User Administration User Guide

EFT Solutions
November 2009

Contents

Revisions, November 2009

Section	Description
All	Apply template and reorganize manual

Revisions, October 2008

Section	Description
Reports	Update information

Revisions, August 2008

Section	Description
Reports	Update information

Introduction

Overview

User Administration is a security system that allows you to manage your institution's user security records and tokens. It gives you a clear view of each user's access and allows you to add user records tailoring access to job functions.

Page Recap

The following table highlights User Administration pages covered in this document.

Page	Description
User Administration	Allows you to open the User Administration application in a new window
User Administration—Choose User	Provides a search feature that you can use to locate user security records. It allows you to add, view, update, or delete user security records
User Administration—User Summary	Displays the security record of an existing user
User Administration—User Details	Allows you to specify basic information related to a user
User Administration—Logos	Allows you to specify logos that a user may access in CWSi
User Administration—Applications	Allows you to specify application access for a user
User Administration—Access Rights	Allows you to specify application access rights granted to a user
User Administration—Special Roles	Allows you to specify special roles for a user
User Administration—Availability	Allows you to specify access times for a user
User Administration—Tokens	Allows you to specify token issuance information
User Administration—User Record	Allows you to save the user record based on the information you have supplied

Using the User Administration Application

Overview

CWSi User Administration is a security system that allows you to manage your institution's user security records and tokens. It gives you a clear view of each user's access and allows you to add user records tailoring access to job functions. It also helps you manage users and token requests by allowing you to submit changes online and monitor their progress on reports.

PSAs, Administrators, and Users

Primary security administrators (PSAs), administrators, and users all have a role in User Administration. These are described below. Note that your institution can have only one PSA and should have at least one administrator as backup.

Description	PSA	Administrator	User
Has any combination of read, add, update, and delete access	X	X	
Has the highest level of access to all applications available to your institution, and is identified on the User Summary page as primary administrator	X		
Must use tokens regularly to avoid losing access due to inactivity	X	X	X
Sets up and maintains all user access to applications used by your institution	X	X	
Receives intial access to new applications	X		
Can only be added, updated, or deleted by an EFT Solutions' security administrator	X		
Has the authority to give access to and manage administrators	X		

Tokens

A token is an electronic device that generates a sequential number called a key. This key is required to log on to Client-Central. Following is important information regarding tokens:

- Each user, PSA, and administrator must have a token to access Client-Central. A token identifies a unique user and is not shared between users.
- Your institution is solely responsible for the use or misuse of tokens. It is also solely responsible for establishing the extent and effectiveness of the institution's security administration program for access to Client-Central.
- A token can be reassigned to a new user. User Administration allows token reassignment when adding a new user.

  If a token is reassigned to a new user, the personal identification number (PIN) must be changed. The original user must do the following:

  – Type the PIN.

  – Press the **ON** button.

  – Press the **MENU** button until CHANGE PIN displays.

  – Press the **ON** button, and then pass the token to the new user.

  – The new user types a new PIN.

  Contact your client services representative if you require any further information.
- A token locks after 6 bad PIN tries. Once locked, call Express Client Services along with the PSA or another active token user who can validate the user needing the new PIN. You will have to select a new PIN as the current PIN cannot be re-entered.
- A lost, stolen, or defective token can be replaced. User Administration allows you to request a token replacement by updating a user security record.

Timeframes

To review the status of a token request and other administrative tasks, select **Request Status** under the Reports tab. The Completion Date indicates the token shipping date if one has been requested. The report contains request information for all open requests and requests completed in the past 30 calendar days.

New Users

An anticipated timeframe of 7 business days is required to complete the necessary functions for a new user to access Client-Central. A token is shipped on completion of necessary functions. Transit duration for the token depends on the mode of shipping.

Existing Users

The following shows anticipated timeframes for existing Client-Central users. The timeframes apply only if accurate information is provided. Incomplete or incorrect information results in a delay. Deletion of a Client-Central user security record takes effect immediately and the user can no longer access Client Central.

Type of Service	Application	Timeframe
New services	CWSi applications	Effective immediately
	ClientView internet (CVi)	7 business days
	Premier Services	7 business days
	CardTracker	7 business days
	TranBlocker	7 business days
	CaseTracker	7 business days
	Nautilus	7 business days
New applications	CWSi applications	Effective immediately
Update access rights	CWSi applications	Effective immediately
	CVi	7 business days
	Premier Services	7 business days
	CardTracker	7 business days
Token replacement	Client-Central	7 business days

Pricing

An authorized service request is submitted with the implementation of Client-Central for your institution. The service request defines the pricing structure for your institution. By accepting the statement charges will apply as set forth in your Client-Central pricing documentation while adding, updating, or deleting users in User Administration, you confirm that all relevant Client-Central pricing as defined for your institution is acceptable. For further information contact your client services representative.

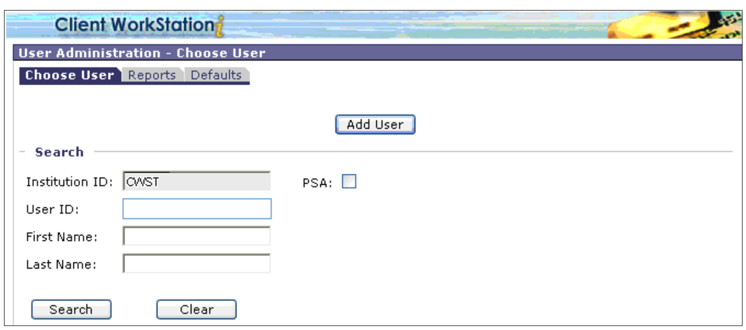
Access User Administration

You must have at least read access to the User Administration application. To access User Administration, perform the following.

Step 1 Log on to Client-Central (see the *EFT* Solutions' *User Manual*, *Getting Started*). The Client-Central home page appears.

Step 2 Click the **User Administration** tab at the top of the home page. The User Administration Overview page appears.

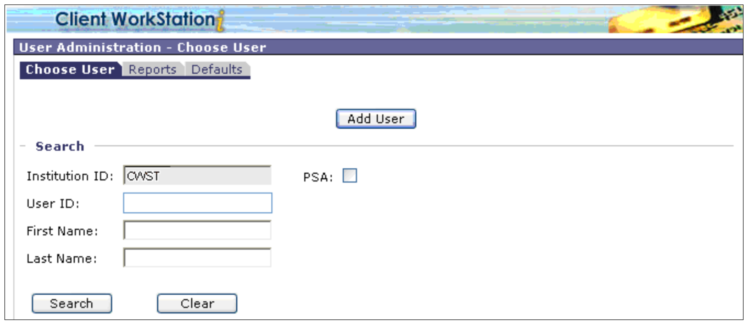
Step 3 Click **User Administration** in the left navigation bar. The Choose User page appears.



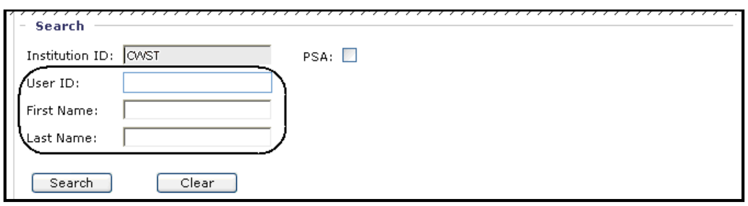
From here you can search, view, download, add, update, and delete user security records of the Client-Central users associated with your institution.

Search for User Security Records

Step 1 Access User Administration (see Access User Administration, page 9). The Choose User page appears.

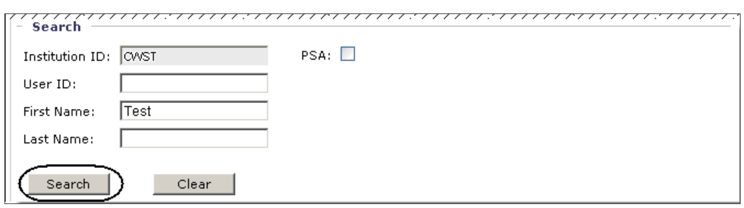


Step 2 Type the user ID, first name, last name, or any combination in these fields to search for a specific user or set of users, or leave these fields blank to view a list of all users for your institution. The institution ID is prefilled based on your user ID and cannot be changed.

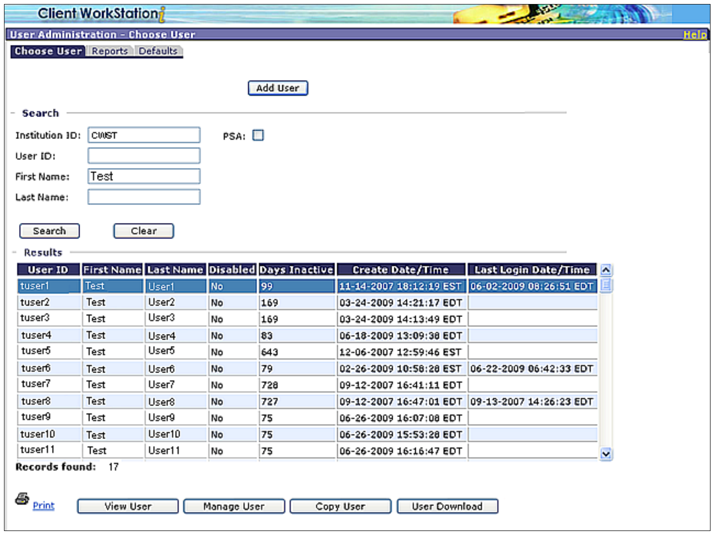


Note: To find your institution's PSA, leave these fields blank and check the PSA check box.

Step 3 Click **Search**.



The Choose User page reappears with a Results section containing a list of users that match your search criteria.



The Results section contains the following information.

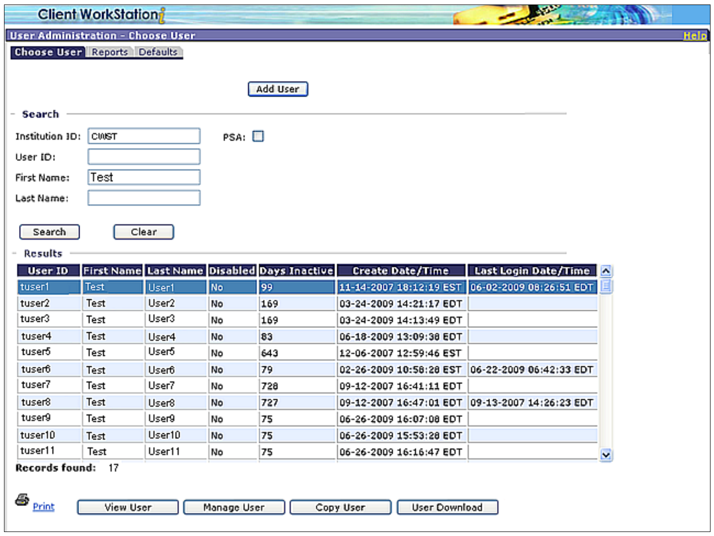
Field/Buttons	Description
User ID	User ID of the user security record
First Name	First name associated with the user ID
Last Name	Last name associated with the user ID
Disabled	Displays No if the user is active and Yes if the user has been disabled. See Disable User, page 38 for instructions on how to disable a user’s access.
Days Inactive	The number of days the user has not logged onto Client-Central causing the user record to be inactive.
Create Date/Time	Date and time when the user security record was initially added
Last Login Date	The date and time that the user last logged on
Records found	Total records returned by your search. Results list is scrollable if more than 11 records are returned.
Print link	Prints the results list displayed
View User button	Takes you to the User Summary page that displays the summary of the selected user. It displays when you have read access to User Administration.

Field/Buttons	Description
Manage User button	Takes you to the User Record page that allows you to update or delete the selected user. It displays when you have update or delete access to User Administration.
Copy User button	Takes you to the Add User Details page that allows you to create a new user record copying the user you have selected. It displays when you have add access to User Administration.
User Download button	This button creates a PDF that contains user summary information for all users contained within the search results list. It can be viewed, printed, or downloaded. If the search results list exceeds 100 users, a Starting Row # field appears beside the User Download button. Since the PDF can only contain user summary information for up to 100 users, this field allows you to designate which group of 100 will be contained within each PDF. To generate a PDF for the first 100 user summary records, enter the starting row value of 1 and click the **User Download** button. Once the PDF for that group has been downloaded or printed, enter a starting row value of 101 to generate a new PDF for the next group and so on until you have captured all records within the search results list.

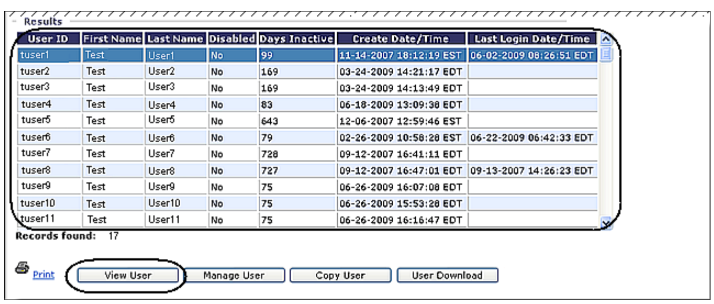
From here you can search for more user security records if you desire.

View User Security Records

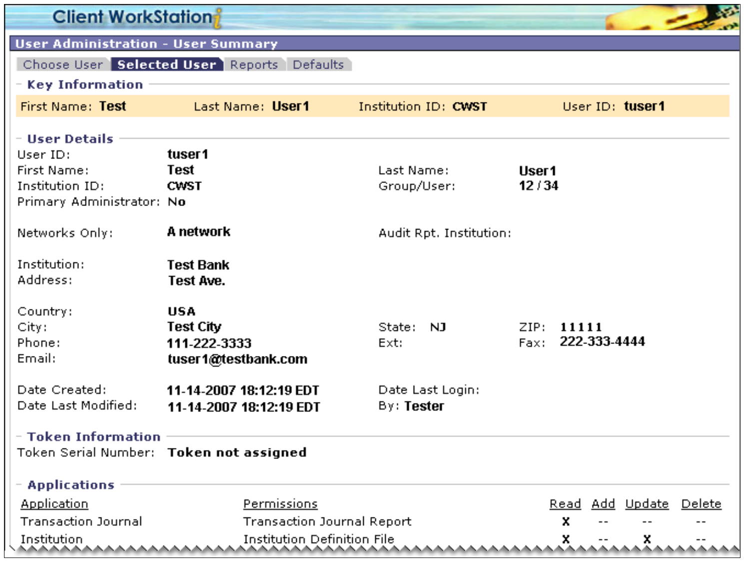
Step 1 Access User Administration and search for a user record (see Search for User Security Records, page 10). The Choose User page appears with a Results section containing a list of users that match your search criteria.



Step 2 Select a user in the Results list and click **View User**.



The User Summary page corresponding to your selection appears.



The User Summary page contains the following sections.

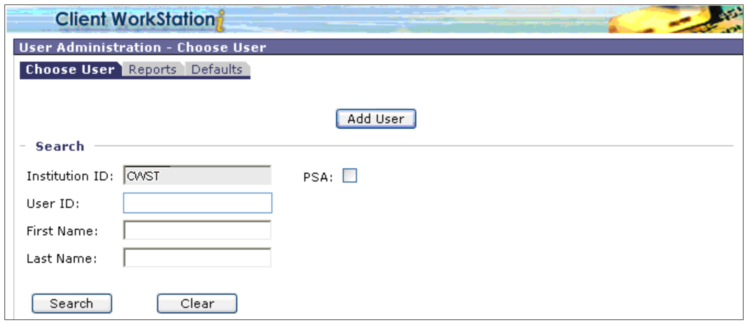
Section/Button	Description
Key Information	Institution and user ID information for the selected user
User Details	Relevant institution, user ID, name, and address information for the user
Token Information	Token serial number assigned to the user. It displays as “Token not assigned” when record is first created and until the number has been assigned.
Applications	Applications the user has access to, and the permissions and access rights that have been granted for each application
Special Roles	Special roles which feature additional access rights given o the user
LOGOs	Institution IDs the user can access
Availability	Time period the user can access the applications in their list of applications
Manage User button	Displays when you have update or delete access to User Administration. It takes you to User Record page where you can update or delete user record.
Print	Prints the page

From here you can:

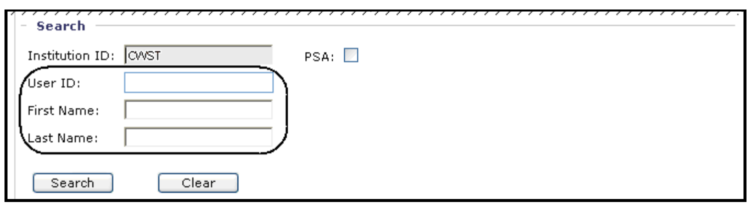
- Print the page
- Manage the user (update, disable, enable, or delete)
- Return to the Choose User page
- Go to the Reports or Defaults tab

Download User Summary Records

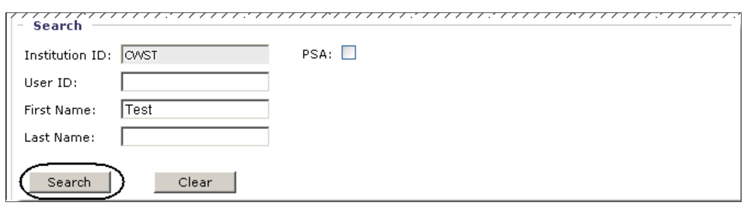
Step 1 Access User Administration (see Access User Administration, page 9). The Choose User page appears.



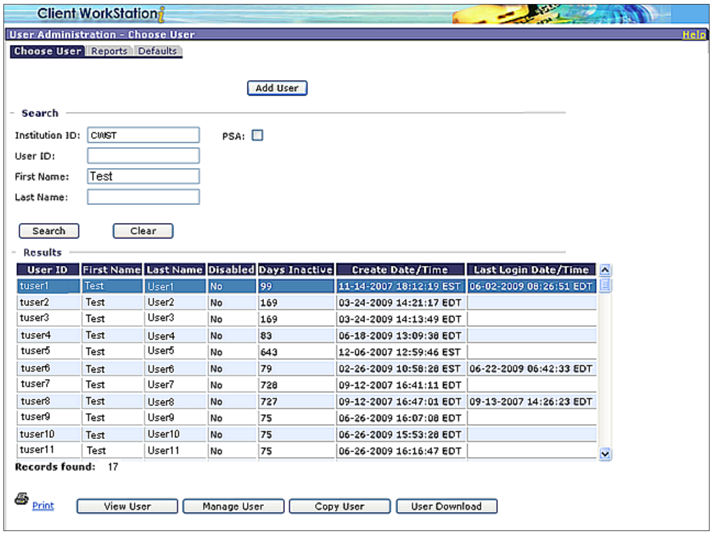
Step 2 Type the user ID, first name, last name, or any combination in these fields to search for a specific user or set of users, or leave these fields blank to view a list of all users for your institution. The institution ID is prefilled based on your user ID and cannot be changed.



Step 3 Click **Search**.

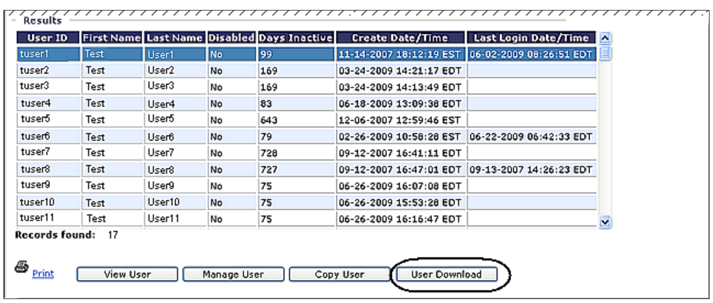


The Choose User page appears with a Results section containing a list of users that match your search criteria.

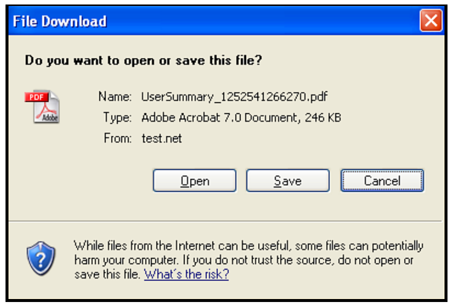


Note: A Starting Row # field will display to the right of the User Download button if your search results list contains more than 100 records. Since the PDF that is created can only contain user summary information for up to 100 users, this field allows you to designate which group of 100 will be contained within each PDF. If this field exists, enter a starting row value prior to clicking the User Download button.

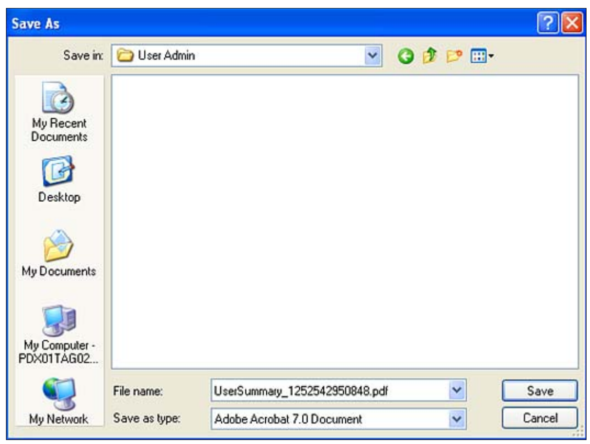
Step 4 Click **User Download**.



A File Download box appears.

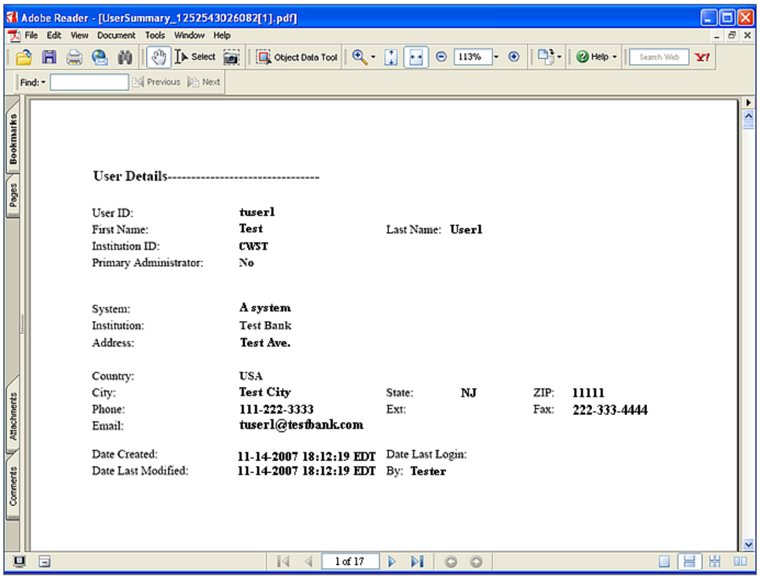


Step 5 To save the file, click **Save**. A Save As box appears allowing you to save the PDF to a desired location.



-or-

To open the file, click **Open**. A PDF opens displaying User Summary information for all of the users in the search results list. This PDF can be printed.



Note: You must have Adobe Acrobat installed on your PC to view the PDF.

From here, you may return to the Choose User page to search for other user security records if you desire.

Administer User Security Records

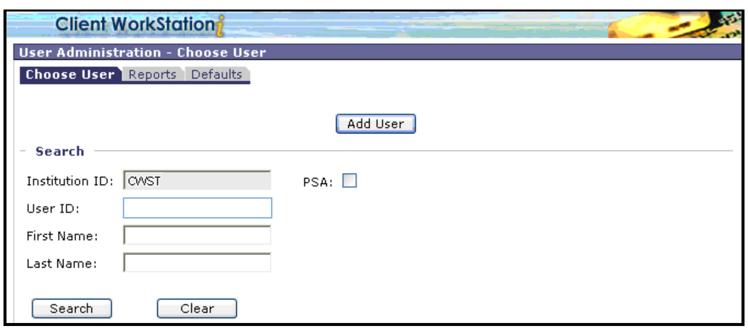
Administrators must have add, update, and delete access in User Administration to manage other users' security records accordingly. This section explains the process of adding, copying, updating, and deleting user security records.

Create a User Security Record

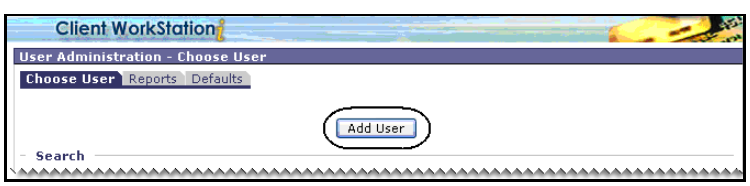
The two options for creating a user security record are:

- **Add user**—Takes you through the add process using your security setup as the starting point. It allows you to add the new user based on your settings. You can modify each page as needed.
- **Copy user**—Takes you through the add process using the setup of the user you have chosen to copy. It allows you to choose a starting point that minimizes the number of modifications required to add the new user record. You can modify access on each page as needed.

Step 1 Access User Administration (see Access User Administration, page 9). The Choose User page appears.

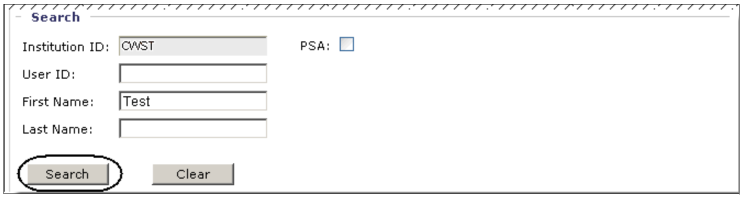


Step 2 To add a user, click **Add User**.

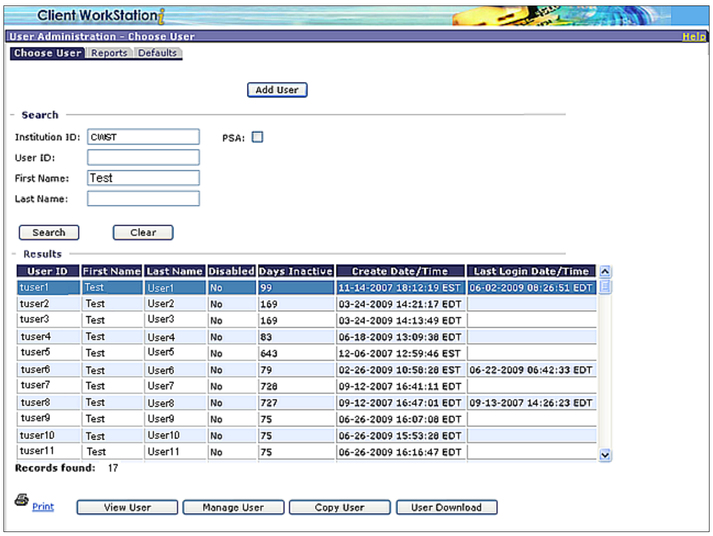


-or-

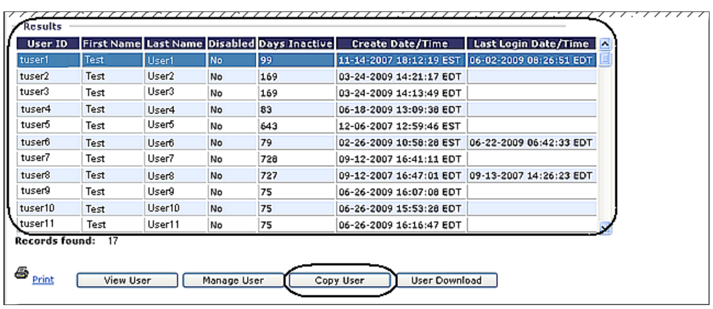
To copy a user, click **Search**.



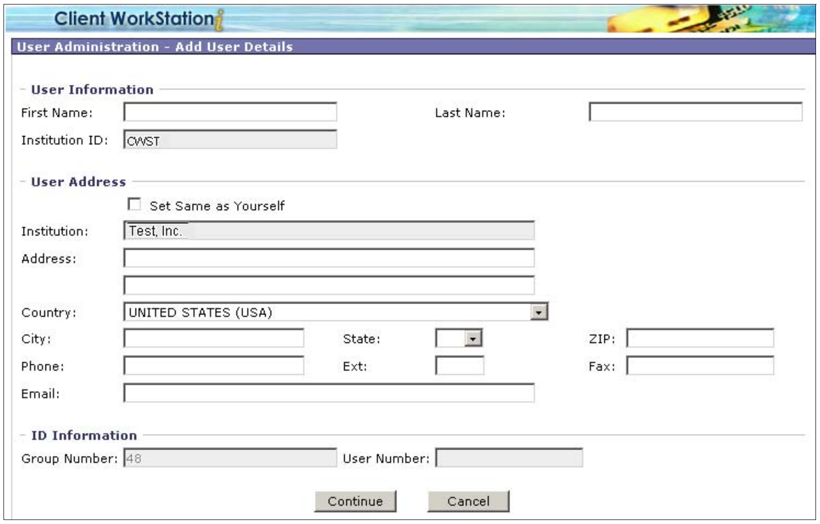
The Choose User page reappears with a Results section containing a list of users that match your search criteria.



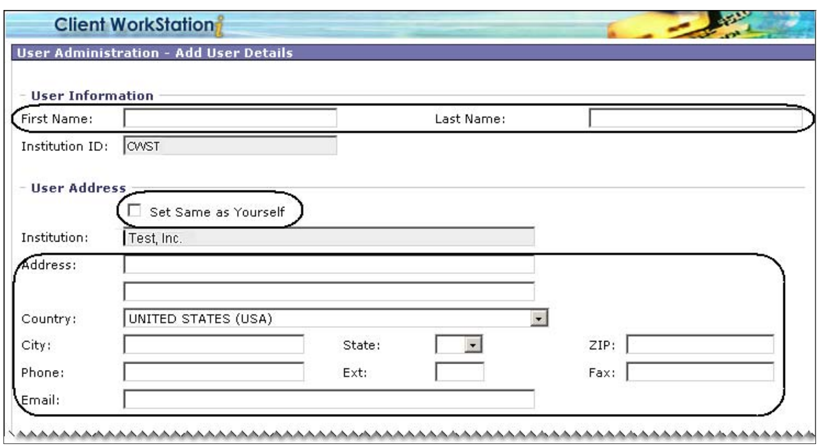
Select a user in the results section and click **Copy User**.



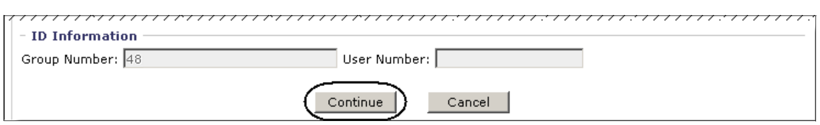
The Add User Details page appears.



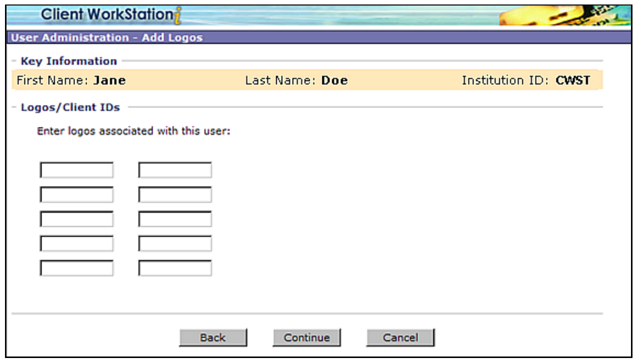
Step 3 Fill in the user name, business address, and other required information. If you like, select the **Set Same as Yourself** check box to prefill the Address field with the address defined on the security record of the administrator creating this record.



Step 4 Click **Continue**.

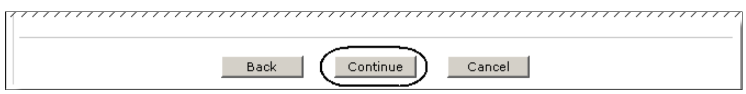


The Add Logos page appears. All logos associated with the user appear in the Selected Logos list box. Displayed values reflect the settings on the security record of the administrator adding the user.

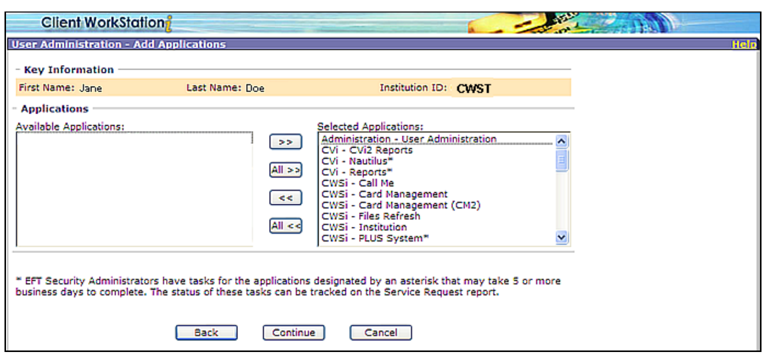


Step 5 Type one or more logos in the fields provided. When a new logo is associated with your institution, your primary administrator should grant access, if applicable, to other administrators and users.

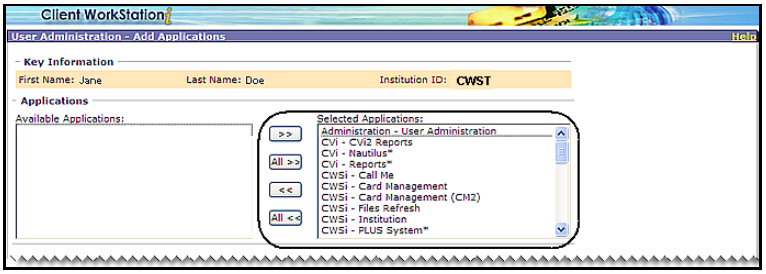
Step 6 Click **Continue**.



The Add Applications page appears. All applications available to you display in the Selected Applications list box.



Step 7 Select one or more applications and use the arrow buttons to move the applications that you do **not** want the user to access to the Available Applications list box. The new user must be granted access to at least one application. EFT Solutions suggests that you grant all users read access to the Message Board application.



Some things to remember:

- **Administrator**—If you are not the primary security administrator (PSA), you will not see the User Administration application in either the Selected Applications list box or Available Applications list box. Only the PSA can give another user access to User Administration.
- **PSA**—If you are the PSA, you will see the User Administration application in the Available Applications list box. If you want this new user to be an Administrator, highlight the application and move it to the Selected Applications list. If this new user will not be an Administrator, leave the application in the Available Applications list. The User Administration application can be given to a user at any time by the PSA.

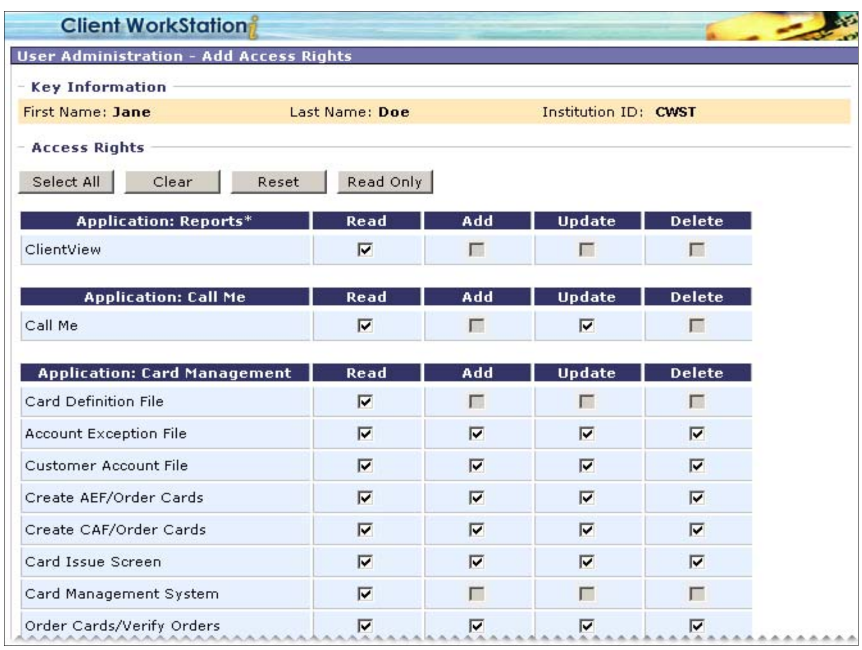
The following are possible applications available depending on the applications used by your institution and your security access.

Application	Permission Description
Administration—User Administration	• Permissions available on Access Rights page • Special roles may be available on the Special Roles page
CVi—Reports	No permissions on Access Rights page, additional setup required by EFT Solutions' Security
CWSi—Card Management	• Permissions available on Access Rights page • Special roles may be available on Special Roles page
CWSi—Terminal	Permissions available on Access Rights page
Premier Services—ATM Cardholder Preferences	No permissions on Access Rights page, additional setup required by EFT Solutions' Security

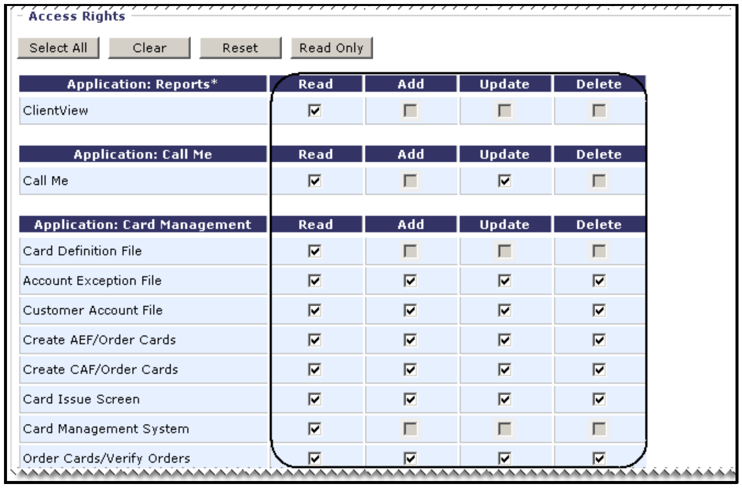
Application	Permission Description
Premier Services—ATM Marketer Admin*	No permissions on Access Rights page, additional setup required by EFT Solutions' Security
Premier Services— ATM Marketer Builder*	• No permissions on Access Rights page, additional setup required by EFT Solutions' Security • Special roles may be available on the Special Roles page
Premier Services—Premier Analytics	No permissions on Access Rights page and no additional tasks required
Premier Services—Premier Manager*	No permissions on Access Rights page, additional setup required by EFT Solutions' Security
Risk Management—Compromised Card	Permissions available on Access Rights page
Risk Management—TranBlocker	Permissions available on Access Rights page

Step 8 Click **Continue**.

The Add Access Rights page appears displaying all applicable permissions for the applications selected on the Add Applications page. Applications that do not require access rights in User Administration are not displayed. Access rights displayed match your level of access or the access of the user you chose to copy.



Step 9 Specify access rights for the user by clicking desired check boxes. Clicking a checked box will uncheck the box and clicking an empty box will check it. Grayed boxes do not apply and can't be checked.



To remove access, click the individual box to remove the check mark or use one of the following buttons:

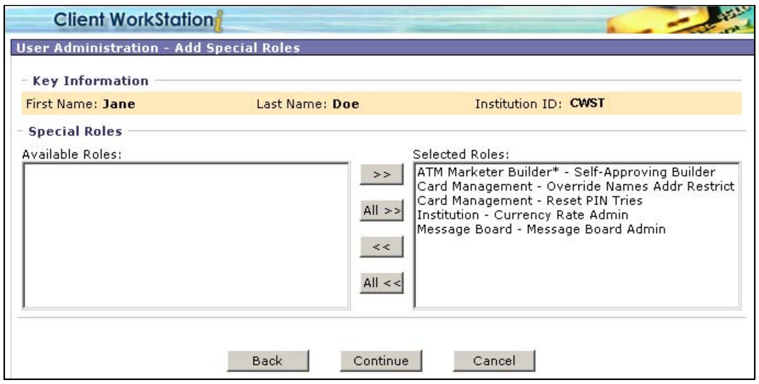
- **Read Only**—Changes all access to read. Modify the access rights from there.
- **Clear**—Removes all access. Select only what you want the user to have. You must give the user read access to an application in order to give them any other available access.
- **Reset**—Returns to the original access when you first came to the page.
- **Select All**—Gives the user full access to all listed applications.

To access the Card Management System (CMS) application, the user must have access to the Card Definition File (CDF). To access the Terminal application, the user must have access to the Terminal Definition File (TDF).

Note: If you click the **Back** button during an add or copy, changes made on the Add Applications page reflect on this page. If an application is removed, it no longer shows up on this page.

Step 10 Click **Continue** at the bottom of the page.

- If you have given the new user access only to applications that do not have special roles, the Add Availability page appears. Skip to Step 13 on page 28.
- If you have given the new user access to applications that do have special roles, the Add Special Roles page appears. All special roles associated with the user display in the Available Roles list box.

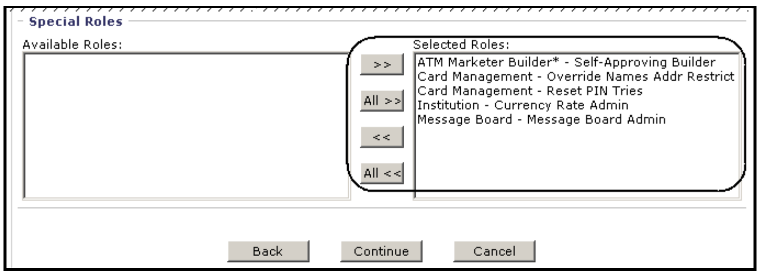


Special roles are used with the access rights assigned for each application and are required in order to do the various tasks. For example, a user will not be allowed to force activate a card record unless they have the force-activate special role.

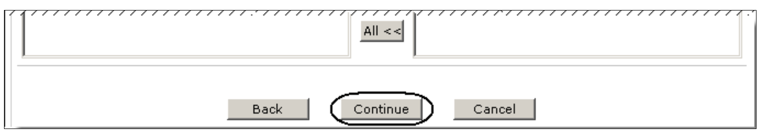
Special Role	Description
Card Management—Change Card Status	Allows you to change the status and reason code of a card record on the Cardholder Details page. Users must have read access to cardholder information before they can be granted this role.
Card Management—Force Activate	Allows you to force-activate a card from both the Cardholder Details and Cardholder Activation pages. Users must have read access to cardholder information before they can be granted this role.
Card Management—Copy Cardholder	Allows you to copy a cardholder record from the Cardholder Details page to create a new record. Users must have read access to cardholder information before they can be granted this role.

Special Role	Description
User Administration—Customize User ID	Allows administrators to create user records with their institution's user ID format instead of the standard user ID format.
ATM Marketer Builder—Self-Approving Builder	Permission given to an ATM builder account in which the user can approve their own campaigns. Without it, the ATM Marketer admin must approve the campaign.

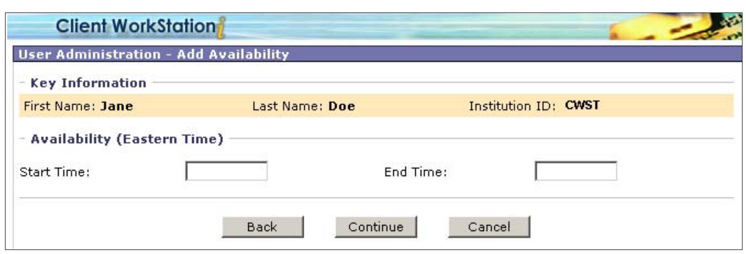
Step 11 Select one or more roles and use the arrow buttons to move the roles that you do **not** want the user to access to the Available Roles list box.



Step 12 Click **Continue**.



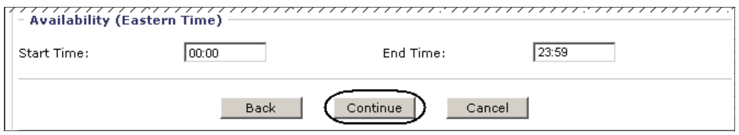
The Add Availability page appears.



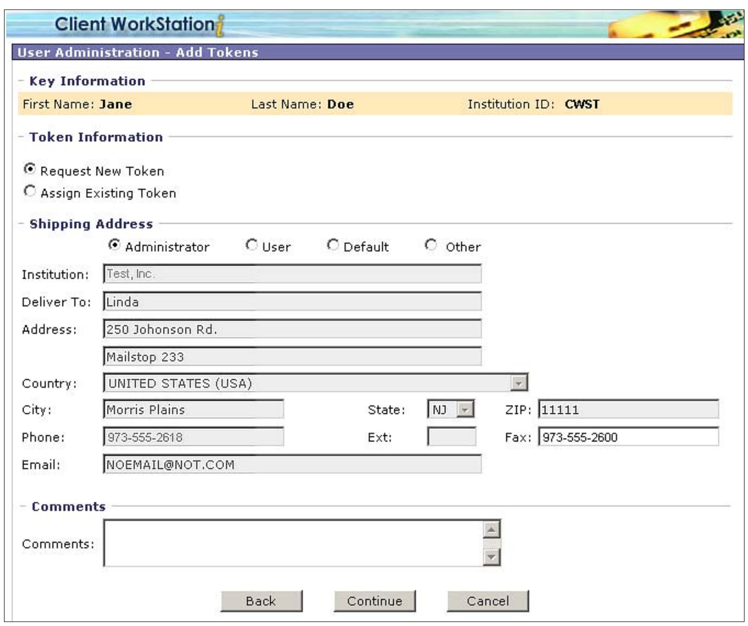
Step 13 Type the start time and end time to set time limits for the user's access. Times are U.S. Eastern and the start time must be earlier than the end time.

- **Start Time**—Time of day when the user can begin to access the applications controlled by User Administration. Format is military time and defaults to 00:00.
- **End Time**—Time of day after which the user can no longer access the applications controlled by User Administration. Format is military and defaults to 23:59.

Step 14 Click **Continue**.



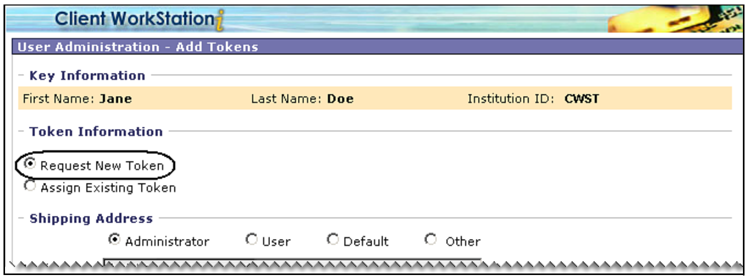
The Add Tokens page appears.



Step 15 On the Add Tokens page, you can either request a new token or assign an existing token. Descriptions of both options follow.

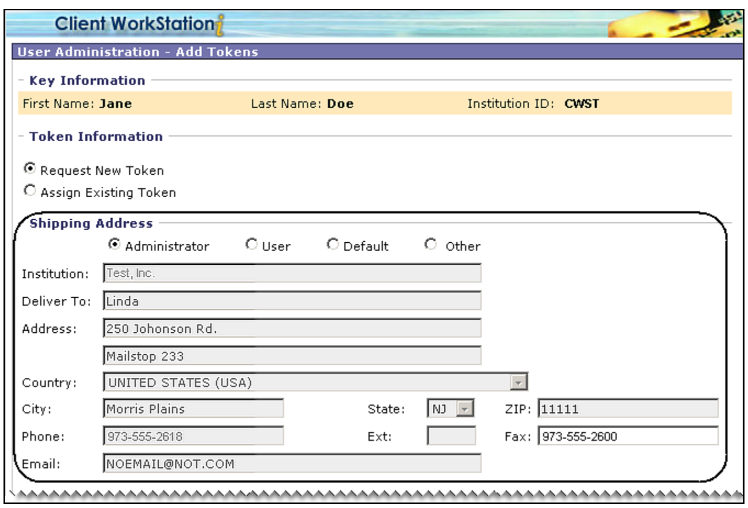
Option 1—Request new token

- First, select **Request New Token**.



This sends a task to EFT Solutions' security administrators. Please allow up to 5 business days to process and approximately 2 days for shipping.

- Next, select a shipping address option and change or provide information as necessary. A description of fields is shown below.

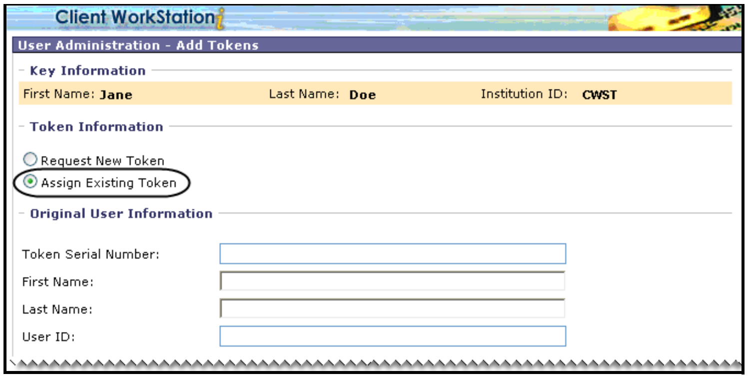


Shipping Address Option	Description
Administrator	Prefills the address fields with the information from your user security record
User	Prefills the address fields with the address information from the details page of this new user
Default	Prefills address fields with address specified as default for your institution
Other	Clears the fields allowing you to type alternate address information (not available when copying a user)

- Then, skip to Step 16 on page 32.

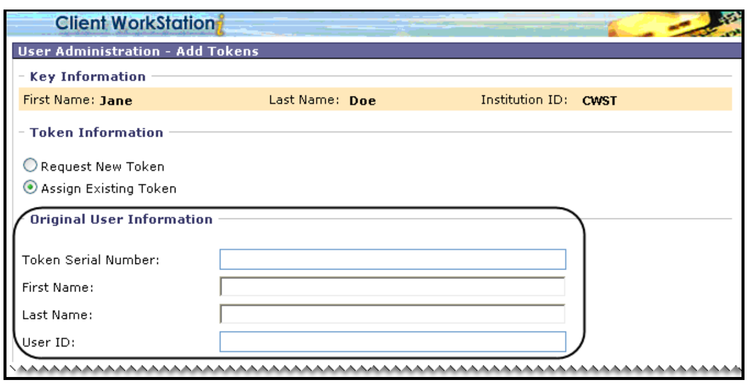
Option 2—Request existing token be reassigned

- Select **Assign Existing Token**. This can be done in either Add or Update mode.



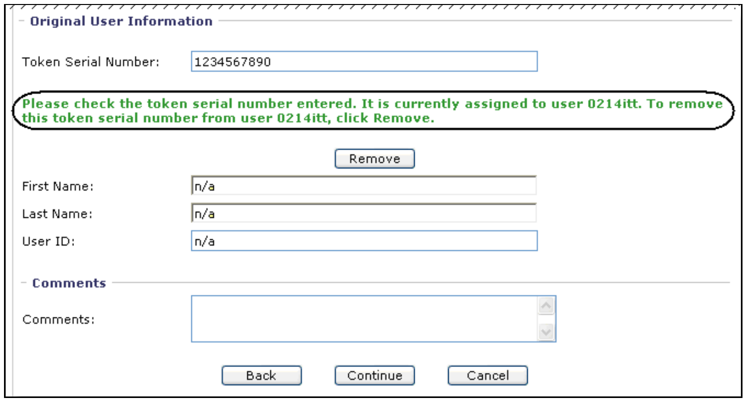
The token is reassigned immediately when the record is saved or updated.

- If you have already deleted the user ID of the original token owner, or if the token is not assigned to another user, complete the Original User Information fields and skip to Step 16 on page 32. Adescription of fields is shown below.

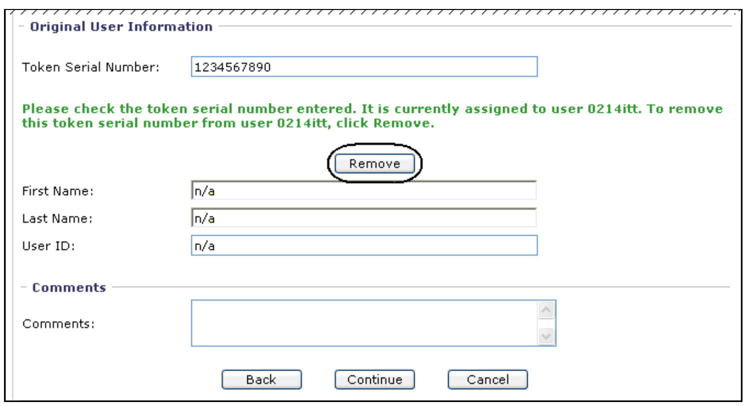


Original User Information Fields	Description
Token Serial Number	Serial number of the token to be reassigned. Tokens cannot be shared; if you have not deleted the user ID of the original owner, you are given the opportunity to remove it on this page.
First Name	First name of the original owner or NA
Last Name	Last name of the original owner or NA
User ID	User ID of the original owner or NA

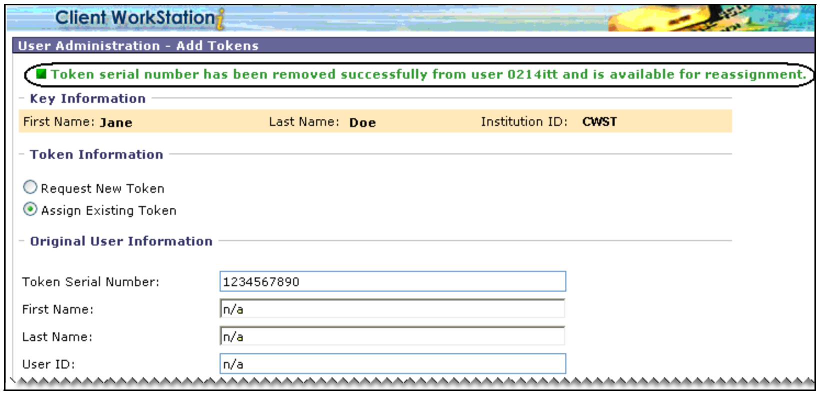
- If the token is assigned to another user ID, a message and the Remove button appear on the Add Tokens page.



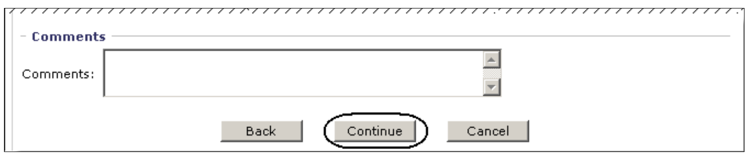
Verify the token serial number entered. If the serial number is incorrect, enter the correct number and skip to Step 16 on page 32. If the serial number is correct, click **Remove**.



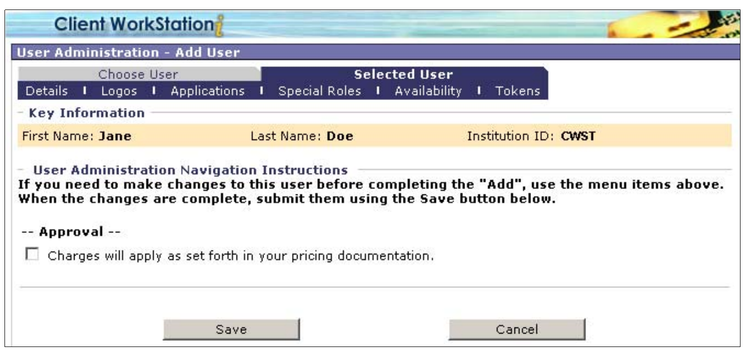
The serial number is removed from the original owner. A success message displays indicating that it is available for reassignment.



Step 16 Click **Continue**.

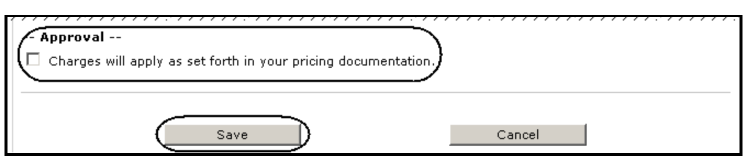


The Add User page appears.

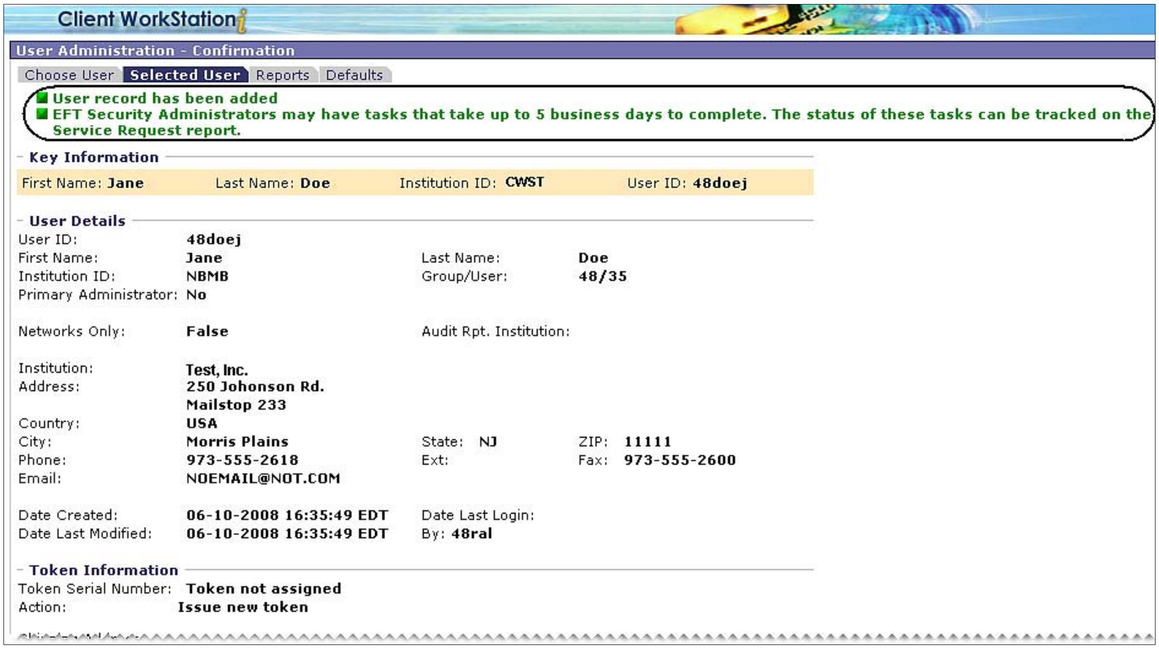


Note: You can edit the user information before saving the record by accessing the relevant page under Selected User tab.

Step 17 Select the **Approval** option check box and click **Save** to continue.



The Confirmation page confirms the addition of the user record.



From here you can:

- Print the page.
- Add another user.
- Use navigation tabs at the top of the page to return to choose user, view the request report, or view the default address.

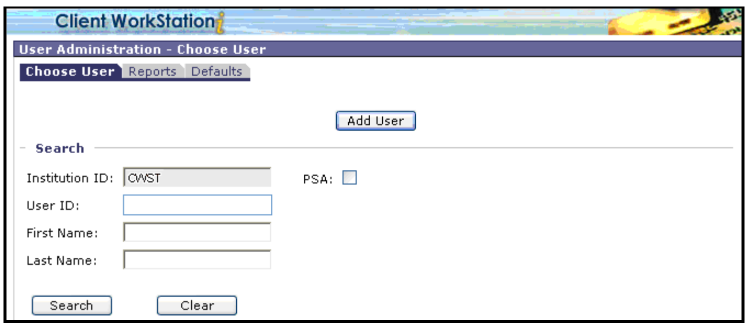
Update User

Only PSAs and administrators having update access can update a user security record.

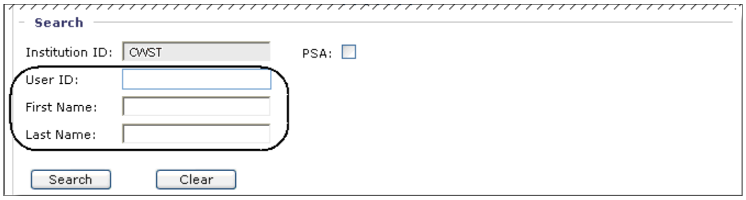
When in update mode, the user security record may display applications, access rights, and other privileges that exceed the ones defined in the security record of the person administering the record. These values cannot be edited.

Note: An administrator cannot grant access exceeding the settings on their own security record.

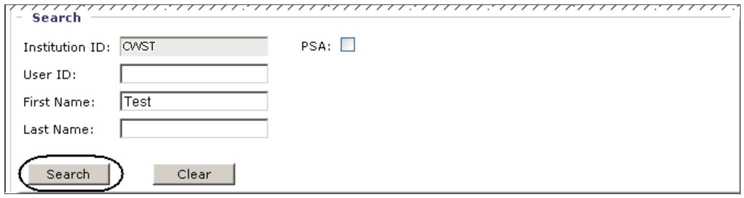
Step 1 Access User Administration (see Access User Administration, page 9). The Choose User page appears.



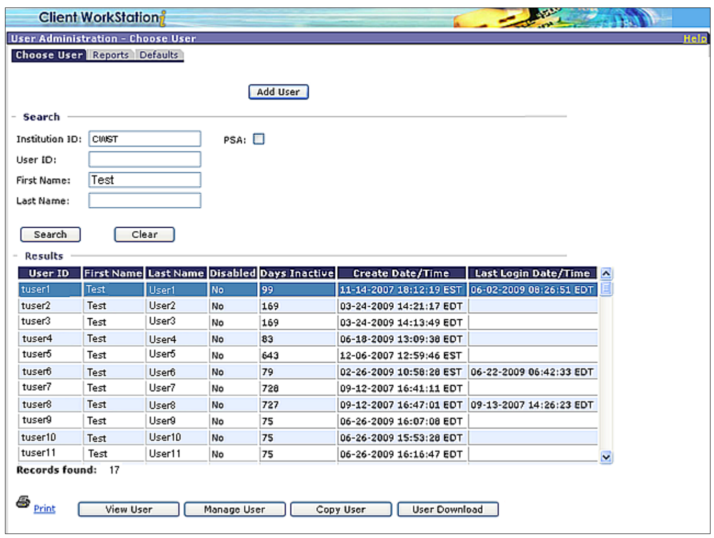
Step 2 Type the user ID, first name, last name, or any combination in these fields to search for a specific user or set of users, or leave these fields blank to view a list of all users for your institution. The institution ID is prefilled based on your user ID and cannot be changed.



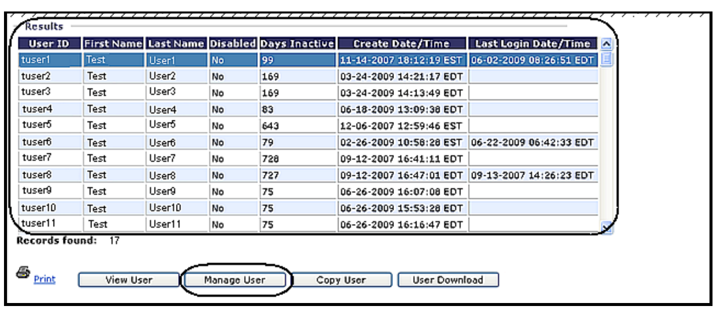
Step 3 Click **Search**.



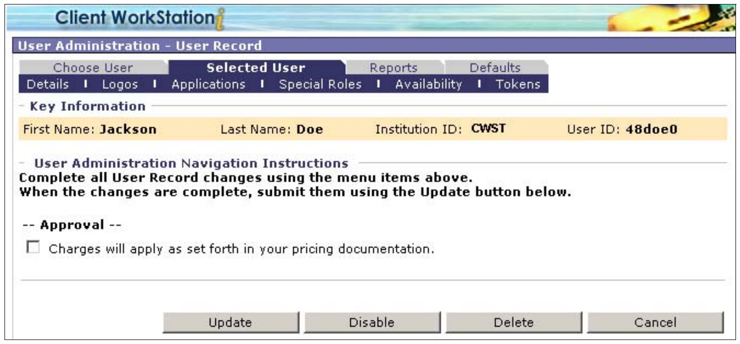
The Choose User page reappears with a Results section containing a list of users that match your search criteria.



Step 4 Select a user in the results section and click **Manage User**.

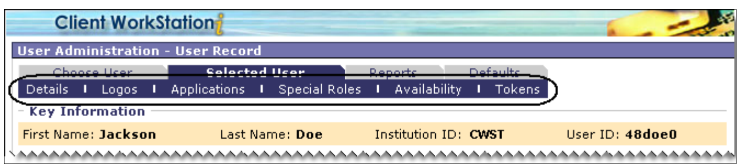


The User Record page appears.



Note: The Update button is visible only if you have update access rights in the User Administration application.

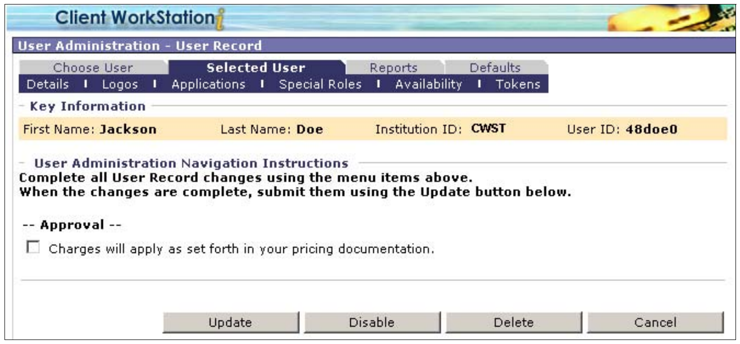
Step 5 Depending on the information you want to update, click **Details**, **Logos**, **Applications**, **Special Roles**, **Availability**, or **Tokens**.



The options are described below:

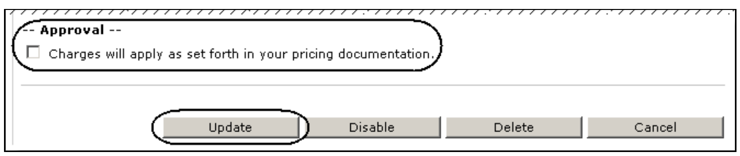
- **Details**—Allows you update user details such as name, address, and phone number
- **Logos**—Allows you to update the logos the user may access
- **Applications**—Allows you to provide the user with access to specific applications
- **Special Roles**—Allows you to assign special roles so that the user may peform specific tasks
- **Availability**—Allows you to specify time restrictions so that the user can only access the application within a select timeframe
- **Tokens**—Allows you to assign an existing token or issue a new token to the user

Step 6 Click **OK** on the selected page. This saves the updates temporarily and returns you to the User Record page.

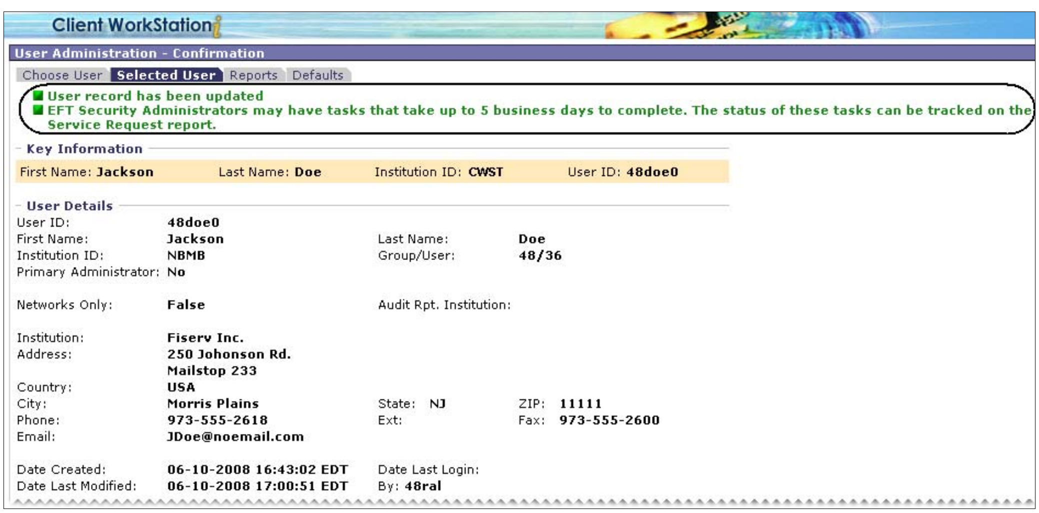


Note: The only exception is the User Administration—Applications page, where you click the **Continue** button to save updates temporarily and proceed to the Access Rights page.

Step 7 Select the **Approval** option check box and click **Update**.



Step 8 The Confirmation page confirms the update and the user security record is updated.

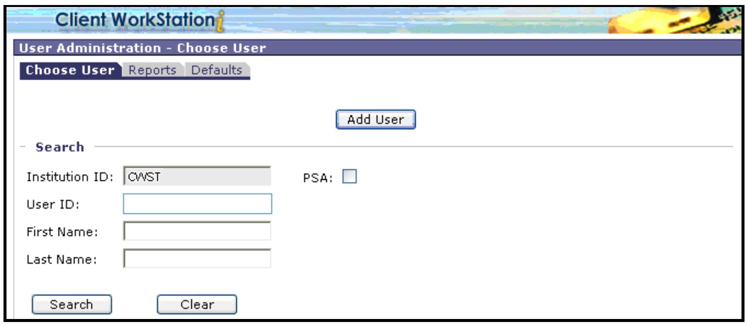


From here you can update another user if you desire.

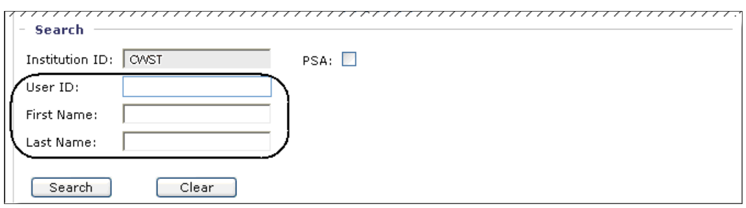
Disable User

A disabled user cannot access the portal. When you disable a user you are not deleting the user ID. Use this function when you do not want a user to have access for a period of time, such as an extended medical leave or long vacation.

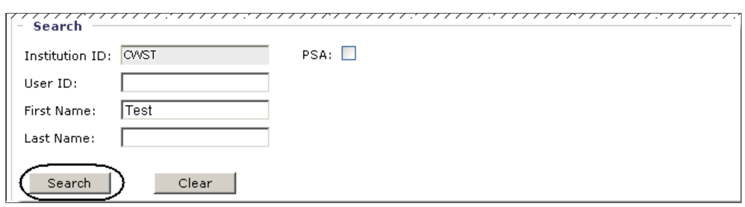
Step 1 Access User Administration (see Access User Administration, page 9). The Choose User page appears.



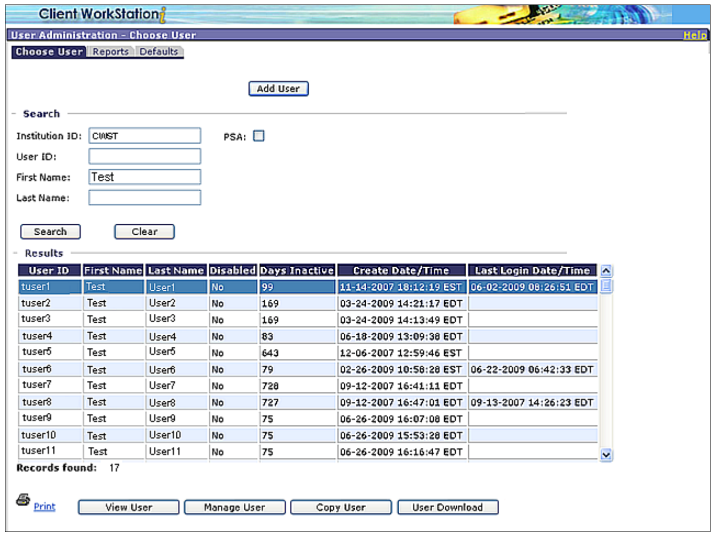
Step 2 Type the user ID, first name, last name, or any combination in these fields to search for a specific user or set of users, or leave these fields blank to view a list of all users for your institution. The institution ID is prefilled based on your user ID and cannot be changed.



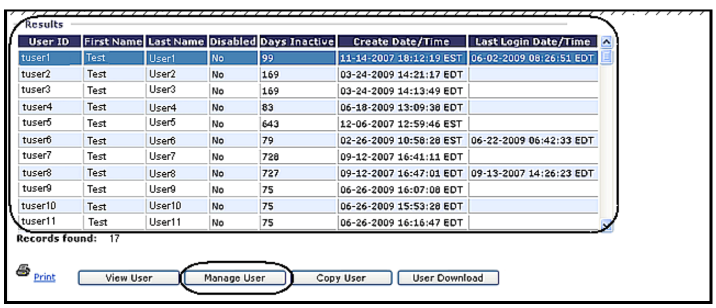
Step 3 Click **Search**.



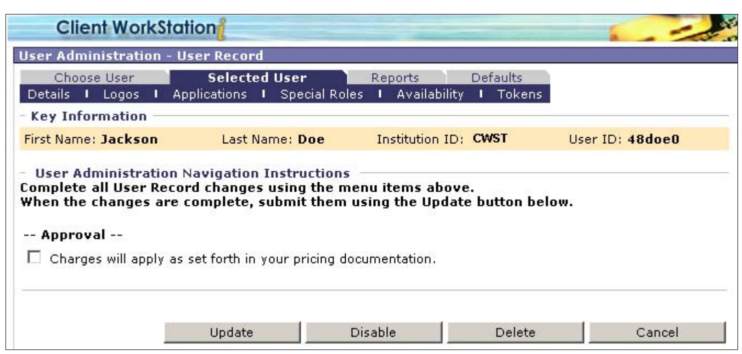
The Choose User page reappears with a Results section containing a list of users that match your search criteria.



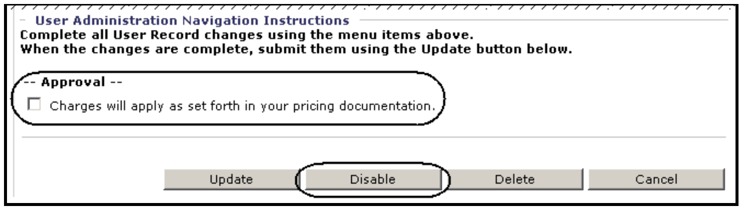
Step 4 Select a user in the results section and click **Manage User**.



The User Record page appears.



Step 5 Select the **Approval** check box and click **Disable**.



The User Record page displays a success message.

Note: Upon disabling the user, the Disabled column on the Choose User page shows “Yes”.

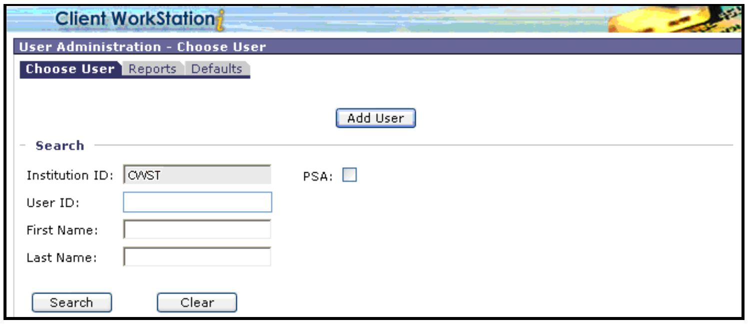
From here you can:

- Use the navigation tabs at the top of the page to view reports and defaults
- Return to the Choose User page and choose another user to view, manage, or copy

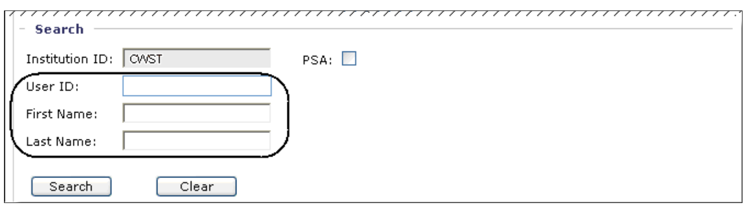
Enable User

Use the enable feature to give disabled user IDs access to the portal, for example, after employee returns from extended leave.

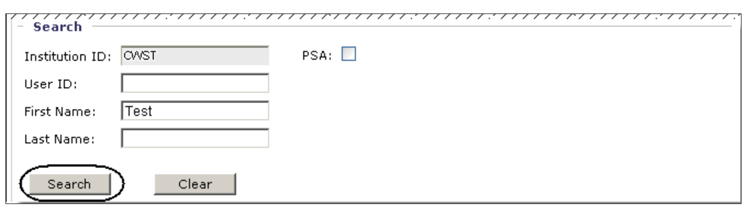
Step 1 Access User Administration (see Access User Administration, page 9). The Choose User page appears.



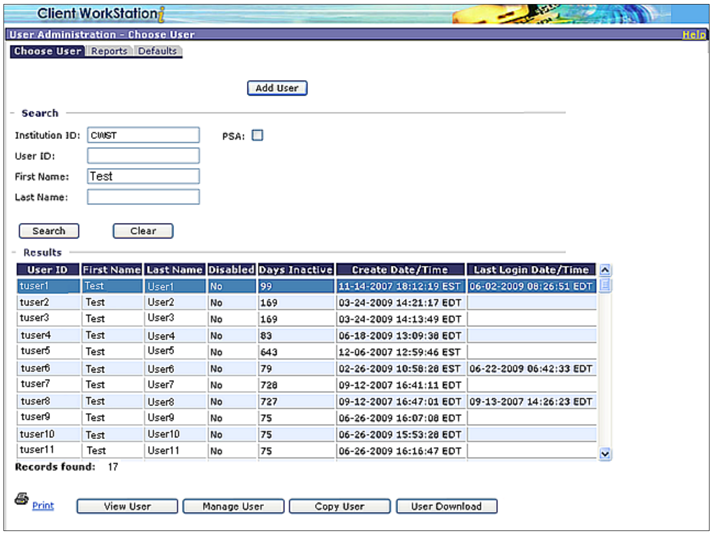
Step 2 Type the user ID, first name, last name, or any combination in these fields to search for a specific user or set of users, or leave these fields blank to view a list of all users for your institution. The institution ID is prefilled based on your user ID and cannot be changed.



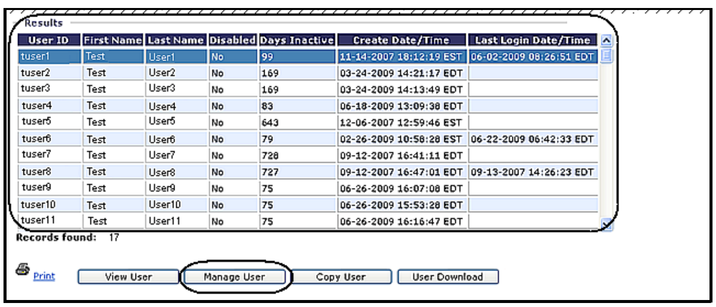
Step 3 Click **Search**.



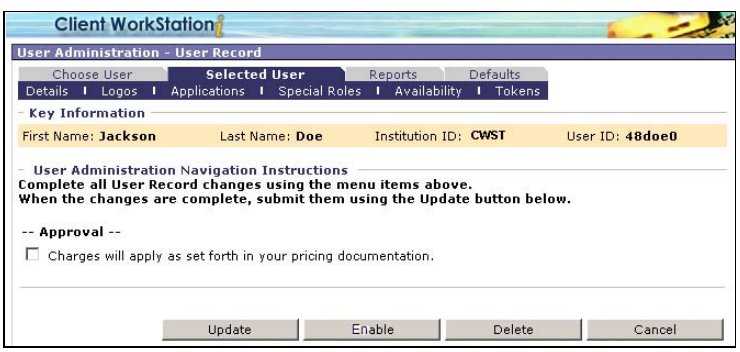
The Choose User page reappears with a Results section containing a list of users that match your search criteria.



Step 4 Select a disabled user in the results section and click **Manage User**.



The User Record page appears.



Step 5 Select the **Approval** check box and click **Enable**.

The User Record page displays a success message.

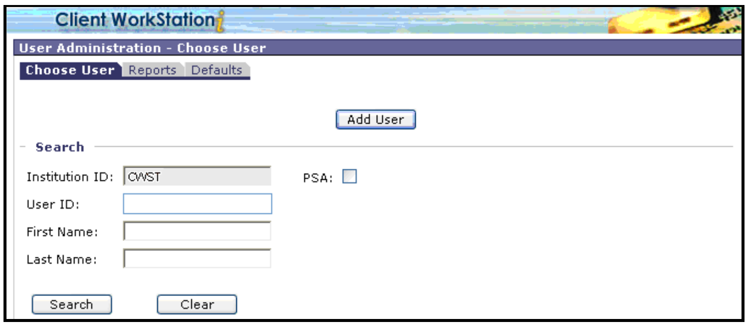
From here you can:

- Use the navigation tabs at the top of the page to view reports and defaults
- Return to the Choose User page to choose another user to view, manage, or copy

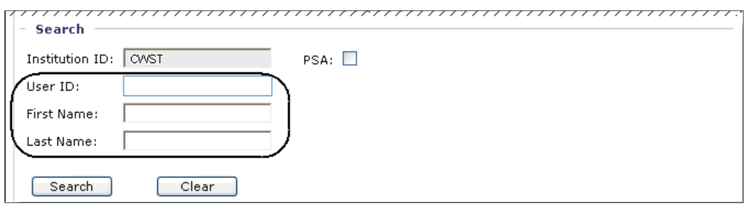
Delete User

Only PSAs and administrators having delete access can delete a user security record.

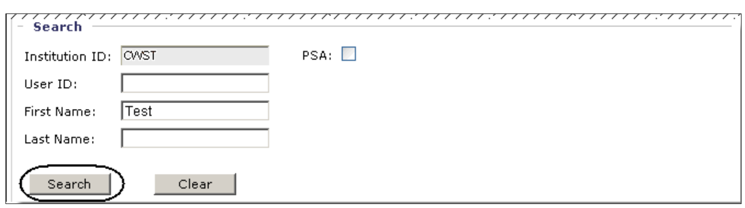
Step 1 Access User Administration (see Access User Administration, page 9). The Choose User page appears.



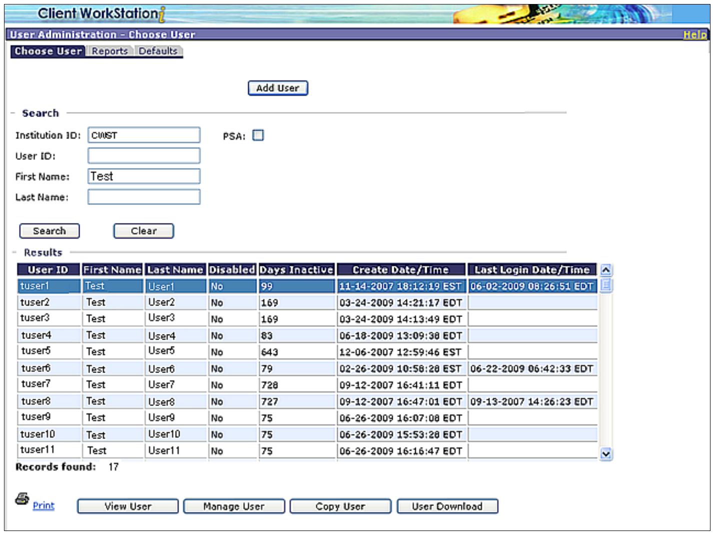
Step 2 Type the user ID, first name, last name, or any combination in these fields to search for a specific user or set of users, or leave these fields blank to view a list of all users for your institution. The institution ID is prefilled based on your user ID and cannot be changed.



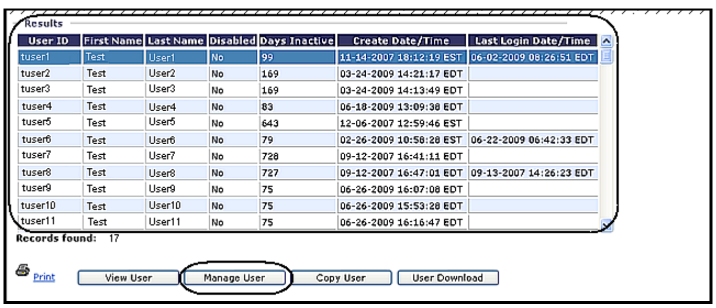
Step 3 Click **Search**.



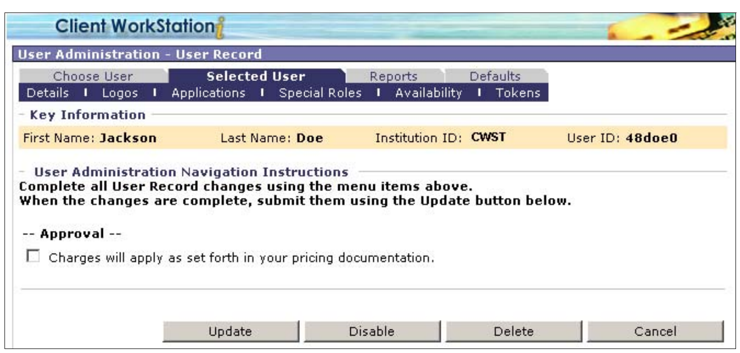
The Choose User page reappears with a Results section containing a list of users that match your search criteria.



Step 4 Select a user in the results section and click **Manage User**.

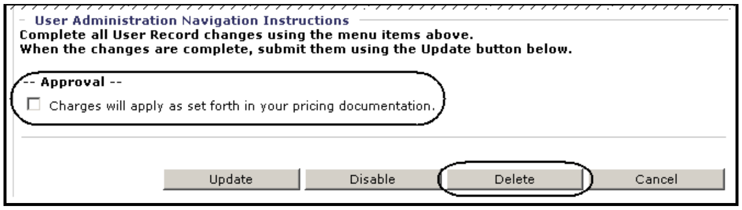


The User Record page appears.

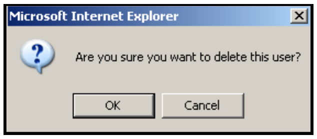


Note: The Delete button is visible only if you have delete access rights in the User Administration application.

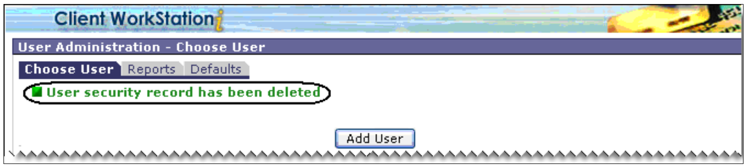
Step 5 Select the **Approval** check box and click **Delete**.



A confirmation dialog box appears.



Step 6 Click **OK**. The Choose User page confirms deletion of the selected user record.

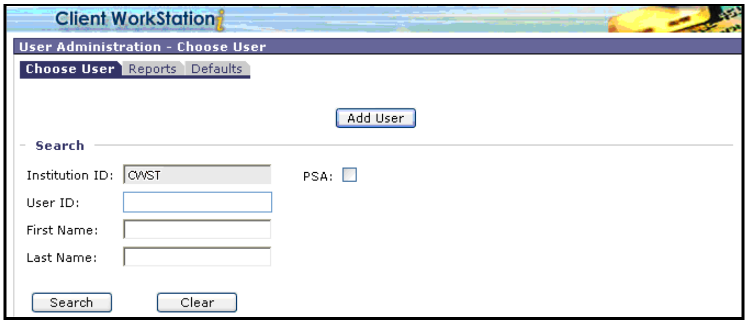


From here you can:

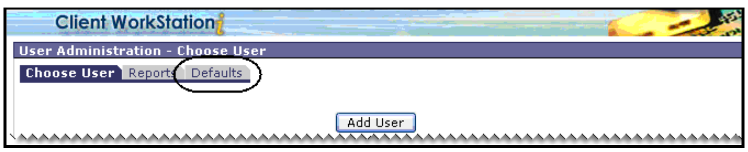
- Use the navigation tabs at the top of the page to view reports and defaults
- Return to the Choose User page to select another user to view, manage, or copy

Set Defaults

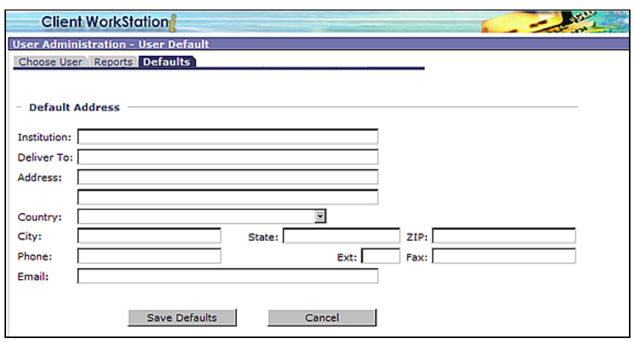
Step 1 Access User Administration (see Access User Administration, page 9). The Choose User page appears.



Step 2 Click **Defaults**.



The User Administration—User Default page appears.

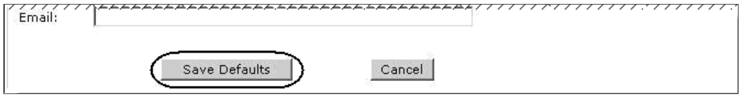


Step 3 Fill in the required information.

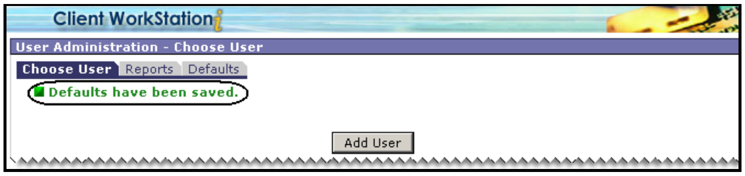
User Administration supports the following defaults:

- **Ship To**—Identifies the shipping address option that is preselected by default when ordering a token
- **Default Address**—Address that populates the shipping address fields when the Default option is selected when ordering a token

Step 4 Click **Save Defaults**.



The User Administration—Choose User page displays a confirmation message.

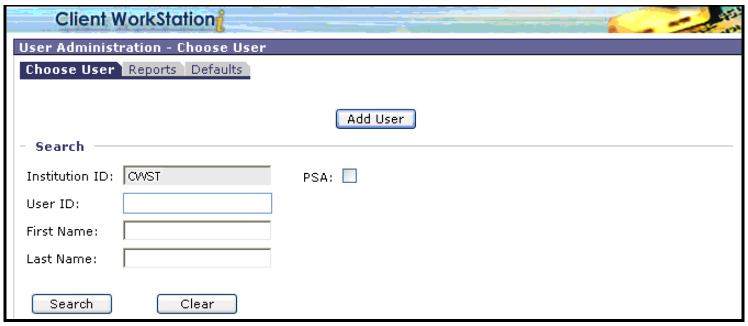


From here you can choose a user to view, manage, or copy the user record.

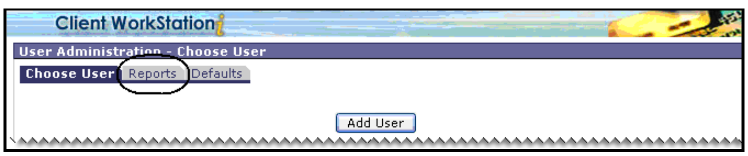
Reports

Reports show maintenance done in User Administration (user adds, deletes, and updates) and provides a status of tasks completed by EFT Solutions' security administrators.

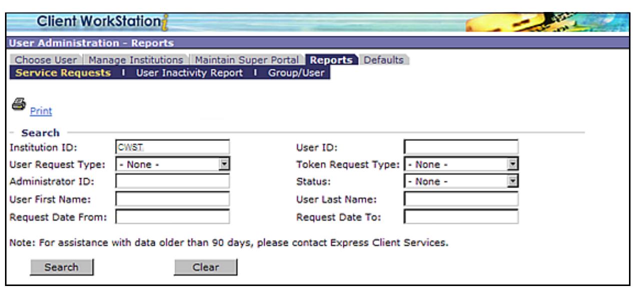
Step 1 Access User Administration (see Access User Administration, page 9). The Choose User page appears.



Step 2 Click **Reports**.



The Reports page appears with search criteria.



Note: You can choose to run a general search using the defaults, or you can enter information in one or more of the available fields to display specific maintenance done in CWSi User Administration. When choosing the print link, you will be given the search criteria information as well as the results.

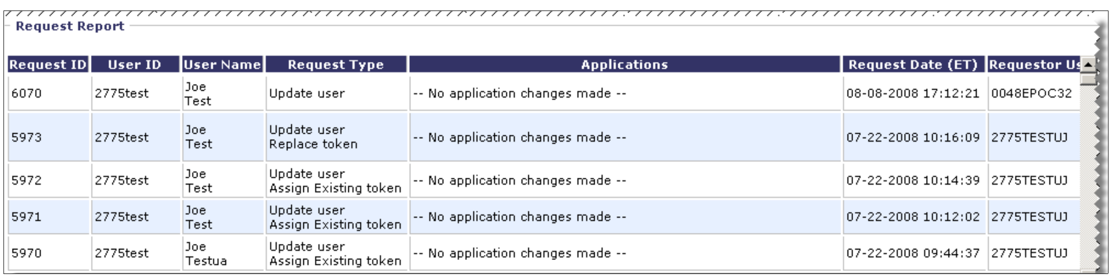
Step 3 Type any of the following required search criteria.

Field	Description
Institution ID	This is the read-only logo associated with your token ID.
User ID	Allows you to search for maintenance done to a specific user ID. If you choose to use this field, you must enter the full user ID.
User Request Type	Allows you to search for specific service request types. The field defaults to None allowing all User Request Type to be returned. List box options: • None (default) • Add User • Delete User • Update User
Token Request Type	Allows you to search for a specific kind of token request. The options available in the drop-down list depend on the User Request Type selected. The field defaults to None allowing all Token Request Types to be returned. List box options if User Request Type—None: • None (default) • Issue new token • Delete token • Replace token • Assign existing token List box options if User Request Type—Add User: • None (default) • Issue new token • Assign existing token List box options if User Request Type—Delete User: • Delete token (default) List box options if User Request Type—Update User: • None (default) • Replace token • Assign Existing token
Administrator ID	Allows you to search for maintenance completed by a specific administrator. If you choose to use this field, you must enter the full user ID.
Status	Allows you to search for specific service requests with a specific status. The field defaults to None allowing both Completed and In progress maintenance to be returned. List box options: • None (default) • Completed • In progress

Field	Description
User First Name	Allows you to search for maintenance done to user security record based on the user’s first name. If you choose to use this field, you must enter the full first name.
User Last Name	Allows you to search for maintenance done to a user security record based on the user’s last name. If you choose to use this field, you must enter the full last name.
Request Date From	This defaults to 90 days prior to the current date but can be changed to narrow the date range of the search.
Request Date To	This defaults to the current date but can be changed to narrow the date range of the search.

Step 4 Click **Search**.

The Reports page reappears with service request report information. Scroll bars allow you to view the entire report.


Request Report

Request ID	User ID	User Name	Request Type	Applications	Request Date (ET)	Requestor Us
6070	2775test	Joe Test	Update user	-- No application changes made --	08-08-2008 17:12:21	0048EPOC32
5973	2775test	Joe Test	Update user Replace token	-- No application changes made --	07-22-2008 10:16:09	2775TESTUJ
5972	2775test	Joe Test	Update user Assign Existing token	-- No application changes made --	07-22-2008 10:14:39	2775TESTUJ
5971	2775test	Joe Test	Update user Assign Existing token	-- No application changes made --	07-22-2008 10:12:02	2775TESTUJ
5970	2775test	Joe Testua	Update user Assign Existing token	-- No application changes made --	07-22-2008 09:44:37	2775TESTUJ

Field	Description
Request ID	Unique identifier for each add, change, or token request
User ID	User ID being added or changed
User Name	Name associated with user ID
Request Type	Type of action request
Applications	Applications and access rights that were added or changed
Request Date (ET)	Date and time the maintenance was done
Requestor User ID	User ID of person adding the record or making the change
Status	Current status of the request (will show In Progress until it is complete)
Deliver To	Token delivery information (applicable only when a new or replacement token is requested)

From here you can generate another report if you desire.