for each of the available statuses, click the **View Sample** button at the top of the **E-file Notifications** page.

Sample: Email for Accepted Status

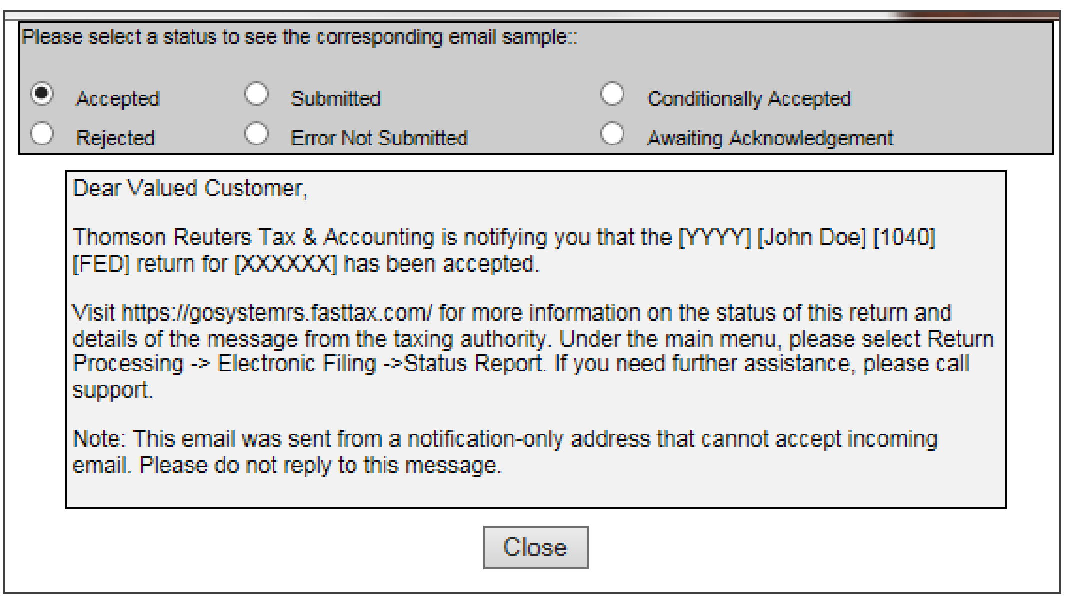
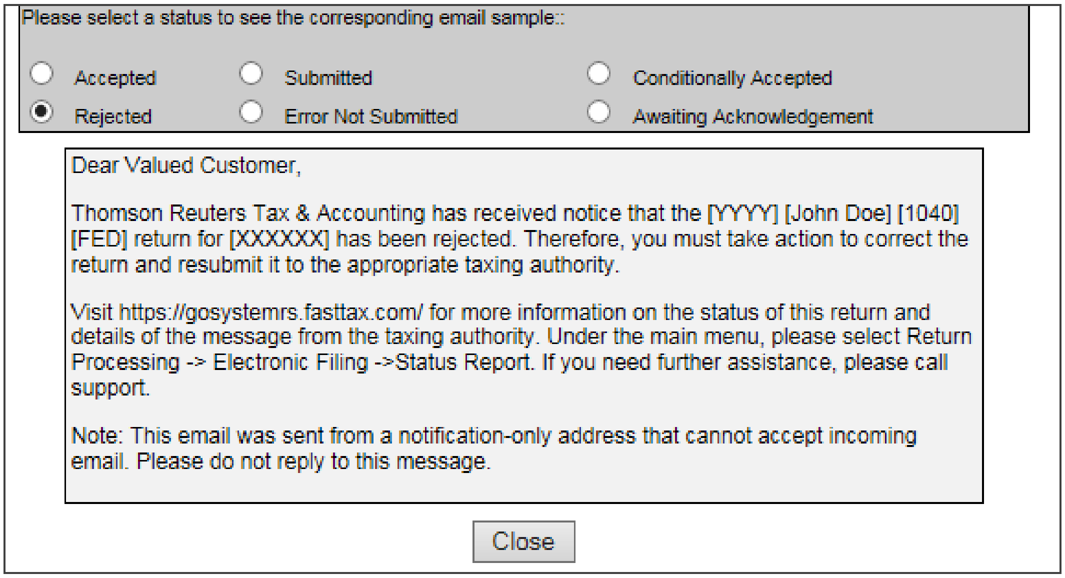


Figure 1:10

Sample: Email for Rejected Status


Please select a status to see the corresponding email sample::

Accepted Submitted Conditionally Accepted
Rejected Error Not Submitted Awaiting Acknowledgement

Dear Valued Customer,

Thomson Reuters Tax & Accounting has received notice that the [YYYY] [John Doe] [1040] [FED] return for [XXXXXX] has been rejected. Therefore, you must take action to correct the return and resubmit it to the appropriate taxing authority.

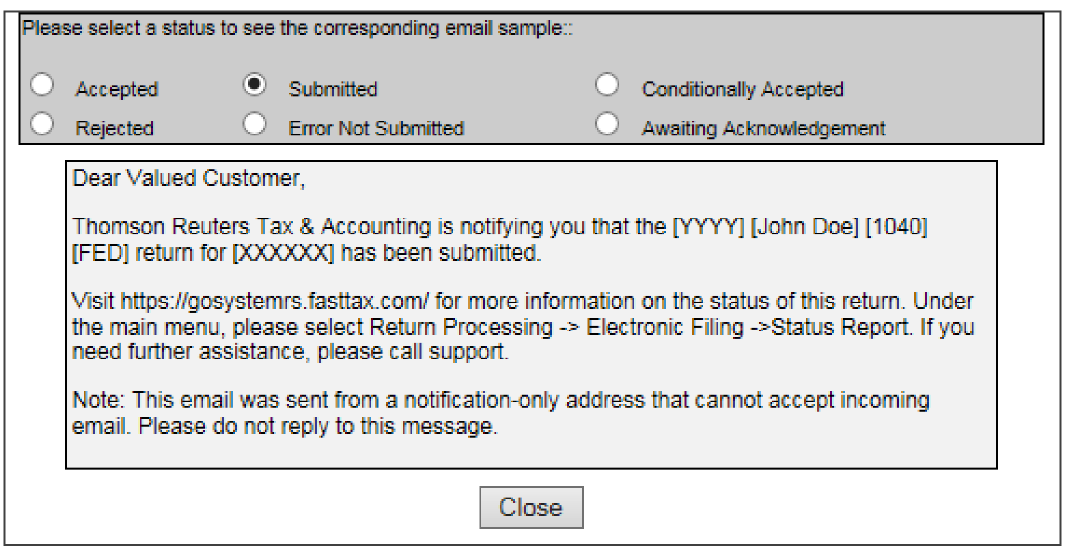
Visit https://gosystemrs.fasttax.com/ for more information on the status of this return and details of the message from the taxing authority. Under the main menu, please select Return Processing -> Electronic Filing ->Status Report. If you need further assistance, please call support.

Note: This email was sent from a notification-only address that cannot accept incoming email. Please do not reply to this message.

Close

Figure 1:11

Sample: Email for Submitted Status


Please select a status to see the corresponding email sample::

Accepted Submitted Conditionally Accepted
Rejected Error Not Submitted Awaiting Acknowledgement

Dear Valued Customer,

Thomson Reuters Tax & Accounting is notifying you that the [YYYY] [John Doe] [1040] [FED] return for [XXXXXX] has been submitted.

Visit https://gosystemrs.fasttax.com/ for more information on the status of this return. Under the main menu, please select Return Processing -> Electronic Filing ->Status Report. If you need further assistance, please call support.

Note: This email was sent from a notification-only address that cannot accept incoming email. Please do not reply to this message.

Close

Figure 1:12

Sample: Email for Error Not Submitted Status

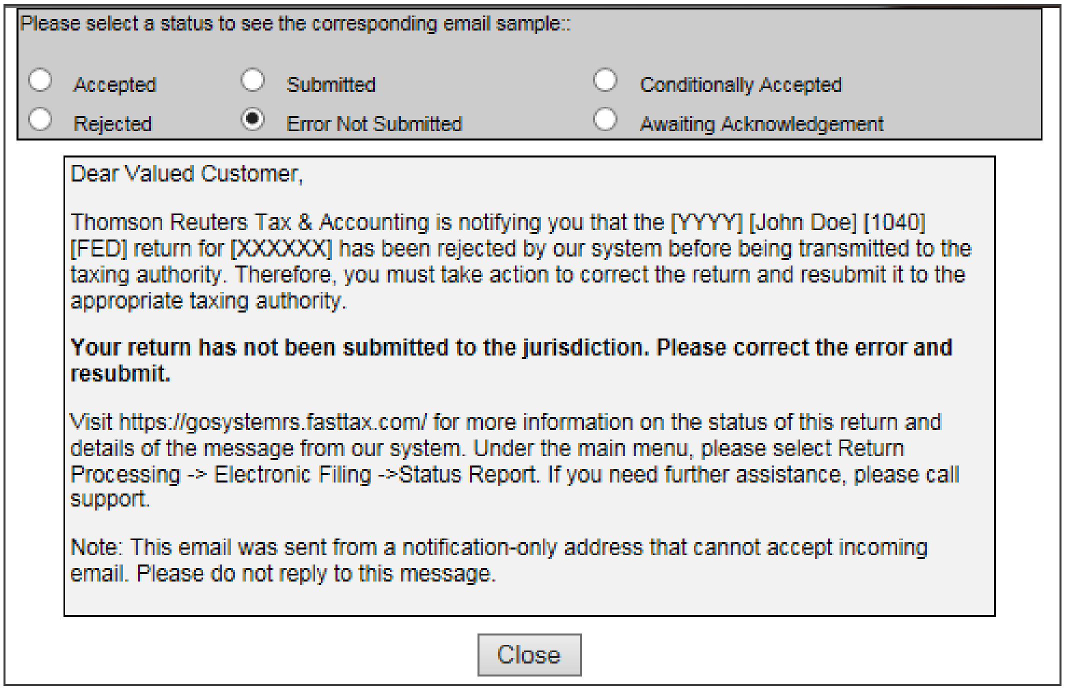


Figure 1:13

Sample: Email for Conditionally Accepted Status

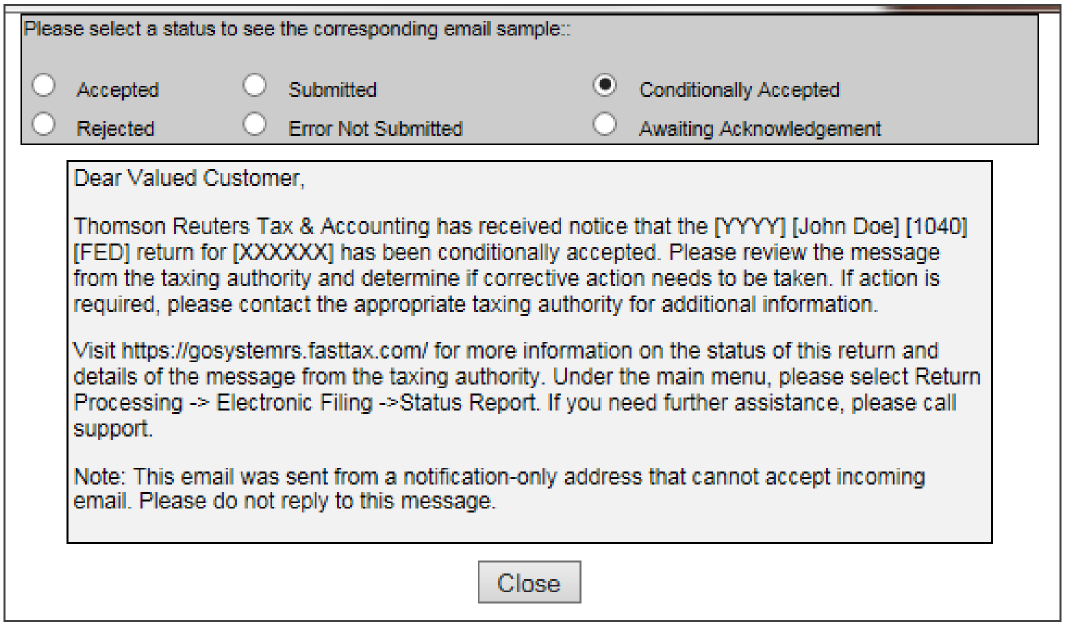


Figure 1:14

Sample: Email For Awaiting Acknowledgment Status

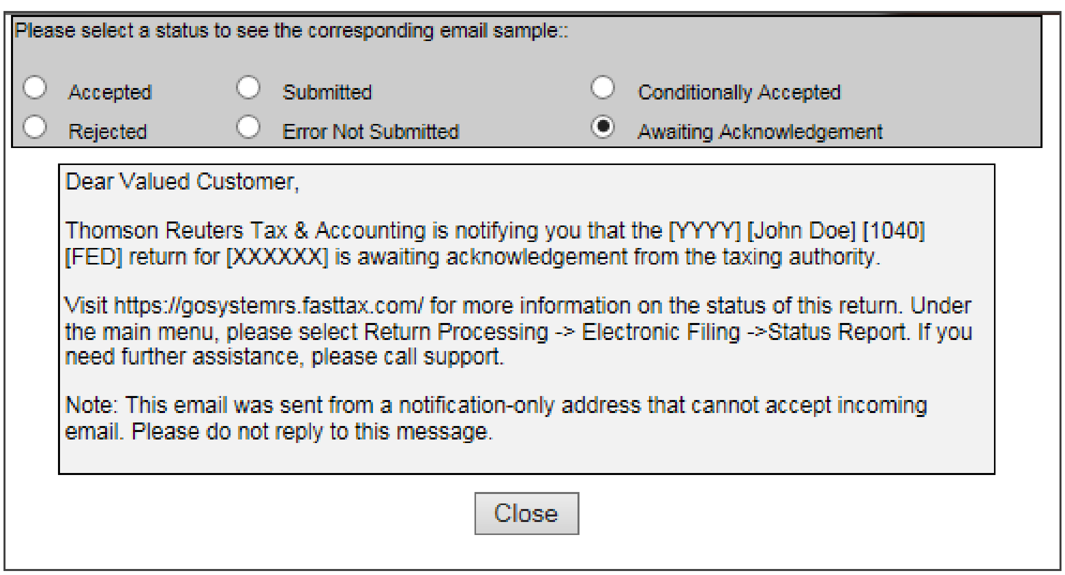


Figure 1:15

CHAPTER 2: SECURITY OPTIONS

PASSWORD RESET FEATURE

Users can reset their passwords without having to rely on their administrators to do it for them. The password reset process sends an email to the user with a link and an encrypted token embedded in the text of the email for the user to follow. The process uses the email address stored in the User Info for each user.

Firm Configuration

The password reset capability is Firm selectable, so the Firm administrator must turn it on in **Firm Configuration** for the users to be able to take advantage of it. Users that try to use it without the option being turned on for their firm will get a notification that it is not available for them. The **Firm Configuration** option exists under the **General Options** tab as follows:

Figure 2:1

Password Reset Process

The password reset feature is accessible via the **Forgot Password?** link on the login page.

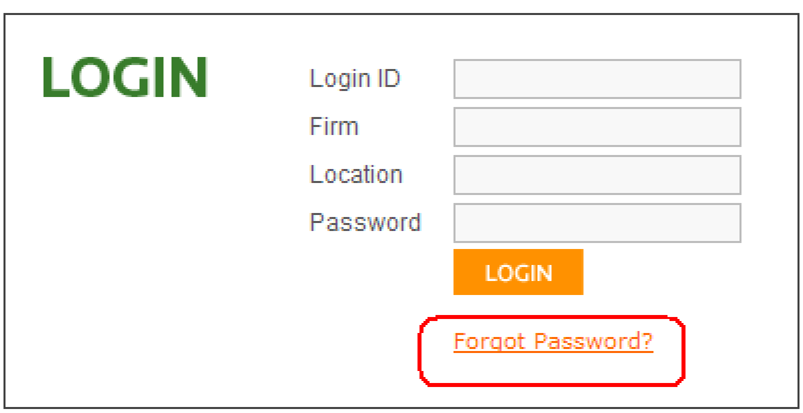


Figure 2:2

After the user clicks on the **Forgot Password** link, a prompt appears for the user’s Login ID, Firm, and Location.

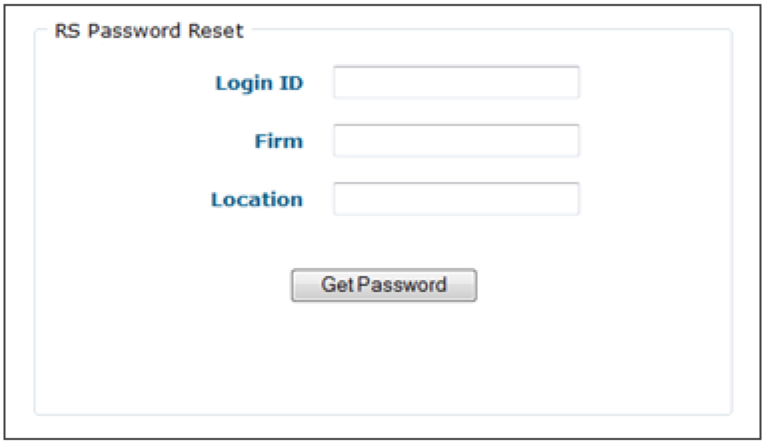


Figure 2:3

The user must enter all requested information and then press the **Get Password** button. The user will then see a dialog containing the current email address stored in the system for the user and asking the user to confirm the email address.

Figure 2:4

Users who do not have an email address stored in the system will receive a dialog stating this and suggesting they contact their administrator.

Once the user has confirmed the email address and has clicked **Continue**, that user will receive a dialog that an email has been sent:

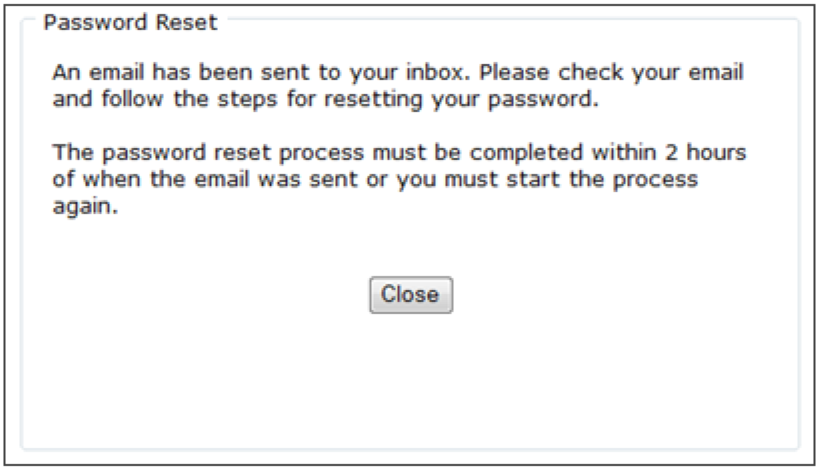
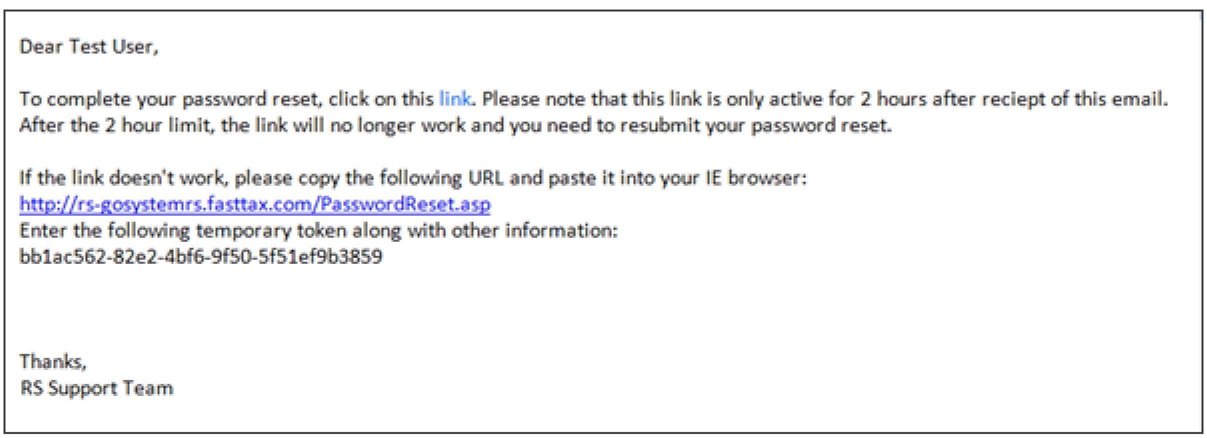


Figure 2:5

For security reasons, the password reset process must be completed within the two hours as seen above. There is a temporary token associated with the request and it will expire after two hours. After the two hours have passed and the temporary token has not been used, the password reset process must be restarted.

The user will receive an email with instructions similar to the following:



Dear Test User,

To complete your password reset, click on this link. Please note that this link is only active for 2 hours after reciept of this email. After the 2 hour limit, the link will no longer work and you need to resubmit your password reset.

If the link doesn't work, please copy the following URL and paste it into your IE browser:
http://rs-gosystemrs.fasttax.com/PasswordReset.asp
Enter the following temporary token along with other information:
bb1ac562-82e2-4bf6-9f50-5f51ef9b3859

Thanks,
RS Support Team

Figure 2:6

Clicking the link within the email brings the user to a page to enter the Login ID, Firm, and Location:

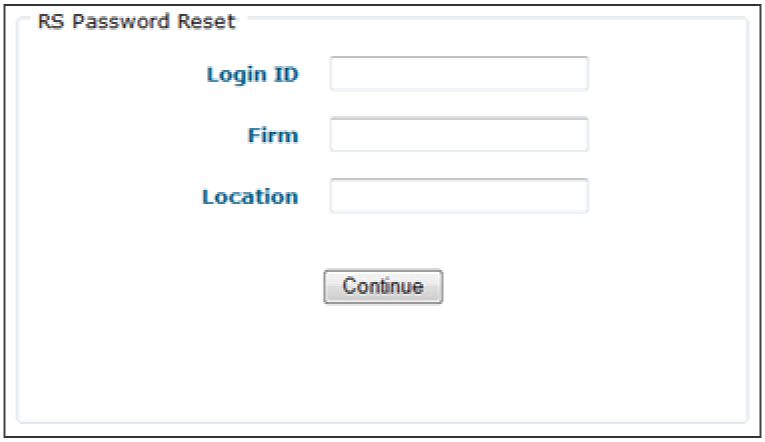


Figure 2:7

If the link does not work, as the email states, the user can copy and paste the URL into the browser. This will take the user to a slightly different page with an additional field to enter the temporary token:

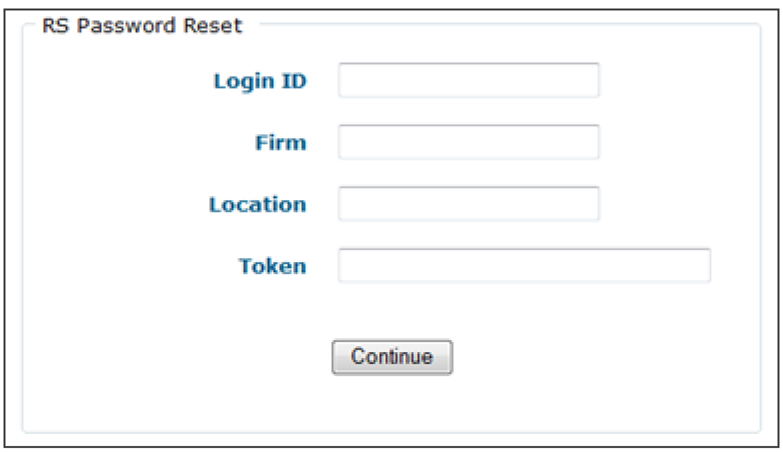


Figure 2:8

After selecting **Continue**, the user can then enter a new password:

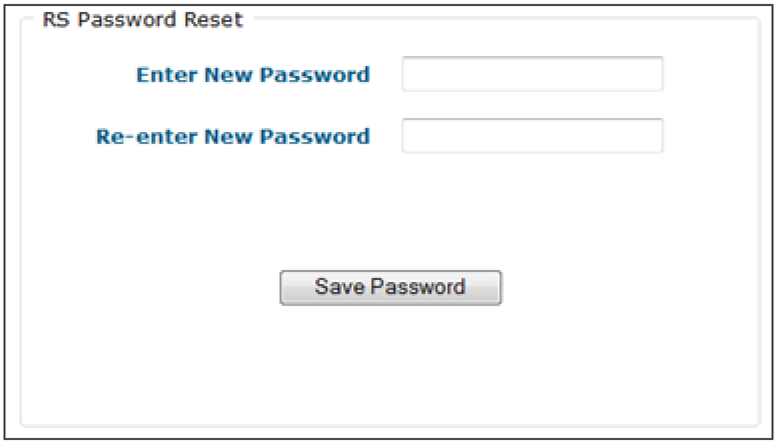


Figure 2:9

A final dialog will display as confirmation that the password reset was completed:

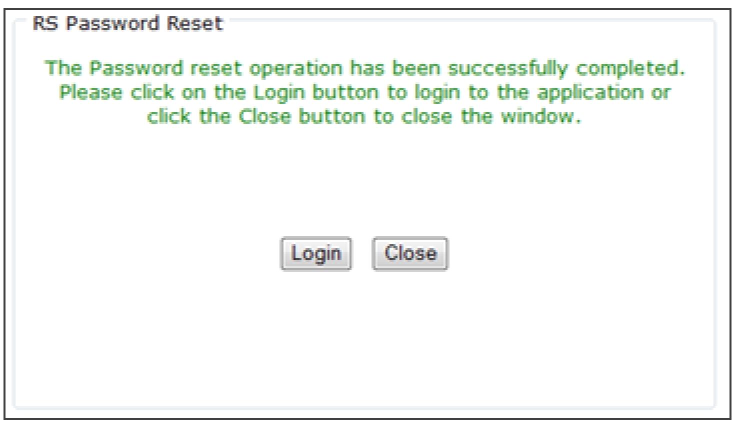
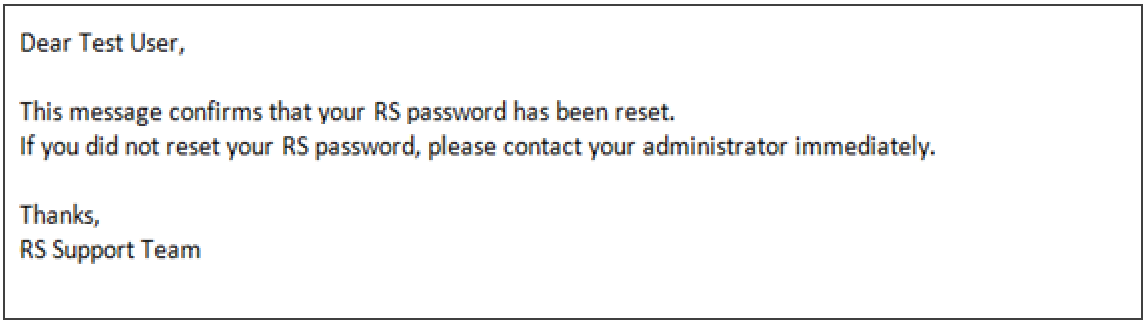


Figure 2:10

A confirmation email is also sent to the user after the process is complete:


Dear Test User,

This message confirms that your RS password has been reset.
If you did not reset your RS password, please contact your administrator immediately.

Thanks,
RS Support Team

Figure 2:11

Multiple Use Token

The password reset link/temporary token can only be used one time. A user who tries to use it a second time will get the following error message:

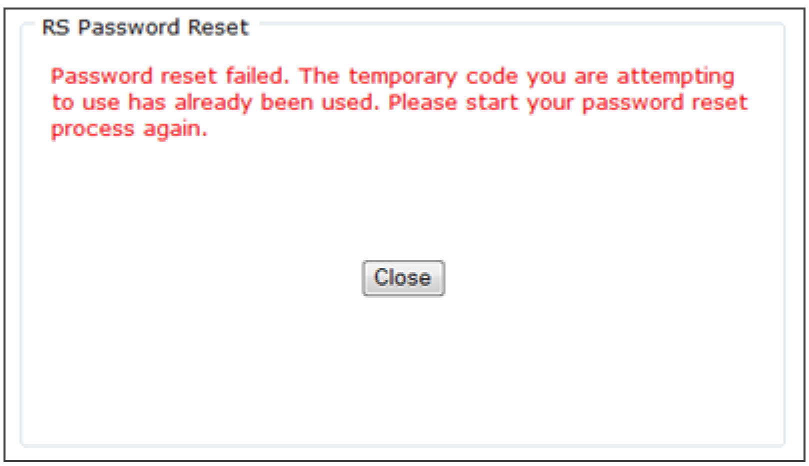


Figure 2:12

History Records

History records are written for the user when the password reset has been requested and also when the password reset process is complete.

Special Situations

Locked Out If a user is locked out after having entered the wrong password too many times, the user is allowed to use the password reset feature. Once the password reset process is complete, the user will no longer be locked out.

Disabled If a user is disabled, meaning an administrator has disabled the Login ID within **Access Control**, that user will not be able to use the password reset feature as long as the Login ID is disabled.

PASSWORD RESTRICTIONS

Use this screen to select password restrictions and configurations for your users.

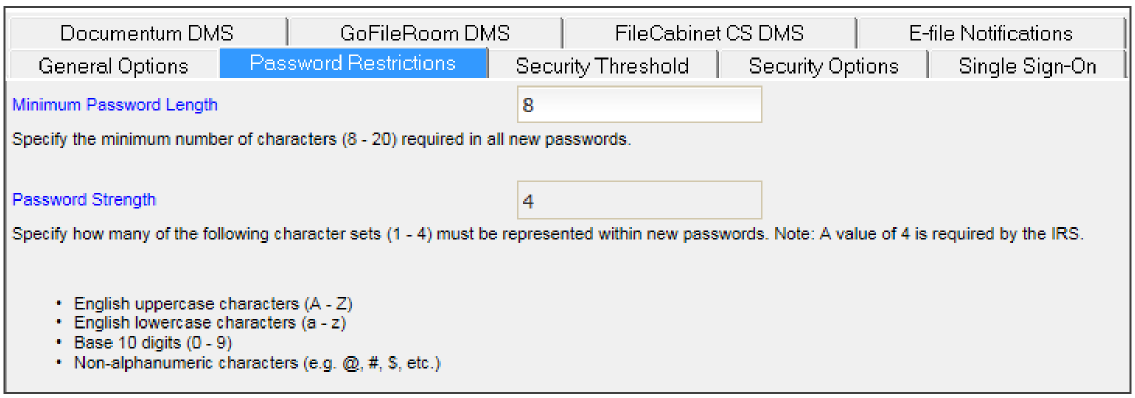


Figure 2:13

1. Select **Admin > Firm Configuration**, and select the **Password Restrictions** tab.

2. **Minimum Password Length**: Specify the minimum number of characters required in all new passwords. Passwords must contain at least eight (8) characters and no more than twenty (20) characters.

3. **Password Strength**: Specify the strength of the passwords. The IRS requires that each password contain all four (4) of the following sets of characters:

   - English uppercase characters (A - Z)
   - English lowercase characters (a - z)
   - Base 10 digits (0-9)
   - Nonalphanumeric characters, such as @, #, $, and so forth).

4. **Maximum Password Age**: Select the maximum password age. This is the number of days that a user may use a password before it expires. The range is from one (1) day to 90 days. A user will be required to change the password during the next login after password expiration, but a user can also elect to change a password at any time before it expires.

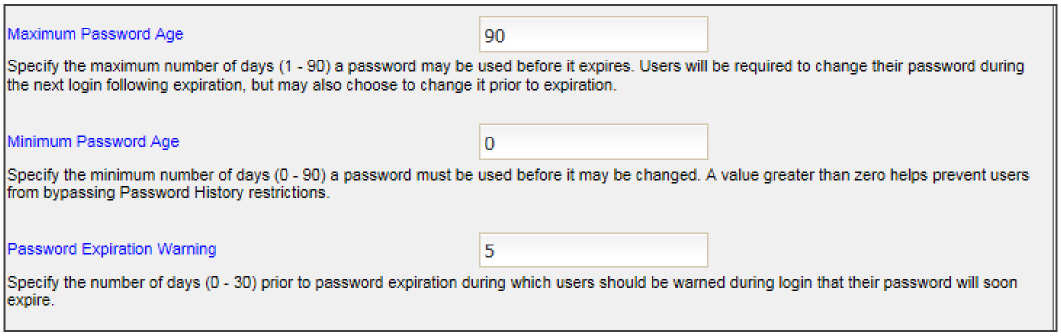


Figure 2:14

5. **Minimum Password Age**: Select the minimum password age. This is the number of days that a user must use a selected password before it expires. This can range from zero (0) days to 90 days. Selecting a value greater than 0 prevents users from bypassing the Password History restrictions.

6. **Password Expiration Warning**: Select the number of days prior to password expiration that a user will see a message warning that the login for that password will soon expire. This can range from zero (0) days to thirty (30) days.

7. **Password History**: Select the number of former passwords (1-24) that the application will store. A user cannot reuse any password stored in the Password History.

8. **New Password Expiration**: Select the option, if desired, for New Password Expiration, and specify the number of hours (1-168) that a New Password remains valid. New Passwords are single-use passwords set by the administrator as part of a password reset request or new account creation. Enabling this feature ensures that new and reset accounts have a user-selected password assigned within the specified interval.

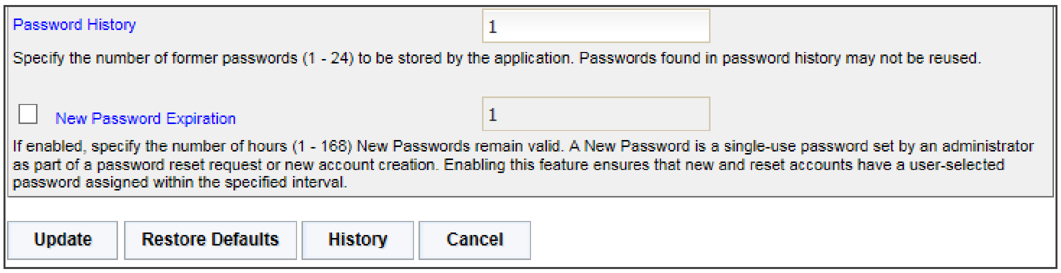


Figure 2:15

9. When you have selected your options, select **Update** to change the system defaults, or select **Restore Defaults** to revert to the system defaults.

SECURITY THRESHOLD

Use this screen to select lockout and inactivity durations for your users.

1. Select **Admin > Firm Configuration**, and select the **Security Threshold** tab.

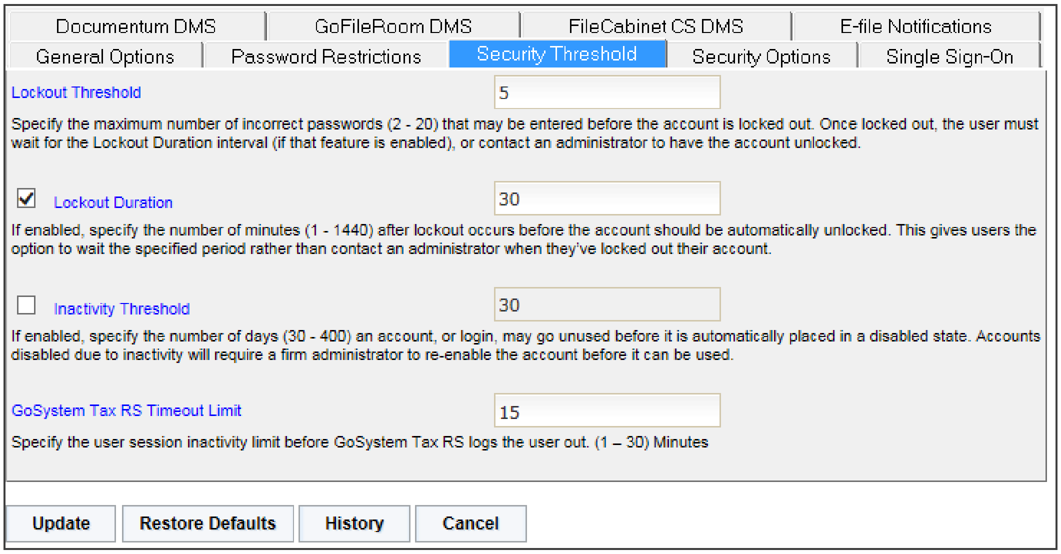


Figure 2:16

2. **Lockout Threshold**: For the lockout threshold, select the maximum number of incorrect passwords (2-20) that a user may enter before the account is locked out. Once locked out, the user must wait for the lockout duration interval (set below) or contact an administrator to have the account unlocked.

3. **Lockout Duration**: If desired, select the option to enable a lockout duration, and set the number of minutes (1-1440) after a lockout occurs before the account is automatically unlocked. This gives locked-out users the option to wait the specified period instead of contacting an administrator.

4. **Inactivity Threshold**: If desired, select the option to enable an inactivity threshold, and specify the number of days (30-400) that an account or login may go unused before it is automatically disabled. Accounts disabled due to inactivity will require a firm administrator to re-enable the accounts before they can be used.

5. **Timeout Limit**: If desired, select the option to specify the number of minutes (1-30) of session activity before the system automatically logs the user out.

6. After making your selections, select **Update** to change your options, or select **Restore Defaults** to return to the system options.

SUPPORT AND OTHER OPTIONS

Use this screen to select support and other options for your users.

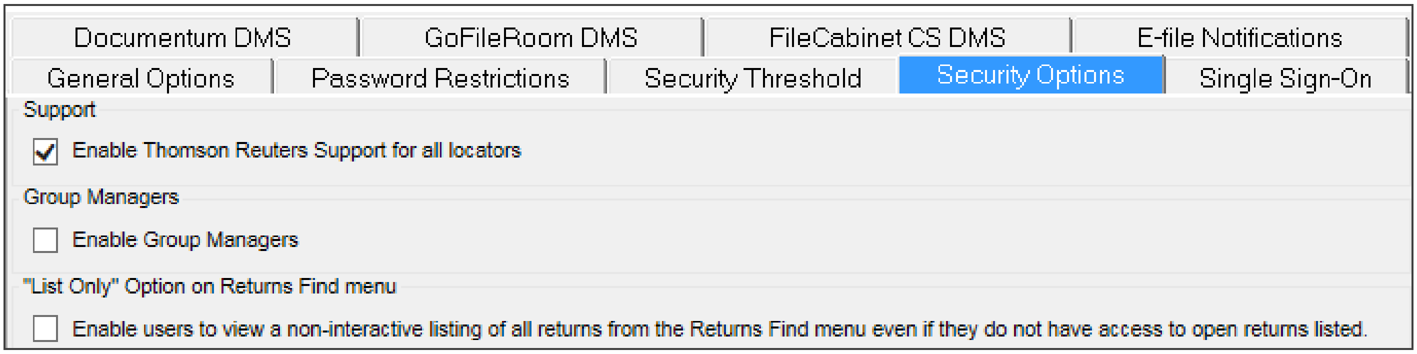


Figure 2:17

1. Select **Admin > Firm Configuration**, and select the **Security Options** tab. If desired, select the **Support** option to enable Thomson Reuters Support for all returns.
2. Select the option, if desired, to enable Group Managers.
3. Select the option, if desired, to enable users to view a non-interactive listing of all returns on the **Returns** menu. They can view the list even if they do not have access to the open returns listed.
4. For the three **Remember Me** options, if desired, enable the following values entered on the login page to be stored on the user's workstation, so that the fields are prepopulated on subsequent visits to the login page:
   - Login ID
   - Firm
   - Location.

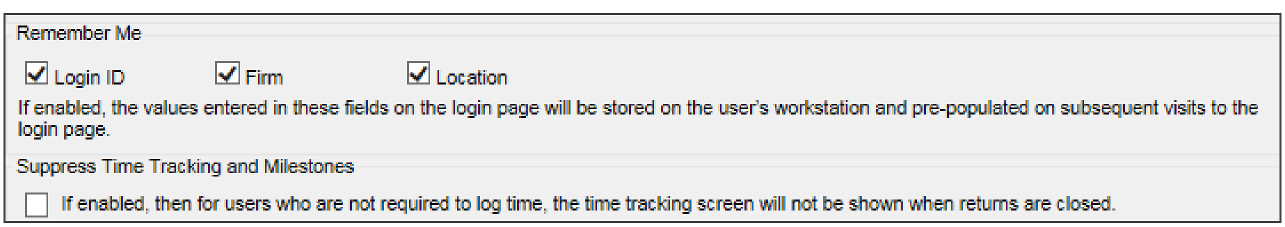


Figure 2:18

5. If desired, select the option to suppress time tracking and milestones. Selecting this option suppresses the time tracking screen when returns are closed for those users who are not required to log in their time.
6. For the **IP Range Subnet Validation**, please see Restricting Access to Accounts by IP Address.
7. After making your selections, select **Update** to change your options, or select **Restore Defaults** to return to the system options.

SINGLE SIGN-ON

Use this screen to enable single sign-on parameters using SAML authentication for your firm.

This is a separate optional product and will not be available unless your firm is licensed for Single Sign-On. ***Please note that the following is for informational purposes only.*** To implement SSO, contact your account manager.

Warning! Do not change any of these settings unless you are certain of the correct values, or you may break your firm's ability to login into the product!

The SSO configuration information is located on the **Admin > Firm Configuration > Single Sign On** tab.

Figure 2:19

On the **Single Sign On** tab, note the following:

1. The box **Enable Single Sign On using SAML Authentication** is used to enable single sign-on access for the firm.
2. **REQUIRE SAML Authentication to login** forces all users to use SSO for product access. The login screen will redirect users to the URL entered in the **(Optional) Client Redirect URL** field, if supplied.
3. **Allow Firm Administrators [in *** Location] to login without SAML Authentication** allows *** location firm administrators to log into RS using the login page when the **REQUIRE SAML Authentication to login** is checked.
4. **Login "Location" is derived from** should always be set to *Map To SAML NameIdentifier*. This uses the **Access > User > Single Sign-On tab > Unique SAML Subject NameIdentifier mapped to this user** entry to the domain user account passed in by the assertion server during SSO login.

5. The bottom section after the **SAML Assertion Portal Configuration** label contains information specific to the client assertion server configuration.

6. The **SAML Source ID (40 hex characters):** contains a hash code assigned to a firm as a unique 40-character firm identifier (Source ID).

7. The URL in the **SAML Assertion Retrieval URL/Issuer:** field shows the client assertion server callback URL that the system calls when a user in the firm enters the product using SSO.

8. The **SAML Assertion Retrieval User Name:** field, usually populated by *ssoassertionuser*, shows the user name used with the assertion server callback.

9. The password in the **SAML Assertion Retrieval Password:** and **Confirm:** fields is the user password used with the assertion server callback. The implementation team that sets up your SSO will enter this for you.

10. The primary and secondary SSO contacts at the firm appears in the **SAML Assertion Portal Emergency Contact 1** and **SAML Assertion Portal Emergency Contact 2** fields.

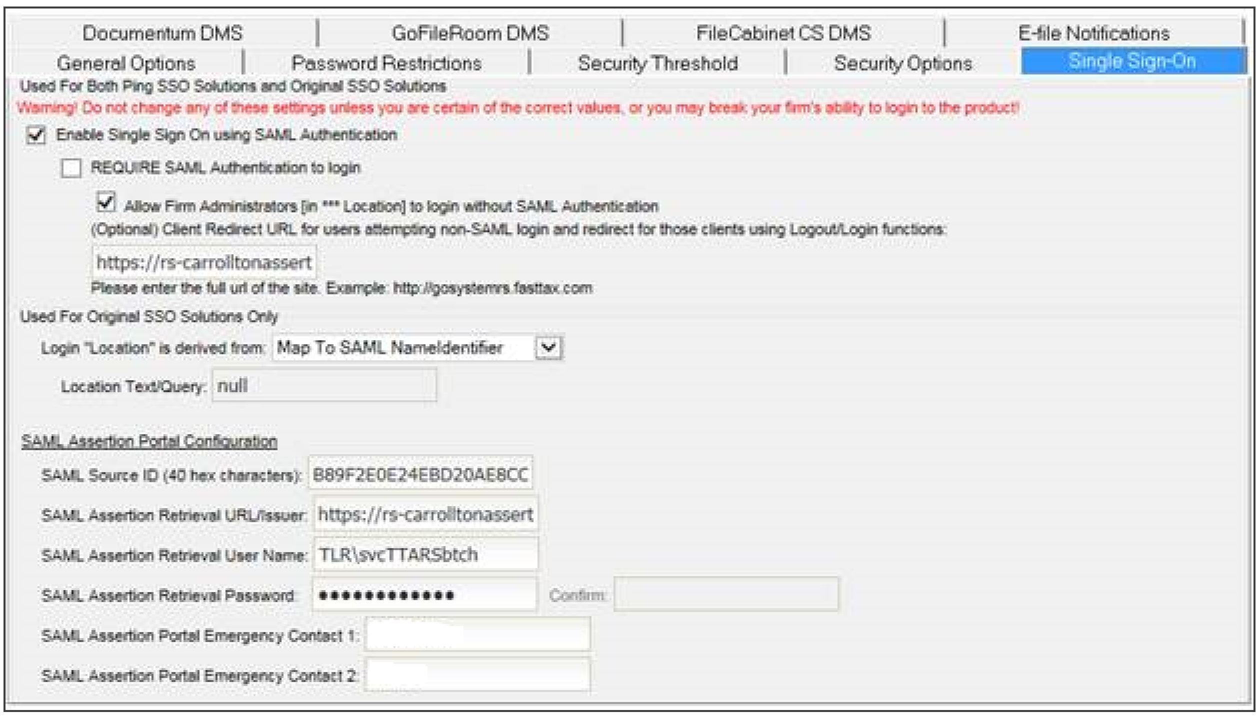


Figure 2:20

PING FEDERATE SSO CONFIGURATION

Four steps are required for a client to use our **Ping Federate SSO** solution.

You must contact your account manager and purchase the SAML Single Sign-On product. This will appear in the **Account Information** page in the **Products** tab.

Complete the Federated Single Sign-On client handout form and return it to Thomson Reuters. The TRTA SSO Admin team will create an entry in the **Ping Federate** system using the information in the form.

Enable Single Sign-On in the **Admin > Firm Configuration > Single Sign-On** tab. Set the other options to support SSO functionality as the client needs.

The first time a user attempts to log in using the SSO system, the **Ping Federate** system will send the user to the RS authentication dialog page with an SSO token. RS will authenticate the user, call the **Ping Federate** system web service to notify **Ping Federate** that the user is authenticated, and pass the SSO token and product credentials. The **Ping Federate** service will save the user information in the database that creates the remote client user account to the RS user account. On all subsequent login attempts, **Ping Federate** will map the incoming user account to the RS user account, and the user will be passed straight into the product, if the user account is still active.

RESTRICTING ACCESS TO ACCOUNTS BY IP ADDRESS

Every computer connected to the Internet has an Internet Protocol (IP) address. Such addresses are written as four numbers separated by periods. Be sure to get a list of the IP addresses and/or ranges you wish to enter before you begin.

Implementing the IP Range Validation

1. Sign in as an administrator (location ***).
2. Navigate to **Admin > Firm Configuration > Security Options**.

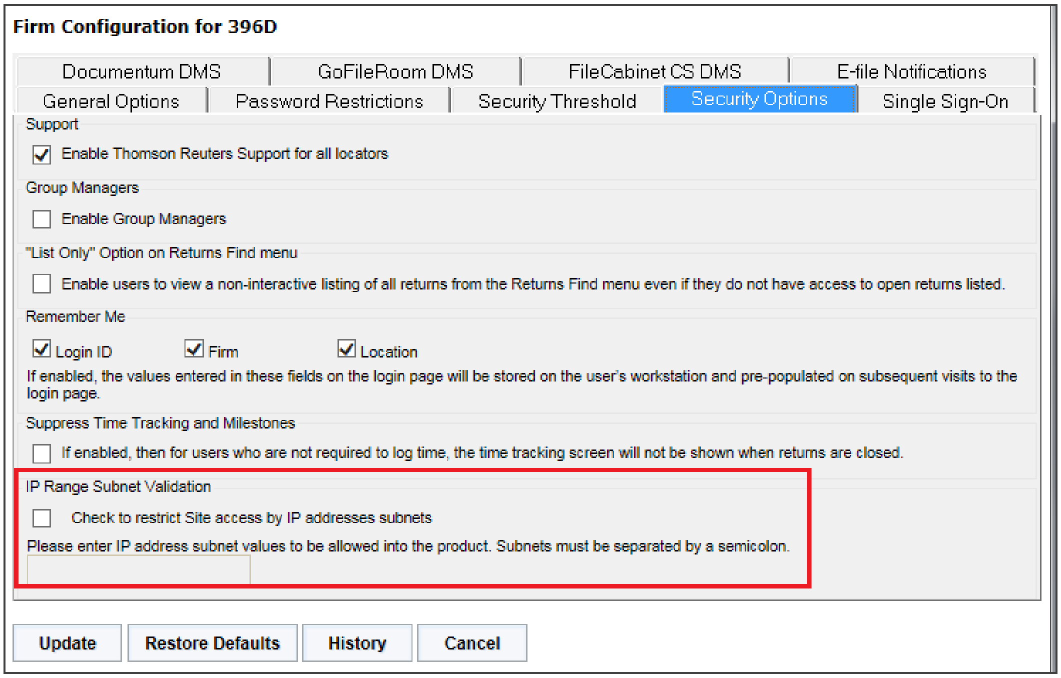


Figure 2:21

3. Scroll to the section labeled **IP Range Validation**.
4. Select the option to restrict access to the site by IP address.
5. Enter the IP addresses that you wish to access your firm accounts. Separate multiple IP addresses by semi-colons.
6. Click **Update**.

Be sure to include your own IP address! If you do not, you will lock yourself out of your account the next time you log in.

Levels of Restriction

There are three levels of restriction:

- by firm
- by group of machines
- by machine.

Firm Level To restrict by firm level, enter the first two sets of numbers in the firm’s IP address(es). For example, for *100.100.10.1*, you would enter *100.100*.

By Group To restrict access to a group of machines (for example, everyone assigned to a specific location), enter the first three sets of numbers in the group’s IP address(es). For example, for *100.100.10.1*, you would enter *100.100.10*.

By Machine Level To restrict access to only certain machines, enter the full IP address of each machine allowed to have access.

> ***Restricting access to machines is not the same as restricting access to people! Be sure, if you intend to restrict access by user, that you use the restrictions in Access Control to guard your accounts.***

REDACTING CERTAIN PERSONALLY IDENTIFIABLE INFORMATION

The IRS has issued Regulation 301.7216-3, providing guidance affecting tax return preparers regarding the disclosure of a taxpayer’s Social Security number to a tax return preparer located outside the United States in order to provide an exception allowing such disclosure with the taxpayer’s consent in limited circumstances.

In most circumstances, such disclosure will not be necessary. In order to protect the privacy of the taxpayer, Thomson Reuters has created a feature that redacts certain personally identifiable information, such as SSNs on tax returns across all tax return types. This feature can be implemented as follows:

- Administrators can enable redaction of certain personally identifiable information at the firm level.
- Administrators can then elect to redact certain personally identifiable information at the group level, so that all accounts assigned to a group will be redacted.
- Administrators can then elect to show certain personally identifiable information for a given return at the return level.

Redacting Information at the Firm Level

Administrators can choose firm-wide options to apply to all accounts and returns within the firm. To enable redaction of certain personally identifiable information at the firm level:

1. Select **Admin > Firm Configuration > General Options**.

2. Select the option to enable masking of personally identifiable information. Masking is the conversion of actual SSN to XXX-XX-NNNN when “NNNN” is the actual last four digits of SSN.

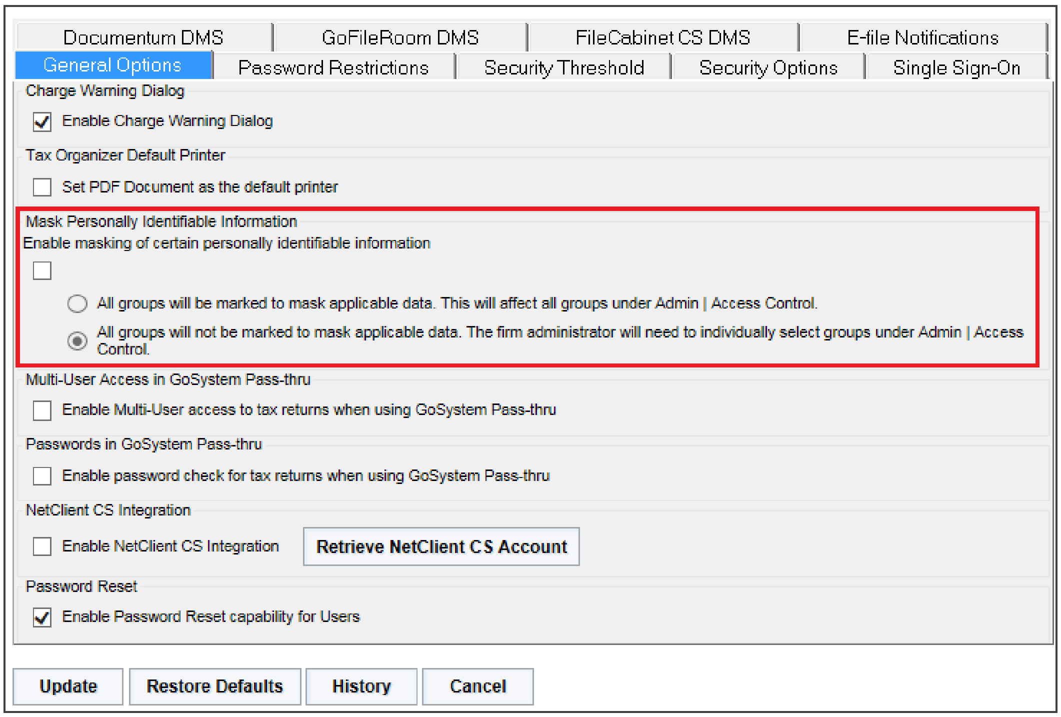


Figure 2:22

3. If you select the option to mask the data in the step above, select one of the following options:

   - **All groups will be marked to redact applicable data** This affects all groups under **Admin > Access Control**.

   - **All groups will not be marked to redact applicable data** The Administrator must select individual groups under **Admin > Access Control** in order to keep those groups from viewing certain personally identifiable information.

4. Click **Update**.

Redacting Information at the Group Level

If the second option under Step 3 above is selected, Administrators must select individual groups for redaction. To do so:

1. Select **Admin > Access Control > Groups**.
2. Select the **Edit** button.
3. Select the option to redact personally identifiable information.

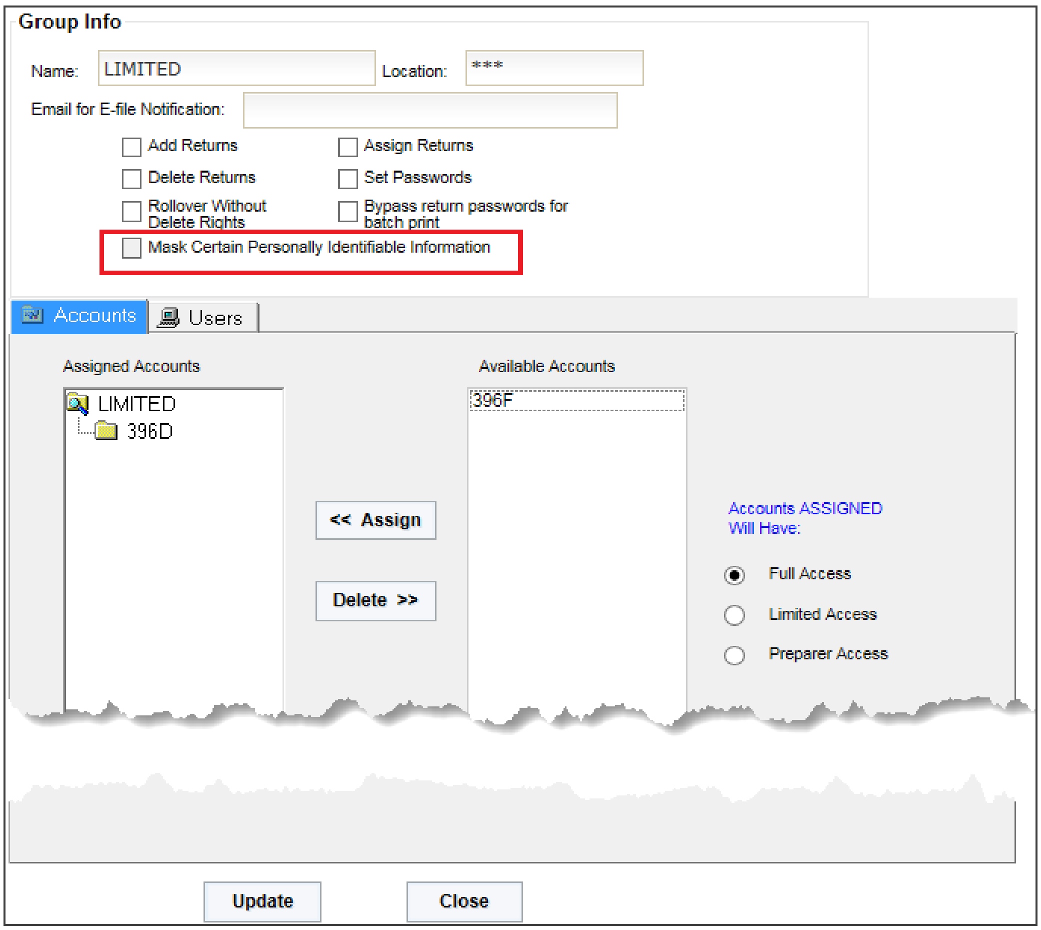


Figure 2:23

4. Click the **Update** button.

A user assigned to a group that has default masking and another group with redacting enabled will inherit the default masking level. The user will be able to view the personal information within the return unless the option is overridden at the return level.

Redacting/Viewing Information at the Return Level

If the firm has enabled redaction of certain personally identifiable information at the firm level, you can unmask the personally identifiable information for a return as follows:

1. Select the return to open.
2. Select **Returns > More > View Personal Information**.
3. Select the option to view personal information.

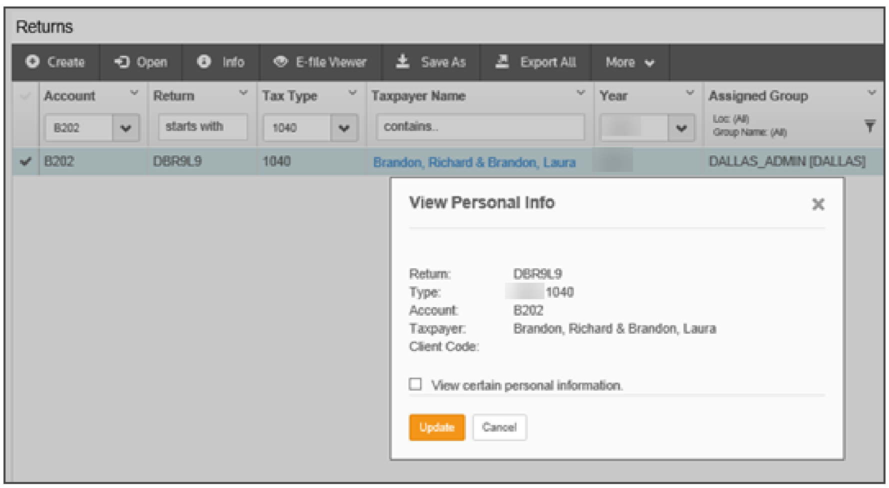


Figure 2:24

4. If this box is checked, and you wish to redact certain personally identifiable information, clear the check box.
5. Click the **Update** button.

Redaction: Known Limitations

PRINT

- The printed return will print with masked data for a user without SSN rights, and will print with unmasked data for a user with SSN rights. The government copy can only be printed by a user with SSN rights. A user without SSN rights could possibly file a paper return (not government copy) with data that has been masked.
- Users with SSN rights have access to Existing Print Files. If a user without SSN rights generated the existing print file, the file will contain masked SSN data. The user can create a new print file to properly print unmasked SSN data. Users need to exercise caution to ensure that the printed return contains unmasked data before filing a return.
- Users without SSN rights do not have access to Existing Print Files. The software cannot mask a print file after it has been generated. We have removed the option to view these artifacts for those users without SSN rights.
- Users without SSN rights do not have access to **Batch Estimates** and **Extensions View/Print** option. The print file is generated with unmasked data.
- Users without SSN rights may have access to unmasked data if a compute is not performed before creating the print file. Some states in Individual returns require a full compute in order to mask all print data.

PRINT PREVIEW

- Users without SSN rights do not have access to Existing Print Preview Files. The software cannot mask a print preview file after it has been generated. We have removed the option to view these artifacts for those users without SSN rights.
- Users with SSN rights have access to Existing Print Preview Files. If a user without SSN rights generated the existing print preview file, the file will contain masked SSN data. The user can create a new print file to properly print unmasked SSN data.
- Users without SSN rights may have access to unmasked data if a compute is not performed before creating the print preview. Some states in Individual returns require a full compute in order to mask all print data.

E-FILE

All users have the ability to create e-files. The e-files will contain unmasked SSN data. To maintain the security of SSN data, users without SSN rights will be unable to view XML electronic files through the XML E-file Viewer or XML download.

OVERRIDDEN SSN DATA

Overrides of SSN data on Tax Forms and Workpapers will not be masked for users without SSN rights.

MULTI-USER ACCESS

- The multi-user access is available. The rights assigned to the first user to open the return decides the rights requirements of subsequent users' access. If the second user has the same rights or higher rights as the first user, the second user will be allowed access and will see the return in its current format (either masked or unmasked). If a user without SSN rights attempts to open a return currently in use by a user with SSN rights, a message will appear informing the user of a rights mismatch.
- When multi-user access is in use and a user enters SSN data, all other users currently in the return will be able to view that data no matter what rights they have.

EXPORT

- **Planner CS** and **To DIF file** export options from within a return are not available to users without SSN rights.
- All exported data is unmasked. Because the exported data is used for import and/or the creation of new returns, the data must be unmasked in order to create a viable return and maintain data integrity.

BUSINESS RETURNS

Redaction is not available for business returns.

MULTI-FACTOR AUTHENTICATION

Thomson Reuters ***strongly recommends*** that you use multi-factor authentication to provide the highest level of security for your firm and client data.

What is Multi-Factor Authentication?

Multi-factor authentication adds an additional layer of security that helps protect your firm's confidential data. Many of your online accounts or software applications are currently protected by a login and password. That password is the single factor in the authentication process — the way that those applications or services confirm your identity.

Multi-factor authentication adds at least one more layer of identity verification to that process so your protection against hacking and fraud attempts is stronger and more secure than a simple password. That additional layer can take many forms, such as a physical ID card, a digital confirmation code, or even your fingerprint. You use multi-factor authentication every time you pay a transaction using a debit card or withdraw cash from an ATM: your debit card is one factor and your PIN is another.

How Does MFA Work?

Thomson Reuters provides multi-factor authentication through the Thomson Reuters Authenticator application. After installing the mobile application on your smartphone and pairing that device with your application login credentials, you'll use the Authenticator to confirm your identity every time you log in to the Thomson Reuters RS system. You do so via a notification that is sent to the Authenticator mobile application, which you can quickly approve on your mobile device.

Software that works with Thomson Reuters Authenticator allows you to authenticate on three levels:

1. Something you **KNOW** (your login and password)
2. Something you **HAVE** (your mobile device with the Thomson Reuters Authenticator application)
3. Something you **ARE** (your fingerprint, if your device has Touch ID enabled)

Using multi-factor authentication makes it difficult for anyone else to use your login, as any would-be hacker must either have your mobile device at hand. If you decide to enable fingerprint authentication, hacking becomes impossible.

Setting Up and Implementing MFA in Your Firm

By default, MFA is an optional feature that individual users can opt into by enabling it for their own accounts. If desired, RS administrators can enable a setting that requires that all staff members log in with MFA.

We ***strongly recommend*** that you use MFA to provide the highest level of security for your firm and client data. MFA requires a mobile device with the Thomson Reuters Authenticator application installed.

By default, MFA is ***optional***. Firms can set it up if they choose. You can make MFA a required security feature for staff. This setting requires the administrator rights to change the setting.

1. Select **Admin > Firm Config**.
2. Select the **Security Options** tab.
3. Under the heading **Multi-factor Authentication**, select the options you wish to use.

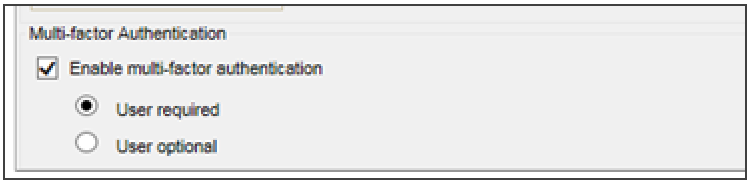


Figure 2:25

- **Required**: When MFA is required, users will be prompted to set up MFA at their next login, after which they must use a mobile device with the Thomson Reuters Authenticator application to log in to the RS system.
- **Optional**: When MFA is optional, users will not be prompted to set up MFA, but they can opt in to using the Thomson Reuters Authenticator application to provide an additional layer of security for their RS logins.

Generating a Temporary Login Code

When a user cannot log in using MFA — such as when users leave their phones at home or a phone is damaged — users with administrative permissions can generate a temporary, 24-hour numerical code to enable the user to log in.

1. Go to **Admin > Access Control**.
2. Select the user who needs the temporary code.
3. Select **User**.
4. At the bottom of the screen, locate the button labeled **Generate 24-Hour OTP for this User**.

5. Click the button. Generating the code disables any codes previously located for that user's account.

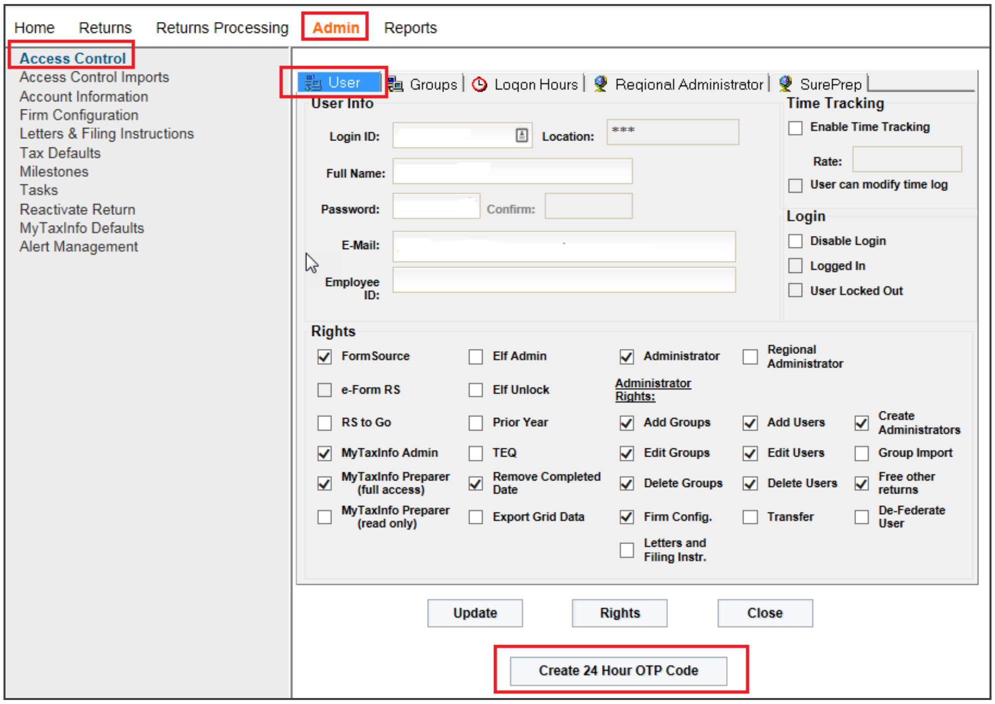


Figure 2:26

6. A dialog appears to the right with the temporary code.

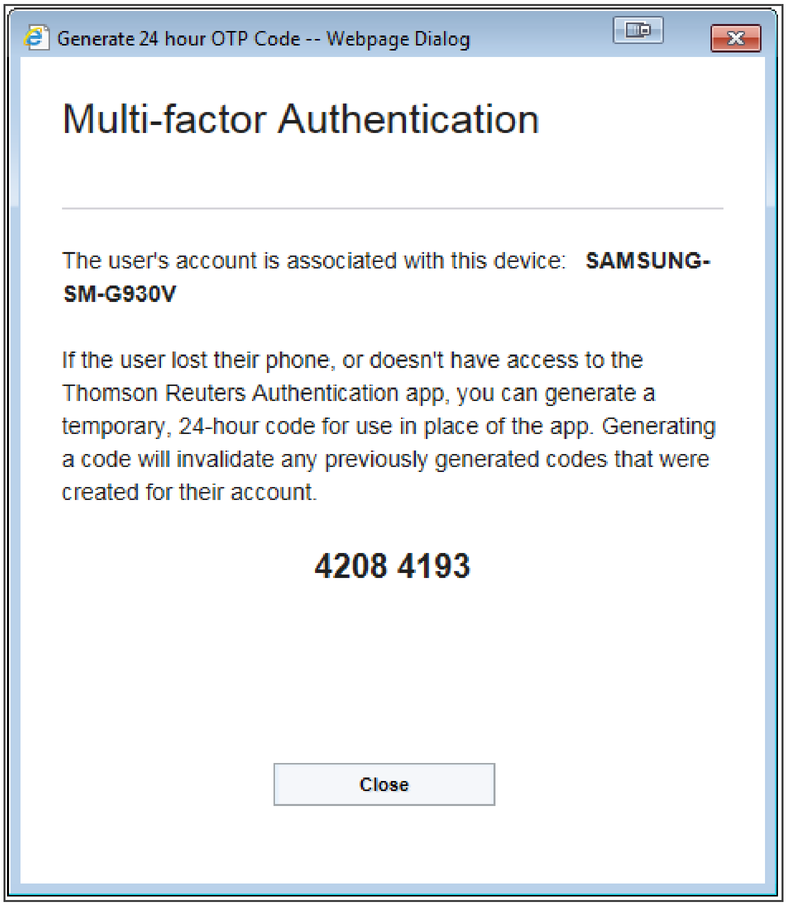


Figure 2:27

7. Send the code to the user.
8. Click **Close**.

CHAPTER 3: USING ACCESS CONTROL TO MANAGE GROUPS AND USERS

The **Access Control** module gives you the flexibility you need to delegate the creation of users and groups within your firm to administrators in various locations. Groups and users created by each location administrator are grouped by location. Groups and users created by the location administrator in Dallas are not visible to the location administrator in Los Angeles, unless the Los Angeles administrator has rights to the same set of accounts.

To restrict administrators so that they can only modify groups and users in specific locations, make them Regional Administrators, and assign them the locations that they should be allowed to administer.

History History buttons are available on several of the **Access Control** dialog boxes. These history logs show users who have created or modified groups or users and the type of edit made.

Administrators who need to set up tax defaults for a given account must have the tax defaults assigned to their location before they can modify their tax defaults. See ***Assigning Owners of Tax Defaults (page 62)*** for a description of how this assignment is made.

USING ACCESS CONTROL

Use the **Access Control** system to set up groups of users who will have access or login rights to the system.

Setting up **Access Control** is a two-step process:

1. Associate specific rights with groups as the groups are created.
2. Associate users with those groups.

The **Access Control** menu option is visible only to users with administrator rights and is found on the **Admin** menu.

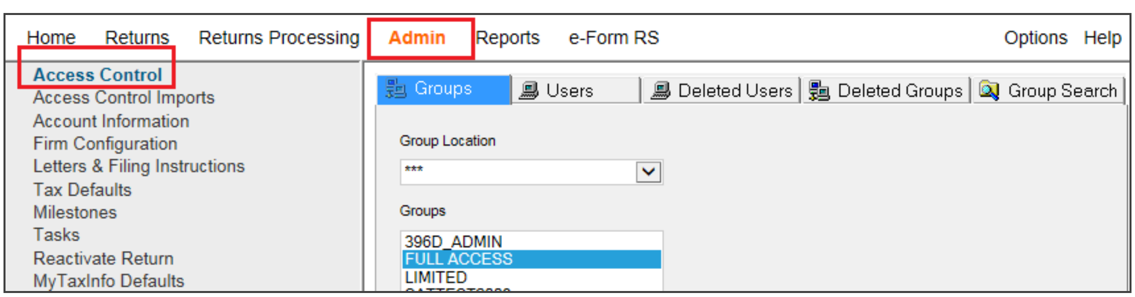


Figure 3:1

TYPES OF USERS AND THEIR RIGHTS

Four types of users are distinguished by the level of rights they have:

FIRM ADMINISTRATORS	• Initiates first login for the firm • Has access to all accounts for the firm • Has access to all users in all groups within the firm • Sets up groups and group access • Sets up the location names used on the login screen • Assigns account numbers to groups • Assigns location administrators to groups • Assigns Tax Defaults to locations
LOCATION ADMINISTRATORS	• Sets up users for their location • Sets user access • Sets user login IDs and passwords • Sets up Administrators within their location • Assigns account numbers for users • Assigns returns to groups or users • Updates Tax Defaults assigned to their locations
REGIONAL ADMINISTRATORS	• Same rights as Location Administrator, but can also setup Administrators in authorized locations.
USERS	• Accesses accounts assigned by Location Administrators • May belong to more than one group if authorized by a Location Administrator • May allow Support to access returns assigned to them

Administrators

Using groups provides administrators a method of granting rights to users at the group level without having to modify each user’s rights individually.

There are three types of administrators:

- firm administrator
- location administrators
- regional administrators.

The firm administrator login must be used initially to set up other firm administrators, regional administrators, and location administrators who can then create their own groups and users. Any administrator can grant the administrator right to another user, although only the firm administrator can grant regional administrator rights to another user.

Firm administrators can designate locations for the users and groups that they create, whereas location administrators cannot designate locations. This keeps each group and user unique from groups and users created in other locations.

User Locations have no relationship to Group Locations. Users in any User Location can be members of any Group, without regard to Group Location.

CREATING GROUPS

Creating a Group

1. Log in as an administrator.
2. Select **Admin > Access Control > Groups** tab.

3. A default **Group Location** of *** and a list of existing groups appear as shown below.

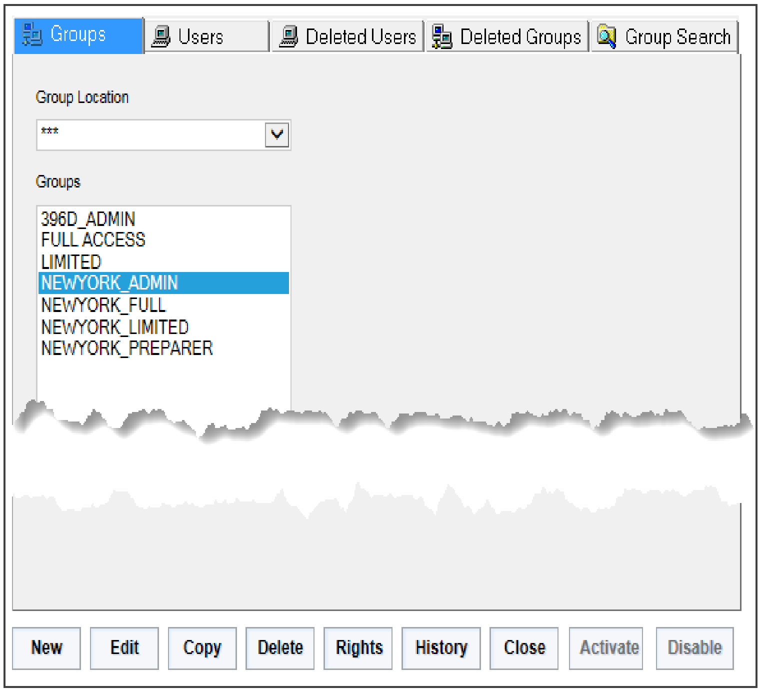


Figure 3:2

4. Initially, only the firm group exists (group location ***). This group name varies depending on the name Thomson Reuters created for the firm during the initial setup. Any member of this firm group has rights to all accounts.

Assume that offices exist in Dallas, New York, and Los Angeles. Each office has an administrator who creates groups and users. The firm administrator can create a group for each location and associate one or more location administrators with any group.

Creating an Administrator Group

1. Click the **Groups** tab, and then click **New**.

2. The screen shown below appears.

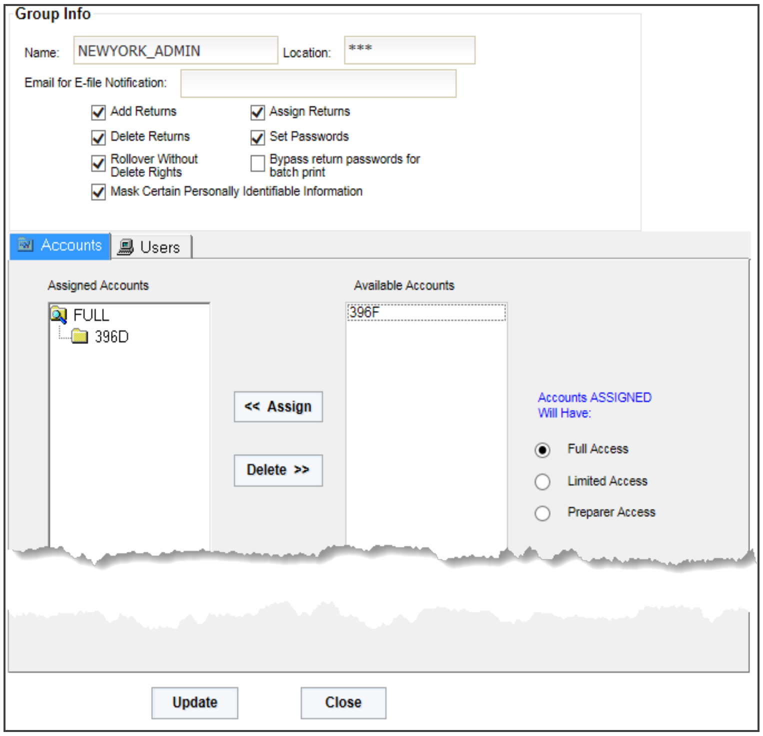


Figure 3:3

3. Enter the name of the group and a descriptive unique location. In this example, NEWYORK_ADMIN is used as the group name, and *** is used as the location.

4. Select the rights to be granted to administrators associated with this group. Administrators that belong to this group can pass whatever rights they were granted on this screen on to their own groups and users.

5. Select each account that the administrator needs to access. Only the assigned accounts are accessible by members of the group. In this example, the account 396D belongs to the New York office.

   Full Access should normally be used when granting access to an entire account. *Limited* and *Preparer Access* restrict access within an account to specific returns assigned to groups or users. See **Using Limited and Preparer Access (page 59)** for more information on limiting access to returns.

   If *Full Access* is used, a user has unrestricted access to see and open all returns in the account.

6. Once you have assigned appropriate rights and accounts to the group, click **Update** to store the new group.

7. Click **OK** to return to this screen for *Full Access*.

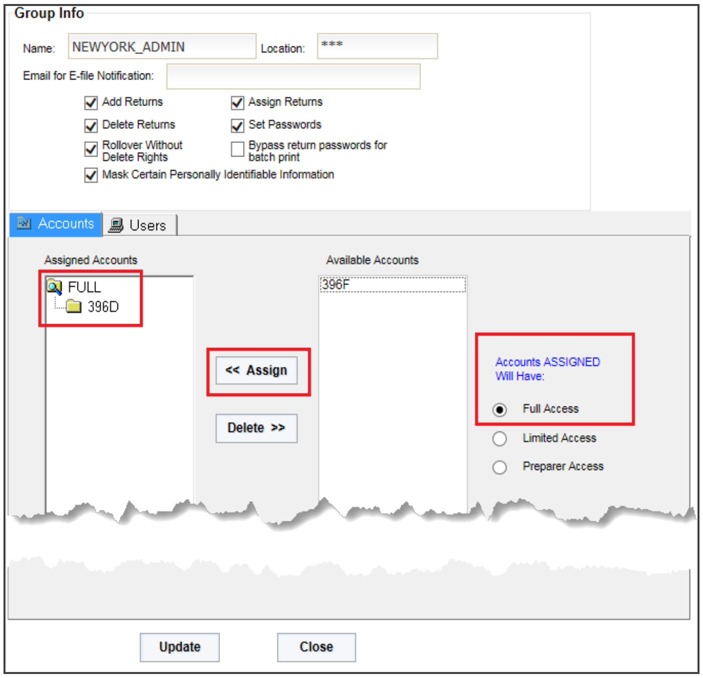


Figure 3:4

8. Click OK to return to this screen for *Preparer Access*.

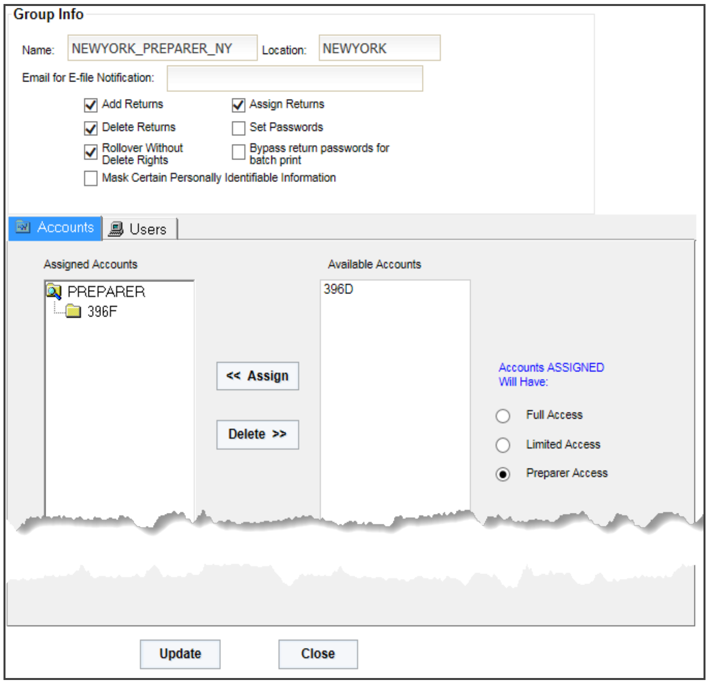


Figure 3:5

9. Click **Close** to return to the **Groups** screen shown below. The new group names should then appear in the group screen as shown. In this example, the group NEWYORK_ADMIN has *Full Access* to Account 396D, and the group NEW YORK_PREPARER has *Preparer Access* to Account 396F.

   Choosing a different **Group Location** in the drop-down arrow box will display different **Groups** that are set up for other **Locations**.

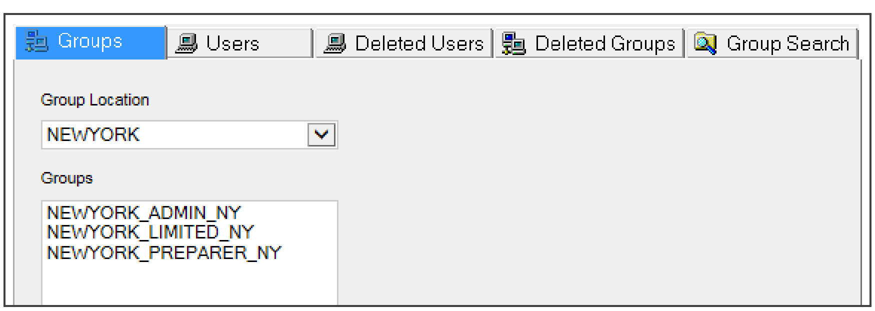


Figure 3:6

Group Rights

Any administrator that is created should be given the maximum rights available so that any new groups or users created by that administrator may be granted appropriate rights. Restricting rights of an administrator will prevent them from granting the rights to any group or user that they create or edit. Each right that can be granted through a group is described below.

Add Returns Having rights to add returns allows users to create new returns by selecting **Returns > Create Return**, or by using the **Save As** option located on the **Returns** menu after displaying a list of returns. The **Import** option found on the **Returns Processing** menu also requires users to have the **Add Returns** right if the import file does not specify an existing locator number for a tax return. The **Add Returns** right does not restrict the user from creating returns when using the **Separate Returns Joint Data (SRJD)** or **Tax Equalization (TEQ)** features in the tax application.

Assign Returns The **Assign Returns** right allows users to make various assignments to returns. Once returns are displayed after selecting **Returns > Find Return**, a user can select the **Assign Users/Dates** menu option. Firms that have purchased GoTracker® will have the **Assign Users/Dates** menu option.

Delete Returns Users having the right to deactivate returns may do so by selecting **Returns > View Return Information** and clicking the **Deactivate Return** button. Users that do not have the deactivate right will not be able to re-roll a tax return since the rollover process will not overwrite existing data unless the user has the **Rollover without Delete Rights** right described below. Users who have the right to deactivate returns will be prompted to **Bypass** or **Overwrite** tax return data during the rollover process.

Set Passwords Users having the right to set passwords may set passwords for tax returns or change those passwords on returns where they already know the existing passwords. Administrators having the **Set Password** right do not have to know the existing return password to change it.

Rollover Without Delete Rights Users who should not be allowed to delete returns but who should be able to re-roll returns will need the **Rollover Without Delete Rights** right. Users who have either the **Deactivate Return** right or the **Rollover Without Delete Rights** right will be prompted to **Bypass** or **Overwrite** tax return data during the rollover process.

Bypass Return Passwords For Batch Print Users who are members of a **Group** with this right can download returns created through the batch print process without having to enter the locator password.

Mask Certain Personal Identifiable Information In order to protect taxpayer privacy, certain personal information such as SSNs will be masked on tax returns assigned to **Groups** with this option checked.

CREATING USERS

The first users that should be created are other Firm Administrators in the *** Location. This ensures that there is a backup *** Administrator login.

Firm Configuration, a right available under **Administrator Rights**, allows access and edit of **Firm Configuration** options. The **Firm Configuration** right may be selected for Administrators in the *** Location only.

The figure below shows the rights that are automatically granted when you select the **Administrator** check box. When you set up new *** Administrators, the **Firm Configuration** and **Letters and Filing Instructions** rights along with the **De-Federate User** right will NOT be automatically enabled when you select the **Administrator** check box. If these rights should be granted, you must select them separately.

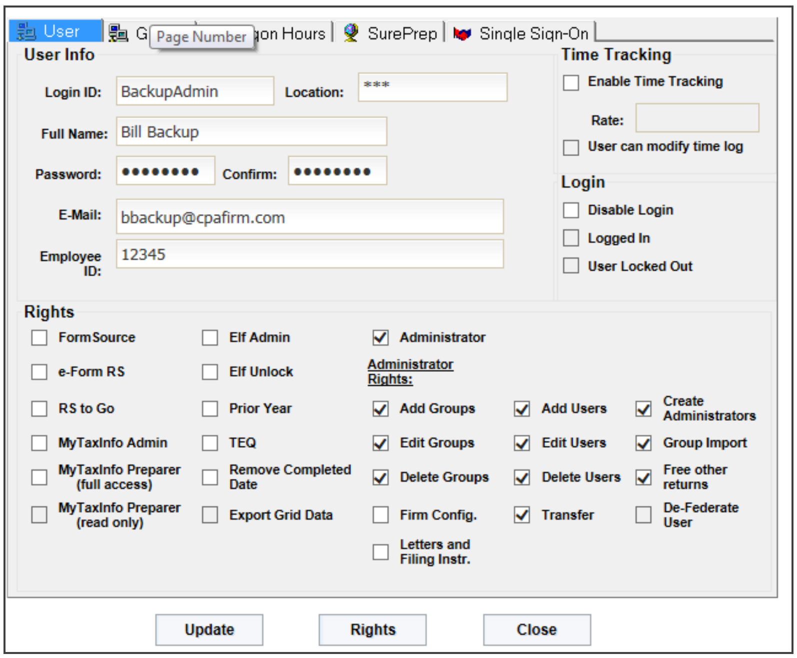


Figure 3:7

The **Firm Configuration** right will be enabled for any existing Administrators in the *** location. The primary *** Firm Administrator should remove the right as necessary to ensure that **Firm Configuration** changes are only made by appropriately authorized *** Administrators.

The next users that should be created are location administrators. This allows them to log in and create their own groups and users.

1. To create a new user, click the **Users** tab. This displays the screen shown below.

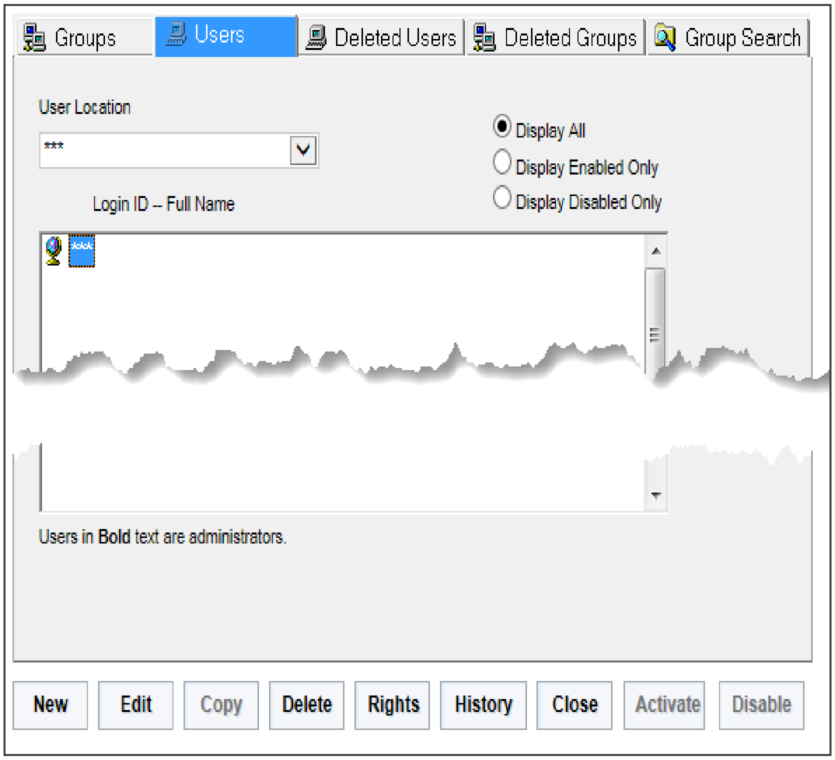


Figure 3:8

2. Users are grouped by location. Select the location in the drop-down arrow box to display the users in a group.

3. Click **New**. The screen where you create new users appears.

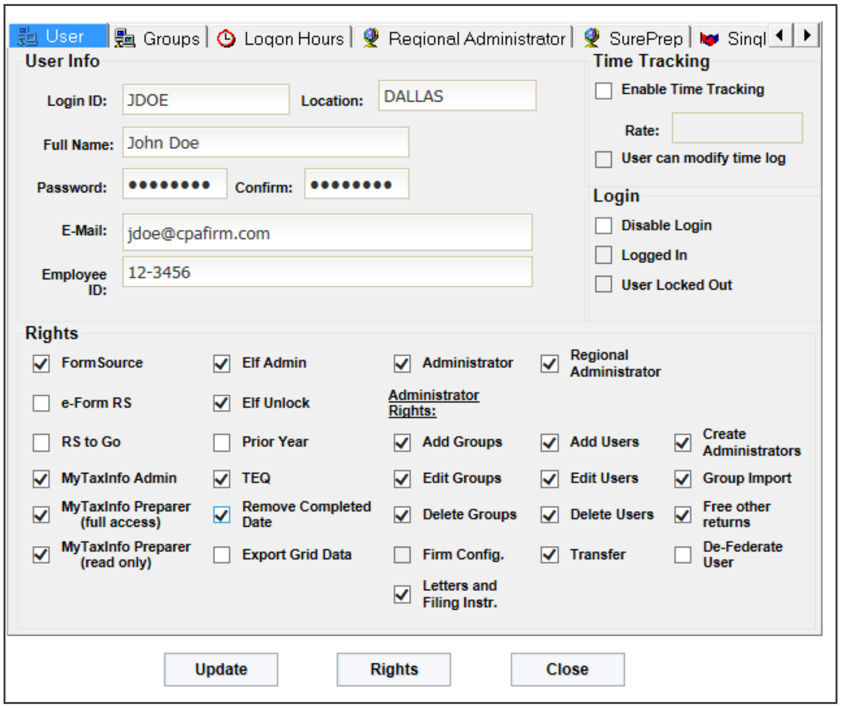


Figure 3:9

4. Enter the user's login ID.

   Only the firm administrator can specify a new location when creating new users.

   Login IDs with a location of *** and who also have the administrator right are considered to be firm or regional administrators.

   Regional administrators may be assigned to multiple locations and will be able to create new users in any of their assigned locations.

   Login IDs with locations other than "***" and the administrator right are considered to be location administrators.

5. Enter the user's full name, password, email address, and Employee ID. Enter the password ***twice*** to verify its accuracy.

6. If the user should log time, check the **Enable Time Tracking** check box and fill in the appropriate hourly rate.

7. Check the box if the user is allowed to modify the time log.

8. In this example, the firm administrator is creating a login ID for JDOE, a location administrator in DALLAS. In the **Rights** section in the lower half of the User tab, check the **Administrator** check box, if the user is to be an administrator.

   Making a user an administrator enables the **Access Control** menu option for that user.

9. By default, all administrator rights are enabled when the **Administrator** check box is selected. You may remove any rights if you wish to restrict what this administrator can do within **Access Control**. For example, if you want the administrator to be able to add or edit groups, but you do not want the administrator to be able to delete groups, remove the **Delete Groups** right.

10. If you wish to make this user a regional administrator, one who can modify groups and users in multiple locations (but not all locations), check the **Regional Administrator** check box, and then click the **Regional Administrator** tab. Select the locations that the regional administrator can modify, and then click **Assign**.

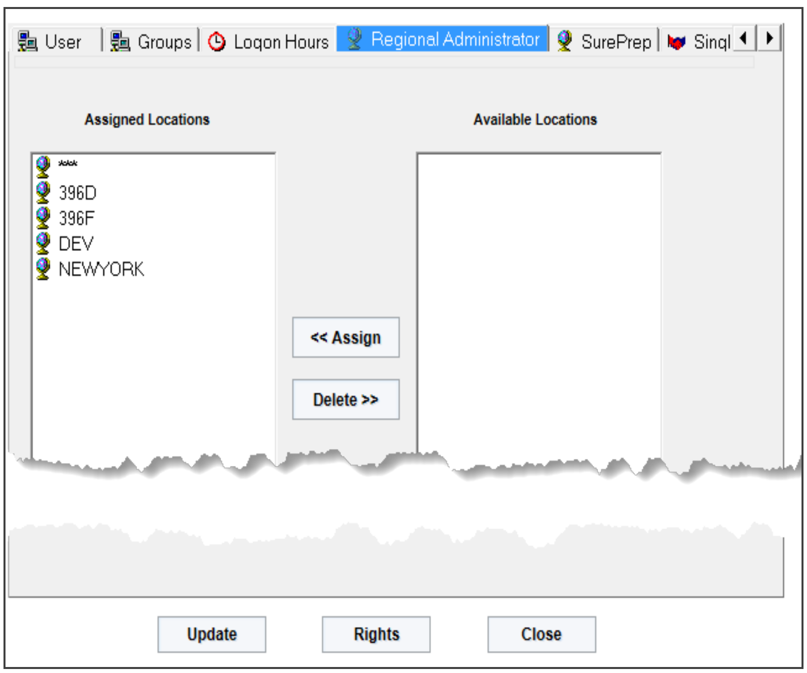


Figure 3:10

11. Additional products may appear in the **Rights** section of the **User** tab. These rights must be granted to each user instead of through groups, since the number of users authorized to access these products or functions may differ from the number of users that can be created in **Access Control**. User rights control whether the user can execute one of these products or functions.

12. Before clicking the **Update** button, you must click the **Groups** tab, as shown below, to make the JDoe login ID a member of at least one group.

A user may belong to multiple groups. If one group grants full access to an account and another group grants Limited or Preparer access to the same account, the user has full access to the account.

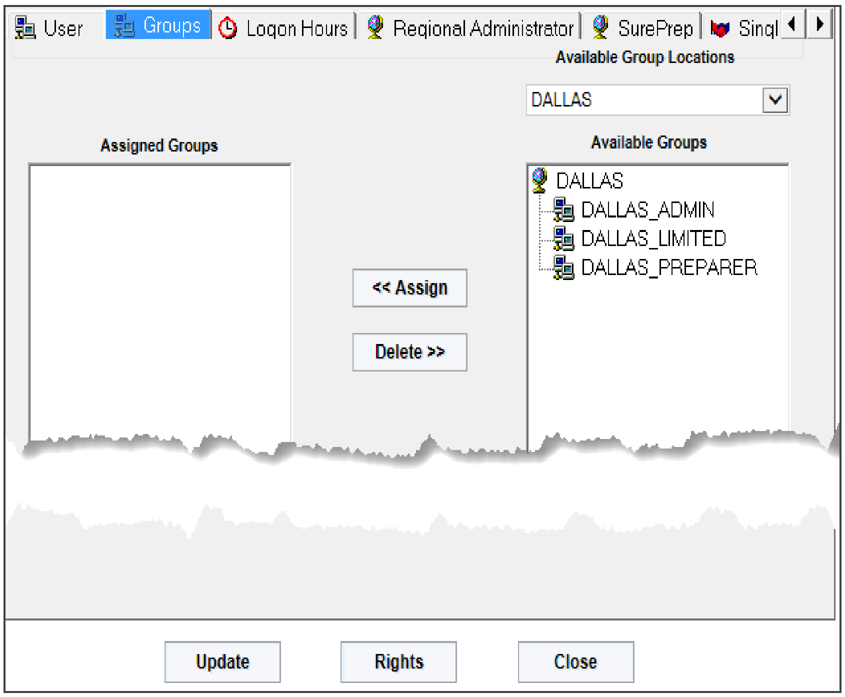


Figure 3:11

13. On the **Groups** tab shown above, first select DALLAS, one of the Available Group Locations. Making that selection displays a list of **Available Groups**. Click the group named DALLAS_ADMIN in the **Available Groups** column. Click **Assign** to make the JDoe login ID a member of this group.

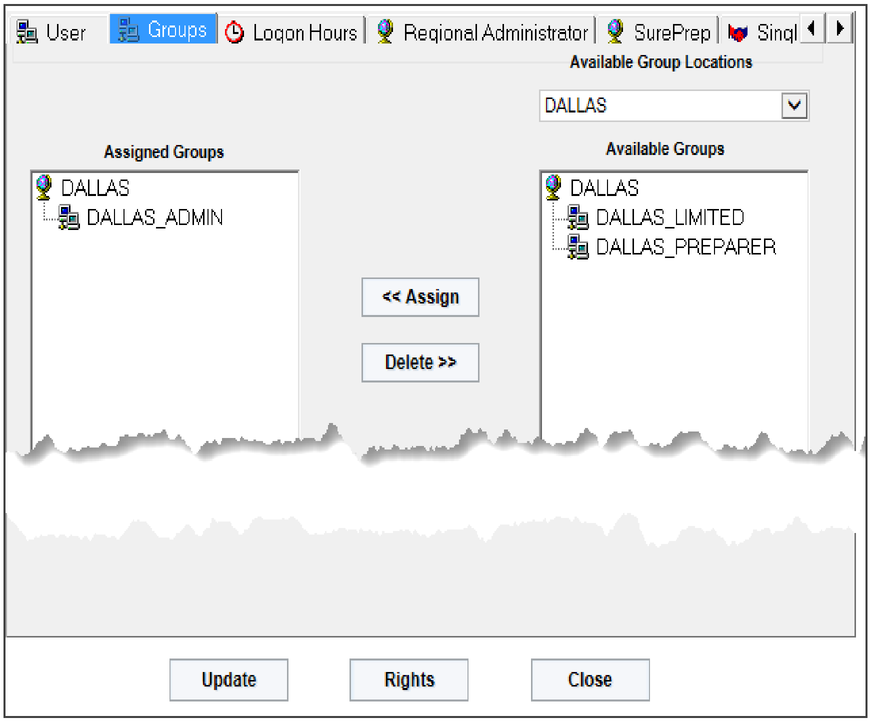


Figure 3:12

> If a user is assigned to only one Group, then the user cannot be deleted unless assigned to another Group. Conversely, if a Group has only one user, then the Group cannot be deleted until another user is assigned to that Group.

14. Click **Update** once you have assigned the user to a group on the **Groups** tab and checked the appropriate product and function rights on the **User** tab.

15. You may use the **Rights** button to verify that the rights of an existing user are set correctly. Selecting the **Rights** button displays a screen showing the Login ID, Location, current login status of the user, the date and time the user last logged in, as well as user rights and effective account rights. The **Rights** screen shows the various accounts the user may access and the access levels of *Full*, *Limited*, or *Preparer* for each of those accounts. The seven group rights that are granted as part of the group setup process and Group Membership are also displayed.

16. Two useful options available to administrators are found on other menus:

    - The **Admin > Account Information** option shows groups that grant access to specific accounts.
    - The **Reports > List Users** report also shows users' rights.

Group Managers

If a user is to be a manager of a user group, the option must be first activated in the **Admin > Firm Configuration > Security Options** tab.

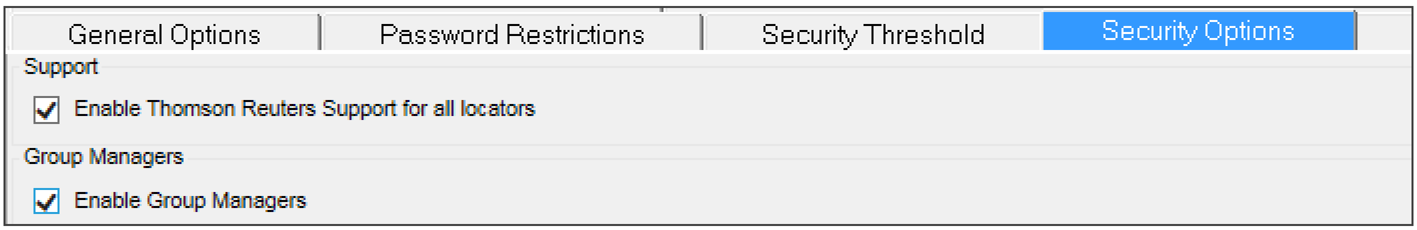


Figure 3:13

In **Access Control**, go to the user who should be a Group Manager. Choose **Edit** on the User's Login ID and proceed to the user's **Groups** tab.

1. Make sure the correct Location is displayed and that the correct **Available Groups** are in the list on the right.
2. Highlight the group that JDOE should manage.
3. Check the **Group Manager** option.
4. When the **Available Group** (in this case, the DALLAS_PREPARER group) is assigned, the group will move from the right column to the **Assigned Groups** column on the left.

5. To show that JDOE is the manager of DALLAS_PREPARER, a plus (+) sign will show in front of DALLAS_PREPARER group.

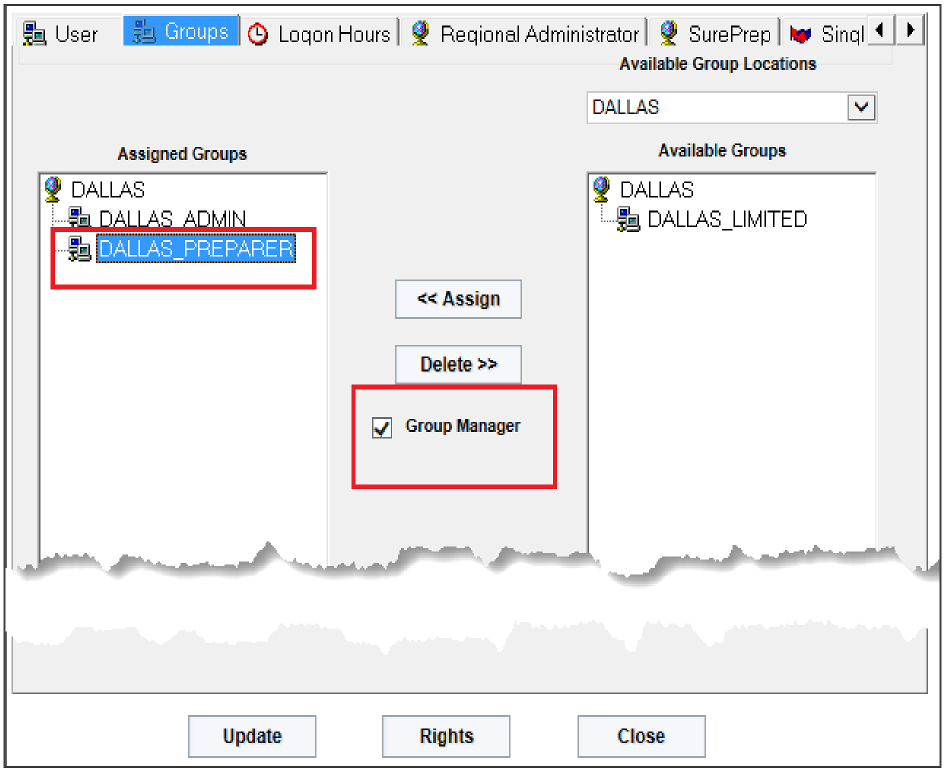


Figure 3:14

The Group Manager can:

- Assign or Remove Accounts
- Add or Remove Members.

Regional Administrators

The **Regional Administrator** role in **Access Control** is intended to assist the firm administrator in cases where there are a large number of accounts and/or users that need to be maintained.

Only an administrator logging in with the login ID ADMINISTRATOR can designate a user as a regional administrator. Once the ADMINISTRATION designates a user as regional administrator, then that new regional administrator can grant regional administrator status to other users.

To create the regional administrator's login ID, you must be logged in using login ID **Administrator** and **Location** ***. The Regional Administrator must be created with a location of ***. The login ID should be made a member of one or more groups, as necessary, to grant access to all accounts within their region. The Regional Administrator will not be able to grant rights or assign returns in accounts to users if those users do not have rights to those accounts.

Regional administrators can assign returns from accounts within their region to any **Location** and **Group** throughout the entire firm.

1. Select the **Regional Administrator** check box shown below.

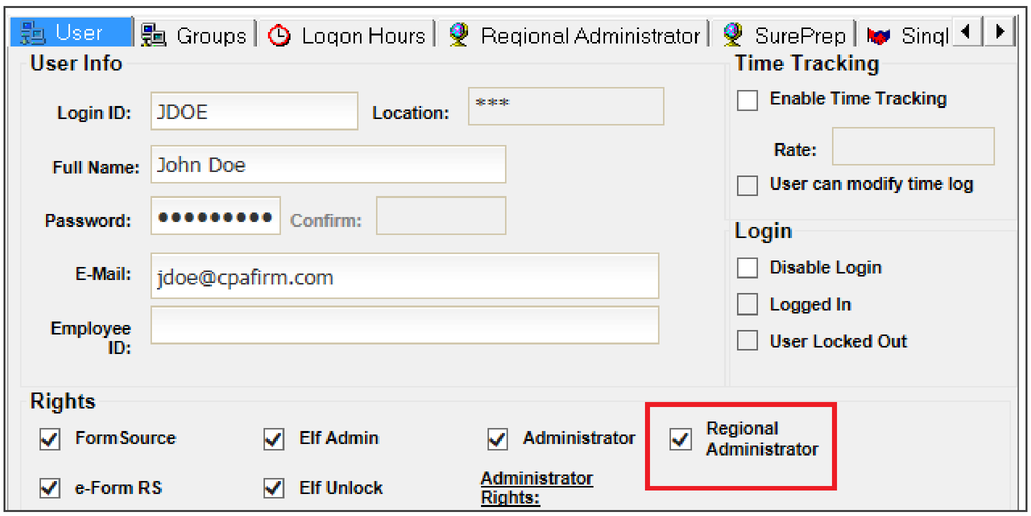


Figure 3:15

2. Then click the **Regional Administrator** tab. Assign the necessary locations to the regional administrator. In this case, JDOE has been made a Regional Administrator for the DALLAS Location.

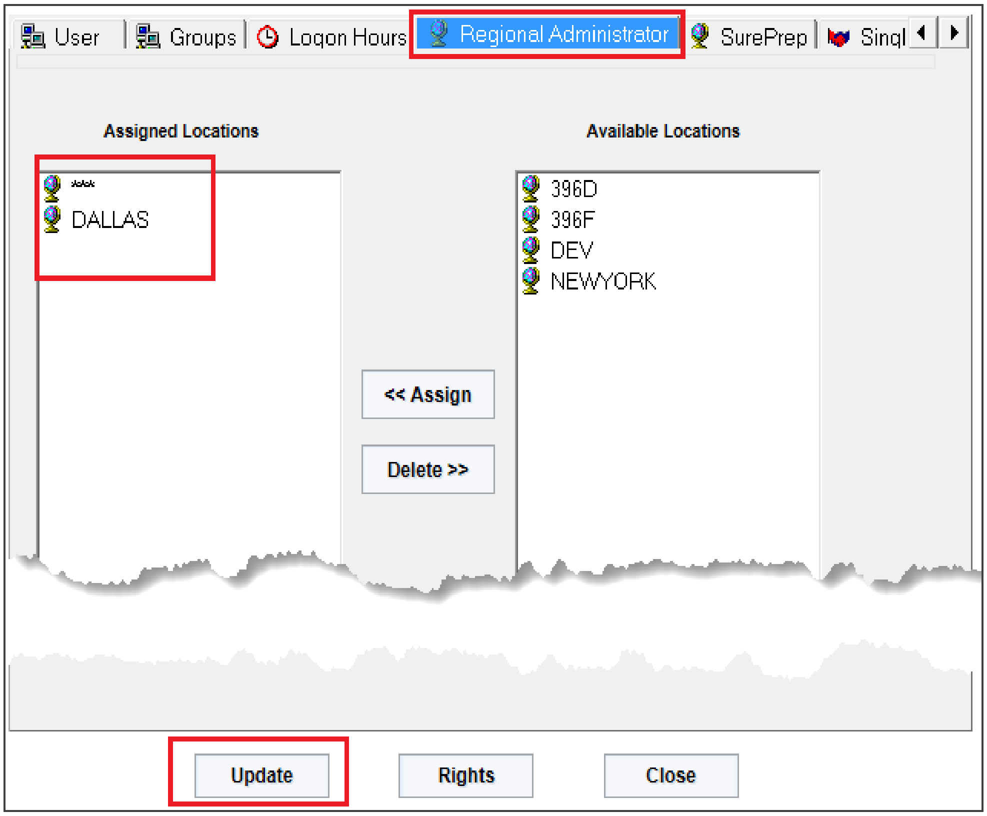


Figure 3:16

Assigning Users to Existing Groups

From the **Group** screen shown below, you can select an existing group to which new users may be added.

1. Select the group, and click **Edit**.

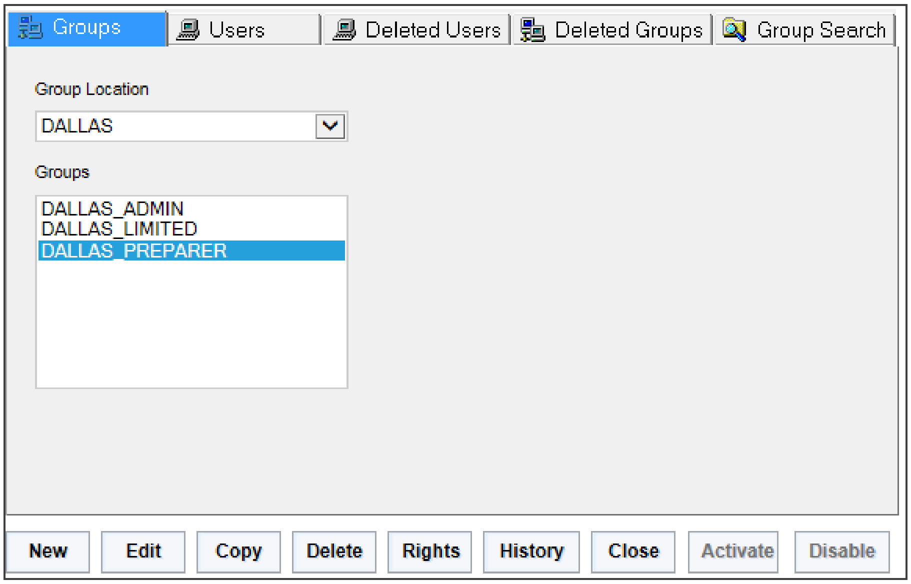


Figure 3:17

2. Click the **Users** tab. The following screen appears.

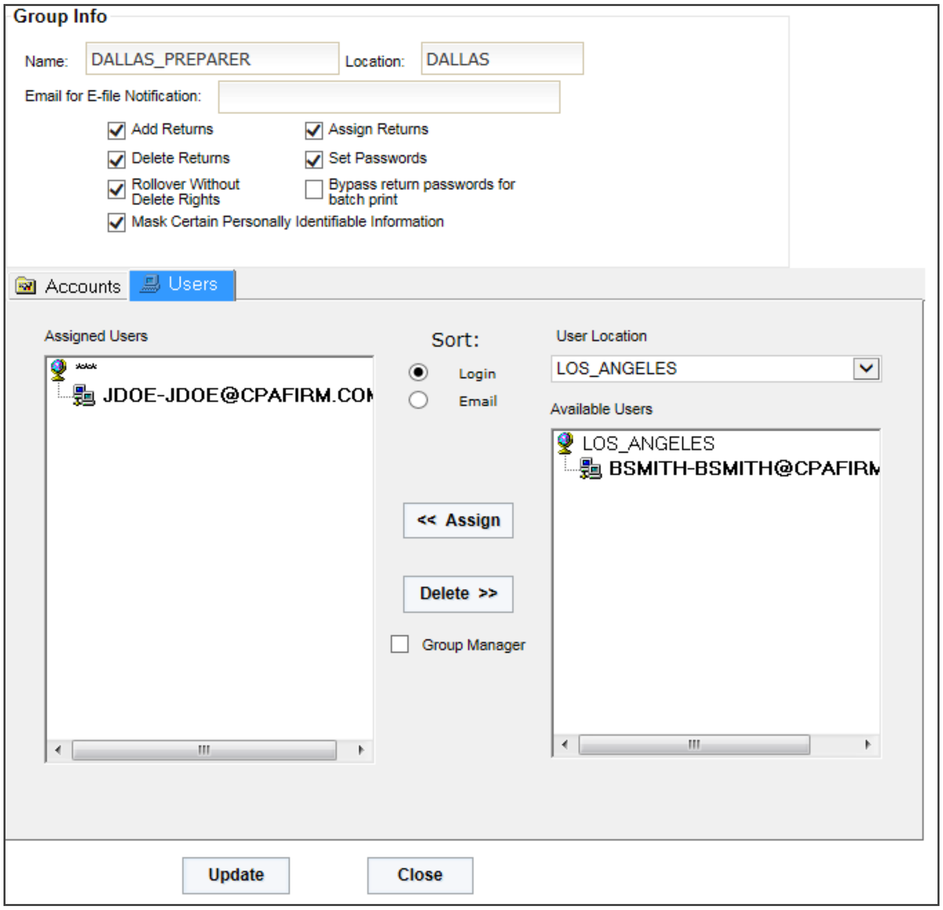


Figure 3:18

The **User Location** list allows selection of a specific location. The **Available Users** list box allows selection of users that currently are not members of the group, including users from other locations. In the example below, the user BSMITH from Los Angeles can be made a member of the DALLAS_PREPARER group. User-administrators appear with their login IDs in bold.

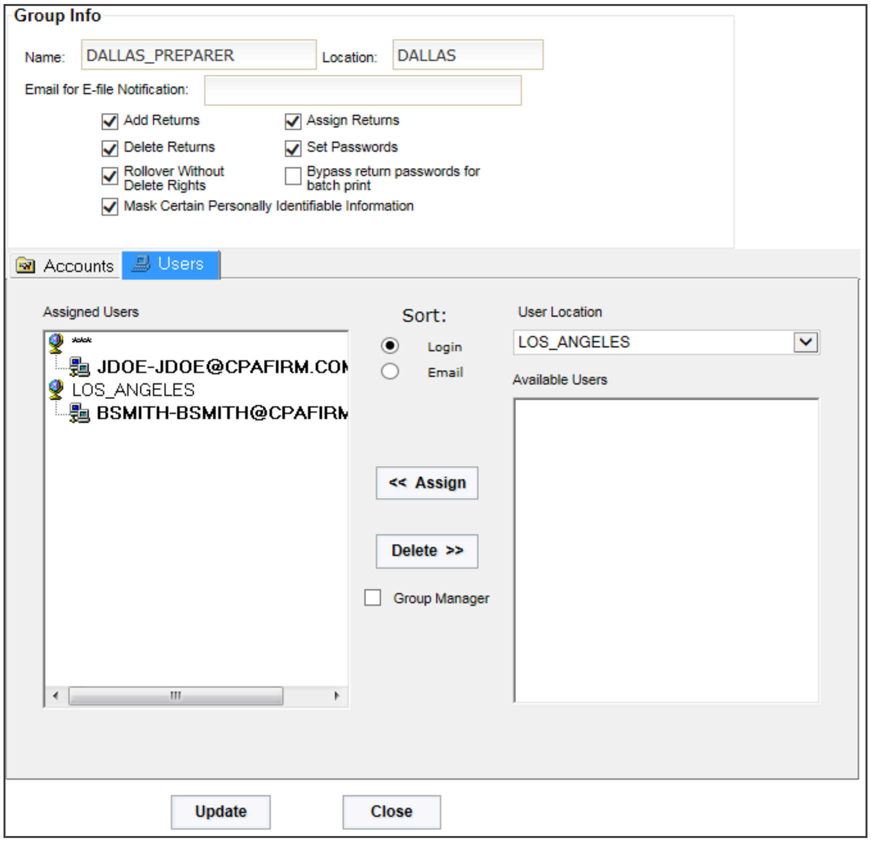


Figure 3:19

Assigning users from other locations to a group allows sharing of group rights without requiring the creation of new groups for these special cases. In this example, user BSMITH in Los Angeles can gain rights to returns in the Dallas location using this method.

Logon Hours

The tab for **Logon Hours** enables you to block out times when users would be denied access to the system. See the screen below for the default settings for 24x7 access.

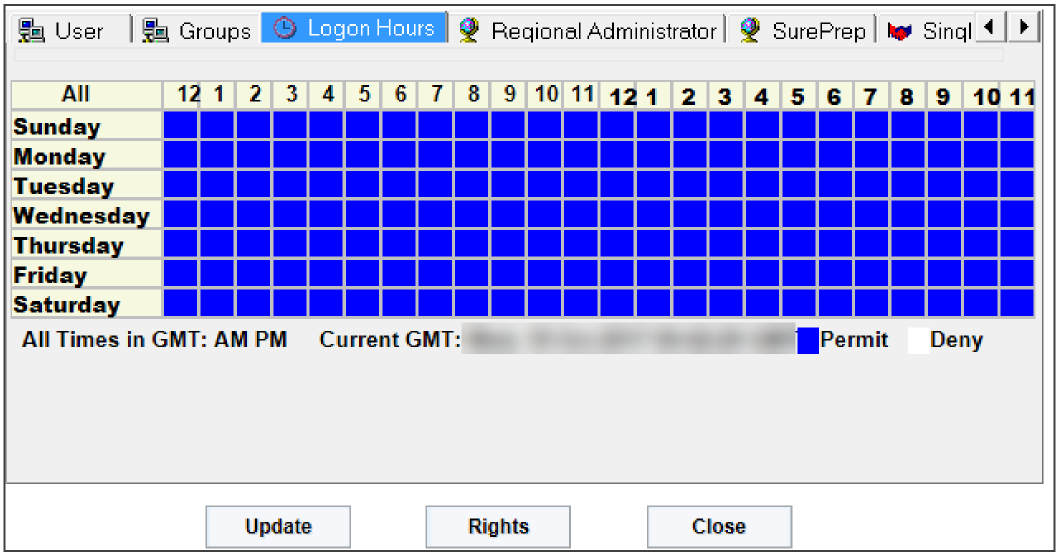


Figure 3:20

This feature could be used if you hire temporaries and you only want them to be able to access the system when they are physically at your office between 8:00 AM and 6:00 PM. All times are tracked in Greenwich Mean Time, so you will need to do some time zone calculation translation when using this feature. Both the top and left borders of the grid act as a toggles for the respective columns and rows. Each of the boxes in the grid can be toggled between **Permit** and **Deny** for that specific hour. Click the word *Sunday* to deny access on Sundays.

Click each of the first 13 columns to deny access from 7:00 PM until 7:59 AM Eastern Standard Time. The screen below shows the appropriate settings to enable access Monday through Friday, from 8:00 AM to 6:00 PM Eastern Standard Time.

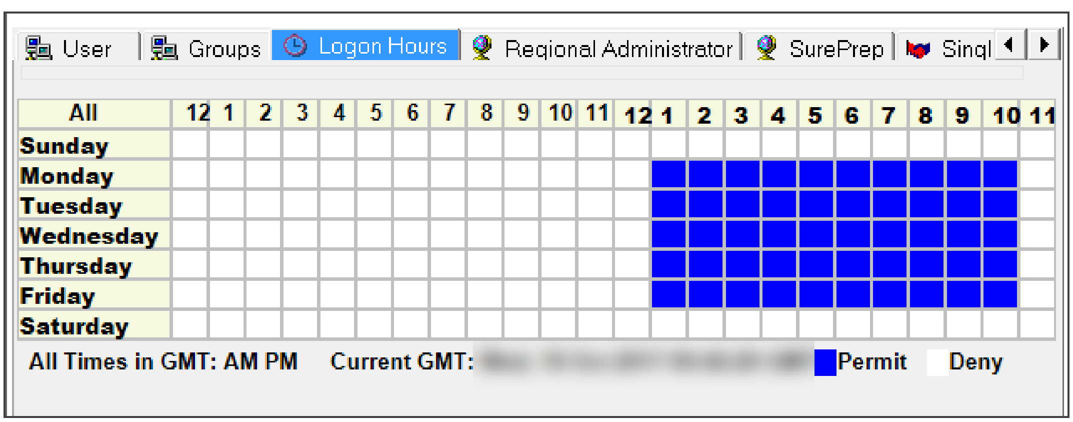


Figure 3:21

Using Limited and Preparer Access

You can restrict what returns a user can see within an account by granting limited or preparer access. If you have several users requiring access to the same set of returns, use *Limited Access*. If you want to grant access to specific returns that a certain user is working with, use *Preparer Access*.

Both of these access methods require:

- an Account to be assigned as either Limited Access or Preparer Access (not Full), and
- a return to be assigned to either a Group or a Preparer.

LIMITED ACCESS

Suppose you create a group called DALLAS_LIMITED in the Dallas location having full access to account 396D and Limited Access to account 396F. Users belonging to group DALLAS_LIMITED can see all returns in account 396F. But members of DALLAS_LIMITED can only see returns if the return(s) in 396D are assigned to DALLAS_LIMITED [DALLAS].

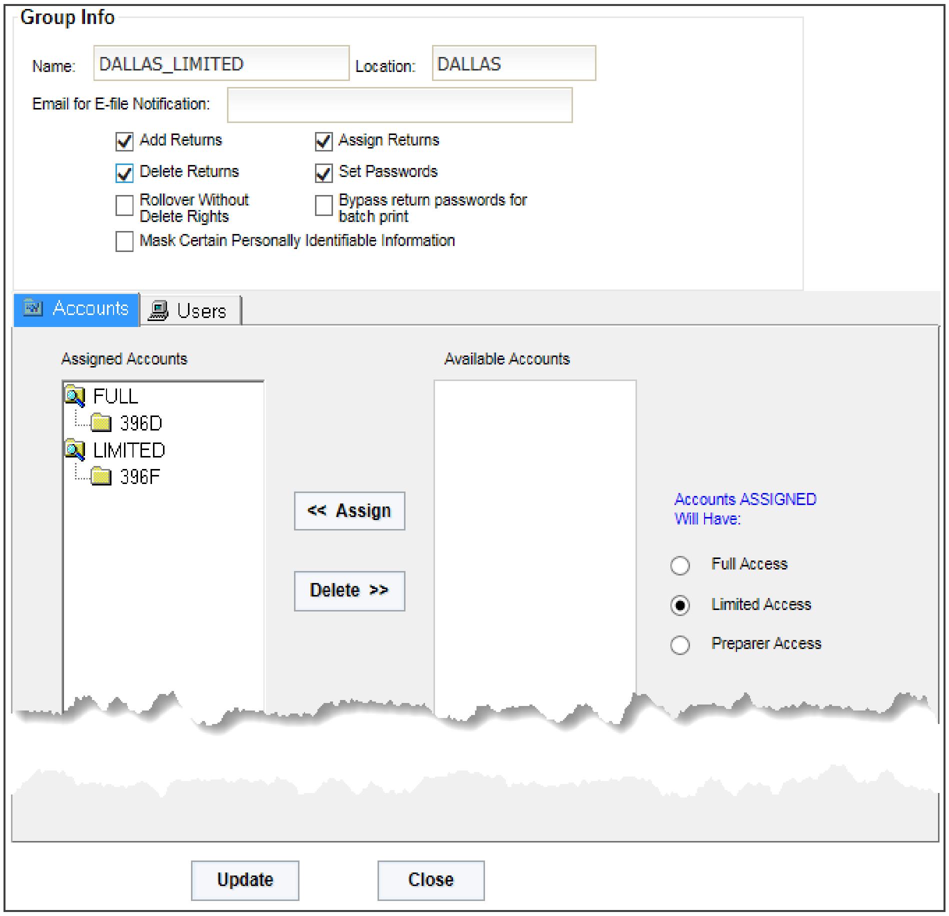


Figure 3:22

PREPARER ACCESS

Preparer Access is similar to *Limited Access*, except that users can only see a return once it is assigned to them.

Although any of the **Group Rights (page 44)** may be granted along with *Limited* or *Preparer* access, greater control over returns would be achieved if only the **Rollover Without Delete Rights** group right is associated with *Limited Access* or *Preparer Access* groups. If the **Add Returns** group right is granted without the Assign Returns group right to a *Limited Access* or *Preparer Access* group, users are able to initially assign any new returns they add, but they would not be able to assign any existing returns that have been assigned to them. If a user forgets to self-assign a return on the **New Return** dialog, someone with **Assign** rights must assign the return to that user.

For example, suppose the group called DALLAS_PREPARER in the Dallas location has *Preparer Access* to account 396D. A user who is a member of this group cannot see any returns in 396D until the returns are assigned to that user by populating the **Assignment Options > Users** tab > **Prepare** field with that user's Location and Login ID as shown below. Click **Add** at the bottom of the **Assignment Options** dialog to move the user's Login ID to the return's **Preparer** column on the left.

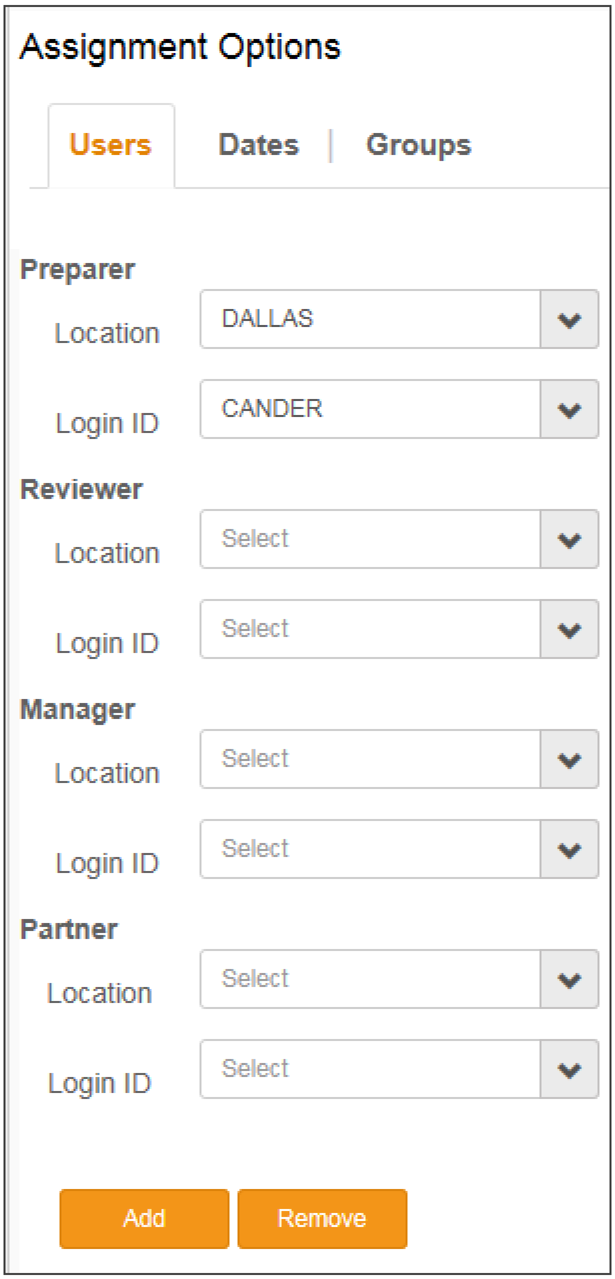


Figure 3:23

As with *Limited access* rights, *Preparer access* is a restricted right. When a user is a member of a *Full* (unrestricted) rights group and a *Limited* (account restricted) group and/or a *Preparer* (locator restricted) group within the same account, the least restricted rights control. In this instance the user will have *Full access* to all locators within the account.

ASSIGNING OWNERS OF TAX DEFAULTS

Within firms having multiple accounts, the firm administrator may need to assign an owner of the tax defaults for each account number of the firm. By creating location administrators, you can designate an owner of the tax defaults for an account to administrators in a given location.

To assign Tax Defaults:

1. Log in as the firm administrator.
2. Select **Admin > Tax Defaults**.
3. The screen shown below appears.

Figure 3:24

4. Firm administrators have an **Assign** button visible on the **Tax Defaults** screen. After selecting the account and year, the firm administrator can assign administrators in the designated location as owners of the tax defaults for account 396D. The following figure shows the assignment screen where you can select the location.

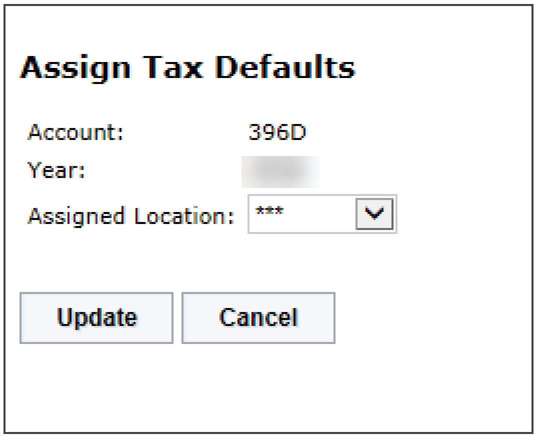


Figure 3:25

This means that any administrator in the selected location can edit tax defaults for account 396D. All returns opened in account 396D will use the 396D tax defaults. No nonadministrator user on account 396D may edit the tax defaults for the account.

This owner designation of the tax defaults for an account gives you control over which administrators can set up and modify your tax defaults.

ASSIGNING RETURNS TO A GROUP OR GROUPS

Administrators or other users with full access to 396D must select a return or returns to begin assigning the DALLAS_LIMITED [DALLAS] group and location. To do so:

1. In **Returns**, find a return or returns to be assigned by placing a check mark next to the return. Select **More > Assign Users/Dates**.

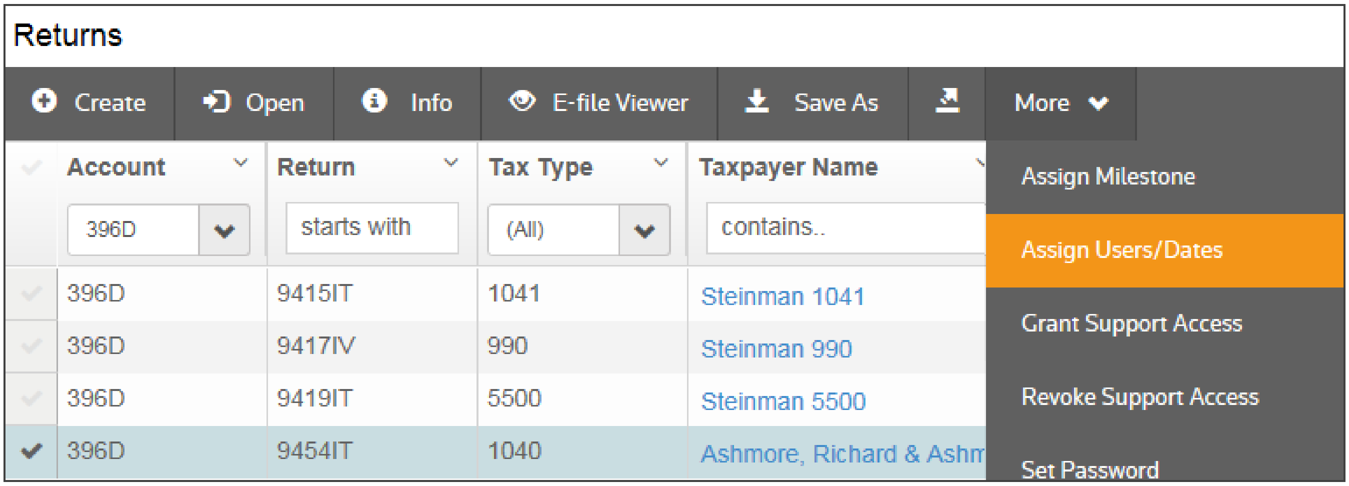


Figure 3:26

2. On the right accordion **Assignment Options** section, select the **Groups** tab. Then select the DALLAS location in the **Locations** drop-down options.

3. Highlight the DALLAS_LIMITED group, and choose **Add**.

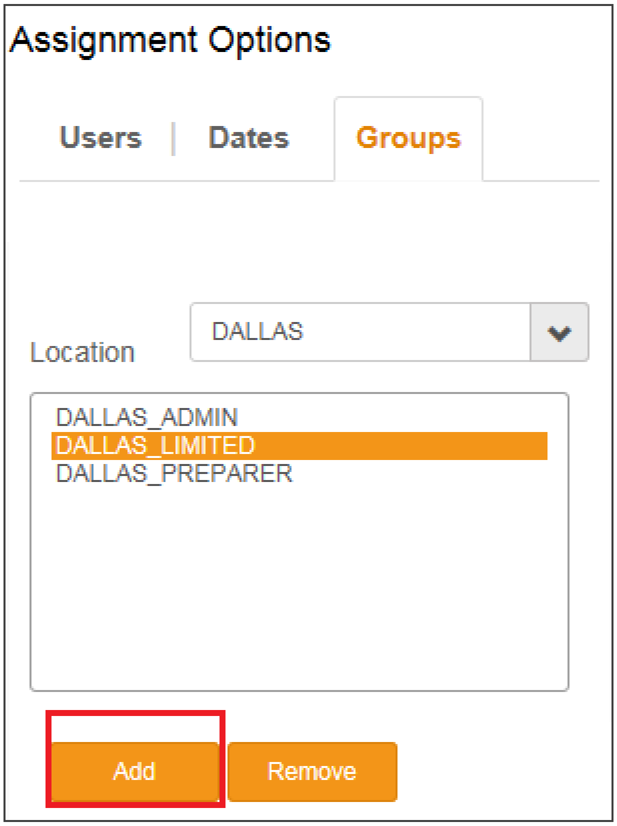


Figure 3:27

4. The **Assigned Group** will show DALLAS_LIMITED. Click **Save Changes**.

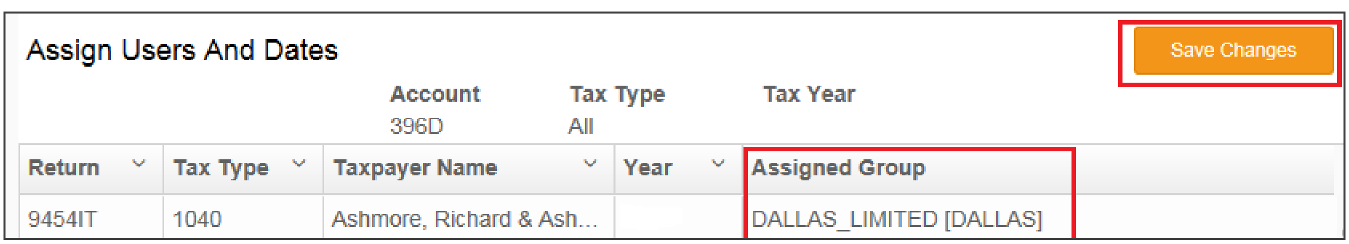


Figure 3:28

5. Click **Returns** in the upper left corner to go back to the **Returns** menu.

6. As each additional return is assigned to DALLAS_LIMITED using this method, all DALLAS_LIMITED group users can see and access these additional returns.

Firms may use *Limited Access* to prevent users from seeing confidential returns, such as partner returns. To do so, all preparers should belong to a group having *Limited Access*. Any new returns created would have to be assigned to the **User Group** when created in order to access those returns.

Assigning Returns to Multiple Group Locations/User Groups

The Administrator now has the ability to assign returns to different group locations and user groups and to display that information from one hyperlink.

- **Assigning Returns to Group Locations (page 66)**
- **Assigning Multiple Returns to a Single Group (page 67)**
- **Assigning Returns to More than One Group/Location (page 69)**
- **Assigning Returns to Users (page 70)**
- **Reviewing Group Locations and User Groups (page 74)**

Assigning Returns to Group Locations

Under **Returns**, select the criteria you wish to use to assign the groups to the correct returns: account, year, tax type, and so forth. Place a check mark beside each return to assign.

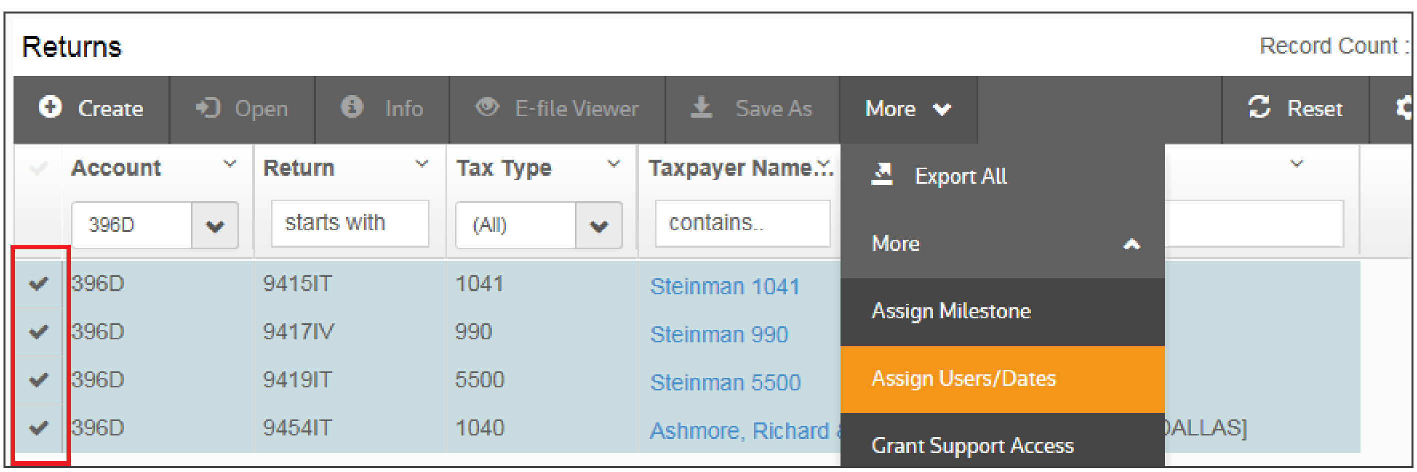


Figure 3:29

Assigning Multiple Returns to a Single Group

After placing check marks beside each return to assign, select **More > Assign Users/Dates**.

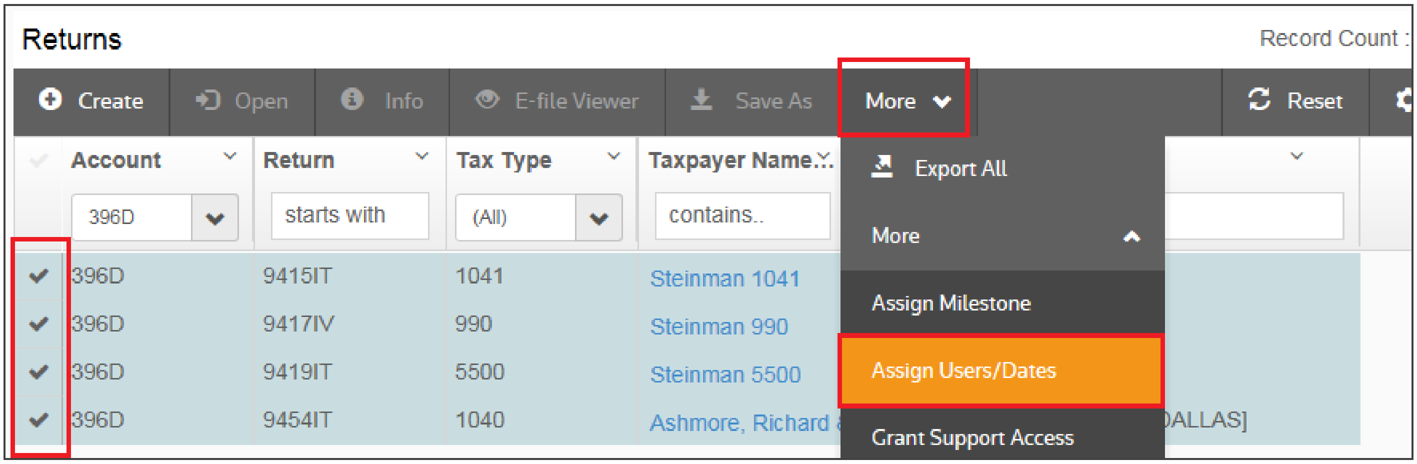


Figure 3:30

The following page appears. Select the **Groups** tab to the right of the screen.

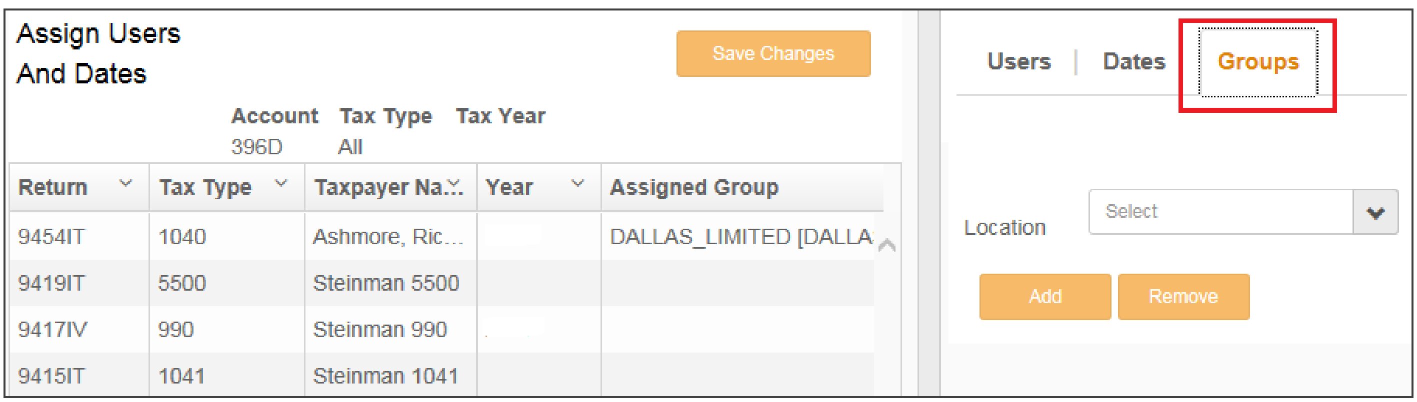


Figure 3:31

Select the **Location** and **Group** to assign to these multiple returns. For this example, we will choose group NEWYORK_PREPARER_NY in Location New York. Choose NEWYORK in the **Location** drop-down list, and highlight NEWYORK_PREPARER_NY group. Then click the **Add** button.

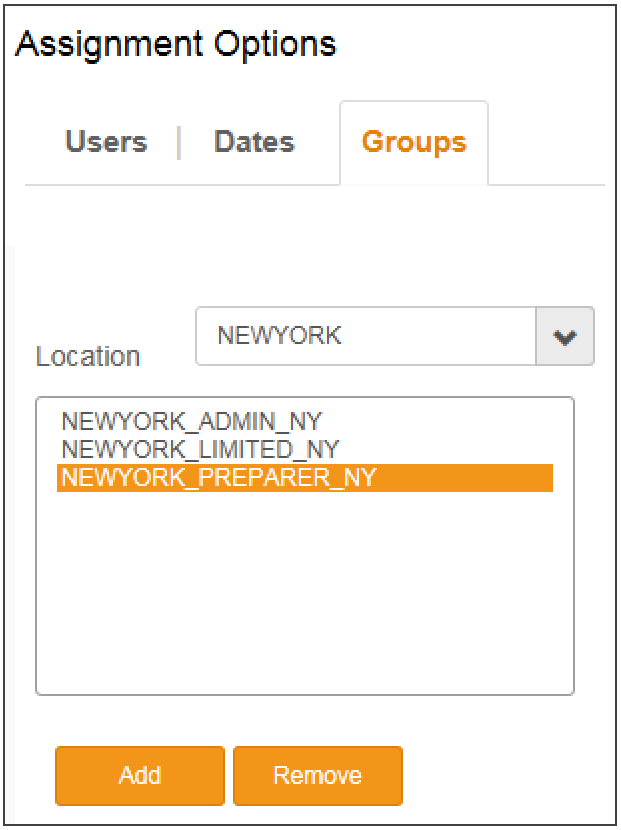


Figure 3:32

The results will appear on the assigned list to the left. Click **Save Changes** in the upper right corner of the **Assign Users and Dates** returns list. When you have completed your options, go back to the **Returns** list page. You can filter your assigned returns by choosing drop-down options in the **Assigned Group** column.

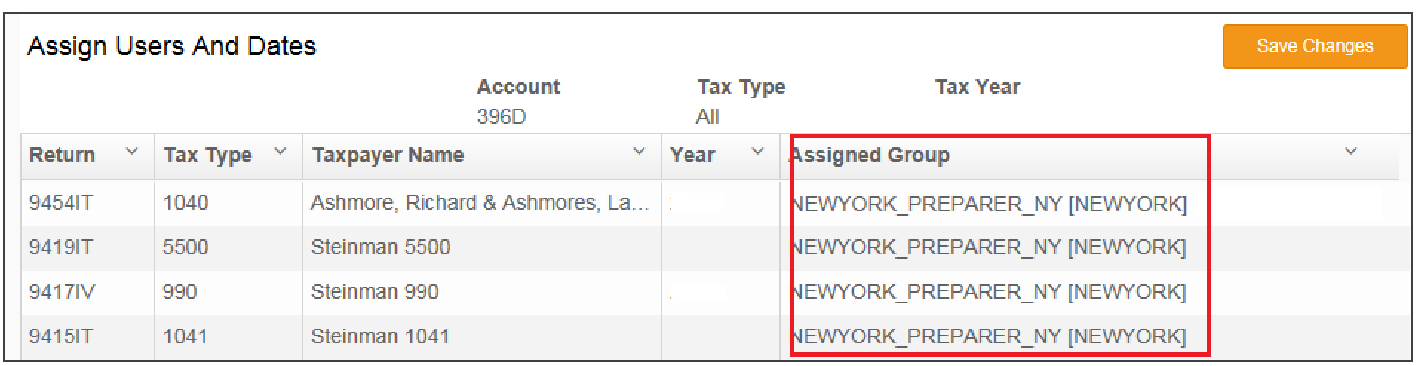


Figure 3:33

Assigning Returns to More than One Group/Location

The process for assigning more than one **Location** to returns is the same as assigning one **Location** to a return.

1. Place a check mark beside the return(s), and go to **More > Assign Users/Dates**.

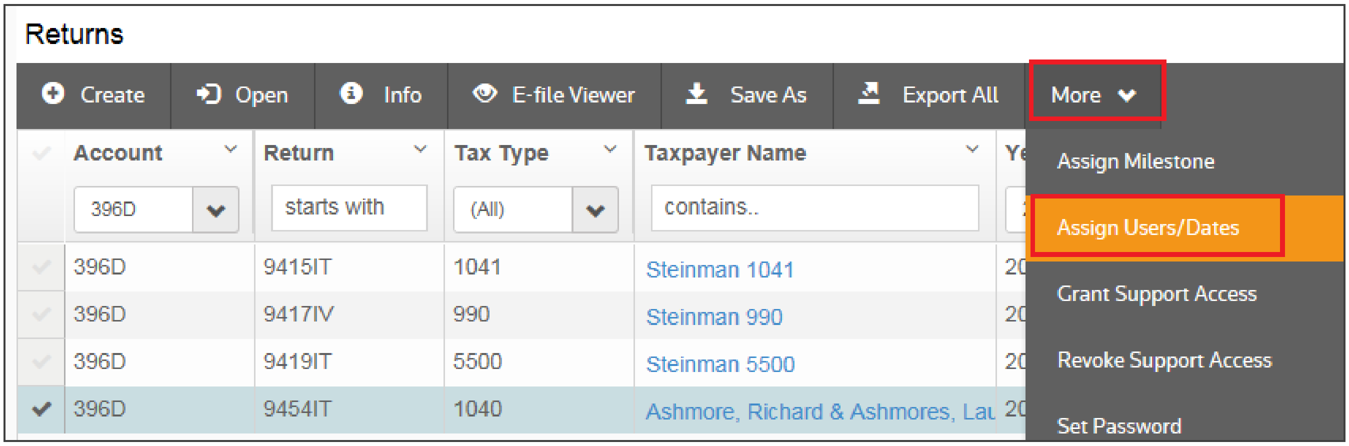


Figure 3:34

2. Go to the **Groups** tab shown in the column on the right side of the screen. Changing your options and clicking **Add** after each selection allows you to assign other **Locations** and **Groups** to the listed returns.

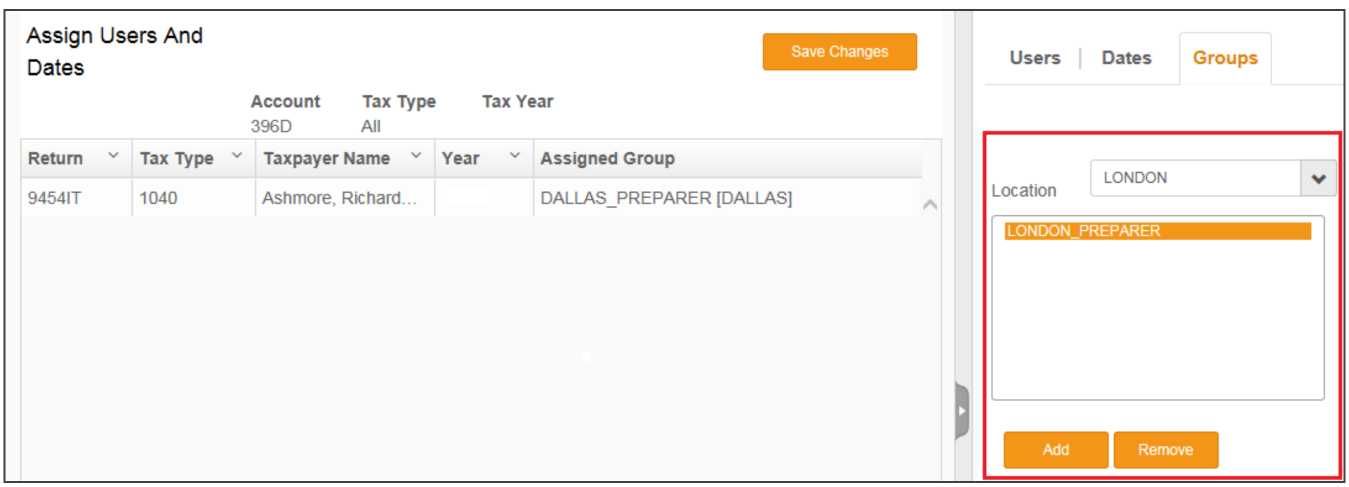


Figure 3:35

Example: Here are the results of the selected 1040 return after adding **Group** LONDON_PREPARER in **Location** LONDON and **Group** DALLAS_PREPARER in **Location** Dallas:

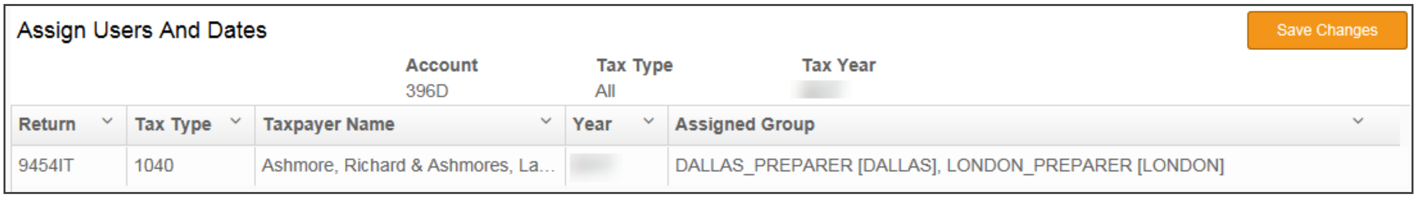


Figure 3:36

Assigning Returns to Users

1. On the **Returns** list page, place a check mark in the left column of the return(s) you wish to be assigned to the same user. Open **More > Assign Users/Dates**.

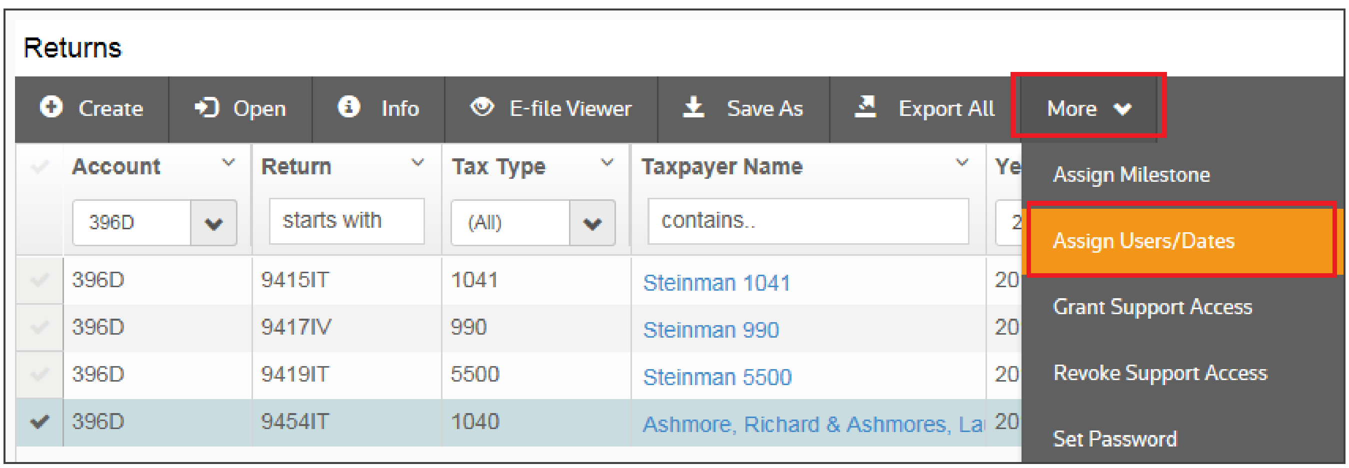


Figure 3:37

2. On the right column of the **Assign Users and Dates** page are the **Assignment Options**. Choose the **Users** tab.

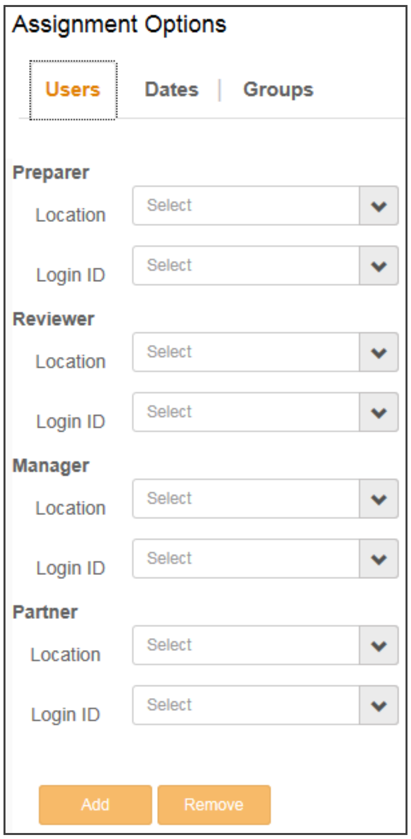


Figure 3:38

3. Open the **Location** and **Login ID** for each assignment you want to make and choose the assigned user from the drop-down list. When you have finished assigning the users to the return(s), click **Add**.

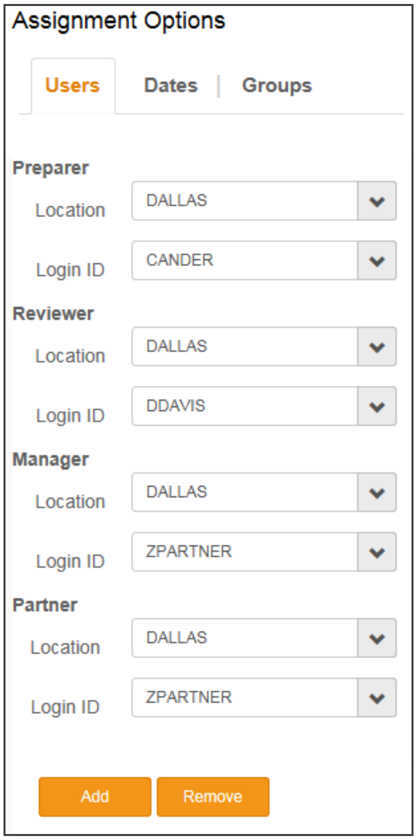


Figure 3:39

4. When the user assignments appear on the left side of the screen, click **Save Changes** and return to the **Returns** list screen.

> In order to see the Preparer, Reviewer, Manager, etc. on the **Returns List** page, you may need to open the **Show/Hide Columns** action item and place check marks in the detail options you want to see on the **Returns List** page. When you have completed your choices, click **Apply**.

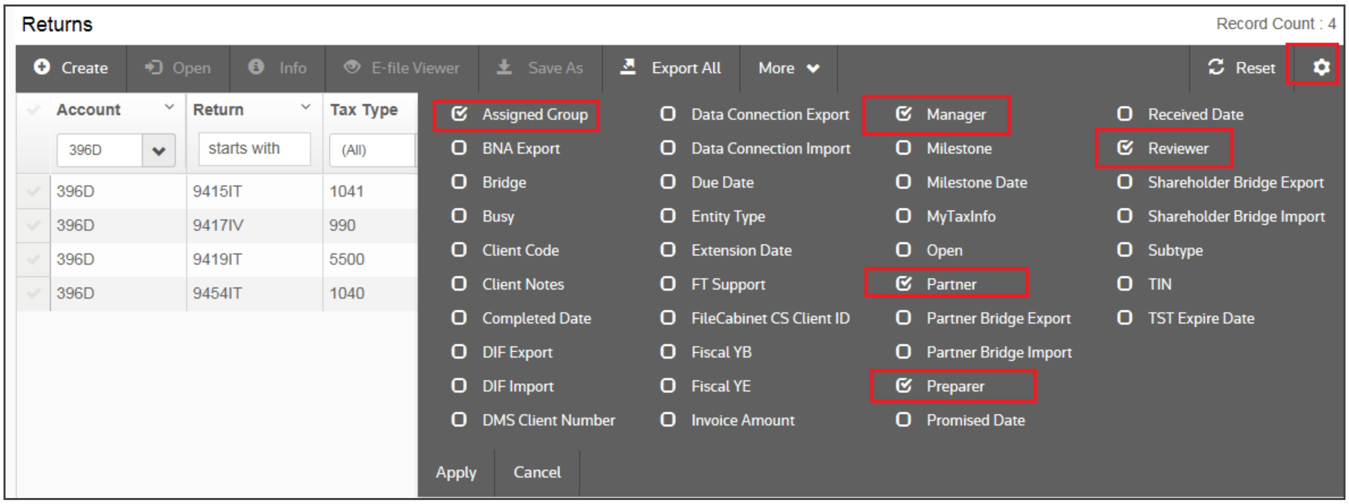


Figure 3:40

Here are the results for the assignment made for preparer, reviewer, manager, and partner.

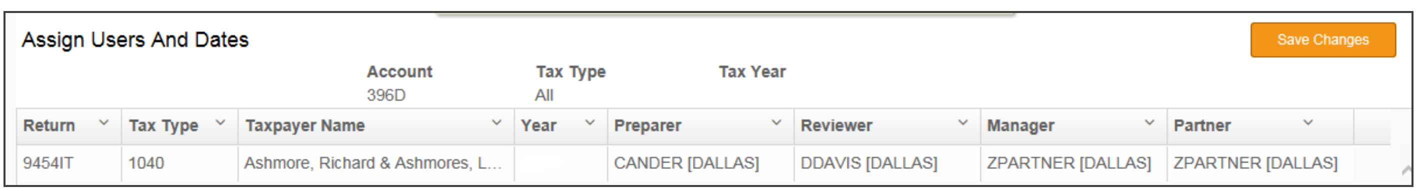


Figure 3:41

Reviewing Group Locations and User Groups

1. Select the return you want to review by checking the box next to the return on the **Returns** screen.
2. Click the **Info** option above the **Returns** list.

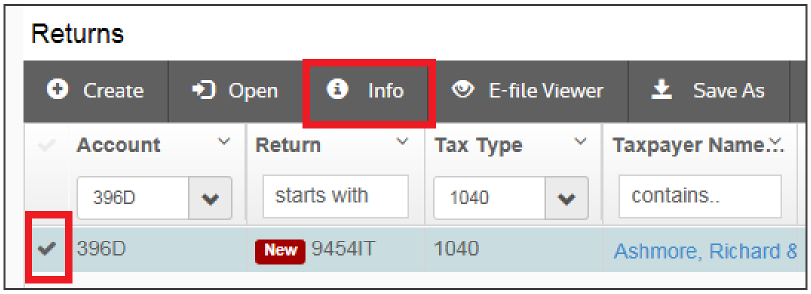
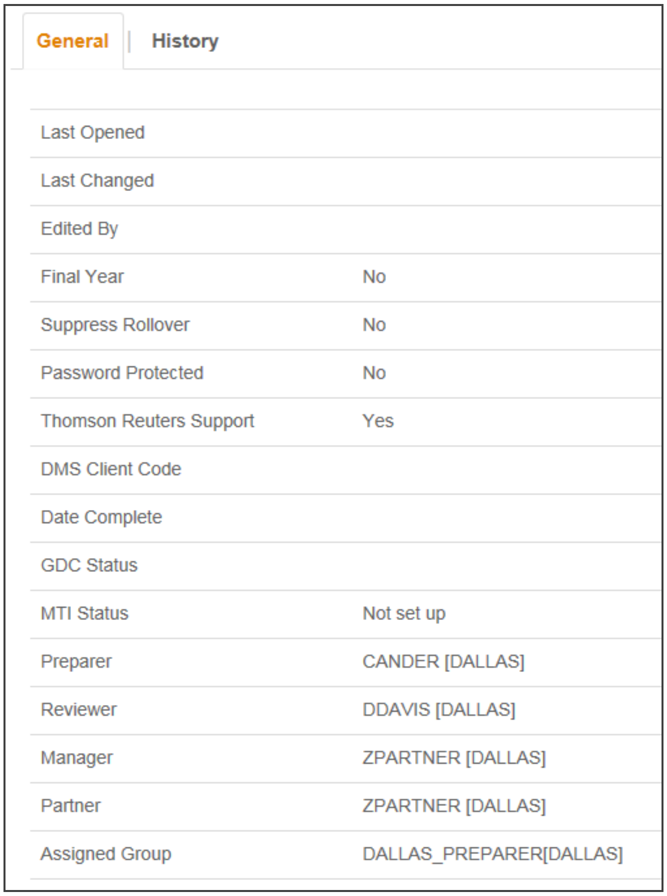


Figure 3:42

3. The information for the selected return will appear along with the user and group assignments on the **General** tab.


General | History

Last Opened	
Last Changed	
Edited By	
Final Year	No
Suppress Rollover	No
Password Protected	No
Thomson Reuters Support	Yes
DMS Client Code	
Date Complete	
GDC Status	
MTI Status	Not set up
Preparer	CANDER [DALLAS]
Reviewer	DDAVIS [DALLAS]
Manager	ZPARTNER [DALLAS]
Partner	ZPARTNER [DALLAS]
Assigned Group	DALLAS_PREPARER[DALLAS]

Figure 3:43

CHAPTER 4: ACCESS CONTROL IMPORTS

Seven (7) different access control imports are available to Administrators who have been granted the **Group Import** right:

- Import New Users (page 77)
- Import New Groups (page 89)
- Import Group Accounts (page 91)
- Import Group - User Assignment (page 93)
- Import Locator - Group Assignments (page 95)
- Disable/Enable Logins (page 97)
- Email Addresses (page 99)

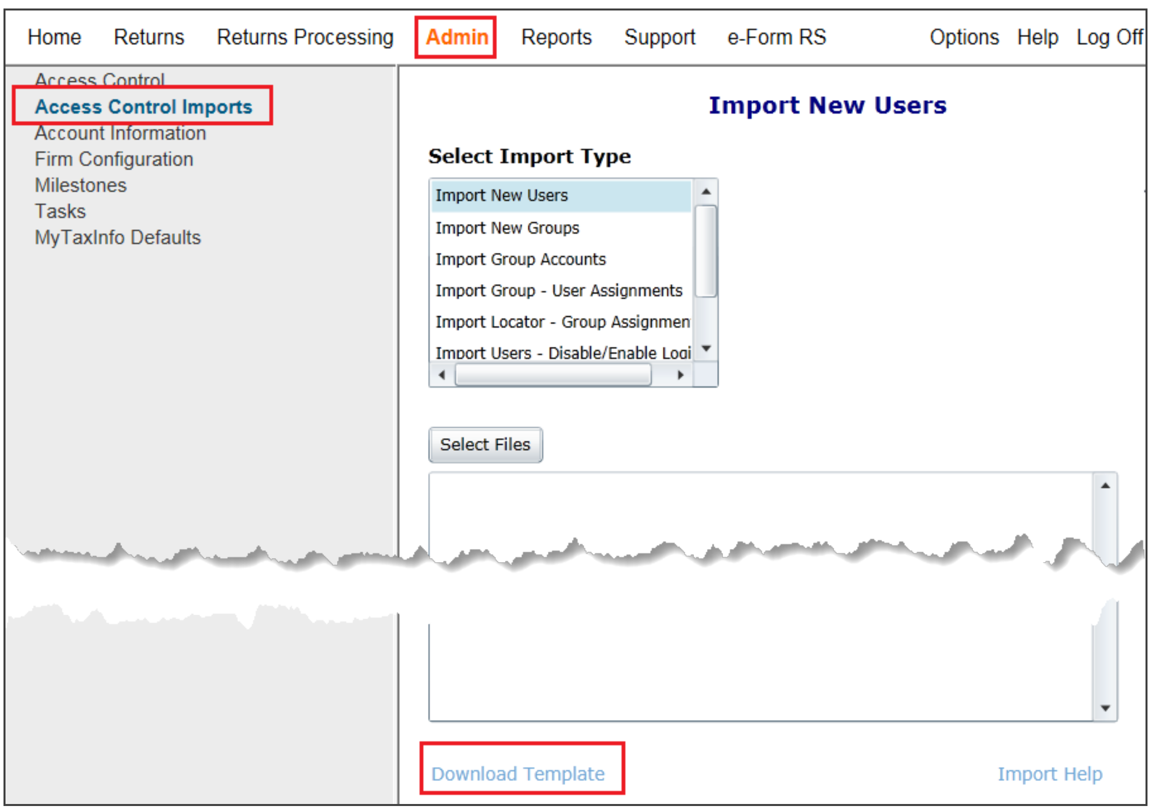


Figure 4:1

For each of these imports, you must create the import file using an Excel worksheet on an XML file (in the case of **Import New Users**).

For all import types except **New Users**, enter the data for each field in a different column (Field Number 1 in Column A, Field Number 2 in Column B, Field Number 3 in Column C, etc.). Save the resulting file as a .csv (column delimited) file prior to import. For numeric account numbers that begin with a leading zero, use a leading apostrophe to format the account number as text.

For all imports except the **Locator – Group Assignment**, placeholders are allowed after the first row for **Group Name** and **Group Location**. Fill in **Group Name** in Column A and **Group Location** in Column B on the first row, then leave Columns A and B blank on subsequent rows until a different **Group Name** or **Group Location** is desired. For the **Locator – Group Assignment** imports, each row or record in the import file must contain all five of the fields specified in the data format.

IMPORT NEW USERS

Downloading the XML Template Example/Creating a New XML Template

The format for importing new users into **Admin > Access Control Imports > Import New Users** is through an XML template.

You can download the **Import New Users** XML templates using the **Download Template** link at the bottom of the **Import New Users** screen in the **Access Control Imports** menu (see the link circled in **red** below).

CSV template downloads are here also for the other **Access Control Import Types**.

To download and create the XML templates, do the following steps:

1. Click the **Download Template** hyperlink.
2. When prompted, enter a name for your XML file.
3. Make sure the file type is still *XML*
4. Click **Save**. Make sure the drive and path is where you want your import XML template to go.

After you save the downloaded template, you can edit your template.

Editing the Template Example

To edit the import information in your XML file, you will need to change the XML template into an editable format. To do this, go to the drive and path where you saved and renamed the XML, and right-click the XML name. Select **Edit**.

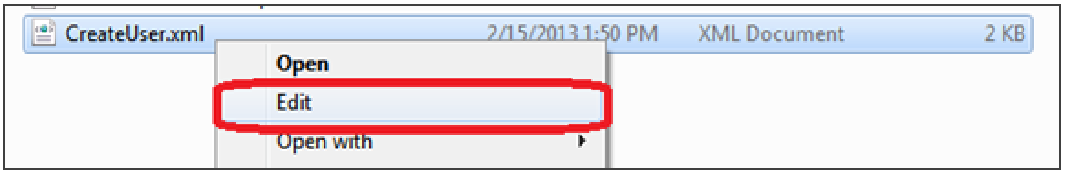


Figure 4:2

By default, the file opens in Notepad. If you select another TXT format, open the XML using the **Open With** option.

```
<?xml version="1.0"?>

<GoSystemRS>
        <NewUser>
                <Firm><![CDATA[Name here2]]></Firm>
                <LoginID><![CDATA[Name here2]]></LoginID>
                <Location><![CDATA[Name here2]]></Location>
                <FullName>
                        <![CDATA[Name here2]]>
                </FullName>
                <Email>
                        <![CDATA[Name here3]]>
                </Email>
                <Password>
                        <![CDATA[Name here4]]>
                </Password>
                <EmployeeID></EmployeeID>
                <UserRights>
                        <FormSource></FormSource>
                        <EFormRS></EFormRS>
                        <RSTOGO></RSTOGO>
                        <TaxInfoAdmin></TaxInfoAdmin>
                        <TaxInfoUserFull></TaxInfoUserFull>
                        <TaxInfoUserReadOnly></TaxInfoUserReadOnly>
                        <ElfAdmin></ElfAdmin>
      <ElfUnlock></ElfUnlock>
                        <PriorYear></PriorYear>
                        <TEQ></TEQ>
                        <RemoveCompletedDate></RemoveCompletedDate>
                </UserRights>
                <IsAdmin></IsAdmin>
                <AdminRights>
                        <AddGroups></AddGroups>
                        <EditGroups></EditGroups>
                        <DeleteGroups></DeleteGroups>
                        <FirmConfig></FirmConfig>
                        <AddUser></AddUser>
                        <EditUser></EditUser>
```

Figure 4:3

When the XML import template opens in a TXT format, it will display the information ready to be edited.

Editing the Template Attributes

Below are the variables that you can edit based upon each user's ID options, information, rights and assignment requirements, etc.

The specific variables with descriptions that can be edited are highlighted in **bold** below.

```
<?xml version="1.0"?>
  <GoSystemRS>
    <NewUser>
      <Firm><![CDATA[Firm Name]]></Firm>
      <LoginID><![CDATA[User Login ID]]></LoginID>
      <Location><![CDATA[Location]]></Location>
      <FullName><![CDATA[User's Full Name]]></FullName>
      <Email><![CDATA[User email address]]></Email>
      <Password><![CDATA[Login Password]]></Password>
      <EmployeeID>User's Employee ID</EmployeeID>
      <UserRights>
        <FormSource>Y or N</FormSource>
        <EFormRS>Y or N</EFormRS>
        <TaxInfoAdmin>Y or N</TaxInfoAdmin>
        <TaxInfoUserFull>Y or N</TaxInfoUserFull>
        <TaxInfoUserReadOnly>Y or N</TaxInfoUserReadOnly>
        <ElfAdmin>Y or N</ElfAdmin>
          <ElfUnlock>Y or N</ElfUnlock>
        <PriorYear>Y or N</PriorYear>
        <TEQ>Y or N</TEQ>
```

```
  <RemoveCompletedDate>Y or N</RemoveCompletedDate>
</UserRights>
<IsAdmin>Y or N</IsAdmin>
<AdminRights>
     <AddGroups>Y or N</AddGroups>
     <EditGroups>Y or N</EditGroups>
     <DeleteGroups>Y or N</DeleteGroups>
     <FirmConfig>Y or N</FirmConfig>
     <AddUser>Y or N</AddUser>
     <EditUser>Y or N</EditUser>
     <DeleteUser>Y or N</DeleteUser>
     <Transfer>Y or N</Transfer>
     <CreateAdmin>Y or N</CreateAdmin>
     <GroupImport>Y or N</GroupImport>
     <FreeReturns>Y or N</FreeReturns>
     <Defederate>Y or N</Defederate>
</AdminRights>
<Groups>
  <GroupCenter>
     <Name><![CDATA[Location]]></Name>
     <AssignedGroups>
        <GroupName><![CDATA[Group Name]]><GroupName>
     </AssignedGroups>
  </GroupCenter>
```

```
        </Groups>
    </NewUser>
</GoSystemRS>
```

Here is an example of a completed TXT template ready to be saved as an XML for import (with the attributes **bolded** for demonstration purposes only).

```
<?xml version="1.0"?>
    <GoSystemRS>
        <NewUser>
            <Firm><![CDATA[2WF5]]></Firm>
            <LoginID><![CDATA[Heresme]]></LoginID>
            <Location><![CDATA[Dallas]]></Location>
            <FullName><![CDATA[Here's Me]]></FullName>
            <Email><![CDATA[me@email.com]]></Email>
            <Password><![CDATA[123456]]></Password>
            <EmployeeID>D123456</EmployeeID>
            <UserRights>
                <FormSource>Y</FormSource>
                <EFormRS>Y</EFormRS>
                <TaxInfoAdmin>Y</TaxInfoAdmin>
                <TaxInfoUserFull>Y</TaxInfoUserFull>
                <TaxInfoUserReadOnly>Y</TaxInfoUserReadOnly>
                <ElfAdmin>Y</ElfAdmin>
                    <ElfUnlock>Y</ElfUnlock>
                <PriorYear>Y</PriorYear>
                <TEQ>Y</TEQ>
```

```
    <RemoveCompletedDate>Y</RemoveCompletedDate>
</UserRights>
<IsAdmin>Y</IsAdmin>
<AdminRights>
    <AddGroups>Y</AddGroups>
    <EditGroups>Y</EditGroups>
    <DeleteGroups>Y</DeleteGroups>
    <FirmConfig>Y</FirmConfig>
    <AddUser>Y</AddUser>
    <EditUser>Y</EditUser>
    <DeleteUser>Y</DeleteUser>
    <Transfer>Y</Transfer>
    <CreateAdmin>Y</CreateAdmin>
    <GroupImport>Y</GroupImport>
    <FreeReturns>Y</FreeReturns>
    <Defederate>Y</Defederate>
</AdminRights>
<Groups>
    <GroupCenter>
        <Name><![CDATA[Dallas]]></Name>
        <AssignedGroups>
            <GroupName><![CDATA[Dallas1]]></GroupName>
        </AssignedGroups>
    </GroupCenter>
```

```
    </Groups>
  </NewUser>
</GoSystemRS>
```

You can now import more than one new user at a time through XML import. To do this within the TXT template, copy and paste the initial user's information (from the beginning `New User` tag to the ending `New User` tag) and edit each of the subsequent users information based on each user's profile.

Saving the TXT Template to the XML Format

Once your TXT template is correct for the user(s) you want to import, you will need to save the template to an XML file. To do this, do the following:

1. Right-click the TXT document and choose **File > Save As**.
2. Make sure the drive and path point to the correct location where you want the XML template saved.
3. Give the file a name followed by the .XML extension.
4. In the **Save as Type** drop-down option field, choose *All Files (*.*)*.
5. Click **Save**.

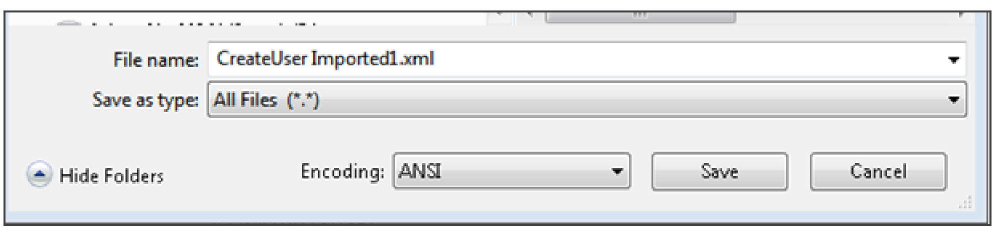


Figure 4:4

6. To verify that the template has been saved as an XML file ready for importing, right-click the XML file you just saved and select **Open**.

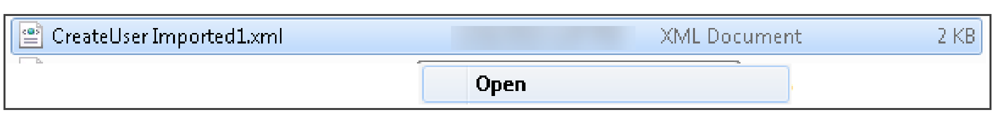


Figure 4:5

7. An XML document will display with the same data as in the TXT form.


```
<?xml version="1.0"?>
<GoSystemRS>
 - <NewUser>
   - <Firm>
       <![CDATA[2WF5]]>
     </Firm>
   - <LoginID>
       <![CDATA[Heresme]]>
     </LoginID>
   - <Location>
       <![CDATA[Dallas]]>
     </Location>
   - <FullName>
       <![CDATA[Here's Me]]>
     </FullName>
   - <Email>
       <![CDATA[me@email.com]]>
     </Email>
   - <Password>
       <![CDATA[123456]]>
     </Password>
     <EmployeeID>D123456</EmployeeID>
   - <UserRights>
```


Figure 4:6

Importing into Users into Admin > Access Control Imports

1. Select **Admin > Access Control Imports**.
2. Highlight **Import New Users**.

3. In the **Select Files** option, find the XML for the user you want to create.

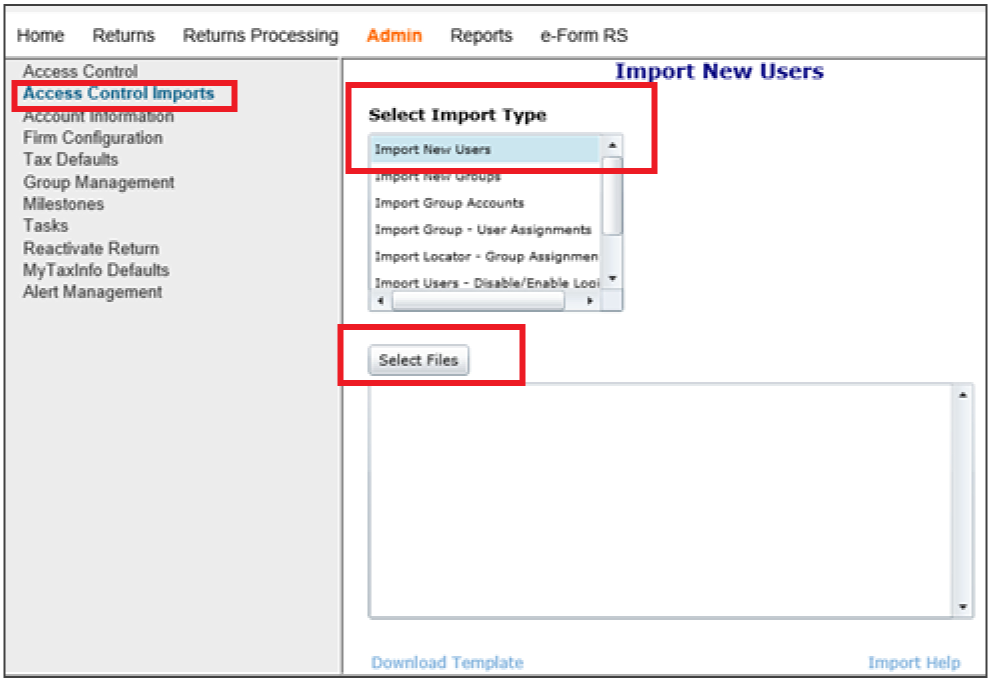


Figure 4:7

4. Populate the **File Name** field, ***making sure that the file type is XML (*.xml)***.

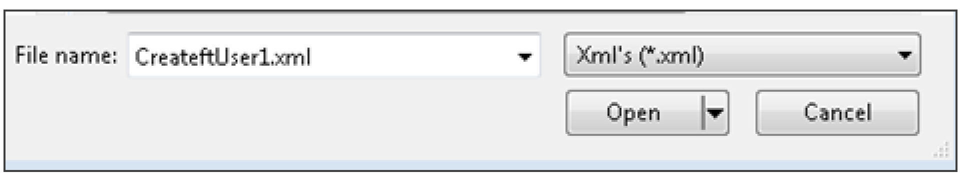


Figure 4:8

5. Select **Open**.

6. Your XML template will appear in the **Import New User Select Files** dialog.

7. When the correct import template appears in the import dialog, select **Import**.

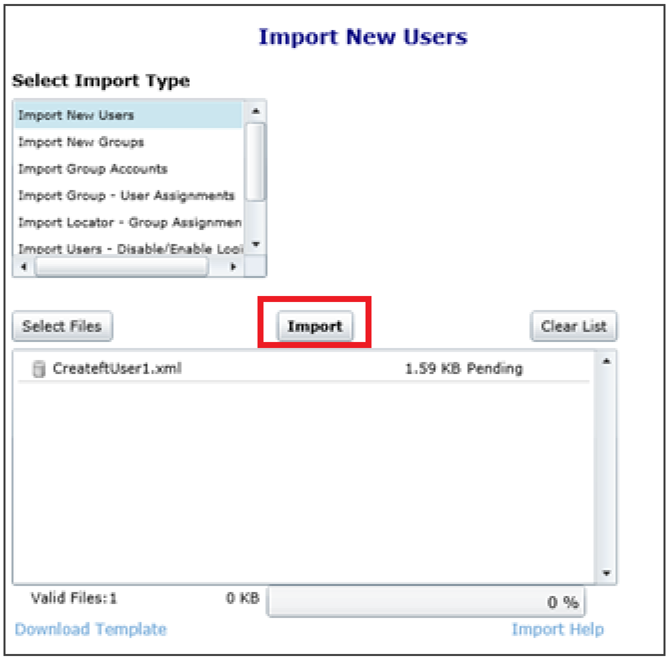


Figure 4:9

8. If the template is correct, the following message will appear:

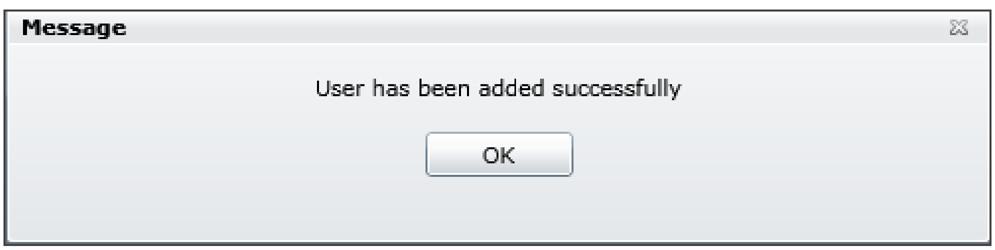


Figure 4:10

9. Below are the results of the XML import using the information for user *Here's Me*:

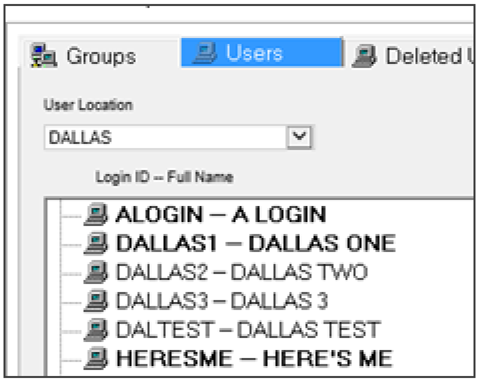


Figure 4:11

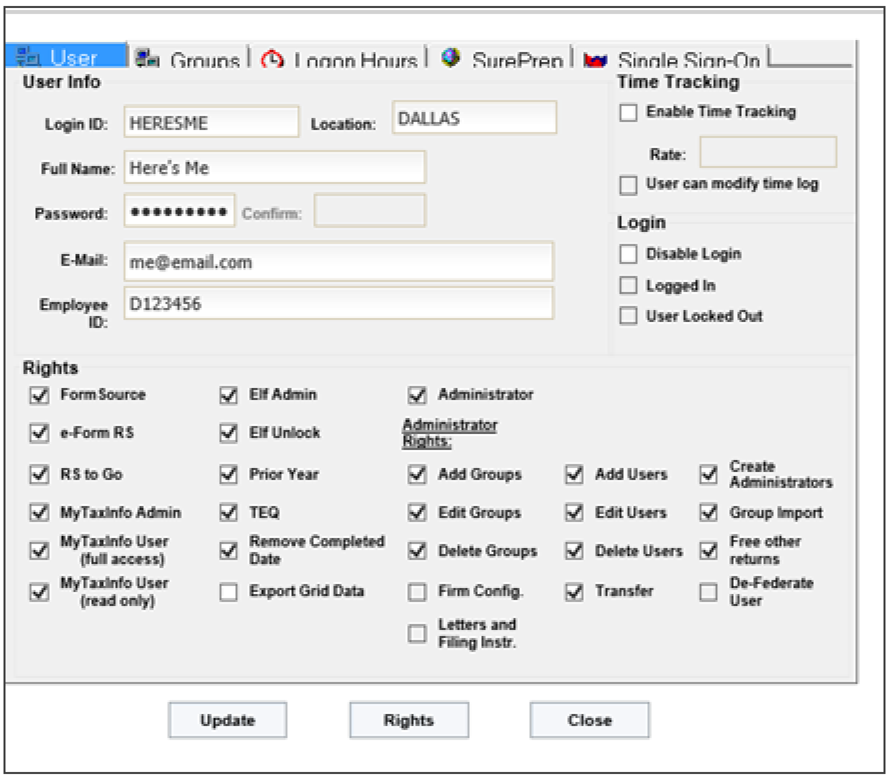


Figure 4:12

10. Below are the results on the **Groups** tab for the *Here's Me* user:

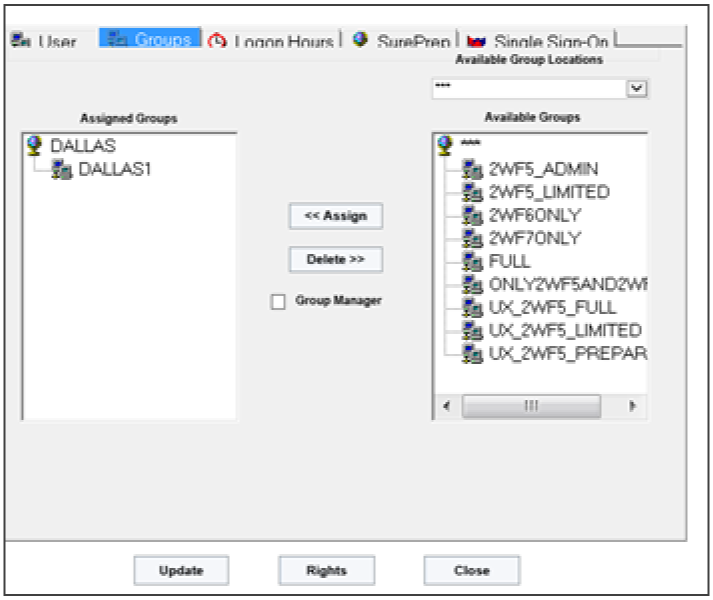


Figure 4:13

IF ERRORS OCCUR...

If you need to correct your template, error messages generated during the import process will give you information about the necessary changes to your XML file.

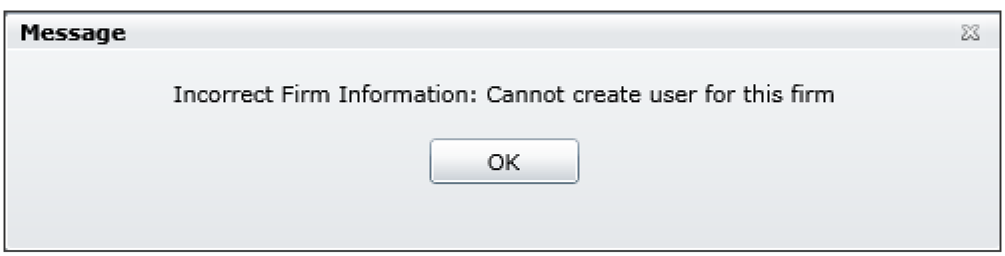


Figure 4:14

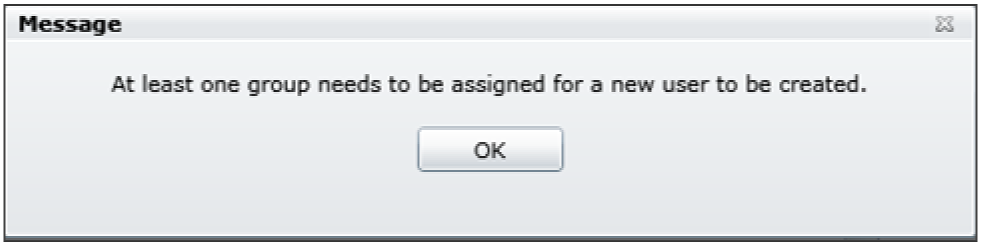


Figure 4:15

To correct the errors, follow the same steps as above:

1. Open the XML file.
2. Edit the TXT file.
3. Save as an XML file.
4. Import the XML file again.

IMPORT NEW GROUPS

1. Log on as the Administrator.
2. Select **Admin > Access Control Imports**.
3. Highlight the **Import New Groups** option, and click the **Select Files** button.
4. Specify the location on your workstation or network in which the Excel .csv import file for new groups resides.
5. Select the correct location where the .csv import file resides. Only files with the filename extension ".csv", which typically designates a comma-delimited file, are allowed for **Access Control Import**.
6. When the correct file and location are selected, click the **Open** button on the **Browse for Folder** dialog. The **Browse for Folder** dialog is immediately closed, and the file in the selected folder with a filename extension of ".csv" appears in the file **Upload** dialog.
7. To start the import of the selected file, click the **Upload** button. To cancel the import, click the **Clear List** button.

8. The data from the selected file is imported into **Access Control** in a single operation which does not require your intervention. When the import is complete, the **New Group Import** results appear, and the data from the import file and the import status of each record appear.

9. Click the **Continue** button to end the import process and return to the **Access Control Imports** screen.

Import New Groups Format

The following table shows the data fields for the new groups import file. Each data field must be followed by a comma except the last data field in the record (row). Each record must be followed by a carriage return.

FIELD #	CONTENTS	EXPLANATION
1	Group name	Group name, alphanumeric and spaces, maximum 20 characters
2	Group Location	Group Location, alphanumeric and spaces, maximum 20 characters
3	Account	4-character alphanumeric code assigned by Thomson Reuters
4	Access Type	Three valid values: Full, Limited, or Preparer. See **Using Limited and Preparer Access (page 59)** for more information.
5	Add Returns	Two valid values: 1 to grant group this right, or 0 to deny this right. See **Group Rights (page 44)** for more information.
6	Delete Returns	Two valid values: 1 to grant group this right, or 0 to deny this right. See **Group Rights (page 44)** for more information.
7	Assign Returns	Two valid values: 1 to grant group this right, or 0 to deny this right. See **Group Rights (page 44)** for more information.
8	Set Passwords	Two valid values: 1 to grant group this right, or 0 to deny this right. See **Group Rights (page 44)** for more information.
9	Rollover without Delete	Two valid values: 1 to grant group this right, or 0 to deny this right. See **Group Rights (page 44)** for more information.

Import New Groups Data Examples

The following is an example of a record containing one assigned account; data fields are explained in the preceding table:

```
New York_Admin,New York,B216,Full,1,1,1,1,1
```

A	B	C	D	E	F	G	H	I	J
New York_Admin	New York	B216	Full	1	1	1	1	1	

Figure 4:16

The following is an example of records containing multiple assigned accounts to the same Group and Location with the same group rights; data fields are explained in the preceding table:

```
NY_Preparers,New York,B216,Full,1,1,1,1,1

NY_Preparers,New York,B202,Limited, , , , ,

NY_Preparers,New York,B160,Preparer, , , , ,

LA_Preparers,Los Angeles,B202,Full,1,1,1,1,1

LA_Preparers,Los Angeles,B160,Limited, , , , ,

LA_Preparers,Los Angeles,B216,Preparer, , , , ,
```

A	B	C	D	E	F	G	H	I	J
NY_Preparers	New York	B216	Full	1	1	1	1	1	
NY_Preparers	New York	B202	Limited	0	0	0	0	0	
NY_Preparers	New York	B160	Preparer	0	0	0	0	0	
LA_Preparers	Los AngelesB	B202	Full	1	1	1	1	1	
LA_Preparers	Los AngelesB	B160	Limited	0	0	0	0	0	
LA_Preparers	Los AngelesB	B216	Preparer	0	0	0	0	0	

Figure 4:17

IMPORT GROUP ACCOUNTS

1. Log on as the Administrator.
2. Select **Admin > Access Control Imports**.
3. Highlight the **Import Group Accounts** option, and click the **Select Files** button.
4. Specify the location on your workstation or network in which the Excel .csv import file for new groups resides.

5. Select the correct location where the .csv import file resides. Only files with the filename extension ".csv", which typically designates a comma-delimited file, are allowed for **Access Control Import**.

6. When the correct file and location are selected, click the **Open** button on the **Browse for Folder** dialog. The **Browse for Folder** dialog is immediately closed, and the file in the selected folder with a filename extension of ".csv" appears in the file **Upload** dialog.

7. To start the import of the selected file, click the **Upload** button. To cancel the import, click the **Clear List** button.

8. The data from the selected file is imported into **Access Control** in a single operation which does not require your intervention. When the import is complete, the **Group Accounts Import** results appear, and the data from the import file and the import status of each record appear.

9. Click the **Continue** button to end the import process and return to the **Access Control Imports** screen.

Import Group Accounts Data Format

The following table shows the data fields for the group accounts import file. Each data field must be followed by a comma except the last data field in the record (row). Each record must be followed by a carriage return.

FIELD #	CONTENTS	EXPLANATION
1	Group name	Group name, alphanumeric and spaces, maximum 20 characters
2	Group Location	Group Location, alphanumeric and spaces, maximum 20 characters
3	Account	4-character alphanumeric code assigned by Thomson Reuters
4	Access Type	Three valid values: Full, Limited, or Preparer. See **Using Limited and Preparer Access (page 59)** for more information.

Import Group Account Data Examples

Following is an example of a record containing one account assignment to a group; data fields are explained in the preceding table:

```
Dallas_Admin,Dallas,B160,Full
```

A	B	C	D	E
Dallas_Admin	Dallas	B160	Full	

Figure 4:18

Following is an example of records containing multiple account assignment to the same group; data fields are explained in the preceding table:

```
LA_Staff,Los Angeles,B202,Full

LA_Staff,Los Angeles,B160,Limited

LA_Staff,Los Angeles,B216,Preparer
```

	A	B	C	D	E
1	LA_Staff	Los Angele	B202	Full	
2	LA_Staff	Los Angele	B160	LIMITED	
3	LA_Staff	Los Angele	B216	preparer	

Figure 4:19

IMPORT GROUP - USER ASSIGNMENT

1. Log on as the Administrator.
2. Select **Admin > Access Control Imports**.
3. Highlight the **Import Group - User Assignments** option, and click the **Select Files** button.
4. Specify the location on your workstation or network in which the Excel .csv import file for new groups resides.
5. Select the correct location where the .csv import file resides. Only files with the filename extension ".csv", which typically designates a comma-delimited file, are allowed for **Access Control Import**.
6. When the correct file and location are selected, click the **Open** button on the **Browse for Folder** dialog. The **Browse for Folder** dialog is immediately closed, and the file in the selected folder with a filename extension of ".csv" appears in the file **Upload** dialog.
7. To start the import of the selected file, click the **Upload** button. To cancel the import, click the **Clear List** button.

8. The data from the selected file is imported into **Access Control** in a single operation which does not require your intervention. When the import is complete, the **Group - User Assignments Import** results appear, and the data from the import file and the import status of each record appear.

9. Click the **Continue** button to end the import process and return to the **Access Control Imports** screen.

Import Group - User Assignment Data Format

The following table shows the data fields for the group user assignments import file. Each data field must be followed by a comma except the last data field in the record (row). Each record must be followed by a carriage return.

FIELD #	CONTENTS	EXPLANATION
1	Group name	Group name, alphanumeric and spaces, maximum 20 characters
2	Group Location	Group Location, alphanumeric and spaces, maximum 20 characters
3	User Login ID	User Login ID
4	User Location	User Location, alphanumeric and spaces, maximum 20 characters

Import Group - User Assignment Data Examples

Following is an example of a record containing one user membership to a Group; data fields are explained in the preceding table:

```
Dallas_Admin,Dallas,JDOE,Dallas
```

A	B	C	D	E
Dallas_Admin	Dallas	JDOE	Dallas	

Figure 4:20

Following is an example of records containing multiple user memberships to a Group; data fields are explained in the preceding table:

```
LA_Preparers,Los Angeles,MSmith,Los Angeles

New York_Preparers,New York,SJones,New York

Dallas_Preparers,Dallas,RGreen,Dallas
```

A	B	C	D	E
LA_Preparers	Los Angele	MSmith	Los Angeles	
New York_Preparers	New York	SJones	New York	
Dallas_Preparers	Dallas	RGreen	Dallas	

Figure 4:21

IMPORT LOCATOR - GROUP ASSIGNMENTS

1. Log on as the Administrator.
2. Select **Admin > Access Control Imports**.
3. Highlight the **Import Locator - Group Assignments** option, and click the **Select Files** button.
4. Specify the location on your workstation or network in which the Excel .csv import file for new groups resides.
5. Select the correct location where the .csv import file resides. Only files with the filename extension ".csv", which typically designates a comma-delimited file, are allowed for **Access Control Import**.
6. When the correct file and location are selected, click the **Open** button on the **Browse for Folder** dialog. The **Browse for Folder** dialog is immediately closed, and the file in the selected folder with a filename extension of ".csv" appears in the file **Upload** dialog.
7. To start the import of the selected file, click the **Upload** button. To cancel the import, click the **Clear List** button.
8. The data from the selected file is imported into **Access Control** in a single operation which does not require your intervention. When the import is complete, the **Import Locator - User Assignments** results appear, and the data from the import file and the import status of each record appear.
9. Click the **Continue** button to end the import process and return to the **Access Control Imports** screen.

Import Locator - Group Assignment Data Format

The following table shows the data fields for the locator group assignments import file. Each data field must be followed by a comma except the last data field in the record (row). Each record must be followed by a carriage return.

FIELD #	CONTENTS	EXPLANATION
1	Account	4-character alphanumeric code assigned by Thomson Reuters
2	Tax return locator code	6-character alphanumeric code used by Thomson Reuters to identify a tax return
3	Tax return type	Valid values include 1120, 1065, 1040, 1041, 5500, 990, 709, and 706
4	Group name	Group name, alphanumeric and spaces, maximum 20 characters
5	Group Location	Group Location, alphanumeric and spaces, maximum 20 characters

Import Locator - Group Assignment Data Examples

Following is an example of a record containing one locator assignment to a Group; data fields are explained in the preceding table:

```
B160,12345J,1040,Dallas_Staff,Dallas
```

A	B	C	D	E	F
B160	12345J	1040	Dallas_Staff	Dallas	

Figure 4:22

Following is an example of records containing multiple locator assignments to multiple groups. Each record in the import file must contain all five of the fields as explained in the preceding table:

```
B160,54321K,1040,Dallas_Staff,Dallas

B202,98765M,1120,NY_Preparers,New York

B216,45678N,1065,LA_Preparers,Los Angeles
```

A	B	C	D	E	F
B160	54321K	1040	Dallas_Staff	Dallas	
B202	98765M	1120	NY_Preparers	New York	
B216	45678N	1065	LA_Preparers	Los Angeles	

Figure 4:23

DISABLE/ENABLE LOGINS

1. Log on as the Administrator.
2. Select **Admin > Access Control Imports**.
3. Highlight the **Import Users - Disable/Enable Logins** option, and click the **Select Files** button.
4. Specify the location on your workstation or network in which the Excel .csv import file for new groups resides.
5. Select the correct location where the .csv import file resides. Only files with the filename extension ".csv", which typically designates a comma-delimited file, are allowed for **Access Control Import**.
6. When the correct file and location are selected, click the **Open** button on the **Browse for Folder** dialog. The **Browse for Folder** dialog is immediately closed, and the file in the selected folder with a filename extension of ".csv" appears in the file **Upload** dialog.
7. To start the import of the selected file, click the **Upload** button. To cancel the import, click the **Clear List** button.
8. The data from the selected file is imported into **Access Control** in a single operation which does not require your intervention. When the import is complete, the **Import Users - Disable/Enable Logins** results appear, and the data from the import file and the import status of each record appear.
9. Click the **Continue** button to end the import process and return to the **Access Control Imports** screen.

Import Users - Disable/Enable Logins Data Format

The import process reads a standard comma delimited file with three pieces of information for each row (user):

- The first element is the **User Login ID**.
- The second element is the **User Location**.

- The third element should be *Y* or *N* to indicate if the user and location specified should be disabled or enabled. The *Y/N* values are as follows:
  - *Y*= Disable
  - *N* = Enable

> All characters other than Y or N in the third position will cause the row to be skipped. No status will display for any row with a character other than Y or N in the third position.

The system takes the value for the Firm from the operating user performing the import process. This guarantees that unique user is being updated in the firm where the operating user is a member.

Import Users - Disable/Enable Logins Data Examples

Following is an example of four records containing user login disable/enable information for a user named Bill Smith. The data fields are explained in the preceding section:

	A	B	C
1	BSmith	***	Y
2	BSmythe	**$	Y
3	BSmythe	***	N
4	BSmythe	***	P

Figure 4:24

```
BSmith,***,Y

BSmythe,**$,Y

BSmythe,***,N

BSmythe,***,P
```

The results of the import appears as a report titled **User Login Status Import**. In the figure above, the user's name is misspelled in the first row, with the following result in the report:

USER LOGIN ID	LOCATION	ENABLE/DISABLE LOGIN FLAG	IMPORT STATUS
BSmith	***	[Y]	User BSmith at location *** does not exist.

In the second row, the location contains an incorrect character, with the following result:

USER LOGIN ID	LOCATION	ENABLE/DISABLE LOGIN FLAG	IMPORT STATUS
BSmythe	**$	[Y]	User BSmythe at location **$ does not exist.

In the third row, all information is correct, with the following result:

USER LOGIN ID	LOCATION	ENABLE/DISABLE LOGIN FLAG	IMPORT STATUS
BSmythe	**$	[N]	User Login Information has been updated.

The fourth row contains an incorrect character for the enable/disable login flag, with the following result:

USER LOGIN ID	LOCATION	ENABLE/DISABLE LOGIN FLAG	IMPORT STATUS
BSmythe	**$	[P]	User Login Information has not been updated successfully.

EMAIL ADDRESSES

1. Log on as the Administrator.
2. Select **Admin > Access Control Imports**.
3. Highlight the **Import Users - Email Addresses** option, and click the **Select Files** button.
4. Specify the location on your workstation or network in which the Excel .csv import file for new groups resides.
5. Select the correct location where the .csv import file resides. Only files with the filename extension ".csv", which typically designates a comma-delimited file, are allowed for **Access Control Import**.
6. When the correct file and location are selected, click the **Open** button on the **Browse for Folder** dialog. The **Browse for Folder** dialog is immediately closed, and the file in the selected folder with a filename extension of ".csv" appears in the file **Upload** dialog.

7. To start the import of the selected file, click the **Upload** button. To cancel the import, click the **Clear List** button.

8. The data from the selected file is imported into **Access Control** in a single operation which does not require your intervention. When the import is complete, the **Users Email** results appear, and the data from the import file and the import status of each record appear.

9. Click the **Continue** button to end the import process and return to the **Access Control Imports** screen.

Import Users - Email Addresses Data Examples

The following is an example of seven rows containing user email address information:

	A	B	C
1	ANEW	***	def@xyz.com
2	USER1	***	abc@xyz.com
3	DDUCK	AUSTIN	abc@xyz.com
4	LIMITED	DALLAS	abc@xyz.com
5	TEST100		abc@xyz.com
6	USER10	****	abc@xyz.com
7	JDOE	HOUSTON	abc@xyz.com

Figure 4:25

- The first element (Column A) is the **User Login ID**.
- The second element (Column B) is the **User Location**.
- The third element (Column C) should be the user's **email address**.