Talking Tech with Vound

Managing Your Team and Case Access with Intella Connect

Document Review with Intella Connect

Unlike Intella Desktop, Connect has been designed to accommodate document review workflows for either individual users or a team of users. This includes batching of document sets, and the functionality for the user to code the documents within those batches.

Connect uses a mixture of user accounts, roles, and permissions. This allows the administrator to set up review tasks, control which users have access to specific documents, and determine which functions they can perform in a case.

User Accounts in Intella Connect

Intella Connect has the ability to use two types of user accounts. These include user accounts derived from LDAP, and user accounts created manually in Connect.

- User accounts derived from LDAP: Connect can be configured to use LDAP directories. This can be useful for large businesses that have a number of Connect users. Connect has a wizard to set up LDAP, however, the details regarding this is outside of the scope of this webinar.

- Manually created accounts: These are accounts which the administrator creates directly in Connect. Creating an account is a simple task for the administrator. The interface only asks for a username and password. Note that permissions are not set here when creating an account.

Roles and Permissions in Intella Connect

The power over who can see specific documents comes from the Roles and Permissions which are set up in Intella Connect. Roles are created for the type of work a user will undertake in a case. For example, roles can be setup for case managers, first or second pass reviewers, restricted reviewers, or for any other type. Permissions are then given to each role to allow specific access to the case and other functionality.

Examples:

- For a restricted reviewer, you may only want them to batch documents that have been assigned to them in batches. In this case, the restricted reviewer role will have very limited permissions. These permissions may only include: The Review UI, Can access a case, and Can see batches.

- For a case manager, this role would include most of the permissions since they would need access to most of the functionality.

- If you do not want a group of users to see items tagged with a specific tag (e.g. privileged items), you can make a Restricted tag role. This role would have the 'Cannot see items tagged with ...' permission.

Putting It All Together

Once you have the users created, the roles created, and the correct permissions assigned to the roles, you are ready to set up your cases. When you click on a case, go into the Authorizations screen. You will see the 'Manage user roles for the case' window. In this window, you will see a list for all of the roles which have been set up. These roles are groups that have permissions set to them. You simply add the users to the role which you want them to undertake. In this example, Jon is added to the Case Admin role which has most of the permissions. Bob is added to the Restricted Reviewer role, which is highly restrictive.

Click to see the full webinar video on YouTube.

Vound
AMERICA • ASIA • EUROPE