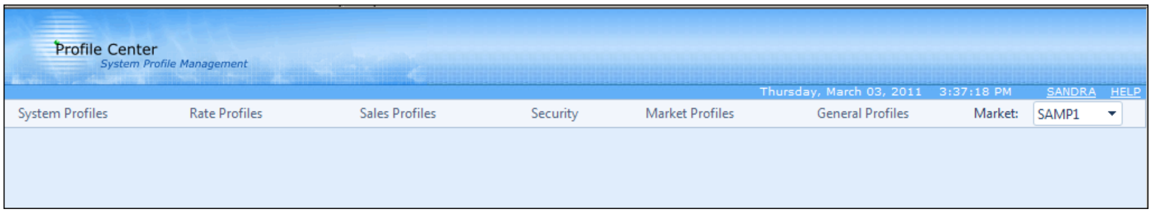
Profile Center

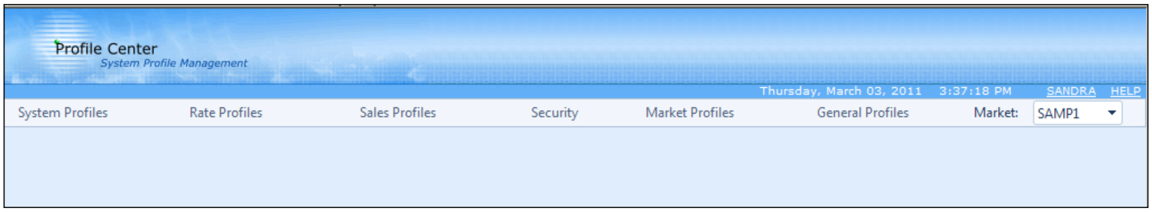


Security

CONTENTS

Profile Center

This document describes the **SECURITY** module found in the Profile Center.



The **PROFILE CENTER** is divided into six modules.

These five modules are used to create profile codes used throughout your database:

- The **SYSTEM PROFILES** module is used to create:
    1. Discounts and Non-Usage Charges
    2. Additional Profile Codes, such as Equipment, Features, Monthly Recurring Changes, and other Profiles that are used throughout the system
    3. Carrier Information codes
    4. And Track Financial Activity

- The **RATES** module is used to create rate tables used to calculate:
    1. Terminating rates
    2. Recurring and Non-Recurring Fees

- The **SALES PROFILES** module is used to create:
    1. Codes representing your Sales Agents
    2. Commission Plans used during production to calculate commissions for your agents
    3. Reports that will assist in paying your agents commissions

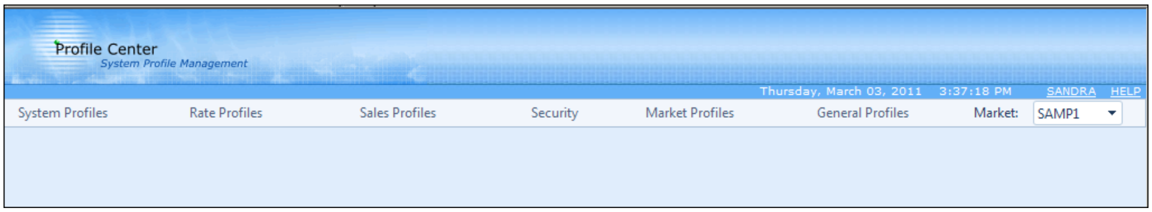
- The **SECURITY PROFILES** module is used to create user ids and passwords for your users to access various areas of the system.

- The **MARKET PROFILES** module is used to setup default information used throughout your database. These items include:
    1. System wide messages
    2. State messages
    3. General Market Defaults
    4. Cycle End Dates
    5. Market Settlements

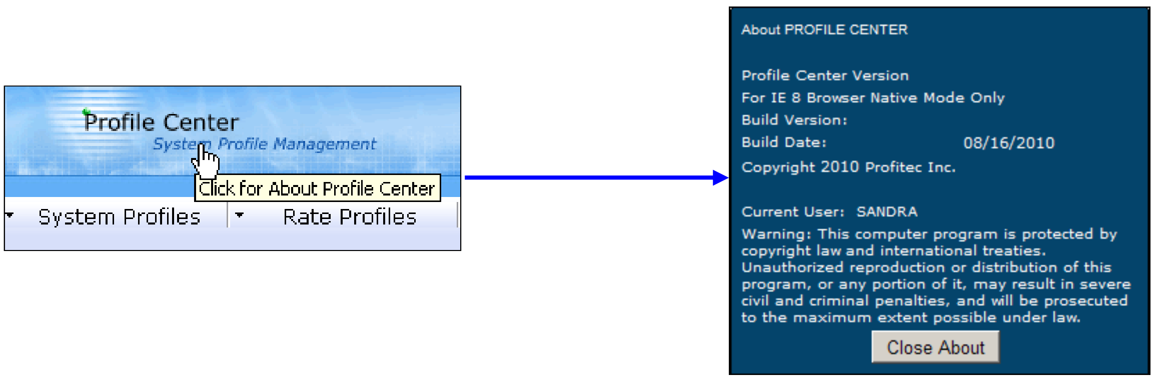
- The **GENERAL PROFILES** module is used to perform various tasks within the system.

Common Profile Center Features

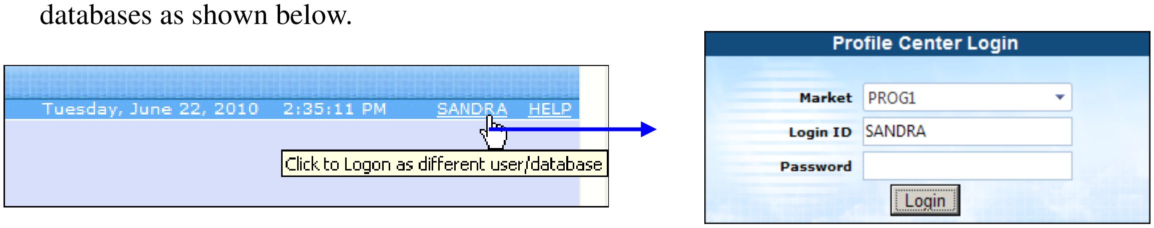
Many areas of the Profile Center include tooltips or short descriptions specific to the Profile Center as you mouse over items.



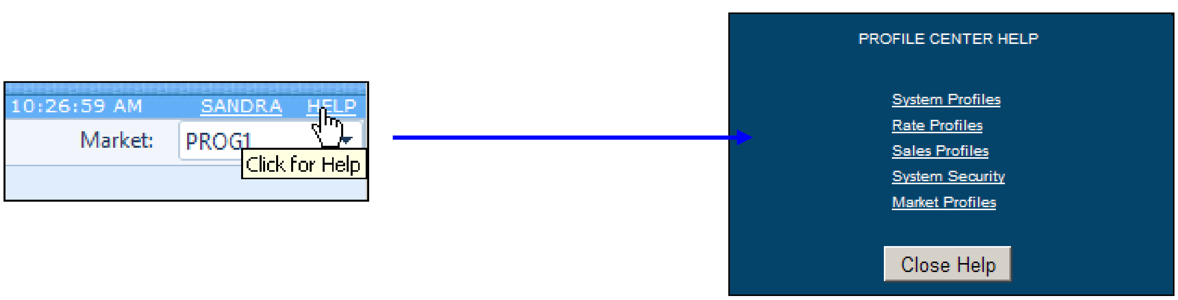
1. **MOUSING** over **/ CLICKING** the words **PROFILE CENTER** in the Profile Center banner displays information about the Profile Center. Build Version as well as Build Date display.



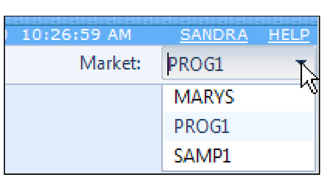
2. **MOUSING** over **/ CLICKING** your **LOGIN NAME** is use to logon as a different user or change databases as shown below.



3. **MOUSING** over **/ CLICKING HELP** displays the Profile Center Help menu. Each module in the Profile center includes a help document as seen below.



4. The down arrow next to the current Market is used to switch to another market within your database.



System Security

SYSTEM SECURITY module is where user rights are established and maintained. Security defines who can access the system and where that user is allowed to function within the system. A user's information is entered in three sections:

USER INFORMATION	RIGHTS	ADVANCED OPTIONS	MESSAGE/SIGNATURE
Defines the user and how OmniBill identifies that user.	Specifies areas the user can view, update, edit, add, or delete information.	Defines which additional tools/privileges the user can access.	Area for message, logo, and scanned signature (CSR profiles only).

The first time OmniBill is accessed, the Admin login ***SUPER*** must be used as the **LOGIN ID**. The **password** should be left **blank** when logging into OmniBill for the ***first time***. The system prompts the user to set a password. The **Admin Login ID** is a default User ID that comes with the OmniBill database. This user ID by default only has access to System Security.

Click **OK** and the **CHANGE OMNIBILL PASSWORD** screen appears. The new password must be typed in the **NEW PASSWORD** area and retyped in the **CONFIRM NEW PASSWORD** area. This only happens the first time the OmniBill is accessed. When **OK** is clicked, the Market General Information screen appears and must be completed before the remainder of the system can be accessed.

When **MARKET GENERAL INFORMATION** is completed and saved, the administrator can only access **SYSTEM SECURITY** or **EXIT** OmniBill. Administrators should proceed by creating their system profile. Administrators usually give themselves master rights so they have access to all areas of the system. The administrator must create user profiles for each user who will use the system. No one can access the system without a profile established in System Security.

Changes made to a user's profile do not take effect until the user logs out and logs in again.

Common Profile Buttons

The following items are used throughout the Profile center.

 The binoculars are used as the **SEARCH** button.

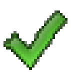
 The eraser is used as the **CLEAR SEARCH CRITERIA** button.

 The green circular plus is used as the **ADD** button.

 The red circular white X is used as the **CLEAR ERROR MESSAGE** button that appears only when an error is encountered and trapped.

 The small blue arrow right is used as the **SELECT** button in grids throughout System Profiles. Clicking this button only selects a row; clicking the blue underlined link-description to the right of the arrow does both a select and a go that displays detail for the selected summary record.

 The small circular red circular white X is the used as the **DELETE** button in grids throughout System Profiles.

 The large green check is used as the **OK** button on pages throughout the Profile Center.

 The large red X is used as the **CANCEL** button on pages throughout the Profile Center.

 The 'sign forbidden' is used as the 'No' button in popup message boxes where the question 'One or more data fields has changed. Do you wish to save these changes now?' is displayed.

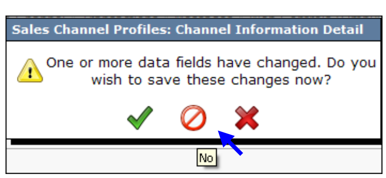
 The floppy disk is used as the **SAVE** button. This is the enabled image.

 The grayed out floppy disk is used as the **SAVE** button to create a disabled appearance.

 The two cylinders are used as the **DUPLICATE** selected Row button to create an exact duplicate of the item selected.

 The add button is used where it's permissible to **ADD A NEW ROW** to a grid.

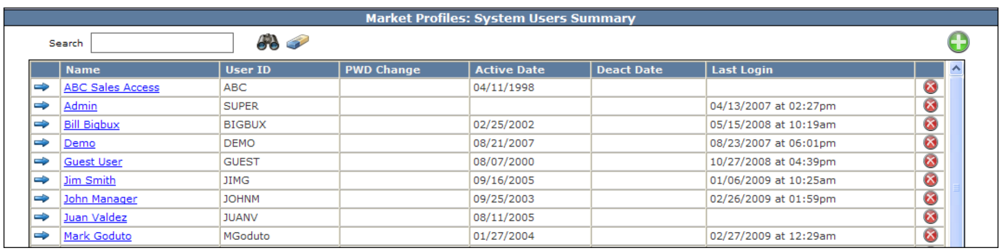
Icons used throughout the Profile Center include a tooltip or a short description specific to the button as you mouse over the item.



Accessing System Security

In order to access any areas of OmniBill, users must have a Login Id, passwords, and user rights assigned to them. The System Administrator as well as users given access rights to the System Security module can assign user rights. Consider a user's job function when assigning rights to individuals. Security controls what information users can view, add, update, edit, and delete in the database.

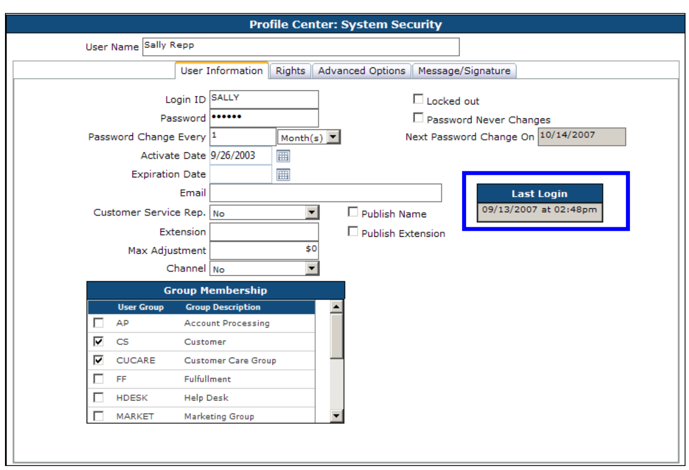
Action	Description
1. Click **SYSTEM USER MAINTENANCE** from **SECURITY**.	The **SYSTEM USERS** screen displays a list of system users.



The **SYSTEM USERS** list shows the **NAME** of each user who has or had access to the system, the **USER ID**, the next date the password needs to be changed (**FORCED PASSWORD**), the first date the **USER ID** is valid (**ACTIVATE DATE**), and the **DEACTIVATE DATE** if the **USER ID** is no longer valid. The last column is a system generated **LAST LOGIN** field. It is used to track the date and time the user last logged into the system.

2. Click the user name from the list to access their System Security detail screen.

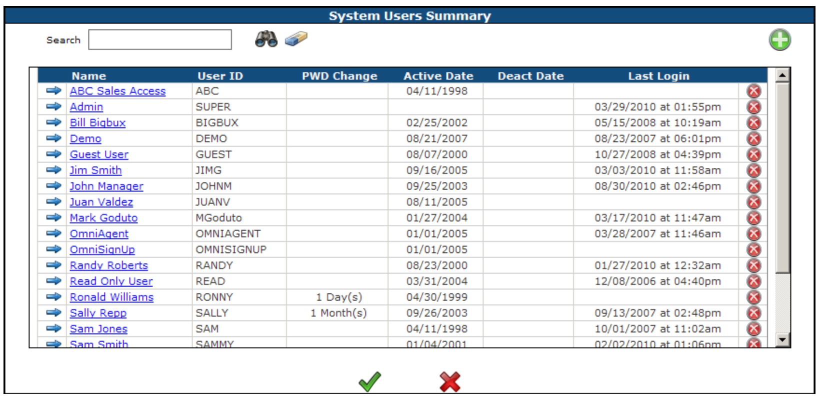
The **LAST LOGIN** field also appears on the User Information tab in the **SYSTEM SECURITY** screen.



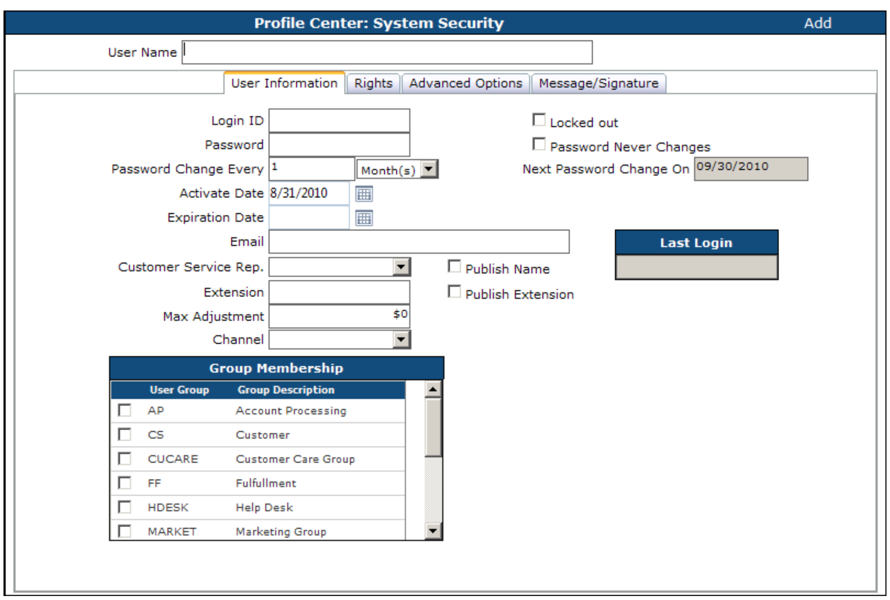
Adding a New User

Before a user can access OmniBill, he or she must have a security profile created and stored in System Security. The user's security profile defines to what extent the user is able to function within the system.

Action	Description
1. Click **SYSTEM USER MAINTENANCE** from the Security drop down list.	The **SYSTEM USERS** list appears.



2. Click the **GREEN PLUS** button.	The **SYSTEM SECURITY** screens opens.



3. Enter the **USER'S NAME**, **LOGIN ID** and **PASSWORD**.	The **PASSWORD** is always encrypted and not visible to any users in the system, regardless of what rights they may have.

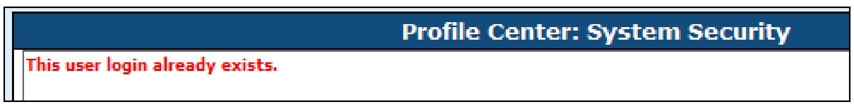
User Name

The **USER NAME** is the complete name that identifies the user.

Login ID

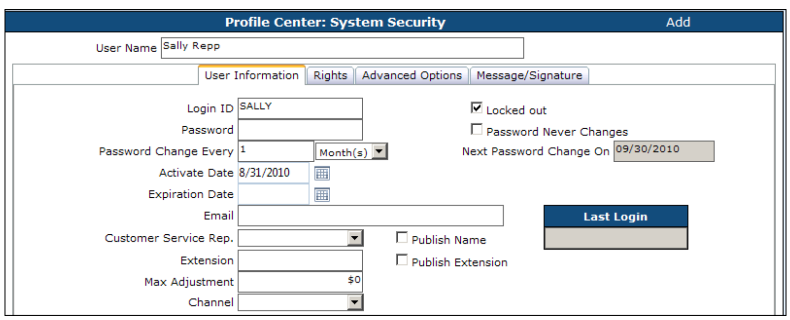
The **LOGIN ID** is used when the user logs into the system. Each action the user performs (transactions, changes to customer's accounts, notes, trouble tickets, etc.) is associated with the **LOGIN ID**.

The Login ID can be alphanumeric and a maximum of eight characters. No users can share the same Login ID and it must be unique for the database. If the same Login ID is entered for multiple users, a message appears when you try to **SAVE** the user profile:



Locked Out

The **LOCK OUT** feature prohibits a user's access to the database. This option functions in two ways depending on the ***initial*** setting for the **LOCK OUT** box.

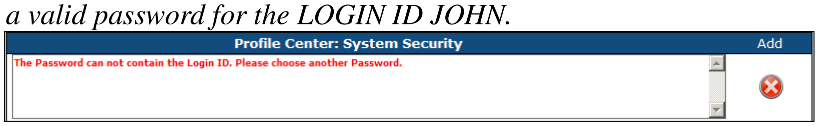


- **Checked** The user login and password no longer are recognized. The user cannot access the system.
- **Unchecked** Three incorrect user login attempts trigger the system to automatically check the box and lock the user out of the system. This is a security precaution intended to prevent an undesignated user from accessing the system. If lockout occurs, only a user with access to the System Security can clear the checkmark.

Password

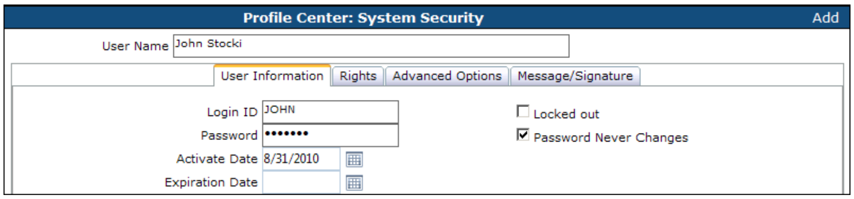
The **PASSWORD** is not case sensitive and must be at least five (5) characters and a maximum of 15 characters. The password can be any combination of letters or numbers.

The password cannot be the same as the Login ID or contain any portion of the LOGIN ID, i.e. JOHN2 is not a valid password for the LOGIN ID JOHN.

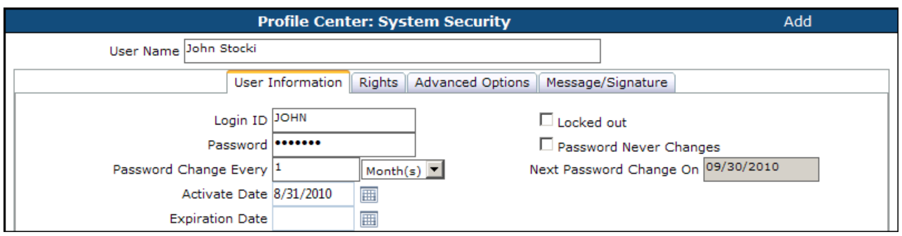


Password Never Changes

When checked, the password for the user never expires. The box is unchecked by default. If checked, the **PASSWORD CHANGE EVERY** and **NEXT PASSWORD CHANGE ON** fields do not appear.



If unchecked, the **PASSWORD CHANGE EVERY** and **NEXT PASSWORD CHANGE ON** fields dictate how often the user is forced to change their password. The first input area uses a numeric value, and the drop down list identifies the measure of time (Days, Weeks, Months, and Years). The system automatically prompts the user to change their password at the appropriate time.



Activate Date

The **ACTIVATE DATE** is the first date the user is allowed to access the system. If no date is defined, the date the profile is created is used.

Expiration Date

The **EXPIRATION DATE** is the last day the user is allowed to access the system using the established user name.

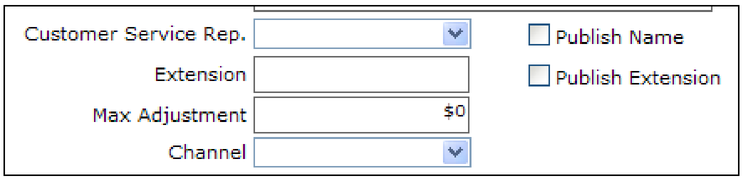
Email

The **EMAIL** field is used in conjunction with the Action Tickets module. Action Tickets are used to identify customer issues and troubles. Entering an email address here allows the user to receive an assigned trouble ticket through email. If the email field is blank, the trouble ticket cannot be delivered to the user.

Customer Service Rep.

This **YES/NO** field defines whether or not the user is a customer service representative. Selecting **YES**:

- Adds the user's name to a CSR selection list when assigning a dedicated customer service representative to an account.
- Enables the Message/Signature tab where a customer service representative can create a message that will print on their account invoices.



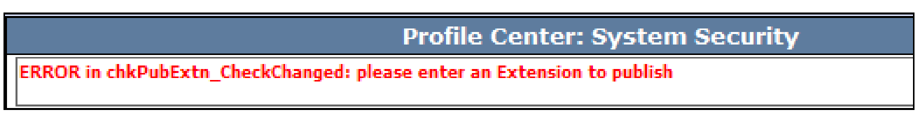
Publish Name

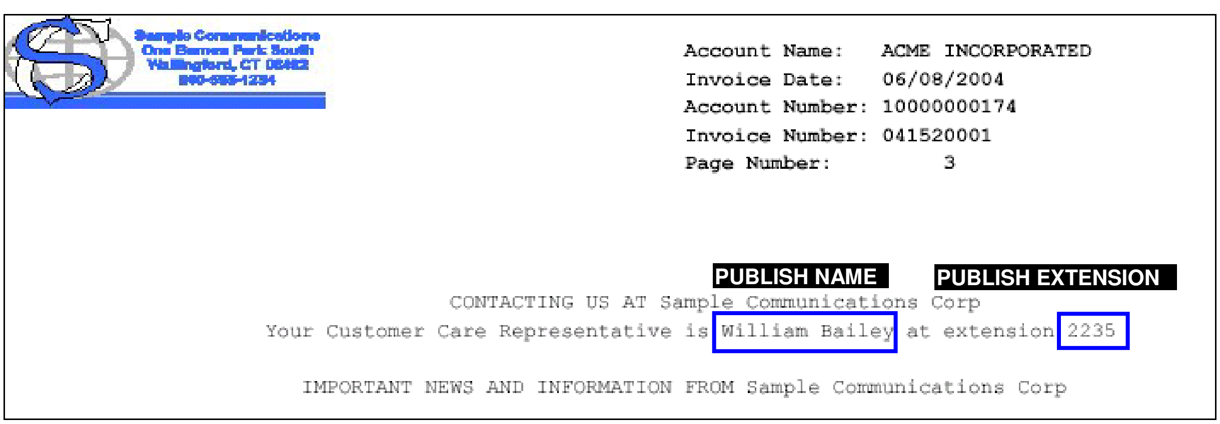
If checked, a user designated as a customer service representative will have their name print on invoices for all accounts for which this user is selected as the dedicated customer service representative. You must select a Customer Service Rep when selecting Publish Name.

Publish Extension

If the user is a customer service representative and has specific customer accounts assigned to them, checking **PUBLISH EXTENSION** causes the customer service representative's extension to print on account invoices.

An extension must be entered in order to publish one, if an extension is not entered and the Publish Extension field is checked a message displays.





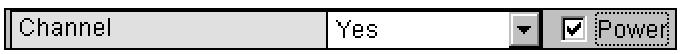
Max Adjustment

The value entered represents the maximum dollar *adjustment* amount the user is allowed to apply to a single transaction with a **Transaction Type** code of **U** or **I**. Only transactions specified as an adjustment-type transaction are affected by the value stored here. The maximum amount that can be entered is 999999 and will display as $999,999.

Channel

The **CHANNEL** drop down list is a **YES/NO** option. When set to **YES**, the user is designated as a Sales Channel in the system and their login ID is automatically applied **READ ONLY RIGHTS**.

READ ONLY RIGHTS for a user designated **YES** as Sales Channel can only be overridden when the **POWER FIELD** is checked.

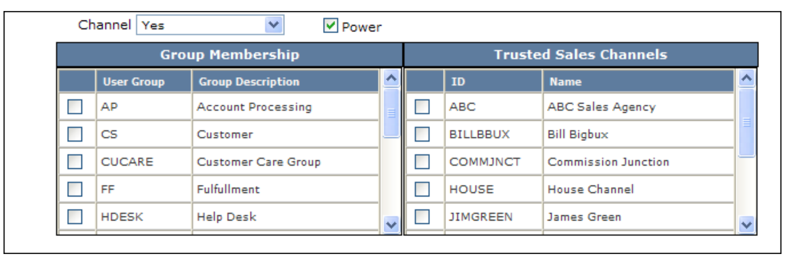


If the **POWER** field is checked, the settings in the **RIGHTS** tab can be customized for the user. **ADD**, **UPDATE/EDIT**, **DELETE** or **READ ONLY** options can be granted for any module.

If the **POWER** option is *not* checked, all settings on the **RIGHTS** tab are ignored, even when Master Rights are selected.

Trusted Sales Channels

The **TRUSTED SALES CHANNELS** grid is used to select which Sales Channel accounts the user can access when logged into the system.



Click the checkbox next to each Channel to give the user access to accounts where:

- They are the Channel ID assigned.
- They are allowed access to other Sales Channel accounts

Sales channels with the **POWER ID** option who are granted **ADD** rights will have their channel Id automatically fill in when they add an account in OmniBill. If they have multiple Channel names highlighted, their channel ID does not automatically fill in, however only the highlighted channel IDs under Trusted Sales Channels appear as a choice.

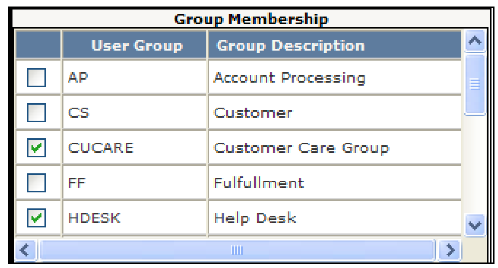
System administrators must be sure to select the Channel ID for which the profile is being created or that channel will not be able to access their own accounts.

Group Membership

Selecting a **USER GROUP** from the Group Membership list is a required step when creating a user's security profile. The **GROUP MEMBERSHIP** list is used in conjunction with Action Tickets. Action Tickets are assigned to Groups for tracking purposes. Refer to Section 13 – Action Tickets for more information.

Users can be associated with multiple groups by selecting them in the list. The default choice, **SYSTEM – SYSTEM GROUP**, ships with the database and can be used to satisfy this requirement if you are not using Action Tickets.

The list at the right shows multiple User Groups selected. The groups are created in System Utilities. Refer to ***Section 21*** for information on creating User Groups.



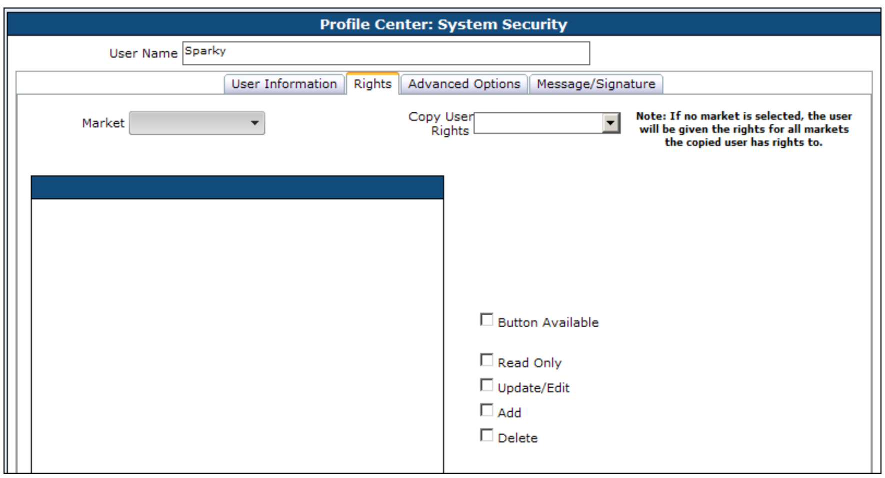
User Rights

User rights should be assigned based on the user's job responsibilities. The **RIGHTS** tab is used to define the areas of the system within a market a user can access. If your company has multiple markets, users can be granted access to different markets using one Login ID.

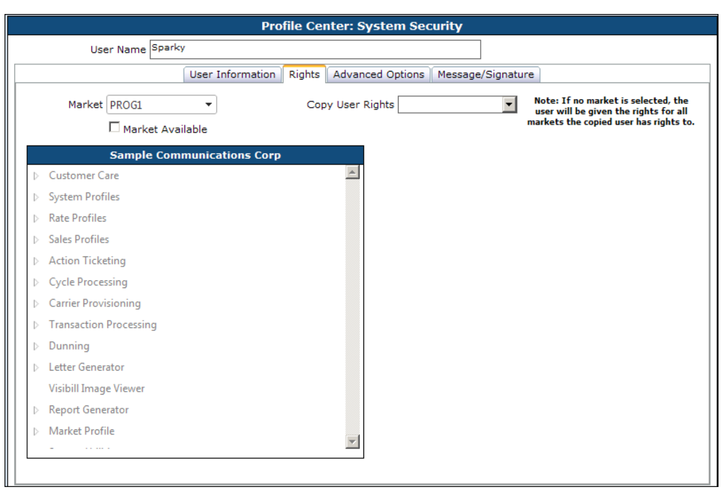
The **RIGHTS** tab is also used to select what level of access the user has in the system. All access can be given to a user by selecting **MASTER RIGHTS**. As a data entry tool, rights can be copied from existing user right profiles to new users.

Selecting User Rights

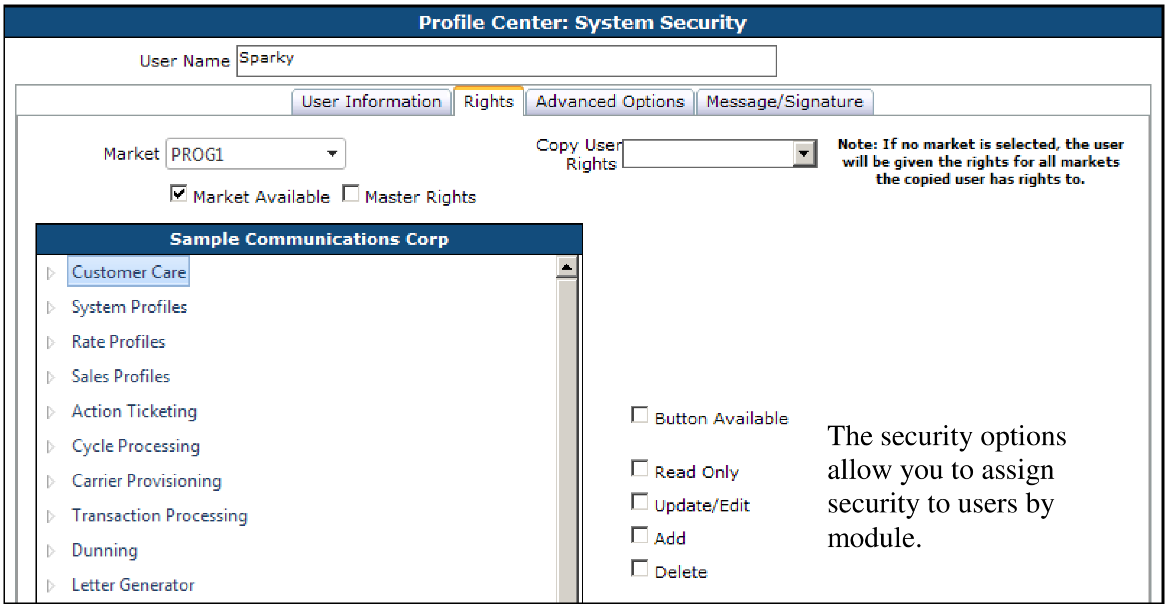
Action	Description
1. Click the **RIGHTS** tab.	Rights for existing users are not displayed until a **MARKET** is selected.



2. Select a **MARKET** from the drop down list. A user needs to have a Security Profile created for each one of your markets.	A **MARKET AVAILABLE** option appears.



Action	Description
3. Check **MARKET AVAILABLE** to allow the user to have access to the selected Market.	When the **MARKET AVAILABLE** box is checked, the **MASTER RIGHTS** box displays along with five security options.



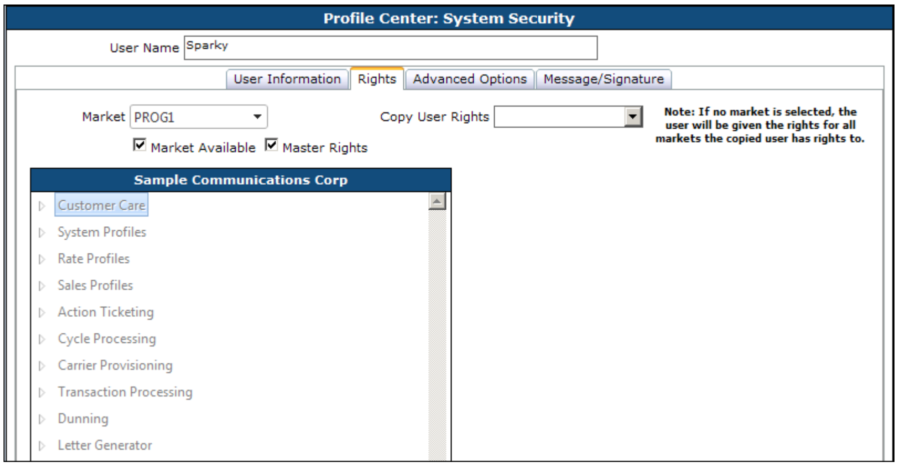
USERS WITH MASTER RIGHTS

A user must have Master Rights in order to do the following within OmniBill.

- Remove the **LOCK-OUT** field on a User Security record.
- View the entire Credit/Debit card number. Users without Master Rights see xxx within the card number.
- Remove Suspend and Reinstate date fields on all customer accounts.
- Invoke the Channel/Commission change utility on the customer screen.
- Change an Action Ticket assignee if not a member of the next assignee group.
- See and use the functions on the Gateway's tab within System Utilities.

Action	Description

NOTE: When **MASTER RIGHTS** is selected, the **FIVE SECURITY OPTIONS** are removed from the screen because a user with **MASTER RIGHTS** has access to all areas of the system. Any user acting as the system administrator should have Master Rights. Options on the **ADVANCED OPTIONS** tab still must be decided upon for the user. Master Rights do not include these options.

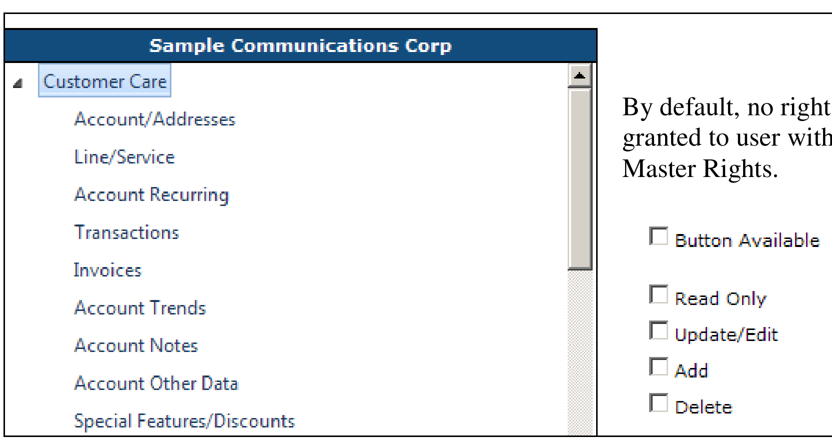


4. Click **MASTER RIGHTS** to give a user access to **ALL** areas of OmniBill.

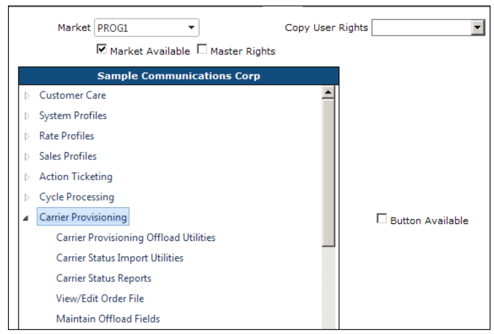
Users that should not have Master Rights to the entire system must be assigned rights to each OmniBill module. Rights can be assigned at the: Main Module level and/or at the individual module level associated with the Main Module.

GRANTING USERS RIGHTS TO INDIVIDUAL OMNIBILL MODULES

Action	Description
1. Click the arrow sign next to a **MODULE** to assign rights.	Individual modules associated with the module selected as well as the **FIVE SECURITY OPTIONS** display.



By default, no rights are granted to user without Master Rights.

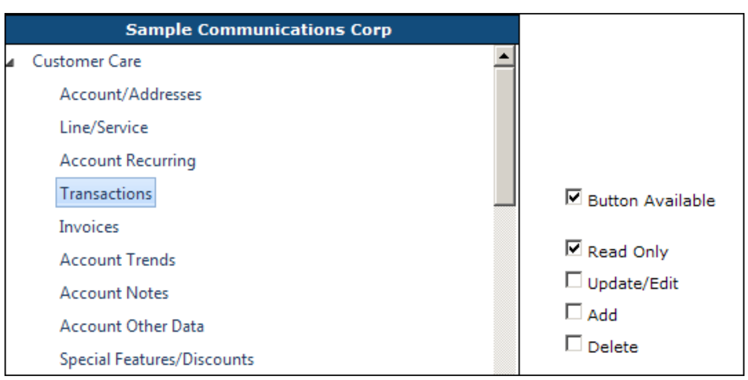
Action	Description
2. Check **BUTTON AVAILABLE** if the user should see the module when they login.	The following modules only have the **BUTTON AVAILABLE** option: • Carrier Provisioning • Transaction Processing • Letter Generator • VisiBill Image Viewer • Report Generator • System Utilities.
For these six modules, the **BUTTON AVAILABLE** option displays only and must be selected for the user to have access to the module.	

By default, **RIGHTS** selected for the Main Module cascade to all modules associated with the selected Module. This alleviates the need to select every sub module when assigning the same rights. However, if you want users to have different rights within the Main Module, you will need to highlight each sub module and grant appropriate rights.

3. Highlight a sub module in the list.

4. Select which **RIGHTS** the user has to the highlighted sub module by checking **READ ONLY**, **UPDATE/EDIT**, **ADD** and/or **DELETE**.

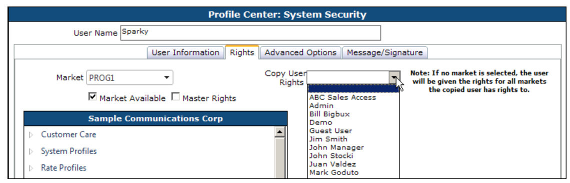
In the below example when the user logs in they will see **LINE/SERVICE** in the Customer Care toolbar, but they will have **READ ONLY ACCESS**. Meaning the user cannot: **UPDATE/EDIT**, **ADD**, or **DELETE**.

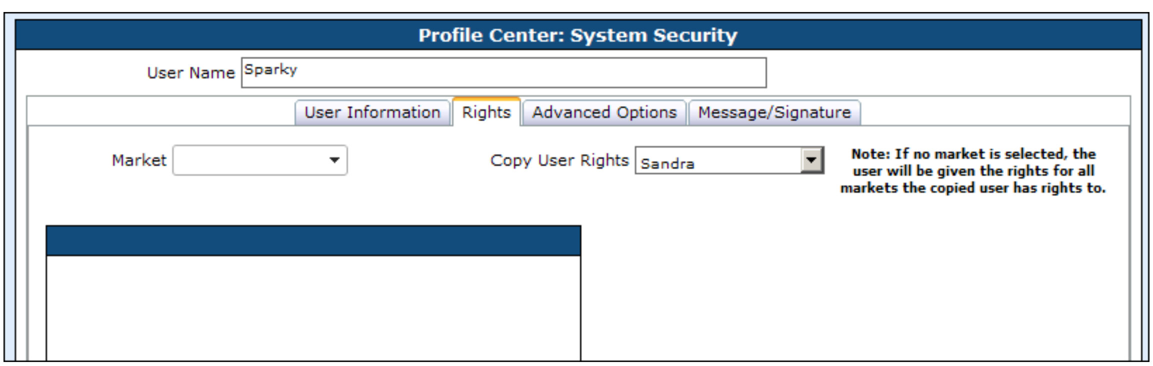


Rights can be customized for every module and sub module in OmniBill.

Copy an Existing User's Rights

The **COPY USER RIGHTS** option is used when it is necessary to give multiple users the same access rights to various system modules. When user rights are copied, the options set on the User Information tab and the Advanced Options tab are *not* included.

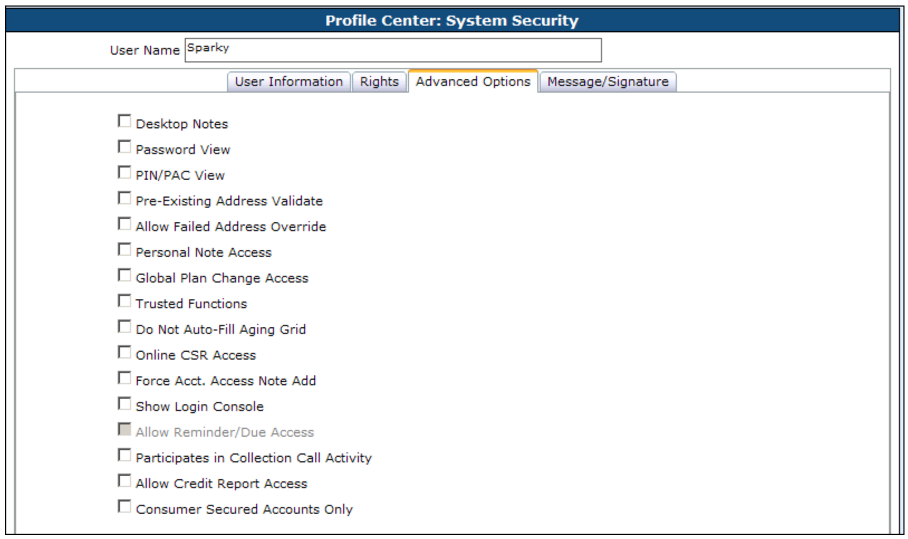
Action	Description
1. Click the **MARKET** drop down list and select a Market.	The **MARKET AVAILABLE** check box appears. 
2. Check **MARKET AVAILABLE**.	When the **MARKET AVAILABLE** box is checked, the **MASTER RIGHTS** box and a list of system modules appear.
3. Click the **COPY USER RIGHTS** drop down list.	A list of existing system users appears. If no Market is selected, the user will be given the rights for all markets the copied user has rights to.
4. Select the **USER** from the list whose rights you want to copy.	The **USER NAME** whose rights were copied displays in the **COPY USER RIGHTS** drop down list. The remainder of the screen is blank.



NOTE: To view the rights just granted to the user, save and exit the profile. Reopen the profile and you will be able to view the rights granted.

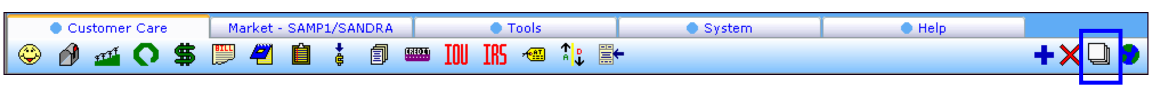
Advanced Options

The **ADVANCED OPTIONS** tab is used to define additional capabilities for system users. Advanced Options are not automatically included for any users.

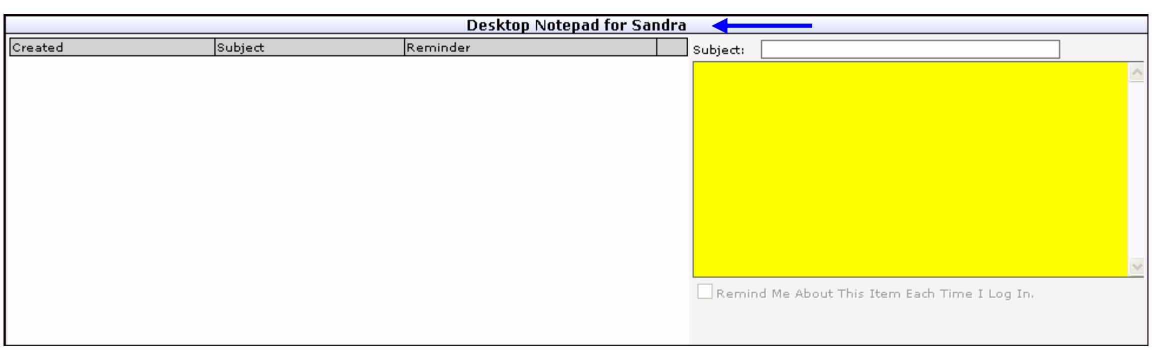


Desktop Notes

Selecting **DESKTOP NOTES** gives the user access to the **DESKTOP NOTES** area in the Main toolbar. If this advanced option is not selected, the user does not see the Desktop Notes icon in the toolbar when they login. This setting is not market-specific. The user will or will not see this button in all established markets depending on the setting.



When the user is logged in, clicking the Desktop Notes icon displays a notepad only for that user. The user's name displays at the top of the screen. These notes are only accessed when using the user's Login ID.



Password View

When **PASSWORD VIEW** is checked, the user is able to view the password set on an **IN** (Internet) **LINE TYPE DETAIL** screen when viewing an Internet line.

PIN/PAC View

When **PIN/PAC VIEW** is checked, the user is able to see the personal identifiers on a customer's travel card or cable line.

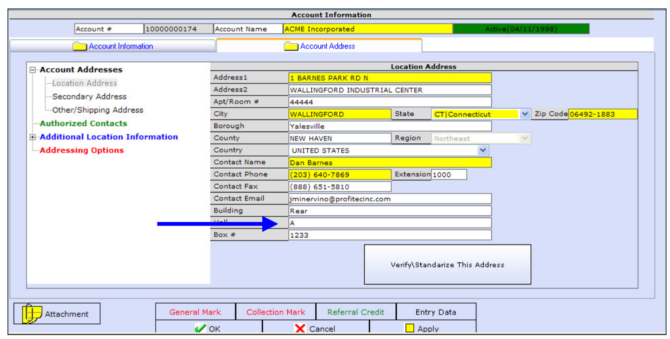
Pre-Existing Address Validate

Customers validating addresses with DesertSoft/Strickiron, a company who validates mailing address in the United States, can use this advanced option to give a user the ability to verify an **EXISTING** address in their database.

In databases using **DESERTSOFT ADDRESS VERIFICATION**, all new addresses entered are verified automatically even if this option is not selected on the user's security profile.

Users with the **PRE-EXISTING ADDRESS VALIDATE** option selected see a **VERIFY\STANDARDIZE THIS ADDRESS** button on the Address Information tab on a customer's account.

Because DesertSoft/Strikiron assesses a cost each time an address is verified, this function should be reserved for a select group of users.



Allow Failed Address Override

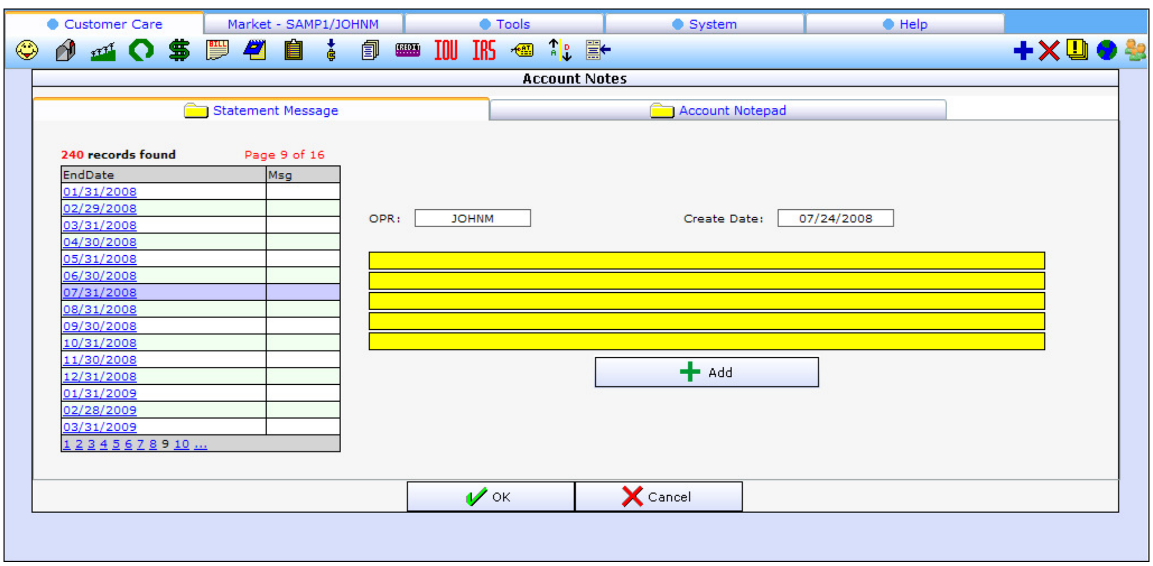
The **ALLOW FAILED ADDRESS OVERRIDE** option is used to indicate that the user has the ability to accept an account even though StrikeIron/Desertsoft was unable to validate the address for the account.

NOTE: An account must be established with StikeIron/DesertSoft, and the Address Verification Parameters screen in the Gateways tab must be completed in OmniBill for these new options in System Security to work.

Refer to Section 21 – **SYSTEM UTILITIES** – Gateways tab for information on setting up Address Verification in OmniBill.

Personal Note Access

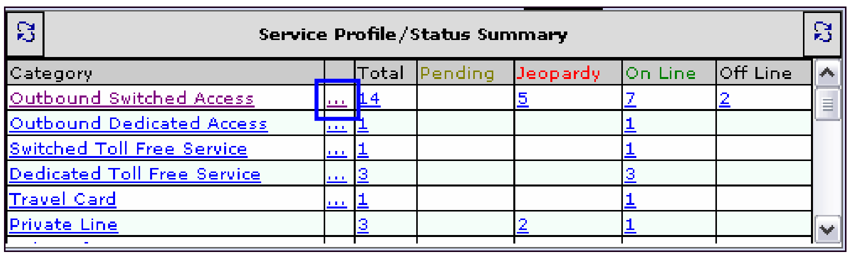
Users with **PERSONAL NOTE ACCESS** can access the **STATEMENT MESSAGES** tab in **ACCOUNT NOTES** when in a customer account. The user is able to select a specific cycle end date and create a message. The message prints on the customer invoice for the selected cycle.



Global Plan Change Access

A user given Global Plan Change Access is able to invoke the **GLOBAL MASTER RATE PLAN UTILITY** by clicking the ... column next to a Service Category on the Service Profile/Status Summary grid in the customer account. The same utility is accessible from the **SPECIAL** tab in **SYSTEM UTILITIES**.

GLOBAL PLAN CHANGE ACCESS should be given to users who don't need access to all the utilities found in System Utilities, but may have a need for the Global Master Rate Plan Change Utility.



Trusted Functions

A user with **TRUSTED FUNCTION** rights can access shortcut menus for specific customer care functions that include:

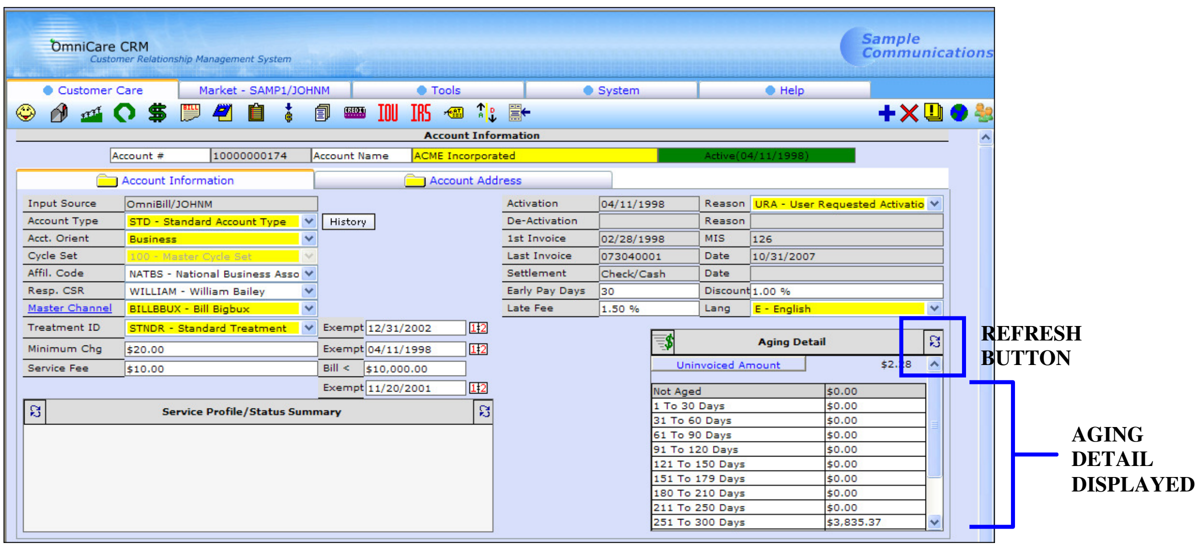
- Accessing the Line Inventory Table.
- Viewing line provisioning history.
- Reprovisioning a line.
- Initiating a global commission plan change and a global master channel change (only if user has master rights).

Do Not Auto Fill Aging Grid

The **DO NOT AUTO FILL AGING GRID** option affects system efficiency. When checked, the system bypasses the aging calculations when an account is opened. The **AGING DETAIL** grid does not display any past due balances in the **AGING** buckets. Only the **TOTAL BILLED DUE** and the **TOTAL AMOUNT DUE** display. The **REFRESH** button to the left of the Aging Detail header must be used to display aging information in the grid.

Users with the **DO NOT AUTO FILL AGING GRID** option checked do not see any aging detail when viewing an account with a past due balance. The user must click the **REFRESH** button in order to fill in **AGING DETAIL** in the grid.

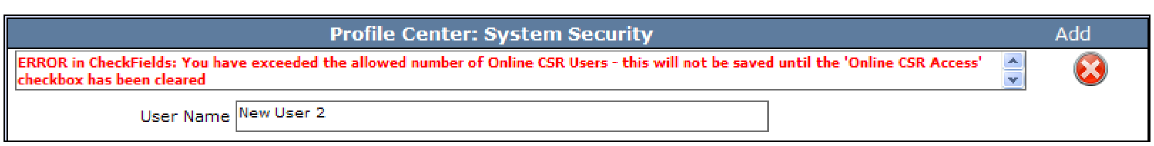
If a User's security profile does not have the **DO NOT AUTO FILL AGING GRID** option selected, they will see Aging Detail when viewing an account with a past due balance.



Online CSR Access

Users given **ONLINE CSR ACCESS RIGHTS** have access to the online chat feature, which can be used in conjunction with OmniBill. Online CSR access is available only if a URL has been set up in Market Defaults and the online chat software has been installed on your server. The current database set-up restricts the number of users that can have this access in your database to two.

If the following message displays, when you try and save a user it means you have exceeded the allowed number of **ONLINE CSR USERS**. The Online CSR Access field must be cleared in order to save the user's security profile.



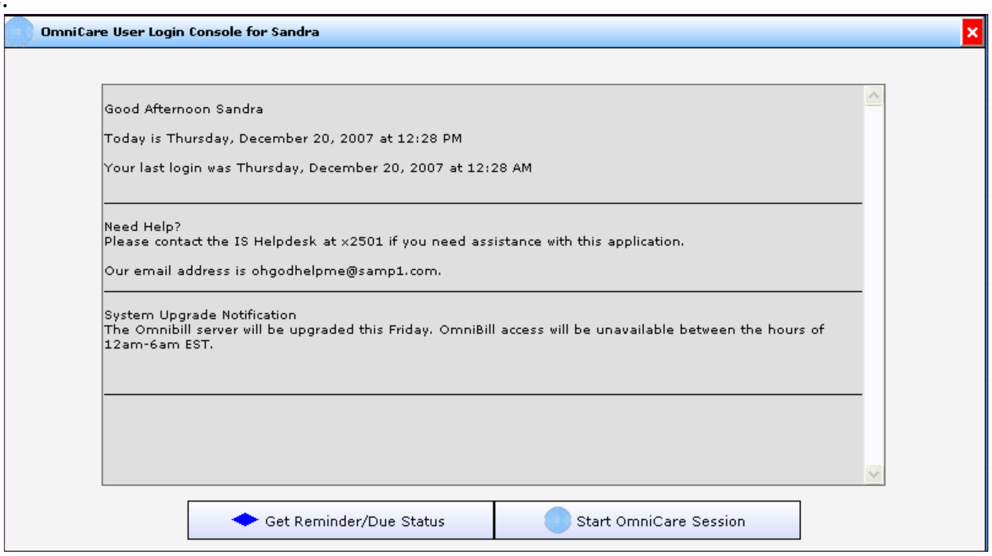
Contact your assigned Billing Analyst if you are implementing this feature and require more users to be enabled.

Force Acct. Access Note Add

Check this option if it is necessary for an account to be annotated *each* time it is accessed. A user cannot leave an account screen without entering a note if this option is checked on their security profile.

Show Login Console

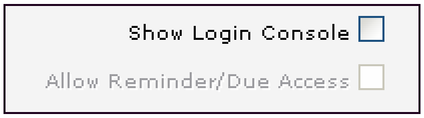
A user with the **SHOW LOGIN CONSOLE** option checked sees the **OMNIBILL USER LOGIN CONSOLE** when they login to the system. Login Console screen displays the last date and time the user Login ID accessed the system The Login Console screen is used to communicate with the user community using date and time sensitive messages and it can also be used to retrieve reminders as long as the user has the Allow Reminder/Due Access option selected in the security profile.

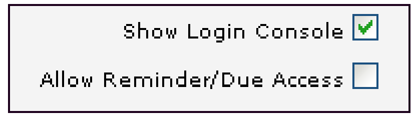


The Login Console messages are created in System Utilities, in the Special Tab, using the **MANAGE USER LOGIN SYSTEM MESSAGES** utility. Refer to Section 21 for information on utilities.

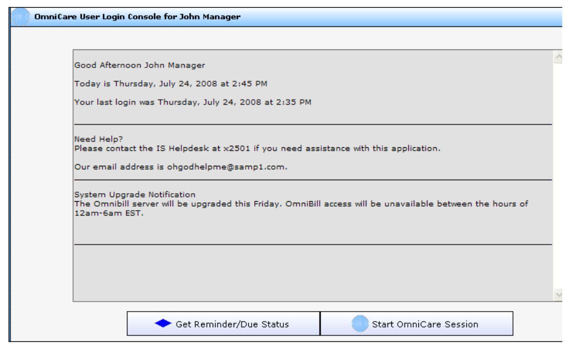
Allow Reminder/Due Access

The **ALLOW REMINDER/DUE ACCESS** option is available only if the **SHOW LOGIN CONSOLE** option is checked.

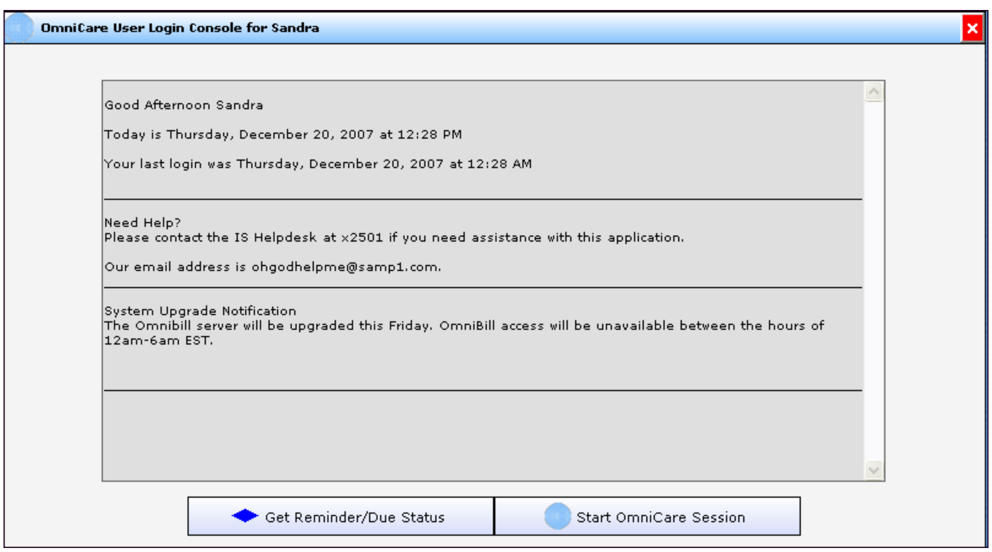




If the **ALLOW REMINDER/DUE ACCESS** option is not selected, when the Login Console screen displays the **GET REMINDER/DUE STATUS** button is grayed out.

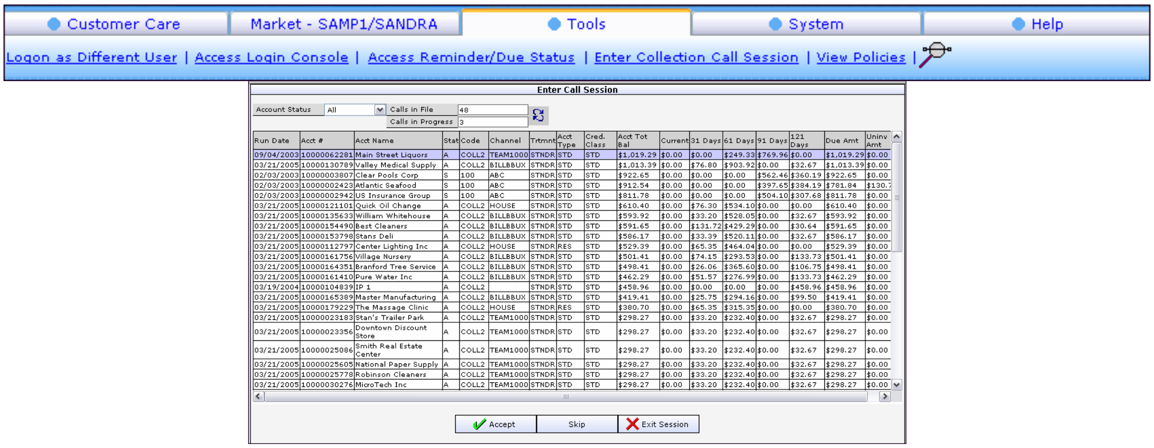


If both options are checked, when a user logs into the system the Login Console screen displays and the **GET REMINDER/DUE STATUS** button is enabled.



Participates in Collection Call Activity

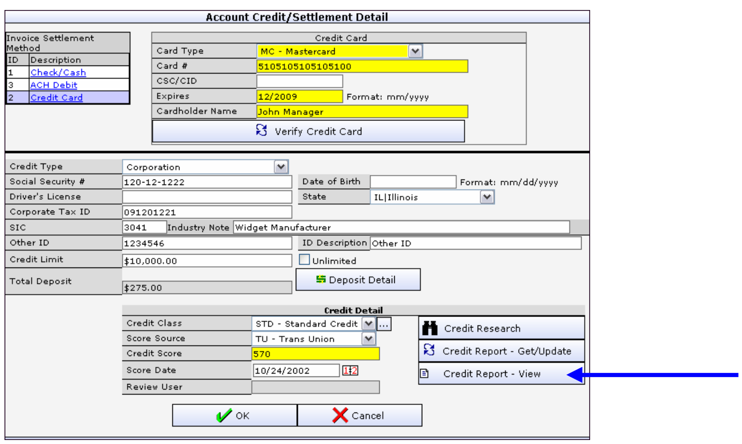
A user with this option selected is able to enter a **COLLECTION CALL SESSION** from the **TOOLS** menu after a call event has been executed from the **MASTER EVENT CALENDAR**. Refer to ***Section 17 Dunning/Collections*** for information regarding the Collection Call Session.



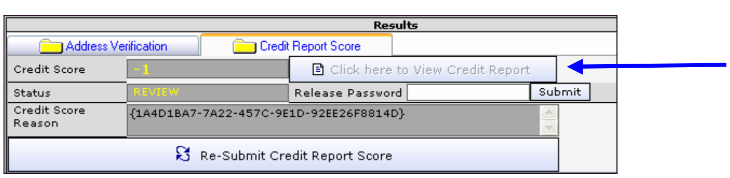
Allow Credit Report Access

Users see the **CREDIT REPORT - VIEW** button on:

- The **ACCOUNT CREDIT/SETTLEMENT DETAIL** screen



- The **CLICK HERE TO VIEW CREDIT REPORT** button on the Add Wizard Detail screen.



Both buttons are used view credit reports returned as a result of running a credit check using the MicroBilt gateway. Refer to ***Section 21 System Utilities*** for more information on MicroBilt.

Consumer Secured Accounts Only

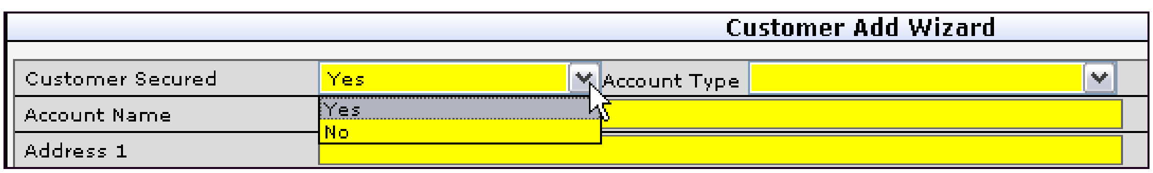
The **CONSUMER SECURED ACCOUNTS ONLY** option, **WHEN CHECKED**, forces the Consumer Secured drop down list to **YES** when a user is creating a new account using the **CUSTOMER ADD WIZARD** as seen in the below screen print from the Customer Add Wizard screen. The customer must go through the credit check process setup in OmniBill.

EXAMPLE FROM OMNICARE

The **CONSUMER SECURED ACCOUNTS ONLY** option, **WHEN UNCHECKED,** gives the user one of two options (YES or NO) when setting up a new account in OmniCare:

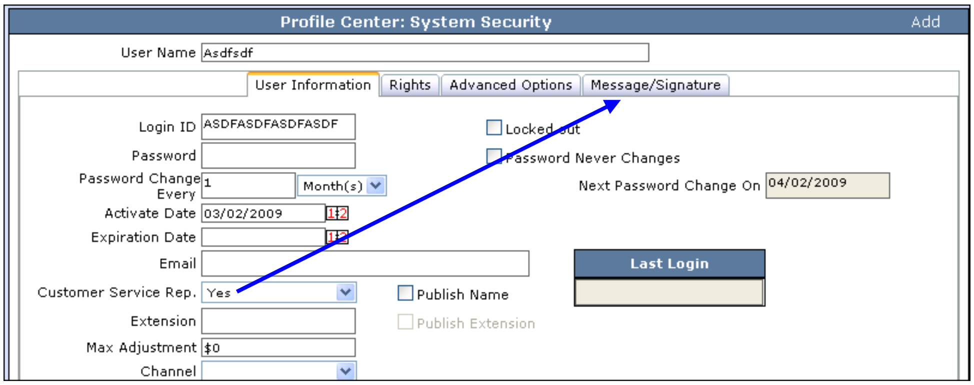
EXAMPLES FROM OMNICARE:

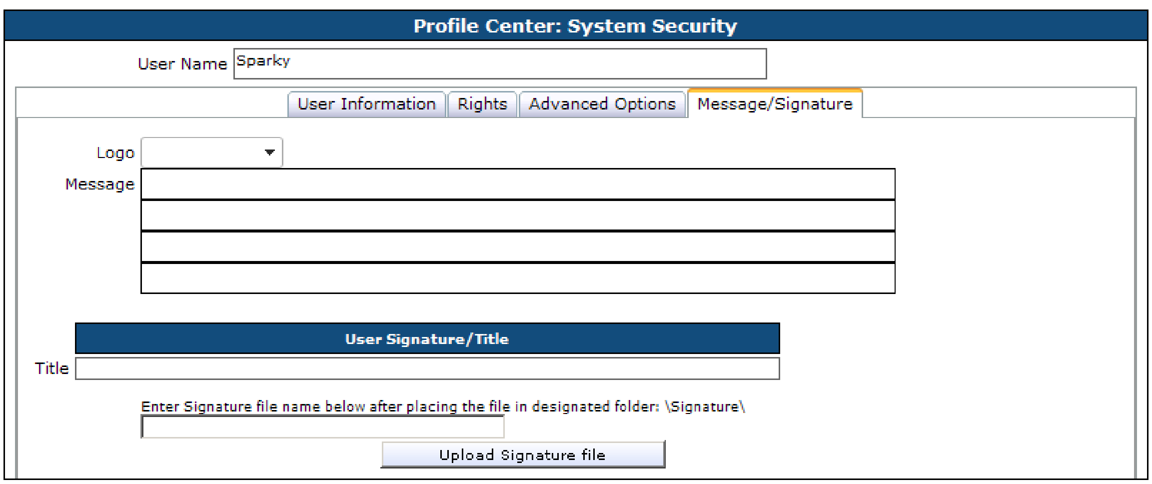
- Selecting **CUSTOMER SECURED – YES** – the account will be run through the credit check before it can be added into OmniCare.
- Selecting **CUSTOMER SECURED – NO** – the account can bypass the credit reporting process.



Message/Signature

The **MESSAGE/SIGNATURE** tab is available only if the user is designated as a customer service representative on the **USER INFORMATION** tab. A message that can be up to four lines, 60 characters a line, can be created and maintained for the user. The message prints on customer invoices each billing cycle for accounts the user is assigned to as the customer service representative. No word-processing capabilities are available.





- The user's title can be entered in the **TITLE** input box.
- A graphic signature file must exist in a folder designated by your System Administrator.
- Enter the exact name of the file in the field provided.
- Click **UPLOAD SIGNATURE FILE**.

The user has the option to use their signature and title on a **QUICK LETTER** generated from **ACCOUNT NOTES** when in a customer account. The signature only appears on letters that are sent directly to the printer.

Updating an Existing User Profile

Any user with access to security can make changes to user profiles. If a user is logged on to the system when changes to their profile are made, the changes do not take effect until next time the user logs into the system.