

# CATEGORY: SECURITY ~ Add New User, Permission & Roles

## Add a New User

Click 'Admin' > [User Maintenance] > [Add] > Choose a permission 'Role' for the user and [Save]

The screenshot shows the 'User Maintenance' interface. At the top, there is a 'Filter Criteria' section with a 'Clear' button and a search box. Below this is a 'User ID' search box with a 'Search' button. A modal window titled 'Enter your Password to Continue' is overlaid on the search box, with a password input field and a 'Submit' button. A blue callout box points to the modal with the text: 'Enter your password and click [Submit]'. Below the search box are 'Add' and 'Delete' buttons. The main form is titled 'User Information' and contains fields for 'User ID' (DDUCK), 'Full Name', 'First Name' (DONALD), 'Last Name' (DUCK), 'Active?' (checked), 'Email' (dduck@gmail.com), 'Etactics User ID', 'Area', 'Phone', 'Ext', 'Password Expiration' (3 Months), 'Temporary Password' (123456), 'Timeout' (10 Minutes (HIPAA Compliant)), 'IP Access Rules', 'Time From', 'Time To', 'Time', 'eBridge User ID', 'List of the Practice DBs' (61), 'User Can Access Following Databases' (OPENPM TEST[61]: checked), 'User Security' (Role: FRONT DESK), and 'System Permissions'. A 'System Permissions' tree is expanded to show 'reference batch' with a search box. The tree includes: Patients, Guarantors, Scheduling, Charges, Accident, Apply Copay, Charges Dashboard, and Charges From Active Reference Batch. A green callout box on the right says: 'We recommend a naming convention of First Initial, Last name as the User ID. This User ID will never change. Do not fill in anything in 'Facility''. The 'Facility' field is empty.

## Permissions

'System Permissions' are organized in a 'tree' for the Administrator to allow or block users from screens and functions. In our example, we typed 'reference batch' which opened the tree for our review.

Click the plus (+) sign by 'System Permissions' to use 'Search' to find specific permissions by searching for the screen name. TIP: Use the name of the page found in the header at the top of each screen and use that in the 'Search' field.

## Roles

Security Roles allow the Administrator to assign 'Roles' to each user. There are six predefined roles. These roles can be modified to affect all users with a role or new ones can be added to meet the unique needs of your practice.

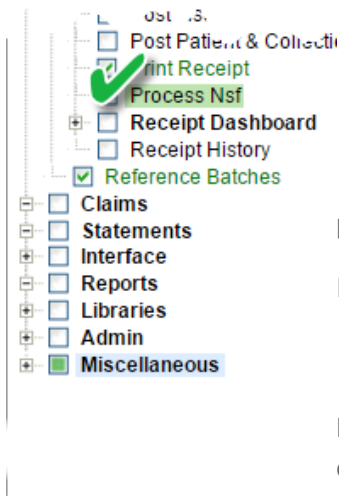
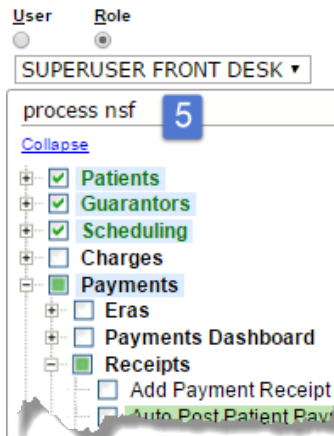
Security Roles		
Name	Permissions	Description
<a href="#">ADMINISTRATOR</a>	<a href="#">View</a>	Complete Access
<a href="#">BILLER</a>	<a href="#">View</a>	Charges, Payments, and Limited Libraries
<a href="#">FRONT DESK</a>	<a href="#">View</a>	Scheduling, Registration, & Receipts
<a href="#">PROVIDER</a>	<a href="#">View</a>	Look-up Access, Schedule, and Reporting
<a href="#">SCHEDULER</a>	<a href="#">View</a>	Scheduling & Registration
<a href="#">VIEW ONLY</a>	<a href="#">View</a>	Limited Look-up Access

# CATEGORY: SECURITY ~ Add New User, Permission & Roles

## How to add a new 'Role' and edit 'Permissions'

Go to Admin > Role >

1. Click [ADD]
2. Create a name and copy an existing Role you want to modify (add or subtract permissions)
3. [Save]
4. Click View to Edit Permission OR to go the Permission button in Admin

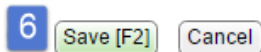


5. Use the 'Search' field, type a feature to open the security tree > check to give a permission, uncheck to take away a permission

In our screenshot we gave the front desk 'super user' the ability to post NSF

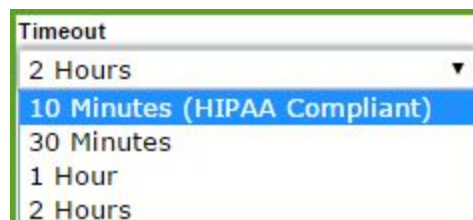
6. [SAVE]

Now this role can be assigned to any User. This makes the task of adding new employees with special security rights very easy.



## I am getting logged out too often, what should I do?

The system admin user is able to Change the 'Timeout' from the system delivered 10 minutes to more time.



## How can I limit a user's access?

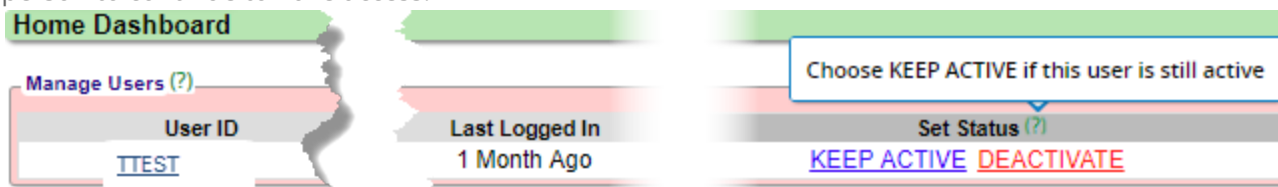
If an IP address is entered, the user will only be able to access from that IP address. You can control the days of the week, and times a user is allowed to log in.

The screenshot shows two sections: 'Timeout' and 'IP Access Rules'. The 'Timeout' section has a dropdown menu set to '10 Minutes (HIPAA Compliant)'. The 'IP Access Rules' section has a yellow background and contains a text input field for an IP address, a 'Time Zone' dropdown set to 'Eastern', and a row of seven checkboxes for days of the week (Mon-Sun), all of which are checked.

## How do I 'Reactivate' a User?

A user who has not logged in for 30 days will not be able to log in until their User has been Reactivated. This is a security measure.

The Site Administrator will be alerted on the 'Home Dashboard' in the 'Manage User' section, which appears when a user(s) has not logged into the system in a month or more. Simply click 'Keep Active' if you wish this person to continue to have access.



You may also, Go to 'Admin' > [User Maintenance] > Click 'Reactivate' in the 'Last Accessed' column with the user name

The screenshot shows the 'User Maintenance' page with a search filter and a table of users. The table has columns for User ID, Last Name, First Name, Group ID, Role, DB List, Reactivated, Last Accessed, and Active. A user with ID 'SUPPORT1' is highlighted in green, with '7 months ago' in the 'Last Accessed' column and a 'Reactivate' link.

User ID	Last Name	First Name	Group ID	Role	DB List	Reactivated	Last Accessed	Active
SUPPORT1	SUPPORT	SUPPORT	SUPPORT	13		✓	7 months ago	Reactivate ✓

## How do I make a user Inactive?

Click 'Admin' > [User Maintenance] > User ID > type your password to get to 'User Information' Un-check the 'Active' check-box, under, 'User Information', when a user is no longer with your organization. The user name is retained in the database, however the user may no longer log in.

The screenshot shows the 'User Information' page for user 'DDUCK'. It displays fields for 'User ID', 'Full Name', 'First Name', and 'Last Name'. The 'Active?' checkbox is checked.