Security

Role Based

Security in each process is role based. Many specific areas of a process can be secured to allow only specific groups of people access.

Security in the Quik Flow Suite is defined at its highest level as a collection of groups. These groups can contain both users and other groups. Groups are used to specify access to specific features and tasks in the Quik Flow Server.

For ease in constructing a security scheme, groups are broken down into the following categories:

Roles

Roles define a class that may extend across various boundaries in an organization. Examples of a role might include a Customer Service Representative, a Corporate Officer, or a Network Administrator. There are several built-in roles that will be described later in this section.

Departments

These types of group generally follow an organization's hierarchy or physical divisions of employees. A user or employee typically belongs to only one department, and this will be designated as that employee's Primary Group. Users can belong to more than one department, but only one can be designated as primary.

Users

Each user of the Quik Flow Suite has a group that initially only includes

themselves. If that user (or a manager) later decides to delegate the tasks, other users can be added to the group. The effect will be that the new user will have the same access to tasks as the original user, or act as a proxy for that user.

User Defined

Any user can create a group, add and remove users and other groups, and use the group for security purposes. User defined groups are only maintainable by the user who created the group.

Built-in Roles

There are several built-in roles that play a special role in the Quik Flow Server security. They are described below:

Administrator

Persons in this group will have access to all tasks, groups, and security functions in the server. Members of this group should be limited and assigned a special account specifically for the purpose of administering the server.

Designer

Allows a user access to the Quik Flow Designer application. Users in this group will be allowed to edit and create processes to be stored on the server.

Department Administrator

Users assigned this role will be allowed to add, delete, and maintain users that share the same primary group. This allows distributed administration on a department basis.

Other Predefined Groups:

Everyone

This group contains all users. Users cannot be added or removed from this group.

Initiator

This special group will allow access only to the user who owns a secured object or resource. In most cases, this will be the user who has initiated a process manually from the Web Interface. The Initiator group is used as a default for most security settings.

My Subordinates

Allows an object's owner's subordinates access to a resource. Subordinates are defined as users whose "Reports To" has been set to the resource owner.

My Supervisor

Allows access to a resource owner's supervisor, as defined by their "Reports To" definition.

Password Access

Each user of the Quik Flow Suite is given their own user name and password. A user's supervisor and the system administrator have access to override a user's task assignment in the event they are absent from work on a particular day.

Encrypted Communications

All communication between the web browser and the Web Interface can be encrypted using the same system that is used when making credit card purchases over the Internet. This allows employees to log into the Web Interface from remote offices or their home without worrying about compromising company information.

Online URL: https://support.quikbox.com/article.php?id=185