Adding Users to a UMContent Site

The User Admin applet of Content Server enables subadministrators to add and delete users of their UMContent sites as well as assign and modify appropriate roles and accounts for those users.

Adding users

Add users to your site through the following steps:

1. From the web-based Content Server, select the Admin Applets link in the Administration section of the left panel.
2. Click on the icon for User Admin in the main content area of the Content Server screen.
3. Click the Add button on the lower left of the pop-up User Admin panel. Alternatively, click Add Similar to create a user having a similar profile of roles and accounts to an existing system user. Profiles of existing users may be modified from the Edit button on this panel.
4. Click OK for the default authorization type of Local on the subsequent pop-up panel.
5. In the Info tab of the Add User window, fill in the user’s Internet ID as Name, complete the Full Name, Password, and E-Mail Address fields, and select the appropriate unit for the User Type field from the dropdown list.

Currently, passwords are assigned to users by subadministrators. Central authentication for UMContent is currently in development.

*Note:* the SubAdmin field should be left at its default value of No. Subadministrators may only be created by system administrators upon receipt of the appropriate release forms from new unit subadmins.
Assigning user permissions using roles and accounts

The permissions assigned to users in UMContent are a combination of the rights assigned to those users through roles and accounts. In general, roles are useful in designating the highest level of access that a user will have anywhere within the UMContent system. In addition to assigning a role, specific access rights must be assigned within accounts to determine the actual permissions that users will be provided within individual content areas. See the “Notes” section at the end for further information about how to apply the security model to establish appropriate access rights for users.

The specific permissions granted through assignment of rights (RWDA) are as follows:

- **Read** - allowed to view files in assigned accounts.
- **Write** - allowed to view, check in, check out, and get a copy of documents in assigned accounts. The author can change the account setting of a document if the non-author has Write permission in the new account.
- **Delete** - allowed to view, check in, check out, get a copy, and delete files in assigned accounts. The configuration setting AuthorDelete=true adds delete permission to all accounts to which the author has Write permission.
- **Admin** - allowed to view, check in, check out, get a copy, and delete files in the assigned account. If this user has Workflow rights, they can start or edit a workflow in that account. Users are also allowed to check in documents in that account with another user specified as the Author. Non-authors can change the account setting of a document if the non-author has write permission in the new account.

To add a role for a user:

1. Switch to the **Roles** tab in the **Add User** panel.
2. Click on the **Add Role** panel.
3. Select the appropriate role to assign to the user by clicking on its name in the list and clicking the **OK** button.

*Note: the four roles of guest (R), contributor (RW), editor (RWD), and manager (RWDA) should serve all needs in assigning roles. Only one role needs to be assigned to a user, and it should contain the highest level of access that user will need anywhere within the UMContent system. User access ultimately will be limited by the user’s account permissions, which will be created using the following procedure.*
Accounts are added in a similar manner. A user may have multiple accounts with varying access rights within each. Please note that access rights are primarily determined by the assignment of accounts, but that the user’s role must allow for the highest level of rights granted to the user within any account. Also, be aware that account rights are established hierarchically. See the “Notes” section for additional details.

To add accounts for a user:

1. Switch to the Accounts tab in the Add User panel.
2. Click on Add to add a new account.
3. Select an appropriate account from the dropdown menu.
4. Select the appropriate access rights using the check boxes provided.
5. Click OK to save.
6. Select a default account for the user from the dropdown menu at the bottom of the window.
7. Click OK to complete or add additional accounts to user profile if needed.

Note: when creating account rights, UMContent initially grants RWDA rights to documents without accounts by default. Since UMContent requires all newly checked-in content to be assigned to an account, no content should remain in this category within the system. However, some system functions including workflows, creation of new sections using Site Studio Manager, and other functions using Site Studio Designer require documents without accounts rights. A recommended approach would be to match the rights to documents without accounts to those assigned by the user’s role.
Notes

- Account permissions are granted hierarchically, which means that it is not possible to grant permissions to higher level accounts without providing equal access to associated subaccounts. For example, it’s not possible to grant read-write (RW) access to PUB/OIT without providing equally high level access to its subaccount PUB/OIT/Training. The converse is possible, however, namely to provide read-write access to PUB/OIT/Training while providing only read access or no access to PUB/OIT.

- Users may be assigned different access rights to different accounts provided those rights conform to the hierarchical model described in the preceding item.

- System rights are the intersection, not the union, of those created using roles and accounts. Consequently, providing a system-wide manager role to a user enables that user to perform that role only for areas to which equivalent permissions have been granted through accounts.

- Since only system-wide roles are being established in the UMContent system, the primary value of roles within UMContent will be to establish the maximum level of access a user will have anywhere in the system. Specific rights within the system should be configured by setting the appropriate level of access in accounts while keeping in mind that a user’s role must provide at least as much access as the strongest level of access established in any account. For example, even if a user has RWD access to the account PUB/OIT, they will be unable to delete files in that account if their only role is as a contributor having RW access.

- Users must have appropriate roles to perform certain basic system functions. For example, even if a user has the appropriate account access to create files (RW), they will be unable to check-in content (and will not see a “New Check-In” option in Content Server) unless they have been assigned a role that provides write access.

- Within all subsystems, RWDA rights are assigned in a step-wise manner. Providing delete (D) rights without providing read and write (RW) rights as well is not possible without extensive workaround customization.