Security Features - Guide For Administrators

Introduction

This help file describes the security features available on the Sprint web stock booking system.

1. Types of User

You can create three types of user account. In order of decreasing privilege these are: SuperUser, Product Owner and User.

Super Users have access to all tabs, including the Reports, the User Manager and the Product Manager tabs, where they can access information about all products and all users.

Product Owners have access to the Reports, the User Manager and the Product Manager tabs, where they can access information about the products and users assigned to them.

Users can order products and access the Address Book. Users can be permissioned to access only certain products, and to order only up to a certain amount of a product ("Max Grab").

2. Roles

In addition to specifying the type of a user account, you can assign one or more specific ***roles*** to a user account .

These roles are: Administrator, Deputy Administrator, Notice Board Editor, Deputy Notice Board Editor.

Your Account Handler assigns the Administrator role on request. Once assigned, the Administrator assigns the remaining roles.

The Administrator and Deputy Administrator can assign roles and view site configuration settings, using the Administrator tab that is available only to them.

The Notice Board Editor and Deputy Notice Board Editor can modify the notice board page using facilities available on the notice board editor tab that is available only to them.

Only Super Users can take on the Administrator and Deputy Administrator role. Any user can take on the Notice Board Editor or Deputy Notice Board Editor role. A user can take on more than one role.

3. Account and Password Management

To request forgotten login credentials, click on the ***forgot your password?*** link on the login page, then enter your email address. The system chooses at random one of three security questions and requests a response. On receiving a correct response, the system emails the login credentials to that email address. You may have two or more accounts with

the same email address. If so, the system prompts you for the account from which to retrieve the security question and response. The email you receive includes the credentials of each account where the specified email address is used.

To use this facility successfully you must first provide answers to the three security questions found on the **My Profile** tab.

Immediately after a successful login, the date and time of the previous successful login is displayed next to the account name, to alert you if the account has been used by anyone other than yourself.

You can change your password at any time by clicking the ***change login password*** link on the My Profile tab. You are then prompted to change your password the next time you log into the system. Super Users can force a user to change password at the next login, using the ***force password change*** check box on the User Manager tab.

Passwords can be up to 12 characters long. A password that has been used previously cannot be re-used.

You can specify a password policy for users. Policy values include: minimum password length, password complexity (minimum number of lower case characters, minimum number of upper case characters, minimum number of digits), password lifetime (elapsed days since the last password change), maximum login attempts before an account is suspended, account inactivity period (in days). Contact your Account Handler to request a change to the password policy.

Once the password lifetime has expired, you will be prompted to enter a new password next time you log in. You must enter the old password, the new password, and then repeat the new password. The new password must conform to the password policy in force.

When you login, you can click the ***remember me on this computer*** check box. Next time you visit the Sprint web site you will be taken directly to the Notice Board, bypassing the login page. This continues until you click the **log out** button. WARNING: Don't do this on a public computer!

If a user fails to enter the correct password more than ***maximum login attempts*** times the account is suspended. It must be re-activated by a Super User from the User Manager tab.

If an account is inactive for more than the ***account inactivity period*** (part of the password policy) the account is suspended. It must be re-activated before it can be used again.

[end]