User Administration User Guide

October 2008

EFT

Contents

Revisions, October 2008

Section	Description
Service Requests Report, page 35.	Removed User Inactivity Report.

Revisions August 2008	
Section	**Description**
Service Requests Report, page 35.	Updated reports search feature.

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.

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 the Service Request report (see Service Requests Report, page 35).

Administrators

CWSi User Administration is a security system that allows administrators to set up and maintain user access to applications on the EFT website.

- An administrator is a user who has any combination of read, add, update, and delete access to the User Administration application.
- The primary security administrator (PSA) has the highest level of access to all applications available to your institution, and is identified on the User Summary page as *Primary Administrator: Yes*.
- Your institution can have only one PSA and should have at least one administrator as a backup.
- The PSA can only be added, updated, or deleted by an EFT security administrator. The PSA creates administrators by giving them access to the User Administration application. The PSA is the only user in your institution with the authority give that access or to manage other administrators.
- PSAs must use their tokens regularly to avoid losing access due to inactivity.

- The PSA and administrators set up and maintain all user access to applications used by your institution. They must have access to the applications themselves before they can give access to other users.
- When your institution purchases a new application, EFT will give access to the PSA, who can then give it to the other users in your institution.

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 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 lost, stolen, or defective token can be replaced. User Administration allows you to request a token replacement by updating a user security record.

See Administering User Security Records, page 12 for the process of ordering, reassigning, and replacing a token.

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. This 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 in order 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 table contains anticipated timeframes for existing Client-Central users. The timeframes apply only if accurate information is provided. Incomplete or incorrect information results in a delay.

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
New applications	CWSi applications	Effective immediately
	Message Board	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

Deletion of a Client-Central user security record takes effect immediately and the user can no longer access Client-Central.

Pricing

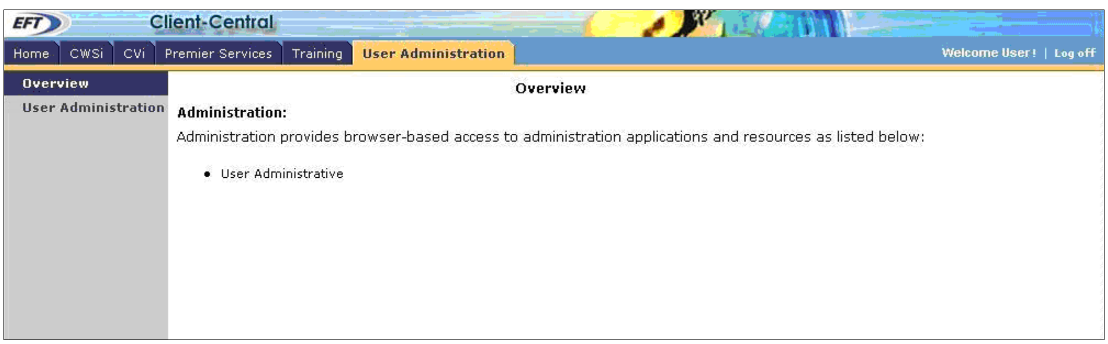
An authorized service request is submitted with the implementation of Client-Central for your institution. The service request defines the pricing structure for your institution. By accepting the statement Charges will apply as set forth in your Client-Central pricing documentation while adding, updating, 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

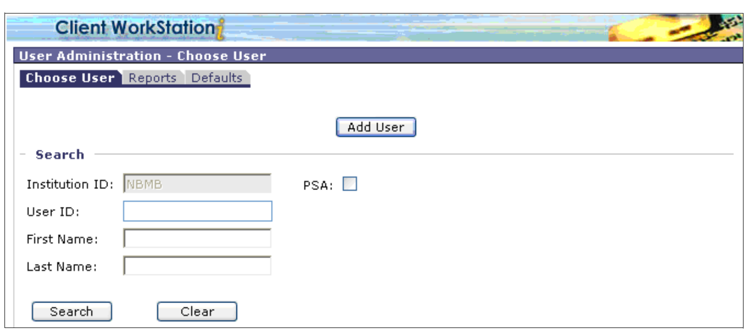
You must have at least read access to the User Administration application. To access User Administration, perform the following.

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

Step 2 Click the **User Administration** tab. The Overview page appears.



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

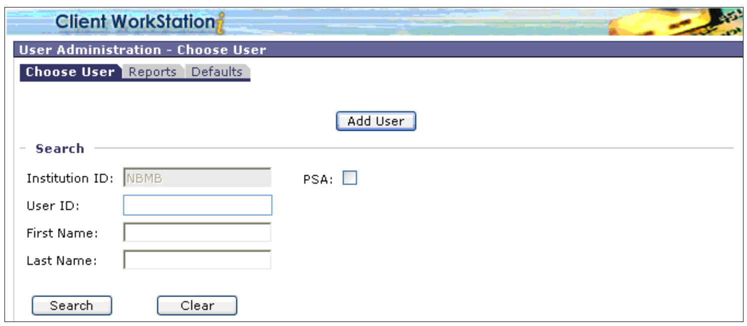


From here you can search, view, add, update, and delete user security records of the Client-Central users associated with your institution.

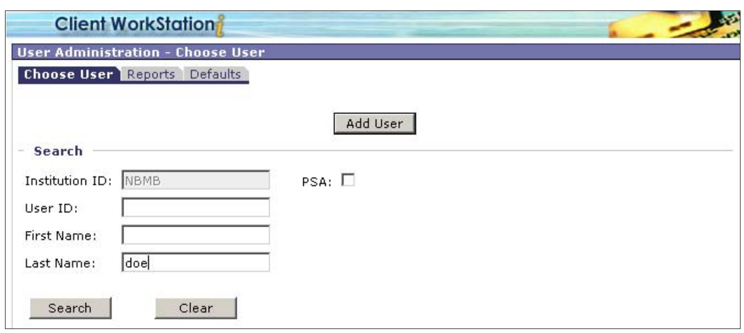
Accessing User Security Records

To view details of a user security record, perform the following.

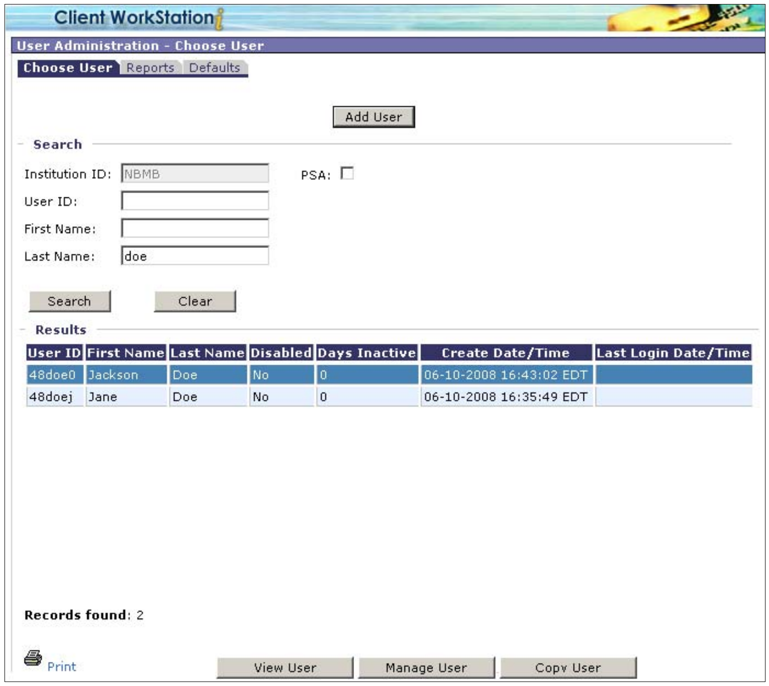
Step 1 Access User Administration and the Choose User page (see Access User Administration, page 9).



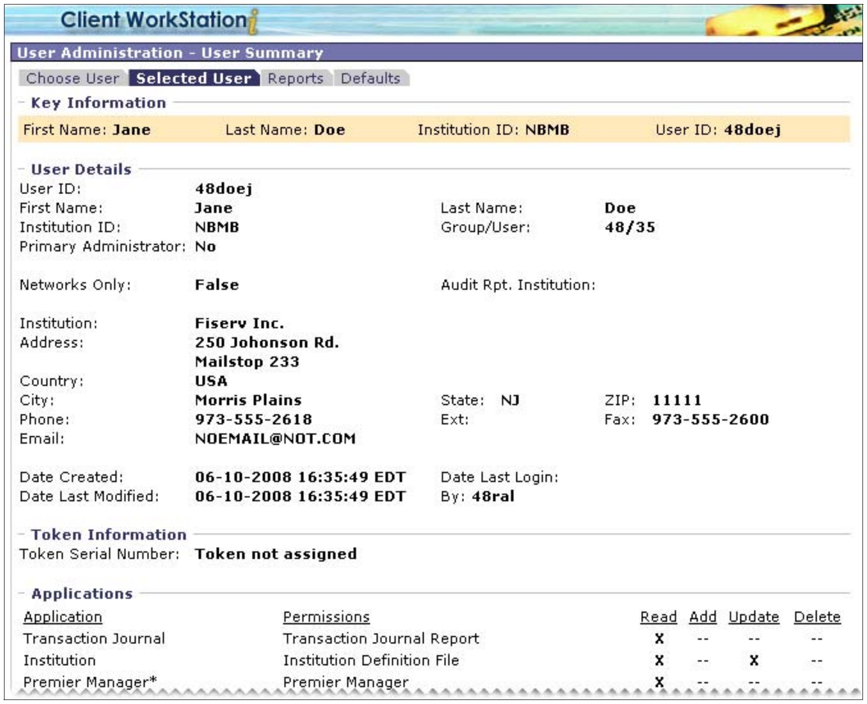
Step 2 Type relevant information in the User ID, First Name, and Last Name fields. You can use any combination of fields to enter search criteria.



Step 3 Click **Search**. Results display in table format on the Choose User page. Each row represents a user security record.



Step 4 Select a record and click **View User**. The User Summary page appears.



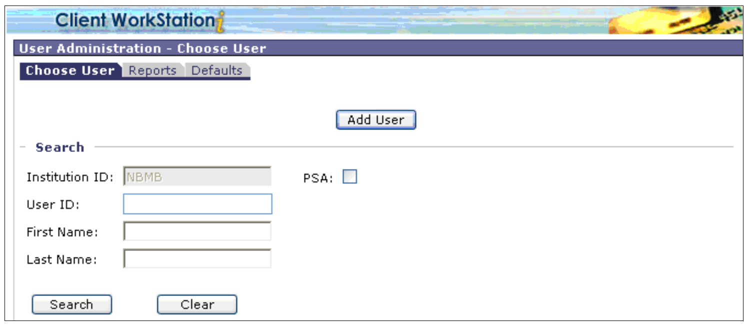
Administering User Security Records

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

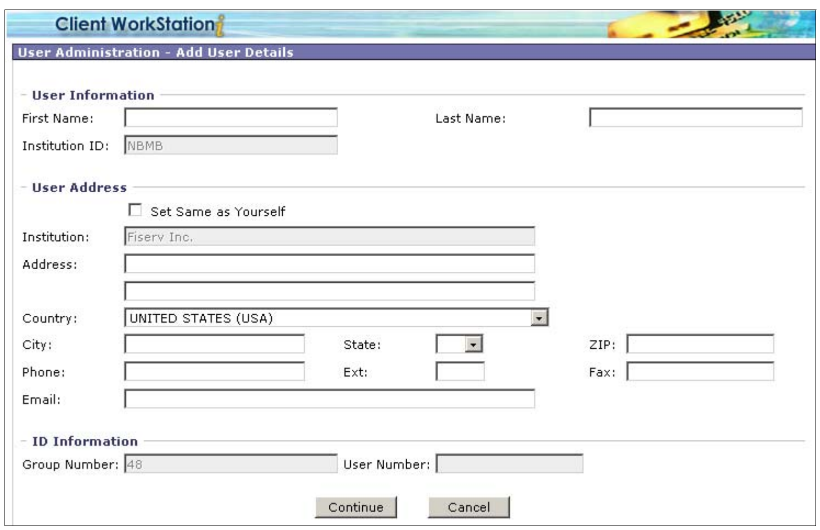
Add User

To add a new user, perform the following.

Step 1 Access User Administration and the Choose User page (see Access User Administration, page 9).

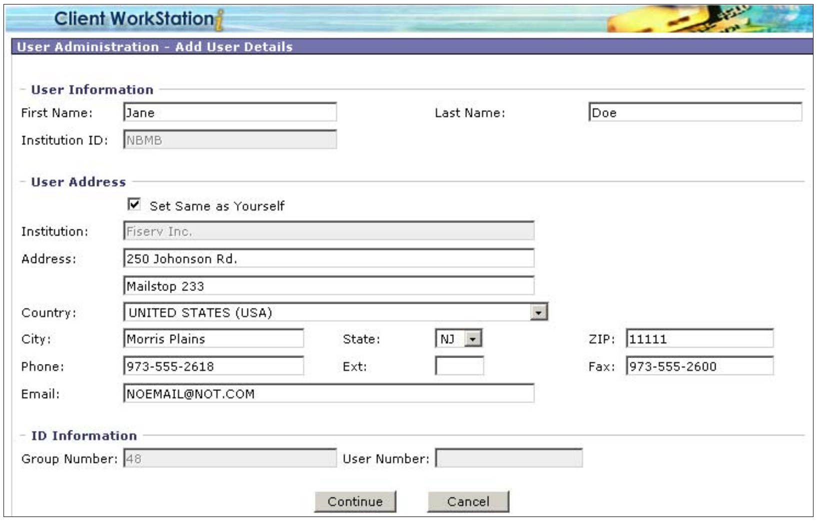


Step 2 Click **Add User**. The Add User Details page appears.

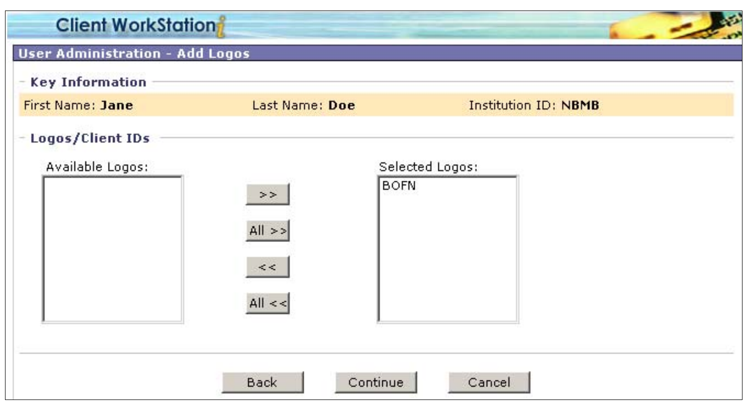


Step 3 Fill in the user name, business address, and other required information.

Selecting the Set Same as Yourself option prefills the Address field with the address defined on the security record of the administrator creating this record.



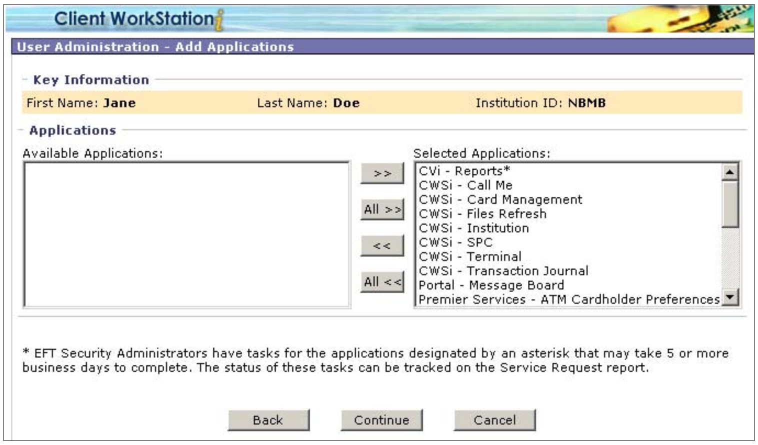
Step 4 Click **Continue**. The Add Logos page appears.



Step 5 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. Move the logos that you do not want the user to access to the Available Logos list box.

Note: 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.

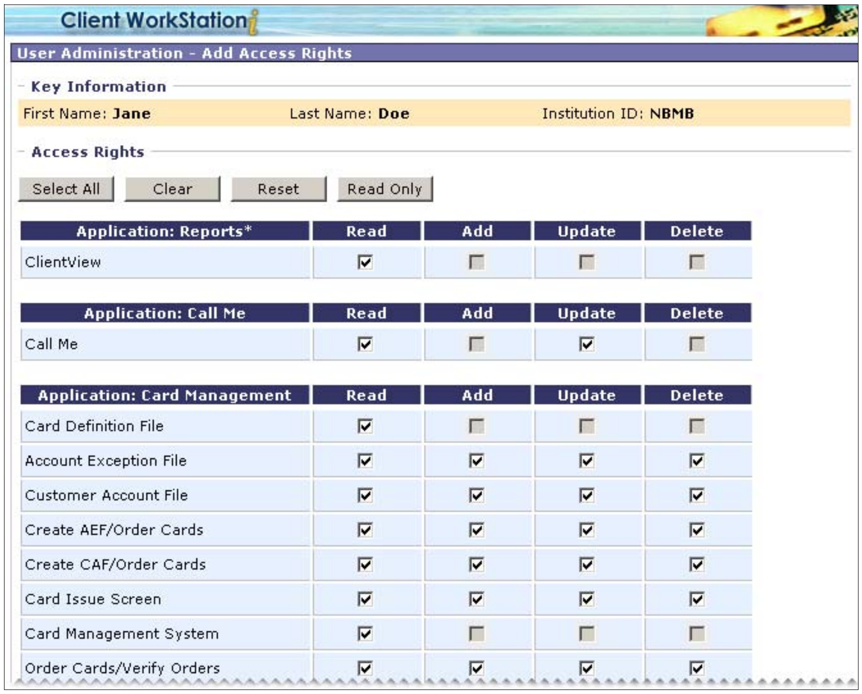


All relevant applications display in the Selected Applications list box except for the User Administration application which is reserved for administrators only.

Step 7 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.

Note: EFT suggests that you grant all users read access to the Message Board application.

Step 8 Click **Continue**. The Add Access Rights page appears and displays all access rights applicable to the selected applications.

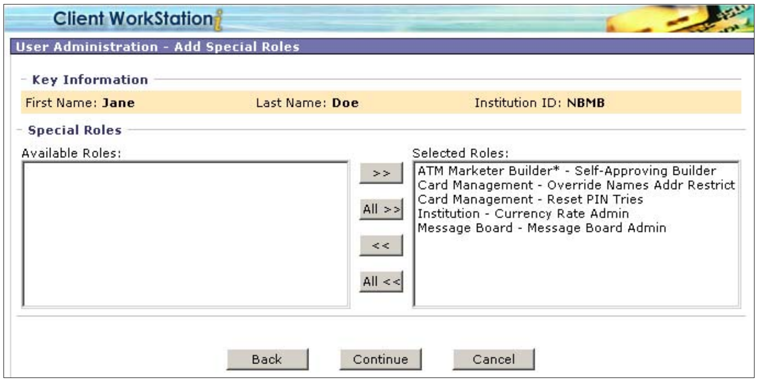


Step 9 Specify access rights for the user.

Note: 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).

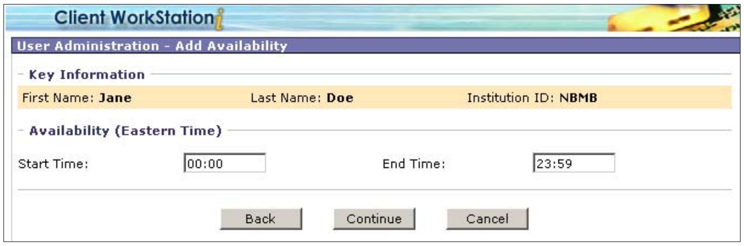
Step 10 Click **Continue**. The Add Special Roles page appears.

Note: The Add Special Roles page appears only if it is applicable to you. Otherwise, the Add Availability page appears.



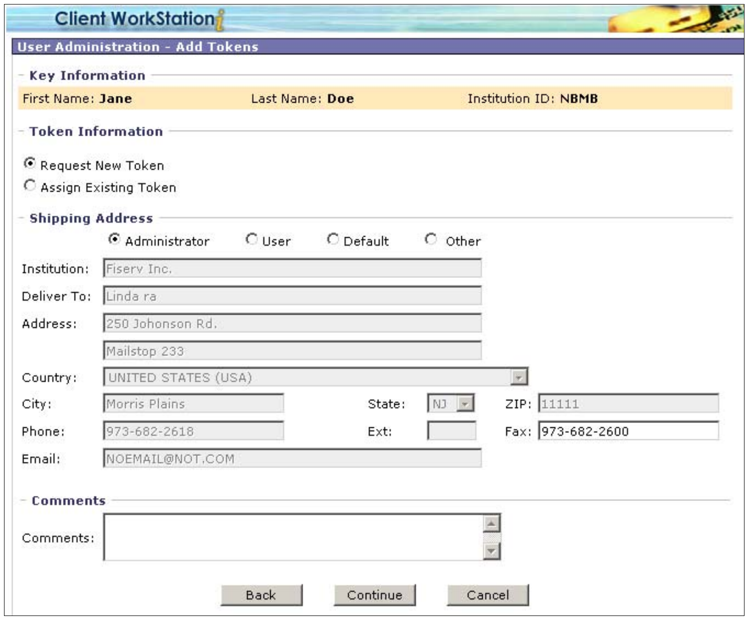
Step 11 All special roles associated with the user display in the Selected Roles list box. Move the roles that you do not want the user to access to the Available Roles list box.

Step 12 Click **Continue**. The Add Availability page appears.



Step 13 Complete the Start Time and End Time fields to specify the time limits for the user's access to Client-Central. Use U.S. Eastern time to specify time limits.

Step 14 Click **Continue**. The Add Tokens page appears.



Step 15 Click the **Request New Token** radio button to request a new token.

OR

Click the **Assign Existing Token** radio button to immediately reassign an existing token.

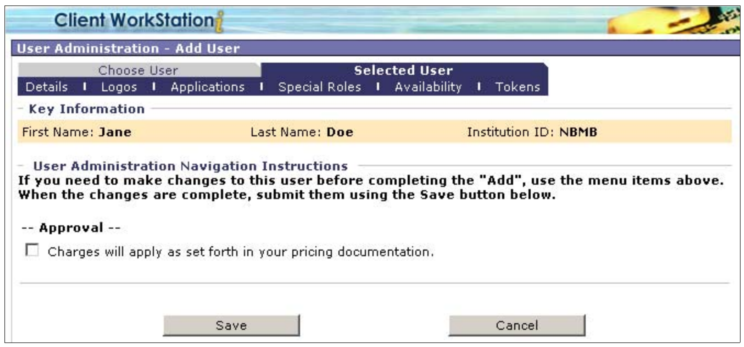
Important! You must delete the user security record of the original token owner before reassigning a token.

Step 16 Choose the shipping address option by clicking the appropriate radio button. The options are:

- **Administrator**—Prefills the address fields with the address of the administrator (the person adding this record).
- **User**—Prefills the address fields with the user address specified on the User Administration—User Record page.
- **Default**—Prefills the address fields with the address specified in the Shipping Address section of the User Administration—Defaults page.
- **Other**—The administrator may specify a different address.

Note: To specify the shipping address that displays if you select the Default option, go to the Defaults page.

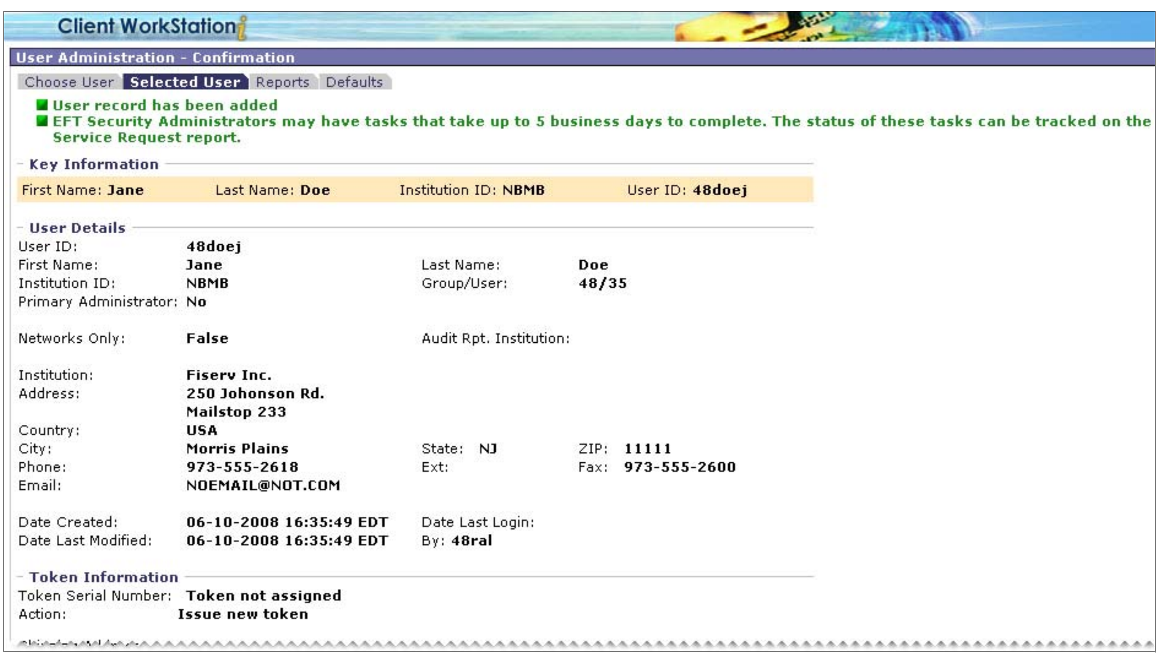
Step 17 Click **Continue**. Add User page appears.



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

Step 18 Select the **Approval** option check box

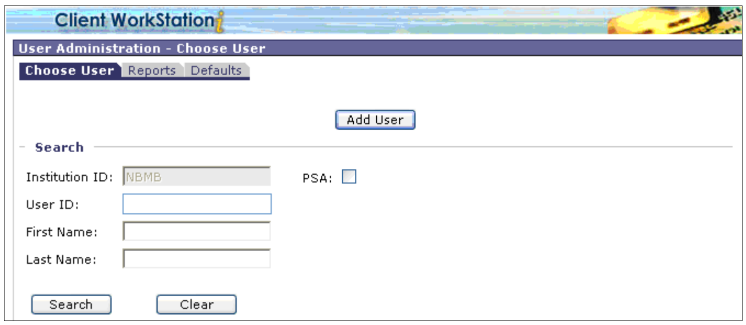
Step 19 Click **Save** to continue. The Confirmation page confirms the addition of the user record.



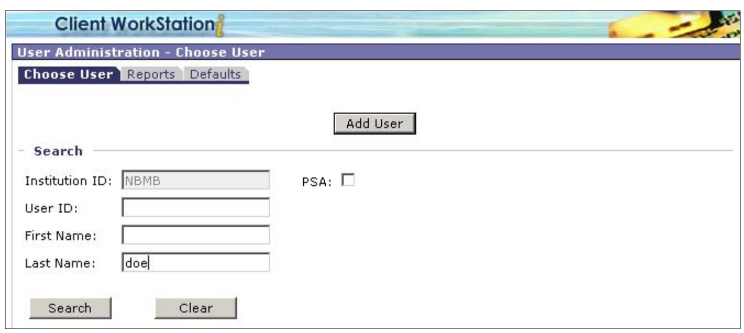
Copy User

To add a new user by copying the rights and settings from an existing user's record, perform the following.

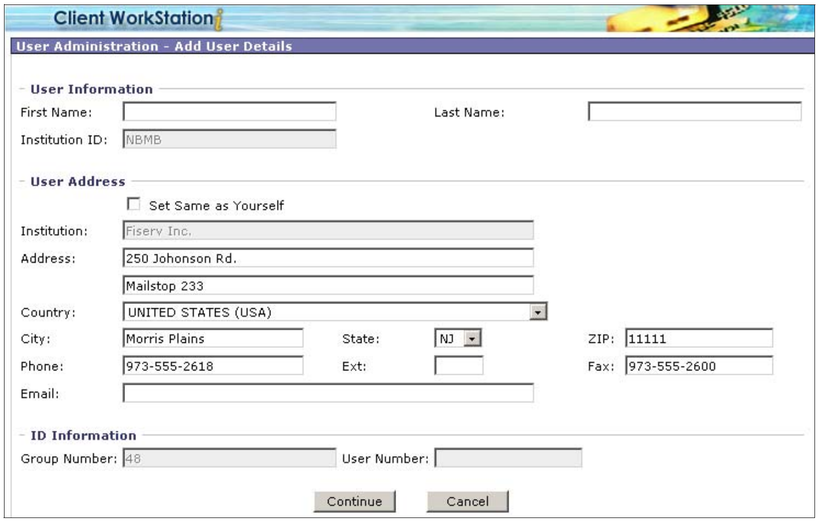
Step 1 Access User Administration and the Choose User page (see Access User Administration, page 9).



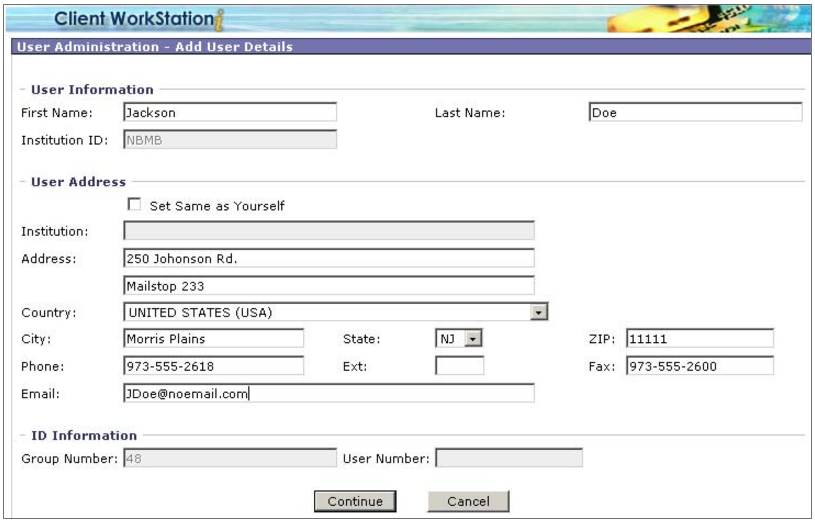
Step 2 Type relevant information in the User ID, First Name, and Last Name fields. You can use any combination of fields to enter search criteria.



Step 3 Select a user in the results section and click **Copy User**. The Add User Details page appears.

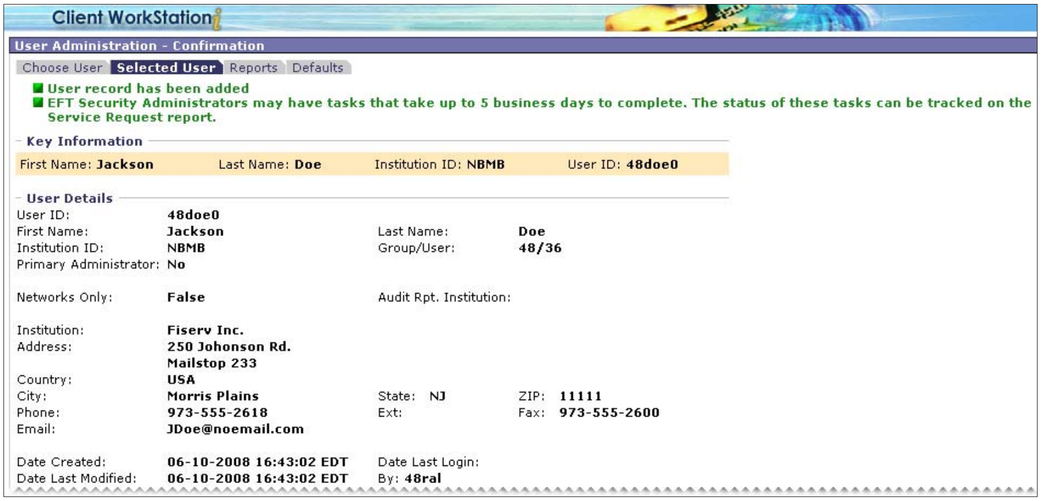


Step 4 Fill in the First Name, Last Name, Phone, Ext, and Email fields. All other information on the record is prefilled with the values from the existing user's record. You may edit the information as required.



Step 5 Complete Step 4, page 14 through Step 18, page 19 in Add User, page 13.

Step 6 Click **Save**. The Confirmation page confirms the addition of the user record.



Note: On the Tokens page, the Copied User option displays in the Shipping Address section instead of Other. You may select this option to prefill the address fields with the user address specified in the copied user's security record.

Update User

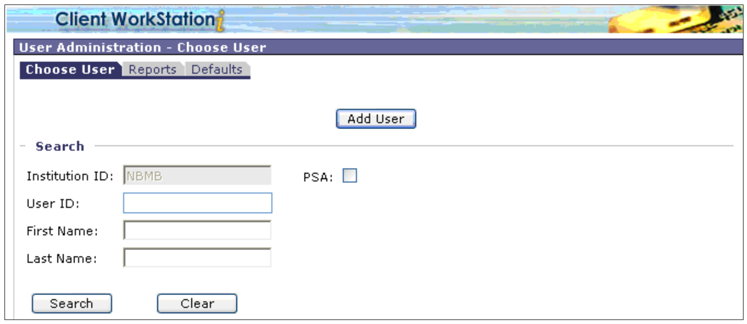
Only primary security administrators and administrators having update access can update a user security record.

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.

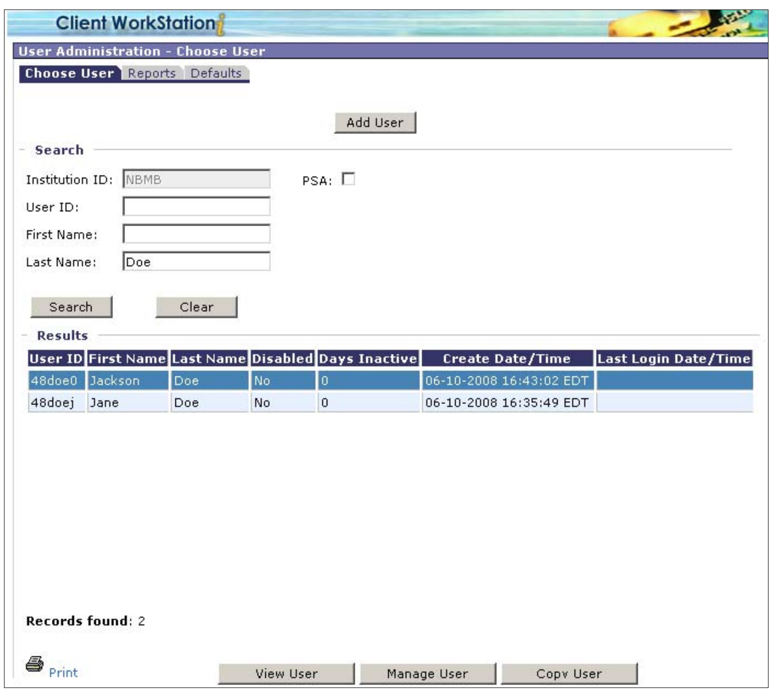
To update an existing user security record, complete the following.

Step 1 Access User Administration and the Choose User page (see Access User Administration, page 9).

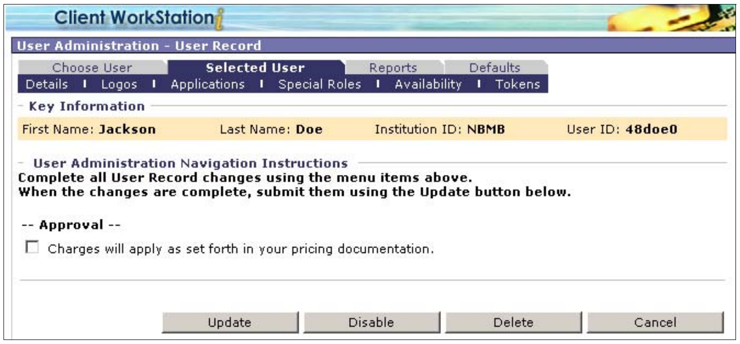


Step 2 Type relevant information in the User ID, First Name, and Last Name fields. You can use any combination of fields to enter search criteria.

Step 3 Click **Search**. Results display in table format. Each row represents a user security record.

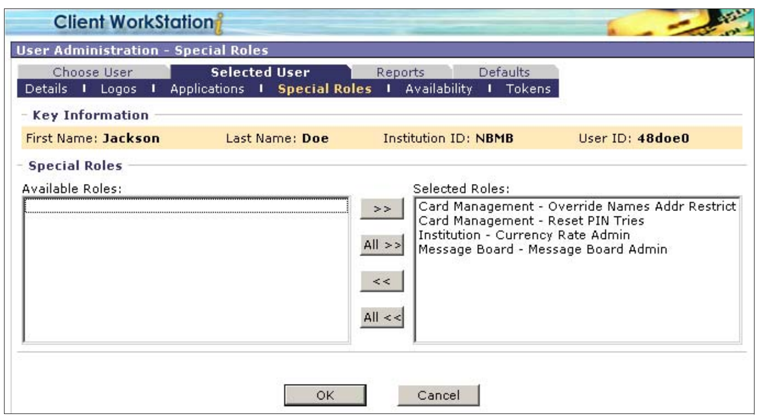


Step 4 Select a record and click **Manage User**. The User Record page appears.

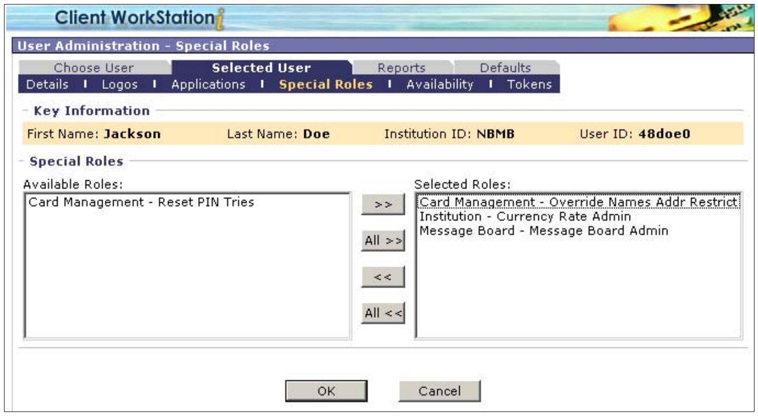


Note: The Update button is visible only if you have update access rights in the User Administration application.

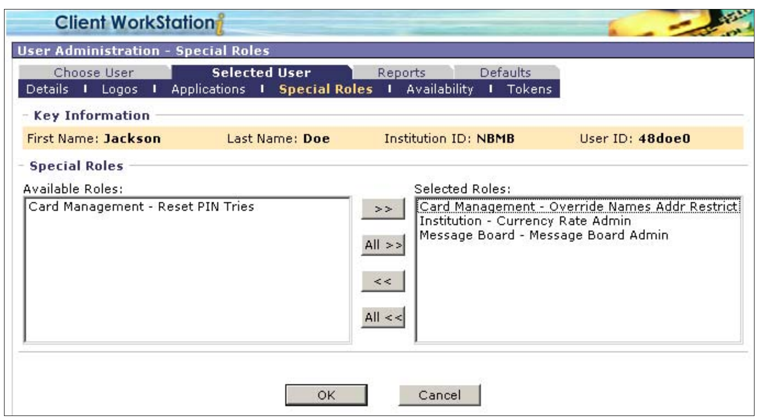
Step 5 Depending on the information you want to update, click the Details, Logos, Applications, Special Roles, Availability, or Tokens page under Selected User tab. The relevant page displays.



Step 6 Update the user information. Tokens allows you to either view the existing token serial number or request a token replacement.

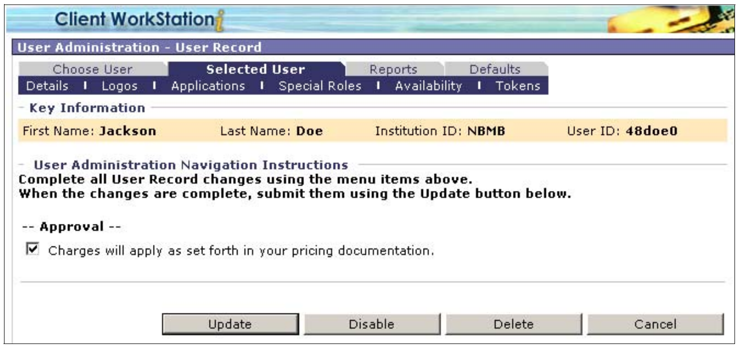


Step 7 Click **OK**. This saves the updates temporarily and returns you to the User Record page.

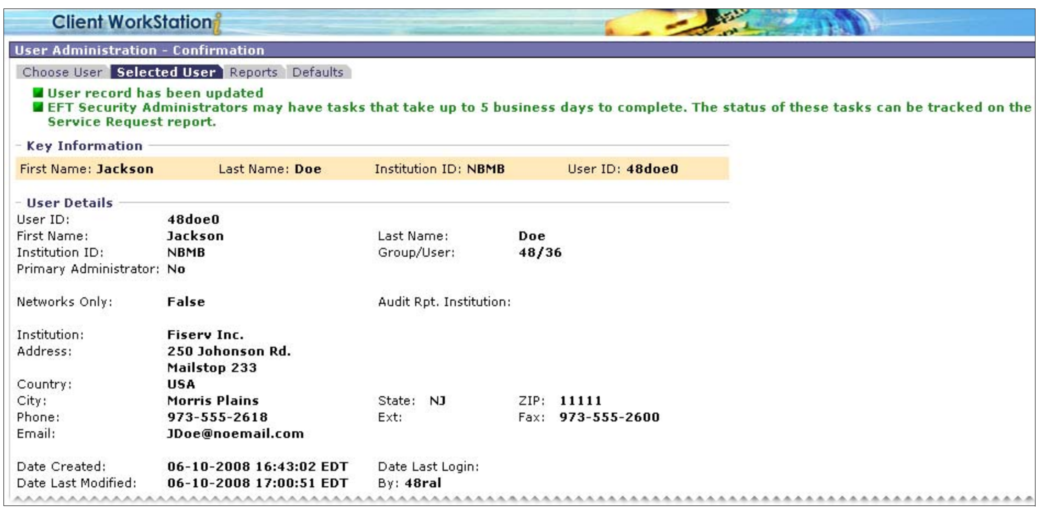


Note: The only exception is the User Administration—Applications page, where you click the Continue button to save updates temporarily and proceed to the Access Rights page.

Step 8 After completing all required changes, select the **Approval** option check box.



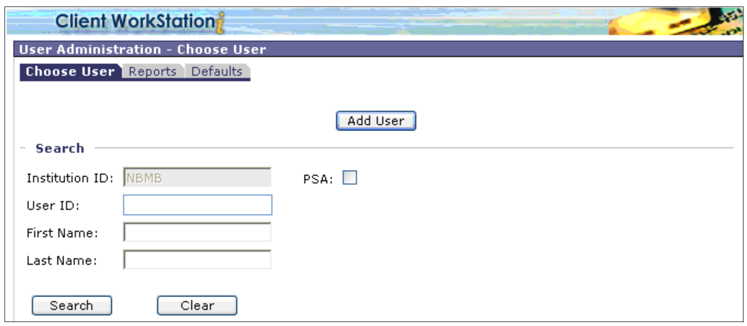
Step 9 Click **Update** to continue. The Confirmation page confirms the update. The user security record is updated and a success message displays on the confirmation page.



Disable User

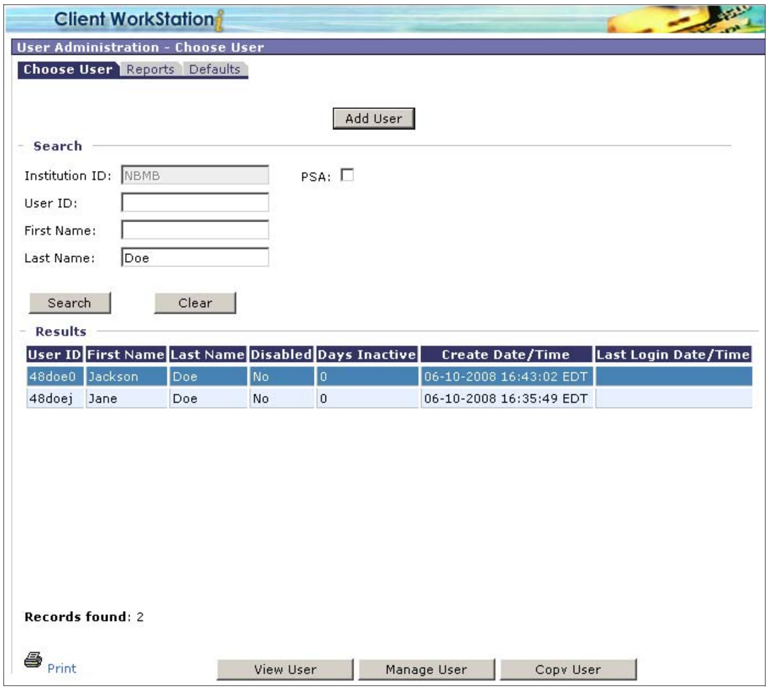
A disabled user cannot access the portal. When you disable a user you are not deleting the user ID. Use this function when you do not want a user to have access for a period of time, such as an extended medical leave or long vacation.

Step 1 Access User Administration and the Choose User page (see Access User Administration, page 9).

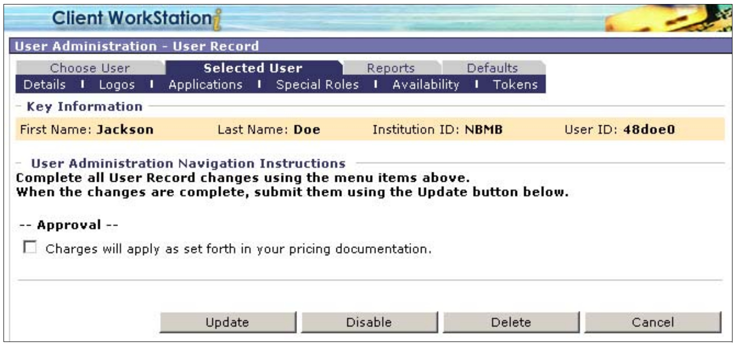


Step 2 Type relevant information in the User ID, First Name, and Last Name fields. You can use any combination of fields to enter search criteria.

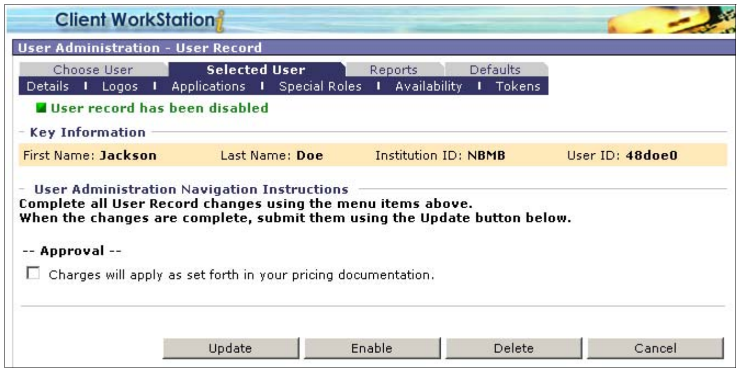
Step 3 Click **Search**. Results display in table format. Each row represents a user security record.



Step 4 Select a user 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.



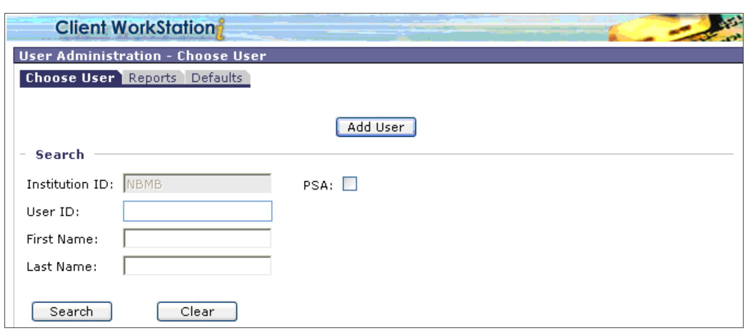
From here you can:

- 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

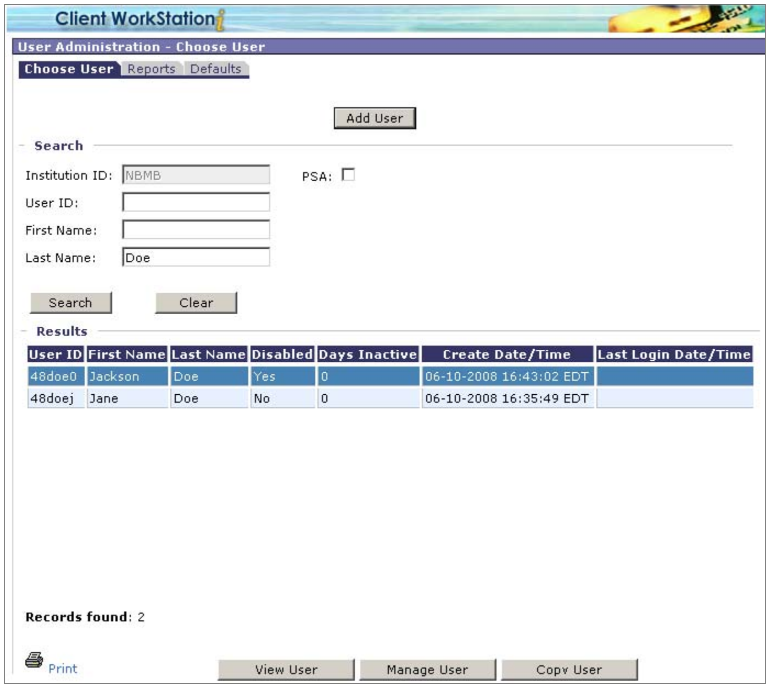
Use the enable feature to give disabled user IDs access to the portal, for example, after an employee returns from an extended leave.

Step 1 Access User Administration and the Choose User page (see Access User Administration, page 9).

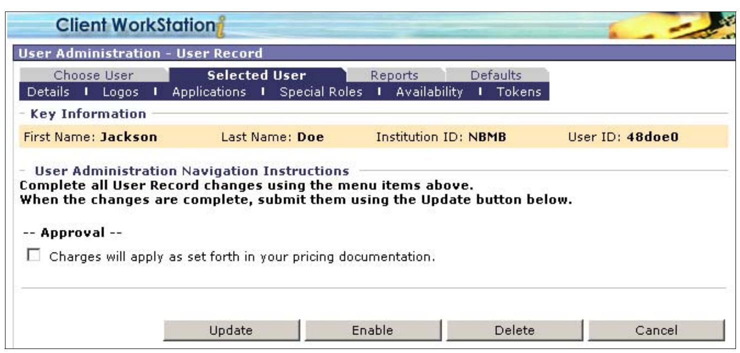


Step 2 Type relevant information in the User ID, First Name, and Last Name fields. You can use any combination of fields to enter search criteria.

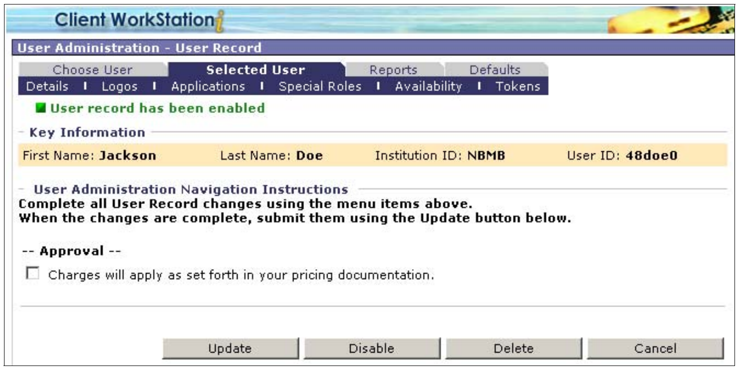
Step 3 Click **Search**. Results display in table format. Each row represents a user security record.



Step 4 Select a disabled user and click **Manage User**. The User Record page appears.



Step 5 Select the **Approval** check box and click **Enable**. The User Record page displays with the success message.



From here you can:

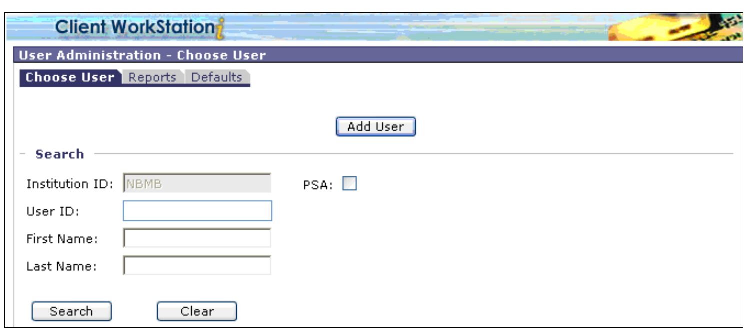
- Use the navigation tabs at the top of the page to view reports and defaults.
- Return to the Choose User page to choose another user to view, manage, or copy.

Delete User

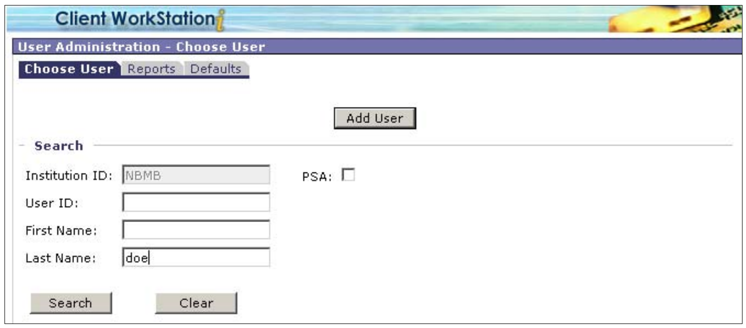
Only primary security administrators and administrators having delete access can delete a user security record.

To delete an existing user security record, complete the following.

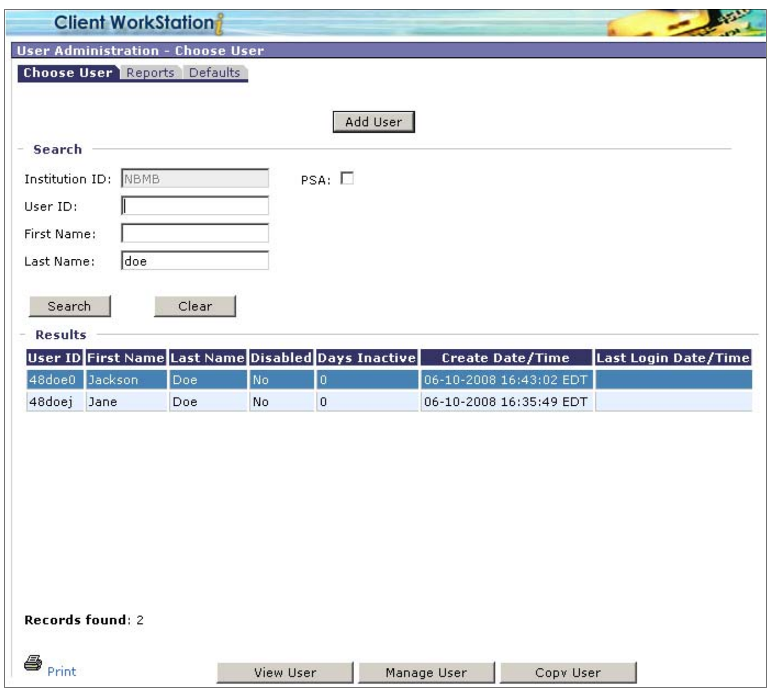
Step 1 Access User Administration and the Choose User page (see Access User Administration, page 9).



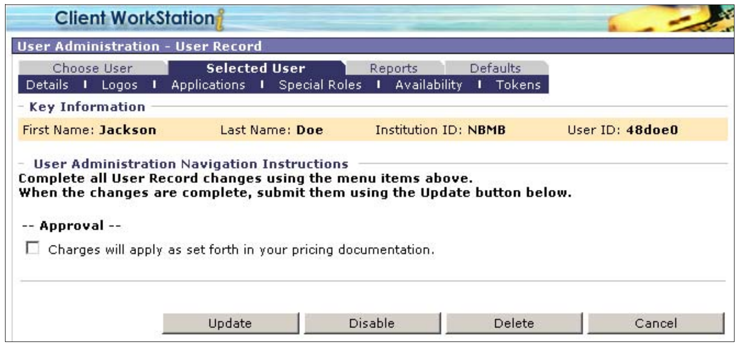
Step 2 Type relevant information in the User ID, First Name, and Last Name fields. You can use any combination of fields to enter search criteria.



Step 3 Click **Search**. Results display in table format. Each row represents a user security record.

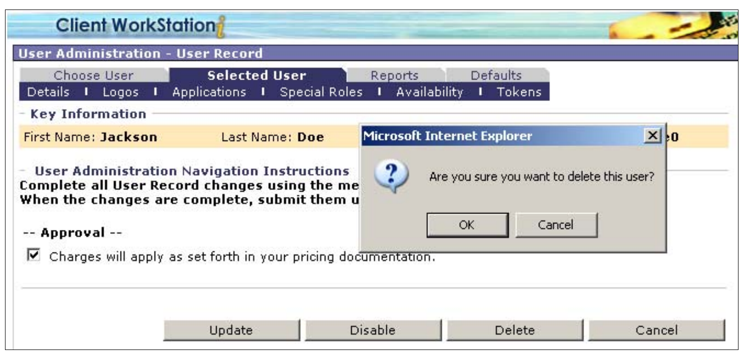


Step 4 Select a record and click **Manage User**. The User Record page appears.

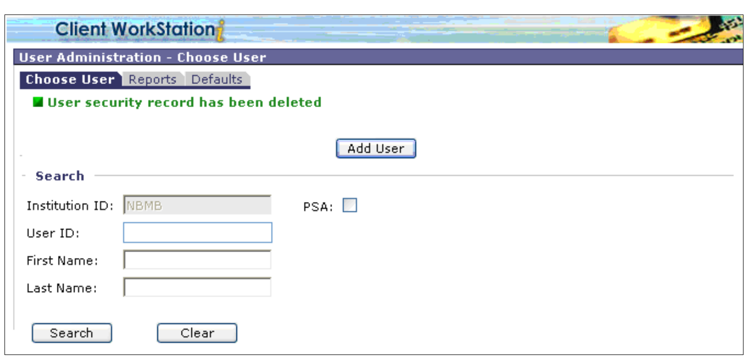


Note: The Delete button is visible only if you have delete access rights in the User Administration application.

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



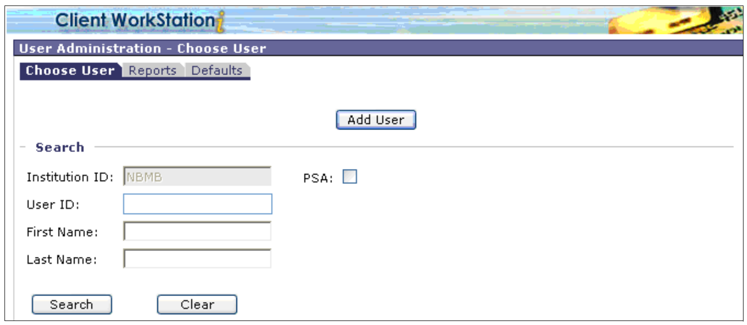
The Choose User page confirms deletion of the selected user record.



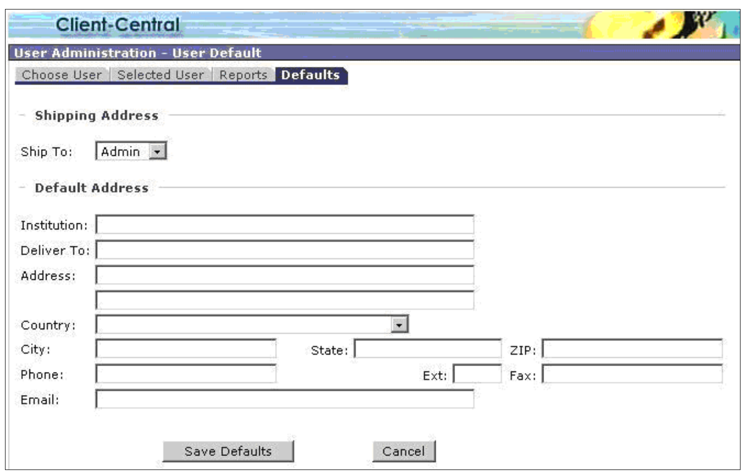
Setting Defaults

To set defaults in User Administration, complete the following.

Step 1 Access User Administration and the Choose User page (see Access User Administration, page 9).



Step 2 Click the **Defaults** tab. The User Administration—User Default page appears.

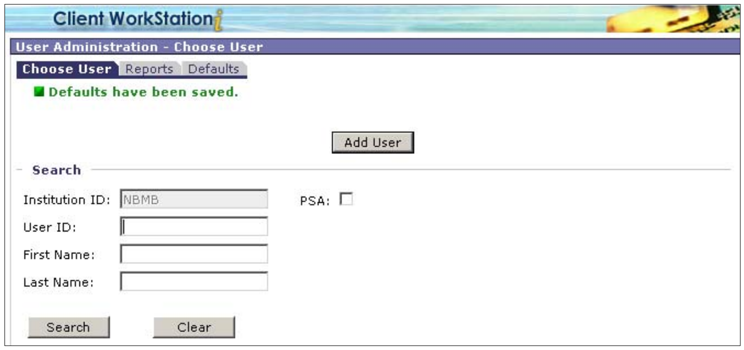


Step 3 Fill in the required information.

User Administration supports the following defaults:

- **Ship To**—Identifies the shipping address option that is preselected by default when you wish to order a token.
- **Default Address**—The address that populates the shipping address fields when the Default option is selected while ordering a token.

Step 4 Click **Save Defaults**. The User Administration—Choose User page displays a confirmation message.



Service Requests Report

The Service Requests report displays maintenance done in User Administration (user adds, deletes, and updates), and gives you a status of the tasks that are completed by EFT 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 showing the Search criteria.

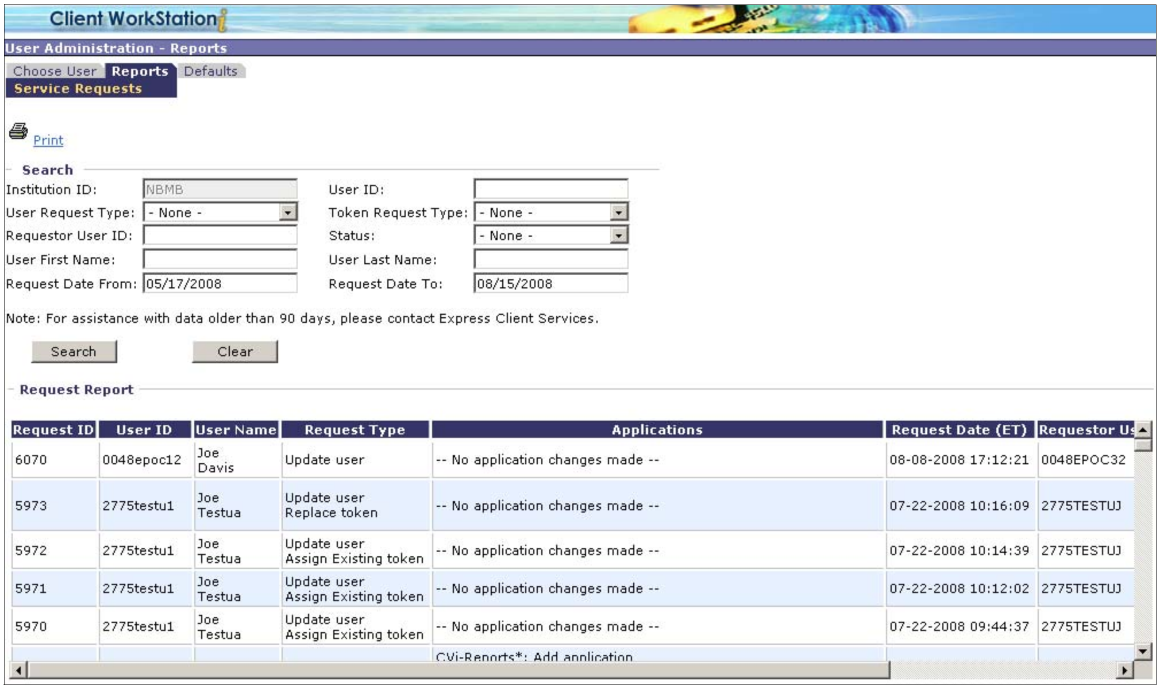
You can choose to run a general search using the defaults, or you can enter information in one or more of the available fields to display specific maintenance done in CWSi User Administration. When choosing the print link, you will be given the search criteria information as well as the results.

Step 3 Type any required search criteria.

Field	Description
Institution ID	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. Drop-down options: • None (default) • Add User • Delete User • Update User

Field	Description
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. User Request Type—None: • None (default) • Issue new token • Delete token • Replace token • Assign existing token User Request Type—Add User • None (default) • Issue new token • Assign existing token User Request Type—Delete User • Delete token (default) User Request Type—Update User • None (default) • Replace token • Assign Existing token
Requestor User 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. Drop-down options: • None (default) • Completed • In progress
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	Defaults to 90 days prior to the current date but can be changed to narrow the date range of the search.
Request Date To	Defaults to current date but can be changed to narrow the date range of the search.

Step 4 Click **Search**. The Service Requests report displays. Scroll bars allow you to view the entire report.



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.