Security Management System (SMS) Manual

2022

Table of Contents

Security Management System – SMS

The Security Management System (SMS) Reference Manual is for facility Security Managers. This manual provides information and instructions for accessing and using the OMH Security Management System (SMS).

Application Overview

The Security Management System (SMS) is a Web-based application used by facilities to authorize staff members' access to NYS Office of Mental Health (OMH) Web applications. SMS greatly improves the efficiency of adding and removing users and expanding or reducing users' access to sensitive data. By appointing a responsible person to authorize data access, each facility in the public mental health system will control access in a secure manner. A Security Manager at each facility accommodates staff turnover, reassignment, or leave from a position.

How does SMS work?

A Facility contacts the OMH Security Office (800-435-7697, select option 2) and requests a new Security Manager email be sent to their Executive Director. OMH Security sends the email, which contains information on how to register as a Security Manager. The Director forwards the Security Manager email to the staff person they want to designate as a Security Manager. The Security Manager follows the instructions in the email to self-register as Security Manager. After OMH receives and approves the electronic self-registration request, the application will issue the Security Manager a User ID and email a SecurID soft token to log-on to SMS.

What is the role of the Security Manager?

The Facility Director designates the Security Manager to use SMS to grant staff persons (from his facility) access to certain OMH applications, and the security groups within the applications. In the PCS application, the Security Manager also associates persons in the "Submitter" security group with selected units or sites. Multiple active Security Managers are allowed from each facility. A person may serve as Security Manager for two facilities, but they must register separately for each facility. A separate User ID will be assigned for each facility.

Help Desk

To resolve SMS questions or problems, contact the OMH Help Desk at (800) 435-7697, select option 2.

NOTE: **Before** contacting the OMH Help Desk, please refer to the instructions provided in this manual.

System Requirements

SMS is accessed only with Internet Explorer. The system does not work properly with other browser applications, e.g., Mozilla or Firefox.

NOTE: Pop-Up Blockers must be turned off or uninstalled for the SMS application to function properly. Examples of pop-up blockers are: Yahoo Toolbar, Google Toolbar and MSN Toolbar. For help turning off pop-up blockers, please contact the OMH Help Desk at (800-435-7697, select option 2).

Token Activation and Pin

Signing into SMS via Web Salute

Individuals granted access to Web Salute in the Security Management System (SMS) will be assigned an OMH User ID and emailed an RSA token.

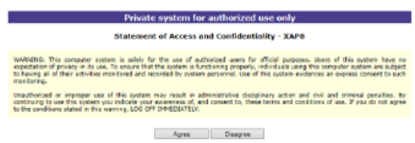
NEW YORK STATE | Office of Mental Health

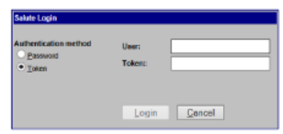
WEB SALUTE Login

Individuals granted access to Web Salute in the Security Management System (SMS) or Aurora will be assigned an:

1. OMH user ID and;
2. RSA SecurID security token; there are two types of security tokens — a physical "hard" token and a software "soft" token".

The user can then follow the steps outlined below to login to Web Salute.

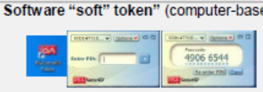




❶ Go to the website: https://mhprovider.omh.ny.gov/websalute/

❷ Click Agree.

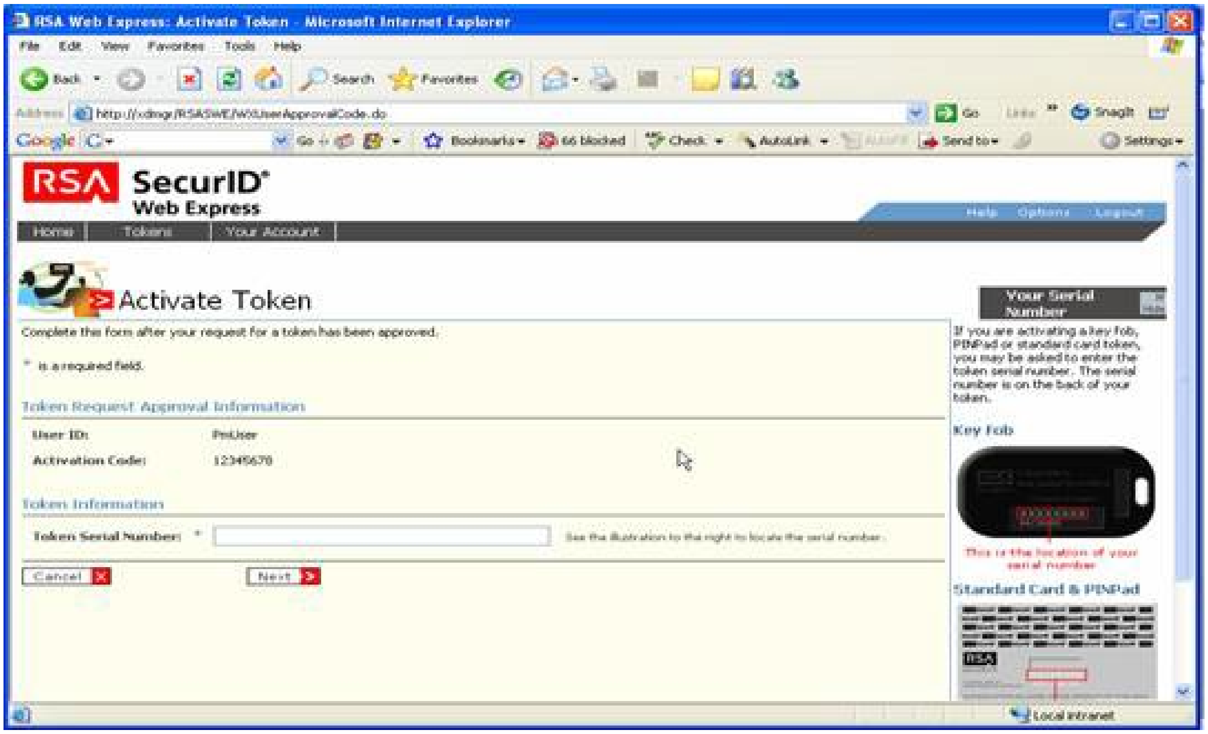
❸ When the Web Salute login page appears, enter your OMH-issued user ID and passcode. The passcode requires a security token; use the table below as a guide to determine your passcode, depending on the type of security token you have and whether it is the first time you are logging in.

	Physical "hard" token	Software "soft" token" (computer-based)
	 (looks like a keychain)	
How to find token	Contact the OMH-Helpdesk to verify delivery status	*If installed:* Search computer for "RSA SecurID Token" software. *If not installed:* Search inbox to locate token email and installation instructions sent from OMH Security at this address: Information_Security_Office@omh.ny.gov.
First time login	1. Enter *only* the 6 digits on the token screen in the passcode box. 2. Follow the instructions to create a 4-digit PIN and proceed to log into the application.	1. Open the RSA SecurID Token application. Leave the "Enter PIN" field empty and click to generate a passcode. An 8-digit passcode will appear. 2. Press Copy on the token. 3. Return to the Web Salute login page, right click in the passcode box, select "Paste," and then click Continue. 4. You will be prompted to create a PIN; follow the instructions on the screen to set your PIN. 5. After you have successfully created your PIN, return to the RSA SecurID token, and click Re-enter PIN. 6. Enter your PIN in the 'Enter PIN' box of your RSA SecurID token and click to generate a passcode; wait for the passcode numbers to change. 7. Press Copy the token, return to the Web Salute login page again, right click in the passcode box, select "Paste," and then click Continue.
Subsequent login	Enter your 4-digit PIN *plus* the 6 digits on the token screen in the passcode box.	Enter your PIN in the RSA SecurID token to generate a passcode and copy and paste this generated passcode into the passcode box of the Web Salute login page.

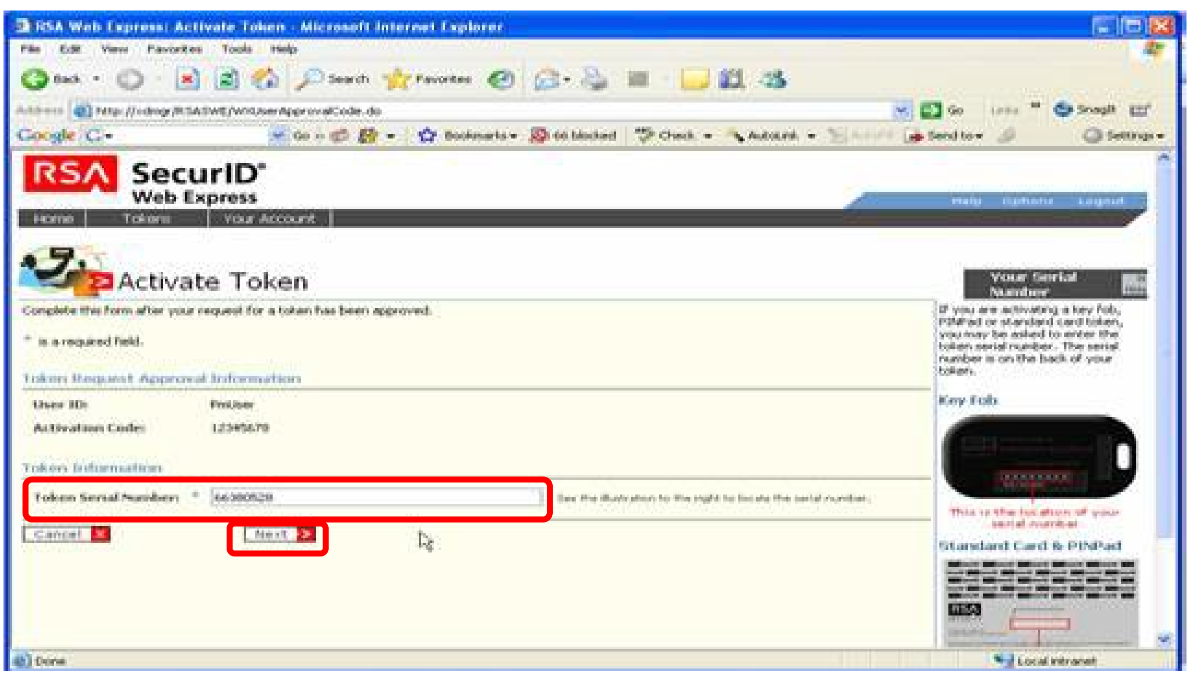
For assistance troubleshooting login issues, contact the ITS Helpdesk: Phone: 518-474-5554 then follow prompt instructions
E-mail: Non-state employees - healthhelp@its.ny.gov; State employees - fixit@its.ny.gov

To activate your own Token Using RSA Deployment Manager

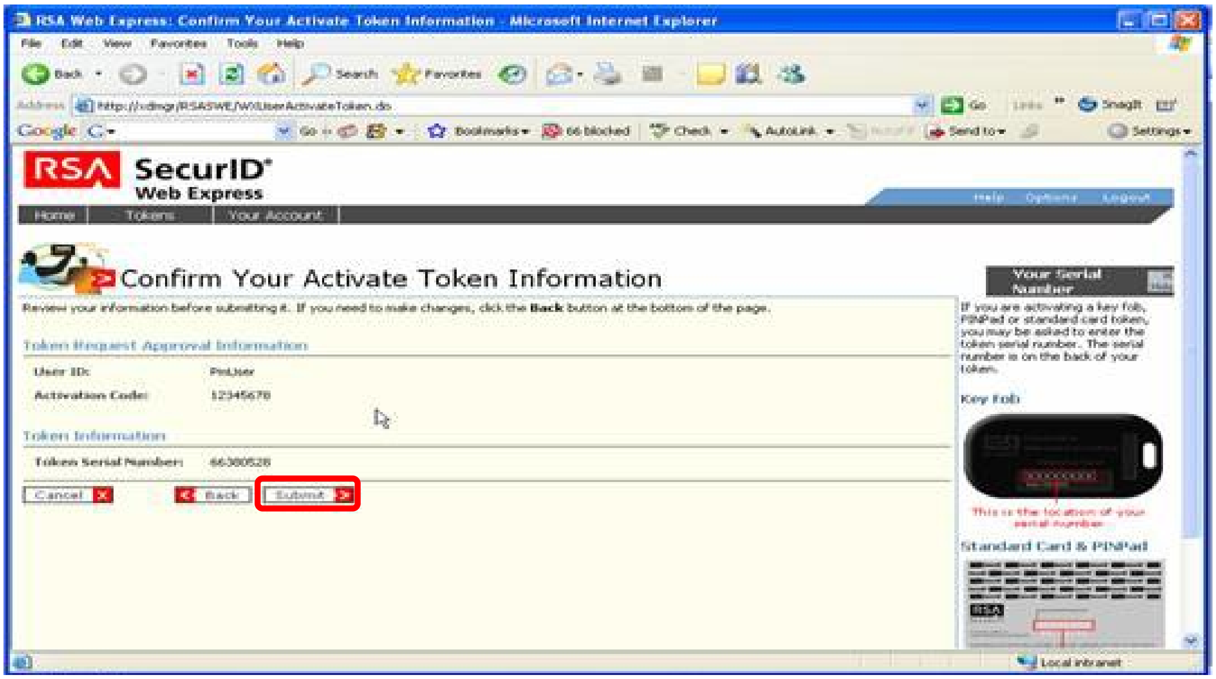
After successfully registering as a Security Manager, the user will receive an email with instructions on how to activate the SecurID token.



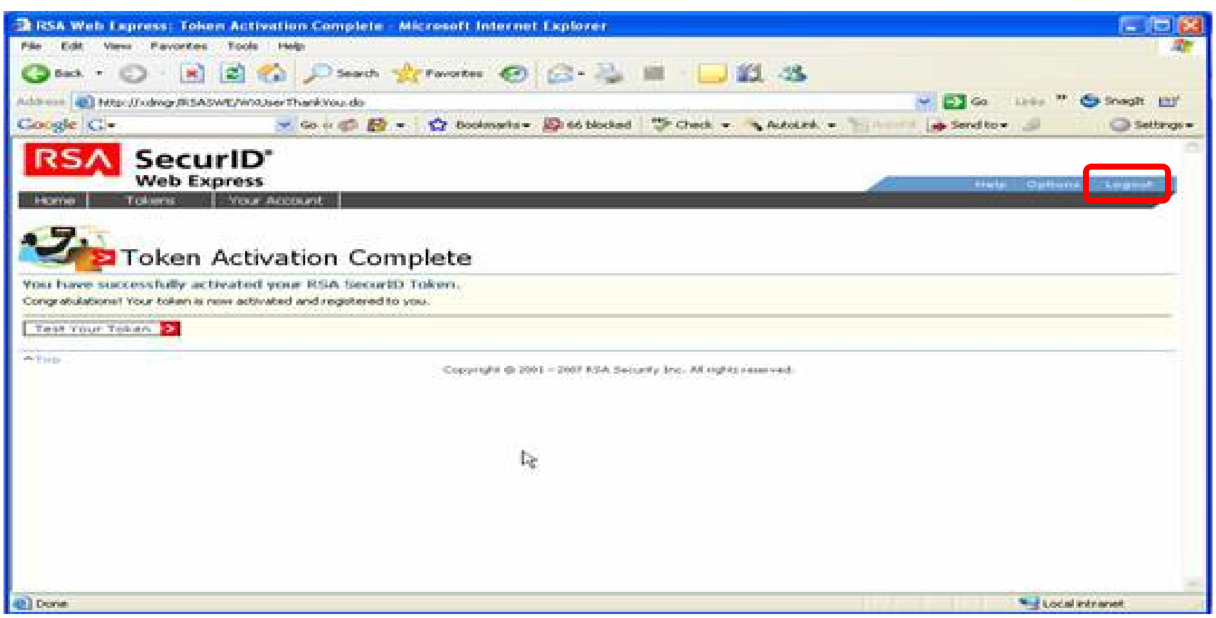
Enter the serial number imprinted on the back of the token in the "Token Serial Number" field and, click "Next". The token serial number is typically 8 or 9 digits long.



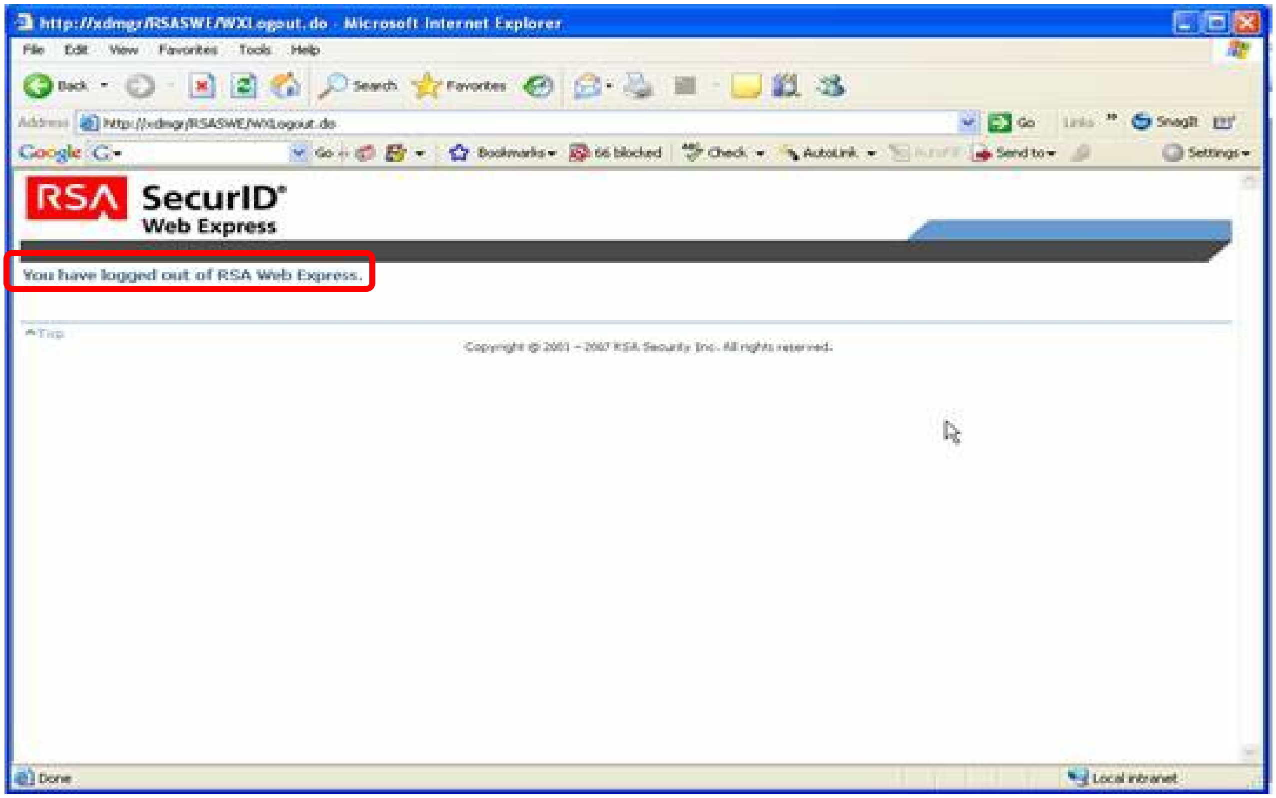
On the "Confirm Your Activate Token Information" page, make sure the User ID and the serial number are correct, and click "Submit".



The following screen displays, noting “Token Activation Complete.” On the "Token Activation Complete" page, click the "Log-out" link on the top right side of the page.



The following page will display noting “You have logged out of RSA Web Express.”

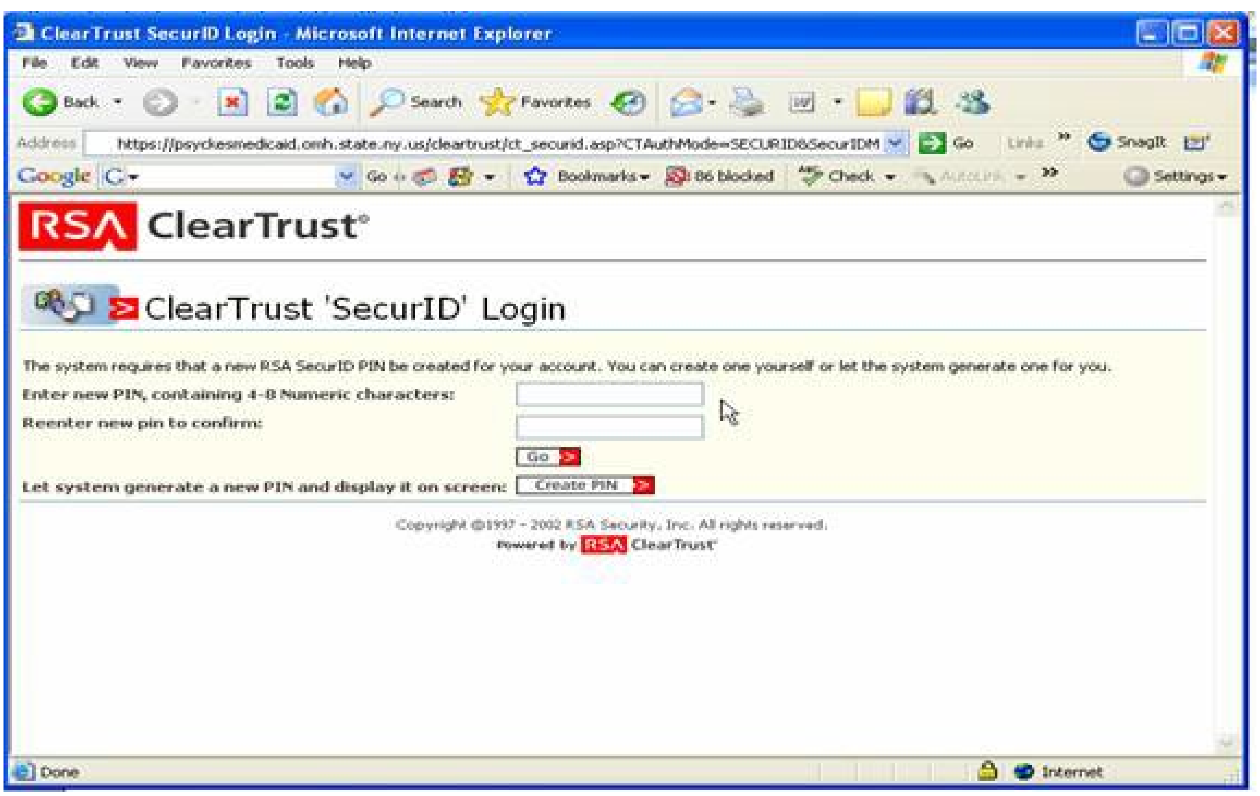


This completes the "Token Activation" process.

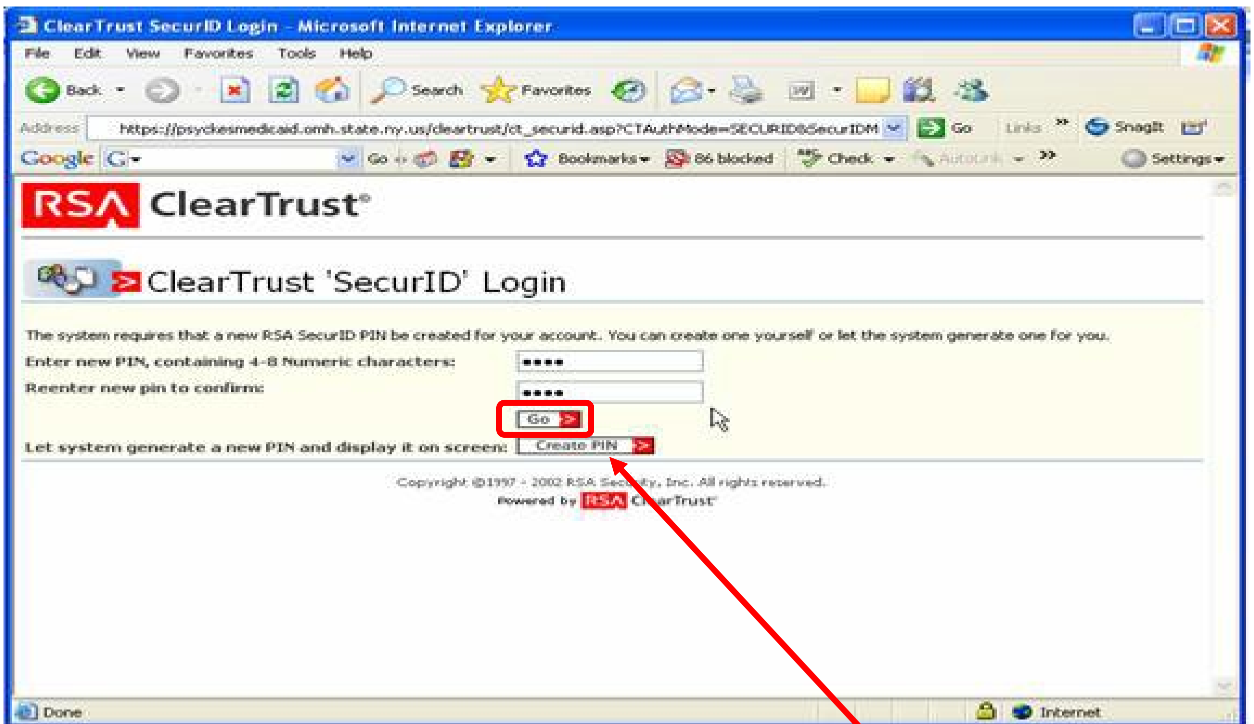
Create PIN

The next step is to create a Personal Identification Number (PIN). Each user must set their own PIN. To start the process, navigate to https://www.omh.ny.gov/omhweb/sms/, enter your User ID in the "User ID" field, and in the "Password or Passcode" field, enter only the 6-digit code displayed on the token.

The following "ClearTrust 'SecurID' Login" page displays.



You can either enter a 8-digit Personal Identification Number (PIN) you have selected or select the option for the system to generate a PIN. The PIN is used with the token to sign-on to and access ClearTrust-protected OMH Web applications. The following is an example of the screen you will see when you select **your own 8-digit PIN**. After clicking the "Go" button, you will be prompted to wait for the number on the token to change, and then enter the new PIN followed by the refreshed token code. If you choose your own PIN, you can skip the next two pages of instructions and proceed to "First-time Log-In."



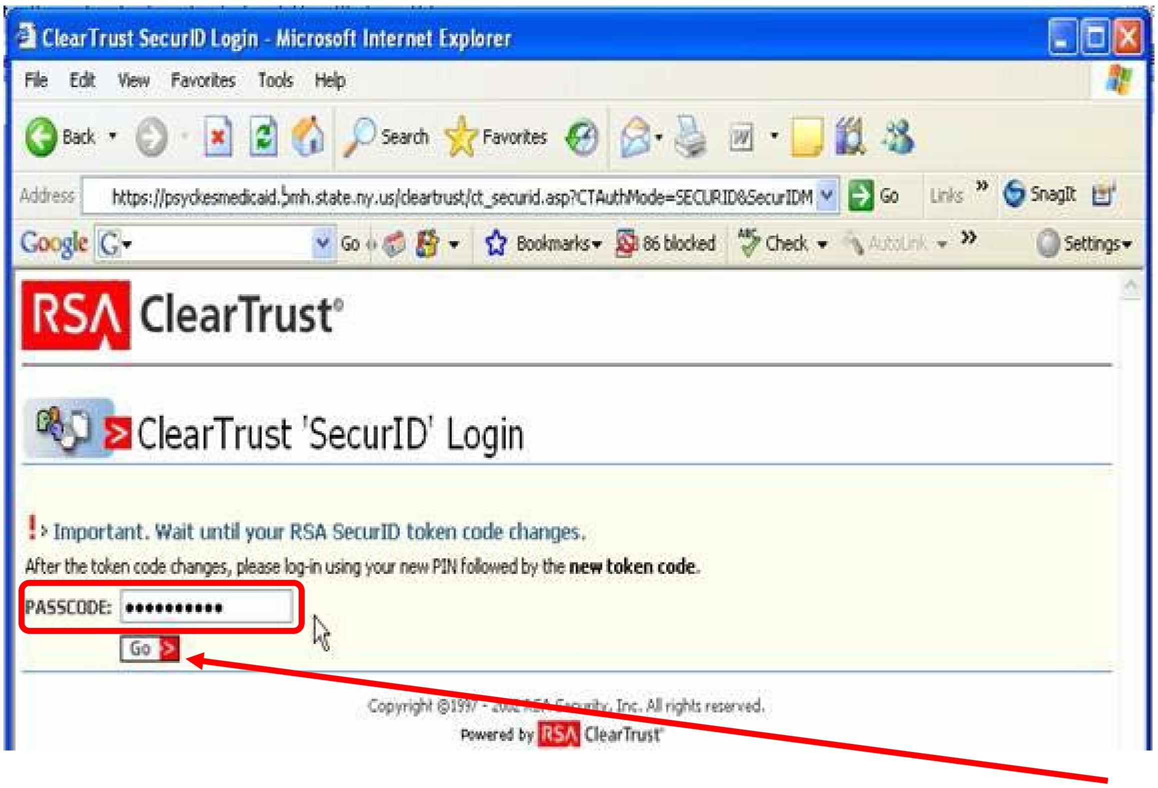
If you choose to let the **system generate a new PIN**, click the "Create PIN" button and the following page displays. You are given the option to proceed (the "Yes" option) or to return to the previous screen (the "No" option) to assign your own PIN. To have the system generate the PIN, you should select option "Yes" and click the "Submit" button.

ClearTrust displays the system generated PIN on a page as shown in the following screen print. You should write down or memorize your PIN. It will be needed to complete the activation process.

First-time Log-In

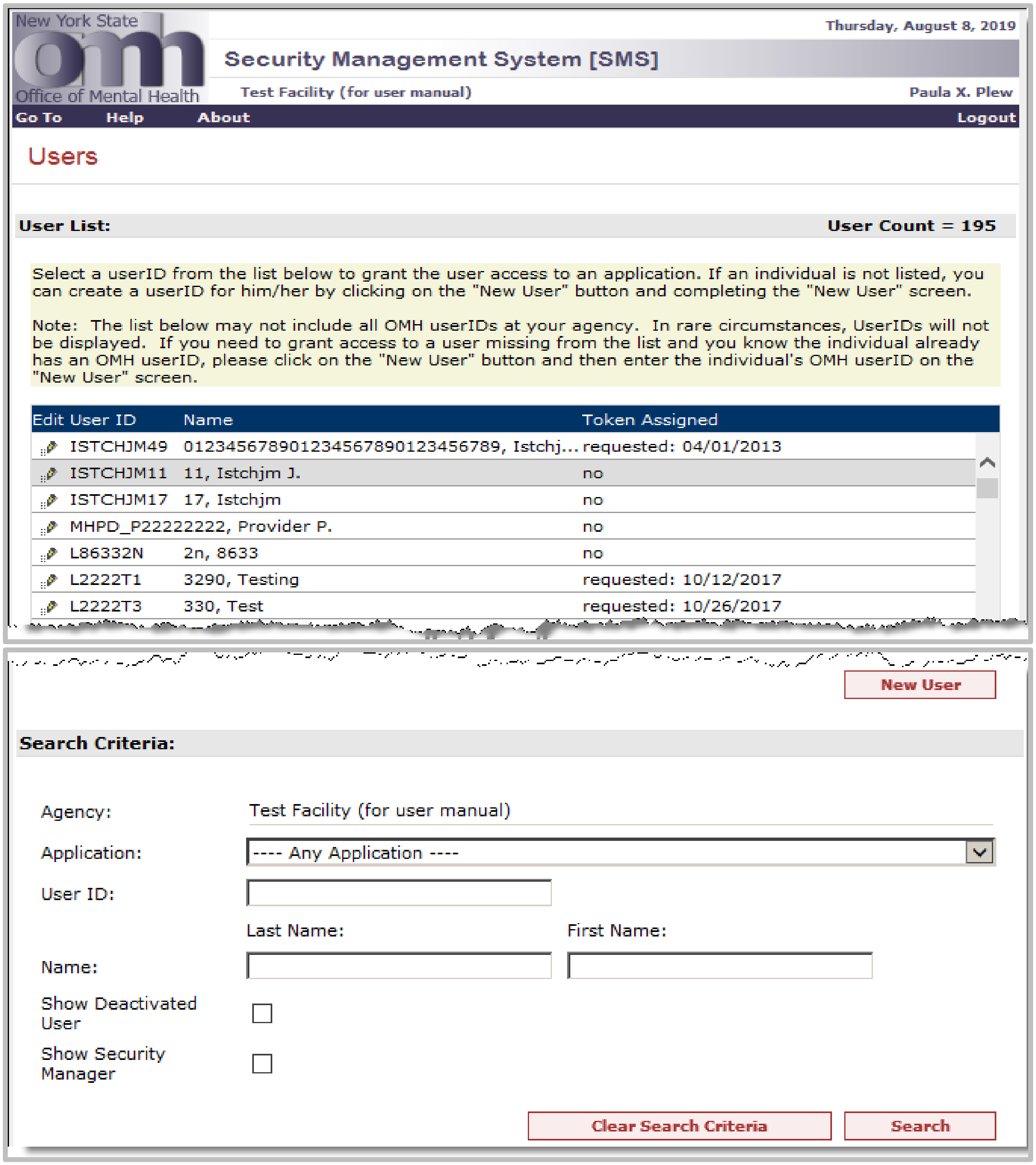
After obtaining your self-selected or system generated PIN, the following ClearTrust Login page displays.

It is important to wait for the 6-digit code on the token to update before proceeding. After the token code changes, enter the new PIN in the Passcode field followed immediately (with no embedded spaces) by the 6-digit code displayed on the token.



After entering the new PIN and 6-digit token code in the Passcode field and clicking the "Go" button, the User List page will display. You have successfully logged-in with your Secure ID Passcode.

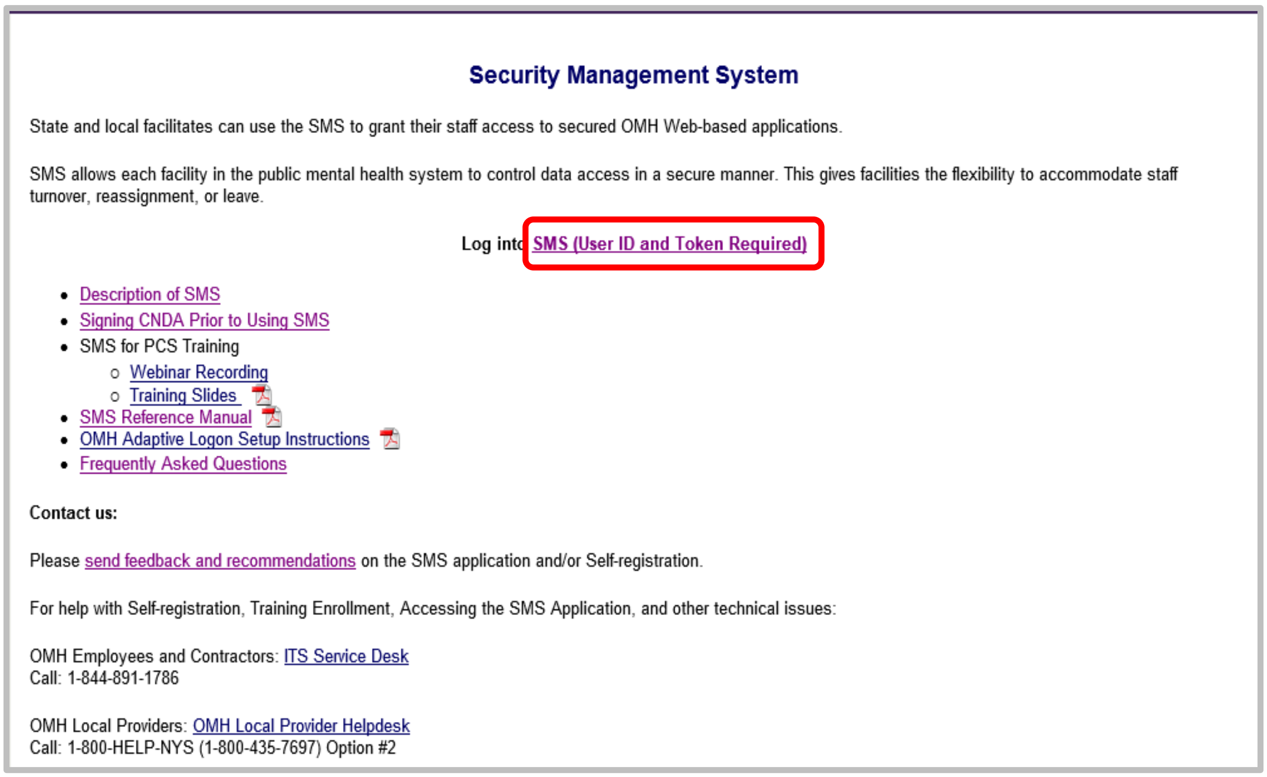
The User List will display.



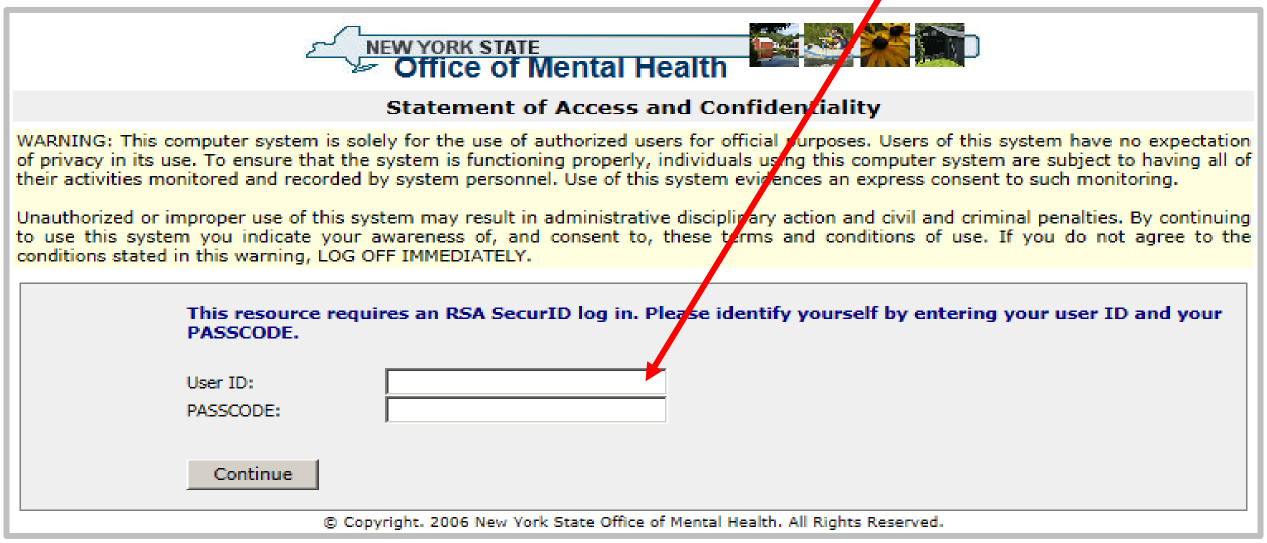
Using SMS

Login Procedure for Security Manager

The Security Management System (SMS) Homepage (https://www.omh.ny.gov/omhweb/sms/), provides a description of the application, the User Manual, answers to Frequently Asked Questions (FAQs), and links for self-registration and log-in to the application. On the SMS homepage click the link, “SMS Application (User ID and Token Required)” to sign into the application.

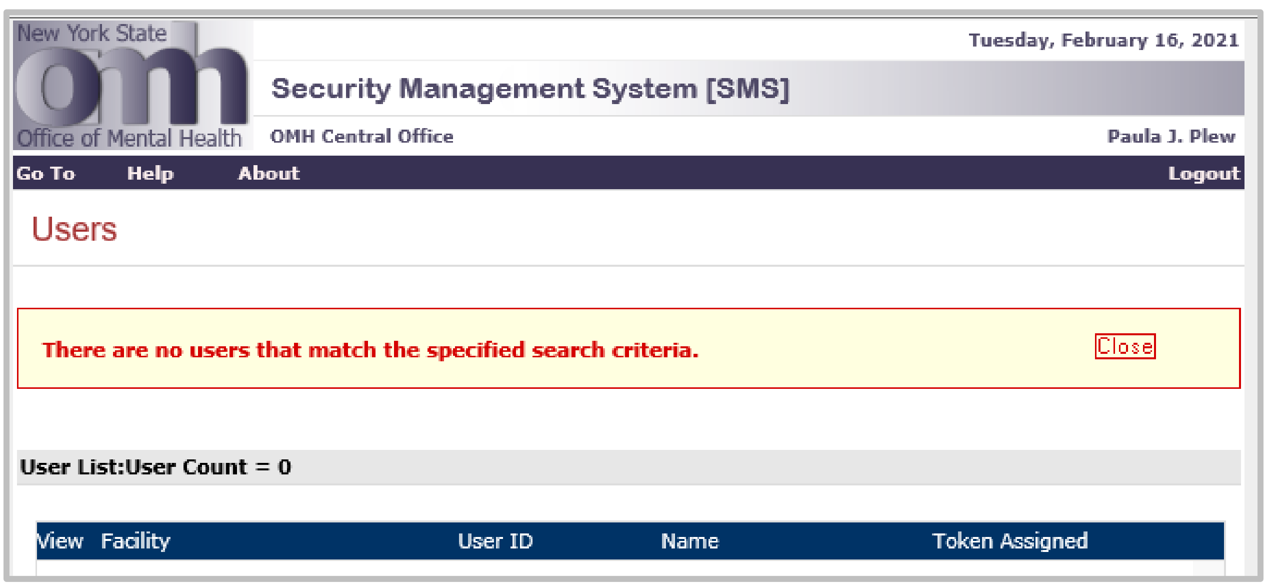


The Security Manager follows the link to SMS, enters the “User ID” and “Passcode” (token).

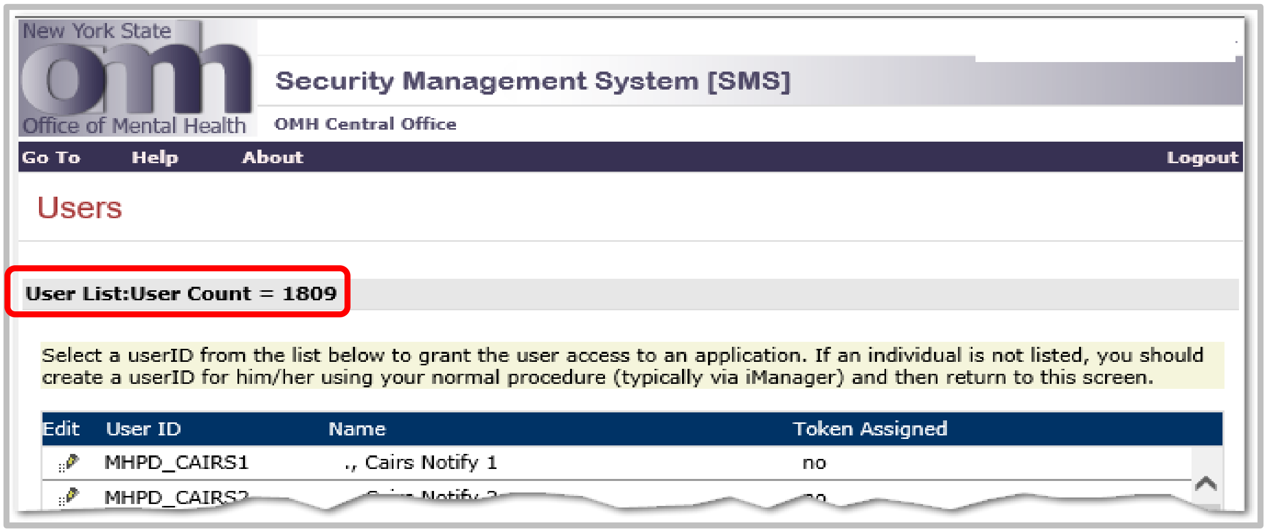


Users Page

After signing into SMS, the Users page will be displayed. This page contains a scrollable list of all the User IDs assigned to your agency. If no users are listed, the message "There are no users" is displayed. Once users are added, this message will no longer appear when entering SMS.



Initially, the list may be empty (indicated by [User Count: 0]), or if your agency has users of OMH applications such as CAIRS, NIMRS, PSYCKES, or NYESS, their User IDs will be displayed. Any User IDs that you add will also appear in this list.



User List Section

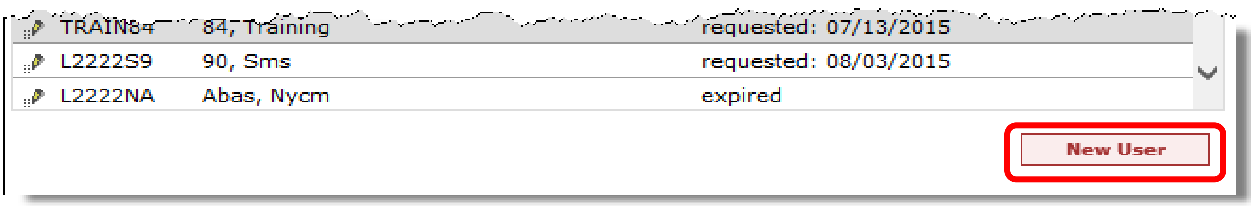
The User List contains one row for each User ID defined for your agency. Each row contains the following columns:

- **Edit** (): Click this icon to edit the user record. This is one of two ways you will grant access to OMH applications. This process is described in the PCS and PSYCKES Medicaid sections of this document.
- **User ID:** This is the OMH identifier for the user. This identifier is used to sign into OMH applications.
- **Name:** This field displays the user's last name, followed by the user's first name and middle initial.
- **Token Assigned:** While some OMH applications may be accessed with a password, others (e.g., PSYCKES Medicaid), require a SecurID token. This column allows the Security Manager to track token status. The possible values are:
    - "Yes" (the user has a SecurID token)
    - "No" (the user does not have a SecurID token)
    - "Expired" (the user has a SecurID token, however it has expired)
    - "Requested-mm/dd/yy" (a token has been requested for this user on the date specified)
    - "Sent-mm/dd/yy" (a token was sent to this user on the date specified)

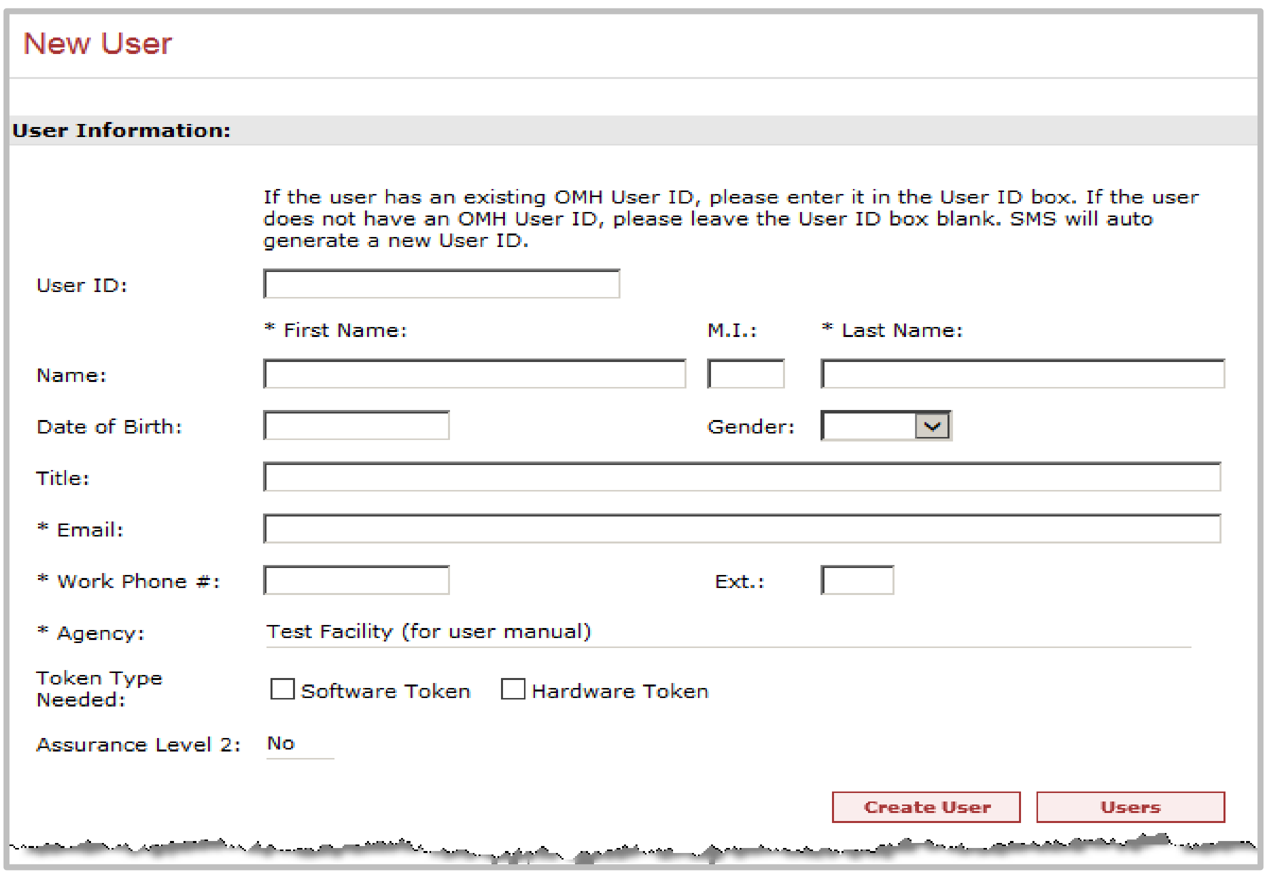
In rare circumstances, it is possible for an individual to have an OMH User ID, but not appear on the User List. In this case, you can create the association between the existing User ID and your agency by using the "New User" function, described in Add New User. The SMS association will be established by entering the existing User ID on the "New User" page.

New User Page

A "New User" button is displayed immediately following the listed users.

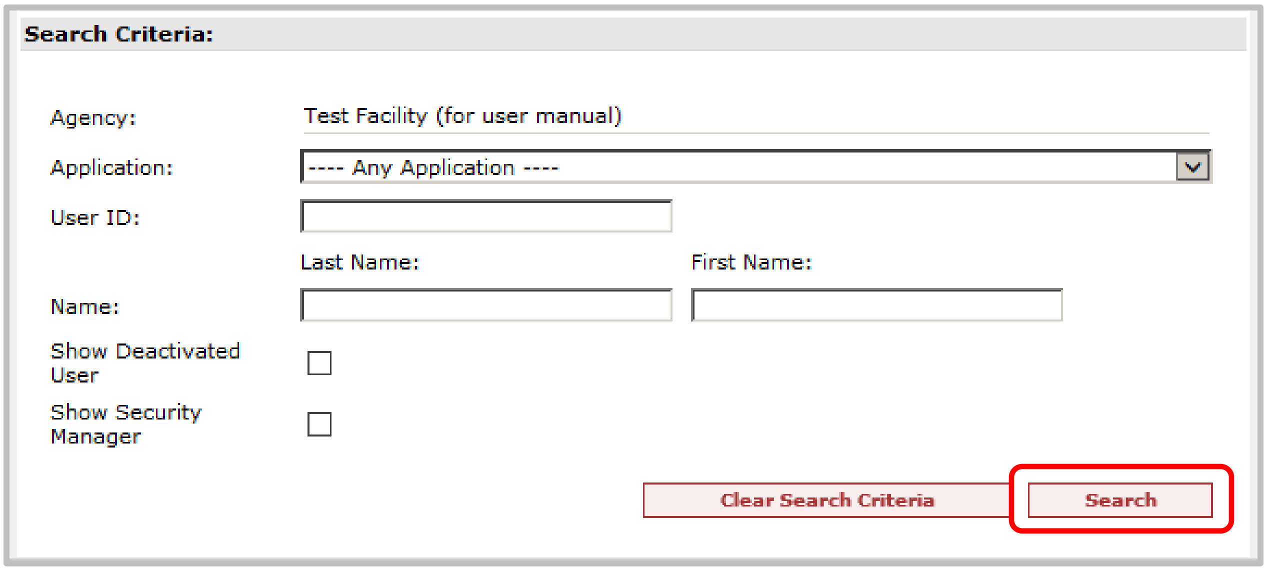


When you click this button, the "New User" page will be displayed. You must use the "New User" page to add a new User ID for your agency or to associate an existing User ID with your agency so it appears on the User List. See "Add New User".

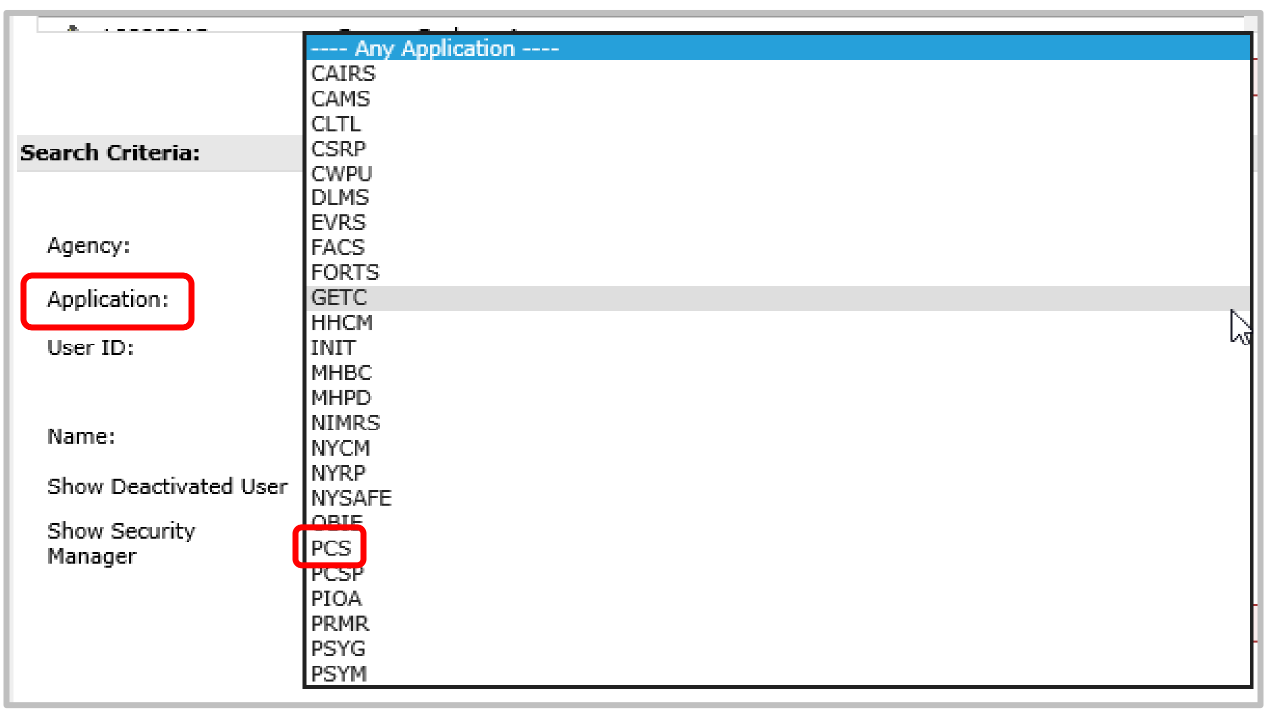


Search Criteria Section

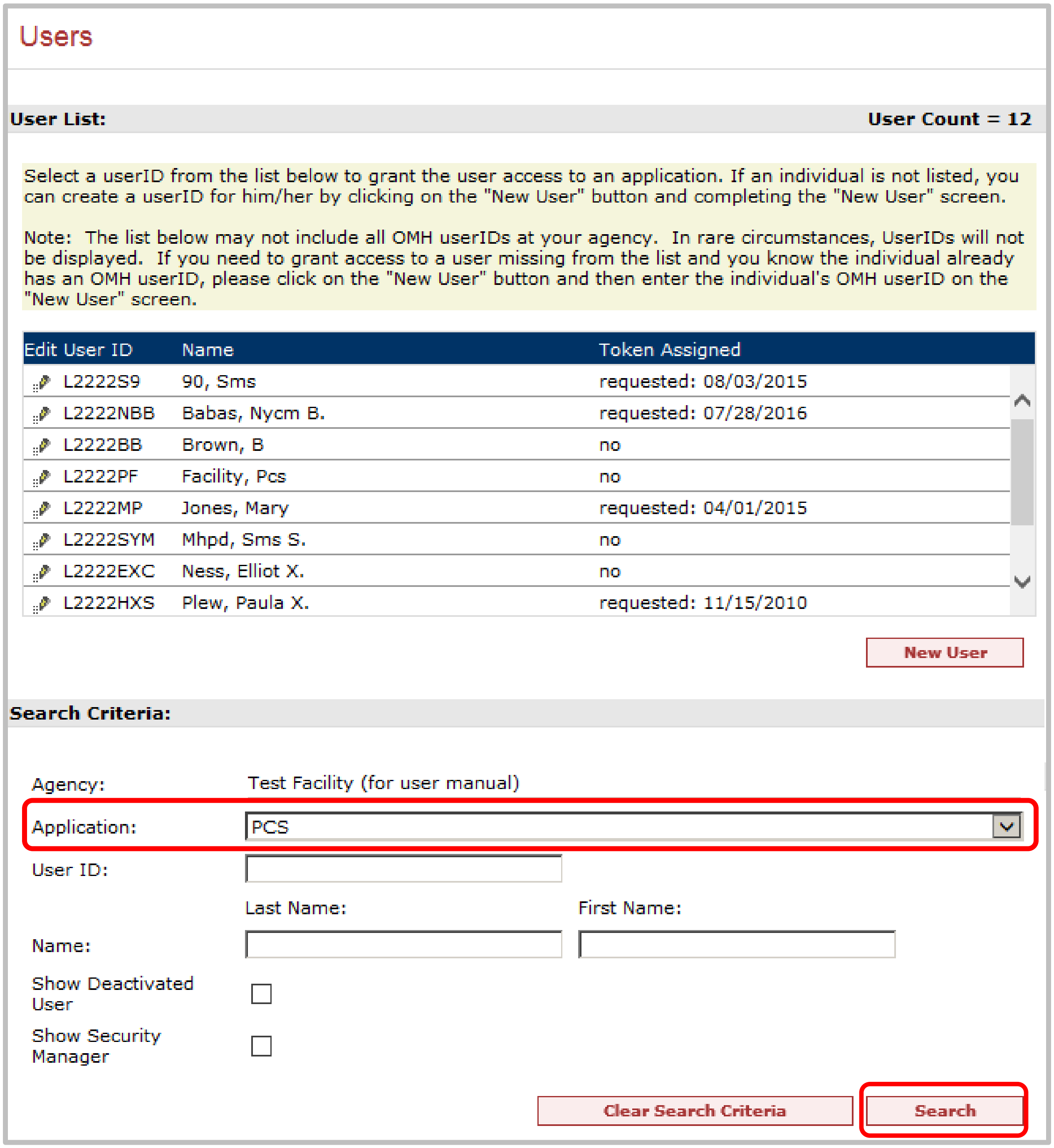
The “Search Criteria” section is located at the bottom of the Users page following the User List and “New User” button. The “Search Criteria” section is the mechanism Security Managers use to limit the User IDs displayed in the User list. It contains the following criteria: “Application” (click drop-down arrow); “User ID” (enter data); “Last Name and First Name” (enter data); “Show Deactivated User” (check box); and “Show Security Manager” (check box).



In your search query you may select an OMH “Application” from the drop-down list, such as PCS.



Enter a specific “User ID,” “Last Name,” or “First Name,” or you may enter the first part of any of these fields. When you click the “Search” button, these fields will be used to filter the search results and display only User IDs that match the criteria you selected. If you enter values in more than one of the fields, the search results displayed in the User list will include only User IDs that match all the criteria selected.



Users

User List: **User Count = 12**

Select a userID from the list below to grant the user access to an application. If an individual is not listed, you can create a userID for him/her by clicking on the "New User" button and completing the "New User" screen.

Note: The list below may not include all OMH userIDs at your agency. In rare circumstances, UserIDs will not be displayed. If you need to grant access to a user missing from the list and you know the individual already has an OMH userID, please click on the "New User" button and then enter the individual's OMH userID on the "New User" screen.

Edit User ID	Name	Token Assigned
L2222S9	90, Sms	requested: 08/03/2015
L2222NBB	Babas, Nycm B.	requested: 07/28/2016
L2222BB	Brown, B	no
L2222PF	Facility, Pcs	no
L2222MP	Jones, Mary	requested: 04/01/2015
L2222SYM	Mhpd, Sms S.	no
L2222EXC	Ness, Elliot X.	no
L2222HXS	Plew, Paula X.	requested: 11/15/2010

New User

Search Criteria:

Agency: Test Facility (for user manual)

Application: PCS

User ID:

Last Name: First Name:

Name:

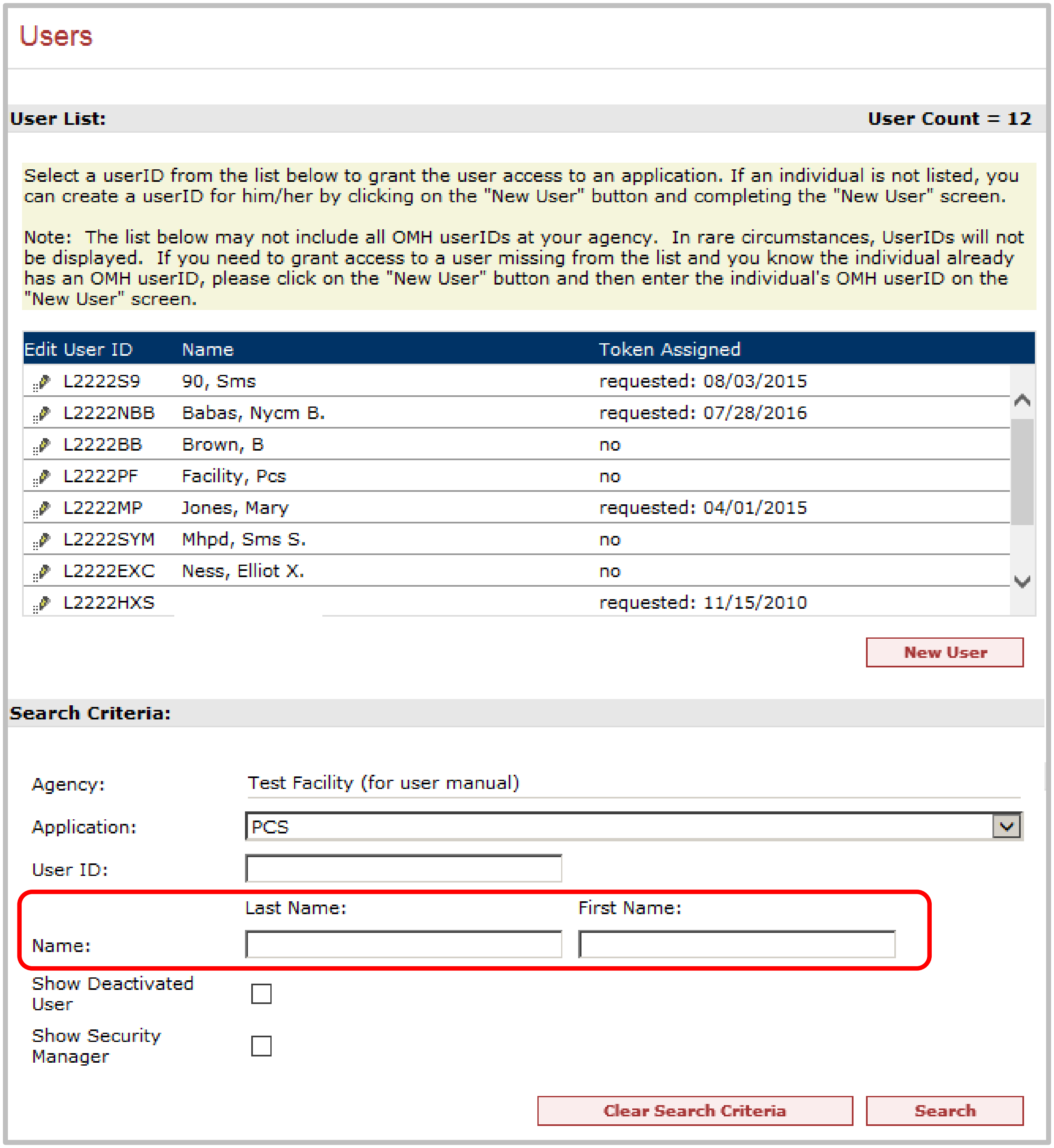
Show Deactivated User

Show Security Manager

Clear Search Criteria Search

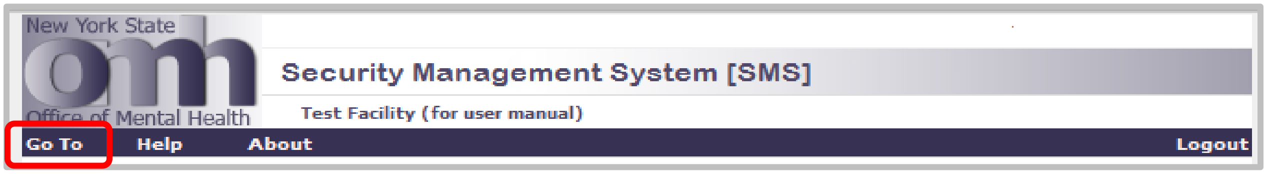
For example, you can search for users with access to the PCS application by selecting the "PCS" option in the drop-down for the application criteria and clicking the "Search" button.

The User List displays users with access only to the selected application (in this case the PCS). Specific users can be searched by User ID and/or first and last names.



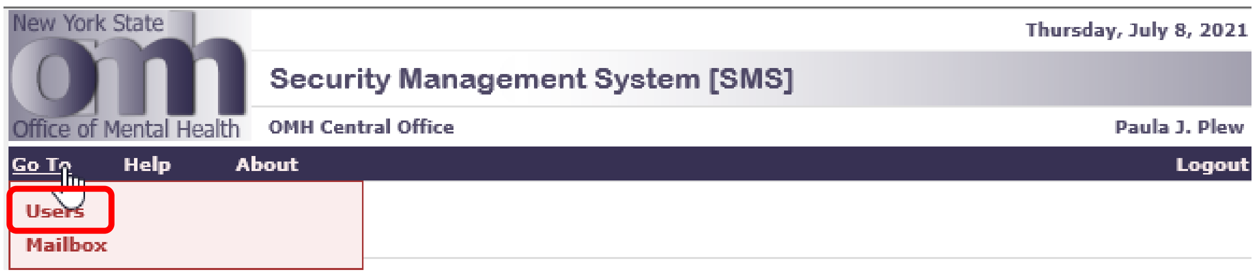
Go To Tab

In the SMS application, you can navigate to other SMS pages (e.g., Update My Mailing Address) by positioning the mouse pointer over the "Go To" link at the top left-hand side of the screen, and clicking on the desired page. “Go To” choices are Users list and "Update My Mailing List".

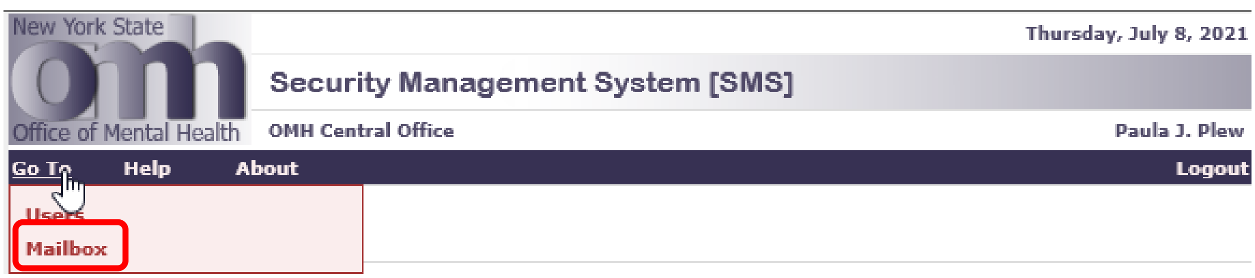


Users Button

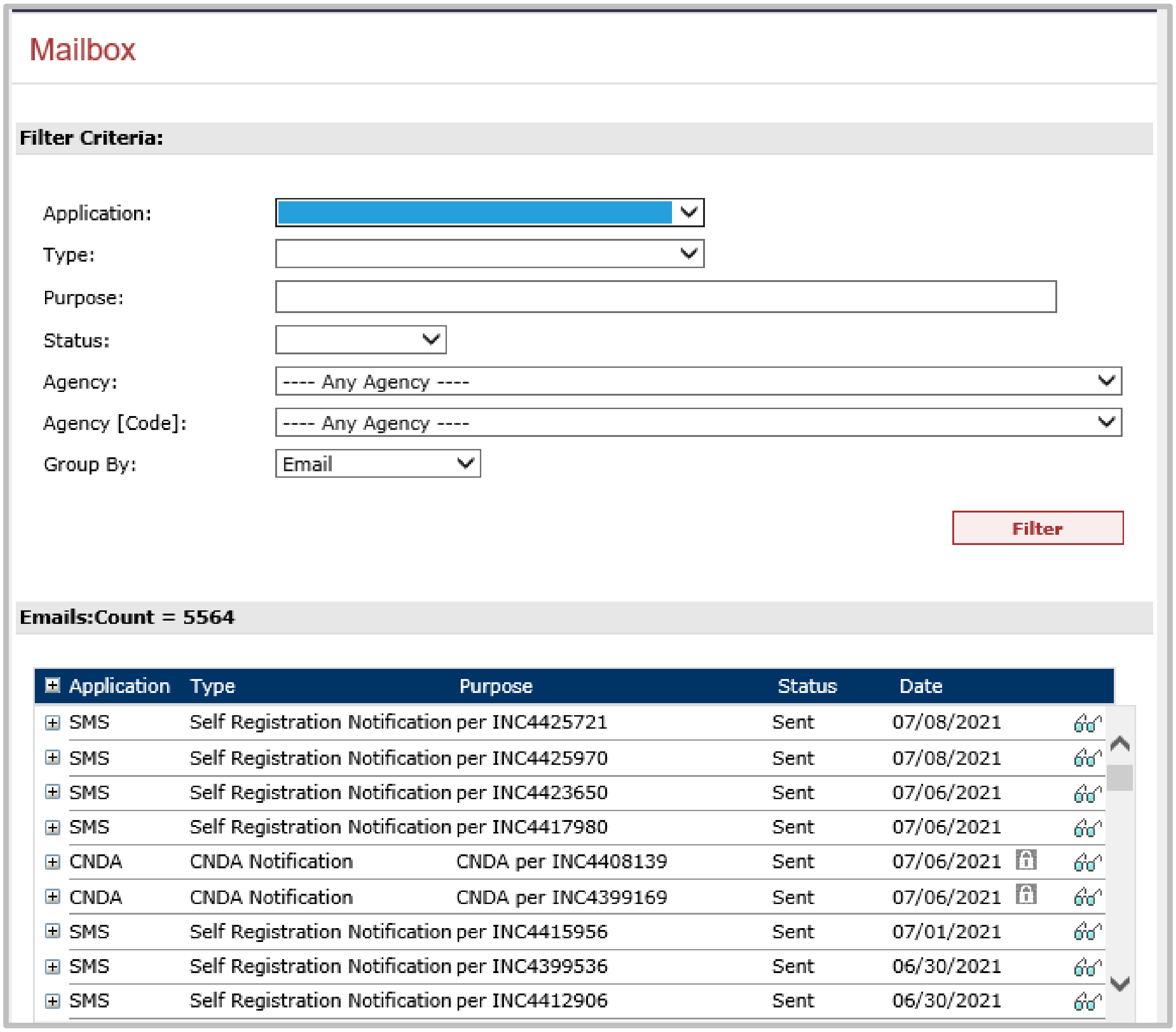
Click the "Users" button to return to the Users page.



Update Mailbox Tab

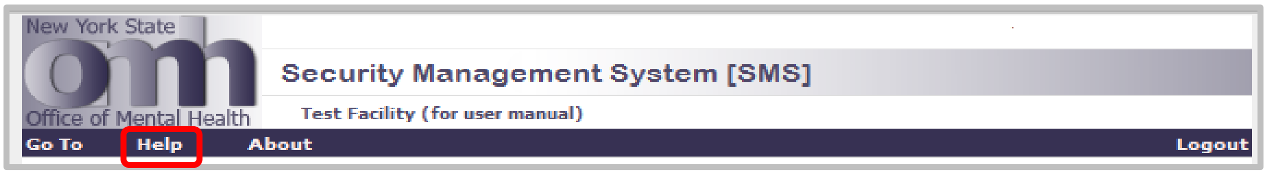


Below is the “Mailbox” screen showing the “Filter Criteria” and “Emails: Count.”



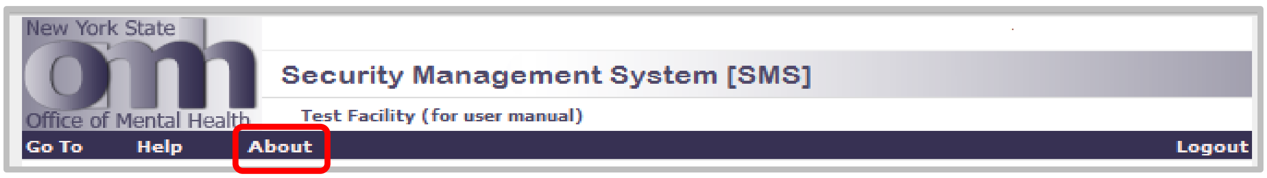
Help Tab

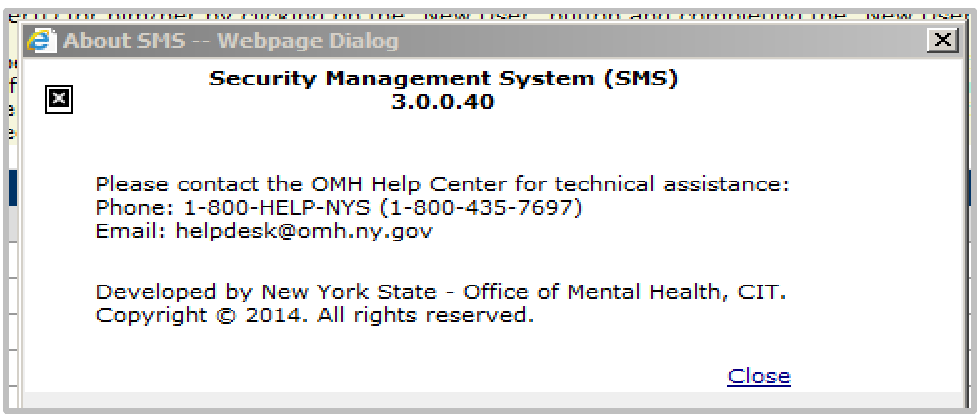
Click the “Help” Tab to open the SMS User Manual.



About Tab

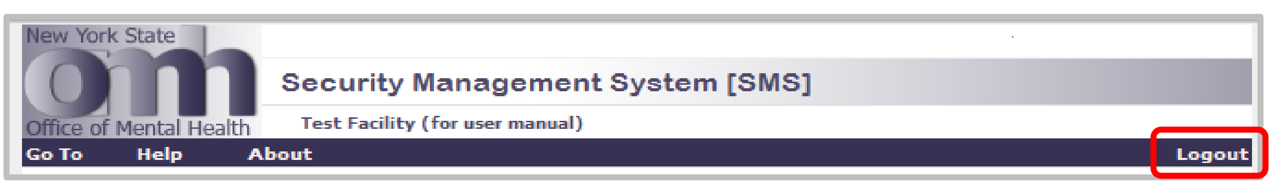
To display the version of SMS the user is currently using and the name of the office and phone number to contact regarding technical issues, click the “About” Tab.





Logout Tab

You can sign-out and exit SMS from the SMS "Users" page, or from any other page in SMS, by clicking on the "Logout" tab at the top right-hand side of the page.

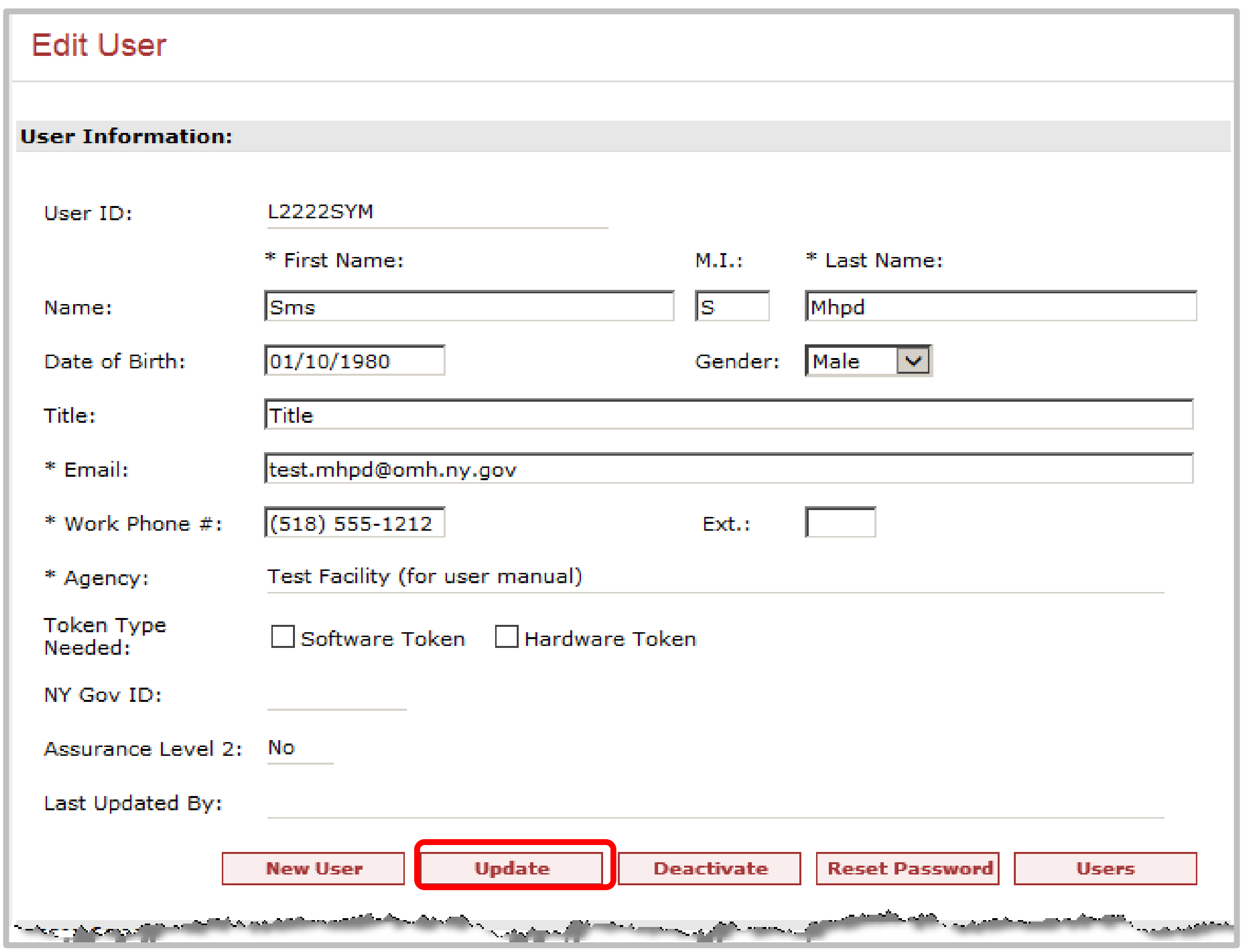


Edit User Information

Accessing the Edit User

To edit the information for an individual at your agency, you will need to sign-in to SMS as described in [Log-in Procedure for Security Manager](). From the SMS Users page, access the Edit User page by clicking on the pencil icon in the "Edit" column on the row for the user in the Users List section.

The "Edit User" page displays the user's name, email address, date of birth, gender, and current application access. If a user wants to change a user's name, email address, date of birth, gender, work phone number, or title, they type over the text boxes with new or corrected information and then click the "Update" button to save the changes.



Edit User Menu Bar

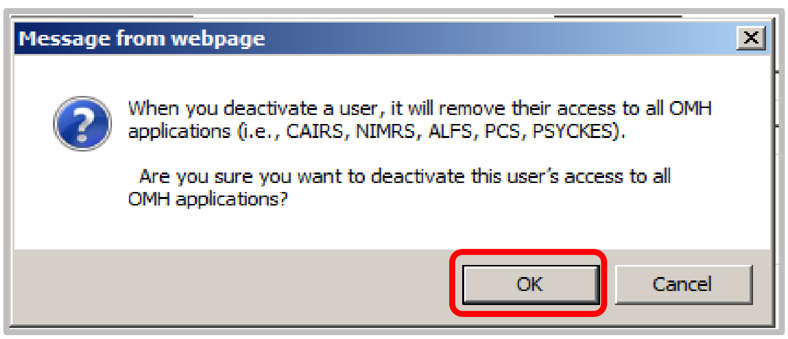
Under the User Information section of the "Edit User" page is the Edit User Menu Bar.

New User Button

At the bottom of the User information section on the "Edit User" page is a "New User" button. Click this button to add a new user for your facility. Clicking the "New User" button, displays the New User page. Add New User describes how to use the New User page.

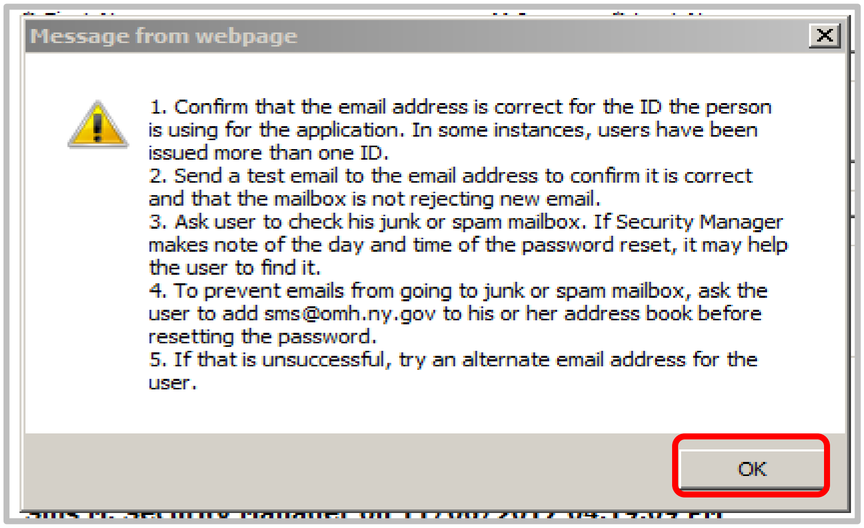
Deactivate Button

Click the "Deactivate" button to remove a user's access to any OMH application. A warning message will appear explaining that the user will lose access to **ALL** OMH applications and ask if you wish to do this. Click the "OK" button in the message to deactivate the user's access.

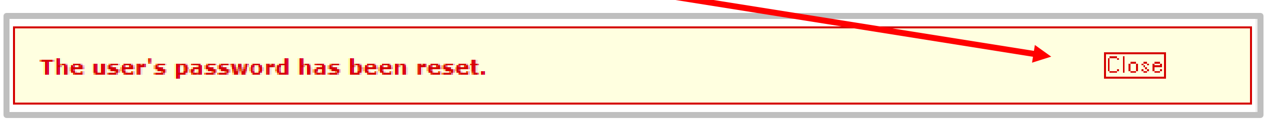


"Reset Password" Button

Click "Reset Password" to reset the user's password. The following message appears, click "OK."



Once the password is reset, click "Close."

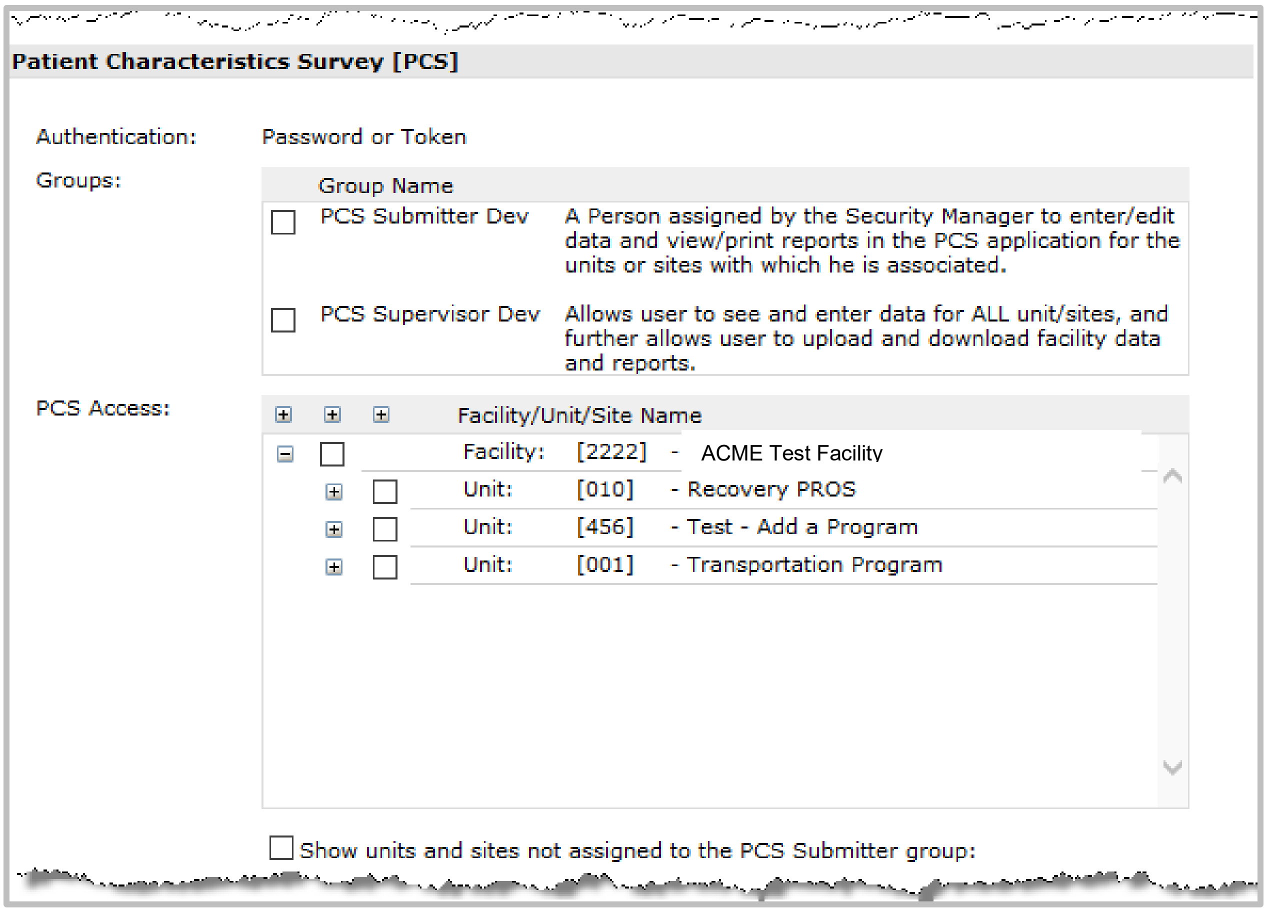


Users Button

Click the "Users" button to return to the Users page.

Various OMH Database Modules

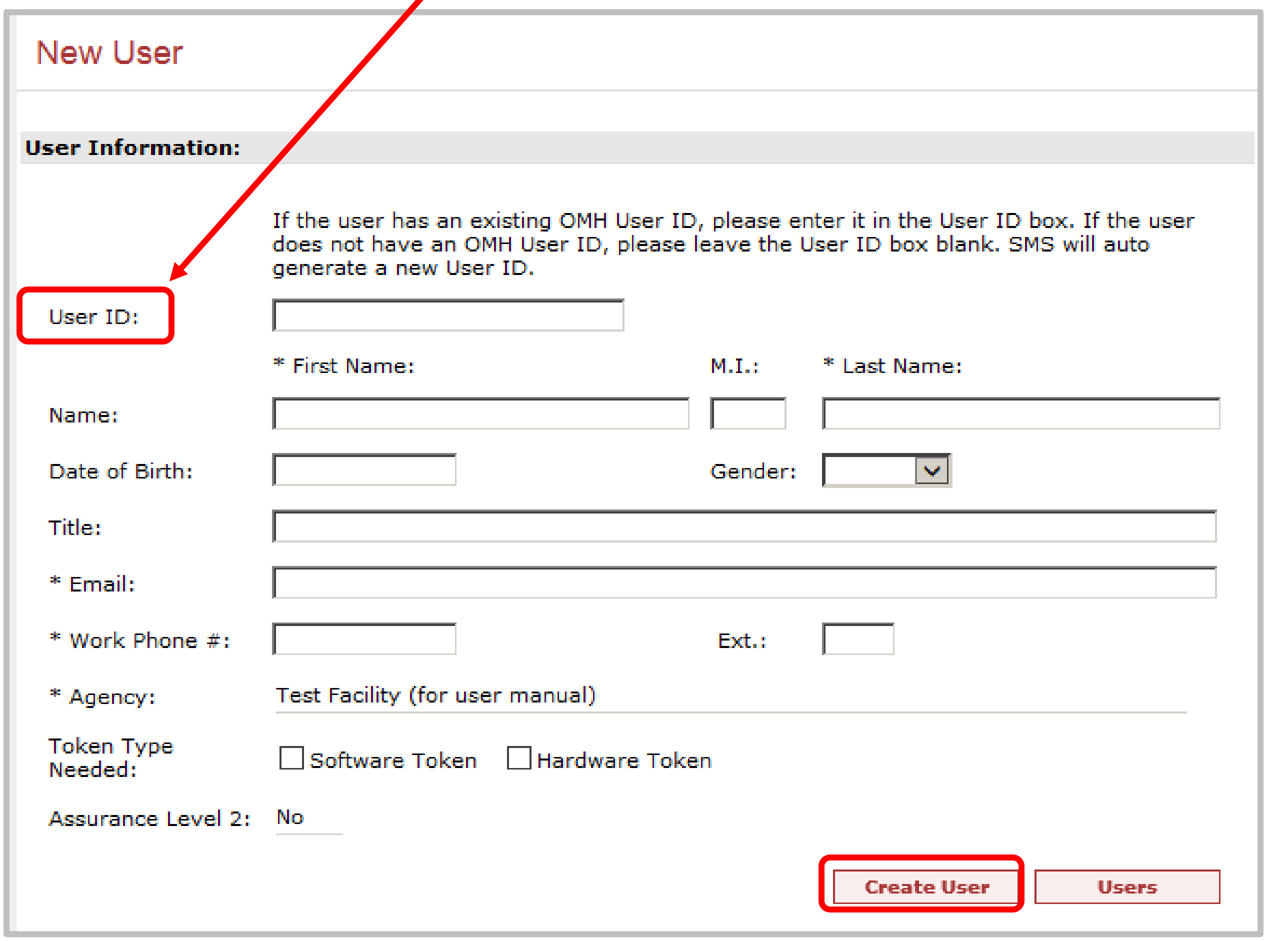
Scroll down the Edit User screen to find the application you want to grant access to, assign users to a security group within the application, and in the case of the PCS, associate users with specific units or sites. These processes describe the application-specific sections.



Add New User

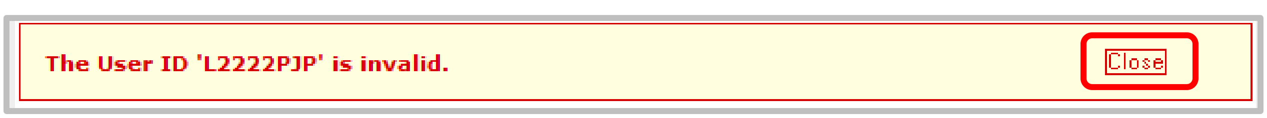
Adding User with Existing User ID

If a user already has an OMH User ID for access to another application, (e.g., MHPD, CAIRS, NIMRS), please enter it in the User ID field and click “Create User.”



Upon entering a current User ID in the field and exiting the field, the screen will respond with a message that the User ID is valid and will display the retrieved user information. Click “Close.”

A similar message will display if the user information is not found in the security database. Click “Close.”



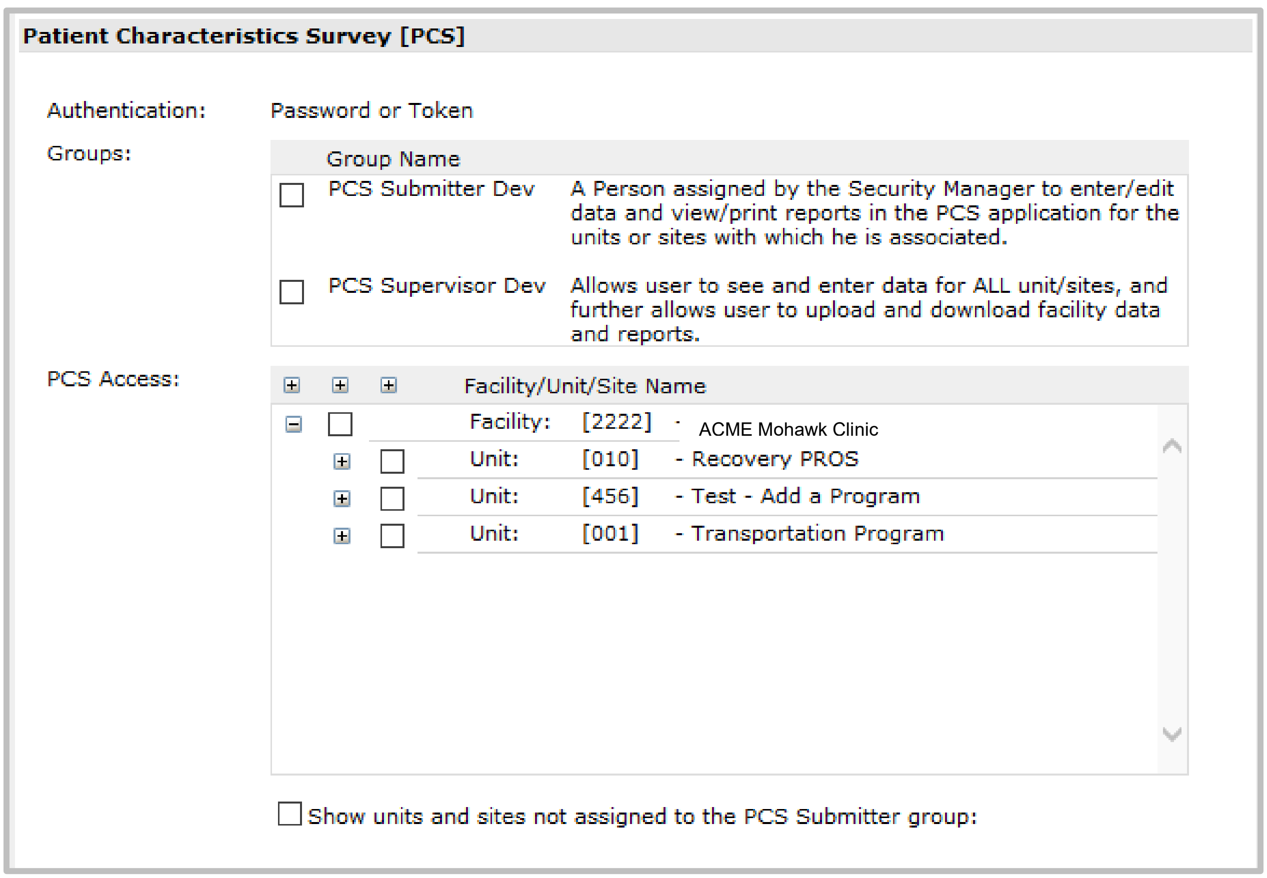
Adding a User who does not have a User ID

If the user does not have an existing ID, leave the “User ID” box blank. The Security Manager proceeds to complete the User Information section and select the "Create User" button. Fields denoted with an asterisk (*) are required. A new User ID will be generated for the user. If a user by that name already exists for the agency, the system will show a message that a user with that name is among the “active” or “inactive” users. To check the inactive users, see the Search Criteria section of the User’s Page.

Applications Using the Security Management System

Patient Characteristics Survey (PCS) Module

Below is an illustration of the PCS module.



How will SMS be used for the PCS web application?

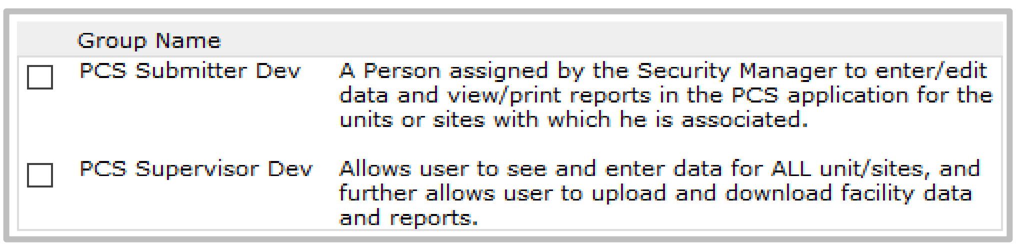
In SMS, each facility's Security Manager will add and edit users and determine each user's level of access to the PCS Web application by assigning the user to a security group. For example, the security manager may grant:

- Persons A and B the ability to submit and view data for service recipients of the facility's unit 010
- Person C the access to submit data for service recipients of the facility's unit 456
- Person D the supervisory authority to submit, view or download client data for all the facility's units.

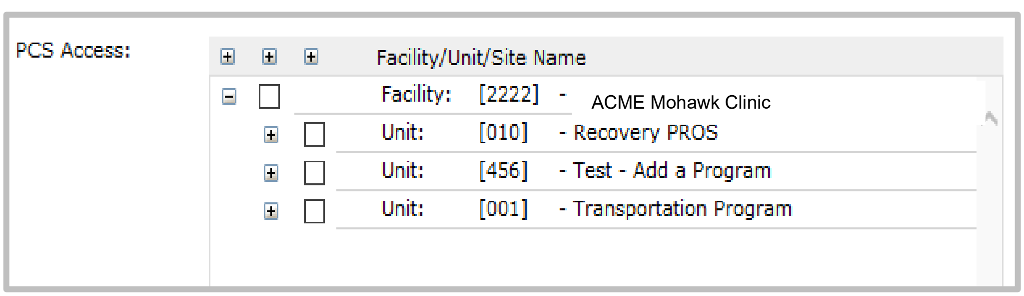
Granting access to the PCS Application

After editing or adding users to the User Page, the Security Manager follows three steps to grant a person access to the PCS application:

1. Assigns the user access to a PCS security group (Submitter or Supervisor) by checking the appropriate box.



2. Associates users in Submitter security group with specific program units and sites by checking the appropriate box.



3. Clicks "Update" to save the user's assigned access.

Assigning User to PCS Security Group

Below the User Information section of both the "Edit User" and "New User" screens, the PCS application is listed and followed by the PSYCKES Medicaid application. To assign a user to a PCS security group, the Security Manager checks one of the two boxes: "PCS Submitter" or "PCS Supervisor". The definitions of PCS security groups are:

- **PCS Submitter** – A person assigned by the Security Manager to enter/edit data and view/print reports in the PCS Web application for the units or sites with which they are associated.

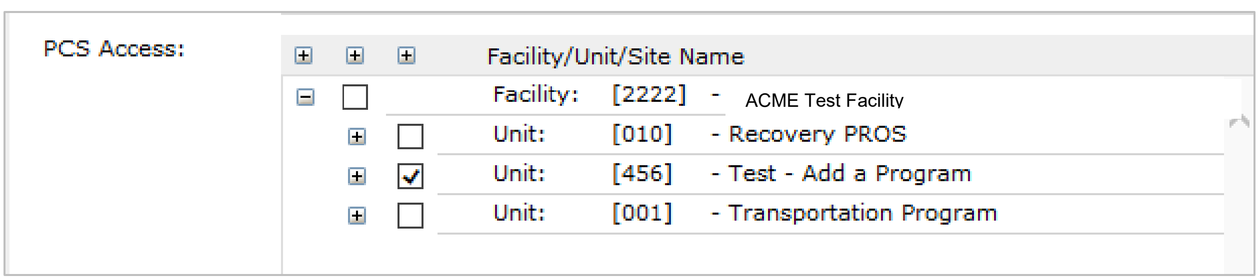
- **PCS Supervisor** – The Supervisor may upload the facility's data into the PCS application (if the facility has received prior approval), perform all the functions of a Submitter for every unit throughout the facility, and may also download the facility's data file in MS Excel.

NOTE: A user can only be a **PCS Submitter OR PCS Supervisor** and cannot be both.

Associating Submitters to Program Units and Sites

When a person is assigned as a Supervisor, all programs and sites in the facility are automatically selected because the Supervisor's access is facility wide.

To assign someone as a Submitter: Click the PCS Submitter check box, and then select the Program/Sites for which this Submitter will be entering PCS information. This associates the Submitter with the selected programs/sites. The Security Manager must associate the Submitter with at least one program/site and up to all programs/sites. The complete list of program units currently listed in the Facility Survey (or PCS Web application) can be viewed on the list.



Once a user is "associated" with sites, the user will be able to enter and edit information in the PCS application for all clients in that site.

By default, program units are shown, but the list can be expanded into sites or collapsed into programs by clicking on the expand and collapse buttons:

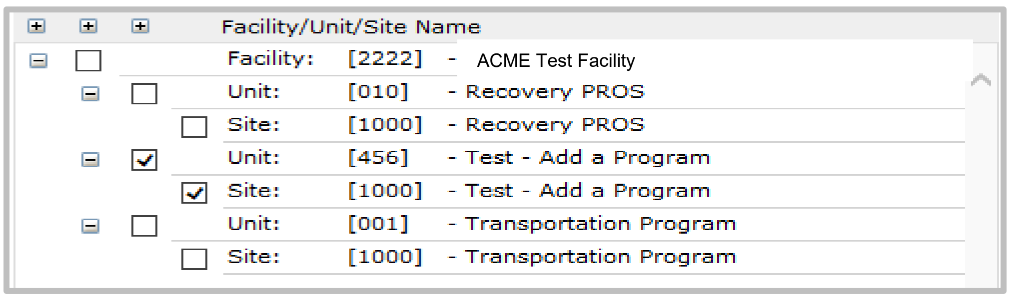
 Expand Button – reveal sites associated with a program

 Collapse Button – hides the site information

For the licensed outpatient program types in the table below, agencies are expected to report Patient Characteristics Survey data at the site-level. The Security Manager may grant site-level access, i.e., grant one-person access to some of the unit's sites and another person access to another set of sites.

Program Type CD	Program Type Name
0200	Day Treatment
0800	Assertive Community Treatment
2200	Partial Hospitalization
6340	Comprehensive PROS with Clinical Treatment
7340	Comprehensive PROS without Clinical Treatment
2100	Clinic Treatment

To grant site-level access, the Security Manager expands the program unit listing and selects the desired sites.



We recommend that the Security Manager collapse the list into program units to associate PCS Submitters with specific programs. If the Security Manager chooses to grant only site-level access for some outpatient programs, they should expand the program/site list for those outpatient programs and associate the PCS Submitters with the specific sites.

What sites are shown?

Information about the facility in the SMS application is drawn from the OMH Master Provider Directory and may be updated by submitting corrections via the Mental Health Provider Data Exchange (MHPD). A description of MHPD is available at http://omh.ny.gov/omhweb/mhpd/
In preparation for the collection of PCS data, providers complete the Facility Survey found on the MHPD's Survey tab. By completing the Facility Survey, the providers can update the facility data and program/unit data for all programs expected to report on the PCS.

For certain facilities, the list of programs/sites may be lengthy: the user may have to scroll down to see all the programs/sites for that facility.

In the SMS application, any list that is displayed on your screen may be printed in its entirety by right-clicking on the screen with the expanded list of programs and their corresponding sites and selecting the "Print" option.

Save the User's Assigned Access

Once the fields are populated and PCS access is assigned for the prospective user, click

“Update” to save the changes.

An email will be generated for the prospective user, giving instructions. If the Security Manager registered the user with an existing OMH User ID, the email will list the ID and instruct the user to use his or her existing password or token. If the PCS user was not registered with an existing User ID, a new ID is sent to the user’s email address along with a notice to expect another email with a password and instructions. The second email will contain the new user password and instructions for use. If the user forgets his password, the Security Manager can reset it.

NOTE: A new PCS user must wait one hour after receiving the 2 system emails, before accessing the PCS application, so that the databases can update.

Upon finishing the request, the Security Manager should click the “Users” tab to exit the current request and return to the User Menu screen.

PSYCKES Medicaid Module

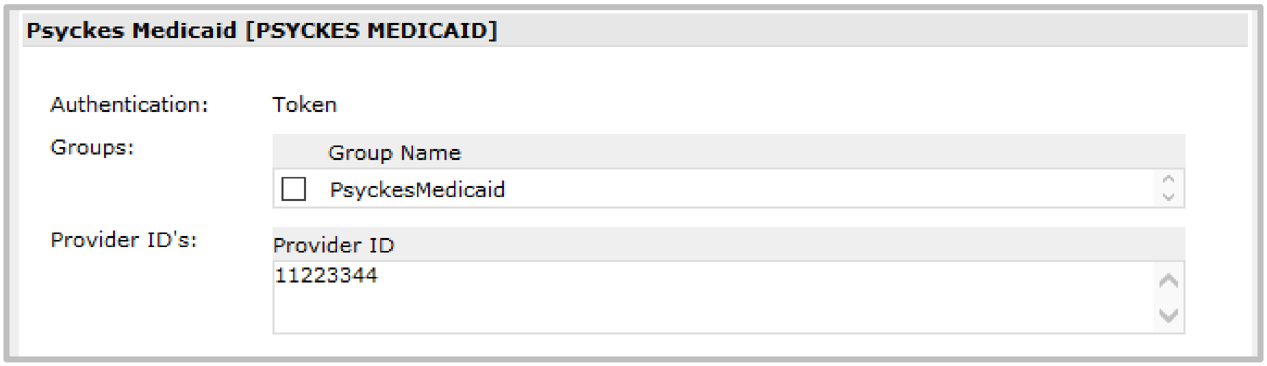
Authorized Access

Agencies are responsible for ensuring that staff have access only to those applications for which they are authorized. Authorized staff at the following types of organizations are eligible for PSYCKES access:

- OMH and OASAS licensed provider agencies
- Hospitals and Emergency Rooms
- Health Homes and Care Management Agencies
- Behavioral Health Care Collaboratives (BHCCs)
- DSRIP Performing Provider Systems (PPS)
- Federally Qualified Health Centers (FQHCs)
- Medicaid Managed Care Plans
- Local Government Units

Granting Access to the PSYCKES Medicaid Application

To add a user to an application, you will need to sign-in to SMS as described in the Login Procedure for Security Manager section. On the SMS Users page, click on the “pencil icon” in the "Edit" column found on the left of the user’s name in the Users List section. The "Edit User" page will display the user’s information and current application access. You can add or remove a user’s access to the PSYCKES Medicaid application by clicking the checkbox next to the application in the "Application Access" section. A check in the box indicates the user has access. If there is no check in the box, the user will not have access.



Save the User’s Assigned Access

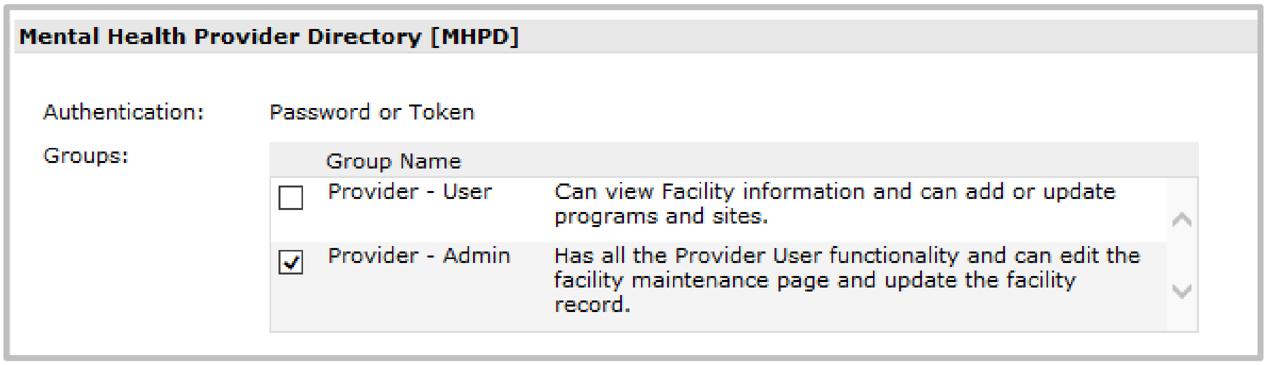
You must click the "Update" button in the User Information section to save your selection. An email will be generated for the prospective user, giving instructions.

Exiting the "Edit User"

You can return to the User List page by clicking the "Users" button, or by positioning the mouse pointer over the "Go To" label at the top left-hand side of the page and clicking the "Users" link.

Mental Health Provider Data Exchange (MHPD) Module

The facility's Security Manager can access SMS and add, deactivate, or edit users. The Security Manager can also assign a user's level of access to MHPD. Only a Security Manager will be able to update a user's name, email address, title, and phone. After adding or editing users on the User Page in SMS, the Security Manager grants the user access to MHPD.



For providers or counties, there are four roles in MHPD, each with their own specific levels of access and responsibility.

- **Provider User**: A user at an individual facility can access all the information currently available for that facility in MHPD. A user with Provider access can submit Change Requests, Administrative Actions and EZ PARs to add, update or close programs.

- **Provider Admin:** A user at an individual facility has all the Provider User functionality and can edit the facility information. Additionally, a user with a Provider Admin role can edit the facility maintenance page and assign persons to receive facility notifications sent out by OMH via email.

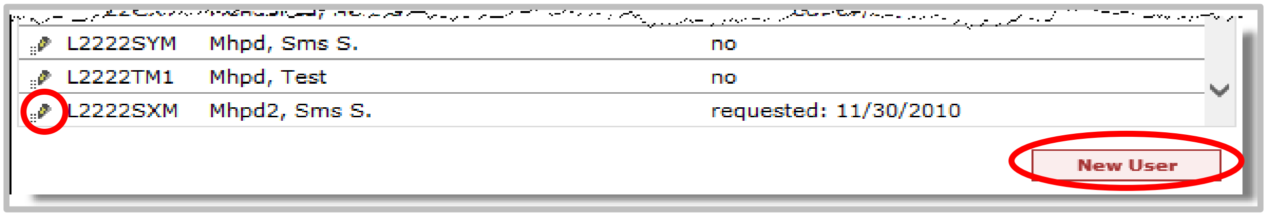
- **County User:** A County or New York City Mental Health Department User can search, view, and request updates to Programs and Sites located in the county. They can view change requests and can request the opening or closing of existing unlicensed programs. They can view but cannot submit Administrative Actions and EZ PARs.

- **County Admin:** A user at a local government unit has the same access as a County User and has all the functionality of the Provider Admin for the County Department of Mental Health and each facility located in the county.

The Security Manager can grant a user only one role, for instance, a user with Provider access cannot also have County access. The Security Manager can grant a user in a Provider role access only to the Security Manager's facility. If the user needs access to a second Facility, they should contact the Security Manager of the second facility; requesting access as a user to the MHPD application.

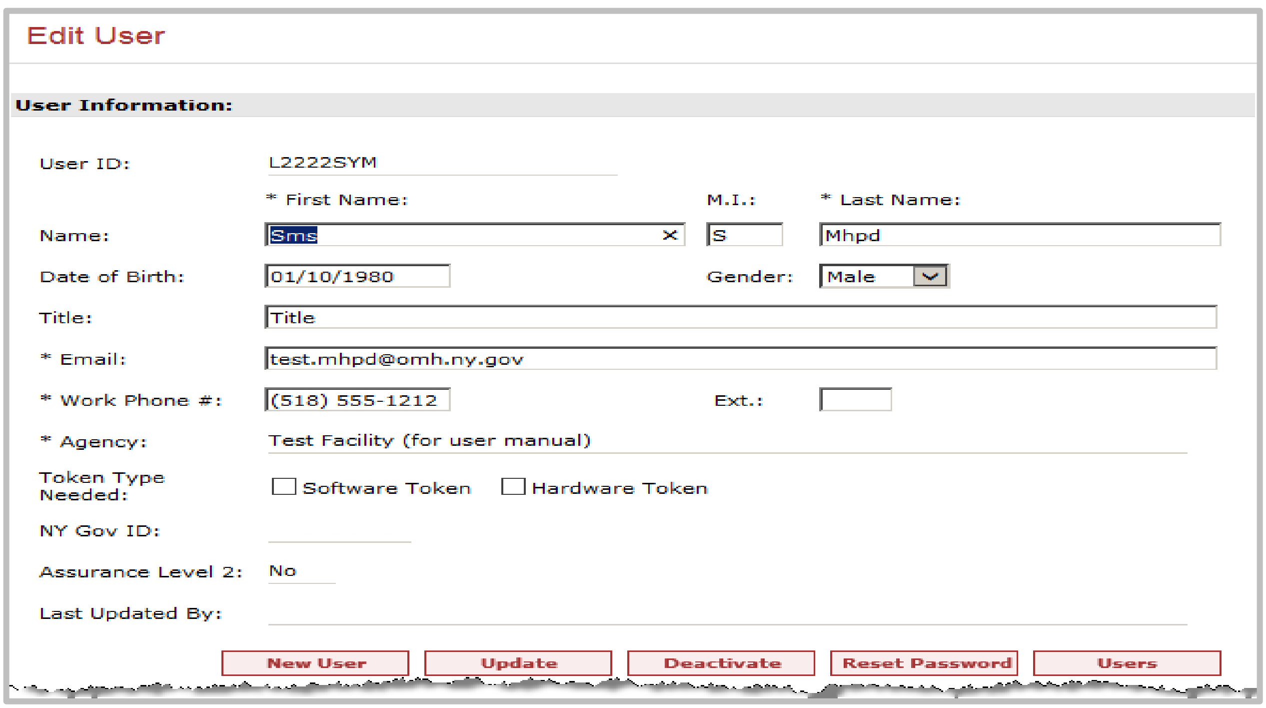
To assign a user a chosen role in MHPD after logging in to SMS, the Security Manager selects the user from the User List or creates a New User if the person does not already have a User ID.

To edit a user, the Security Manager clicks the “Edit” icon (the small pencil to the left of the User ID). To create a New User, the Security Manager clicks the “New User” button and follows the steps indicated.

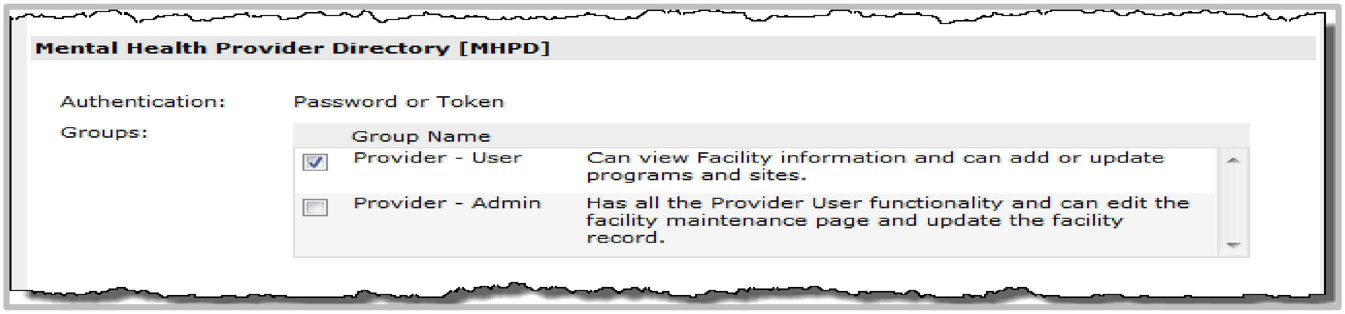


User List

Once in the “Edit User” Screen, the Security Manager should first verify the user’s information, and then scroll down to the MHPD Module section of the screen. If any of the required fields (marked with asterisks*) are blank, the Security Manager will be directed to enter information before being allowed to update.



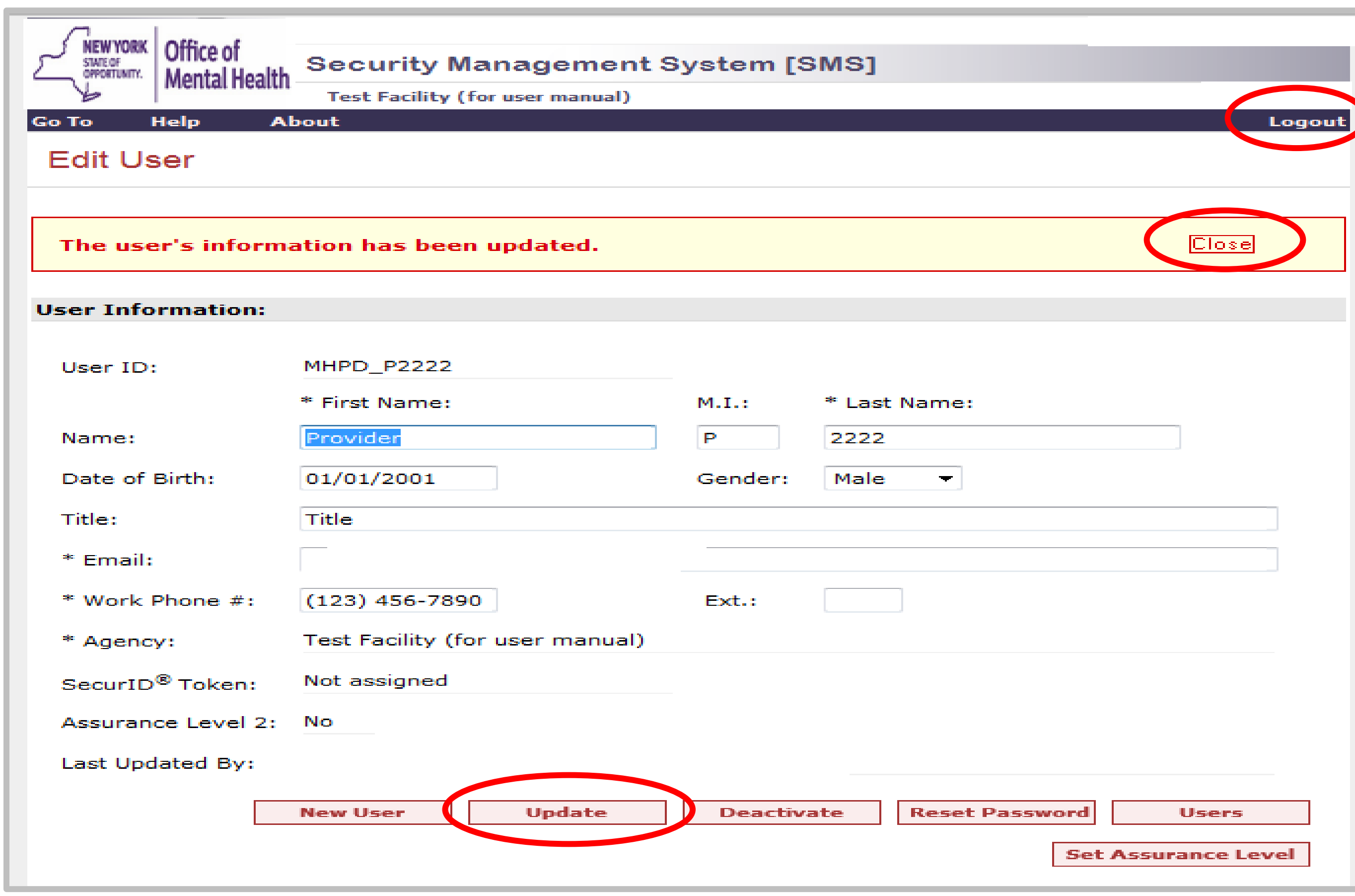
Click in the "Provider – User" or "Provider – Admin" checkbox. Go back up to the "Edit User" information and click the "Update" tab.



Edit User Screen

To assign MHPD access, the Security Manager selects the appropriate access level from the list – either "Provider User" or "Provider Amin." Only one access level can be selected.

When finished with all edits, click the "Update" button below the "Edit User" section. Click the "Users" button to return to the User List, "Close" to return to this "Edit User" screen, or "Logout" at the top right-hand corner of the screen to log out of SMS and quit the application.



Updating User Information

The Security Manager is the person who updates the user's email address, title, and phone number in SMS.

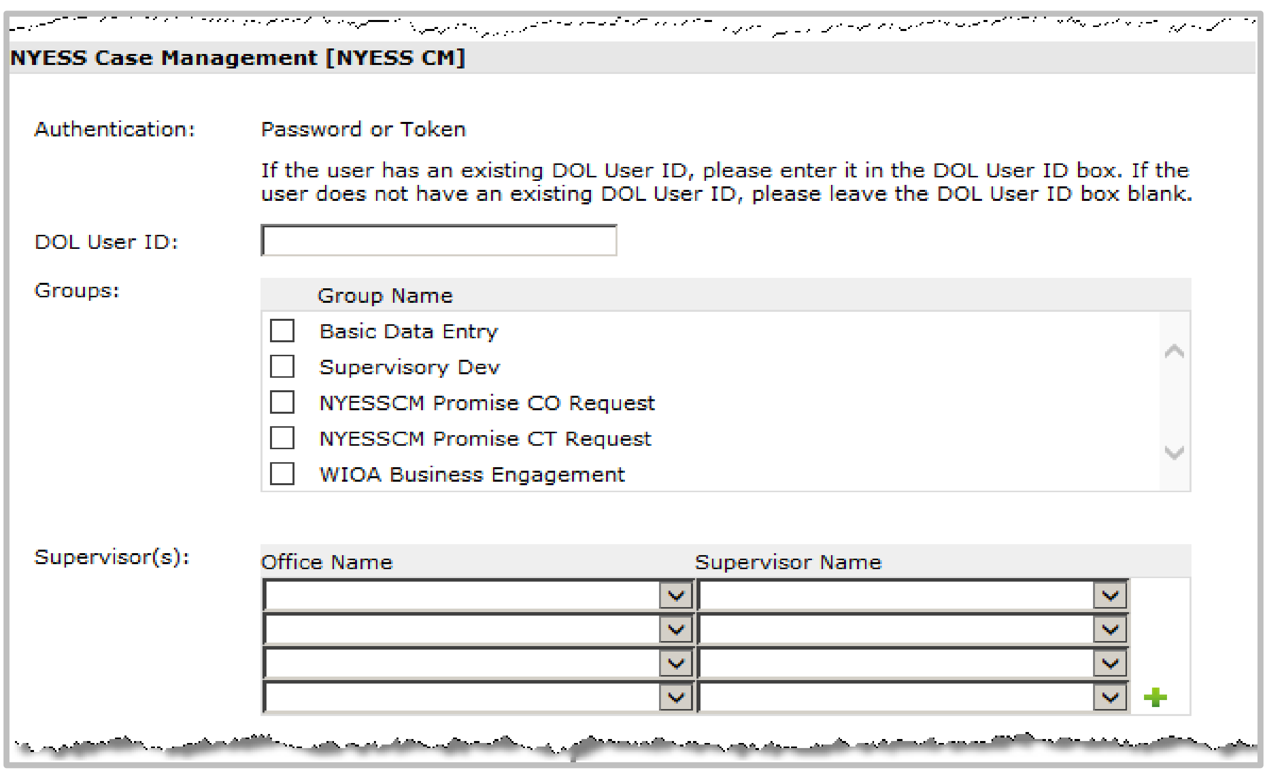
It is important to keep this information current so that MHPD users receive email notifications of Change Requests, Administrative Actions, and EZ PARs that they submit. Also, so that they may be contacted by phone or email by OMH or County staff who are reviewing the requests. To update user information, the Security Manager will select the user from the User List by clicking the "Edit Icon" to the left of the User ID. Once on the User Information Screen, the Security Manager simply corrects any information that needs updating, and then clicks the "Update" button. When finished, the Security Manager can log out at the top right-hand corner of the screen or click the "Users" button to return to the User List and select a different user to edit.

Email Notification

A duplicate notification email is sent to the Security Manager's and user's email addresses whenever a new user is entered in the system and/or a new password is generated. An email notification is also sent when a user is granted access to an application, such as when an MHPD Group Name is assigned. No email is sent when user information is updated.

New York Employment Services System (NYESS) Module

In SMS the facility's Security Manager can manage user access to the New York Employment Services Systems (NYESS). The next few screenshots show the NYESS Module. See www.nyess.ny.gov for details about this program.


NYESS Case Management [NYESS CM]

Authentication: Password or Token

If the user has an existing DOL User ID, please enter it in the DOL User ID box. If the user does not have an existing DOL User ID, please leave the DOL User ID box blank.

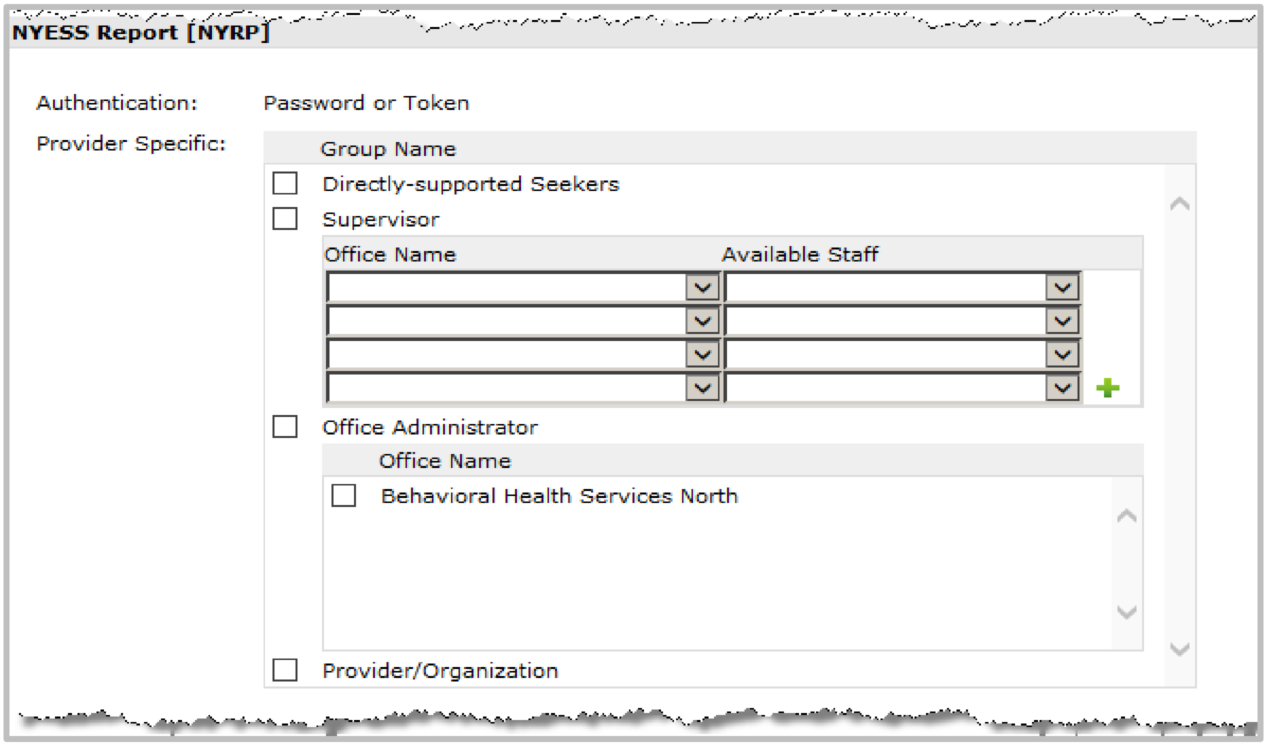
DOL User ID:

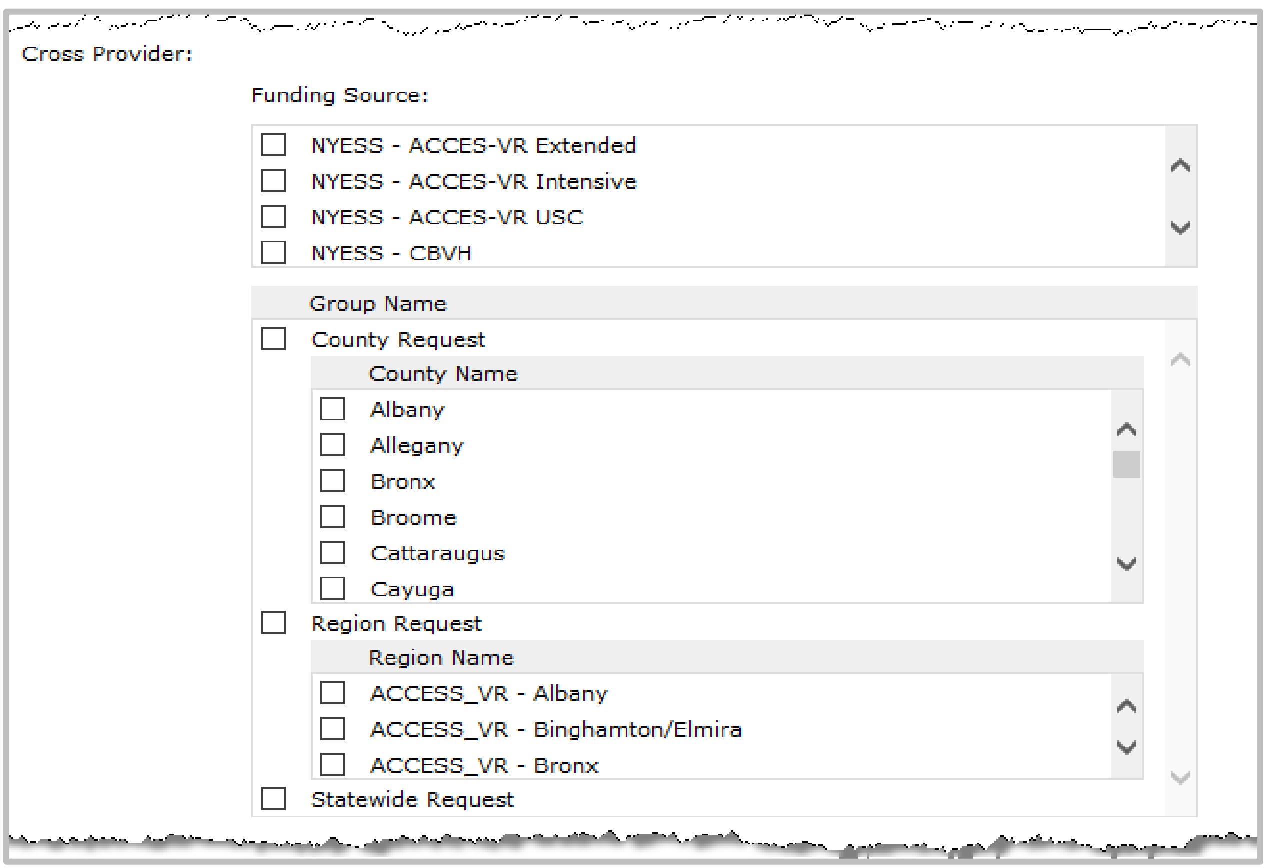
Groups:

	Group Name
☐	Basic Data Entry
☐	Supervisory Dev
☐	NYESSCM Promise CO Request
☐	NYESSCM Promise CT Request
☐	WIOA Business Engagement

Supervisor(s):

Office Name	Supervisor Name





Several types of NYESS access are available: NYESS CM and NYESS Report (NYRP). Within these categories, various roles are available.

Typically, users of the NYESS Case Management system will require NYESSCM Basic Data Entry. This provides access needed to use the Case Management (OSOS) system for delivery of employment services.

Office supervisors may require NYESSCM Supervisory access, which allows staff to manage service offerings and data for their office. Users need NYESSCM Basic Case Data Entry or NYESSCM Supervisory.

NYESSCM Supervisors (s): Office Name and Supervisor Name drop-down must contain data for reports to function appropriately.

Additional case management roles may also be available to select organizations. Questions about these roles should be addressed via the NYESS Contact Form.

NYESS Reporting is available at four role levels

These are:

- **Directly Supported Seekers:** This provides report access to job seekers for whom you are providing case management support directly. This is essentially reporting of the information you have entered in the case management (OSOS) system
- **Supervisor:** This provides you access to not only individuals for whom you are providing direct case-management support, but also those job seekers who are being supported by staff you supervise.
- **Office Administrator:** This role provides report access to all job seekers supported by your selected office(s).
- **Provider/Organization:** This group grants access to Ticket To Work and other reports for all job seekers handled by all offices within your organization.

NYESS Cross-provider Reporting is available to oversight organizations, such as state and local jurisdictions and provides aggregated data based on locale and/or funding streams. Access to these roles will require review and approval by the NYESS business office.

If you have additional questions or concerns, please contact us at mhpd@omh.ny.gov or (800) 430-3586.