

Remote User Account Management

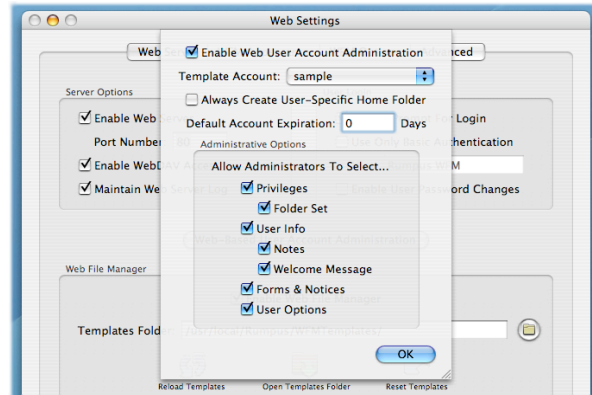
Managing user accounts from anywhere, using a Web browser interface.

In most cases, as the Rumpus server administrator, you will probably not need to adjust most basic configuration options on a regular basis. The exception to this is configuring User Accounts, which may need to be added, updated, or deleted frequently. In addition, you may find that you need to allow other trusted people to create and manage user accounts, as well as yourself.

For this reason, Rumpus supports Web-based user account management. This allows you to configure users and their access privileges from anywhere on the Internet using a standard Web browser. You can also allow users to change their own passwords using a Web browser, improving security by encouraging frequent password rotation.

Configuring Remote Administration

Remote Web administration requires that the Rumpus Web service and Web File Manager be enabled. To configure Web-based administration, click the “Web-Based User Account Administration” button on the “Web Server” tab of the Web Settings window. The “Remote Administration” sheet will drop down, as shown here:



Start by checking the “Enable Web User Account Administration” option, to turn on remote administration. Next, select a user account which will serve as a template when new user accounts are created via Web administration. When a new account is created, all of the settings specified for the template account will be used as default values for the new account, except the account name and password, of course.

The “Always Create User-Specific Home Folder” option allows you to choose between two different ways of defining new user home folders. When this option is disabled, Web administrators will be able to set the home folder for user accounts as they like. User account home folders will always be restricted to the administrator’s own home folder, but when “Always Create User-Specific Home Folder” is off, specifying the user home folder will be up to the administrator.

When this option is turned on, however, Web administrators will not be allowed to set user home folders, and in fact won't even see the user account home folder in the Web interface. Instead, a folder will be created inside the administrator's home folder with the name of each newly created user account, and this folder will be set as the new user home. For example, if the administrator "Bob", whose home folder is "/Users/Shared/Bob/" creates a new user account called "Mary", a new folder will be created at "/Users/Shared/Bob/Mary/", and that folder will be set as Mary's home. This not only simplifies and restricts folder setup for administrators, but it also allows them to view and manage the content of their own users when logged in through the normal FTP or Web interfaces.

The "Default Account Expiration" option allows you to have new user accounts automatically expire after a specified number of days. This option is ignored if the selected Template Account is configured as a "Permanent" user account. If the account type is set as "Disable" or "Delete" however, the date set for the expiration will be the date on which the account is created, plus the specified number of days. When Web administrators can adjust user account "User Options", the expiration date will be set as a default. If the "User Options" settings are disabled in the "Administrative Options" box, then the expiration date will be enforced and outside of the administrator's control.

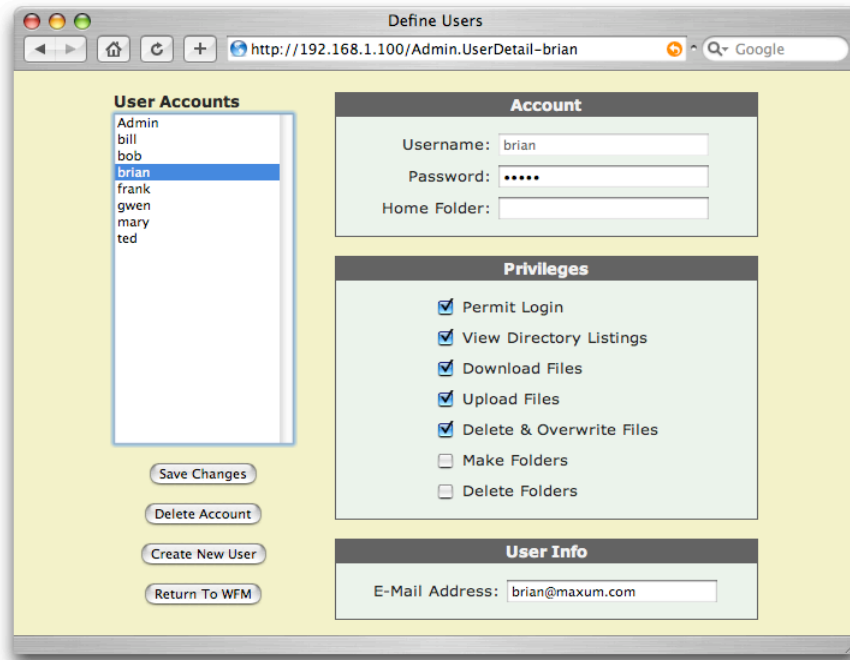
Choosing What Administrators Choose

To simplify the interface for your administrators, and to prevent them from inadvertently changing user account options that aren't relevant for your server, Rumpus allows you to choose what user account settings are configurable via the Web. In the "Administrative Options" box, simply enable or disable each set of user account settings your administrators should be able to see and manage. User account settings that are hidden from the administration interface will always remain at their default value, as defined for the template user account.

For example, to allow administrators to create user accounts, but only adjust the user account privileges and e-mail address, check the "Privileges" and "User Info" checkboxes, leaving all others off. In this case, only the necessary user account options will be suppressed in the Web administration interface, and will be left at the default values assigned to the template user account.

Using Rumpus Remote Administration

With Web user administration enabled, users with "Administrator Access" privileges can manage users simply by logging in the the Web File Manager. In the task bar on the main WFM page, administrators will see a "Manage Users" icon that can be used to access the user administration page, shown below.



In this example, only the “Privileges” and “User Info” user account options have been enabled on the “Remote Administration” sheet, so only those options are presented. The list of user accounts, and the account settings, operate in essentially the same way as they do on the “Define Users” window in Rumpus.

To create a new user account, click the "Create New User" link. Accounts can be deleted by selecting the account and clicking “Delete Account”. To modify an existing account, simply select the user account from the list, causing the options for that account to be shown, and make the needed changes. Note that after making settings changes, the “Save Changes” button must be used to save them to the server.

Important! Be sure to click “Save Changes” after making any user account settings changes. If the “Save Changes” button isn’t clicked, changes will be lost as soon as another user account is selected.

Administration Groups

When a Web administrator (a Rumpus user with “Administrator Access” enabled) has a home folder assigned as “ROOT”, meaning that they have full access to the Rumpus FTP root folder, then that administrator will be allowed to view and manage all user accounts, and create new ones without restriction. However, when the administrator’s home folder is set to allow them access only to a specific folder, then user accounts managed by that administrator will also be restricted to that folder. In this case, the user account with administration privileges can be considered a sub-administrator, since new user accounts they create will be restricted to home folders that reside within the administrator’s home folder, and they will only be able to view and manage user accounts that fall within their own home folder group.

When creating a new user account, a sub-administrator will specify a partial path for the new user home folder, simplifying account setup. For example, if a sub-administrator were to create a new user account with a home folder of “mary”, then a folder called “mary” would be created within the sub-administrator’s own home folder, and the new user account home folder would be set to that folder’s path.

Allowing Users To Change Their Own Passwords

To enable users to update their own passwords, the Web File Manager needs to be enabled, as described in the “Web File Manager” article in the Rumpus package. Also, check the "Enable User Password Changes" option on the "Web Server" tab of the Web Settings window within Rumpus.

With this option enabled, WFM users will see a “Change Your Password” link at the bottom of the “Account Info” area on the primary WFM page. Clicking this link takes the user to a simple form allowing them to select and confirm a new password for accessing the Rumpus server.

The password change form can be customized as needed. For details see the “Customizing The WFM Interface” section of the “Web File Manager” article in the Rumpus package.