SECURITY

Table of Contents

Introduction

Quantify security is multilayered; and is comprised of Roles and Permission assignments and optional Location-Based Security. Permissions are assigned to roles, which in turn are assigned to end-user accounts.

End-user Account

Each Quantify end-user will have an Account created for them with an assigned Role. A Role dictates what the end-user can and cannot do when logged into Quantify.

Roles and Permissions

A role is a group of permissions. There are seven standard roles available in addition to the Administrator role. Three additional roles may be custom created if needed. Each role has a set of permissions that match tasks that an end-user assigned that role has the ability to do in Quantify. The group of permissions assigned to roles may be modified as needed.

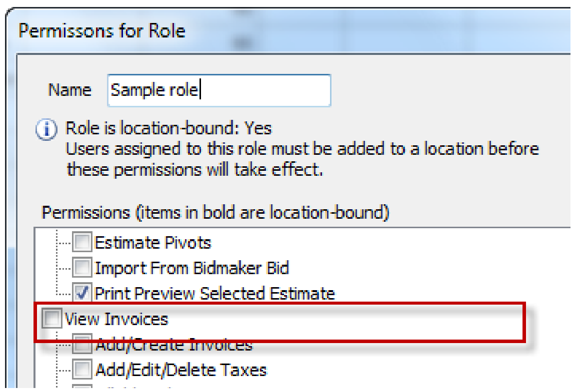
The Administrator role has all rights and permissions and may not be customized. All other roles may be customized as needed.

Permissions Types

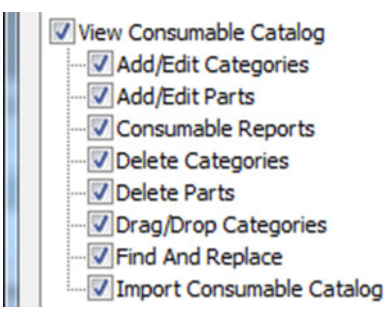
There are three types of permissions, Invisible, Visible with Full Permissions, and Visible with Partial Permissions.

Invisible

The ‘View’ level of a Permission section in the Permissions for Role dialog controls whether the item will be visible to the end-user.   If unchecked, then the Role will not see this item when logged into Quantify. In this example an End-user assigned this Sample Role would not see the Invoices tab when logged into Quantify.



Visible with Full Permissions



When the View checkbox is checked and all checkboxes within that section have been checked, then the role has full access to the feature.

In this example the End-user would be able to access and view the Consumable Catalog, and would have full access to the Consumable Catalog functionality.

Visible with Partial Permission

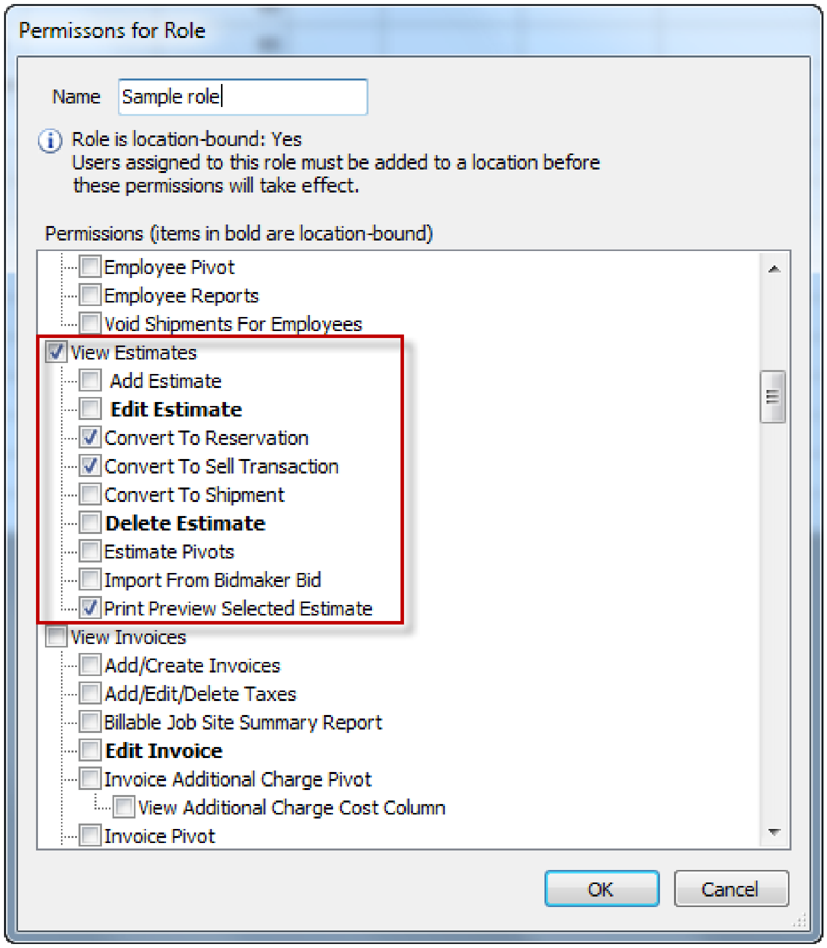
If the View item is checked, the tab or feature is viewable by the role. Partial permissions may be assigned using the additional checkboxes within that Permission section.

In this Role, the Estimates tab would be visible to the End-user.

This Role has partial permissions for the Estimate feature.

This role may convert an estimate to a reservation or convert the estimate to a Sell Transaction, but may not Edit Estimates.

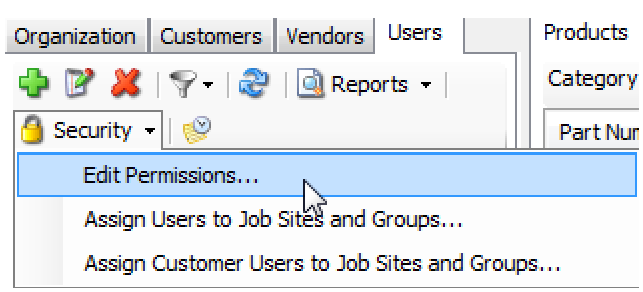
This role may also print preview an estimate. All other Estimate functionality is disabled for this role.

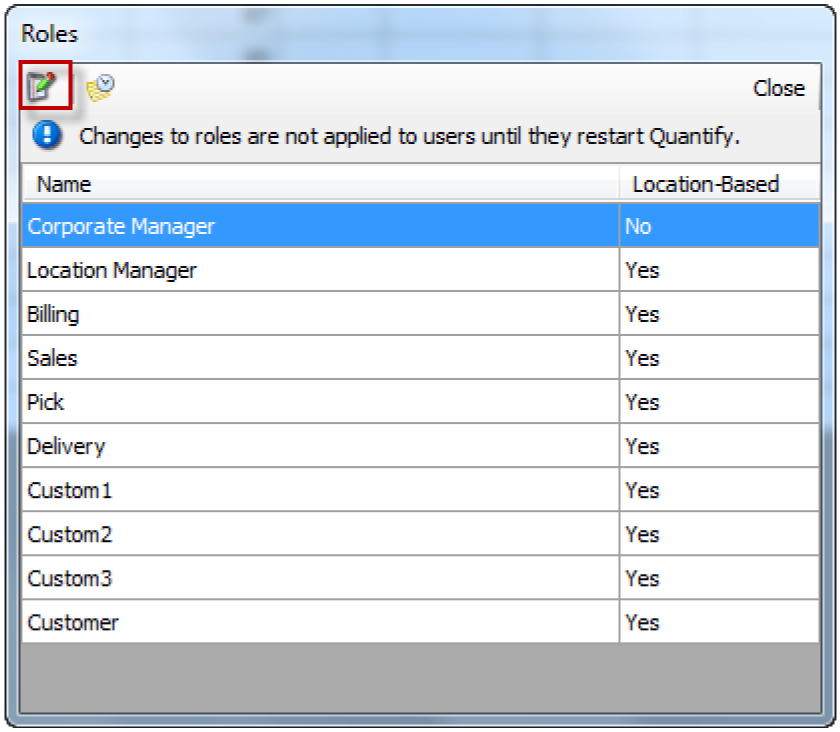


Standard Roles

Quantify is installed with seven Standard Roles, which are assigned default permissions. The permissions assigned to the standard roles may be edited as needed. As the Administrator role has all rights and permissions and may not be edited, it is not displayed in the Roles dialog. In addition, Quantify includes three custom roles that may be edited and customized to create nonstandard roles.

To access the Roles, select 'Edit Permissions…' from the Security drop down field on the Users tab. The 'Roles' dialog will launch.





Editing a Role

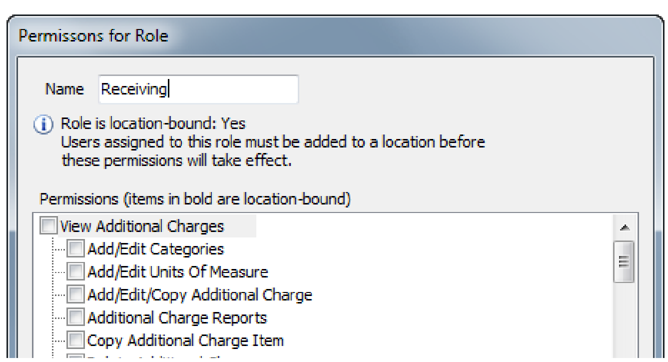
To edit a Role, double-click; or focus on the role and click the EDIT button. The 'Permissions for Role' dialog will launch.

Custom Roles

To create a custom role, edit one of the three provided Custom Roles from the 'Roles' dialog. In this example Custom1 will be edited to create a new customized role.

Focus on Custom1 and then edit the role. This will launch the 'Permissions for Role' dialog for the Custom1 Role.

Enter the name for the new role in the Name field. In this example, the role will be named Receiving.



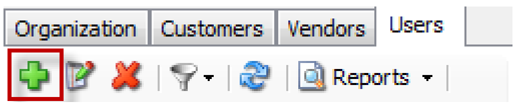
Check off the View checkboxes and additional permissions controls in the Permissions section as appropriate for this new role.

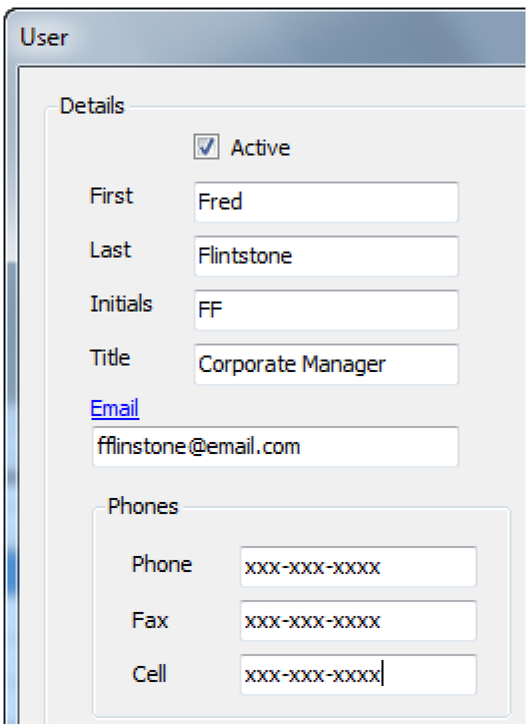
Click OK when ready. Note that the Receiving role is now visible in the ’Roles’ dialog.

Creating User Accounts, Roles, and Locations

End-user accounts are created and maintained on the Users tab.

To Add a User Account to the database, navigate to the Users tab and click the ADD button. This will launch the ‘User’ dialog.





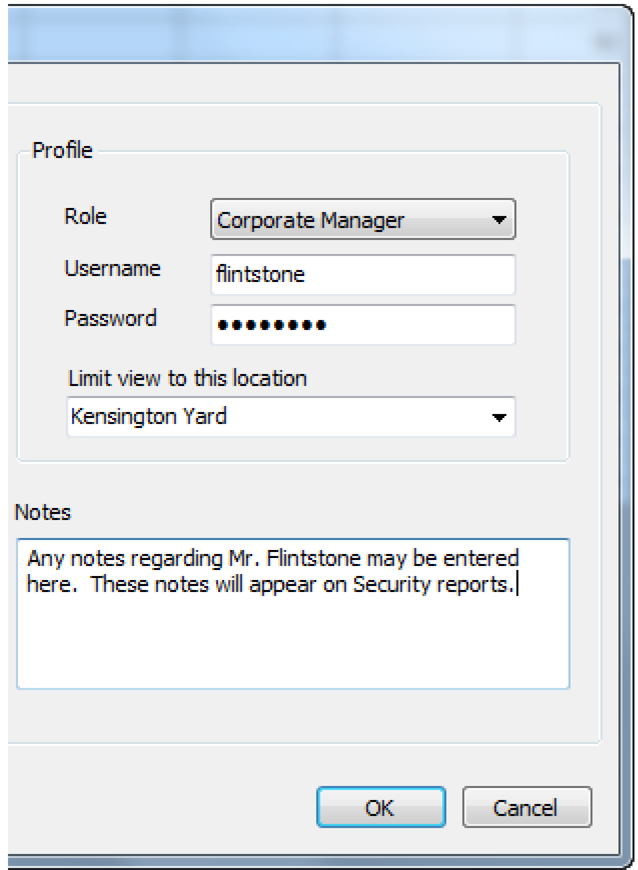
Complete the Details section on the ‘User’ dialog.

First: enter first name of Account Holder. This is a required field.

Last: enter last name of Account Holder. This is a required field.

All other fields as shown are optional.

Complete the Profile section on the ‘User’ dialog.



Role: assign a Role to this account. Select the Role drop down and choose from the appropriate role for this End-user. This is a required field.

In this example, the End-user has been assigned a Corporate Manager role.

Username: assign a Username to the account. The user name must be unique to the database. This is a required field.

Limit view to this location: if there is more than one Branch Office in the database, the account may be restricted to view one location. This is an optional field. If not selected then the Account will be able to view all locations.

Notes: enter any optional notes as needed.

Click OK when ready.

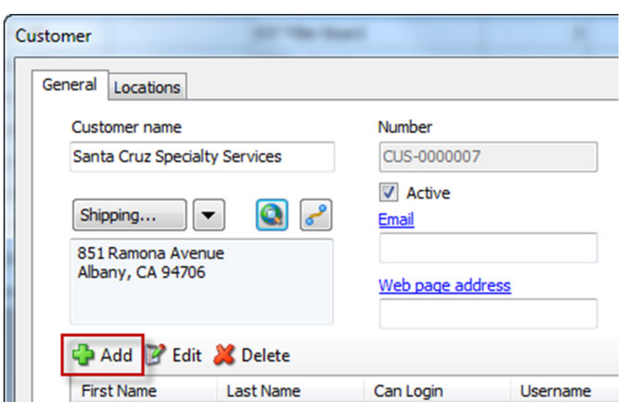
Customer Accounts

Customer Accounts can be created to allow customers to view their own information in Quantify. Customer account views are limited to their own job sites, shipments and invoices.

To login through a customer account, the customer must be on the same network as the Quantify database or have access through Quantify Web. See the *Quantify Web* guide for additional information.

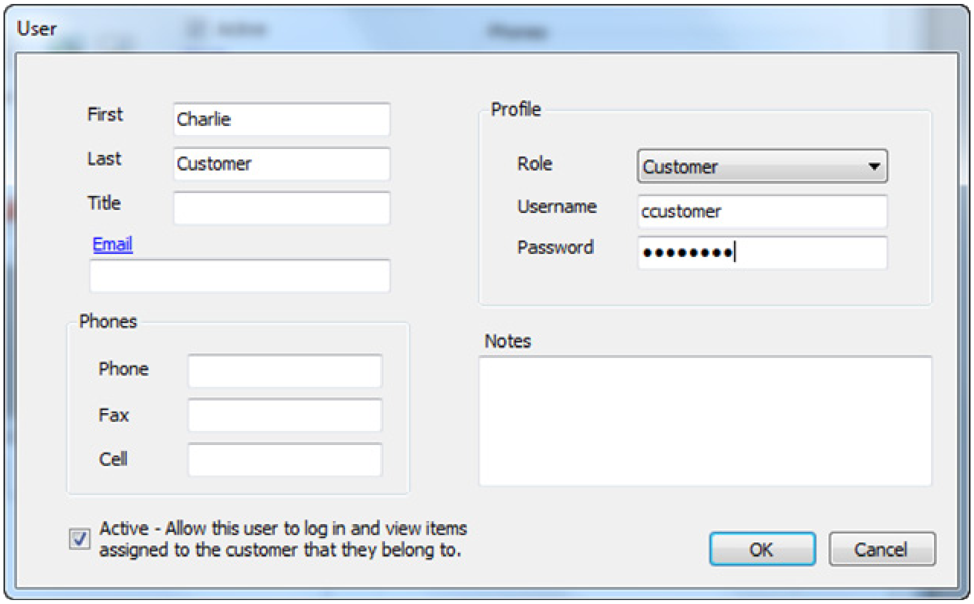
Set up a Customer Account

Customer accounts are created for Customer Contacts through the company record on the Customers tab. In the example below a Customer Contact is added to an existing company record.



The customer contact will be added through the ADD button.

This launches the ‘User’ dialog where the customer contact will be entered.

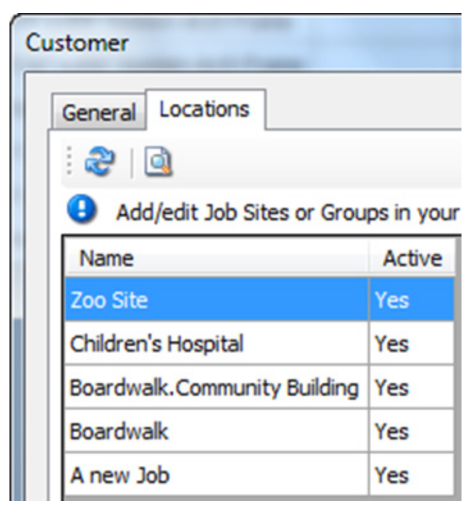


Required fields for Customer Contact include, First, Last, Username, and Password. Other fields are optional and can be used as needed.

The Role field defaults to Customer and is the only Role available for customer contacts.

The 'Active – Allow this user to log in and view items assigned to the customer that they belong to' check box is checked by default. This check box must be checked in order for the customer to log in to Quantify.

Click OK when ready. The Customer Contact has been added to the Customer record and will be able to log in and view their own information in Quantify.



The Location tab on the Customer record displays the locations the customer contact will be able to view.

As job sites are added for this customer in the database the customer contact will automatically be added to those locations.

If Location-Based Security is turned on, see the *Multi-Assign Customer Accounts to Job Sites* section for adding Customer accounts to Job Site security.

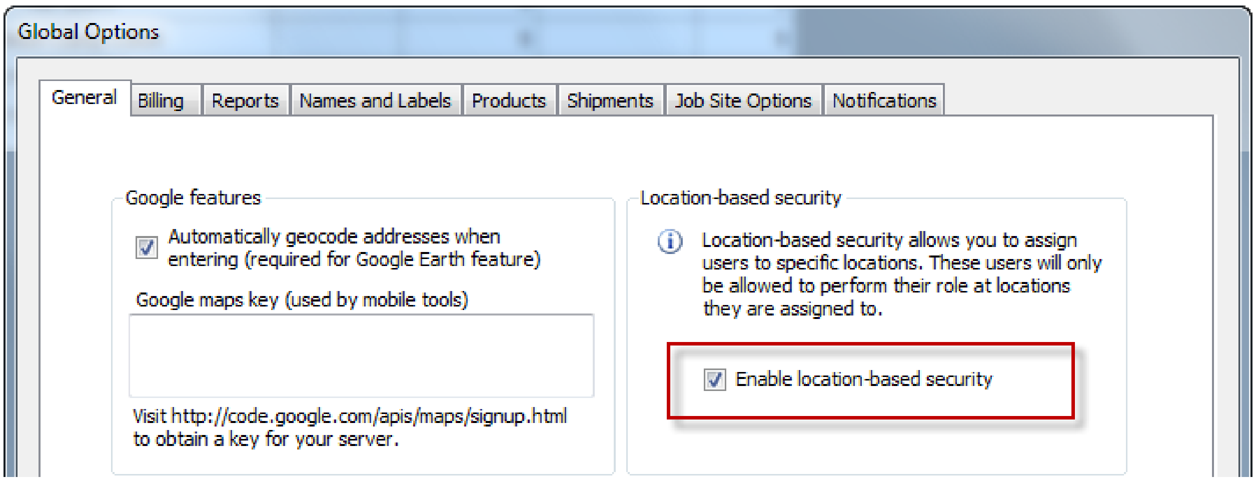
Location-Based Security

Location-based security allows individual users to be assigned to specific locations. Once assigned these users will only be allowed to perform their role at locations they are assigned to. For example, you may have billing personnel at two different branch offices who can create invoices for their own locations, but not each other's location.

Enabling Location-Based Security

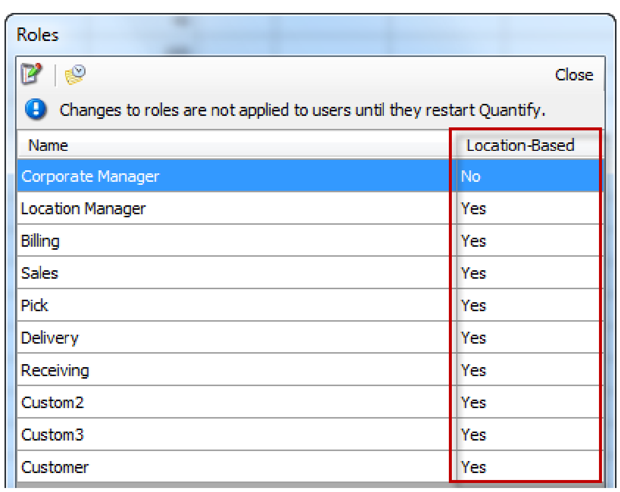
To set up Location-based Security the feature must first be enabled globally. Once Location-based Security has been turned on, then user accounts can be assigned to their appropriate locations.

To turn on Location-based Security, select Global Options from the **Tools** menu. On the General tab, check the 'Enable location-based security' check box.



Roles and Location-Based Security

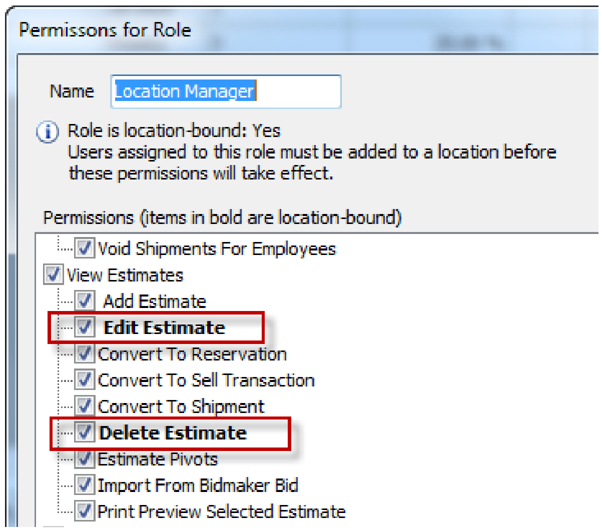
Not all roles are location-based. The Administrator role has all rights and permissions for all locations and is not Location-based. The role Corporate Manager is bound by permissions but not by location. All other standard roles are location-based. The Location-Based status of a role can be viewed on the 'Roles' dialog.



Permissions and Location-based Security

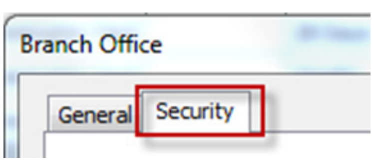
Not all permissions are affected by Location-Based Security. The permissions that are affected by Location-Based security are displayed in bold text in the 'Permissions for Role' dialog. The example below shows sample permissions for the role 'Location Manager'. In the Estimates section the 'Edit Estimate' and 'Delete Estimate' permissions are displayed in bold. These permissions are affected by Location-Based security when Location-Based security has been turned on.

With Location-Based security being used in the database an end-user with the Location Manager role would only be able to edit and delete estimates for locations (branch offices) that they were assigned to. The other estimate permissions in the Estimate section are not location-based and there would be no location-based restrictions for these permissions.



Branch Office Location-Based Security

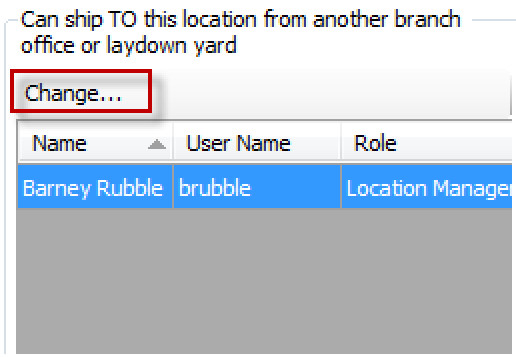
Branch Offices and Laydown Yards have four security areas. Each area is responsible for controlling a different security area for the location. End-users need to be assigned to each of the separate security areas in order to perform the tasks or features within that security area for the Branch Office or Laydown Yard.



To access Branch Office security, edit the Branch Office and navigate to the Security tab. Note the Security tab is only visible when Location-Based Security has been enabled in the database.

Branch Office Security Areas

The four security areas and their associated tasks and/or features are outlined below.

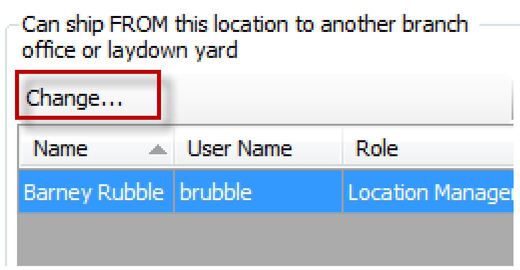


The 'Can ship TO this location from another branch office or laydown yard' security section displays the End-users that have the ability to ship deliveries to this branch from another branch.

To maintain this list click the CHANGE… button.

To assign an end-user account to this security area, check the check box for the end-user account.

Click OK when ready.

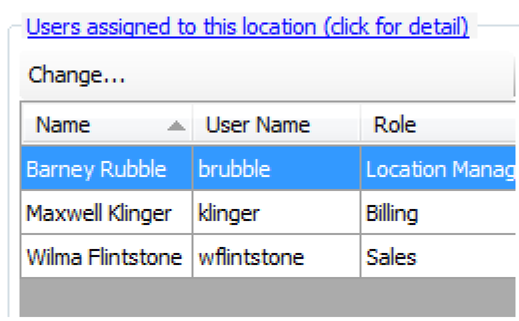


The 'Can ship FROM this location to another branch office or laydown yard' security section displays the end-users that have the ability to ship deliveries from this branch to another branch or laydown yard.

To maintain this list click the CHANGE… button.

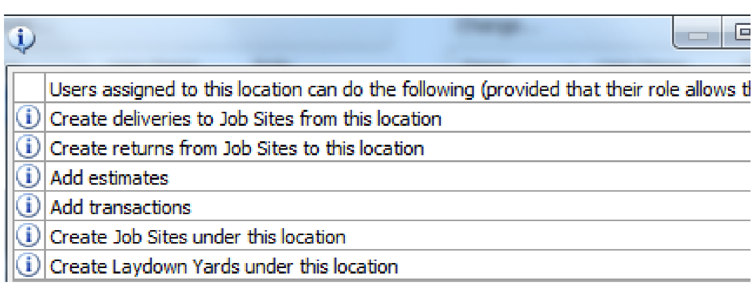
The 'Users assigned to this location (click for detail)' hyperlink lists various additional task areas controled by this security section.

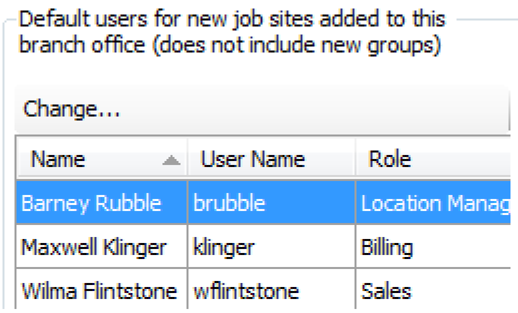
Click the hyperlink to view a list of these tasks.



Use the CHANGE… button to maintain the list of end-users assigned to this security section.

End-users assigned to this security section will be able to perform these tasks for this branch office or laydown yard, limited by the permissions assigned to their role.



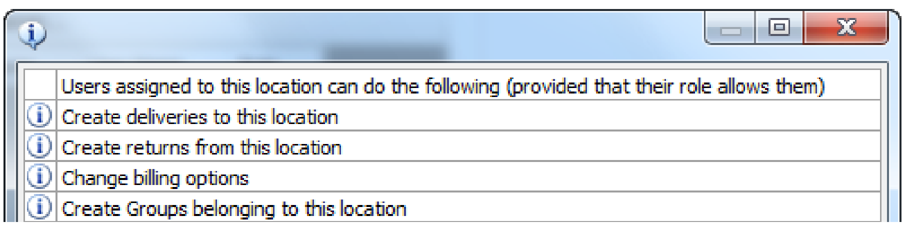


The 'Default users for new job sites added to this branch office (does not include new groups') security section allows end-users to be automatically added to job site security when new job sites are created.

Use the CHANGE… button to maintain the list of end-users assigned to this security section.

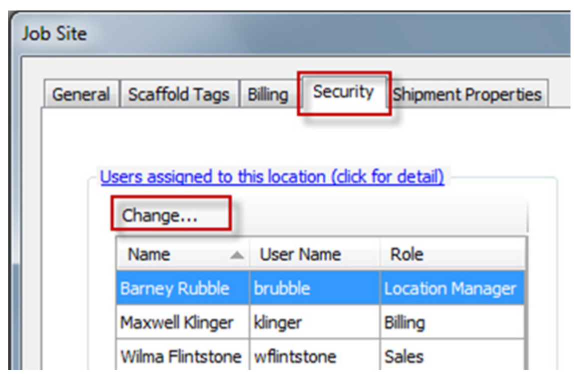
Job Site Location-Based Security

Certain tasks for job sites can be restricted to end-users assigned to the job site through Job Site Location-Based Security. The tasks as shown below can only be performed by end-users assigned to a job site through Job Site Based Security.



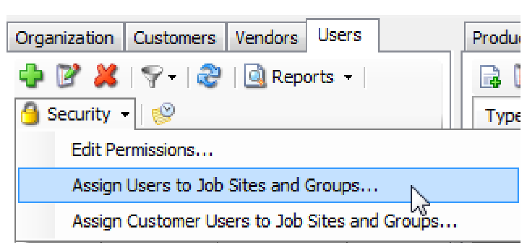
The Security tab on the Job Site will display the end-users that have been assigned to the job site and will have the ability to perform these tasks, limited by the permissions assigned to their role.

Use the CHANGE… button to maintain the end-users assigned to this job site.



Multi-Assign End-users to Job Sites

The Multi-Assign feature can be used to assign end-users to multiple job sites at once. Select 'Assign Users to Job Sites and Groups…' from the Security drop down on the Users tab.



The 'Multi-Assign User to Job Sites and Groups' dialog launches.

Select the End-user from the *User* field drop down.

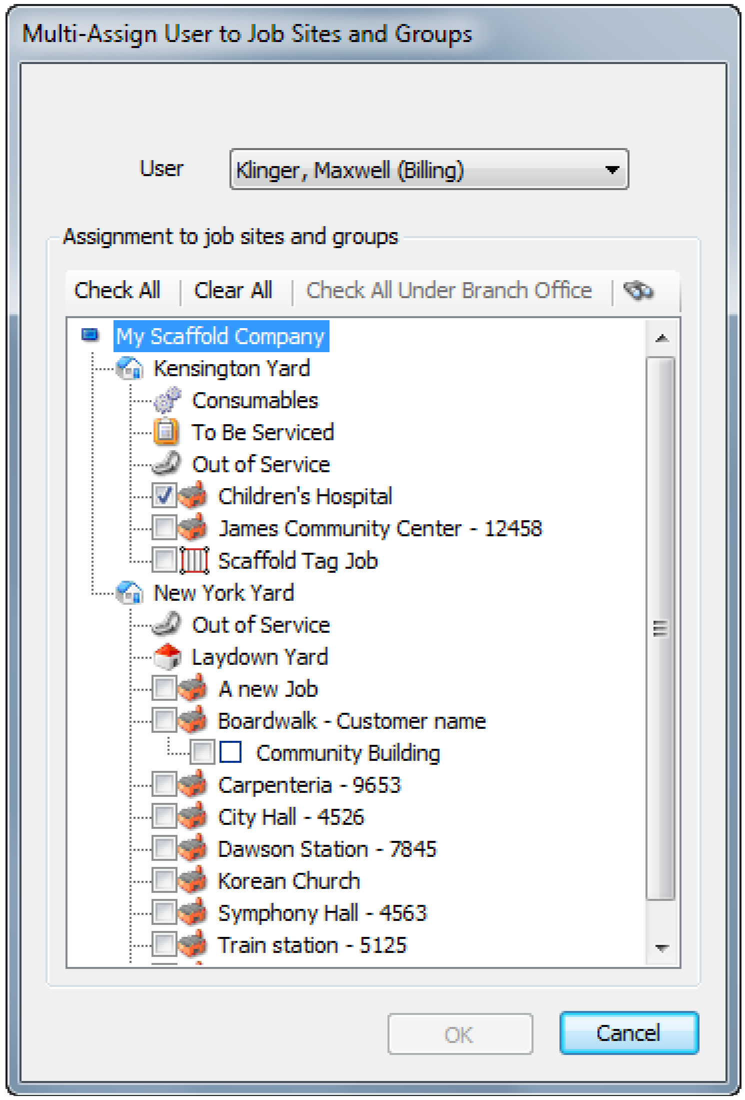
Job Sites this end-user is assigned to will be automatically checked in the Assignment to job sites and groups section.

Add or remove job site assignments as appropriate for this end-user by adding or removing check marks.

The Check All and Clear All buttons may be used to quickly select all or remove all check marks.

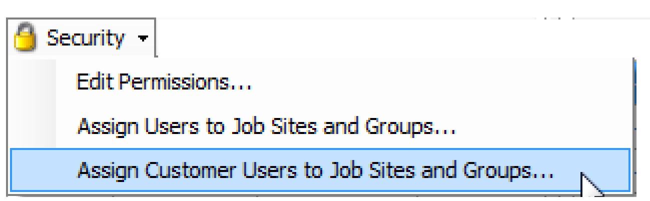
When focus is on a Branch Office level, the Check All Under Branch Office button will be available to select jobs sites for that Branch Office.

Click OK when ready.

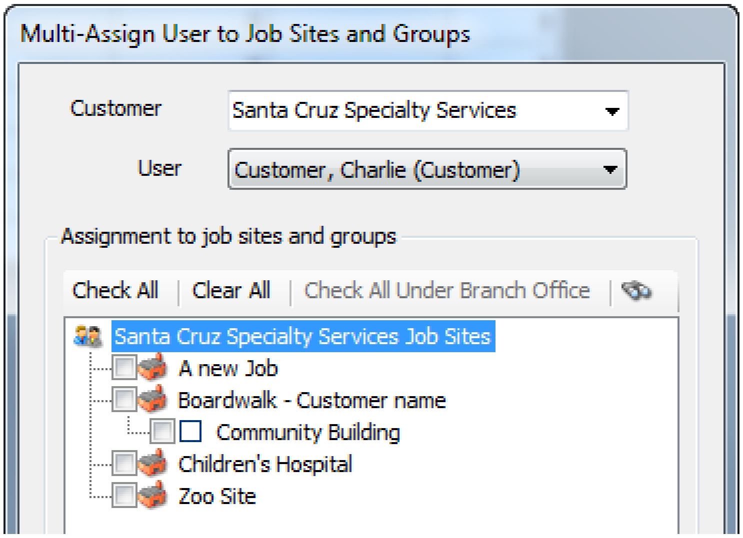


Multi-Assign Customer Accounts to Job Sites

The Multi-Assign feature can be used to assign Customer Accounts to multiple job sites at once. Select 'Assign Customer Users to Job Sites and Groups…' from the Security drop down on the Users tab.

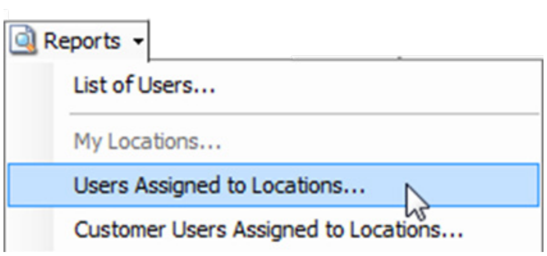


Select the Customer from the Customer drop down. This will populate the *User* drop down field with Customer Contacts set up for the Customer. Select the User from the User drop down. The Job Sites associated with the Customer will populate the Assignment to job sites and groups section. Check the checkboxes for the sites for the User. Click OK when ready.



Security Reports

Security Reports are available from the Reports drop down on the Users tab.



End-user and Security Reports available:

List of Users…
Users Assigned to Locations…
Customer Users Assigned to Locations…

My Locations… this report is available to non-administrative end-users to view the locations that they have been assigned to.