Summation User Guide

AccessData

AccessData Legal and Contact Information

Document date: May 7, 2012

Legal Information

©2012 AccessData Group, LLC All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

AccessData Group, LLC makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, AccessData Group, LLC reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, AccessData Group, LLC makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, AccessData Group, LLC reserves the right to make changes to any and all parts of AccessData software, at any time, without any obligation to notify any person or entity of such changes.

You may not export or re-export this product in violation of any applicable laws or regulations including, without limitation, U.S. export regulations or the laws of the country in which you reside.

AccessData Group, LLC.
384 South 400 West
Suite 200
Lindon, Utah 84042
U.S.A.

www.accessdata.com

AccessData Trademarks and Copyright Information

- AccessData® is a registered trademark of AccessData Group, LLC.
- AD Summation is a registered trademark of AccessData Group, LLC

A trademark symbol (®, ™, etc.) denotes an AccessData Group, LLC. trademark. With few exceptions, and unless otherwise notated, all third-party product names are spelled and capitalized the same way the owner spells and capitalizes its product name. Third-party trademarks and copyrights are the property of the trademark and copyright holders. AccessData claims no responsibility for the function or performance of third-party products.

Documentation Conventions

In AccessData documentation, a number of text variations are used to indicate meanings or actions. For example, a greater-than symbol (>) is used to separate actions within a step. Where an entry must be typed in using the keyboard, the variable data is set apart using [*variable_data*] format. Steps that require the user to click on a button or icon are indicated by **Bolded text**. This *Italic* font indicates a label or non-interactive item in the user interface.

A trademark symbol (®, ™, etc.) denotes an AccessData Group, LLC. trademark. Unless otherwise notated, all third-party product names are spelled and capitalized the same way the owner spells and capitalizes its product name. Third-party trademarks and copyrights are the property of the trademark and copyright holders. AccessData claims no responsibility for the function or performance of third-party products.

Registration

The AccessData product registration is done at AccessData after a purchase is made, and before the product is shipped. The licenses are bound to either a USB security device, or a Virtual CmStick, according to your purchase.

Subscriptions

AccessData provides a one-year licensing subscription with all new product purchases. The subscription allows you to access technical support, and to download and install the latest releases for your licensed products during the active license period.

Following the initial licensing period, a subscription renewal is required annually for continued support and for updating your products. You can renew your subscriptions through your AccessData Sales Representative.

Use License Manager to view your current registration information, to check for product updates and to download the latest product versions, where they are available for download. You can also visit our web site, www.accessdata.com anytime to find the latest releases of our products.

For more information, see Managing Licenses in your product manual or on the AccessData website.

AccessData Contact Information

Your AccessData Sales Representative is your main contact with AccessData Group, LLC. Also, listed below are the general AccessData telephone number and mailing address, and telephone numbers for contacting individual departments.

Mailing Address and General Phone Numbers

You can contact AccessData in the following ways:

AD Mailing Address, Hours, and Department Phone Numbers

Corporate Headquarters:	AccessData Group, LLC. 384 South 400 West Suite 200 Lindon, UT 84042 USA *Voice*: 801.377.5410 *Fax*: 801.377.5426
General Corporate Hours:	Monday through Friday, 8:00 AM – 5:00 PM (MST) AccessData is closed on US Federal Holidays

AD Mailing Address, Hours, and Department Phone Numbers (Continued)

State and Local Law Enforcement Sales:	*Voice*: 800.574.5199, option 1 *Fax*: 801.765.4370 *Email*: Sales@AccessData.com
Federal Sales:	*Voice*: 800.574.5199, option 2 *Fax*: 801.765.4370 *Email*: Sales@AccessData.com
Corporate Sales:	*Voice*: 801.377.5410, option 3 *Fax*: 801.765.4370 *Email*: Sales@AccessData.com
Training:	*Voice*: 801.377.5410, option 6 *Fax*: 801.765.4370 *Email*: Training@AccessData.com
Accounting:	*Voice*: 801.377.5410, option 4

Technical Support

Free technical support is available on all currently licensed AccessData products.

You can contact AccessData Customer and Technical Support in the following ways:

AD Customer & Technical Support Contact Information

AD SUMMATION	Americas/Asia-Pacific: 800.786.2778 (North America). 415.659.0105. Email: support@summation.com
Web Site:	http://www.AccessData.com/Support
	The Support website allows access to Discussion Forums, Downloads, Previous Releases, our Knowledgebase, a way to submit and track your "trouble tickets", and in-depth contact information.
Standard Support:	Monday through Friday, 6:00 AM– 6:00 PM (PST), except corporate holidays.
After Hours Support:	Monday through Friday by calling 415.659.0105.
After Hours Email-only Support:	Between 12am and 4am (PST) Product Support is available only by email at afterhours@accessdata.com.

Contents

Introducing the Summation Implementation Guide

This *Summation Implementation Guide* includes all of the user documentation for AccessData Summation and includes the following parts:

The informaion in each of these parts are also available as individual Guides which can be used by different users depending on their role. The individual guides can be downloaded from http://summation.accessdata.com.

Administrating Summation

The part describes how to administer Summantion and includes the following sections:

1 Introduction

This document is designed to help administrators set up Summation users, groups, roles, and system settings.

1.1 Introducing Summation

1.1.1 About the Summation Console

The Summation interface is a web-based console that only retains full functionality in Internet Explorer. Summation may be opened in other browsers, but will not be fully functional. You can open the Summation application from any computer with network connectivity.

Internet Explorer 7 or higher is required to maintain full functionality of the Summation console. Internet Explorer 8 is recommended.

What you can access and do within the console depends on the rights and permissions that an administrator has granted you. Users may have limited privileges based on the work that they will do.

See About Users on page 20.

All users are required to enter proper authentication credentials (username, password) in order to open the console.

1.1.2 About User Accounts

Each user that uses the Summation Console must log in with an account. Administrators configure the user accounts.

Depending on how Summation is configured, your account may be either a local Summation account or an Integrated Windows Authentication account.

The type of account that you have will affect a few elements in the Summation interface, for example, whether or not you can change your password within the console.

1.2 Opening the Summation Console

You can use the Summation console to manage cases from case creation to production set export.

See About the Summation Console on page 8.

You can start the console from any computer that has network connectivity to the Summation server.

To start the console, you need to know the IP address or the host name of the computer on which the Summation server is installed.

When you first access the console, you are prompted to log in. Your Summation administrator will provide you with your username and password.

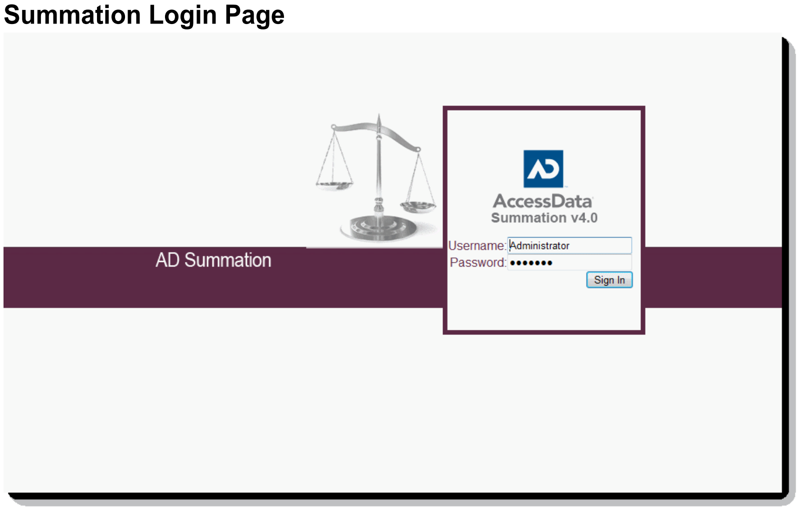
To open the Summation console

1. Open Internet Explorer.

> **Note:** Internet Explorer 7 or higher is required to use the Summation console for full functionality. Internet Explorer 8 is recommended.

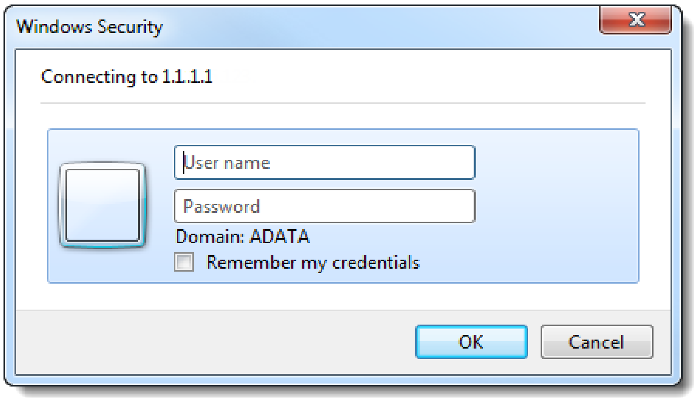
2. Type the following URL in the browser's address field:
   https://<host_name>/ADG.map.Web/
   where `<host_name>` is the host name or the IP address of the Summation server.
   This opens the login page.
   You can save this web page as a favorite.
3. On the login page, enter the username and password for your account.
   About User Accounts (page 8)
   If you are logging in as the administrator for the very first time, do one of the following:
   3a. If you have not enabled Integrated Window Authentication, enter the pre-set default user name and password. Contact your Technical Account Representative for login information.
   3b. Click **Login**.
   You will see one of two login pages:
   - If you are *not* using Integrated Windows Authentication, you will see the following login page.

Summation Login Page



Note: If you are using Integrated Windows Authentication and are not on the domain, you will see a Windows login prompt.

Integrated Window Authentication Page



4. Click **Login**.

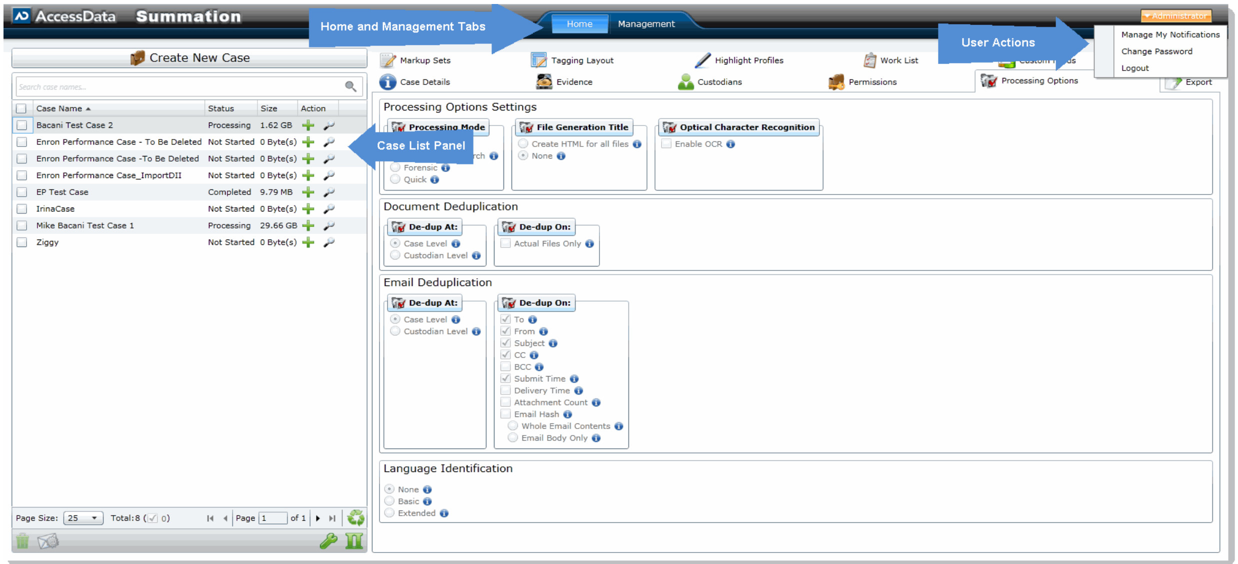
   If you are authenticated, you will have access to the Summation console.

   See About Users on page 20.

   If you cannot log in, contact your Summation administrator.

1.3 Introducing the Summation Console

Summation Main Window



The main interfaces of Summation are listed in the following table.

Elements of the Summation Main Window

Component	Description
Home page	The *Home* page lets you create, view, manage, and review cases based on the permissions that you have. This is the default page when you open the console. See the Case Manager Guide for more information on the Home page.
User Actions	Actions specific to the logged-in user that affects the user's account. See User Actions on page 18.
Management page	The *Management* page lets administrators perform global management tasks. See Management Page on page 13.
Case Review page	The *Case Review* page lets you analyze, filter, code and label documents for a selected case. You access Case Review from the *Home* page. See the Reviewer Guide for more information on the Case Review page.

The work that you do in the console will depend on the permissions that you have been given. You may have permissions to view only parts of the Summation console. For example, a user with permissions to only perform case reviews will not see the *Management* page.

In the top right corner, you will see the user login name. Click the drop-down arrow to perform user-specific actions.

1.4 Workflows for Administrators

Administrators and managers configure and manage the global Summation environment.

Before creating and reviewing cases, you should review and perform the following tasks for configuring Summation.

Workflow for Configuring Summation

Step	Task	Link to the Tasks
1	Decide which authentication mode to use	See Opening the Summation Console on page 9.
2	Manage users, groups, and roles	See Managing Users on page 27. See Configuring and Managing Groups on page 34. See About Planning User Roles on page 22.
3	Configure default case settings	See Configuring Default Case Settings on page 43.

At regular intervals, administrators should perform the following tasks to manage the overall system health and performance of Summation.

Workflow for Managing Summation

Step	Task	Link to the tasks
1	Monitor system activity using logs	See Using the System Log and Security Log on page 56.
2	Monitor the performance of the Distribution Server and the Work Managers	See Using the System Administration Console on page 54.

Most of these administrative tasks are performed in the Summation console in the **Management** page.

1.4.1 Opening the Management Page

Administrators, and users with management permissions, use the *Management* page to manage global settings and permissions.

To access the Management page

1. Log in to the Summation console as administrator or as a user with management permissions.
   See Opening the Summation Console on page 9.
   See Managing Users on page 27.
2. In the Summation console, click **Management**.

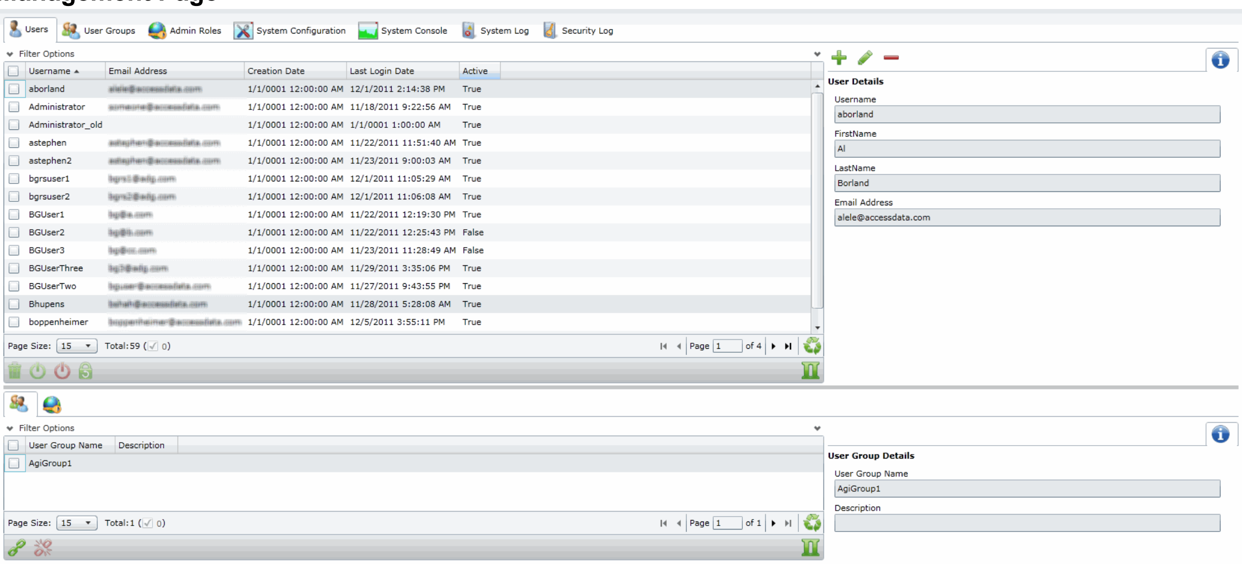
On the *Management* page, there are several different tabs where you perform administrative tasks.

1.5 Management Page

You can use the *Management* page to maintain the list of people who use Summation, including their specific usage rights and roles. From *Management*, you can view system and security logs.

You can also configure Active Directory, agent credentials, a notification email server. The system administration console area of the *Management* page lets you view Work Manager status.

Management Page



Management Page Features and Options

Management Feature	Available Options
Users	See Users Tab on page 20.
User Groups	See User Groups Tab on page 35.
Admin Roles	See Admin Roles on page 23.
System Configuration	See Configuring Active Directory Synchronization on page 40. See Configuring an Email Notification Server on page 42. See Configuring Default Case Settings on page 43.
System Console	See System Console Tab on page 52.
System Log	See System Log Tab on page 56.
Security Log	See Security Log Tab on page 58.

1.6 About Content in Lists and Grids

Many objects within the Home, Management, and Case Review tabs are made up of lists and grids. Many items in the lists and grids recur in the panels, tabs, and panes within the interface. The following sections describe these recurring elements.

You can manage how the content is displayed in the grids.

- See Refreshing the Contents in List and Grids on page 14.
- See Managing Columns in Lists and Grids on page 14.
- See Sorting by Columns on page 15.
- See Filtering Content in Lists and Grids on page 16.
- See Managing the Grid’s Pages on page 16.

1.6.1 Refreshing the Contents in List and Grids

There may be times when the list you are looking at is not dynamically updated. You can refresh the contents by clicking .

1.6.2 Managing Columns in Lists and Grids

You can manage the columns of data that are displayed in lists and grids. You can select which columns to display and the order of the columns.

To manage columns

1. In the grid, click **Columns**.

   Note: In the Case Review, the Columns button appears as Columns .

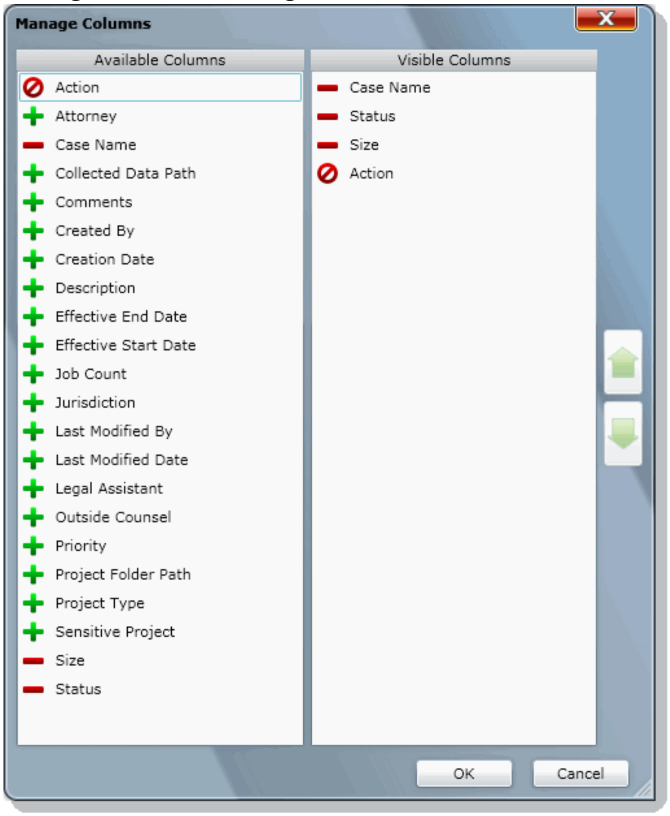
   ---

2. In the *Manage Columns* dialog, there are two lists:
   - *Available Columns*
     This lists all of the Columns that are available to display. They are listed in alphabetical order.

     If the column is configured to be in the Visible Columns, it has a .

     If the column is not configured to be in the Visible Columns, it has a .
   - *Visible Columns*
     This lists all of the Columns that are displayed. They are listed in the order in which they appear.

Manage Columns Dialog



3. To configure columns to be visible, in the *Available Columns* list, click the for the column you want visible.
4. To configure columns to not be visible, in the *Visible Columns* list, click the for the column you want not visible.
5. To change the display order of the columns, in the *Visible Columns* list, select a column name and click or to change the position.
6. Click **OK**.

1.6.3 Sorting by Columns

You can sort grids by columns. This is available on most columns.

To sort a grid by columns

1. Click the column head to sort by that column in an ascending order.
2. Click it a second time to sort by descending order.

1.6.4 Managing the Grid's Pages

When a list or grid has many items, you can configure how many items are displayed at one time on a page. This is helpful for customizing your view based on your display size and resolution and whether or not you want to scroll in a list.

To configure page size

1. Below a list, click the **Page Size** drop-down menu.
2. Select the number of items to display in one page.
3. Use the arrows by **Page *n* of *n*** to view the different pages.

1.6.5 Filtering Content in Lists and Grids

When a list or grid has many items, you can use a filter to display a portion of the list. Depending on the data you are viewing, you have different properties that you can filter for.

For example, when looking at the Activity Log, there could be hundreds of items. You may want to view only the items that pertain to a certain user. You can create a filter that will only display items that include references to the user.

For example, you could create the following filter:

Activity contains BSmith

This would include activities that pertain to the BSmith user account, such as when the account was created and permissions for that user were configured.

You could add a second filter:

Activity contains BSmith

OR Username = BSmith

This would include the activities performed by BSmith, such as each time she logged in or created a case.

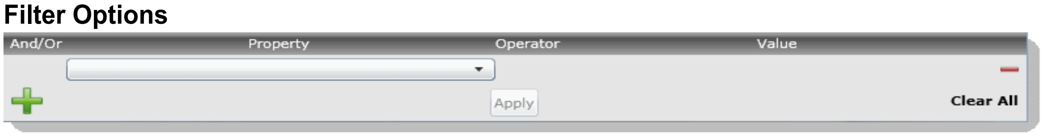
In this example, because an OR was used instead of an AND, both sets of results are displayed.

You can add as many filters as needed to see the results that you need.

To use filters

1. Above the list, click **Filter Options**.
   This opens the filter tool.

Filter Options



2. Use the *Property* drop-down to select a property on which to filter.
   This list will depend on the page that you are on and the data that you are viewing.
3. Use the *Operator* drop-down to select an operator to use.
   You can use **=** (equals),**!= (**does not equal), **Contains**, **StartsWith**, or **EndsWith**.
4. Use the *Value* field to enter the text on which you want to filter, such as a name, date, or text string.

5. Click **Apply**.

   The results of the filter are displayed.

   Once a filter had been applied, the text *Filter Enabled* is displayed in the upper-right corner. This is to remind you that a filter is applied and is affecting the list of items.

6. To further refine the results, you can add additional filters by clicking **Add**.
7. When adding additional filters, be careful to properly select *And/Or*.

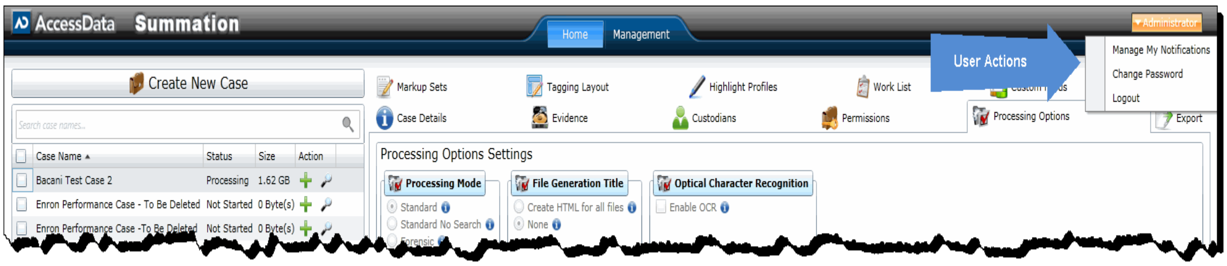
   If you select **And,** all filters must be true to display a result. If you select **OR**, all of the results for each filter will be displayed.

8. After configuring your filters, click **Apply**.
9. To remove a single filter, click .
10. To remove all filters, click **Clear All**.
11. To hide the filter tool, click **Filter Options**.

1.7 User Actions

Once in the Summation console, there are actions that can be performed that are specific to the logged-in user.

User Actions



In the top right corner of the console, there are links and user information.

Links in Top Right Corner of Summation Page

Link	Description
Logged-on user	The username of the logged-on user is displayed; for example, administrator.
Change password	This link lets the logged-on user change their password. See Changing Your Password (page 18). **Note:** This function is hidden if you are using Integrated Windows Authentication.
Logout	This link logs the user off and returns to the login page.

1.7.1 Changing Your Password

Note: This function is hidden if you are using Integrated Windows Authentication. Change your password using Windows methods.
See About User Accounts on page 8.

Any logged-in user can change their password. You may want to change your password for one of the following reasons:

- You are changing a default password after you log in for the first time.
- You are changing your password on a schedule, such as quarterly.
- You are changing your password after having a password reset.

To change your own password

1. Log in using your username and current password.
   See Opening the Summation Console on page 9.
2. In the upper right corner of the console, click **Change Password**.

3. In the **Change Password** dialog, enter the current password and then enter and confirm the new password in the respective fields. The following are password requirements:
   - The password must be between 7 - 20 characters.
   - At least one Alpha character.
   - At least one non-alphanumeric character.
4. Click **OK**.

Managing Cases

The part describes how to manage Summantion cases and includes the following sections:

2 Configuring and Managing System Users, Groups, and Roles

This chapter will help administrators to set up global users.

2.1 About Users

A user is any person who logs in and performs tasks in the web console. Each person should have their own user account. You can configure accounts to have specific permissions to perform specific tasks.

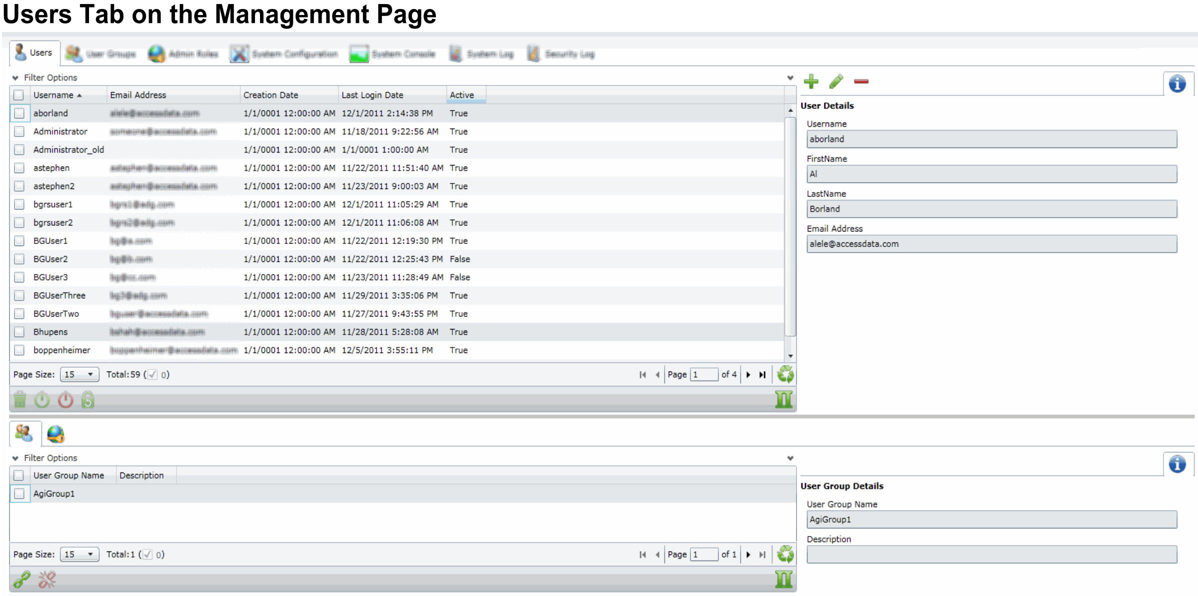
There are three types of users:

- **Administrator**: An Administrator has all privileges.
- **Case Manager**: Case Manager has some administrative privileges to manage cases.
- **Reviewers**: Users can be assigned different permissions to perform various tasks.
  See About User Permissions on page 22.
  See Adding Users on page 28.

2.1.1 Users Tab

The Users tab on the Management page can be used by administrators to add, edit, delete, and associate users on a global scale. Users are people who are logging in and working in Summation.

Users Tab on the Management Page



From the *Users* list, you can also add, edit, or delete Summation users. You can set users as active or inactive, reset user passwords, and set global and group permissions.

The *Users* list pane view is the default page when you click **Management** on the menu bar. The *Admin Roles* tab below the *Users* list pane identifies the permissions that are associated with a highlighted user.

Changes to permissions for a currently logged-in user take effect when they log out and log back in.

Elements of the Users Tab

Element	Description
Filter Options	Allows you to filter users in the list. See Filtering Content in Lists and Grids on page 16.
Users List	Displays all users. Click the column headers to sort by the column.
Refresh	Refreshes Users List. See Refreshing the Contents in List and Grids on page 14.
Columns	Click to adjust what columns display in the Users List. See Sorting by Columns on page 15.
Delete	Click to delete the selected user. Only active when a user is selected. See Deleting Users on page 31.
Add Users	Click to add a user. See About Users on page 20.
Edit User	Click to edit the selected user. You can add or change a selected user's email address that is used for notifications of Summation events. See Editing the Email Address of a User on page 29.
Delete User	Click to delete the selected user(s). See Deleting Users on page 31.
Reset a User's Password	Assigns a new password for the selected Summation user. See Resetting a User's Password on page 30.
Deactivate Users	Makes selected user inactive in Summation. See Deactivating a User on page 31.
Activate Users	Reactivates selected Summation user. See Activating a User on page 31.
Groups Tab	Associate or disassociate groups to users. See Associating a Group to a User on page 32.
Admin Roles Tab	Associate or disassociate admin roles to users. See Associating Admin Roles to a User on page 28.
Add Association	Click to associate a user to a group or admin role.

Elements of the Users Tab (Continued)

Element	Description
Remove Association 	Click to disassociate a user from a group or admin role.

2.1.2 About Planning User Roles

Before creating users, plan the kind of user roles that users will perform. This will make it easier to know which permissions to assign to which users.

See About User Accounts on page 8.

For example, consider the following:

- How many users should have Administrator permissions?
- How do you want to distinguish between users who can create and manage cases versus those who only review them?
- Who should perform case exports?

2.1.3 About User Permissions

You can assign users different permissions based on the tasks that you want them to perform. For example, you can have one set of users manage the creation of cases while another group only reviews files in a case.

See Associating Admin Roles to a User on page 28.

You can configure people or groups of people to do the following:

- Manage global settings like user permissions
- Create and manage cases
- View a case
- Review data in a case

The permissions that a user has affects the items that they see in the web console when they log in.

A user needs one of the following permissions to see the *Management* page in the console:

- Administrator
- Create/Edit Case
- Delete Case
- Manage User Groups
- Manage Admin Roles
- Manage Users

You can assign permissions at the system management level or at the individual case level.

Changes to permissions for a currently logged-in user take effect when they log out and log back in.

2.2 Admin Roles

You can create admin roles that you can assign to users or groups. The admin roles permissions allow users to manage users, cases, and permissions.

When you create an admin role, you can grant users Administrator permissions (all permissions) or grant a combination of individual permissions.

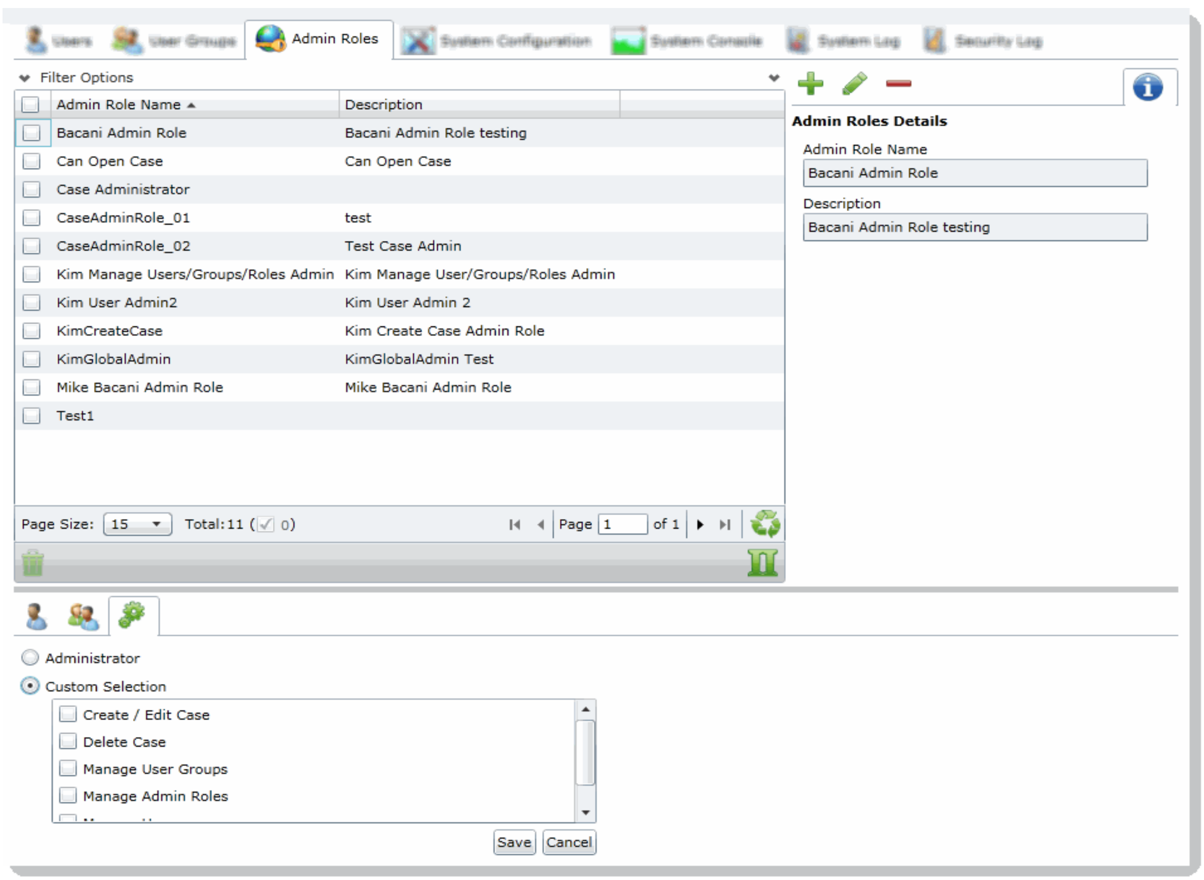
If you want to grant permissions to a user that only lets them review a case, use case-level permissions, rather than admin roles.

See Case-level Permissions on page 26.

2.2.1 Admin Roles Tab

The *Admin Roles* tab on the *Management* page can be used to add, edit, delete, and associate admin roles. Admin roles are a set of global permissions that you can associate with a user or a group.

Admin Roles Tab



Elements of the Admin Roles Tab

Element	Description
Filter Options	Allows you to filter admin roles in the list. See Filtering Content in Lists and Grids on page 16.
Admin Roles List	Displays all admin roles. Click the column headers to sort by the column.
Refresh	Refreshes Admin Roles List. See Refreshing the Contents in List and Grids on page 14.
Columns	Click to adjust what columns display in the Admin Roles List. See Sorting by Columns on page 15.
Delete	Click to delete the selected admin roles. Only active when an admin roles is selected. See Admin Roles on page 23.
Add Admin Roles	Click to add an admin role. See Creating an Admin Role on page 24.
Edit Admin Roles	Click to edit the selected admin roles.
Delete Admin Roles	Click to delete the selected admin roles.
Users Tab	Associate or disassociate users to an admin role.
Groups Tab	Associate or disassociate groups to an admin role.
Features Tab	Add administrator permissions to an admin role. See Adding Permissions to an Admin Role on page 25.

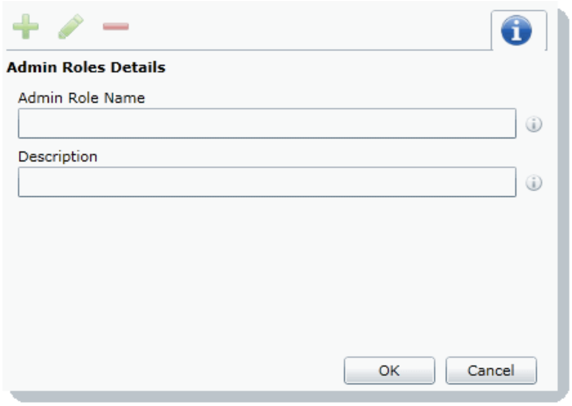
2.2.2 Creating an Admin Role

Before you can assign permissions to an admin role, you have to create the role.

To create an admin role

1. Log in to the Summation Console using administrator rights.
2. Click on the **Management** tab.
3. Click on the **Admin Roles** tab. See Admin Roles on page 23.
4. Click the **Add** button .

Admin Roles Details



5. Enter a name for the admin role and a description.
6. Click **OK**.
   The role is added to the Admin Role list.

2.2.3 Adding Permissions to an Admin Role

After you have created an admin role, you need to add permissions to it before you assign it to a user or a group.

To add permissions to an admin role

1. Log in to the Summation Console using administrator rights.
2. Click on the **Management** tab.
3. Click on the **Admin Roles** tab. See Admin Roles on page 23.
4. Select the role from the *Admin Roles List*.
5. Click on the **Features** tab  .
6. Select the Permissions:
   - **Administrator**: Grants all rights to the user/group for all cases.
   - **Custom**: Select the administrator roles that you want. The following are available:
     - **Create/Edit Case**: Grants the right to create and edit cases on the Home page.
     - **Delete Case**: Grants the right to delete cases on the Home page.
     - **Manage User Groups**: Grants the right to add, edit, delete, and assign roles to groups.
     - **Manage Admin Roles**: Grants the right to add, edit, delete and assign admin roles.
     - **Manage Users**: Grants the rights to add, edit, delete, activate, deactivate, reset passwords, and assign admin roles to users.

   Note: Users with the Manage Admin Roles, Manage Users, or Manage User Groups permission have the ability to upgrade themselves or other users to system administrators.

7. Click **Save**.

2.2.4 Case-level Permissions

Case-level permissions are set by the case manager, see the Case Manager documentation for more information on how to set case-level permissions. These are permissions that are given only to individuals working on a specific case.

2.3 Managing Users

Administrators, and users assigned the Manage Users permission, manage users by doing the following:

- Managing the List of Users (page 27)
- Adding Users (page 28)
- Editing the Email Address of a User (page 29)
- Resetting a User's Password (page 30)
- Deleting Users (page 31)
- Deactivating a User (page 31)
- Activating a User (page 31)
- Associating Admin Roles to a User (page 28)

2.3.1 Managing the List of Users

You create and manage users from the *Users* tab on the *Management* page.

To open the Users tab

1. Log in as an administrator or a user that has the Manage Users permission.
   See Opening the Summation Console on page 9.
2. Click **Management**.
3. Click **Users**  .

   The users list lets you view all the users, including the following columns of information about them:
   - Username
   - Email Address of the user
   - Date that the user was created
   - Date of last login for the user
   - Active status of a user
   - First and Last name of the user
   - Description

From the users list, you can also add, edit, or delete users. You can set users as active or inactive, reset user passwords, and associate groups to users and admin roles.

When you create and view the list of users, they are displayed in a grid. You can do the following to modify the contents of the grid:

- Control which columns of data are displayed in the grid.
- If you have a large list, you can apply a filter to display the items that you want.

2.3.2 Adding Users

Each person that uses the console must log in with a username and password. Each person should have their own user account.

Administrators, and users assigned the Manage Users permission, can add new user accounts.

When a user is created, an entry is created in the system databases.

How you add users is a little different depending on whether or not you are using Integrated Windows Authentication.

If you are *not* using Integrated Windows Authentication, you configure both the username and password.

In this mode, a password is required, and the *Password* field is bolded.

If you *are* using Integrated Windows Authentication, you enter the domain username and *do not* enter a password.

In this mode, a password is *not* required, and the Password field is hidden.

To add a user

1. Open the *Users* tab.
   See Managing the List of Users (page 27).
2. In the *User Details* pane, click (add).
3. In the **Username** field, enter a unique username.
   The name must be between 7 - 32 characters and must contain only alphanumeric characters.
   If you *are* using Integrated Windows Authentication, enter the user's domain and username. For example, <domain>\<username>.
4. Enter the First and Last name of the user.
5. (Optional) In the **Email Address** field, enter the email address of the user.
6. If you are *not* using Integrated Windows Authentication, in the **Password** and the **Reenter Password** fields, enter a password.
   The password must be between 7 - 20 characters.
7. Click **OK**.

2.3.3 Associating Admin Roles to a User

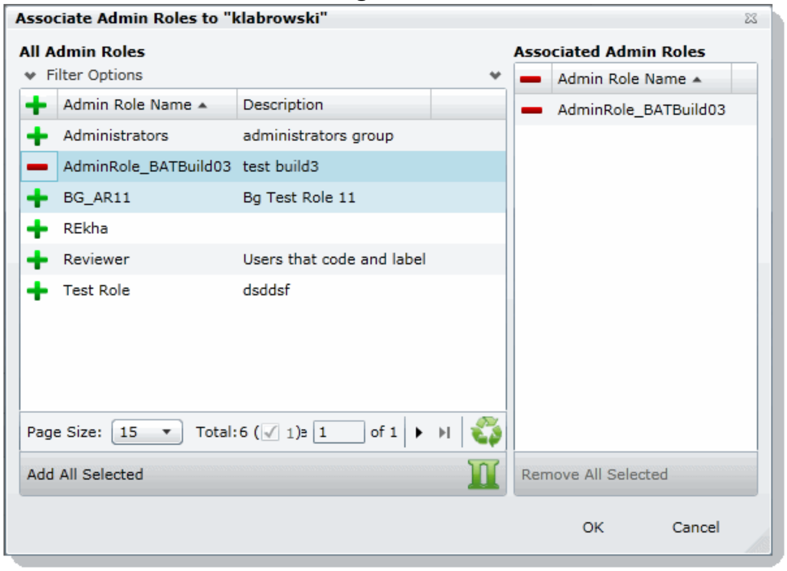
Administrators, and users assigned the Manage Users permission, can associate admin roles to users.

See About User Permissions on page 22.

To associate admin roles to user

1. Open the *Users* tab.
   See Managing the List of Users (page 27).
2. In the user list pane, select a user who you want to associate to an admin role.
3. In the bottom pane, select the **Admin Roles** tab.
4. Click the **Add Association** button .

Associate Admin Roles Dialog



5. Click the plus sign to add the role to the user.
6. Click **OK**.

2.3.4 Disassociating an Admin Role from a User

Administrators, and users assigned the Manage Users permission, can disassociate admin roles from users.

See About User Permissions on page 22.

To disassociate admin roles from a user

1. Open the *Users* tab.
   See Managing the List of Users (page 27).
2. In the user list pane, select a user who you want to disassociate from an admin role.
3. In the bottom pane, select the **Admin Roles** tab.
4. Check the role that you want to remove.
5. Click the **Remove Association** button .

2.3.5 Editing the Email Address of a User

Administrators, and users assigned the Manage Users permission, can change the email address of an existing user. If you need to make more than an email change (such as changing the username), you must delete the user, and then recreate the user with the correct information.

To edit the email address of a user

1. Open the *Users* tab.
   See Managing the List of Users (page 27).
2. In the user list pane, select the user whose email address you want to edit.

3. In the *User Details* pane, click (edit).
4. In the *Email Address* field, enter the email address of the user.
5. Click **OK**.

2.3.6 Resetting a User's Password

If a user has forgotten their password, administrators and users assigned the Manage Users permission can reset password for users.

Note: This function is hidden if you are using Integrated Windows Authentication. Reset a password using Windows methods.

You cannot reset the password of the Service Account.

See Changing the Password of the Service Account on page 30.

When you reset a user's password, a new password is automatically created. You can then give the new password to the user. After they log in with the new password, they can change the password themselves.

You cannot reset your own password. To change your own login password, you do not use the *User* page, but the *Change Password* dialog instead.

See Changing Your Password on page 18.

To reset the password of an administrator or user

1. Open the *Users* tab.
   See Managing the List of Users (page 27).
2. In the user list pane, check a user.
3. Click .
   A new password for the user is generated and displayed.
4. Copy the password and email it to the user, informing them that they can change the password after logging in.

2.3.6.1 Changing the Password of the Service Account

This only applies if you *are not* using Integrated Windows Authentication. The service account password can only be changed by the user who is logged in as the master administrator. This person is typically the one who initially performed the installation. The username cannot be changed.

See Changing Your Password on page 18.

You can use the same process as you do for a user.

See Resetting a User's Password on page 30.

2.3.7 Deleting Users

Users can be deleted by an administrator or a user with the right to delete users.

If you try to recreate a deleted user, you receive a warning that the user already exists in Summation and was marked as deleted. You can continue to create the user anyway and assign user rights as if they are a new user.

To delete users

1. Open the *Users* tab.
   See Managing the List of Users (page 27).
2. Do one of the following:
   - In the users list, highlight the user that you want to delete. In the *User Details* pane, click (delete).
   - In the users list, check one or more users that you want to delete. Click **Delete.**
3. In the **Confirm Deletion** dialog box, click **OK**.

2.3.8 Deactivating a User

You can deactivate users as needed to make the console unavailable to them. When you deactivate a user, that user remains in the users list of the *Users* tab, and has the status of *False* in the *Active* column. The user's data remains in the database; however, the user cannot log in, and they are not available for any other assignments or work. The user remains inactive until an administrator reactivates them. You can activate or deactivate users individually or collectively.

See Activating a User on page 31.

To deactivate a user

1. Open the *Users* tab.
   See Managing the List of Users (page 27).
2. In the user list pane, check one or more users whose **Active** status is **True**.
3. Click Deactivate.
4. In the *Deactivate user* message box, click **Yes**.

2.3.9 Activating a User

You can activate users as needed. When a user is activated, they can log in and be available for work. An activated user remains active until an administrator deactivates them. You can activate or deactivate users individually or collectively.

See Deactivating a User on page 31.

To activate a user

1. Open the *Users* tab.
   See Managing the List of Users (page 27).
2. In the user list pane, check one or more users whose *Active* status is *False*.

3. In the bottom of the middle pane, click .
4. In the *Activate user* frame, click **Yes**.

2.3.10 Associating a Group to a User

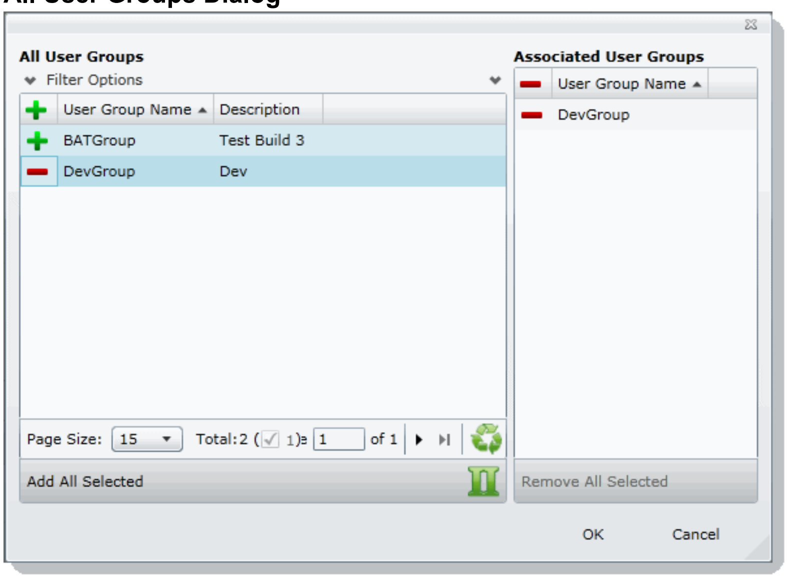
Groups are a set of users grouped together that perform the same tasks. Putting users into groups makes it easier to assign and manage case permissions for users. Administrators, and users assigned the Manage Users permission, can associate groups to users.

See About User Permissions on page 22.

To associate groups to user

1. Open the *Users* tab.
   See Managing the List of Users (page 27).
2. In the user list pane, select a user who you want to associate to a group.
3. In the bottom pane, select the **User Groups tab**.
4. Click the **Add Association** button .

All User Groups Dialog



5. Click the plus sign to associate the user to the group.
6. Click **OK**.

2.3.11 Disassociating a Group from a User

Administrators, and users assigned the Manage Users permission, can disassociate groups from users.

See About User Permissions on page 22.

To disassociate groups from user

1. Open the *Users* tab.
   See Managing the List of Users (page 27).
2. In the user list pane, select a user who you want to disassociate from a group.
3. In the bottom pane, select the **User Groups tab**.
4. Check the group you want to remove.
5. Click the **Remove Association** button .

2.4 Configuring and Managing Groups

Groups are a set of users grouped together. Groups allow you to put sets of users together who perform the same tasks. Putting users into groups makes it easier to assign and manage case permissions for users.

The case permissions that you assign to users define the tasks that they can perform. Therefore, if you have a group of users who all are going to review documents, you can put them in a group and grant them permissions to review, code, and label documents.

Administrators, and users assigned the Manage Groups permission, can manage groups.

2.4.1 Opening the User Groups Tab

To open the User Groups tab

1. Log in as an administrator or a user with the Manage Groups admin role.
   See Opening the Summation Console (page 9).
2. Click **Management**.
3. Click **User Groups**  .

   The users list lets you view all the groups, including the following columns of information about them:
   - User Group Name
   - Description

From the group list, you can also add, edit, or delete groups. You can associate groups to users and admin roles.

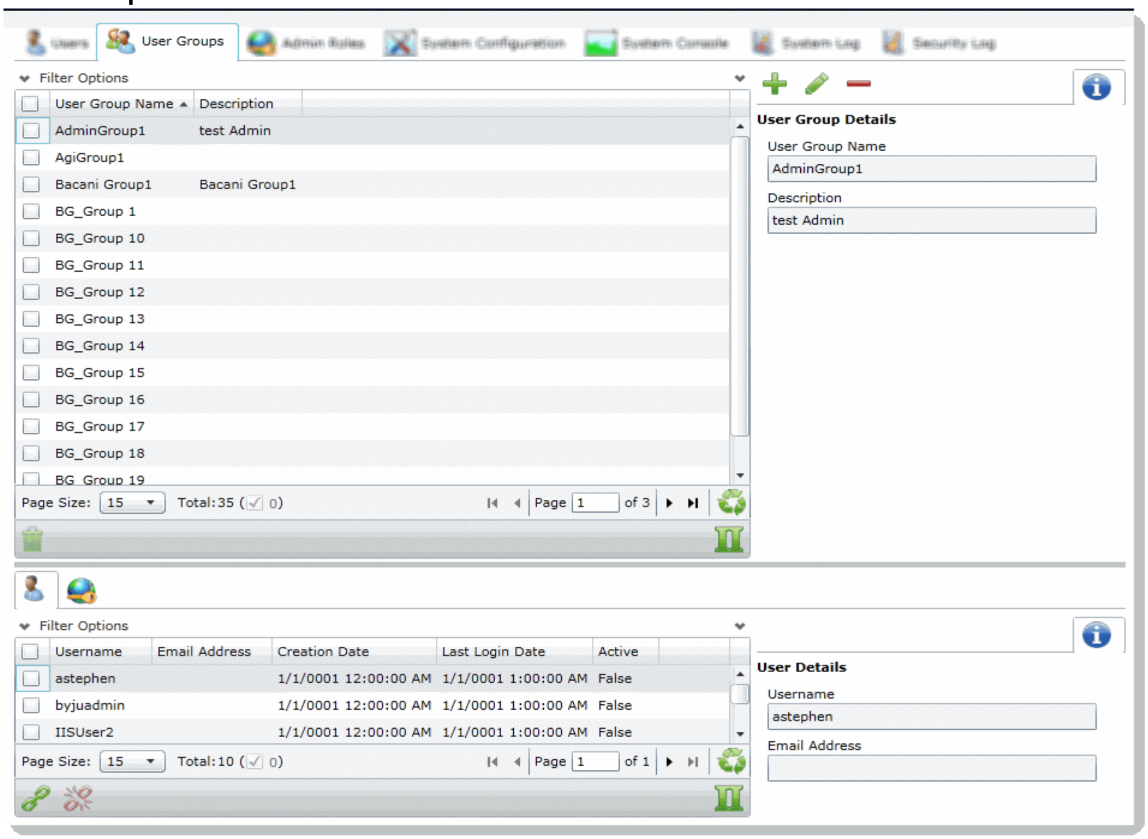
When you create and view the list of groups, they are displayed in a grid. You can do the following to modify the contents of the grid:

- Control which columns of data are displayed in the grid.
- If you have a large list, you can apply a filter to display the items that you want.

2.4.2 User Groups Tab

The *User Groups* tab on the *Management* page can be used to add, edit, delete, and associate user groups on a global scale. Groups are collections of users who perform the same tasks in Summation.

User Groups Tab



Elements of the User Groups Tab

Element	Description
Filter Options	Allows you to filter groups in the list. See Filtering Content in Lists and Grids on page 16.
Groups List	Displays all groups. Click the column headers to sort by the column.
Refresh 	Refreshes Groups List. See Refreshing the Contents in List and Grids on page 14.
Columns 	Click to adjust what columns display in the Groups List. See Sorting by Columns on page 15.
Delete 	Click to delete the selected group. Only active when a group is selected. See Deleting Groups on page 37.

Elements of the User Groups Tab (Continued)

Element	Description
Add Groups	Click to add a group. See Adding Groups on page 36.
Edit Groups	Click to edit the selected group. See Editing Groups on page 37.
Delete Groups	Click to delete the selected group. See Deleting Groups on page 37.
Users Tab	Associate or disassociate users to groups. See Associating Users/Admin Roles to a Group on page 37.
Admin Roles Tab	Associate or disassociate admin roles to groups. See Associating Users/Admin Roles to a Group on page 37.
Add Association	Click to associate a group to a user or admin role.
Remove Association	Click to disassociate a group from a user or admin role.

2.4.3 Adding Groups

To add a group

1. Open the *User Groups tab*.
   See Opening the User Groups Tab (page 34).
2. In the *Groups Details* pane, click (add).
3. In the **User Group Name** field, enter a unique username.
   The name must be between 7 - 32 characters and must contain only alphanumeric characters.
4. Enter a *Description*.
5. Click **OK**.

2.4.4 Deleting Groups

To delete a group

1. Open the *User Groups tab*.
   See Opening the User Groups Tab (page 34).
2. Do one of the following:
   - In the groups list, highlight the group that you want to delete. In the *Groups Details* pane, click (delete).
   - In the users list, check one or more users that you want to delete. Click **Delete.**
3. In the *Confirm Deletion* dialog box, click **OK**.

2.4.5 Editing Groups

To edit a group

1. Open the *User Groups* tab.
   See Opening the User Groups Tab (page 34).
2. In the *Groups Details* pane, click (edit).
3. In the **User Group Name** field, enter a unique username.
   The name must be between 7 - 32 characters and must contain only alphanumeric characters.
4. Enter a *Description*.
5. Click **OK**.

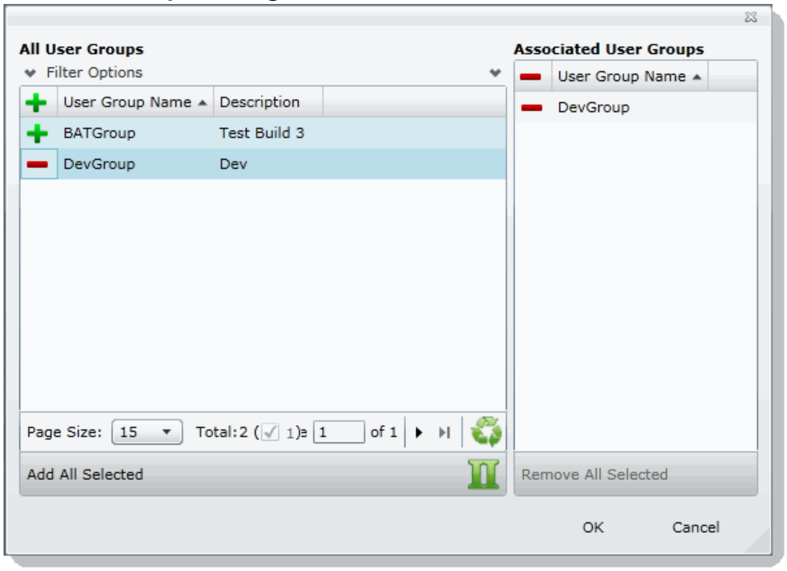
2.4.6 Associating Users/Admin Roles to a Group

From the *User Groups* tab, you can associate users and admin roles to the selected group.

To associate users/admin roles to a group

1. Open the *User Groups* tab.
   See Opening the User Groups Tab (page 34).
2. In the user list pane, select a group who you want to add an association to.
3. In the bottom pane, do one of the following:
   - Select the **Users** tab to associate users to the group.
   - Select the **Admin Roles** tab to associate roles to the group.
4. Click the **Add Association** button .
5. Click the plus sign to add users/roles.
6. Click **OK**.

All User Groups Dialog



7. Click the plus sign to associate the user to the group.
8. Click **OK**.

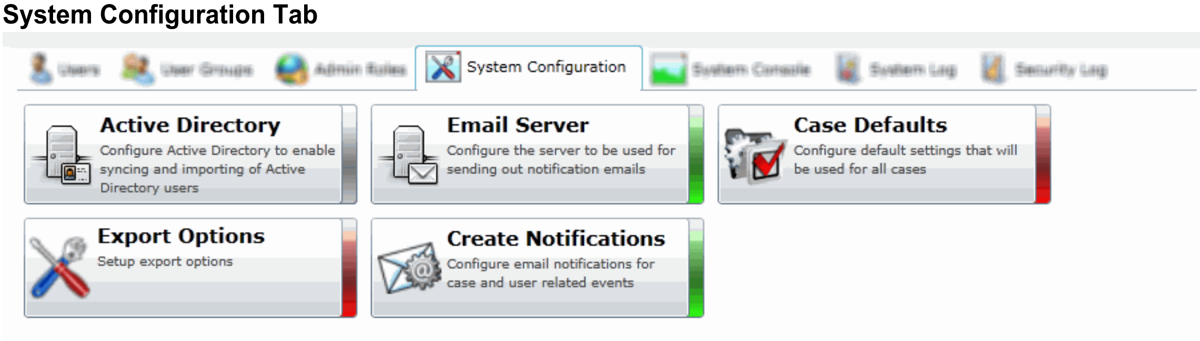
3 Configuring the System

This chapter will help administrators configure the Summation system to their preferences.

3.1 System Configuration Tab

The *System Configuration* tab on the *Management* page allows you to configure multiple items. This section describes each item.

System Configuration Tab



Elements of the System Configuration Tab

Element	Description
Active Directory	You can configure Active Directory to synchronize and import Active Directory users. Synchronization is from Active Directory to Summation only. See Configuring Active Directory Synchronization on page 40.
Email Server	You can configure the *Email Notification Server* so that when you create a job, notification emails are sent to the email address that is specified for a particular Summation user. See Configuring an Email Notification Server on page 42.
Case Defaults	You can configure the following settings that will be used every time you create a case: ● Default paths for case data ● Default options for processing evidence in cases See Configuring an Email Notification Server on page 42.

3.2 Configuring Active Directory Synchronization

You can sync with Active Directory to import your domain users to be Summation custodians.

Note: When you sync with Active Directory, all users will be imported.

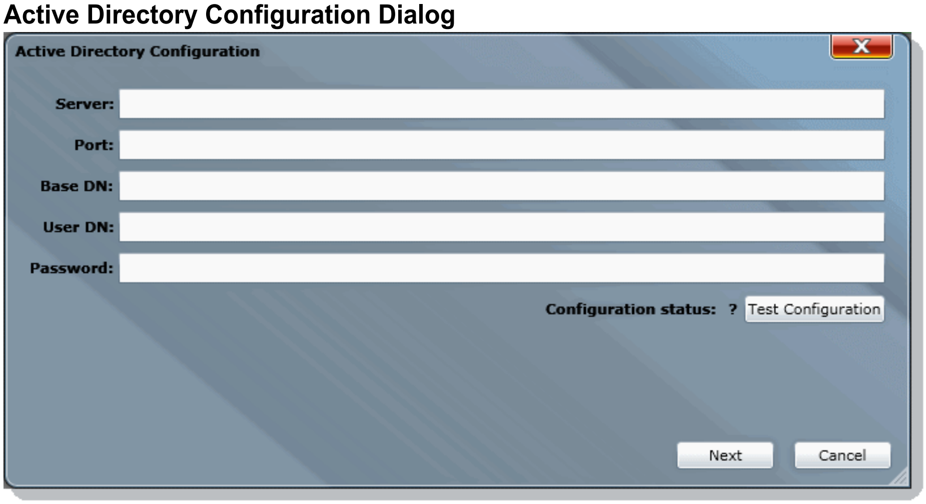
Synchronization is only one direction from Active Directory.

Note: Domain Users can be imported, but they cannot be Summation users. They will only be used as custodians.

To configure Active Directory synchronization

1. Log in as an administrator.
   See Opening the Summation Console (page 9).
2. Click **Management.**
3. Click **System Configuration**.
4. Click **Active Directory**.

Active Directory Configuration Dialog



5. In the *Active Directory Configuration* dialog box, set all options and then click **Next**.

Options in the Active Directory Configuration Dialog

Option	Description
Server	Enter the server name of a domain controller in the enterprise.
Port	Enter the connection port number used by Active Directory. The default port number is 389.

Options in the Active Directory Configuration Dialog (Continued)

Option	Description
Base DN	Enter the starting point in the Active Directory hierarchy at which the search for users and groups begins. The Base DN (Distinguished Name) describes where to load users and groups. For example, in the following base DN dc=**domain**,dc=**com** you would replace **domain** and **com** with the appropriate domain name to search for objects such as users, computers, contacts, groups, and file volumes.
User DN	Enter the distinguished name of the user that connects to the directory server. For example tjones or <domain>\tjones
Password	Enter the password that corresponds to the User DN account; used when connecting to the directory server.
Test Configuration	Click to test the current configuration to ensure proper communication exists with the Active Directory server.

6. Click **Next.**
7. Select which Active Directory fields you want to import into User information.

   In the *Active Directory Fields* dialog box, in the *Active Directory Fields* list box, select an alias attribute and then click  next to the user field that you want associated with the attribute.

   User field names that are bold are required fields.

   The following are examples of fields that you can use:

Active Directory Fields

Active Directory Field	Custodian Field
givenname	*First Name* (Required)
sn	*Last Name* (Required)
samaccountname	*Username* (Required)
displayname	Notes Username
mail	Email

8. Click **Next.**
9. Do one of the following:
   - To save the settings, but not perform a sync, click **Save**.
   - If you have completed all the settings and are ready to sync, click **Save and Sync**.
10. View the imported user in the Users tab.

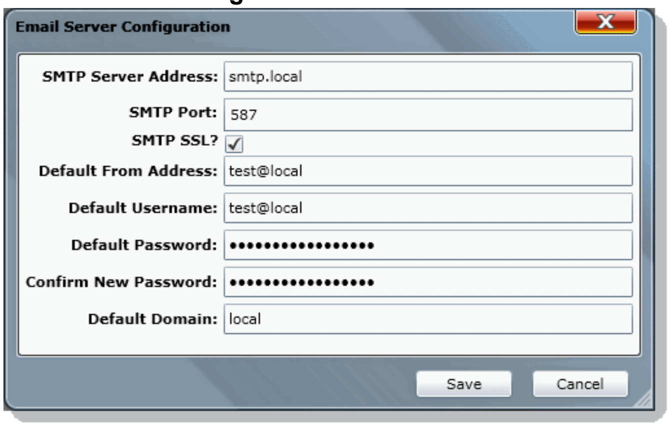
3.3 Configuring an Email Notification Server

You can configure the *Email Notification Server* so that when you create a job, notification emails are sent to the email address that is specified for a particular Summation user.

To configure an email notification server

1. Click **Management**.
2. Click **System Configuration**.
3. Click **Email Server**.

Email Server Configuration



4. In the *Email Server Configuration* dialog box, set the email options that you want. The following table describes the available options.

Email Server Configuration Options

Option	Description
SMTP Server Address	Specifies the address of the SMTP mail server (for example, smtpserver.domain.com or server1) on which you have a valid account. You must have an SMTP-compliant email system, such as a POP3 mail server, to receive notification messages from Summation.
SMTP Port	Port 25 is the standard non-SSL SMTP port, but it could also be different. If a connection is not established with default port 25, contact the email server administrator to get the correct port number.
Default From Address	Specifies the name of the default email account from which alerts and notifications are sent.
SMTP SSL	Lets you configure the use of SSL by the SMTP server. The default SSL port is 465.
Default Username	Specifies the sender’s name. The default credentials (Username, Password, Domain) are optional.
Default Password	Specifies the sender’s password.
Default Domain	Specifies the sender’s domain.

5. Click **Save**.

3.4 Configuring Default Case Settings

3.4.1 About Default Case Settings

You can configure the following settings that will be used every time that you create a case:

- Default paths for case data
- Default options for processing evidence in cases

It is not mandatory to set defaults. For processing options, there are defaults that are pre-set.

If no default case paths are configured, the person creating the case will have to provide this information.

If you do configure default settings, you can also choose whether or not to display those settings when a case is created. If you allow the values to be shown, the user creating the case can both see and change the values.

You can configure the default values to be hidden. If you hide them, the person creating the case does not see the options and cannot change them. Therefore, if you want to force certain default settings, you can set the defaults and then hide them.

See Setting Default Case Settings on page 43.

See Default Evidence Folder Options on page 44.

See Default Evidence Processing Options on page 44.

3.4.2 Setting Default Case Settings

You can set default case evidence settings.

See About Default Case Settings on page 43.

To set default case options

1. Log in as an administrator.
   See Opening the Summation Console (page 9).
2. Click **Management**.
3. Click  **System Configuration**.
4. Click **Case Defaults**.
5. On the *Info* tab, set the default path settings.
   See Default Evidence Folder Options on page 44.
6. On the *Processing Options* tab, set the default evidence processing options.
   See Default Evidence Processing Options on page 44.
7. Click **Save**.

3.4.3 Default Evidence Folder Options

You can define default locations where the case data is stored. These locations are set whenever you create a case.

See Configuring an Email Notification Server on page 42.

Local paths only work on single box installations.

If a network UNC path is specified, you can validate the path to ensure that the application can access the location. If the path is not validated, you may need to re-enter the path correctly, or specify a new path.

To verify the path, click .

Paths

Case Folder Path	Lets you specify a local path or a UNC network path to the case folder.
Job Data Path	The responsive folder path is the location of reports data.

3.4.4 Default Evidence Processing Options

The processing options that are set here are the default options used by a case when it is created.

See About Default Case Settings on page 43.

See Evidence Processing and Deduplication Options on page 46.

You can also choose whether or not to display these settings when a case is created. If you allow the values to be shown, the user creating the case can both see and change the values.

You can configure the default values to be hidden. If you hide them, the person creating the case does not see the options and cannot change them. Therefore, if you want to force certain default settings, you can set the defaults and then hide them.

Hover the mouse over the information icon to get information about each item.

The installed defaults are specified below:

Default Evidence Processing Options

Option	Description
Hide Processing Options	Lets you hide the processing options dialog when a user creates a case. This forces the case to use the default values set here. Pre-set default is off.
Processing Mode	Standard (Pre-set default mode) See Evidence Processing and Deduplication Options on page 46.
	Standard No Search See About Indexing for Text Searches of Content of Files on page 51.
	Forensic

Default Evidence Processing Options (Continued)

Option	Description
	Quick
Optical Character Generation	Enable OCR. Pre-set default is off. See About Optical Character Recognition on page 51. See Evidence Processing and Deduplication Options on page 46.
Document Deduplication: De-dup At:	Case level (Pre-set default) See Evidence Processing and Deduplication Options on page 46. See Deduplication Options on page 48.
	Custodian Level
Document Deduplication: De-dup On:	Actual Files Only Pre-set default is off.
Email Deduplication: De-dup At:	Case level (Pre-set default) See Evidence Processing and Deduplication Options on page 46. See Deduplication Options on page 48.
	Custodian Level
Email Deduplication: De-dup On:	
	To (Pre-set default)
	From (Pre-set default)
	Subject (Pre-set default)
	CC
	BCC
	Submit Time (Pre-set default)
	Delivery Time
	Email Hash
	Whole Email Contents
	Email Body Only
Cluster Analysis:	
	Perform Cluster Analysis: Invokes the extended analysis of documents to determine related, near duplicates, and email threads.
	Cluster Threshold: Determines the level of similarity required for documents to be considered related or near duplicates.
Language Identification:	
	None: Performs no language identification, all documents are assumed to be written in English. This is the faster processing option.

Default Evidence Processing Options (Continued)

Option	Description
	Basic: Performs language identification for English, Chinese, Spanish, Japanese, Portuguese, German, Arabic, French, Russian, and Korean.
	Extended: Performs language identification for 71 different languages. This is the slowest processing option.

3.4.5 Evidence Processing and Deduplication Options

The options you select determine the data that is contained in cases, reports, and consequently, production sets.

Note: You cannot edit any settings on the **Processing Options** section after you have added evidence to a case

The following table describes the **Processing Options**.

See Deduplication Options on page 48.

See Default Evidence Processing Options on page 44.

Processing Options

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Standard Mode</td><td>Enables the default Summation processing options.
Note: These defaults are not editable.
Will include:
Hashing (MD-5 only)
KFF (NIST modules only)
eDiscovery Deduplication - Case level for both Documents and Email
Flag bad extensions
Expand Compound Files (archive expansion) of the following file types:
IPD, BZIP, DBX, GZIP, NSF, MBOX, EDB, MS Office, MSG, PKCS, PST, RAR, RFC822, TAR, ZIP
Will index:
Text data
Will not include:
HTML file listing
Deleted files
Thumbnails for graphics
Refinement options:
File slack
Free space
KFF ignorable files
Microsoft OLE Streams
Microsoft OPC documents
Office 2010 package contents
Zero length files
OS/File System Files
Will not index:
Graphic files, executable files, and email headers</td></tr>
<tr><td>Standard No Search</td><td>Uses the default Summation processing options, but does not include the indexing of text data.</td></tr>
</table>

Processing Options (Continued)

Option	Description
Forensic	Will include: ● Hashing (MD-5, SHA-1, SHA-256) ● Flag bad extensions ● Thumbnails for graphics ● Deleted files ● Microsoft OLE Streams ● Microsoft OPC documents ● Refinement options: ■ File slack ■ Free space Will index: ● all file types Will not include: ● KFF (for faster processing) ● Expand Compound Files (archive expansion) ● HTML file listing ● eDiscovery Deduplication
Quick	Increases the speed of the processing of evidence by using minimal options to expedite the processing. Indexing, hashing, archive file drill down, and file identification are disabled (files are identified by header analysis instead of file extension). If you click this option, the *KFF Lookup* option is disabled. The reason for this behavior is because *Field Mode* is a processing option that is intended to speed up the process; it turns off indexing, hashing, and other options that tend to slow down data processing. The *KFF Lookup* option takes time to process and slows down data processing. Therefore, if both *Field Mode* and *KFF Lookup* were both enabled, it would defeat the purpose of the Quick option.
Enable OCR	Generates text from graphics files and indexes the resulting content. You can then use *Case Review* to search and label the content, and treat it as you would any other text in the case. AccessData uses the GlyphReader engine for optical character recognition. Checking this option can increase processing time up to 50%. It also may give you results that differ between processing jobs on the same computer, with the same piece of evidence.

3.4.5.1 Deduplication Options

Deduplication helps a case investigation by flagging duplicate electronic document (e-document) files and emails within the data of a case or custodian. The duplicates filter, when applied during case analysis, removes all files flagged “True” (duplicate) from the display, significantly reducing the number of documents an investigator needs to review and analyze to complete the case investigation.

If you set document deduplication at the case level, and two custodians have the same file, one file is flagged as primary and the other file or files are flagged as duplicates. The file resides in the case and the file paths are tracked to both custodians. To limit the production set, the file is only created one time during the load file/native file production. You can also deduplicate email, marking the email, email contents, or email attachments as duplicates of others.

Note: In *Case Review*, if the duplicate filter is on, and if you do a search for a file using a word that is part of the file path, and that path and file name is a duplicate, the search will not find that file. For example, suppose there is a spreadsheet that is located in one folder called Sales and a duplicate of the file exists in a folder called Marketing. And suppose that the file in Sales is flagged as the primary and the file in Marketing is flagged as a duplicate. If you do a search for spreadsheets in the folder named Sales, it will be found. However, if you do a search for spreadsheets in the folder named Marketing, it will not be found. You would have to turn off the duplication filter and then perform the search.

See Evidence Processing and Deduplication Options on page 46.

Deduplication options are integrated on the *Processing Options* page.

The following tables describe the deduplication options that are available in the *Processing Options*.

Document Deduplication Options

Option	Description
Case Level	Deduplication compares each of the e-documents processed within a case against the others as they receive their hash during processing. If the hash remains singular throughout processing, it receives no duplicate flag. In the case of duplicate files, the first hash instance receives a “primary” flag and each reoccurrence of the hash thereafter receives a “secondary” flag.
Custodian Level	Deduplication compares the e-documents found in each custodial storage location against the other files from that same custodial location (custodians, or in the case of no custodian, the storage location). If the hash remains singular throughout processing, it receives no duplicate flag. In the case of duplicate files the first hash instance receives a “primary” or “master” flag and each reoccurrence of the hash thereafter receives a “duplicate” flag.
Actual Files Only	Deduplicates actual files instead of all files. Checking this option excludes OLE files and Alternate Data Stream files.

You can also deduplicate email, marking the email, email contents, or email attachments as a duplicate of others.

Email Deduplication Options

Option	Description
Case Level	The scope of the email deduplication. Deduplication compares each of the emails processed within a case against the others as they are processed. If the deduplication value remains singular throughout processing, it receives no duplicate flag. In the case of duplicate email, the first value instance receives a “primary” flag and each reoccurrence of the value thereafter receives a “duplicate” flag. If two custodians have the same email, it is marked as a duplicate.

Email Deduplication Options (Continued)

Option	Description
Custodian Level	The scope of the email deduplication. Deduplication compares the email found in each custodial storage location against the other emails from that same custodial location (custodians, or in the case of no custodian, the storage location). If the value remains singular throughout processing it receives no duplicate flag. In the case of duplicate emails, the first email instance receives a “primary” or “master” flag and each reoccurrence of the email thereafter receives a “duplicate” flag. In the case of duplicate files the first value instance receives a “primary” flag and each reoccurrence of the value thereafter receives a “duplicate” flag.
Email To	Deduplicates email based on the recipients in the “To” field.
Email From	Deduplicates email based on the senders in the “From” field.
Email CC	Deduplicates email based on the recipients in the “Carbon Copy” field.
Email Bcc	Deduplicates email based on the recipients in the “Blind Carbon Copy” field.
Email Subject	Deduplicates email based on the contents in the “Subject” field.
Email Submit Time	Deduplicates email based on the date and time the email was initially sent.
Email Delivery Time	Deduplicates email based on the date and time the email was delivered to the recipients.
Email Attachment Count	Deduplicates email based on the number of attached files.
Email Hash	Deduplicates email based on the hash value.
Body and Attachments	Includes email body, recipients (the “To” field), sender (the “From” field), CC, BCC, Subject field contents, body message, the number of attachments, and the attachments for deduplication.
Body Only	Includes only the email body and the list of attachment names for deduplication.

3.4.6 About Optical Character Recognition

Optical Character Recognition (OCR) is a feature of the processing options for Summation. The OCR process generates text from graphic files and then indexes the content so extracted text can be searched, labeled, and so forth.

Note: It is important to understand the limitations and variability of the OCR process.

Therefore, the following information may prove useful as you incorporate the use of OCR in the processing of your cases:
- OCR can have inconsistent results. OCR engines by nature have error rates which means that it is possible to have results that differ between processing jobs on the same machine with the same piece of evidence.
- Some large images can cause OCR to take an extraordinarily long time to complete and under some circumstances not generate any output for a given file.
- Graphical images that have no text or pictures with unaligned text can generate garbage output.
- OCR is best on typewritten text that is cleanly scanned or similarly generated. All other picture files can generate unreliable output that can vary from run to run.

OCR is only a helpful tool for the investigator to locate images from index searches and OCR results should not be considered evidence without further review.

3.4.7 About Indexing for Text Searches of Content of Files

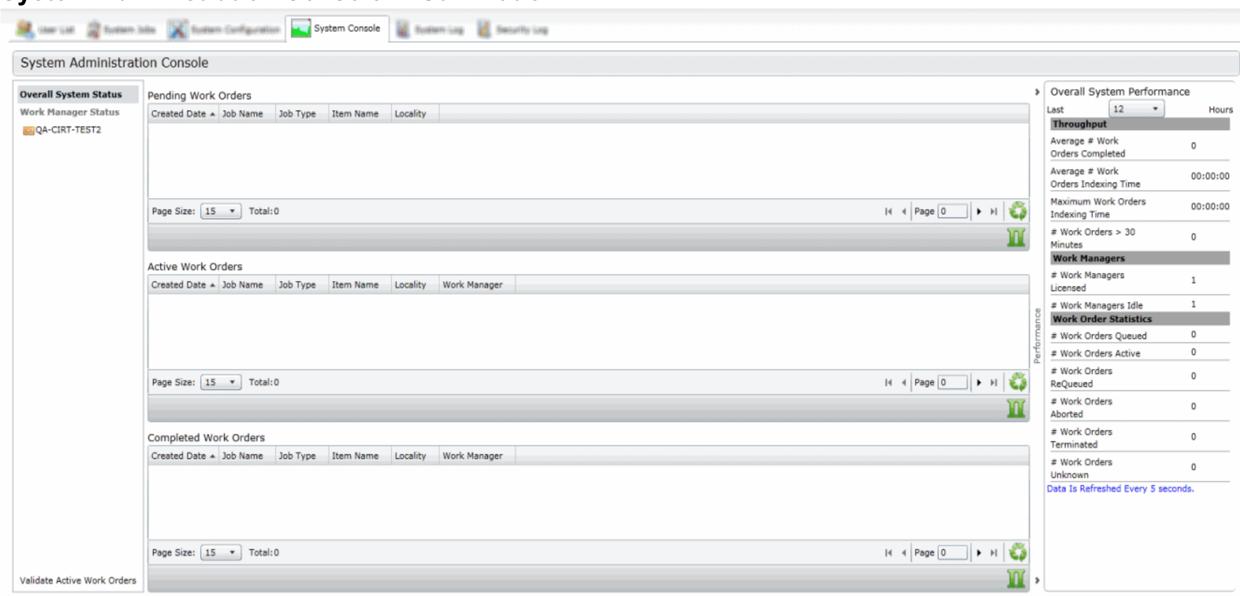
By default, when you add evidence to a case, the files are indexed so that the content of the files can be searched. You can select a *No Search* processing mode, which is much faster, but does not index the evidence.

4 Using the System Console and Logs

4.1 System Console Tab

The *System Console* tab, on the *Management* page, allows administrators to monitor the performance of the *Distribution Server* and the *Work Managers*. The following figures display a sample of each screen available. You can click on any work manager node by name to view specific server details.

System Administration Console in Summation



As a Summation administrator, you can use the *System Administration Console* to view pending, active, or completed work orders. You can also view the performance of the entire system or specific Work Managers.

Elements of the System Console Tab

Element	Description
Overall System Status Pane	Select to either view the performance of the entire system or specific Work Managers.
Pending Work Orders	Displays pending work orders.
Active Work Orders	Displays active work orders.
Completed Work Orders	Displays completed work orders.
Overall System Performance	You can access the *Overall System Performance* panel by expanding the *Performance* pane on the right side of the page. On the *Overall System Performance* panel, the displayed time range indicates the time frame in which the status information was collected.

See Validating Activate Work Orders on page 54.
See Viewing the System Log or Security Log on page 59.
See Configuring a Work Manager on page 54.

4.2 Using the System Administration Console

In the **System Administration Console** page, the Administrator can monitor the performance of the **Distribution Server** and the **Work Managers**. You can click on any work manager node by name to view specific server details.

As an administrator, you can use the *System Administration Console* to view pending, active, or completed work orders. You can also view the performance of the entire system or specific Work Managers.

4.2.1 Opening the System Administration Console

To open the System Administration Console page

1. Log in as an administrator.
   See Opening the Summation Console (page 9).
2. Click **Management**.
3. Click **System Console**.

4.2.2 Validating Activate Work Orders

You can use **Validate Active Work Orders** to remove orphaned work orders from the Active Work Orders table. Work orders can become orphaned when the work manager handling the work order shuts down, or in some way loses contact with the Distribution server. When this happens, however, it does not change the status of the associated job in the Jobs list.

See Using the System Console and Logs (page 52)

To validate active work orders

1. In *System Administration Console*, click a work manager name to view active work orders.
2. In the left pane, at the bottom, click **Validate Active Work Orders** to confirm and update current work orders and their status.

4.2.3 Configuring a Work Manager

You can configure a selected Work Manager by setting various property values.

See Using the System Console and Logs (page 52).

To configure a Work Manager

1. Open the *System Administration Console*.
   See Opening the System Administration Console (page 54).

2. In the *System Administration Console*, in the left pane, under *Overall System Status,* click a work manager name.
3. In the right pane, click the **Configuration** tab.
4. In the *Configuration* pane, click (edit).
5. When completed, click **OK**.

4.3 Using the System Log and Security Log

4.3.1 About the System Log

When certain internal events occur in the system, it is recorded in the system log. This can be used in conjunction with the security log to monitor the work and status of your system.

The following are examples of the types of events that are recorded:

- Completion of evidence processing for an individual case
- Exports started and finished
- Starting of internal services
- Job failures
- System errors
- Errors accessing computers and shares

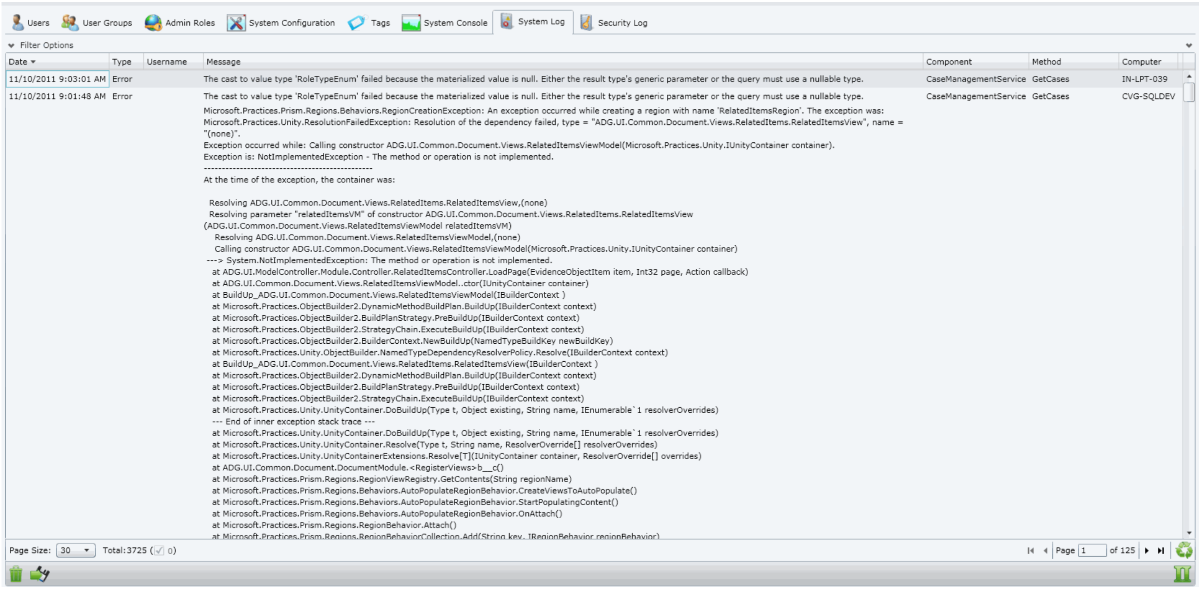
You can filter the log information that is displayed based on the following different types of criteria:

- Date and time of the log message
- Log type such as an error, information, or warning
- Log message contents
- Which component caused the log entry
- Which method caused the log entry
- Username
- Computer name

4.3.2 System Log Tab

The *System Log* tab on the *Management* page is only accessible to the Summation administrator. This log maintains an historical record of the events that take place in the Summation software. The Summation administrator can view, clear, and export the log file.

System Log Tab



Elements of the System Log Tab

Element	Description
Filter Options	Allows you to filter the items in the system log. See Filtering Content in Lists and Grids on page 16.
System Log	Displays all the events. Click the column headers to sort by the column.
Clear Log 	Click to delete all the events in the log. See Clearing the Log on page 59.
Export Log 	Click to export the log. It is recommended that you export and save logs before you clear them. See Exporting the Log on page 59.

4.3.3 About the Security Log

When certain internal activities occur in the system, it is recorded in the Security log. This can be used in conjunction with the system log to monitor the work and status of your system.

See About the System Log on page 56.

The following are examples of the types of activities that are recorded:

- A user logged out
- A user is forced to log out due to inactivity

You can filter the log information that is displayed based on the following different types of criteria:

- Activity
- Activity Date
- Username

4.3.4 Security Log Tab

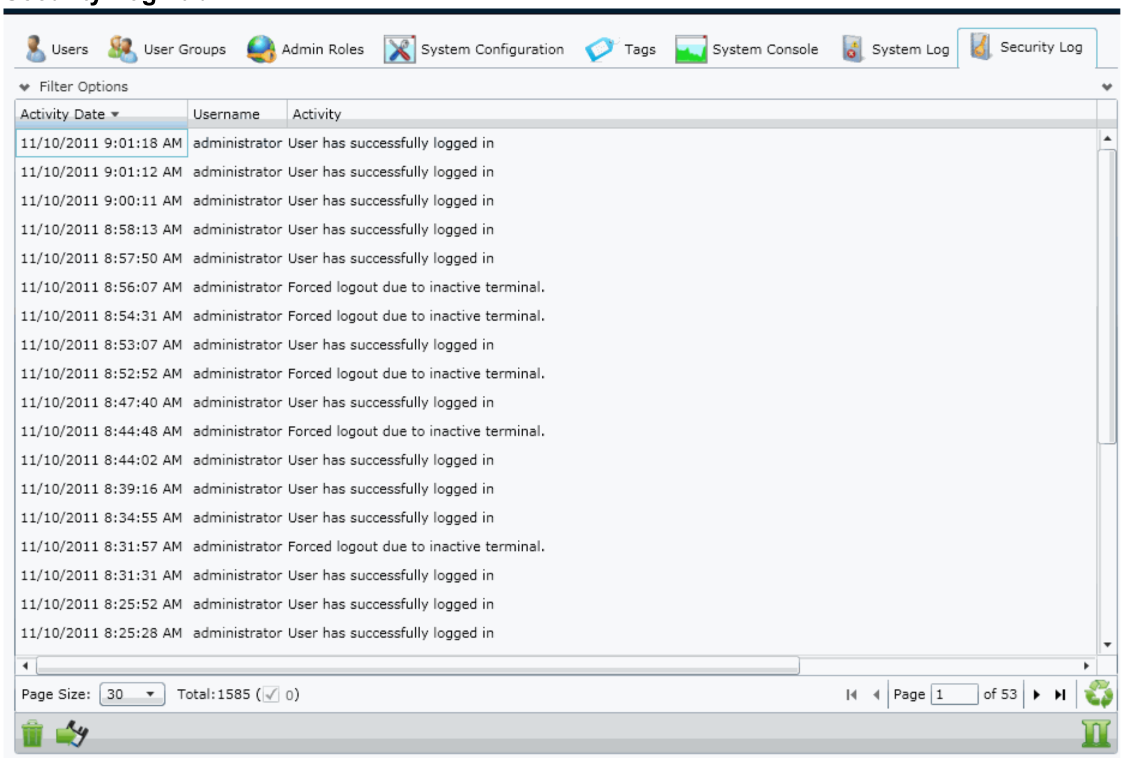
The *Security Log* tab on the *Management* page tracks the log in and log out attempts by administrators and users of Summation.

The *Security Log* can help you detect and investigate attempted and successful unauthorized activity in Summation and to troubleshoot problems.

The *Security Log* event columns include the activity date, username, activity message, and user ID.

Only an administrator can view, clear, and export the *Security Log* file.

Security Log Tab



Elements of the Security Log Tab

Element	Description
Filter Options	Allows you to filter the items in the security log. See Filtering Content in Lists and Grids on page 16.
Security Log	Displays all the events. Click the column headers to sort by the column.
Clear Log	Click to delete all the events in the log.
Export Log	Click to export the log. It is recommended that you export and save logs before you clear them.

Elements of the Security Log Tab

Element	Description
Refresh	Refreshes security log. See Refreshing the Contents in List and Grids on page 14.
Columns	Click to adjust what columns display in the security log. See Sorting by Columns on page 15.

4.3.5 Viewing the System Log or Security Log

An administrator can view, clear, and export the log file.

When you view the list of events, they are displayed in a grid. You can do the following to modify the contents of the grid:

- Control which columns of data are displayed in the grid.
- If you have a large list, you can apply a filter to display only the items you want.

To open the Log page

1. Log in as an administrator.
2. Click **Management**.
3. Click **System Log** or **Security Log**.
4. To refresh the log view, click (refresh).

4.3.6 Clearing the Log

An administrator can clear the log. When you clear the log, you delete all log entries across all pages. A new entry is creating stating that the log was cleared and the user who cleared it. Before you clear the log, you may want to consider exporting the log file to keep a historical record.

To clear the log

1. Open the *Logs* page.
2. In the bottom left corner, click **Clear Log**.
3. Click **Yes** to confirm the deletion.

4.3.7 Exporting the Log

Exporting the log lets you maintain a historical record of events in the software and is useful if you intend to clear the log. Only an administrator can view, clear, and export the log file. You can export the log to a CSV file to give others, who may not have view log access, the ability to query and access the saved events.

To export the log

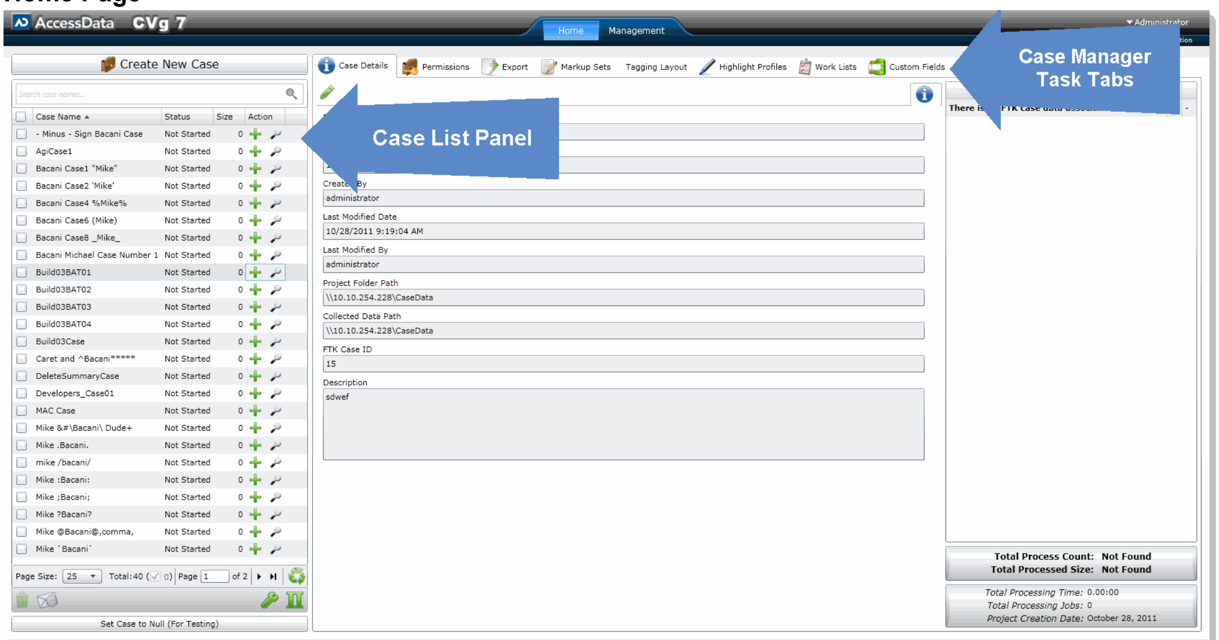
1. Open the *Logs* page.
   See Security Log Tab (page 58).
2. In the bottom left corner of the **View Log** pane, click **Export Log**.
3. In the **Save As** dialog box, specify a file name and file location.
4. Click **Save**.

1 Introduction

This guide is designed to help case managers perform common tasks. Case manager tasks are performed on the Home page and in Case Review. Case managers can perform their tasks as long as the administrator has granted the case manager the correct permission. See the Administrators guide for more information on how administrators can grant global permissions.

1.1 Introducing the Home Page

Home Page



Elements of the Home Page

Elements	Description
Case List Panel	See The Case List Panel on page 10.
Case Details	See Viewing Details About the Case on page 15.
Permissions	See Setting Case Permissions on page 17.
Export	See the Export documentation.
Markup Sets	See Configuring Markup Sets on page 31.
Evidence	See Evidence Tab on page 29.
Custodians	See Custodians Tab on page 24.

Elements of the Home Page (Continued)

Elements	Description
Tagging Layout	See Tagging Layout Tab on page 38.
Highlight Profiles	See Highlight Profiles Tab on page 43.
Work List	See Work List Tab on page 48.
Custom Fields	See Custom Fields Tab on page 35.
Processing Options	See the Admin Guide for more information.

1.1.1 The Case List Panel

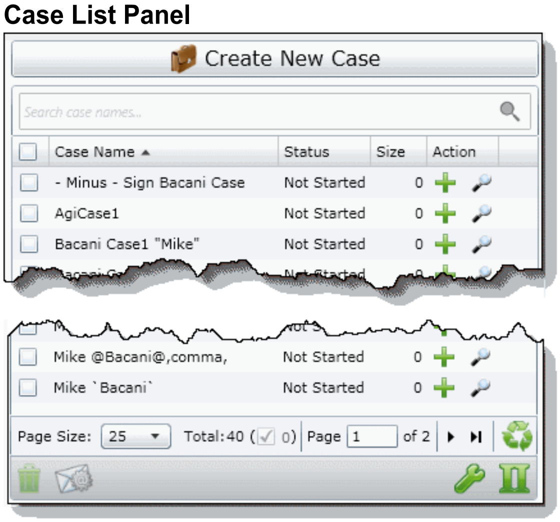
The *Home* page includes the *Case List* panel. The *Case List* panel is the default view after logging in. Users can only view the cases for which they have been given permissions.

Administrators and users, given the correct permissions, can use the case list to do the following:

- Create cases. See Creating a Case on page 14.
- View a list of existing cases.
- Add evidence to a case. See the Loading Data documentation.
- Launch Case Review.

If you are not an administrator, you will only see either the cases that you created or cases you were granted permissions to.

Case List Panel



The following table lists the elements of the case list. Some items may not be visible depending on the permissions that you have.

Elements of the Case List

Element	Description
Create New Case	Click to create a new case.
Search Bar	If there are a large number of cases in the list, you can use the search bar to narrow the list. Type a text string and any cases that have that text in the name will be displayed. Click the X to clear the search results.
Case Name Column	Lists the names of all the cases that the logged-in user has permissions to.
Status Column	Lists the status of the cases: Not Started - The case has been created but no evidence has been imported. Processing - Evidence has been imported and is still being processed. Completed - Evidence has been imported and processed. See Refresh below.
Size Column	Lists the size of the data within the case.
Action Column	Lets you add evidence to a case or enter Case Review.
Add Data	Lets you add data to the selected case.
Case Review	Lets you review the case using Case Review. See the Reviewers Guide for more information.
Page Size Drop-down	Lets you select how many cases to display in the list. The total number of cases that you have permissions to see is displayed.
Total	Lists the total number of cases displayed in the Case List.
Page	Lets you view another page of cases.
Refresh	If you create a new case, or make changes to the list, you may need to refresh the case list
Custom Properties	Add, edit, and delete custom columns with the default value that will be listed in the Case list panel. When you create a case, this additional column will be listed in the case creation dialog.
Columns	Add, or remove viewable columns in the Case List.
Delete	Highlight case and then click the **Delete Case** button to delete it from the Case List.

1.2 About Cases

When you want to assess a set of evidence, you create a case and then add evidence to the case. When evidence is added to the case, the data is processed so that it can be later reviewed, coded, and labeled by a team of reviewers using the Case Review interface.

1.2.1 Workflow for Case Managers

Administrators, or users that have been given rights to manage cases, use the *Home* page of the console to create and manage cases by doing the following tasks.

Basic Workflow for Case Managers

Task	Link to the tasks
Create a case	See Creating a Case on page 14.
Configure the user/group permissions for a case	See Setting Case Permissions on page 17.
Loading Data	You can load data using import or by processing the evidence into the system. See the Loading Data documentation for more information.
Manage evidence and custodians	See Managing Custodians on page 24.
Configure the review tools to be used in case review	See Configuring Markup Sets on page 31. See Creating Category Values on page 37. See Configuring Custom Fields on page 35. See Configuring Highlight Profiles on page 43. See Configuring Tagging Layouts on page 38. See Managing Review Sets on page 56. See Managing Tags on page 61.
View details about the case	See Viewing Details About the Case on page 15.
Manage cases: Back-up, archive, detach/ attach, restore, and delete cases and evidence	See the Summation Best Practices Guide.
Monitor the Work List	See Work List Tab on page 48. See Monitoring the Work List on page 48.
Manage Document Groups	See Managing Document Groups on page 50.
Upload Transcripts/Exhibits	See Managing Transcripts and Exhibits on page 53.
Create Production Sets	See the Exporting documentation.
Export the selected evidence	See the Exporting documentation.

1.3 Viewing the Case List

Administrators, and users given permissions, use the case list to do the following:

- Create cases
- View a list of existing cases
- Add evidence to a case
- Launch Case Review

If you are not an administrator, you will only see either the cases that you created or cases you were granted permissions to.

To view the case list

1. Log in to the Summation console.
2. In the Summation console, click **Home**.
   The Case List Panel is on the left-side of the page.

See The Case List Panel on page 10.

Administrators, and users with the Create/Edit Cases permission, create cases to add and process evidence.

See About Cases on page 12.

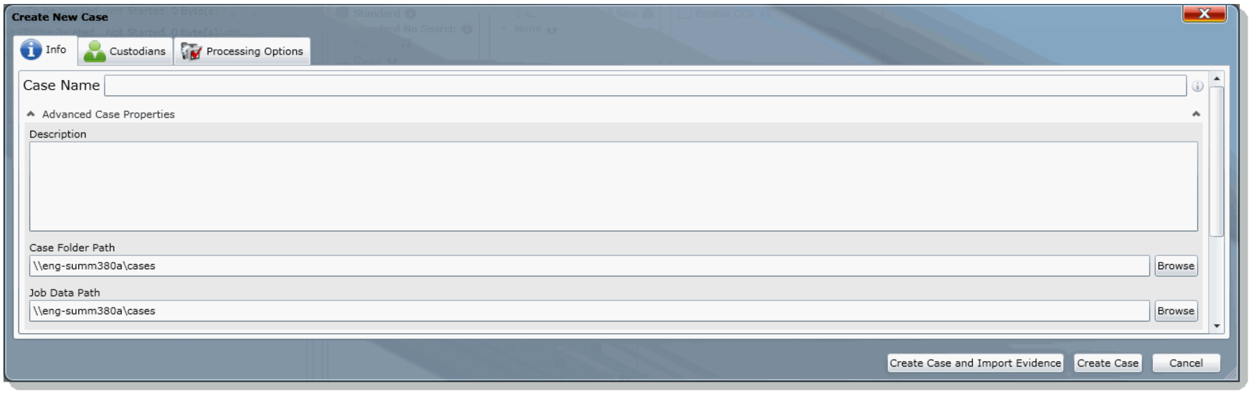
2 Creating a Case

Administrators and case managers with the Create Case admin role can create cases from the Case List panel.

To create a new case

1. Log in as an administrator or as a user that has permissions to create cases.
2. Click **Create New Case**.

Create New Case Info Tab



3. Enter a *Case Name* and a *Description*.

Note: Case Names must be only alphanumeric characters. Special characters will cause the case creating to fail.

4. Enter the *Case Folder Path* and the *Job Data Path*.

Note: This setting may have a default value that you can use or change, or this setting may be configured and hidden by the administrator. See the Admin Guide for information on configuring case defaults.

Paths

Case Folder Path	Lets you specify a local path or a UNC network path to the case folder. This path is the location where all non-Oracle case data is stored.
Job Data Path	The responsive folder path is the location of reports data.

5. (Optional) Click the **Custodians** tab to add custodians to the case.
   This is where you configure the custodians of the evidence of this case.
   Custodians for the case can be configured later, but should be done before processing evidence.
   See Setting Case Permissions on page 17.

6. Click the **Processing Options** tab to set the processing options for the case.

   This is where you set the options for how the evidence is processed when it is added to the case.

   This setting may have a default value that you can use or change, or this setting may be configured and hidden by the administrator.

   See the Admin Guide for more information on setting default processing options.

   Note: You cannot change the processing options after you have created the case.

7. Select one of the following options:
   - **Create Case**: Click to create the case without importing evidence. This option will create the case and return you to the Case Management page. You can then configure the case by adding evidence, assigning permissions, and so on.
   - **Create Case and Import Evidence**: Click to create the case and begin importing evidence. See the Loading Data documentation for information on how to import evidence.

2.1 Viewing Details About the Case

You can view the following details about the case on the *Case Details* tab:

- Case Name
- Creation and modification date and time
- Case creator
- Person who last modified the case
- Paths
- Case ID
- Case description (editable)
- Listing of evidence statistics:
  - Counts and sizes of files
  - Processing statistics

To access the Case Details tab

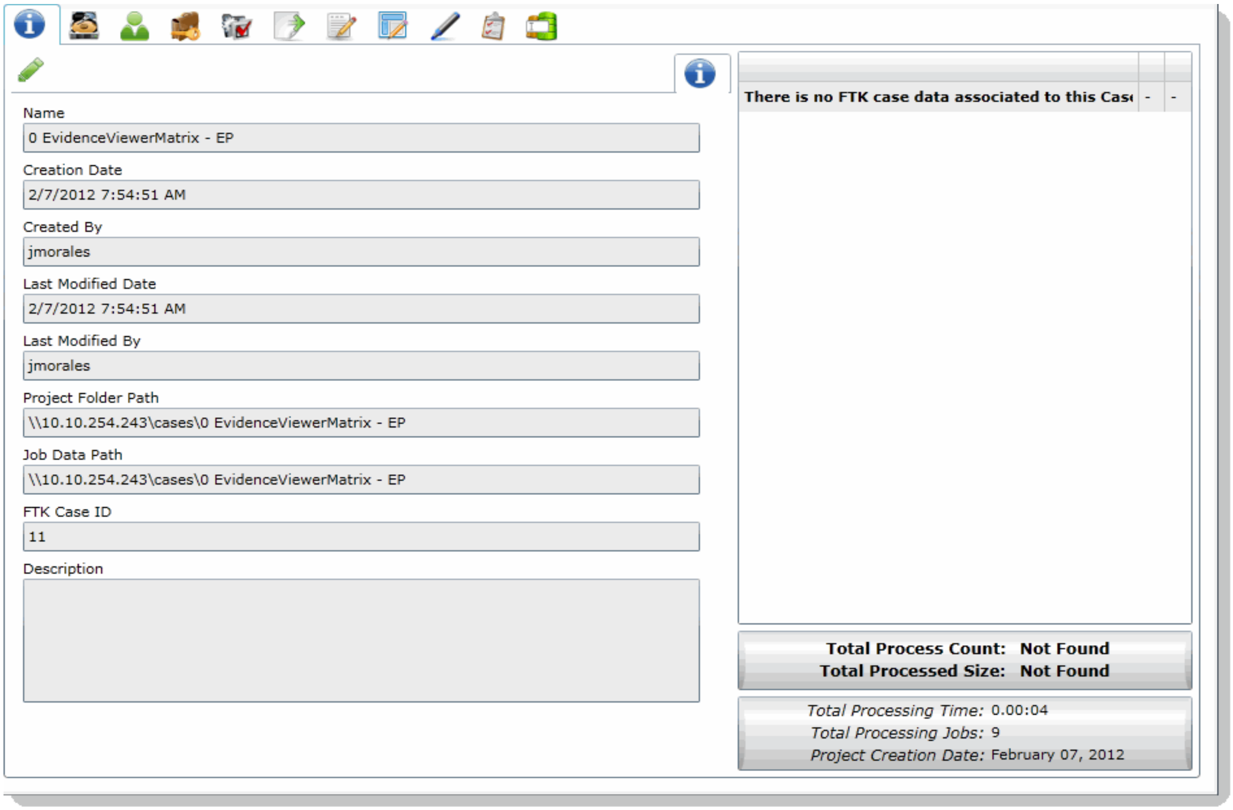
- ❖ From the *Home* page, select a case, and click the **Case Details** tab.

See Case Details Tab on page 15.

2.1.1 Case Details Tab

The *Case Details* tab displays data for the selected case. You can also edit some of the case data from this tab.

Case Info Tab



Elements of the Case Information Tab

Element	Description
Edit Button 	Click the edit button to edit information about the selected case. Only the *Name*, *Collected Data Path*, and the *Description* can be edited.
Name	Displays the name of the case.
Creation Date	Displays the date that the case was created.
Created By	Displays the user who created the case.
Last Modified Date	Displays the date when the case was last modified.
Last Modified By	Displays the user who last modified the case.
Project Folder Path	Displays the path where the case folder is stored.
Job Data Path	Displays the path where collected data is stored.
FTK Case ID	Displays the case ID for the associated FTK case if applicable.
Description	Displays any description that was given to the case.
Associated FTK Case Pane	Displays any associated FTK cases.

3 Setting Case Permissions

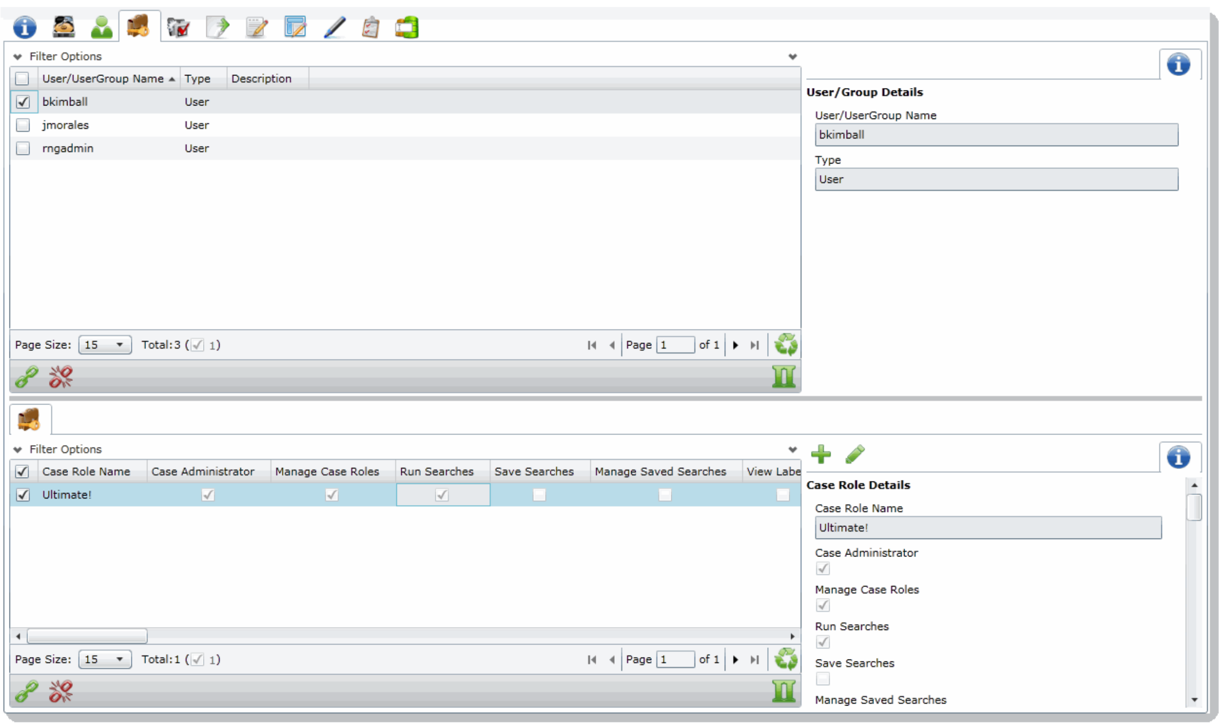
Administrators and case managers with the necessary permissions can manage permissions for users of a case using the *Permissions* tab on the *Home* page.

The *Permissions* tab is case specific, not global. For information on how to manage global permissions, see the Admin Guide.

3.1 Permissions Tab

The *Permissions* tab on the *Home* page is used to assign users or groups permissions within the case.

Permissions Tab



Elements of the Permissions Tab

Element	Permission
Filter Options	Allows the user to filter users in the list.
Users/Group List	Displays the users and groups associated with the case. Click the column headers to sort by the column.

Elements of the Permissions Tab (Continued)

Element	Permission
Refresh	Refreshes User/Group List.
Columns	Click to adjust what columns display in the User/Group List.
Add Association	Click to add either a group/user to a role or a role to a group/user.
Remove Association	Click to disassociate a group/user from a role or disassociate a role from a group/user.
User/Group Details Pane	Displays the details for the selected user or group.
Case Roles Tab	Displays the available roles for the case.
Add Role	Click to add a role. Specify the permissions of the role in this data form.
Edit Role	Click to edit the selected role.

To access the Permissions tab

❖ From the *Home* page, select a case, and click the **Permissions** tab.

To apply permissions to a user or group, you must create a case role. You can then associate that case role to a user or group on the Permissions tab.

See Creating a Case Role on page 21.

See Associating Users and Groups to a Case on page 22.

See Case-level Permissions on page 19.

3.2 Case-level Permissions

Administrators, and users with Create/Edit Cases rights, can assign users specific permissions to an individual case. These are permissions that are given to individuals working on a specific case.

When you assign any of the custom permissions, the View Case permission is also assigned. In the case list, users will only see cases that they have permissions to.

The following table describes the available case permissions on the *Permissions* tab.

Case-level Permissions

Permission	Description
Case Administrator	● Can Manage Case Roles. ● Can assign access permissions to users & groups. ● Has all case level functional permissions listed below. ● Can import/export. ● Can see job list for jobs created for his case.
Manage Case Roles	Can assign access permissions to users & groups.
Run Searches	Can run searches in the Case Review. **Note:** User must have this permission to perform other search functions as well.
Save Searches	Can save searches that the user performs themselves.
Manage Saved Searches	Can share your saved searches with other groups.
View Labels	Can view the labels everywhere that labels appear.
Create Labels	Can create and edit labels in the Case Explorer in Case Review. **Note:** Must have View Labels permission as well to create and delete labels.
Delete Labels	Can delete labels in Case Review.
Assign to Labels	Can label documents.
Manage Labels	Can grant permissions to labels
View Review Sets	Can view the review sets in the Case Explorer and Review Batches panel in the Case Review.
Create Review Sets	Can create review sets.
Delete Review Sets	Can delete review sets in Case Review.
Manage Review Sets	Can assign review sets to users/groups.
View Native	Can view the Native panel in Case Review.
View Text	Can view the Text panel in Case Review.
View Coding Layout	Can view the Coding panel in Case Review.
Edit Document	Can change data for documents using tagging layouts.
View Categories	Can view categories in Case Review.

Case-level Permissions (Continued)

Permission	Description
Assign Categories	Can assign a document to a category.
Create Categories	Can create or edit categories in Case Review.
Delete Categories	Can delete categories in Case Review.
Manage Categories	Can assign permissions for categories and category values.
View Issues	Can view issues in Case Review.
Assign Issues	Can assign issues to a document.
Create Issues	Can create and edit issues in Case Review.
Delete Issues	Can delete issues in Case Review.
Manage Issues	Can assign permissions for issue values.
View Notes	Can view notes everywhere that they appear in Case Review.
Add Notes	Can add notes in Case Review.
Delete Notes	Can delete notes in Case Review.
View Annotations	Can view annotations in Image, Natural, and Transcript panels in Case Review.
Add Annotations	Can add annotations in Case Review.
Delete Annotations	Can delete annotations in Case Review.
View Activity History	Can view Activity panel in Case Review.
Create Production Set	Can create production sets in Case Review.
Delete Production Set	Can delete production sets in Case Review.
Manage Production Set	Can edit and assign permissions for production sets.
Delete Summaries	Can delete document records that were loaded using Import. See the Loading Data documentation for more information.
Imaging	Can perform the imaging mass action in the Item List panel and can create an image using the Annotate option in the Natural panel.
Create Transcript Group	Can create a transcript group in Case Review.
Upload Transcripts	Can upload transcripts in Case Review.
Upload Exhibits	Can upload exhibits in Case Review.
Manage Transcripts	Can assign permissions to Transcript Groups.

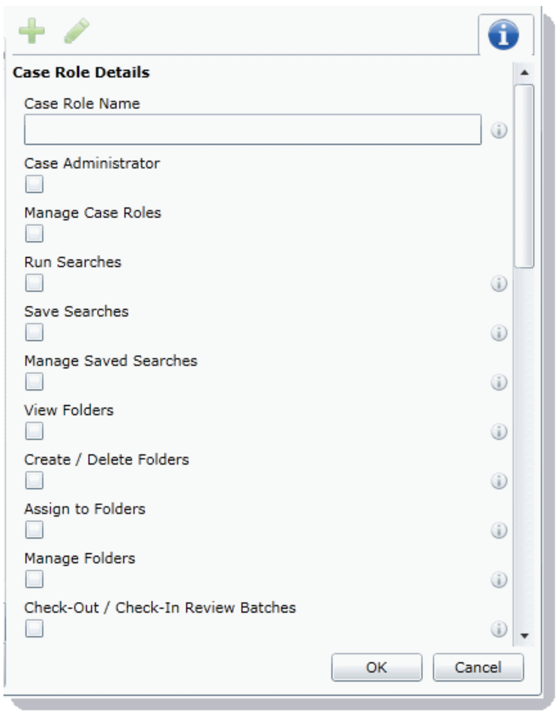
3.3 Creating a Case Role

Before you can apply permissions to a user or group, you must set up case roles. A case role is a set of permissions that you can associate to multiple users or groups. Creating a case roll simplifies the process of assigning permissions to users who perform the same tasks.

To create a case role

1. On the *Home* page, select a case, and click the **Permissions** tab.
2. In the *Case Roles* pane at the bottom of the screen, click the add button .

Add Case Roles Data Form



3. Enter a *Case Role Name*.
4. Check the permissions that you want to include in the role.
   See Case-level Permissions on page 19.
5. Click **OK**.

3.3.1 Editing a Case Role

You can edit case roles if you want to alter the permissions in the role.

To edit a case role

1. On the *Home* page, select a case, and click the **Permissions** tab.
2. In the *Case Roles* pane at the bottom of the screen, click the add button .
3. Edit the permissions in the data form and click **OK**.

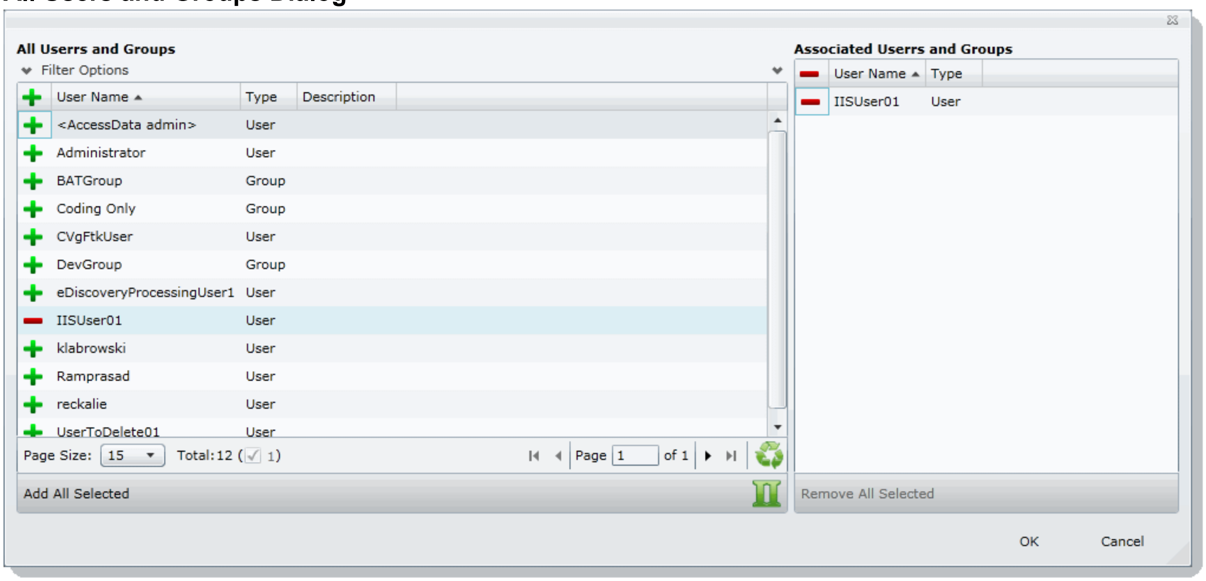
3.4 Associating Users and Groups to a Case

Before you can apply a case role to a user or group, you must first associate the user or group to the case. Administrators and case managers with the correct permissions can associate users and groups to a case in the *Permissions* tab. Once a user or group is added to a case, the user can see and access the case in the *Case List* panel.

To associate a user or group to a case

1. On the *Home* page, select a case, and click the **Permissions** tab.
2. In the User/Group list pane, click the **Add Association** button .

All Users and Groups Dialog



3. Click the plus sign to add the user or group to the case.
4. Click **OK**.

3.4.1 Disassociate Users and Groups from a Case

Administrators and case managers with the correct permissions can remove users from a case by disassociating them from the case in the Permissions tab.

To disassociate a user or group to a case

1. On the *Home* page, select a case, and click the **Permissions** tab.
2. Check the user or group you want to remove from the case in the User/Group list pane.
3. In the User/Group list pane, click the **Remove Association** button .

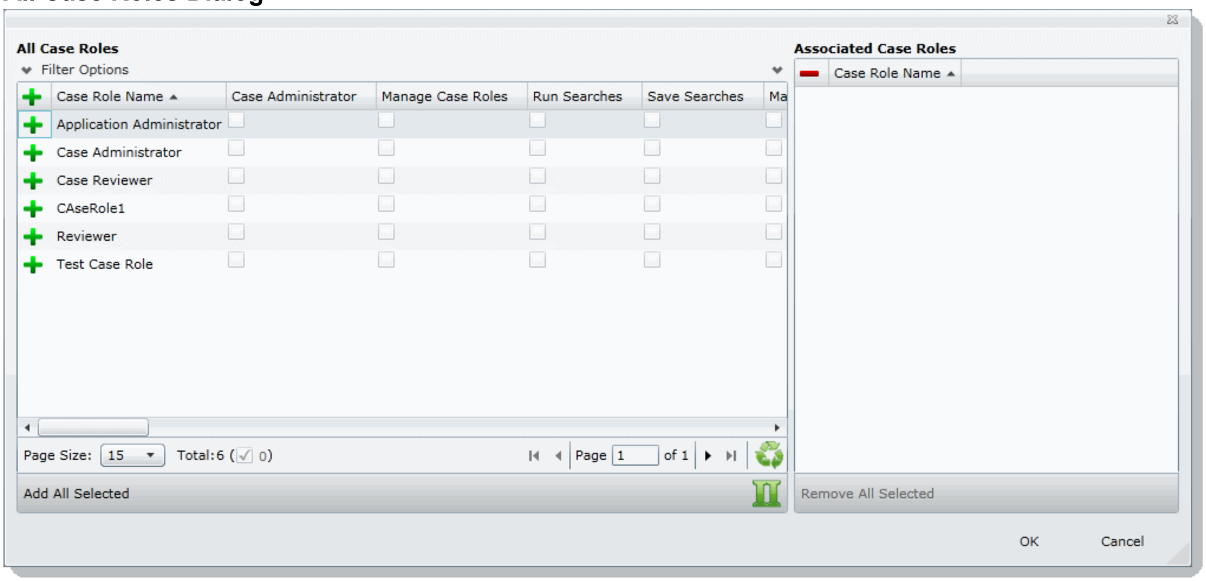
3.5 Associating Case Roles to Users and Groups

Administrators, and users with the Manage Case Permissions rights, can associate case roles to users and groups for a specific case.

To associate a case roll to a user or group

1. On the *Home* page, select a case, and click the **Permissions** tab, select users/groups that you want to set permissions for.
2. In the *Case Roles* pane, click the **Add Association** button .

All Case Roles Dialog



3. Click the plus sign to assign the case role to the user or group.
4. Click **OK**.

3.5.1 Disassociating Case Roles from Users or Groups

Administrators, and users with the Manage Case Permissions rights, can disassociate case roles from users and groups for a specific case.

To disassociate a case role to a user or group

1. On the *Home* page, select a case, and click the **Permissions** tab, select the users/groups that you want to set permissions for.
2. Check the users or groups that you want to disassociate in the Users/Groups list pane.
3. In the *Case Roles* pane, click the **Remove Association** button .

4 Managing Custodians

Administrators, and users with the Create/Edit Case permission, manage custodians for a case using the *Custodians* tab on the *Home* page.

For information on user permissions, see Setting Case Permissions (page 17).

The *Custodians* tab is case specific, not global.

Note: In order for custodians to be used in Case Review, custodians must be created and selected before you process the evidence.
See Evidence Tab on page 29.

4.1 Custodians Tab

Administrators, and users with the Create/Edit Case permission, manage custodians for a case using the *Custodians* tab on the *Home* page.

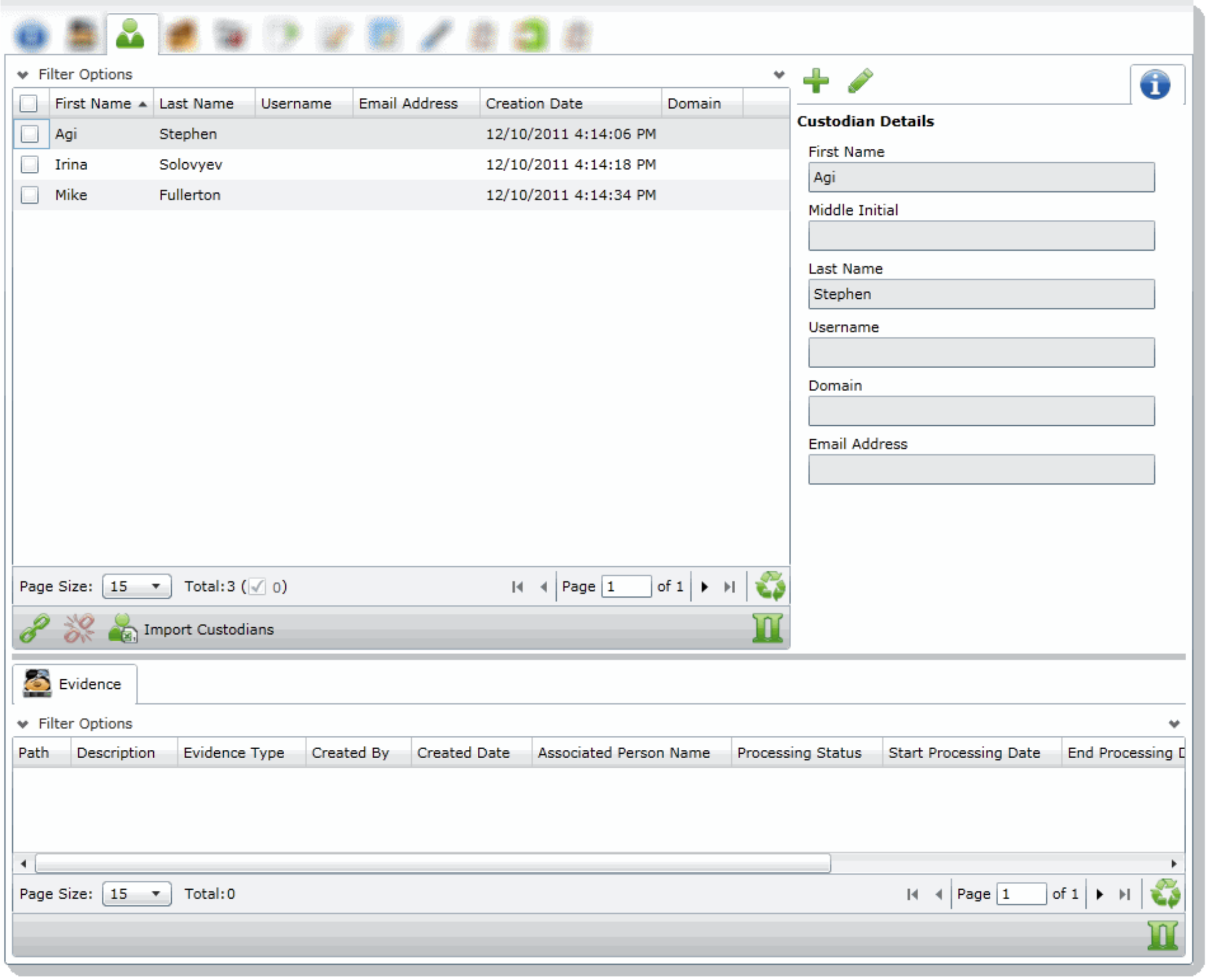
To manage custodians for a case

- From the *Home* page, select a case, and click the **Custodians** tab.

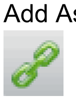
When you create and view the list of custodians, they are displayed in a grid. You can do the following to modify the contents of the grid:

- Control which columns of data are displayed in the grid.
- If you have a large list, you can apply a filter to display only the items you want.Custodians Tab.

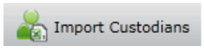
Custodians Tab



Elements of the Custodians Tab

Element	Description
Filter Options	Allows the user to filter the list.
Custodians List	Displays the custodians for the case. Click the column headers to sort by the column.
Refresh 	Refreshes Evidence Path List.
Columns 	Click to adjust what columns display in the Evidence Path List.
Add Association 	Click to associate existing custodians to the case.
Remove Association 	Click to disassociate an existing custodian from the case.

Elements of the Custodians Tab (Continued)

Element	Description
Import Custodians 	Click to import custodians from a file.
Add Custodian 	Click to add a custodian.
Edit Custodian 	Click to edit the selected custodian.
Evidence Tab	Lists the evidence associated with the selected custodian.

4.2 Adding a Custodian to a Case

Administrators, and users with the Create/Edit Case permission, can add custodians to a case.

You can add case-level custodians in the following ways:

- Adding case-level custodians from the Shared Custodians list
- Manually adding custodians
- Importing custodians from a file
  See Importing Custodians From a File on page 28.
- Creating or importing custodians while importing evidence
  See the Loading Data documentation for more information on creating custodians during import.

If you manually add or import custodians, they are added to the shared list of custodians.

To add a custodian from shared custodians

1. On the **Home > Custodians** tab, click **Add**.
   The *Associate Custodians to case* page opens.
2. Select the shared custodians that you want associated with the case.
   You can click a singe custodian or use Shift-click or Ctrl-click to select multiple custodians.
3. Click or **Add all Selected**.
   This moves the custodians to the *Associated Custodians* list.
   You can also check the selection box next to *First Name* to add all of the custodians.
4. You can remove custodians from the *Associated Custodians* list by selecting custodians and clicking or **Remove All Selected**.
   You can also clear the selection box next to *First Name* to remove all of the custodians.
5. Click **OK**.

You can also add case-level custodians from shared custodians using the *Custodians* tab when creating a case.

See Creating a Case on page 14.

4.2.1 Manually Creating Custodians for a Case

To manually create a case-level custodian

1. On the **Home > Custodians** tab, click (add).
2. In *Custodian Details*, enter the custodian details.
3. Click **OK**.

You can also manually create custodians from the Custodians tab when creating a case.

See Creating a Case on page 14.

4.2.2 Editing a Custodian

You can edit any custodian that you have added to the case.

To edit a case-level custodian

1. On the **Home > case > Custodians** tab, select a custodian that you want to edit.
2. Click (edit).
3. In *Custodian Details*, edit custodian details.
4. Click **OK**.

4.2.3 Removing a Custodian

You can remove one or more custodians from a case. This does not delete the custodian from the shared custodians, it just disassociates it from the case.

To remove one or more custodians from a case

1. On the **Home > Custodians** tab, select the check box for the custodians that you want to remove.
2. Below the custodian list, click **Remove**.

To confirm the deletion, click **OK**.

4.2.4 Importing Custodians From a File

You can import one or more custodians into a case from a file. Even though you perform this task at the case level, it will also add the custodians to the global custodians list.

The source file can be either in TXT or CSV format. The file must not contain any headers.

The custodian name can in the following format:

- First and last name separated by a space
  For example, John Smith or Bill Jones

For example, you can create a TXT or CSV file with the following text:

Chris Clark

Sarah Ashland

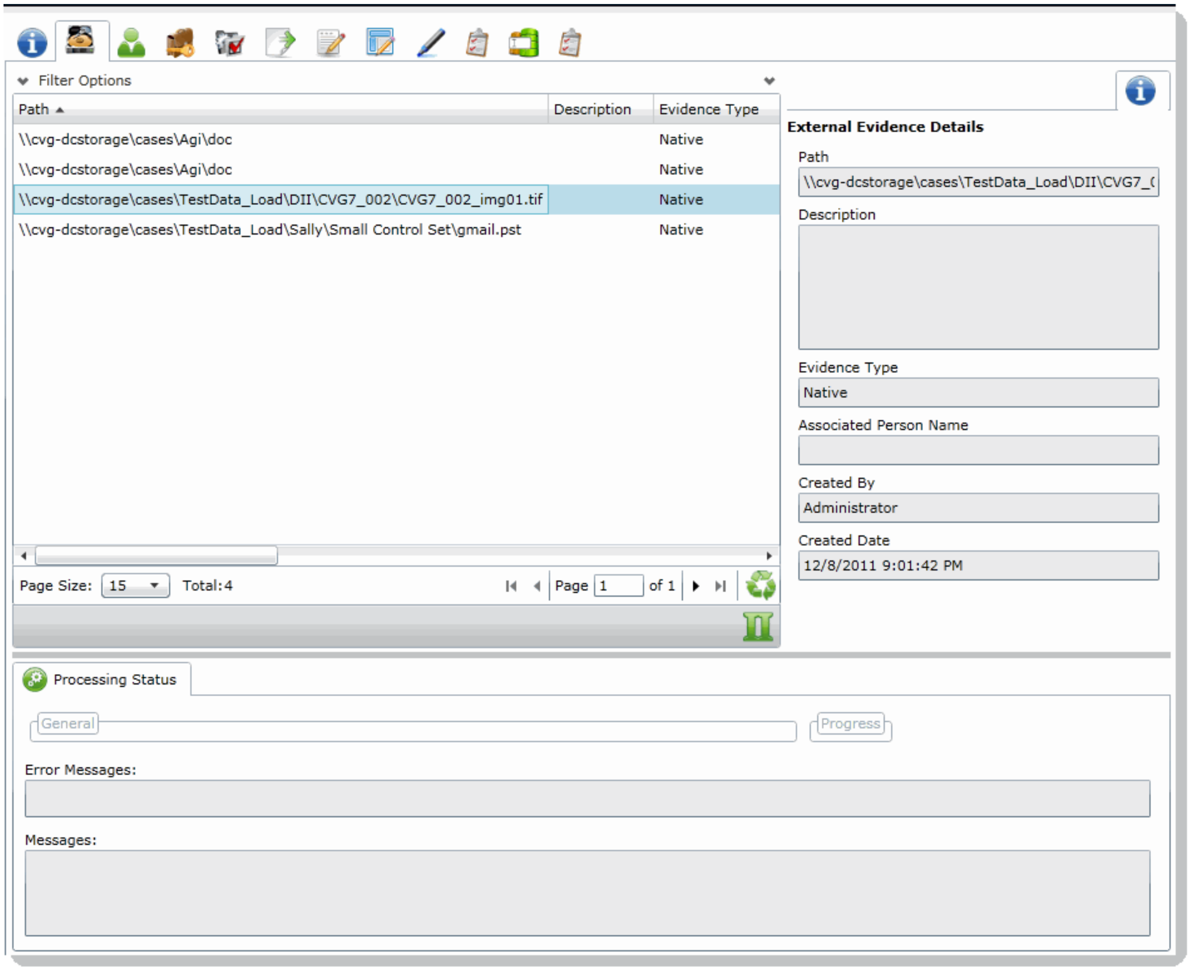
To import custodians from a file

1. On the **Home > Custodians** tab, click **Import Custodians from File**.
2. Browse to the TXT or CSV file.
3. Click **Open**.
4. When the import is complete, view the summary and click **OK**.

4.3 Evidence Tab

Users with permissions can view information about the evidence that has been added to a case. To view the *Evidence* tab, users need one of the following permissions: administrator, create/edit case, or manage evidence.

Evidence Tab



Elements of the Evidence Tab

Element	Description
Filter Options	Allows the user to filter the list.
Evidence Path List	Displays the paths of evidence in the case. Click the column headers to sort by the column.
Refresh 	Refreshes Evidence Path List.
Columns 	Click to adjust what columns display in the Evidence Path List.

Elements of the Evidence Tab (Continued)

Element	Description
External Evidence Details	Includes editable information about imported evidence. Information includes: ● That path from which the evidence was imported ● A description of the case, if you entered one ● The evidence file type ● What custodians were associated with the evidence ● Who added the evidence ● When the evidence was added
Processing Status	Lists any messages that occurred during processing.

4.3.1 About Associating a Custodian to an Evidence Item

You can use custodians to associate data to its owner.

You can associate a custodian to an evidence item in one of two ways, however, the results are different.

- Specify a custodian when importing an evidence item.

  This associates the custodian when the evidence is processed. You can then use custodian data when in Case Review and in exports.

  See Managing Custodians on page 24.

  See the Loading Data documentation for more information on creating custodians on import.

  When you associate a custodian to an evidence item, the custodian will be associated to all evidence in that item, whether the evidence item contains a single file or a folder of many files, messages, and so on.

- Edit an evidence item that has already been imported and associate a custodian.

  If you do this, the custodian association will not be visible or usable in Case Review nor in exports. You can only view this association in the *Evidence* and *Custodians* tabs of the *Home* page.

5 Configuring Review Tools

Case managers with the correct permissions can configure many of the review tools that case reviewers use in Case Review. See Setting Case Permissions (page 17) for information on the permissions needed to set up review tools. The following review tools can be set up from the Home page:

- Markup Sets: Configuring Markup Sets (page 31)
- Tagging Layouts: Creating Category Values (page 37)
- Highlight Profiles: See Configuring Highlight Profiles on page 43.
- Custom Fields: See Configuring Custom Fields on page 35.

5.1 Configuring Markup Sets

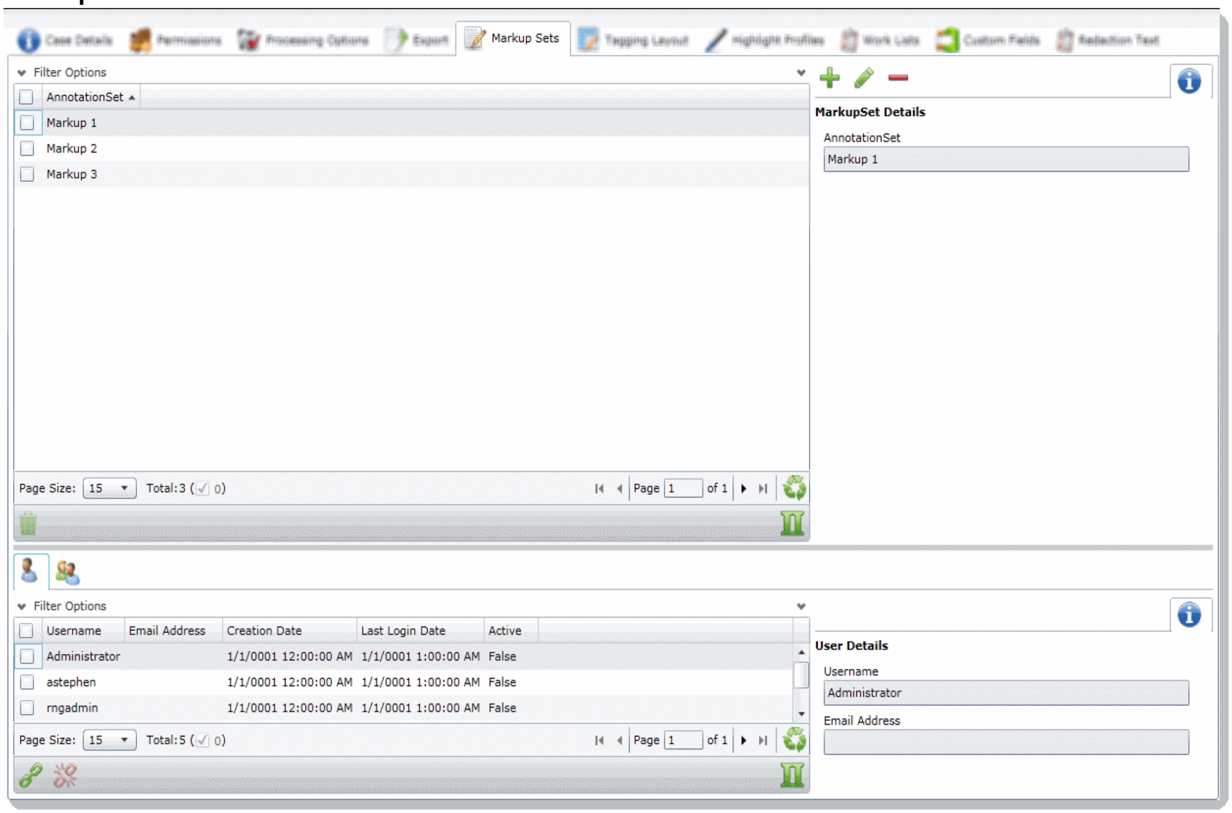
Markup sets are a set of redactions and annotations performed by a specified group of users. For example, you can create a markup set for paralegals, then when paralegal reviewers perform annotations on documents in the Case Review, all of their markups will only appear when Paralegal is selected as the markup for the document in the Natural or Image panel.

Note: Only redactions and annotations are included in markup sets.

5.1.1 Markup Sets Tab

The *Markup Sets* tab on the *Home* page can be used to create markup sets for reviewers to use. Markup sets are a set of redactions and highlights performed by a specified group of users.

Markup Sets Tab



Markup Sets Elements

Element	Description
Filter Options	Allows the user to filter markup sets in the list.
Markup Sets List	Displays the markup sets already created for the case. Click the column headers to sort by the column.
Refresh 	Refreshes the Markup Sets List.
Columns 	Click to adjust what columns display in the Markup Sets List.
Delete 	Click to delete selected markup set. Only active when a markup set is selected.
Add Markup Set 	Click to add a markup set.

Markup Sets Elements (Continued)

Element	Description
Edit Markup Set	Click to edit the selected markup set.
Delete Markup Set	Click to delete the selected markup set.
Users Tab	Use this tab to associate users to a markup set.
Groups Tab	Use this tab to associate groups to a markup set.
Add Association	Click to associate a group/user to a markup set.
Remove Association	Click disassociate a markup set from a user/group.

5.1.2 Adding a Markup Set

Before you can assign a markup set to a user or group, you must first create the markup set on the *Home* page. Case managers with the Case Administrator permission can create, edit, and delete markup sets.

To add a markup set

1. Log in as a user with Case Administrator rights.
2. Click on the **Markup Sets** tab.
   See Markup Sets Tab on page 32.
3. Click the **Add** button .
4. In the *Markup Set Detail* form, enter the name of the *Annotation Set*.
5. Click **OK**.

5.1.3 Deleting a Markup Set

To delete a markup set

1. Log in as a user with Case Administrator rights.
2. Click on the **Markup Sets** tab.
   See Markup Sets Tab on page 32.
3. Select the markup set that you want to delete.
4. Click the **Delete** button .
5. In the confirm deletion dialog, click **OK**.

5.1.4 Editing the Name of a Markup Set

You can edit the name of an existing markup set if you have Case Administrator rights.

To edit a markup set

1. Log in as a user with Case Administrator rights.
2. Click on the **Markup Sets** tab.
   See Markup Sets Tab on page 32.
3. Select the markup set that you want to edit.
4. Click the **Edit** button .
5. Change the name of the *Annotation Set*.
6. Click **OK**.

5.1.5 Associating a User or Group to a Markup Set

If you are a user with Case Administrator rights, you can associate users or groups to markup sets. Once associated, annotations that the user performs in the Case Review will appear on the document in Native or Image view when the markup set is selected.

To associate a user or group to a markup set

1. Log in as a user with Case Administrator rights.
2. Click on the **Markup Sets** tab.
   See Markup Sets Tab on page 32.
3. Select the markup set that you want to associate to a user or group.
4. Click the *User* or *Group* tab at the bottom of the page.
5. Click the **Add Association** button .
6. In the *All Users* or *All User Groups* dialog, click the plus sign to add the user or group to the markup set.
7. Click **OK**.

5.1.6 Disassociating a User or Group from a Markup Set

If you are a user with Case Administrator rights, you can disassociate users or groups to markup sets.

To disassociate a user or group from a markup set

1. Log in as a user with Case Administrator rights.
2. Click on the **Markup Sets** tab.
   See Markup Sets Tab on page 32.
3. Check the markup set that you want to disassociate to a user or group.
4. Click the *User* or *Group* tab at the bottom of the page.
5. Click the **Remove Association** button .

5.2 Configuring Custom Fields

Custom fields include the columns that appear in the Case Review and categories that can be coded in Case Review. You can create custom fields that will allow you to display the data that you want for each document in Case Review, in production sets, and in exports. Custom fields allow you to:

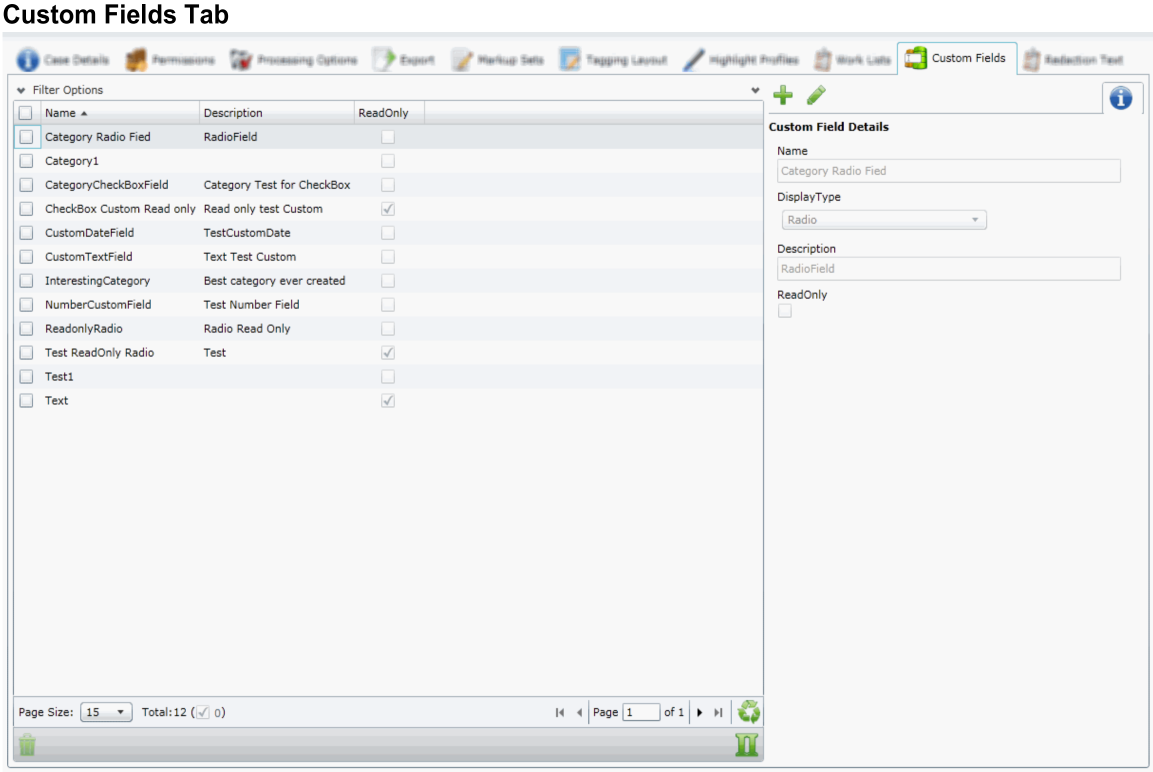
- Map fields from documents upon import to the custom fields you create. See the Loading Data documentation for more information on mapping fields.
- Code documents for the custom fields in Case Review, using tagging layouts. See the Reviewer Guide for more information on coding data.
  - See Adding Custom Fields on page 36.
  - See Creating Category Values on page 37.
  - See Adding a Tagging Layout on page 40.

Note: Once created, you cannot delete a custom field.

5.2.1 Custom Fields Tab

The *Custom Fields* tab on the *Home* page can be used to add and edit custom fields for Case Review and coding.

Custom Fields Tab



Elements of the Custom Fields Tab

Element	Description
Filter Options	Allows the user to filter custom fields in the list.
Highlight Custom Fields	Displays the custom fields already created for the case. Click the column headers to sort by the column.
Refresh	Refreshes Custom Fields List.
Columns	Click to adjust what columns display in the Custom Fields List.
Delete	Click to delete selected custom fields. Only active when a custom field is selected.
Add Custom Fields	Click to add a custom field.
Edit Custom Fields	Click to edit the selected custom field.

5.2.2 Adding Custom Fields

Case managers with the Case Administrator permission can create and edit custom fields. You can use the custom fields to add categories, text, number, and date fields.

To add a custom field

1. Log in as a user with Case Administrator rights.
2. Click on the **Custom Fields** tab.
   See Custom Fields Tab on page 35.
3. Click the **Add** button .
4. In the *Custom Field Detail* form, enter the name of the custom field.
5. Select a Display Type:
   - Check box: Create a column that contains a check box. This is for coding categories only.
   - Date: Create a column that contains a date.
   - Number: Create a column that contains a number.
   - Radio: Create a column that contains a radio button. This is for coding categories only.
   - Text: Create a column that contains text.
6. Enter a *Description* for the custom field.
7. Check **ReadOnly** to make the column un-editable.
8. Click **OK**.

5.2.3 Editing Custom Fields

Case managers with the Case Administrator permission can create and edit custom fields. You cannot edit the Display Type of the custom field.

To edit a custom field

1. Log in as a user with Case Administrator rights.
2. Click on the **Custom Fields** tab.
   See Custom Fields Tab on page 35.
3. Select the custom field you want to edit.
4. Click the **Edit** button.
5. Make your edits.
6. Click **OK**.

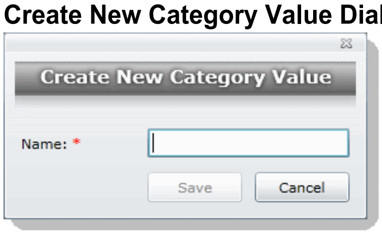
5.2.4 Creating Category Values

After you have created a Custom Field for check boxes or radio buttons, you can add values to the check boxes and radio buttons in *Case Review*. You can create multiple values for each category.

To add values to categories

1. Log in as a user with Assign Categories permissions.
2. Click the **Case Review**  button next to the case in the *Case List*.
3. In the *Case Explorer*, click the **Tags** tab.
4. Expand the *Categories*.
5. Right-click on the category and select **Create Category Value**.

Create New Category Value Dialog



6. Enter a *Name* for the value.
7. Click **Save**.

5.3 Configuring Tagging Layouts

Tagging Layouts are layouts used for coding in the Case Review that the case manager creates. Users must have Case Administration permissions to create, edit, delete, and associate tagging layouts. First, you must create the layout, then associate fields to the layout for the reviewer to code, and finally, associate users or groups to the layout so that they can code with it in Case Review.

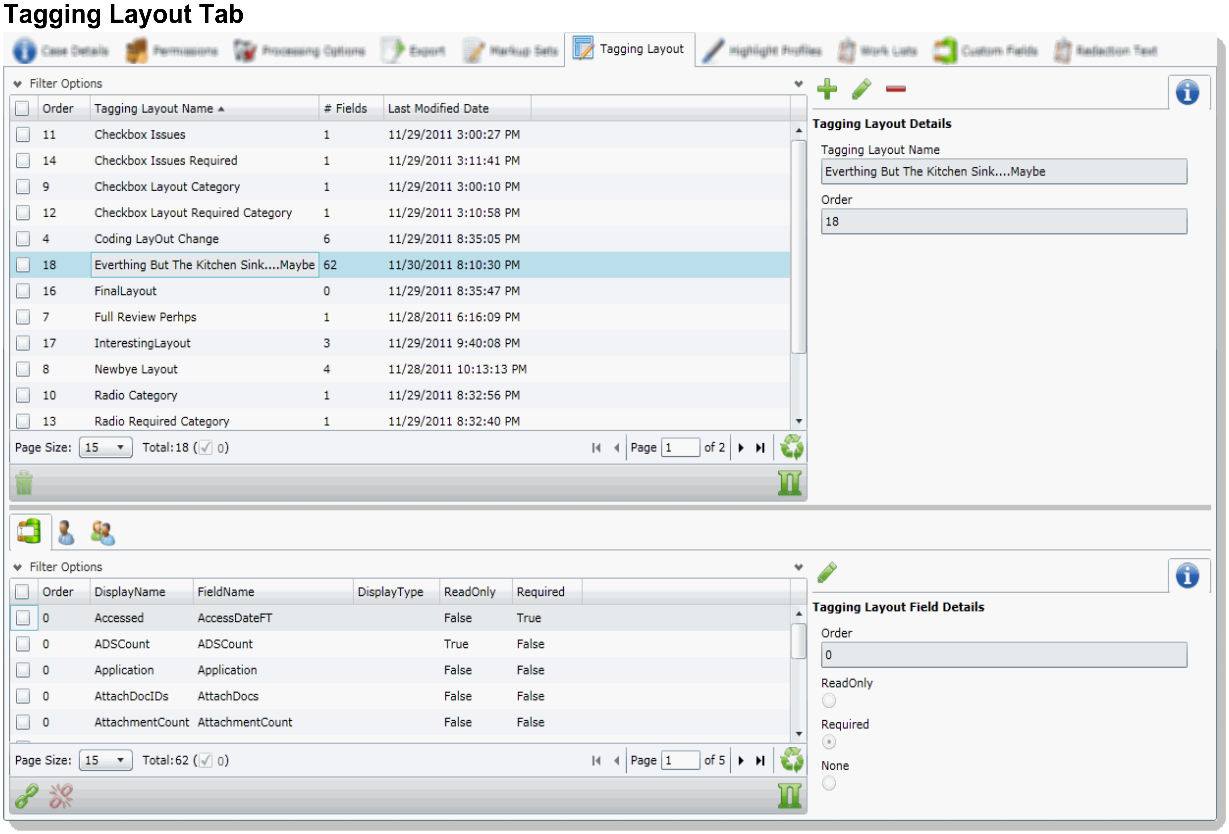
Custom fields must be created by the case manager before they can be added to a tagging layout. See Configuring Custom Fields (page 35) for information on how to create custom fields.

Tagging Layouts can be used to code fields in the Case Review for documents in the case. Coding is editing the data that appears in the fields for each document.

5.3.1 Tagging Layout Tab

The *Tagging Layout* tab on the *Home* page can be used to create layouts for coding in the *Case Review*.

Tagging Layout Tab



Elements of the Tagging Layout Tab

Element	Description
Filter Options	Allows the user to filter tagging layouts in the list.

Elements of the Tagging Layout Tab (Continued)

Element	Description
Tagging Layout List	Displays the tagging layouts already created for the case. Click the column headers to sort by the column.
Refresh	Refreshes Tagging Layout List.
Columns	Click to adjust what columns display in the Tagging Layout List.
Delete	Click to delete selected tagging layout. Only active when a tagging layout is selected.
Add Tagging Layout	Click to add a tagging layout.
Edit Tagging Layout	Click to edit the selected tagging layout.
Delete Tagging Layout	Click to delete the selected tagging layout.
Tagging Layout Fields Tab	Use this tab to associate/disassociate fields to a tagging layout.
Users Tab	Use this tab to associate users to a tagging layout.
Groups Tab	Use this tab to associate groups to a tagging layout.
Add Association	Click to associate a group, user, or field to a tagging layout.
Remove Association	Click to disassociate a tagging layout from a user, group, or field.

5.3.2 Adding a Tagging Layout

Case managers with the Case Administrator permission can create, edit, delete, and associate tagging layouts.

To add a tagging layout

1. Log in as a user with Case Administrator rights.
2. Click on the **Tagging Layout** tab.
   See Tagging Layout Tab on page 38.
3. Click the **Add** button .
4. In the *Tagging Layout Detail* form, enter the name of the *Tagging Layout*.
5. Enter the number of the order that you want the layout to appear to the user in the Case Review. Repeated numbers appear in alphabetical order.
6. Click **OK**.

5.3.3 Deleting a Tagging Layout

Case managers with the Case Administrator permission can create, edit, delete, and associate tagging layouts.

To delete a tagging layout

1. Log in as a user with Case Administrator rights.
2. Click on the **Tagging Layout** tab.
   See Tagging Layout Tab on page 38.
3. Check the layout that you want to delete.
4. Click the **Delete** button .

   Note: You can also delete multiple layouts by clicking the trash can delete button.

5. In the confirmation dialog, click **OK**.

5.3.4 Editing a Tagging Layout

Case managers with the Case Administrator permission can create, edit, delete, and associate tagging layouts.

To edit a tagging layout

1. Log in as a user with Case Administrator rights.
2. Click on the **Tagging Layout** tab.
   See Tagging Layout Tab on page 38.
3. Click the **Edit** button .
4. In the *Tagging Layout Detail* form, enter the name of the *Tagging Layout*.
5. Enter the number of the order that you want the layout to appear to the user in the Case Review. Repeated numbers appear in alphabetical order.
6. Click **OK**.

5.3.5 Associating Fields to a Tagging Layout

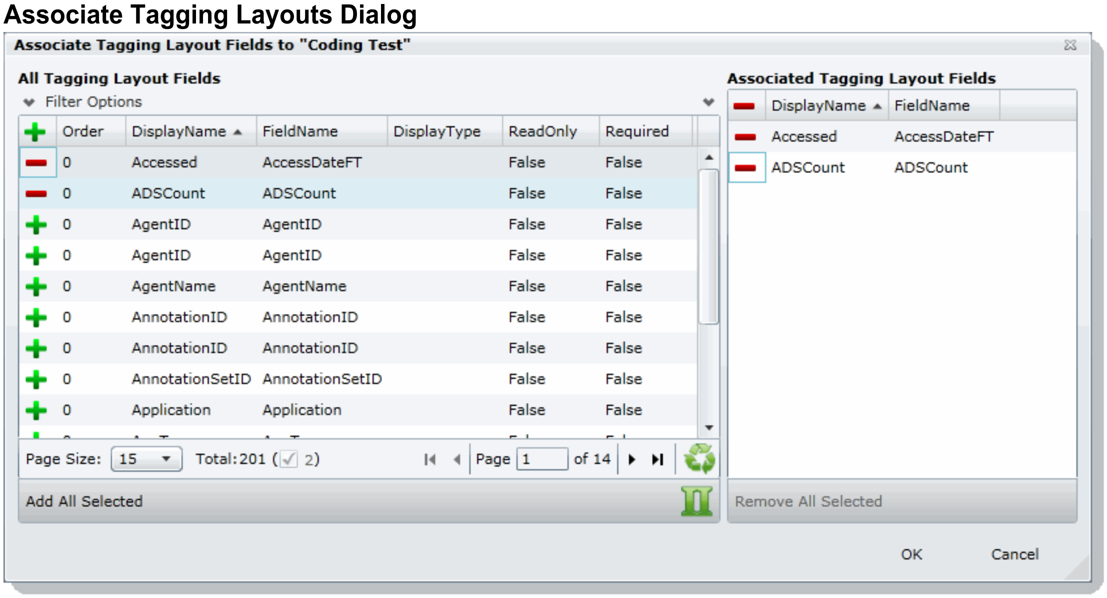
Case managers with the Case Administrator permission can create, edit, delete, and associate tagging layouts. Custom fields must be created before you can associate them with a tagging layout.

See Configuring Custom Fields on page 35.

To associate fields to a tagging layout

1. Log in as a user with Case Administrator rights.
2. Click on the **Tagging Layout** tab.
   See Tagging Layout Tab on page 38.
3. Select the layout that you want from the Tagging Layout list pane.
4. Select the fields tab in the lower pane  .
5. Click the **Add Association** button .

Associate Tagging Layouts Dialog



6. Click the plus sign to add the field to the layout.
7. Click **OK**.
8. Enter a number for the Order that you would like the fields to appear in the coding layout.
9. Check the fields that you just added (one at a time) and click the Edit button in the Tagging Layout Field Details. Select one of the following:
   - **Read Only**: Select to make the field read only and disallow edits. Any standard or custom field that is defined to be 'Read Only' cannot be redefined as a "Required" or "None."
   - **Required**: Select to make the field required to code before the reviewer can save the coding.
   - **None**: Select to have no definition on the field.
10. Click **OK**.

Note: Some fields are populated by processing evidence or are system fields and cannot be changed. These fields, when added to the layout, will have a ReadOnly value of True.

5.3.6 Disassociating Fields from a Tagging Layout

Case managers with the Case Administrator permission can disassociate tagging layouts.

To disassociate fields from a tagging layout

1. Log in as a user with Case Administrator rights.
2. Click on the **Tagging Layout** tab.
   See Tagging Layout Tab on page 38.
3. Check the layout that you want from the Tagging Layout list pane.
4. Click the fields tab in the lower pane .
5. Click the **Remove Association** button .

5.3.7 Associate User or Group to Tagging Layout

Case managers with the Case Administrator permission can create, edit, delete, and associate tagging layouts.

To associate users or groups to a tagging layout

1. Log in as a user with Case Administrator rights.
2. Click on the **Tagging Layout** tab.
   See Tagging Layout Tab on page 38.
3. Select the layout that you want from the Tagging Layout list pane.
4. Select either the *User* or *Groups* tab.
5. Click the **Add Association** button .
6. In the *All Users* or *All User Groups* dialog, click the plus sign to add the user or group to the tagging layout.
7. Click **OK**.

5.3.8 Disassociate User or Group to Tagging Layout

Case managers with the Case Administrator permission can disassociate tagging layouts.

To disassociate users or groups from a tagging layout

1. Log in as a user with Case Administrator rights.
2. Click on the **Tagging Layout** tab.
   See Tagging Layout Tab on page 38.
3. Check the layout that you want from the Tagging Layout list pane.
4. Select either the *User* or *Groups* tab.
5. Check the user or group that you want to disassociate.
6. Click the **Remove Association** button .

5.4 Configuring Highlight Profiles

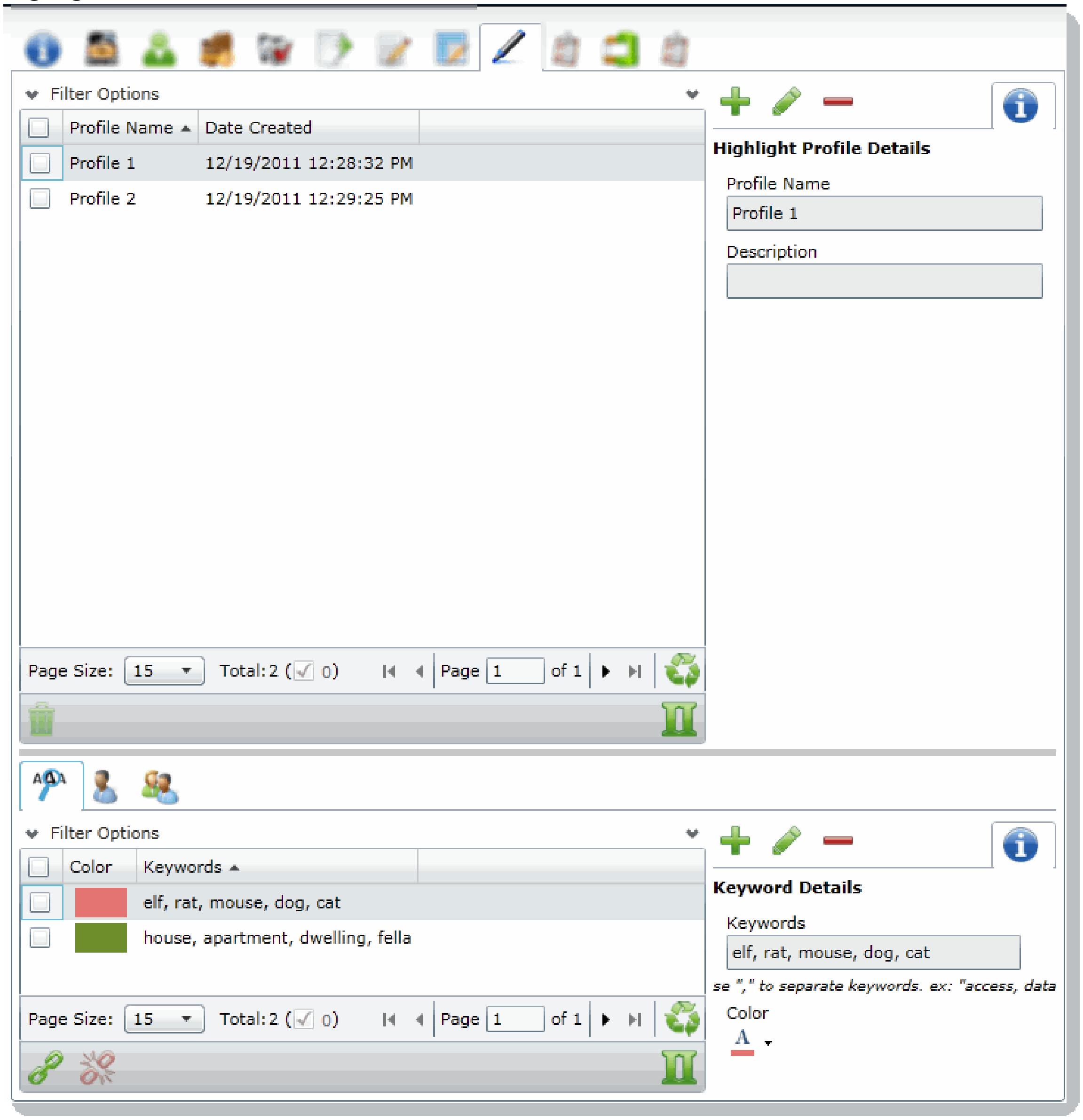
You can set up persistent highlighting profiles that will highlight predetermined keywords in the *Natural* panel of the document. Persistent highlighting profiles are defined by the administrator or case manager and can be toggled on and off using the *Select Profile* drop-down in the *Case Review*.

See Highlight Profiles Tab on page 43.

5.4.1 Highlight Profiles Tab

The *Highlight Profiles* tab on the *Home* page can be used to set up persistent highlighting profiles that will highlight predetermined keywords in the Natural View of the document. Persistent highlighting profiles are defined by the administrator or case manager and can be toggled on and off using the Select Profile drop-down in the Case Review.

Highlight Profiles Tab



Elements of the Highlight Profiles Tab

Element	Description
Filter Options	Allows the user to filter highlight profiles in the list.
Highlight Profiles List	Displays the highlight profiles already created for the case. Click the column headers to sort by the column.
Refresh 	Refreshes Highlight Profiles List.
Columns 	Click to adjust what columns display in the Highlight Profiles List.

Elements of the Highlight Profiles Tab (Continued)

Element	Description
Delete	Click to delete selected highlight profiles. Only active when a highlight profile is selected.
Add Highlight Profiles	Click to add a highlight profile.
Edit Highlight Profiles	Click to edit the selected highlight profile.
Delete Highlight Profiles	Click to delete the selected highlight profile.
Highlight Profile Keywords	Use this tab to add keywords and highlights to the highlight profile.
Users Tab	Use this tab to associate users to a highlight profile.
Groups Tab	Use this tab to associate groups to a highlight profile.
Add Association	Click to associate a user or group to a highlight profile.
Remove Association	Click to disassociate a highlight profile from a user or group.

5.4.2 Adding Highlight Profiles

Case managers with the Case Administrator permission can create, edit, delete, and associate highlight profiles.

To add a highlight profile

1. Log in as a user with Case Administrator rights.
2. Click on the **Highlight Profiles** tab.
   See Highlight Profiles Tab on page 43.
3. Click the **Add** button .
1. In the *Highlight Profile Detail* form, enter a *Profile Name*.
2. Enter a *Description* for the profile.
3. Click **OK**.

5.4.3 Editing Highlight Profiles

Case managers with the Case Administrator permission can create, edit, delete, and associate highlight profiles.

To edit a highlight profile

1. Log in as a user with Case Administrator rights.
2. Click on the **Highlight Profiles** tab.
   See Highlight Profiles Tab on page 43.
3. Select the profile that you want to edit.
4. Click the **Edit** button .
5. In the *Highlight Profile Detail* form, enter a *Profile Name*.
6. Enter a *Description* for the profile.
7. Click **OK**.

5.4.4 Deleting Highlight Profiles

Case managers with the Case Administrator permission can create, edit, delete, and associate highlight profiles.

To delete a highlight profile

1. Log in as a user with Case Administrator rights.
2. Click on the **Highlight Profiles** tab.
   See Highlight Profiles Tab on page 43.
3. Select the profile that you want to delete.
4. Click the **Delete** button .

Note: You can also delete multiple profiles by clicking the trash can delete button.

5.4.5 Add Keywords to a Highlight Profile

After you have created a highlight profile, you can add keywords to the profile that will appear highlighted in the Natural panel of the Case Review when the profile is selected.

To add keywords to a highlight profile

1. Log in as a user with Case Administrator rights.
2. Click on the **Highlight Profiles** tab.
   See Highlight Profiles Tab on page 43.
3. Select a profile.
4. Select the **Keywords** tab .
5. Click the **Add Keywords** button.

6. In the *Keyword Details* form, enter the keywords (separated by a comma) that you want highlighted.
7. Expand the color drop-down and select a color you want to use as a highlight.
8. Click **OK**.
9. You can add multiple keyword highlights, in different colors, to one profile.

Note: You can edit and delete keyword details by clicking the pencil or minus buttons in the **Keywords** tab.

5.4.6 Associating a Highlight Profile

Case managers with the Case Administrator permission can create, edit, delete, and associate highlight profiles. You can associate highlight profiles to users and groups.

To associate a highlight profile to a user or group

1. Log in as a user with Case Administrator rights.
2. Click on the **Highlight Profiles** tab.
   See Highlight Profiles Tab on page 43.
3. Select the profile that you want to associate to a user or group.
4. Click on either the *User* or *Groups* tab.
5. Click the **Add Association** button .
6. In the *All Users* or *All User Groups* dialog, click the plus sign to associate the user or group with the profile.
7. Click **OK**.

5.4.7 Disassociating a Highlight Profile

Case managers with the Case Administrator permission can disassociate highlight profiles from users or groups.

To disassociate a highlight profile from a user or group

1. Log in as a user with Case Administrator rights.
2. Click on the **Highlight Profiles** tab.
   See Highlight Profiles Tab on page 43.
3. Select the profile that you want to disassociate from a user or group.
4. Click on either the *User* or *Groups* tab.
5. Check the user or group that you want to disassociate.
6. Click the **Remove Association** button .

6 Monitoring the Work List

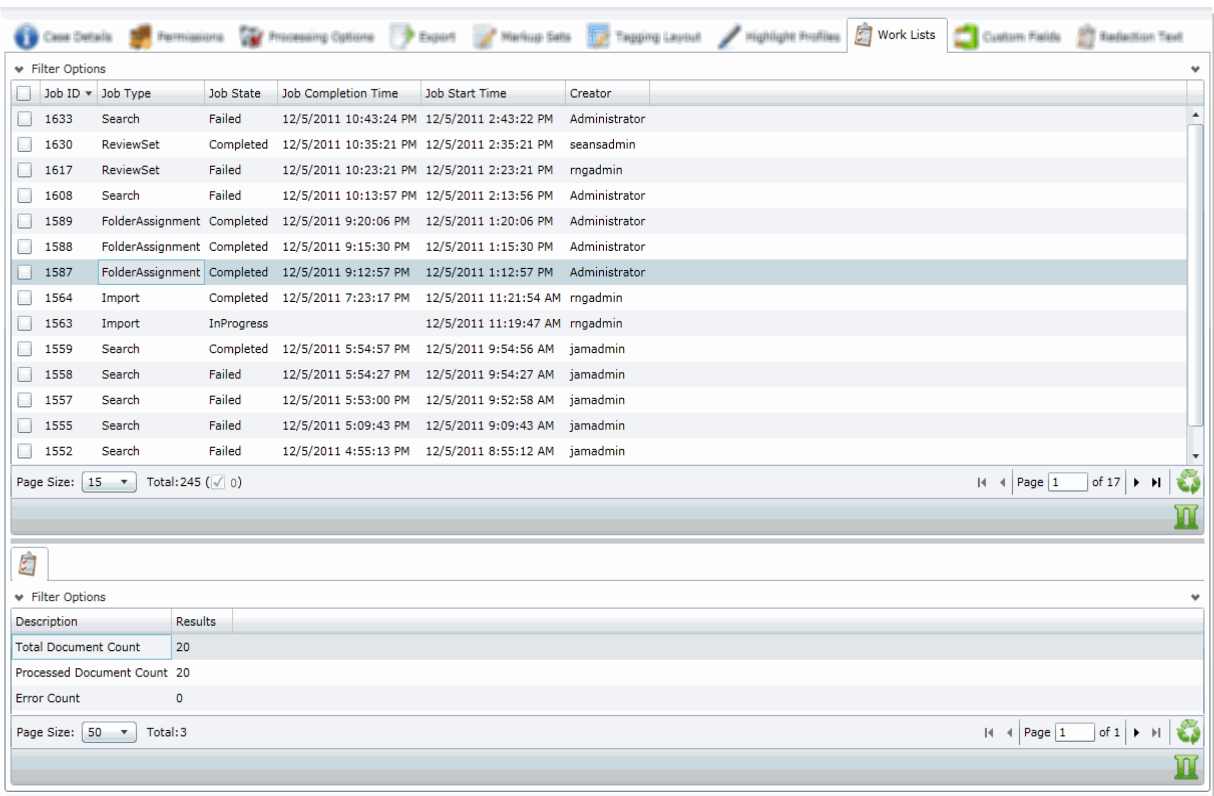
The case manager can use the *Work List* tab on the *Home* page to monitor certain activities on the case. The following items are recorded in the Work List: searches, review sets, imaging, label assignments, imports, bulk coding, cluster analysis, bulk labeling, transcript/exhibit uploading, and delete summaries.

The Job IDs are unique to every job. Jobs cannot be deleted or edited, only monitored. Case managers can be informed as to the actions performed in the case and errors that users have encountered in the case from the *Work List* tab.

6.1 Work List Tab

The *Work List* tab on the *Home* page can be used to view data for the selected case. The bottom panel displays the number of documents processed and number of errors. This will be updated periodically to reflect current status.

Work List Tab



Elements of the Work List Tab

Element	Description
Filter Options	Allows the user to filter jobs in the list.
Work List	Displays the jobs associated with the case. Click the column headers to sort by the column.
Refresh 	Refreshes the Work List.
Columns 	Click to adjust what columns display in the Work List.
Overview Tab 	Displays the statistics on the data found in the Work List.

7 Managing Document Groups

Case Managers with Folders and Case Administration permission can manage document groups. Document groups are folders where imported evidence is stored. Document groups can contain numerous documents. You can create document groups when importing evidence, or in Case Review.

You cannot assign permissions for documents unless the documents are in a document group. All documents in a group will be assigned DocIDs. Documents not within a document group, will NOT have DocIDs.

7.1 Creating a Document Group During Import

A document group is a way for you to organize your evidence. You can name your document group to reflect where the files were located, it can be a job number, a business name, or anything that will allow you to recognize what files are contained in the group. While importing evidence, you can create a document group. You can also place the documents into an existing document group.

See the Loading Data documentation for information on how to create new document groups while importing evidence and putting evidence into existing document groups.

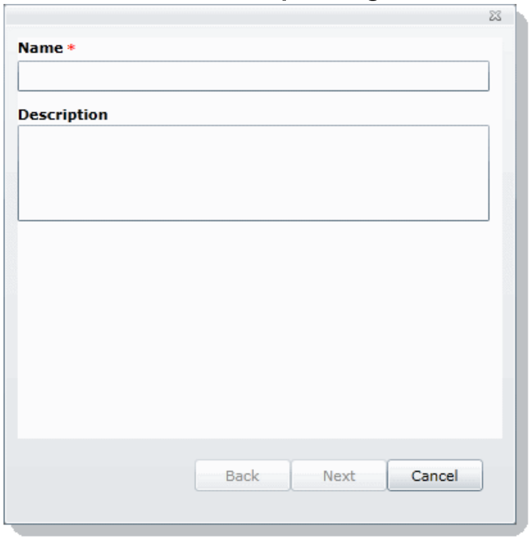
7.1.1 Creating a Document Group in Case Review

Case Managers with Folders permissions can create Document Groups in the Case Review.

To create document groups in Case Review

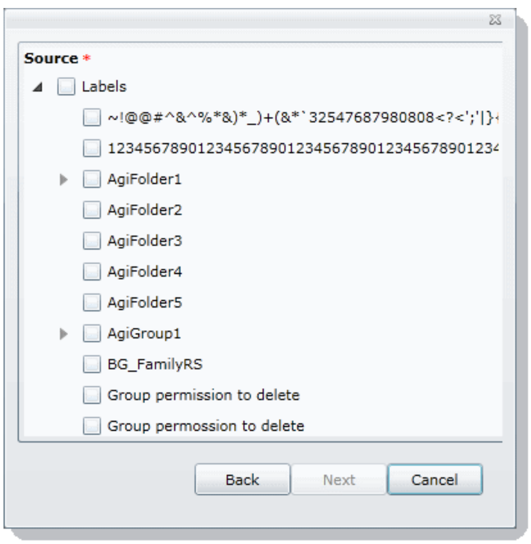
1. Log in as a user with Case Administrator rights.
2. Click the **Case Review**  button next to the case in the *Case List*.
3. In the *Case Explorer*, right-click the **Document Groups** folder and select **Create Document Group**.

Create Document Group Dialog



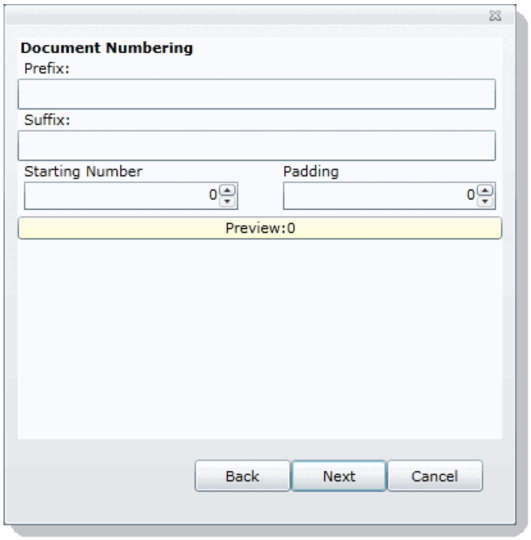
4. Enter a *Name* for the document group.
5. Enter a *Description* for the document group.
6. Click **Next.**

Select Labels



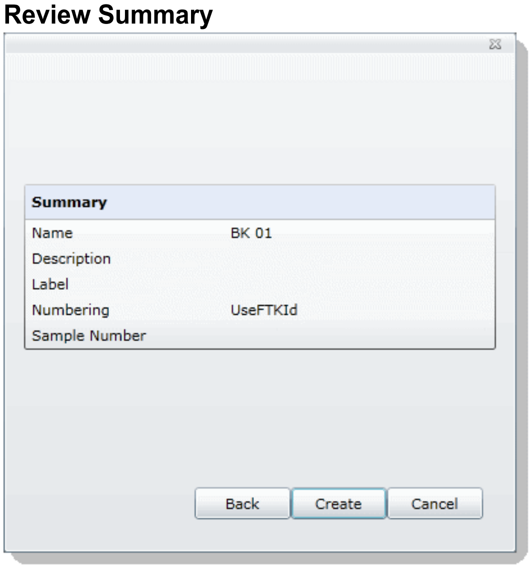
7. Check the labels that you want to include in the document group.
8. Click **Next.**

Renumber Documents



9. Select the **Re-Number Documents** radio button if you want to renumber the documents in the group. To leave numbering the same, select the blank radio button.
   - 9a. Enter a *Prefix* for the new numbering.
   - 9b. Enter a *Suffix* for the new numbering.
   - 9c. Select a *Starting Number* for the documents.
   - 9d. Select the *Padding* for the documents.
   - 9e. Click **Next**.

Review Summary



10. Review the *Summary* and click **Create**.
11. Click **OK**.

8 Managing Transcripts and Exhibits

Case managers with the Upload Exhibits, Upload Transcripts, and Manage Transcripts permissions can upload transcripts, create transcript groups, grant transcript permissions to users, and upload exhibits. Transcripts are uploaded from Case Review and can be viewed and annotated in the Transcripts panel.

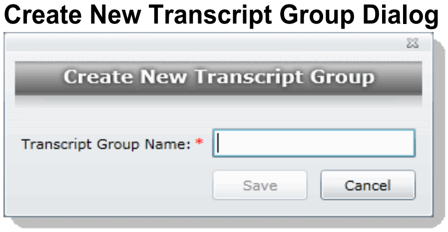
8.1 Creating a Transcript Group

Case managers with the Create Transcript Group permission can create transcript groups to hold multiple transcripts.

To create a transcript group

1. Log in as a user with Create Transcript Group rights.
2. Click the **Case Review**  button next to the case in the *Case List*.
3. In the *Case Explorer*, right-click the *Transcripts* folder and select **Create Transcript Group**.

Create New Transcript Group Dialog



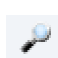
4. Enter a *Transcript Group Name*.
5. Click **Save**.

Note: You need to refresh your browser before you can add transcripts to the group.

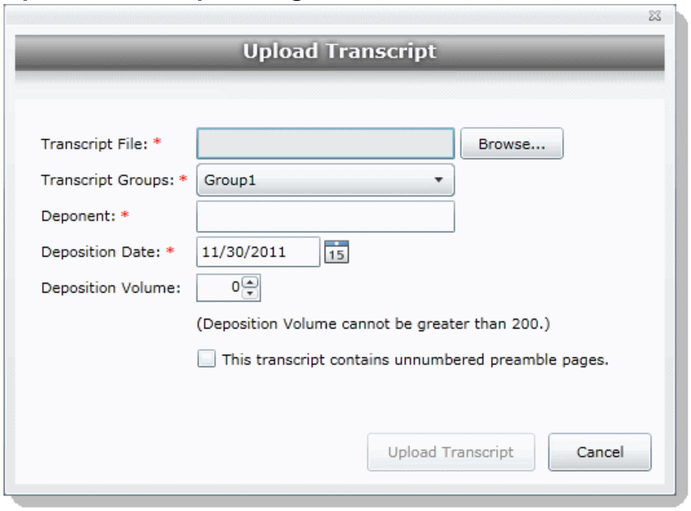
8.1.1 Uploading Transcripts

Case managers with the Upload Transcripts permission can upload transcript (.txt) files and put them in transcript groups. You can only add transcripts one at a time.

To upload transcripts

1. Log in as a user with Upload Transcripts rights.
2. Click the **Case Review**  button next to the case in the *Case List*.
3. In the *Case Explorer*, right-click the *Transcripts* folder and select **Upload Transcript**.

Upload Transcript Dialog

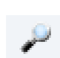


4. Browse to the location of the transcript .txt file.
5. Select a *Transcript Group* from the drop-down.
   See Creating a Transcript Group on page 53.
6. Enter the name of the *Deponent*.
7. Select the *Deposition Date*.
8. If you are uploading more than one transcript from the same day, specify the volume number to differentiate between the transcripts uploaded on the same date.
9. Check the **This transcript contains unnumbered preamble pages** to indicate that there are pages prior to the testimony. If you check this, enter the number of preamble pages prior that occur before the testimony. These pages will be numbered as “Preamble 0000#.” The numbering continues as normal after the preamble pages.
10. Click **Upload Transcript**.

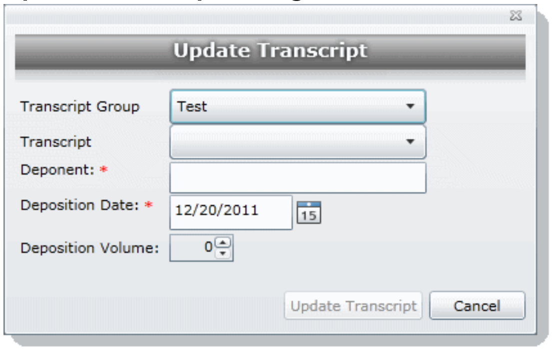
8.1.2 Updating Transcripts

Case managers with the Upload Transcripts permission can update transcripts in transcript groups. You can only update transcripts one at a time.

To update transcripts

1. Log in as a user with Upload Transcripts rights.
2. Click the **Case Review**  button next to the case in the *Case List*.
3. In the *Case Explorer*, right-click the *Transcripts* folder and select **Update Transcript**.

Update Transcript Dialog



4. Select a *Transcript Group*.
5. Select a *Transcript*.
6. Enter the *Deponent* name.
7. Enter the *Deposition Date*.
8. If you are uploading more than one transcript on the same day, specify the volume number to differentiate between the transcripts uploaded on the same date.
9. Click **Update Transcript**.

8.1.3 Uploading Exhibits

Case managers with the Upload Exhibits permission can upload exhibits in Case Review. Exhibits can be viewed in the exhibits panel.

To upload an exhibit

1. Log in as a user with Upload Exhibits rights.
2. Click the **Case Review**  button next to the case in the *Case List*.
3. In the *Case Explorer*, right-click the *Transcripts* folder and select **Upload Exhibits**.

Upload Exhibit Dialog

4. Select the *Transcript Group* where you want to place the exhibit.
5. Browse to the exhibit file.
6. Enter a *Description* of the exhibit.
7. Click **Upload Exhibit.**

9 Managing Review Sets

Review sets are batches of documents that users can check out for coding and then check back in. Review sets aid in the work flow of the reviewer; it allows the reviewer to track the documents that have been coded and still need to be coded. Case managers with Create/Delete Review Set permissions can create and delete review sets.

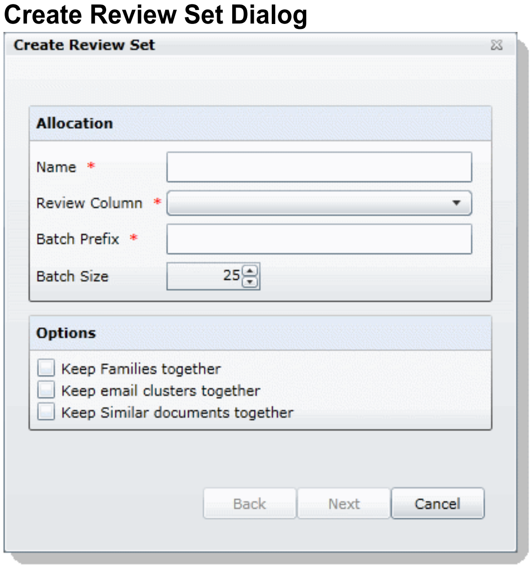
9.1 Creating a Review Set

Case managers with Create/Delete Review Set permissions can create and delete review sets.

To create a review set

1. Log in as a user with Case Administrator rights.
2. Click the **Case Review**  button next to the case in the *Case List*.
3. Click the **Review Sets** button in the *Case Explorer*.
   See the Reviewer Guide for more information on the Review Sets tab.
4. Right-click the **Review Sets** folder and select **Create Review Set**.

Create Review Set Dialog



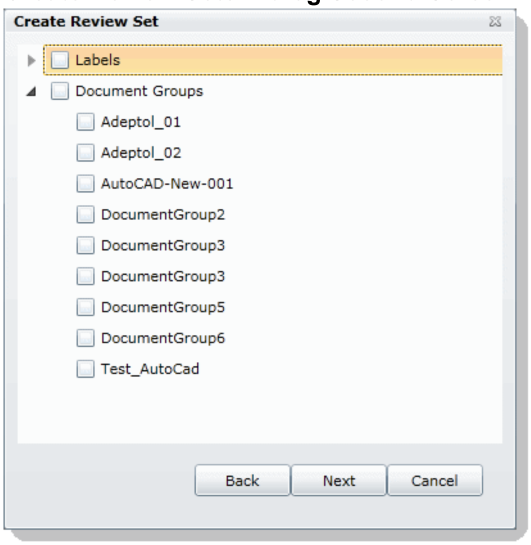
5. Enter a *Name* for the review set.
6. Select a **Review Column** that indicates the status of the review. New columns can be created in the *Custom Fields* tab of the *Home* page.
   See Custom Fields Tab on page 35.
7. Enter a prefix for the batch that will appear before the page numbers of the docs.
8. Increase or decrease the *Batch Size* to match the number of documents that you want to appear in the review set.

9. Check the following options if desired:
   - **Keep Families together**: Check this to include documents within the same family as the selected documents in the batch.
   - **Keep email clusters together**: Check this to include email threads of the selected documents in the batch.
   - **Keep Similar document sets together**: Check this to include documents related to the selected documents in the batch.

   Note: Any “Keep” check box selected will override the restricted Batch Size.

10. Click **Next.**

Create Review Sets Dialog Second Screen



11. Expand *Labels* and check the labels that you want to include in the review set. All documents with that label applied will be included in the review set. This is only relevant if the documents have already been labelled by reviewers.
12. Expand the *Document Groups* and check the document groups that you want to include in the review set.
13. Click **Next.**
14. Review the summary of the review set to insure everything is accurate and click **Create**.
15. Click **Close.**

9.2 Deleting Review Sets

Case managers with Create/Delete Review Set permissions can create and delete review sets.

To create a review set

1. Log in as a user with Case Administrator rights.
2. Click the **Case Review**  button next to the case in the *Case List*.
3. Click the **Review Sets** button in the *Case Explorer*.
   See the Reviewer Guide for more information on the Review Sets tab.
4. Expand the *All Sets* folder.
5. Right-click the review set that you want to delete and select **Delete**.
6. Click **OK**.

9.3 Renaming a Review Set

Case managers with Manage Review Set permissions can rename review sets.

To rename a review set

1. Log in as a user with Case Administrator rights.
2. Click the **Case Review**  button next to the case in the *Case List*.
3. Click the **Review Sets** button in the *Case Explorer*.
   See the Reviewer Guide for more information on the Review Sets tab.
4. Expand the *All Sets* folder.
5. Right-click the review set that you want to rename and select **Rename**.
6. Enter a name for the review set.

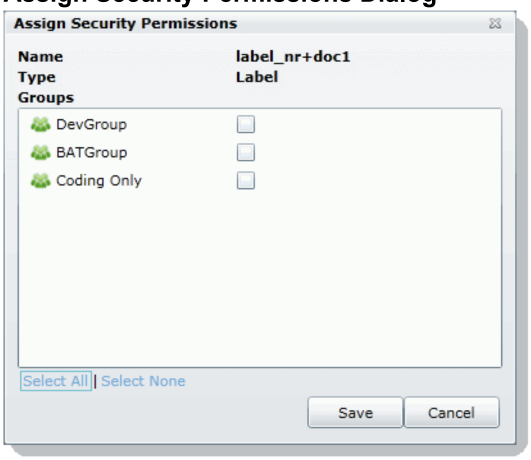
9.4 Manage Permissions for Review Sets

Case managers with Manage Review Set permissions can manage the permissions for review sets.

To rename a review set

1. Log in as a user with Case Administrator rights.
2. Click the **Case Review**  button next to the case in the *Case List*.
3. Click the **Review Sets** button in the *Case Explorer*.
   See the Reviewer Guide for more information on the Review Sets tab.
4. Expand the *All Sets* folder.
5. Right-click the review set that you want to manage permissions for and select **Manage Permissions**.

Assign Security Permissions Dialog



6. Check the groups that you want to grant permissions to the review set. Groups granted the Check In/ Check Out Review Batches permission will be able to check out the review sets to which they are granted permission.
7. Click **Save**.

10 Managing Tags

Case managers can manage the tags for a case in the Case Review. The following tags can be created, deleted, renamed, and managed for permissions:

- Labels: See Managing Labels on page 61.
- Issues: See Managing Issues on page 64.
- Categories: See Creating Category Values on page 37.

10.1 Managing Labels

Labels are a tool that reviewers can use to group documents together. Reviewers apply labels to documents, then case managers can use the Labels folder to view all the documents under the selected label. Before reviewers can use a label, the case manager must create it.

10.1.1 Creating Labels

Case Managers can create labels for reviewers to use when reviewing documents.

To create a label

1. Log in as a user with Case Administrator rights.
2. Click the **Case Review**  button next to the case in the *Case List*.
3. Click the **Tags**  button in the *Case Explorer*.
   See the Reviewer Guide for more information on tags.
4. Expand the *Tags* folder.
5. Right-click the *Labels* folder and select **Create Label**.

Create Label Dialog

6. Enter a *Label Name*.
7. Check **Is Label Group** if the label is a group to contain other labels and then skip to the last step.

8. Do one of the following:
   - **No Color**: Select this to have no color associated with the label.
   - **Color**: Select this and then select a color to associate a color with the label.

   Note: The default color is black if you select the Color option. The color selected appears next to the label in the labels folder.

9. Click **Save**.

10.1.2 Deleting Labels

Case Managers can delete existing labels.

To delete a label

1. Log in as a user with Case Administrator rights.
2. Click the **Case Review** button next to the case in the *Case List*.
3. Click the **Tags** button in the *Case Explorer*.
   See the Reviewer Guide for more information on tags.
4. Expand the *Tags* folder.
5. Expand the *Labels* folder.
6. Right-click the label that you want to delete and select **Delete**.
7. Click **OK**.

10.1.3 Renaming a Label

Case Managers can rename labels in the Case Review.

To rename a label

1. Log in as a user with Case Administrator rights.
2. Click the **Case Review** button next to the case in the *Case List*.
3. Click the **Tags** button in the *Case Explorer*.
   See the Reviewer Guide for more information on tags.
4. Expand the *Tags* folder.
5. Expand the *Labels* folder.
6. Right-click the label that you want to rename and select **Rename**.
7. Enter the new name for the label.

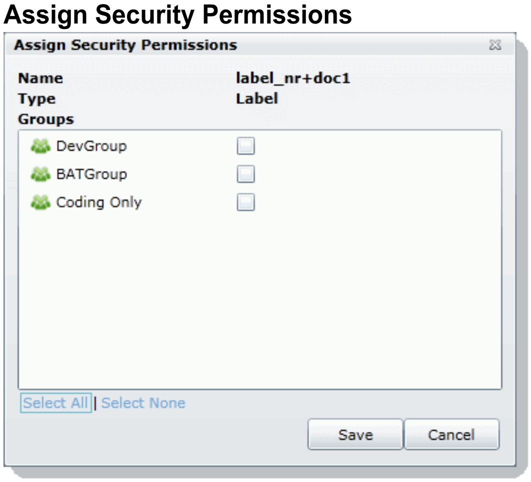
10.1.4 Managing Label Permissions

Case Managers can grant permissions of labels to groups for use. Groups of users can only use the labels for which they have permissions.

To manage permissions for labels

1. Log in as a user with Case Administrator rights.
2. Click the **Case Review**  button next to the case in the *Case List*.
3. Click the **Tags**  button in the *Case Explorer*.
   See the Reviewer Guide for more information on tags.
4. Expand the *Tags* folder.
5. Expand the *Labels* folder.
6. Right-click the label for which you want to grant permissions and select **Manage Permissions**.

Assign Security Permissions



7. Check the groups that you want to grant permissions for the selected label.

   Note: By default, all groups that the logged-in user belongs to will be checked. To make it a personal label, all groups should be un-checked.

8. Click **Save**.

10.2 Managing Issues

Case managers with View Issues and Assign Issues permissions can create, delete, rename, and assign permissions for issues. Issues work like labels. Reviewers can apply issues to documents to group similar documents.

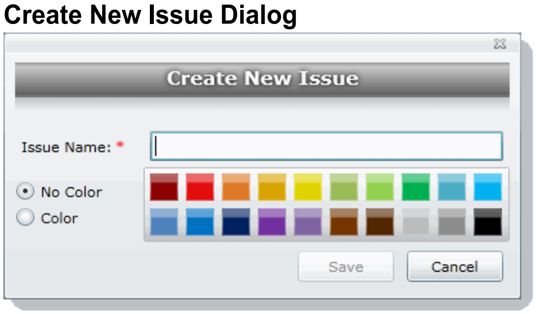
10.2.1 Creating Issues

Case managers with View Issues and Assign Issues permissions can create issues for other users to code.

To create an issue

1. Log in as a user with View Issues and Assign Issues rights.
2. Click the **Case Review** button next to the case in the *Case List*.
3. Click the **Tags** button in the *Case Explorer*.
   See the Reviewer Guide for more information on tags.
4. Expand the *Tags* folder.
5. Right-click the *Issues* folder and select **Create Issue**.

Create New Issue Dialog



6. Enter an *Issue Name*.
7. Do one of the following:
   - **No Color**: Select this to have no color associated with the issue.
   - **Color**: Select this and then select a color to associate a color with the issue.
8. Click **Save**.

10.2.2 Deleting Issues

Case managers with View Issues and Assign Issues permissions can delete issues.

To delete an issue

1. Log in as a user with View Issues and Assign Issues rights.
2. Click the **Case Review** button next to the case in the *Case List*.

3. Click the **Tags** button in the *Case Explorer*.
   See the Reviewer Guide for more information on tags.
4. Expand the *Tags* folder.
5. Expand the *Issues* folder.
6. Right-click the issue that you want to delete and select **Delete**.
7. Click **OK**.

10.2.3 Renaming Issues

Case managers with View Issues and Assign Issues permissions can rename issues.

To delete an issue

1. Log in as a user with View Issues and Assign Issues rights.
2. Click the **Case Review** button next to the case in the *Case List*.
3. Click the **Tags** button in the *Case Explorer*.
   See the Review Guide for more information on tags.
4. Expand the *Tags* folder.
5. Expand the *Issues* folder.
6. Right-click the issue that you want to rename and select **Rename**.
7. Enter the new name for the issue.

10.2.4 Managing Issue Permissions

Case Managers can grant permissions of issues to groups for use. Groups of users can only use the labels for which they have permissions.

To manage permissions for labels

1. Log in as a user with View Issues and Assign Issues rights.
2. Click the **Case Review** button next to the case in the *Case List*.
3. Click the **Tags** button in the *Case Explorer*.
   See the Reviewer Guide for more information on tags.
4. Expand the *Tags* folder.
5. Expand the *Issues* folder.
6. Right-click the issue for which you want to grant permissions and select **Manage Permissions**.

Assign Security Permissions

7. Check the groups that you want to grant permissions for the selected issue.
8. Click **Save**.

10.2.5 Applying Issues to Documents

After an issue has been created and associated with a user group, it can then be added to a tagging layout for coding.

To apply an issue to a document

1. Create an issue.
   See Creating Issues on page 64.
2. Grant permissions for the issue.
   See Managing Issue Permissions on page 65.
3. Add Issues to the Tagging Layout.
   See Associating Fields to a Tagging Layout on page 41.
4. Check out a review set of documents. (optional)
   See the Reviewer Guide for more information on checking out review sets.
5. Code the documents in the review set with the issues you created.
   See the Reviewer Guide for more information on coding.

Loading Summation Data

The part describes how to load Summantion data and includes the following sections:

1 Imporing Data Introduction

1.1 Importing Data

This document will help you import data into your case. You create cases in order to organize data. Data can be added to cases in the forms of native files, such as DOC, PDF, XLS, PPT, and PST files, or as evidence images, such as AD1, E01, and AFF files.

To manage evidence, administrators, and users with the Create/Edit Cases permission, can do the following:

- Add evidence items to a case
- View properties about evidence items in a case
- Edit properties about evidence items in a case
- Associate custodians to evidence items in a case

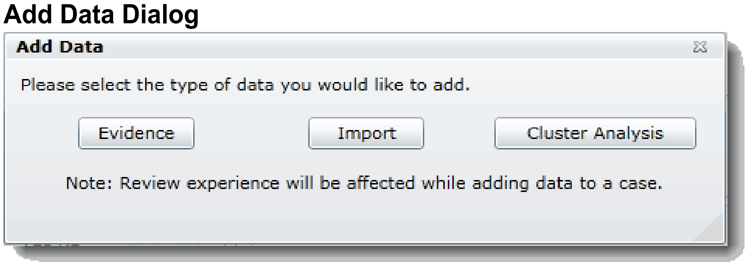
Note: You will normally want to have custodians created and selected before you process evidence.

See About Creating Custodians when Adding Evidence Items on page 10.

To import data

1. Log in as a case manager.
2. Click the Add Data button next to the case in the Case List panel.

Add Data Dialog



3. In the Add Data dialog, select on of the method by which you want to import data. The following methods are available:
   - Evidence (wizard):
   - Import:
   - Cluster Analysis:

2 Using the Evidence Wizard

2.1 About Adding Evidence Items Using the Evidence Wizard

When you add evidence to a case, you can use the Add Evidence Wizard to specify the data that you want to add. You specify to add either parent folders or individual files.

Note: If you activated Cluster Analysis as a processing option when you created the case, cluster analysis will automatically run after processing data.

You select sets of data that are called “evidence items.” It is useful to organize data into evidence items because each evidence item can be associated with a unique custodian.

For example, you could have a parent folder with a set of subfolders.

\\10.10.3.39\EvidenceSource\

\\10.10.3.39\EvidenceSource\John Smith

\\10.10.3.39\EvidenceSource\Bobby Jones

\\10.10.3.39\EvidenceSource\Samuel Johnson

\\10.10.3.39\EvidenceSource\Edward Peterson

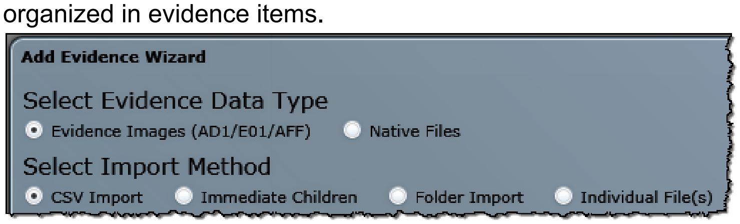
\\10.10.3.39\EvidenceSource\Jeremy Lane

You could import the parent \\10.10.3.39\EvidenceSource\ as one evidence item. If you associated a custodian to it, all files under the parent would have the same custodian.

On the other hand, you could have each subfolder be its own evidence item, and then you could associate a unique custodian to each item.

An evidence item can either be a folder or a single file. If the item is a folder, it can have other sub-folders, but they would be included in the item.

When you use the Evidence Wizard to import evidence, you have options that will determine how the evidence is organized in evidence items.



When you add evidence, you select from the following types of files.

Evidence File Types

File Type	Description
Evidence Images	You can add AD1, E01, or AFF evidence image files.
Native Files	You can add native files, such as PDF, JPG, DOC PPT, PST, XLSX, and so on.

When you add evidence, you also select one of the following import methods.

Import Methods

Method	Description
CSV Import	This method lets you create and import a CSV file that lists multiple paths of evidence and optionally automatically creates custodians and associates each evidence item with a custodian. Like the other methods, you specify whether the parent folder contains native files or image files. See About Using the CSV Import Method for Importing Evidence on page 10. This is similar to adding custodians by importing a file. See the Case Manager Guide for more information on adding custodians by importing a file.
Immediate children	This method takes the immediate subfolders of the specified path and imports each of those subfolders' content as a unique evidence item. You can automatically create a custodian based on the child folder's name (if the child folder has a first and last name separated by a space) and have it associated with the data in the subfolder. See About Using the Immediate Children Method for Importing Evidence on page 12. Like the other methods, you specify if the parent folder contains native files or image files.
Folder Import	This method lets you select a parent folder and all data in that folder will be imported. You specify that the folder contains either native files (JPG, PPT) or image files (AD1, E01, AFF). A parent folder can have both subfolders and files. Using this method, each parent folder that you import is its own evidence item and can be associated with one custodian. For example, if a parent folder had several AD1 files, all data from each AD1 file can have one associated custodian. Likewise, if a parent folder has several native files, all of the contents of that parent folder can have one associated custodian.
Individual File(s)	This method lets you select individual files to import. You specify that these individual files are either native files (JPG, PPT) or image files (AD1, E01, AFF). Using this method, each individual file that you import is its own evidence item and can be associated with a custodian. For example, all data from an AD1 file can have an associated custodian. Likewise, each PDF, or JPG can have its own associated custodian.

Note: The source network share permissions are defined by the administrator credentials.

2.1.1 About Creating Custodians when Adding Evidence Items

When you add evidence items to a case, you can also create custodians at the same time. There are three ways you can create custodians while adding evidence to a case:

- Using a CSV Evidence Import.
  See About Using the CSV Import Method for Importing Evidence on page 10.
- Importing immediate children.
  See About Using the Immediate Children Method for Importing Evidence on page 12.
- Adding a custodian in the Add Evidence Wizard.
  You can select a custodian from the drop-down wizard or enter a new custodian name.
  See the Case Manager Guide for more information on creating custodians.

2.1.2 About Using the CSV Import Method for Importing Evidence

When specifying evidence to import in the Add Evidence Wizard, you can use one of two general options:

- Manually browse to all evidence folders and files.
- Specify folders, files, and custodians in a CSV file.
  There are several benefits of using a CSV file:
  - You can more easily and accurately plan for all of the evidence items to be included in a case by including all sources of evidence in a single file.
  - You can more easily and accurately make sure that you add all of the evidence items to be included in a case.
  - If you have multiple folders or files, it is quicker to enter all of the paths in the CSV file than to browse to each one in the wizard.
  - If you are going to specify custodians, you can specify the custodian for each evidence item. This will automatically add those custodians to the system rather than having to manually add each custodian.

When using a CSV, each path or file that you specify will be its own evidence item. The benefit of having multiple items is that each item can have its own associated custodian. This is in contrast with the Folder Import method, where only one custodian can be associated with all data under that folder.

Specifying custodians is not required. However, if you do not specify custodians, when the data is imported, no custodians are created or associated with evidence items. Custodian data will not be usable in Case Review.

See the Case Manager Guide for information on associating a custodian to an evidence item.

If you do specify custodians in the CSV file, you use the first column to specify the custodian name and the second column for the path.

If you do not specify custodians, you will only use one column for paths. When you load the CSV file in the Add Evidence Wizard, you will specify that the first column does not contain custodian names. That way, the wizard imports the first column as paths and not custodians.

If you do specify custodians, they can be in one of two formats:

- A single name or text string with no spaces
  For example, JSmith or John_Smith
- First and last name separated by a space
  For example, John Smith or Bill Jones

In the CSV file, you can optionally have column headers. You will specify in the wizard whether it should use the first row as data or ignore the first row as headers.

CSV Example 1

This example includes headers and custodians.

In the wizard, you select both **First row contains headers** and **First column contains custodian names** check boxes.

When the data is imported, the custodians are created and associated to the case and the appropriate evidence item.

```
Custodians, Paths
JSmith,\\10.10.3.39\EvidenceSource\JSmith
JSmith,\\10.10.3.39\EvidenceSource\Sales\Projections.xlsx
Bill Jones,\\10.10.3.39\EvidenceSource\BJones
Sarah Johnson,\\10.10.3.39\EvidenceSource\SJohnson
Evan_Peterson,\\10.10.3.39\EvidenceSource\EPeterson
Evan_Peterson,\\10.10.3.39\EvidenceSource\HR
Jill Lane,\\10.10.3.39\EvidenceSource\JLane
Jill Lane,\\10.10.3.39\EvidenceSource\Marketing
```

This will important any individual files that are specified as well as all of the files (and additional sub-folders) under a listed subfolder.

You may normally use the same naming convention for custodians. This example shows different conventions simply as examples.

CSV Example 2

This example does not include headers or custodians.

In the wizard, you clear both **First row contains headers** and **First column contains custodian names** check boxes.

When the data is imported, no custodians are created or associated with evidence items.

```
\\10.10.3.39\EvidenceSource\JSmith
\\10.10.3.39\EvidenceSource\Sales\Projections.xlsx
\\10.10.3.39\EvidenceSource\BJones
\\10.10.3.39\EvidenceSource\SJohnson
\\10.10.3.39\EvidenceSource\EPeterson
```

\\10.10.3.39\EvidenceSource\HR

\\10.10.3.39\EvidenceSource\JLane

\\10.10.3.39\EvidenceSource\Marketing

2.1.3 About Using the Immediate Children Method for Importing Evidence

If you have a parent folder that has children subfolders, when importing it through the Add Evidence Wizard, you can use one of three methods:

- Folder Import
- Immediate Children
- CSV Import
  See About Using the CSV Import Method for Importing Evidence on page 10.

When using the Immediate Children method, each child subfolder of the parent folder will be its own evidence item. The benefit of having multiple evidence items is that each item can have its own associated custodian. This is in contrast with the Folder Import method, where all data under that folder is a single evidence item with only one possible custodian associated with it.

Specifying custodians is not required. However, if you do not specify custodians, when the data is imported, no custodians are created or associated with evidence items. Custodian data will not be usable in Case Review.

See the Case Manager Guide for more information on associating a custodian to evidence.

When you select a parent folder in the Add Evidence Wizard, you select whether or not to specify custodians.

If you do specify custodians, the custodian names are based on the name of the child folders.

Imported custodian names can be imported in one of two formats:

- A single name or text string with no spaces
  For example, JSmith or John_Smith
- First and last name separated by a space
  For example, John Smith or Bill Jones

For example, suppose a parent folder had four subfolders, each containing data from a different user. Using the Immediate Children method, each subfolder would be imported as a unique evidence item and the subfolder name could be the associated custodian.

\Userdata\ (parent folder that is selected)

\Userdata\INewstead (unique evidence item with INewstead as custodian)

\Userdata\KHetfield (unique evidence item with KHetfield as custodian)

\Userdata\James Ulrich (unique evidence item with James Ulrich as custodian)

\Userdata\Jill_Hammett (unique evidence item with Jill_Hammett as custodian)

Note: In the Add Evidence Wizard, you can manually rename the custodians if needed.

The child folder may be a parent folder itself, but anything under it would be one evidence item.

This method is similar to the CSV Import method in that it automatically creates custodians and associates them to evidence items. The difference is that when using this method, everything is configured in the wizard and not in an external CSV file.

2.2 Adding Evidence to a Case Using the Evidence Wizard

You can import evidence for cases you have permissions for.

When you add evidence, it is processed so that it can be reviewed in Case Review.

Note: Some data cannot be changed after it has been processed. Before adding and processing evidence, do the following:

- Configure the Processing Options the way you want them.
  See the Admin Guide for more information on default processing options.
- Plan whether or not you want to specify custodians.
  See the Case Manager Guide for more information on associating a custodian to evidence.
- Unless you are importing custodians as part of the evidence, you must have custodians already associated with the case.
  See the Case Manager Guide for more information on creating custodians.

To import evidence for a case

1. In the case list, click (add evidence) in the case that you want to add evidence to.
2. Select **Evidence**.
3. In the *Add Evidence Wizard*, select the *Evidence Data Type* and the *Import Method*.
   See About Adding Evidence Items Using the Evidence Wizard on page 8.
4. Click **Next**.
5. Select the evidence folder or files that you want to import.
   This screen will differ depending on the *Import Method* that you selected.

   5a. If you are using the *CSV Import* method, do the following:

   - If the CSV file uses the first row as headers rather than folder paths, select the **First row contains headers** check box, otherwise, clear it.
   - If the CSV file uses the first column to specify custodians, select the **First column contains custodian names** check box, otherwise, clear it.
     See About Using the CSV Import Method for Importing Evidence on page 10.
     - Click **Browse**.
     - Browse to the CSV file and click **OK**.
       The CSV data is imported based on the check box settings.
       Confirm that the custodians and evidence paths are correct.
       You can edit any information in the list.
       If the wizard can't validate something in the CSV, it will highlight the item in red and place a red box around the problem value.
       If a new custodian will be created, it will be designated by .

   5b. If you are using the *Immediate Children* method, do the following:

   - If you want to automatically create custodians, select **Sub folders are custodian names**, otherwise, clear it.
     See About Using the Immediate Children Method for Importing Evidence on page 12.
   - Click **Browse**.
   - Enter the IP address of the server where the evidence files are located and click **Go**.
     For example, 10.10.2.29
   - Browse to the parent folder and click **Select**.

Each child folder is listed as a unique evidence item.

If you selected to create custodians, they are listed as well.

Confirm that the custodians and evidence paths are correct.

You can edit any information in the list.

If the wizard can't validate something, it will highlight the item in red and place a red box around the problem value.

If a new custodian will be created, it will be designated by .

5c. If you are using the Folder Input or Individual Files method, do the following:

- Click **Browse**.
- Enter the IP address of the server where the evidence files are located and click **Go**.

  For example, 10.10.2.29
- Expand the folders in the left pane to browse the server.
- In the right pane highlight the parent folder or file and click **Select**.

  If you are selecting files, you can use Ctrl-click or Shift-click to select multiple files in one folder.

  The folder or file is listed as a unique evidence item.

6. If you want to specify a custodian, select one from the *Custodian Name* drop-down list or type in a new custodian name to be added.

   If you enter a new custodian that will be created, it will be designated by .

   You can also edit a custodian name if it was imported.
7. Specify a Timezone.

   From the Timezone drop-down list, select a time zone.

   See Evidence Time Zone Setting on page 15.
8. (Optional) Enter a *Description*.

   This is used as a short description that is displayed with each item in the *Evidence* tab.

   For example, "Imported from Filename.csv" or "Children of *path*".

   This can be added or edited later in the *Evidence* tab.
9. (Optional) If you need to delete an evidence item, click the for the item.
10. Click **Next**.
11. In the *Evidence to be Added and Processed* screen, you can view the evidence that you selected so far. From this screen, you can perform one of the following actions:
    - *Add More*: Click this button to return to the *Add Evidence* screen.
    - *Add Evidence and Process*: Click this button to add and process the evidence listed.

    When you are done, you are returned to the case list. After a few moments, the job will start and the case status should change to *Processing*.
12. If you need to manually update the list or status, click (refresh).
13. When the evidence import is completed, you can view the evidence items in the *Evidence* and *Custodians* labels.

2.2.1 Evidence Time Zone Setting

Because of worldwide differences in the time zone implementation and Daylight Savings Time, you select a time zone when you add an evidence item to a case.

In a FAT volume, times are stored in a localized format according to the time zone information the operating system has at the time the entry is stored. For example, if the actual date is Jan 1, 2005, and the time is 1:00

p.m. on the East Coast, the time would be stored as 1:00 p.m. with no adjustment made for relevance to Greenwich Mean Time (GMT). Anytime this file time is displayed, it is not adjusted for time zone offset prior to being displayed.

If the same file is then stored on an NTFS volume, an adjustment is made to GMT according to the settings of the computer storing the file. For example, if the computer has a time zone setting of -5:00 from GMT, this file time is advanced 5 hours to 6:00 p.m. GMT and stored in this format. Anytime this file time is displayed, it is adjusted for time zone offset prior to being displayed.

For proper time analysis to occur, it is necessary to bring all times and their corresponding dates into a single format for comparison. When processing a FAT volume, you select a time zone and indicate whether or not Daylight Savings Time was being used. If the volume (such as removable media) does not contain time zone information, select a time zone based on other associated computers. If they do not exist, then select your local time zone settings.

With this information, the system creates the case database and converts all FAT times to GMT and stores them as such. Adjustments are made for each entry depending on historical use data and Daylight Savings Time. Every NTFS volume will have the times stored with no adjustment made.

With all times stored in a comparable manner, you need only set your local machine to the same time and date settings as the case evidence to correctly display all dates and times.

3 Using Import

3.1 Importing Evidence Using Import

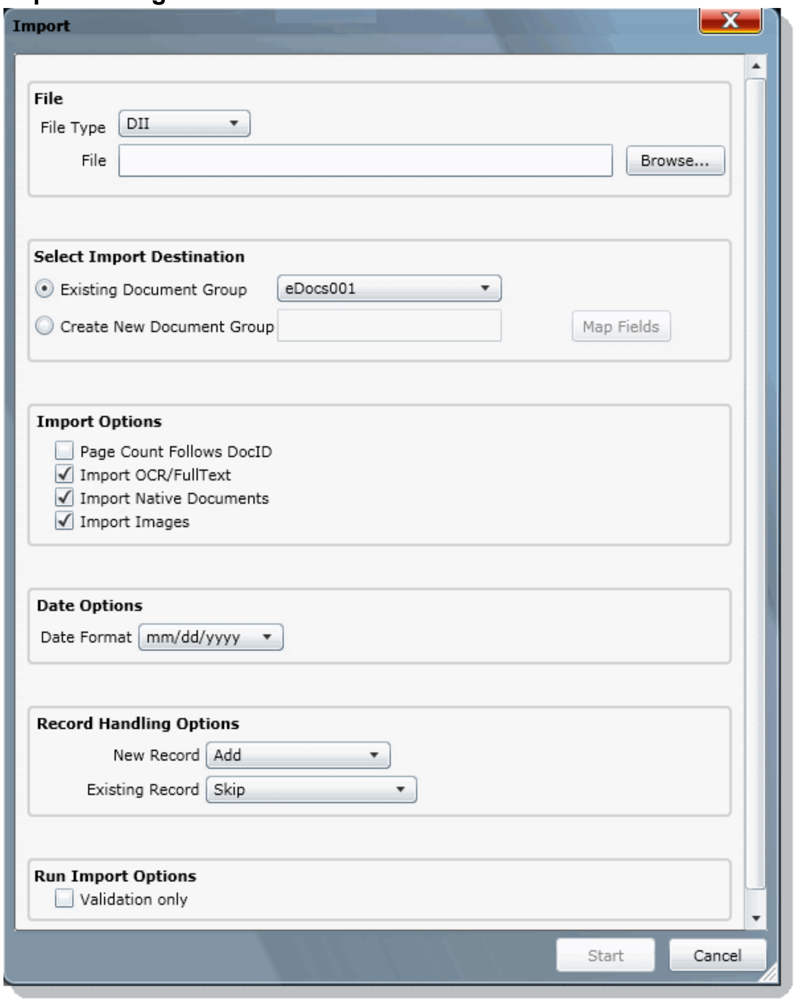
Administrators and Case Managers with the Create/Edit Case Admin Role can import evidence for a case. Your documents must be compiled into a DII or CSV file format in order to import them into Summation using the Import feature.

Transcripts and exhibits are uploaded from the Case Reviewer and not from the Import dialog; see the Case Manager Guide for more information on how to upload transcripts and exhibits.

To import evidence into a case

1. Log in to Summation as an Administrator or a user with Create/Edit Case rights.
2. In the *Case List* panel, click the **Add Evidence** button  next to the case.
3. Select **Import**.

Import Dialog



4. In the *Import* dialog, select the file type, either DII or CSV. These are the only supported file types.
5. Enter the location of the file, or **Browse** to the location.
6. Select the Import Destination:
   - **Existing Document Group**: Select this to add the documents to an existing document group. Select the group from the drop-down.

     See the Case Manager Guide for more information on managing document groups.
   - **Create New Document Group**: Select this to add the documents to a new document group. Enter the name of the group in the field next to this radio button.
7. Click the **Map Fields** button to map the fields in the documents of the CSV or DII file to the custom fields that you have created in the case. Mapping the fields will put the correct information about the document in the correct columns in the *Case Review*. The check file process is run after clicking the *Map Fields* button. Any errors that have to be corrected before the file can be imported are reported at this time.

   Note: If you need custom fields, you must create them in the Custom Fields tab on the Home page before importing in order to map to those fields.

   This process may take a long time for large DII files.

7a. Select **Skip Unmapped** to skip items that do not map.

7b. Click **Reset** to return the fields back to their original state.

Note: Every time you click the *Map Fields* button, the fields are reset to their original state.

8. Select the Import Options for the file. These options will differ depending on whether you select DII or CSV.
   - DII Options:
     - **Page Count Follows Doc ID**: Check if your DII file has an @T value that contains both a Doc ID and a page count.
     - **Import OCR/Full Text**: Check to import OCR/Full Text documents for each record.
     - **Import Native Documents/Images**: Check to import Native Documents and Images for each record.
   - CSV Options:
     - **First Row Contains Field Names**: Check if the CSV file being imported contains a row header.
     - **Separators**: Enter the symbols for the different separators that the CSV file being imported contains. Each separator value must match the CSV separators exactly or the field being imported for each record will not be populated correctly.
     - **Return Placeholder**: Choose the same value that the CSV file being imported contains as a replacement value for carriage return and line feed characters.
9. Select the way that you want the dates to appear in the documents by selecting an option from the **Date Options** drop-down.
10. Select the Record Handling Options.
    - **New Record**:
      - Add: Select to add new records.
      - Skip: Select to ignore new records.
    - **Existing Record**:
      - Update: Select to update duplicate records with the record being imported.
      - Overwrite: Select to overwrite the duplicate records with the record being imported.
      - Skip: Select to skip the duplicate file.
11. Select the *Run Import Options*.
    - **Validation Only**: Check to validate whether the file is good to import.
    - **Stop Immediately on First Error**: Check to stop the import when it encounters an error. If you do not check this, it will skip items with errors and continue the import, excluding those files.

4 Using Cluster Analysis

4.1 Cluster Analysis

You can use Cluster Analysis to group Email Threaded data and Near Duplicate data together for quicker review.

Note: If you activated Cluster Analysis as a processing option when you created the case, cluster analysis will automatically run after processing data and will not need to be run manually.

To perform cluster analysis

1. Load the email thread or near duplicate data using Evidence Processing or Import.
2. On the *Home* page, in the *Case List* panel, click the **Add Evidence** button next to the case.
3. In the *Add Data* dialog, click **Cluster Analysis**.
4. Select a threshold to group the documents based on similarity. The default value is 80%.
5. Click **Start**.

   The data for the email thread appears in the *Conversation* tab in Case Review. The data for Near Duplicate appears in the *Related* tab in Case Review.

   An entry for cluster analysis will appear in the Work List.

5 Editing Evidence

5.1 Editing Evidence Items in the Evidence Tab

Users with Create/Edit case admin permissions can view and edit evidence for a case using the Evidence tab on the Home page.

To edit evidence in the Evidence tab

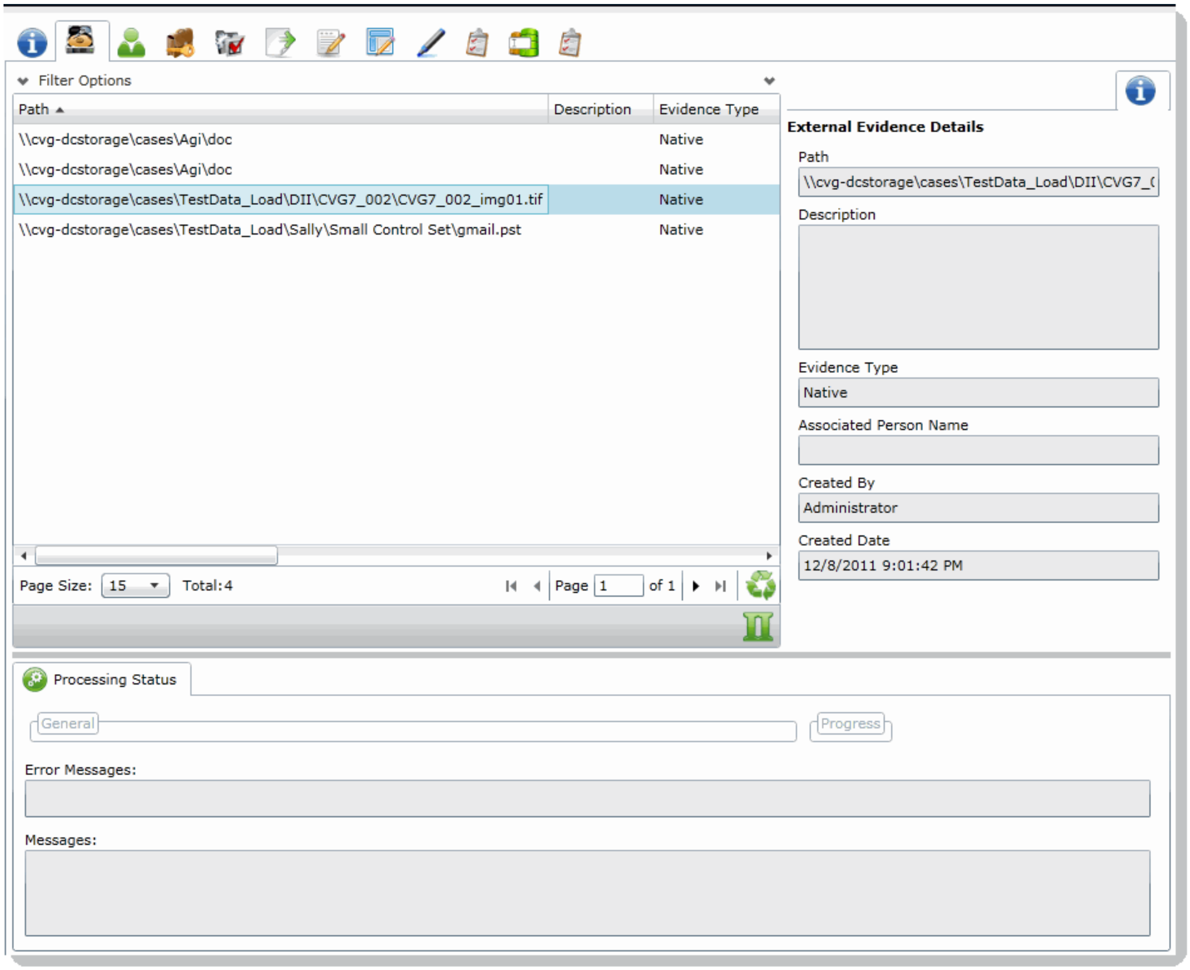
1. Log in as a user with *Create/Edit* case admin permissions.
2. Select a case from the *Case List* panel.
3. Click on the **Evidence** tab.
4. Select the evidence item you want to edit and click the **Edit** (pencil) button.

In the *External Evidence Details* form, edit the desired information.

5.2 Evidence Tab

Users with permissions can view information about the evidence that has been added to a case. To view the *Evidence* tab, users need one of the following permissions: administrator, create/edit case, or manage evidence.

Evidence Tab



Elements of the Evidence Tab

Element	Description
Filter Options	Allows the user to filter the list.
Evidence Path List	Displays the paths of evidence in the case. Click the column headers to sort by the column.
Refresh 	Refreshes Evidence Path List.
Columns 	Click to adjust what columns display in the Evidence Path List.

Elements of the Evidence Tab (Continued)

Element	Description
External Evidence Details	Includes editable information about imported evidence. Information includes: ● That path from which the evidence was imported ● A description of the case, if you entered one ● The evidence file type ● What custodians were associated with the evidence ● Who added the evidence ● When the evidence was added
Processing Status	Lists any messages that occurred during processing.

Reviewing Summation Data

The part describes how to review Summantion data and includes the following sections:

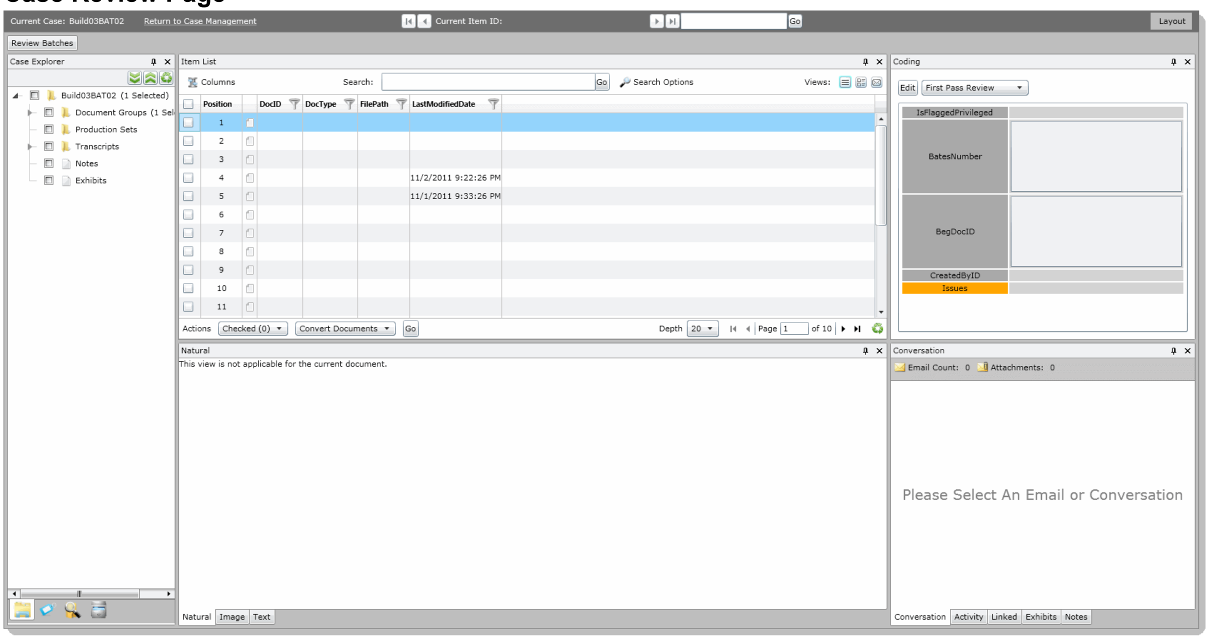
1 Introduction

This guide is designed to aid reviewers in performing tasks in the Case Review interface.

1.1 Introducing the Case Review Page

You can use the Case Review page to search, analyze, filter, code, annotate, and label evidence for a selected case. You have access to Case Review for the cases that you have created or that you are associated with. You can access Case Review by clicking the magnifying glass button next to the case in the Case List panel.

Case Review Page



The Case Review page is made up of a case bar and below that, multiple panels that are customizable.

Case Bar

Elements of the Case Bar

Element	Description
Current Case	The name of the current case.
Return to Case Management 	Click this button to return to the *Home* page.

Elements of the Case Bar

Element	Description
Next and Previous Buttons 	Click previous page or previous document button to move around in the Item List panel. Click next page or next document to move around in the Item List panel.
Current Item ID	Only available if the selected document has been assigned to a Document Group and has a DocID value.
Go to Doc ID 	Enter a DocID and click **Go** to go to that document in the Item List panel. **Note:** If you processed data using evidence processing, you will need to put the documents into a Document group in order to use this feature.
Layout	Click to manipulate panels in the Case Review. Panels can be hidden, shown, dragged, and/or docked to customize the Case Review page for your workflow.

The Case Review page is made up of many panels that can be visible or hidden. The following table briefly overviews each panel available in the Case Review.

Panels in the Case Review

Panel	Description
Activity	Lists the history of actions performed on the selected document. See The Activity Panel on page 28.
Case Explorer	Contains five tabs: filters, explorer, tags, searches and review sets. See The Explore Tab on page 18.
Coding	Use to select and edit coding layout. See The Coding Panel on page 51.
Conversation	Displays email conversation threads. See The Conversation Panel on page 32.
Exhibits	Displays exhibits for the selected transcript. See The Exhibits Panel on page 40.
Facets	Lists available filters to apply to documents. See the Searching documentation.
Family	Lists the family relationships for email documents. See The Family Panel on page 33.
Image	Displays the selected document as an image. You can perform annotations, redactions, and make notes in this view. See Using Image Panel on page 26.
Item List	Lists the filtered evidence for the selected case. This panel also includes the search bar. See Using the Item List Panel on page 19.
Labeling	Lists available labels in the case to apply to evidence. Also displays the selected label for the document currently being viewed. See The Labeling Panel on page 43.
Linked	Two types of documents are displayed in this view: ● Documents manually linked to other documents of the same case ● Documents linked to other documents during import See The Linked Panel on page 35.
Natural View	This viewer displays a file's contents as it would appear normally without having to use the native application. The first time you use this view, you will need to follow the prompts to install the viewer application. See Using the Natural Panel on page 25.

Panels in the Case Review (Continued)

Panel	Description
Notes	Use to display the notes for the currently selected document. See The Notes Panel on page 31.
Production	Displays the history of production. See the Loading Data documentation.
Similar	Use to set relationships between documents. See The Similar Panel on page 29.
Review Batches	Displays review batches. You can check in and check out batches from this panel. See The Review Batches Panel on page 49.
Text	The Text view displays the file's content as text. You can configure the text view so that sentences wrap if they are longer than the panel's width. You can also limit how much text is displayed by setting the Page Depth in characters. See Using the Text Panel on page 27.
Transcript	Displays transcripts for the case. See The Transcript Panel on page 36.

1.1.1 Accessing Case Review

To access the Case Review page

From the case list on the *Home* page, click  next to the desired case.

1.2 Workflow for Case Reviewers

Although there is no formal order in which you process evidence, you can use the following basic workflow as a guide.

Basic Workflow

Step	Task	Link to the tasks
1	After you process a collection, you open the resulting case in Case Review	See Working with Layouts on page 15. See Working with Layouts on page 15.
2	View Data	See Viewing Data in Panels on page 17.
3	Search Documents	See the Searching documentation.
4	Imaging Documents	See Imaging Documents on page 41.
5	Culling Documents	See the Searching documentation.
6	Coding Documents	See Coding Documents on page 48.
7	Annotating Documents	
8	Work with Transcripts	See Viewing Transcripts on page 37. See Annotating Transcripts on page 37. See Viewing Exhibits on page 40. See Searching in Transcripts on page 39.
9	Deleting Documents	See Deleting Documents on page 62.

2 Customizing the Case Review Layout

You can customize the Case Review panels for your workflow. Layouts are specific to the logged-in user.

You can save custom layouts for future use.

You can customize the layout by doing the following:

- Hiding and Showing Panels (page 12)
- Collapsing and Showing Panels (page 13)
- Moving Panels (page 14)
- Resetting Layouts (page 15)
- Saving Layouts (page 15)
- Managing Saved Custom Layouts (page 16)

2.1 Working with Panels

2.1.1 Hiding and Showing Panels

You can hide and show panels to fit your needs.

To hide a panel

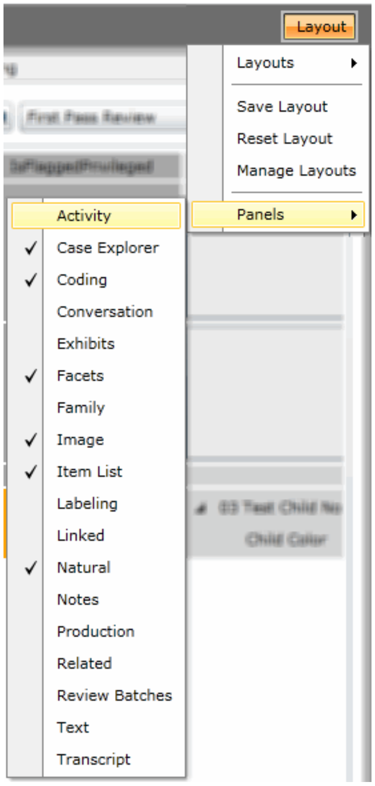
❖ To hide a panel, do one of the following:

- Click the close button (x) on the panel.
- Click **Layout** > **Panes** and uncheck the panel you want to hide.

To show a panel

❖ Click **Layout** > **Panes** and check the panel from the list.

Layout Panel Drop-down



2.1.2 Collapsing and Showing Panels

You can collapse a panel so that it is still open, but not shown unless you hover your mouse over it. This is useful for panels that you want to view less frequently.

To collapse a panel

1. In top-right corner of the panel, click  .
   The panel is collapsed and the name of the panel is displayed in a box on the left side.
   If the panel was in the top half of the page, the collapsed panel name is displayed in the top-left corner. If the panel was in the bottom half of the page, it will be displayed in the bottom-left corner.

Collapsed Panels

2. To view a collapsed panel, mouse over the panel name and the panel will be shown until you move the mouse away from the panel.
3. To un-collapse a panel, view the panel, and in the top-right corner of the panel, click  .

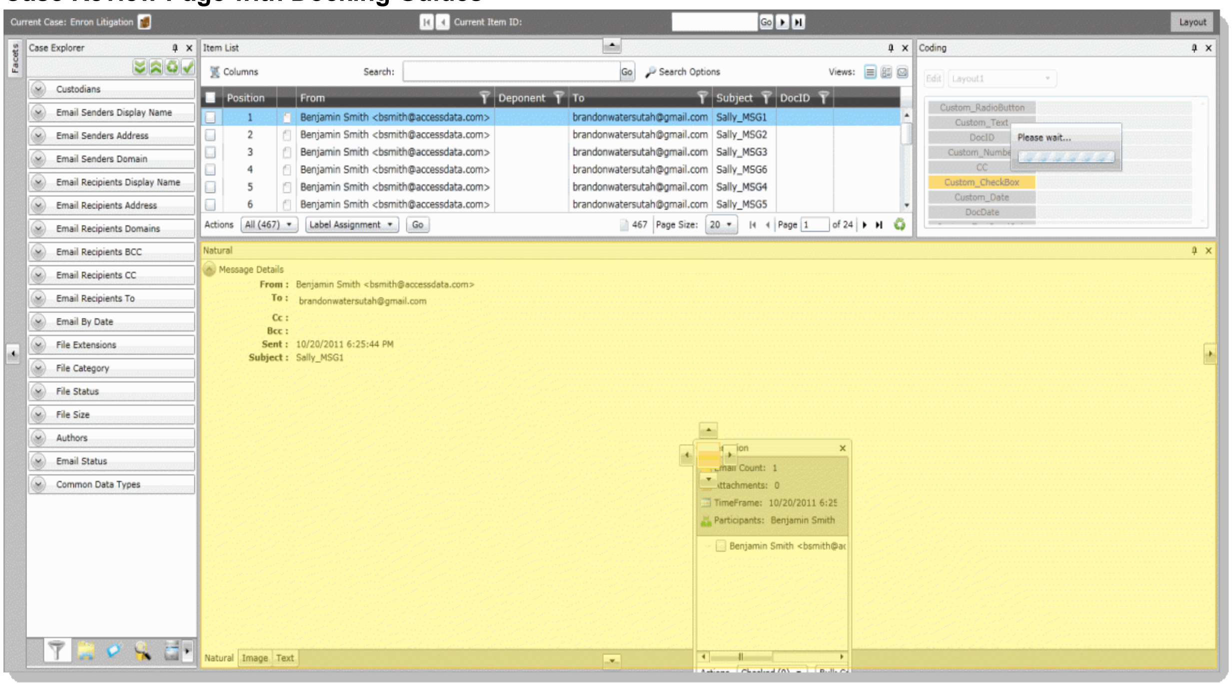
2.1.3 Moving Panels

You can move panels to different locations in the Case Review page. When you move a panel, you can position it in one of the following ways:

To move Case Review panels

1. Click and drag the panel that you want to move.
   Docking guides appear on the page.

Case Review Page with Docking Guides



2. Place the panel by doing one of the following:
   - Floating: Leave the panel floating on top of the page.
   - Docking to a location on the page: Dock the panel by dragging the panel to one of the docking guide arrows and releasing the mouse button.
     There are four page docking guides on the outside of the page.
   - Docking as a tab on another panel: Drag the panel on top of another panel and onto the center of the docking cluster and release the mouse button.
     There is a cluster of four page docking guides on the panel.

2.2 Working with Layouts

2.2.1 Resetting Layouts

If you have hidden, collapsed, or moved panels, you can return to the original layout.

To reset a layout

❖ Select **Layout > Reset Layout**.
If you have modified a custom layout, it will reset to the last saved state.

2.2.2 Saving Layouts

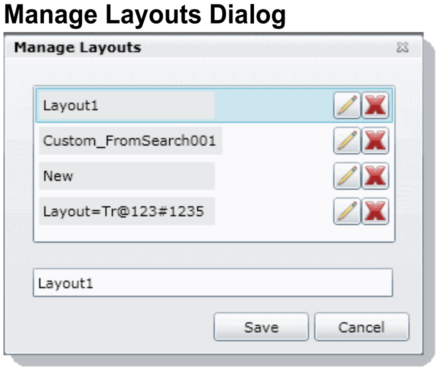
If you have customized the default layout, you can save it as a custom layout. You can save multiple layouts.

To create a second custom layout, you must first return to a default layout, modify it, and then save it. If you make changes to a custom layout, and save it, it will save it as an update.

To save a layout

1. Customize the layout.
2. Click **Layout** > **Save Layout**.

Manage Layouts Dialog



3. Enter the name of the layout and click **Save**.

2.2.3 Selecting a Layout

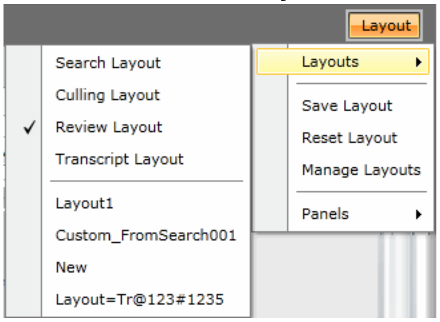
You can view default layouts and custom layouts that you have saved in Case Review. The following are the available default layouts:

- Search Layout: Designed to aid reviewers in searching documents
- Culling Layout: Designed to aid reviewers in culling documents
- Review Layout: Designed to aid reviewers in viewing documents
- Transcript Layout: Designed to aid reviewers in working with transcripts

To select a layout

❖ In Case Review, select **Layout > Layouts >** and select a layout.

Default and Custom Layouts



Default layouts appear above the line and custom layouts appear below the line.

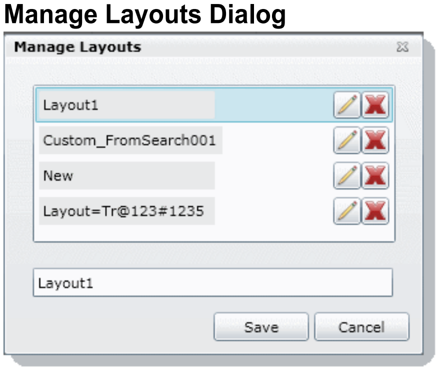
2.2.4 Managing Saved Custom Layouts

You can rename and delete custom layouts that you have saved. You cannot delete the currently selected layout using the Manage Layouts dialog.

To manage a saved custom layout

1. Select **Layout > Manage Layouts**.

Manage Layouts Dialog



2. To rename a layout, select the layout, and enter a new name.
3. To delete a layout, click the X next to the layout, and click **OK**.
4. Click **Save**.

3 Viewing Data

3.1 Viewing Data in Panels

The following panels allow you to view documents in Case Review.

Document Viewing Panels

Panel	Links
Explorer	See The Explore Tab on page 18.
Item List	See Viewing Documents in the Item List Panel on page 20.
Natural	See Using the Natural Panel on page 25.
Image	See Using Image Panel on page 26.
Text	See Using the Text Panel on page 27.

Note: The language identification feature only works in the following categories: documents, spreadsheets, and email

The following panels allow you to view data about the selected document..

Document Data Panels

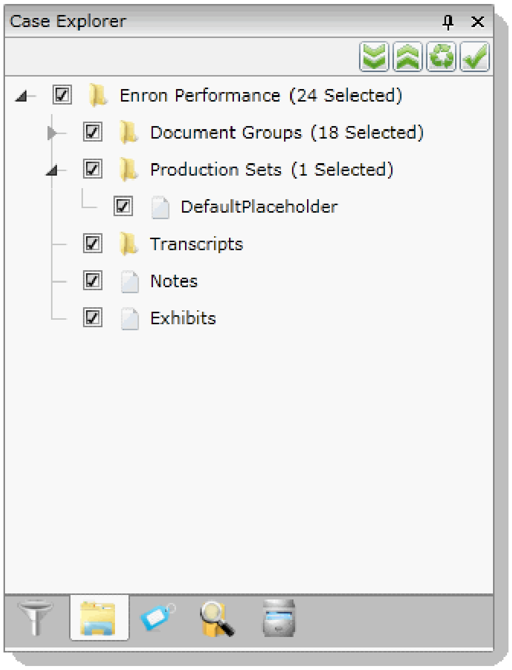
Panel	Link
Activity	See The Activity Panel on page 28.
Similar	See The Similar Panel on page 29.
Production	See The Production Panel on page 30.
Notes	See The Notes Panel on page 31.
Conversation	See The Conversation Panel on page 32.
Family	See The Family Panel on page 33.
Linked	See The Linked Panel on page 35.

3.2 The Explore Tab

The Explore tab in the Case Explorer panel can be used to search by the following items:

- Document Groups
- Production Sets
- Transcripts
- Notes
- Exhibits

Document Tree



When you check an item in the document tree, all documents in that category will be included in your search query.

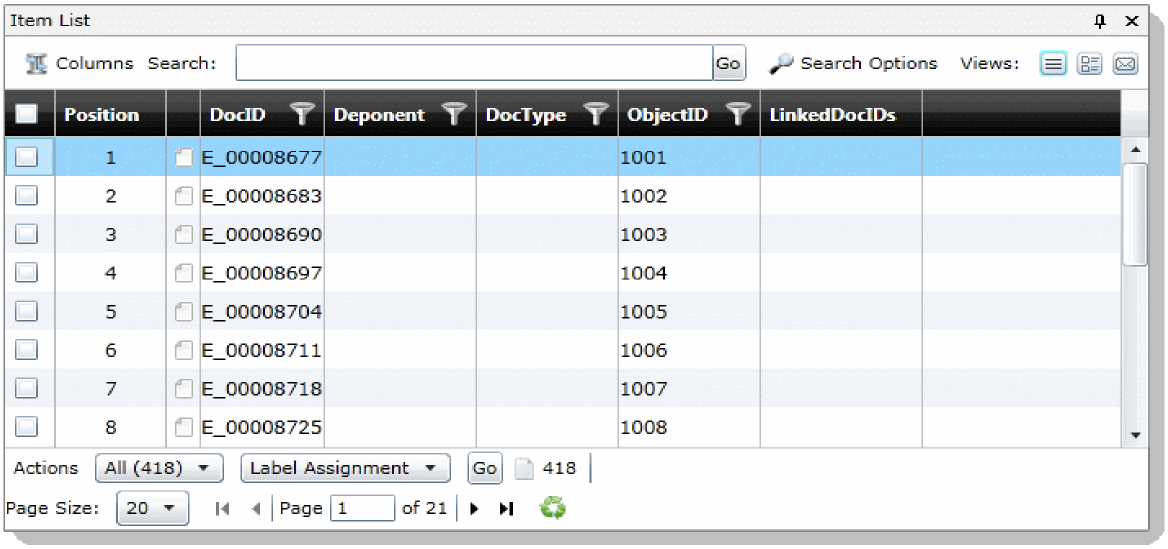
Elements of the Document Tree

Element	Description
Document Groups	Check to include document groups in your search. Right-click to create document groups.
Production Sets	Check to include production sets in your search. Right-click to create productions sets.
Transcripts	Check to include transcripts in your search. Right-click to create transcript groups, upload transcripts, update transcript, and upload exhibits.
Notes	Check to include notes in your search.
Exhibits	Check to include exhibits in your search.

3.3 Using the Item List Panel

The Item List Panel lists the filtered evidence for the selected case. This panel also includes the search bar and the ability to perform mass actions.

Item List Panel



Elements of the Item List Panel

Element	Description
Columns Button	Click to select the columns visible in the Item Grid.
Search Field	Enter search terms to perform a quick search of documents checked in the Document Tree. Results appear in the Item Grid.
Go Button	Click to execute your quick search.
Search Options	Select to perform the following actions: Clear Searches, Advanced Search, Expansion, Settings, and Generate Search Reports.
Views	The following view buttons are available: Grid view, Summary view, and Conversation view.
Actions (Checked)	Select Checked to perform mass actions on documents checked in the Item Grid. Select All to perform mass actions on all documents in the Item Grid.
Actions (Convert)	Select the mass action that you want to perform on the documents in the Item Grid. The following actions are available: Convert Documents, Label Assignments, Delete, and Bulk Coding.
Go Button (bottom of panel)	Click to execute the selected mass action.
Depth	Select the number of documents you want visible in the Item List.
Page	Lists the page you are on and the number of pages. Click the next arrow to see the next page.

Elements of the Item List Panel (Continued)

Element	Description
Refresh	Click the refresh button to update the Item List.

The following are the default columns in the Grid View.

Elements of the Item List Panel in Grid View

Element	Description
Position Column	Lists the position of the evidence item.
Source File Column	Displays an icon of the source file, based on the file extension, for the evidence item.
Labels Column	Select a label to apply to the evidence See Applying Labels to Single Documents on page 44.
Object Name Column	Lists the name of the evidence item.
Custodian Column	Lists the custodian for the evidence item.
Extension Column	Lists the extension for the evidence item.
Path Column	Lists the path for the evidence item.
Create Date Column	Lists the date the evidence file was created.
Last Access Date Column	Lists the last date the evidence file was accessed.
Modify Date	Lists the date that the evidence file was last modified.
Logical Size	Lists the size of the evidence file.
File Type	The type of file.

3.3.1 Viewing Documents in the Item List Panel

The *Item List* panel displays the documents in the case in three different formats:

- Grid view: See Using Grid View on page 21.
- Summary view: See Using Summary View on page 22.
- Conversation view: See Using Conversation View on page 22.

To view documents in the Item List panel

1. In *Case Review*, show the *Case Explorer* and *Item List* panel if they are not already showing.
2. In *Case Explorer* panel, check folders in the *Explore*, *Tags*, or *Review Sets* tabs that contain documents that you want to view.
3. Click the **Apply** (check mark) button in the *Case Explorer* panel.
   The documents in the selected folders appear in the *Item List* panel.
   See Using the Item List Panel on page 19.

3.3.2 Using the Quick Filter

The Item List panel includes a Quick Filter that you can use to quickly refine the list of evidence.

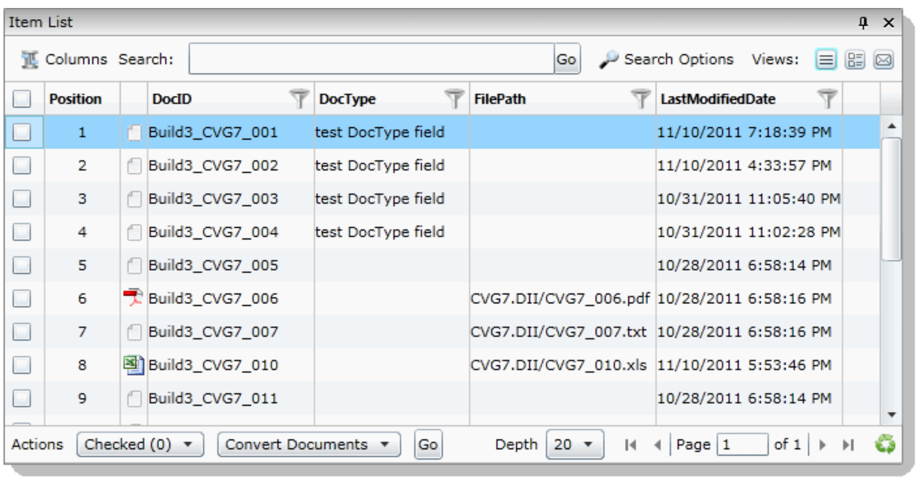
Quick Filters

Filter	Description
Show Duplicates	Enabling this will show duplicate items.
Show Folders	Enabling this will show folder items.
Show eDiscovery Refinement	Enabling this shows extra files that may not be important. For example, this includes embedded files, such as XML, RELS, and graphics that are embedded in office documents.

3.3.3 Using Grid View

The default view in the Item List panel is the grid view. Grid view is a grid that displays each document.

Grid View



In the Grid and Summary view, you can perform the following tasks.

Tasks Performed in the Grid View

Task	Link
Search Documents	See the Searching documentation.
Bulk Coding	See Coding Multiple Documents on page 53.
Convert Documents	See Imaging Documents on page 41.
Assign Labels	See Applying Labels to Multiple Documents on page 45.
Delete Documents	See Deleting Documents on page 62.

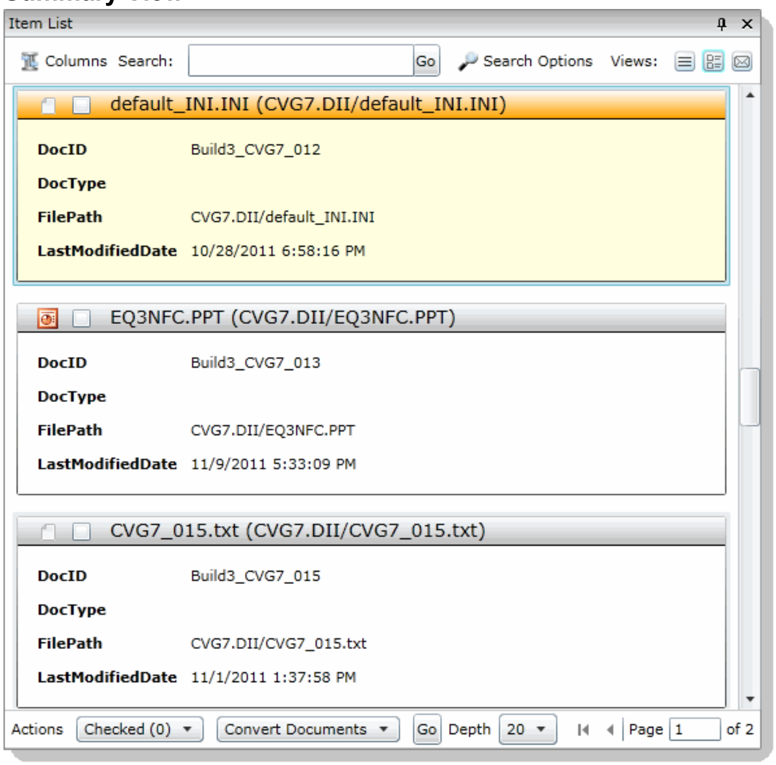
3.3.4 Using Summary View

The Summary view displays a detail of the documents.

To access Summary view

❖ In the Item List panel, click the Summary View button .

Summary View



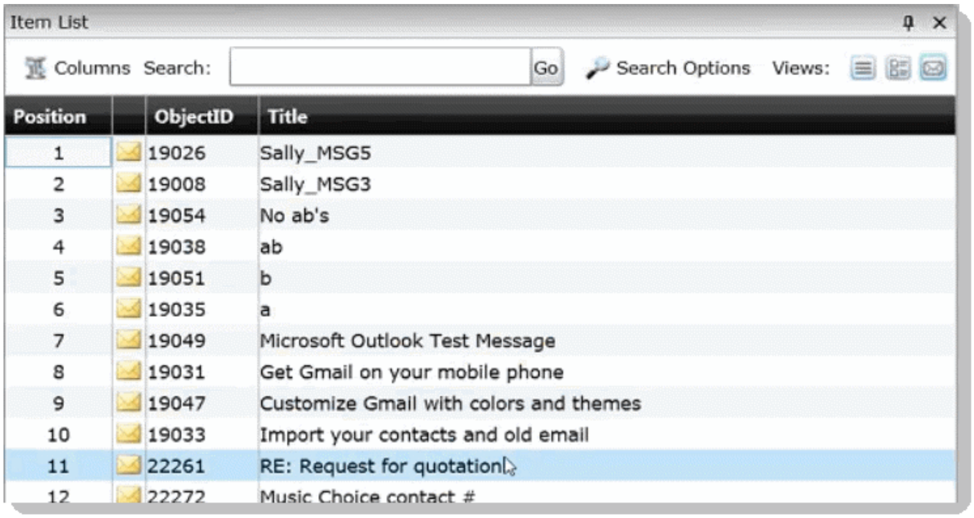
3.3.5 Using Conversation View

Conversation view displays all the conversation threads for emails.

To access the conversation view

❖ In the Item List panel, click the Conversation View button .

Conversation View



3.3.6 Using Columns in the Item List Panel

You can customize, sort, and reposition the columns of information in the *Item List* panel in Grid.

3.3.6.1 Moving Columns in Grid View

You can rearrange columns in the Grid view in the *Item List* panel in any order you want. Some columns have pre-set default positions. Column widths are also sizable.

To move columns

- ❖ In the Grid view, click and drag columns to the position you want them.

3.3.6.2 Sorting Documents in Grid View by Column

You can sort information under a column heading in ascending or descending order.

To sort Grid view by column

- ❖ In Grid view, click the column heading.

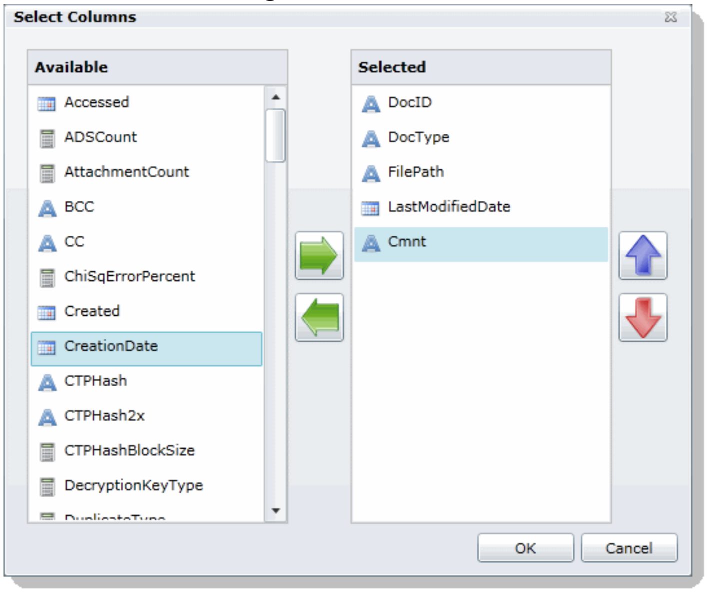
3.3.6.3 Selecting Visible Columns

You can select the columns that you want visible in the Grid view. Case Managers can create custom columns in the Custom Fields tab on the home page.

To customize visible columns

1. In the *Item List* panel in *Grid* view, click the **Columns** button and select **Select Columns**.

Select Columns Dialog



2. Click the right arrow to add columns to the grid and the left arrow to remove them from the grid.
3. Organize the order of the columns by clicking the up and down arrows.

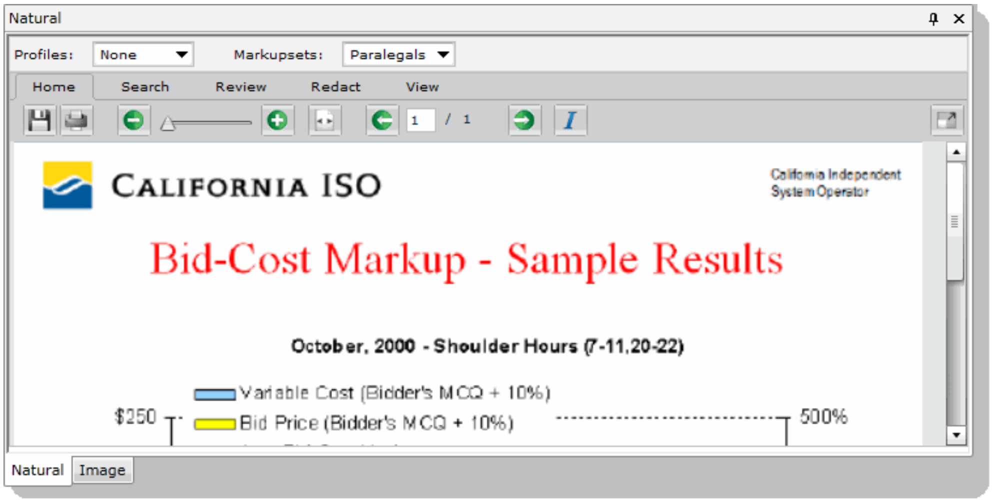
Note: The first three columns in the Item List Grid cannot be hidden or moved.

3.4 Using the Natural Panel

The Natural panel displays a file's contents as it would appear normally without having to use the native application.

The first time you use this, you will need to follow the prompts to install the viewer application.

Natural Panel



Elements of the Natural Panel

Element	Description
Profiles	Contains the highlight profiles for the logged-in user.
Markup Sets	Contains the markup sets for the logged-in user.
Home Tab	Contains a Save button, Print button, zoom in and out buttons and slider bar, Fit to width button, Previous Page button, Next Page button, and Select Text tool.
Search Tab	Contains search field and search button.
Review Tab	Contains a Save button, Print button, Select Text tool, Transparent Rectangle tool, Color tool, Delete button, and Toggle View Off button.
Redact Tab	Contains a Save button, Filled Rectangle tool, Select Text tool, Delete button, and Toggle View Off button.
View Tab	Fit to Width button, Rotate tools, and Thumbnail view button.
Go Fullscreen Button	Click to expand the image to the full screen.

To view documents in the Natural view

1. In *Case Review*, select a file in the *Item List* panel.
2. Click on the **Natural** tab.

   If the Natural panel isn't showing, select the panel from the Layouts drop-down.

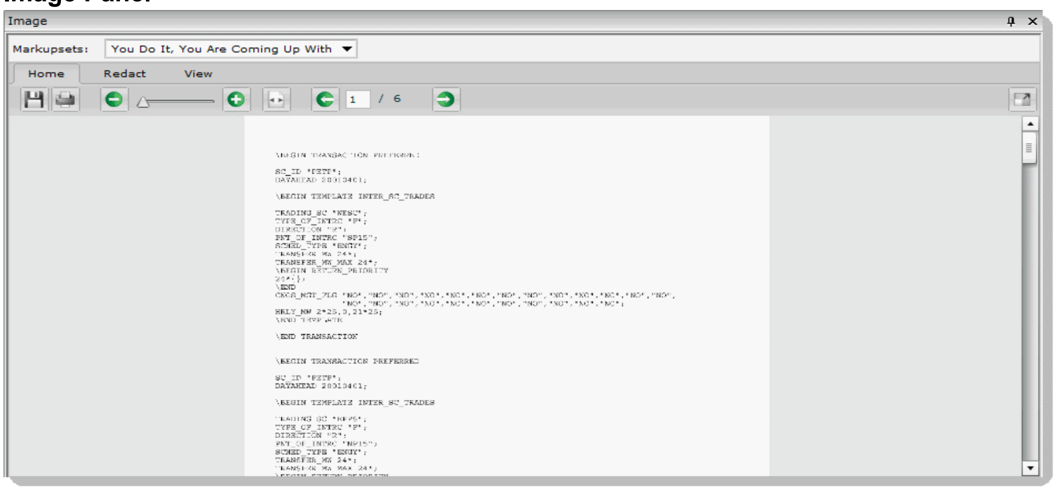
3.5 Using Image Panel

The Image view displays image documents and electronic documents that have been converted into images. in the Natural panel.

3.5.1 Image Panel

The Image panel displays the selected document as an image. You can perform annotations and make notes in this view.

Image Panel



Elements of the Image Panel

Element	Description
Markup Sets	Select a predefined markup set to view specified users annotations.
Home Tab	Contains the following buttons: Save, Print, Zoom In, Zoom Out, Fit to Width, Previous Page, and Next Page.
Redact Tab	Contains the following buttons: Save, Print, Filled Rectangle, Transparent Rectangle, Delete Redaction, and Toggle Redaction On/Off.
View Tab	Contains the following buttons: Fit to Width, Rotate Single Page, Rotate All Pages, and Thumbnail View.
Go To Full Screen	Click to make the image a full screen.

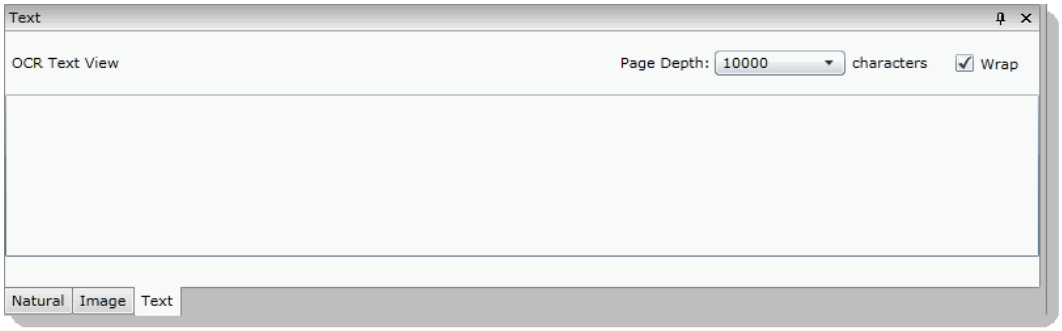
To view documents in Image view

1. In *Case Review*, select a file in the *Item List* panel.
2. Click on the **Image** view tab.
   If the Image panel isn't showing, select the panel from the Layouts drop-down.

3.6 Using the Text Panel

The Text panel in Case Review displays the file's content as text. You can configure the text view so that sentences wrap if they are longer than the panel's width. You can also limit how much text is displayed by setting the Page Depth in characters.

Text Panel



Elements of the Text Panel

Element	Description
Page Depth	Select the number of characters you want visible in the Text Panel.
Wrap Check Box	Check to wrap the text in the panel.

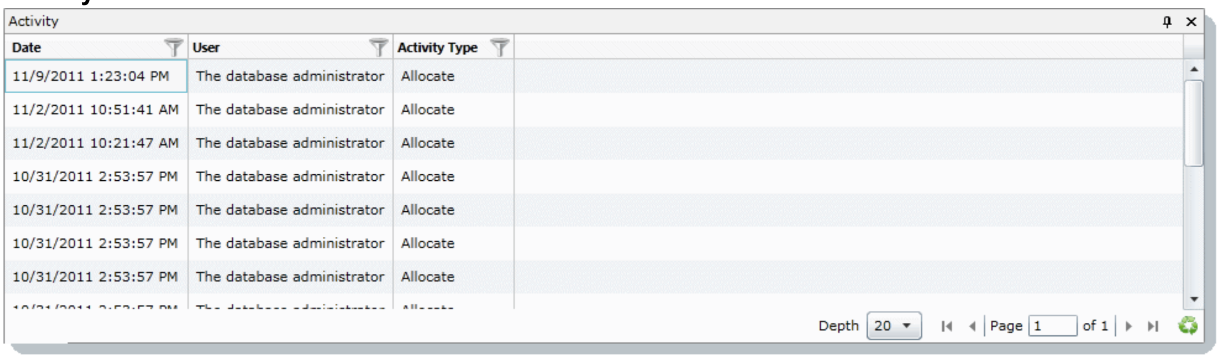
To view documents in Text view

1. In *Case Review*, select a file in the *Item List* panel.
2. Click on the **Text** view tab.
   If the Text panel isn't showing, select the panel from the Layouts drop-down.

3.7 The Activity Panel

The *Activity* panel on the *Case Review* page lists the history of actions performed on the selected document.

Activity Panel



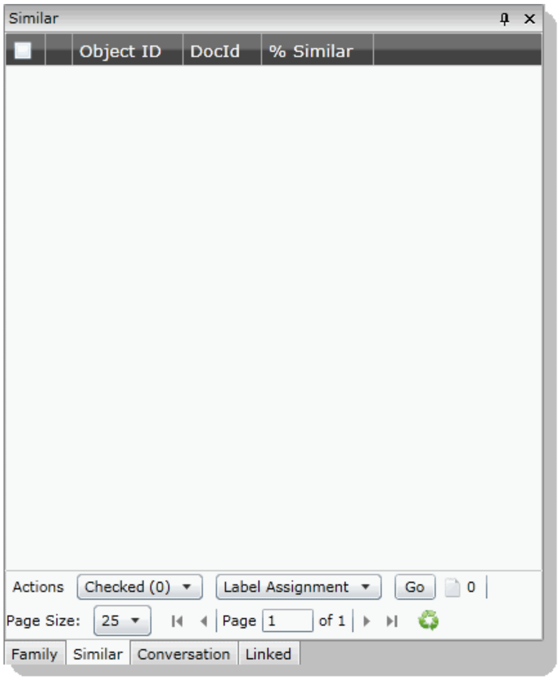
Elements of the Activities Panel

Element	Description
Date Column	Displays the date of the action performed.
User	Displays the user that performed the action.
Activity Type	Displays the type of activity that was performed.

3.8 The Similar Panel

The Similar panel in Case Review can be used to set relationships between documents.

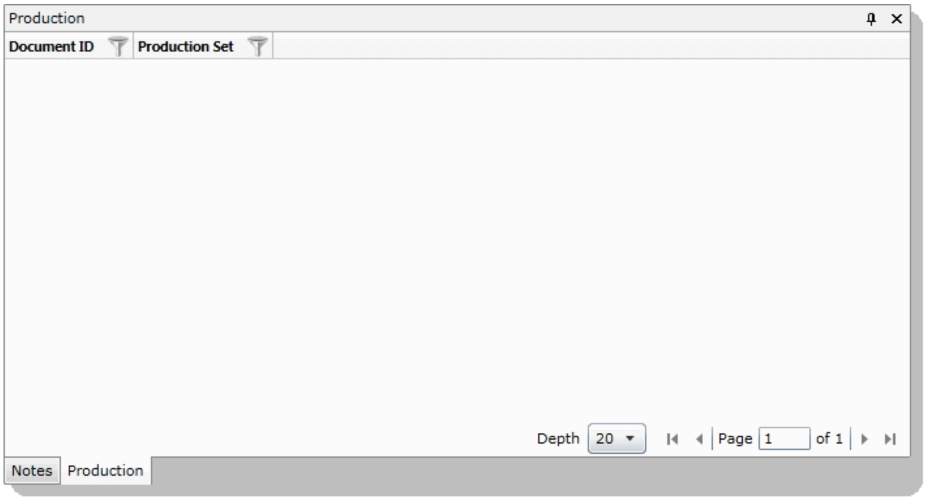
Similar Panel



3.9 The Production Panel

The *Production* panel in *Case Review* displays the history of production for the case.

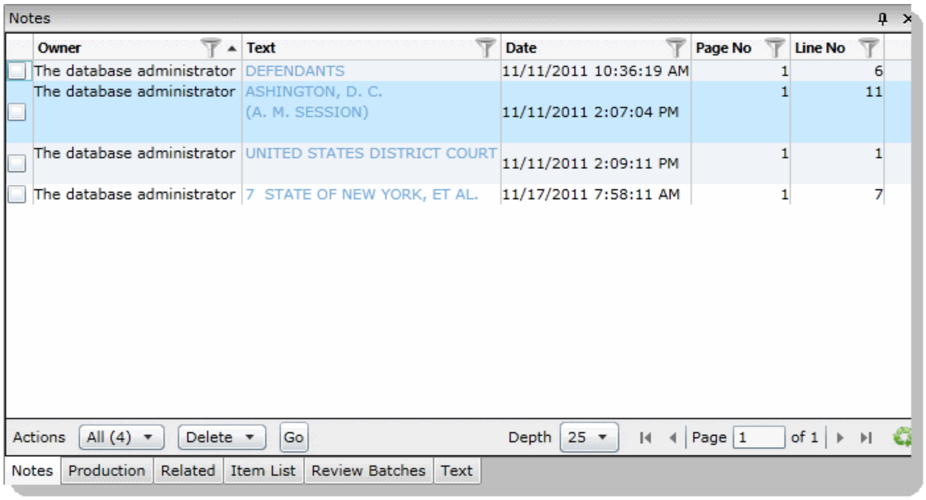
Production Panel



3.10 The Notes Panel

The Notes panel in Case Review can be used to view, navigate, and delete notes.

Notes Panel



Elements of the Notes Panel

Element	Description
Owner Column	Lists the author of the note.
Texts Column	Displays the text of the note.
Date Column	Displays the date that the note was created.
Page No Column	Displays the page on which the note was made.
Line No Column	Displays the line number on which the note was made.
Actions	Expand the first actions drop-down and select one of the following options: ● All: To include all notes visible in the panel in the action ● Checked: To include checked notes in the action ● Unchecked: To include all the unchecked notes in the action ● This Page: To include all the notes on the current page in the action
Actions Cont...	Select an action to perform from the drop-down.
Go Button	Click to execute the selected action.
Depth	Select the number of documents you want visible in the Linked Panel.
Page	Lists the page you are on and the number of pages. Click the next arrow to see the next page.
Refresh	Click the refresh button to update the Linked Panel.

3.11 The Conversation Panel

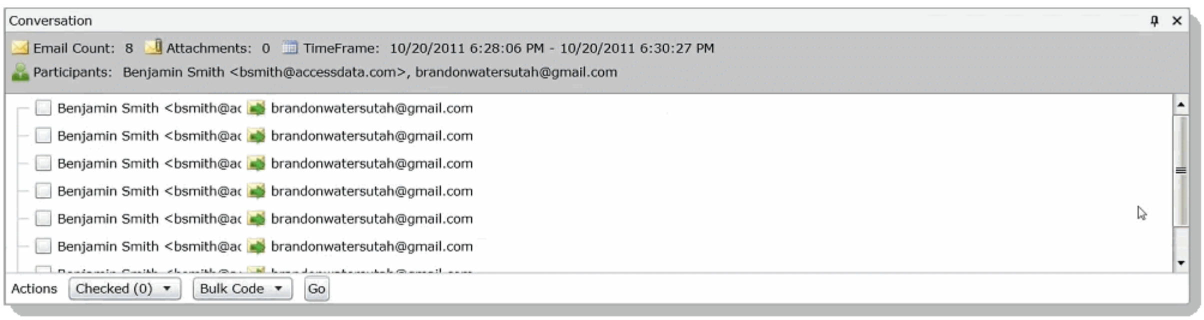
The Conversation panel in Case Review displays email conversation threads and emails from a cluster. The Conversation panel shows any compilation of related messages that makes up a conversation. The displayed threads are those emails that are sent and answered or answered emails with the originals and any string of threads that went back and forth for each message.

Emails are organized by cluster in the conversation panel.

- The email clusters are displayed in a hierarchical order with the original message displayed first, followed by subsequent messages for any email that have a conversational ID.
- There may be an email in the cluster that is from the thread which is not necessarily a part of the cluster since they are a part of the thread.
- Emails may be identified because they are in the cluster, but not a part of the thread.
- Clusters are green.
- Threaded items are black.
- Significant items in a cluster are marked with a star.

You can use the *Filters* panel to refine the list by: who the email was sent to, who the email is from, and a date range.

Conversation Tab



Elements of the Conversation Tab

Element	Description
Email Count	Displays the number of emails in the thread.
Attachments	Displays the number of attachments.
Time Frame	Displays the time frame when the emails were sent.
Participants	Displays the email address of the email participants.
Actions Drop-down Checked	Select Checked or All to perform mass actions.
Actions Drop-down Bulk Code	Select the type of mass action that you want to perform.
Go	Click to start the mass actions.

3.12 The Family Panel

The Family panel in Case Review lists the family relationships for email documents. The Family panel shows the email message and any attachments to the message.

The Family panel will only display related documents if you select the parent document. If you select a child document you will not see the related documents.

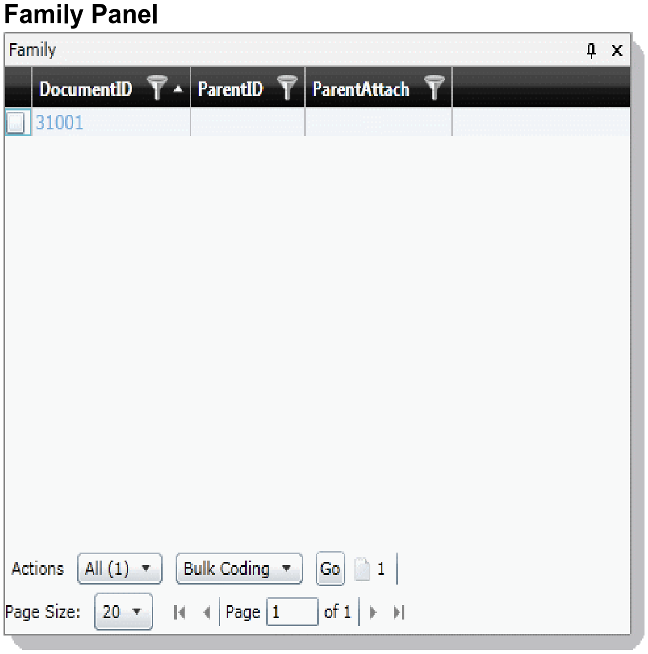
For both the message file and the attachments, you can do the following:

- Click the item to view the item in the Natural panel.
- Apply labels.
  See Applying Labels to Single Documents on page 44.

When you click the child attachment in the *Family* panel, that child document will be displayed in the document view panel. Also, the Current Item ID will also change to reflect the child's record number so that you can select the hyperlink and open the child record in its native format.

However, the *Item List* panel will not change to highlight the child's record; it will still remain on the parent's record.

Family Panel



Elements of the Family Panel

Element	Description
DocumentID	Displays the DocID for the documents in the same family as the selected document.
ParentID	Displays the DocID for the parent document.
ParentAttach	Displays whether the parent document has attachments.

Elements of the Family Panel (Continued)

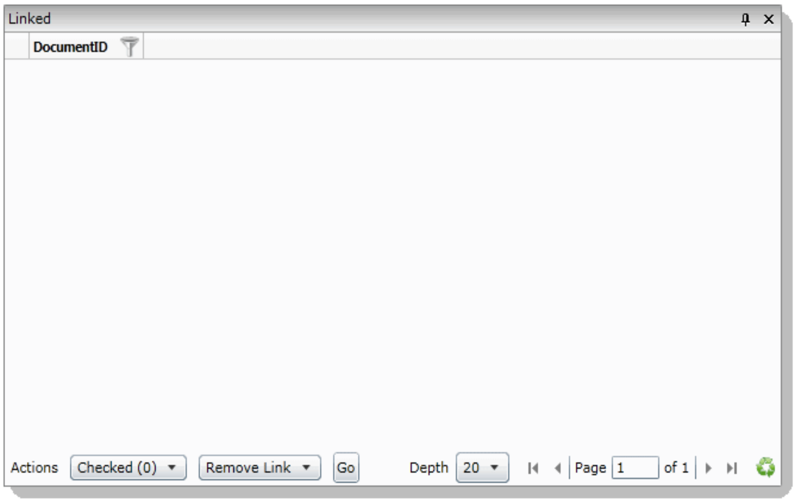
Element	Description
Actions Drop-down All	Select to perform a mass action.
Action Drop-down	Select the action that you want to perform.
Go	Click to start the mass action.

3.13 The Linked Panel

The Linked panel in Case Review displays two types of documents:

- Documents manually linked to other documents of the same case
- Documents linked to other documents during import

Linked Panel



Elements of the Linked Panel

Element	Description
Actions (Checked)	Select Checked to perform actions on documents checked in the Linked Panel. Select All to perform actions on all documents in the Linked Panel.
Actions (Convert)	Select the action that you want to perform on the documents in the Linked Panel. The following actions are available: Link Documents and Remove Links.
Go Button	Click to execute the selected action.
Depth	Select the number of documents you want visible in the Linked Panel.
Page	Lists the page you are on and the number of pages. Click the next arrow to see the next page.
Refresh	Click the refresh button to update the Linked Panel.

4 Working with Transcripts and Exhibits

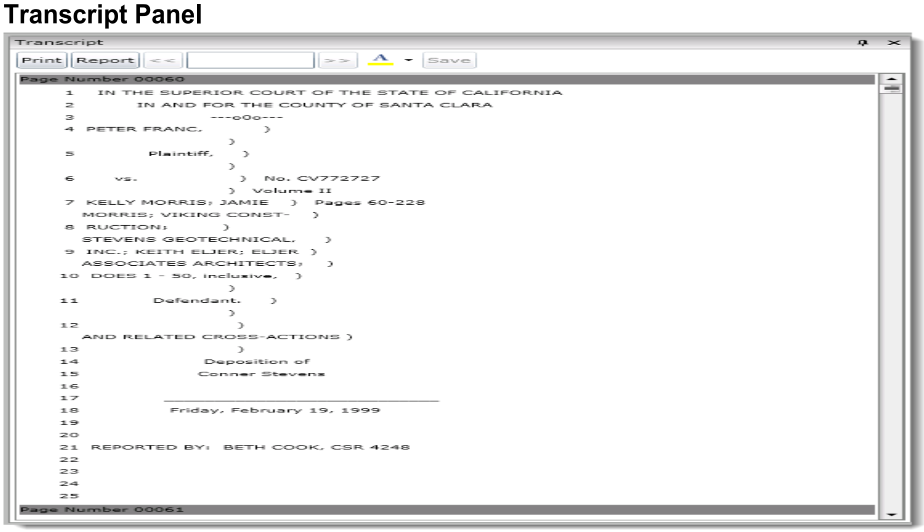
4.1 Working with Transcripts

Reviewers can view and annotate transcripts using the *Transcripts* panel in *Case Review*. Case managers with the Upload Exhibits, Upload Transcripts, and Manage Transcripts permissions can upload transcripts, create transcript groups, grant transcript permissions to users, and upload exhibits.

4.1.1 The Transcript Panel

The Transcripts panel in Case Review displays transcripts for the case. You can add and edit notes in the transcript view.

Transcript Panel



Elements of the Transcript Panel

Element	Description
Print Button	Click to print the transcript.
Report	Click to print a report of the transcript with notes and highlights optionally included.
Search Field	Enter text that you want to search for in the selected transcript.
Previous Button	Click to go to the previous hit of the search term.
Next Button	Click to go to the next hit of the search term.

4.1.2 Viewing Transcripts

Anyone can view transcripts in the *Transcripts* panel of the *Case Review*.

To view transcripts

1. In the *Case Review*, ensure the *Case Explorer, Item List* and *Transcript* panels are showing.
2. In the *Case Explorer*, in the *Document Tree*, expand the *Transcript* folder.
3. Select the transcript group you want to view.
4. In the *Item List* panel, select the transcript you want to view.
   The transcript appears in the *Transcript* panel.

4.1.3 Annotating Transcripts

Reviewers with the *Add Annotations* permission can annotate transcripts in the *Transcripts* panel.

You can add the following annotations to a transcript:

- See Adding a Note to a Transcript on page 37.
- See Adding Highlights to a Transcript on page 38.
- See Adding Links to a Transcript on page 38.

4.1.3.1 Adding a Note to a Transcript

Reviewers with the Add Notes permission can add notes to transcripts in the *Transcripts* panel of the *Case Reviewer*. Notes can be viewed and deleted from the *Notes* panel for users with the View Notes and Delete Notes permission.

See The Notes Panel on page 31.

To add a note to a transcript

1. View a transcript in the Transcripts panel.
   See Viewing Transcripts on page 37.
2. In the Transcripts panel, highlight the text to which you want to add a note.
3. Right-click and select **Add Note**.
4. In the *Create Note View* dialog, enter a note in the *Note* field.
5. Select a *Date* for the note.
6. (Optional) Check issues related to the note.

   Note: If you check an issue that has a color associated with it, the selected text will be highlighted that color.

7. Check the groups with which you want to share the note.
8. Click **Save**.

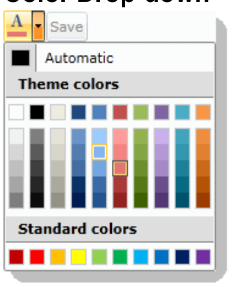
4.1.3.2 Adding Highlights to a Transcript

Reviewers with the Add Annotations permission can add highlights to a transcript in the *Transcripts* panel of *Case Review*.

To add a highlight

1. Log in as a user with Add Annotations permission.
2. Click the *Case Review* button  in the *Case List* panel next to the case.
3. View a transcript in the *Transcripts* panel.
   See Viewing Transcripts on page 37.
4. In the *Transcripts* panel, expand the color drop-down and select a color for your highlight.

Color Drop-down



5. Highlight the text and a highlight is added.

4.1.3.3 Adding Links to a Transcript

Reviewers with the Add Annotations permission can add links to transcripts in the *Transcripts* panel of *Case Review*.

To add a link

1. Log in as a user with Add Annotations permission.
2. Click the *Case Review* button  in the *Case List* panel next to the case.
3. View a transcript in the *Transcripts* panel.
   See Viewing Transcripts on page 37.
4. In the Transcripts panel, highlight the text to which you want to add a link.
5. Right-click and select **Add Link**.
6. In the *Add Linked Document* dialog, in the *Search* field, enter the DocID of the document you want to link to.
7. Press the tab button to activate the *Go* button and click **Go**.
8. Select the document you want link to from the search results.
9. Click **OK**.

4.1.4 Searching in Transcripts

You can search within a transcript by keyword using the Transcripts panel.

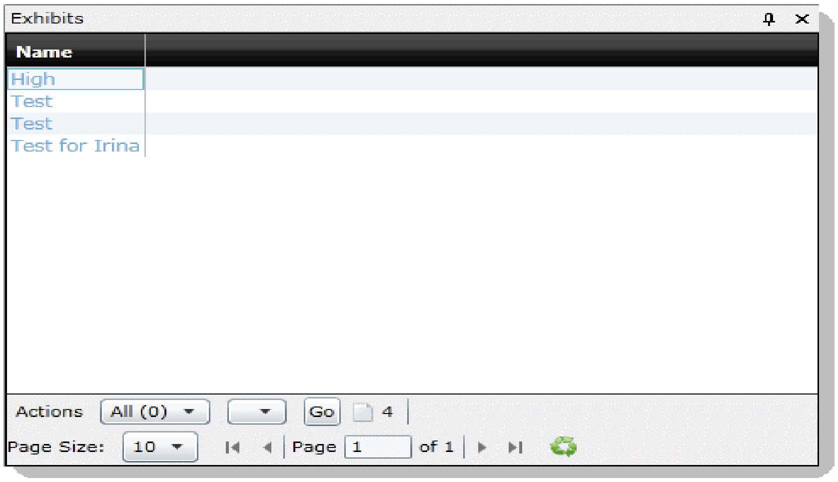
To search within a transcript

1. View a transcript in the *Transcripts* panel.
   See Viewing Transcripts on page 37.
2. Enter a keyword in the search field.
3. Click the Next button to see the first instance of the keyword. The keyword is highlighted in the transcript.
4. Click the Next or Previous buttons to see more instances of the keyword.

4.2 The Exhibits Panel

The Exhibits tab in the Case Review displays the exhibits for the selected transcript.

Exhibits Tab



Elements of the Exhibits Tab

Element	Description
Name	Lists the name of the exhibit for the selected transcript.
Actions Drop-down All	Select to perform a mass action.
Action Drop-down	Select the action that you want to perform.
Go	Click to start the mass action.

4.2.1 Viewing Exhibits

You can use the Exhibits panel to view the list of exhibits for the selected transcript. Exhibits are imported by the case manager.

To view exhibits

1. In the *Case Review*, ensure the *Case Explorer*, *Exhibits*, *Item List*, and *Natural* panel are showing.
2. Select a transcript group in the *Case Explorer*.
3. In the *Item List*, select a transcript.
4. In the *Exhibits* panel, select an exhibit.
   The exhibit is displayed in the *Natural* panel.

5 Imaging Documents

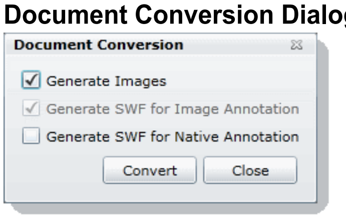
Reviewers with the Imaging permission can convert multiple documents to an image using the *Imaging* mass action in the *Item List* panel.

5.1 Converting a Document to an Image

To convert documents to an image

1. Log in as a user with Imaging permission.
2. Click the *Case Review* button  in the *Case List* panel next to the case.
1. In the *Case Review*, ensure the *Item List* panel is showing.
2. In the *Item List* panel, check the documents that you want to convert to images. Skip this step if you are converting all the documents to images.
3. In the first *Actions* drop-down at the bottom of the panel, do one of the following:
   - Select **Checked** to convert all the checked documents.
   - Select **All** to convert all documents, including documents on pages not visible.
4. In the second *Actions* drop-down, select **Imaging**.
5. Click **Go**.

Document Conversion Dialog



6. In the *Document Conversion* dialog, check **Generate Images** to create TIFFs.
7. Check **Generate SWF for Native Annotation** if you want to create a SWF file where the you can annotate in the Natural panel.
8. Check **Generate SWF for Image Annotation** if you want to be able to do annotations on the created image file.
9. Click **Convert.**

   The job is sent to the Work List where the case manager can complete the job and convert the documents to images.

6 Applying Tags

6.1 The Tags Tab

The *Tags* tab in the *Case Explorer* can be used to create labels, create issues, and view categories. You can view documents assigned to tags using the Tags tab in the Case Explorer.

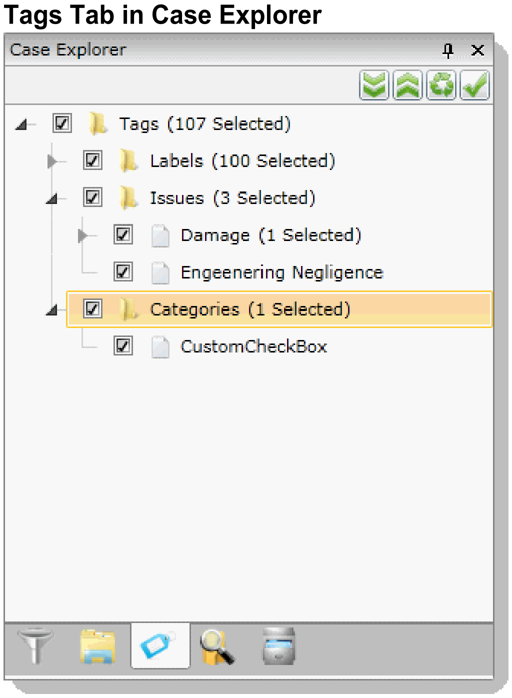
See Viewing Documents with a Label Applied on page 47.

See Viewing Documents with an Issue Coded on page 47.

See Viewing Documents with a Category Coded on page 47.

Case Managers can create labels and issues for the case reviewer to use.

Tags Tab in Case Explorer



Elements of the Tags Tab

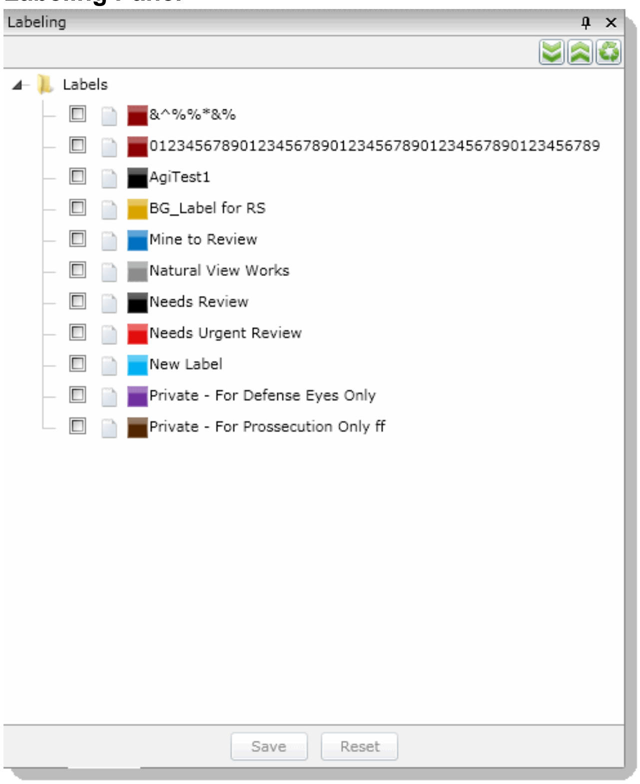
Elements	Description
Tags	Contains the Labels, Issues, and Categories folders.
Labels	Contains all the existing labels. Right-click to create a new label for the case.
Issues	Displays all the existing issues. Right-click to create a new issue for the case.
Categories	Displays all the existing categories for the case. Right-click to create category values.

6.2 The Labeling Panel

The Labeling panel in Case Review can be used to apply labels to documents. You can organize your documents by applying labels using the Labeling panel. The Labeling panel allows you to apply labels to documents one at a time.

See Applying Labels to Multiple Documents on page 45.

Labeling Panel



Elements of the Labeling Tab

Element	Description
Labels Folder	Expand to see the labels created by the case manager.
Collapse All Button	Click to collapse all the folders.
Expand All Button	Click to expand all the folders.
Refresh	Click to refresh the label list.
Save	Click to apply the selected labels to the selected document.
Reset	Click to reset the labels to their original condition.

6.3 Applying Labels to Single Documents

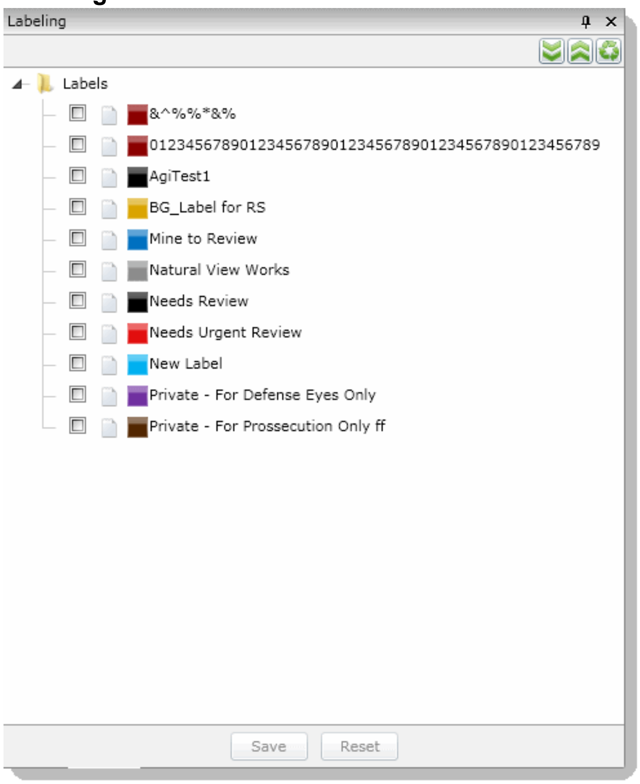
You can apply labels to documents one at a time by using the Labeling panel. Labels can be created by the case manager.

Note: Production set records cannot be labeled.

To apply labels to single documents

1. In the *Case Review*, ensure the *Labeling* and *Item List* panels are showing.

Labeling Panel



2. In the *Item List* panel, highlight the document to which you want to apply a label.
3. In the *Labeling* panel, check the label(s) that you want to apply and click **Save**.

6.3.1 Removing Labels from a Single Document

You can remove labels from a single document using the Labeling panel.

To remove labels from a single document

1. In the *Case Review*, ensure the *Labelling* and *Item List* panels are showing.
2. In the *Item List* panel, highlight the document from which you want to remove a label.
3. In the *Labeling* panel, uncheck the label(s) that you want to remove and click **Save**.

6.4 Applying Labels to Multiple Documents

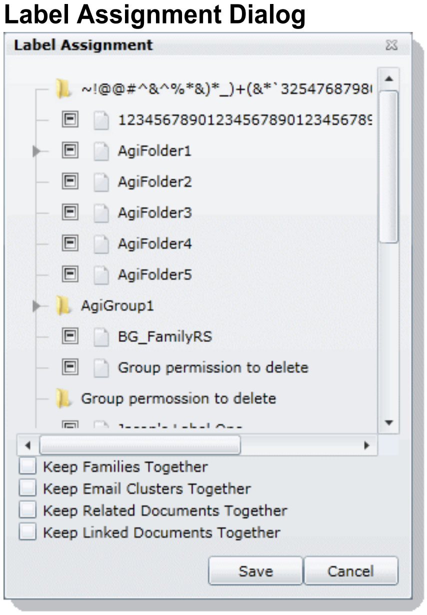
You can apply labels to multiple documents at once using the mass actions in the Item List panel. Labels can be created by the case manager.

Note: Production set records cannot be labeled.

Applying labels to multiple documents

1. In the *Case Review*, ensure the *Item List* panel is showing.
2. Check the documents to which you want to apply labels. If applying labels to all documents, skip this step.
3. In the first *Actions* drop-down at the bottom of the panel, do one of the following:
   - Select **Checked** to apply labels to all the checked documents.
   - Select **All** to apply labels to all documents, including documents on pages not visible.
4. In the second *Actions* drop-down, select **Label Assignment**.
5. Click **Go**.

Label Assignment Dialog



6. Check the labels that you want to assign to the documents.

   Note: Boxes with a dash (-) indicate that one or more (but not all) of the documents are already assigned that label. Click the box until it becomes a check mark to apply the label to all the selected documents.

7. (Optional) Check the following Keep Together check boxes if desired:
    - **Keep Families Together**: Check to apply the selected label to documents within the same family as the selected documents.
    - **Keep Email Clusters Together**: Check to apply the selected label to email documents within the same cluster as the selected documents.
    - **Keep Related Documents Together**: Check to apply the selected label to all documents related to the selected documents.
    - **Keep Linked Documents Together**: Check to apply the selected label to all documents linked to the selected documents.
8. Click **Save**.

6.4.1 Removing Labels from Multiple Documents

You can remove labels from multiple documents by using the mass actions in the Item List panel.

To remove labels from multiple documents

1. In the *Case Review*, ensure the *Item List* panel is showing.
2. Check the documents from which you want to remove labels. If removing labels from all documents, skip this step.
3. In the first *Actions* drop-down at the bottom of the panel, do one of the following:
    - Select **Checked** to remove labels from all the checked documents.
    - Select **All** to remove labels from all documents, including documents on pages not visible.
4. In the second *Actions* drop-down, select **Label Assignment**.
5. Click **Go**.
6. In the *Label Assignment* dialog, click the check boxes until they are blank on the labels that you want to remove.
7. Click **Save**.

6.5 Viewing Documents with Tags

6.5.1 Viewing Documents with a Label Applied

You can view all the documents assigned to a specific label using the *Tags* tab in the *Case Explorer*.

To view documents assigned a label

1. In the *Case Review*, ensure the *Case Explorer* and *Item List* panel are showing.
2. In the *Case Explorer*, click on the **Explore** tab. Ensure all the folders are checked on this tab.
3. In the *Case Explorer*, click on the **Tags** tab.
   See The Tags Tab on page 42.
4. Uncheck everything on the *Tags* tab, then expand the **Labels** and check the label(s) that you want to see.
5. Click the **Apply** check mark button in the *Case Explorer* panel.
   All documents with the selected label appear in the *Item List* panel.

6.5.2 Viewing Documents with an Issue Coded

You can view all the documents assigned to a specific issue using the *Tags* tab in the *Case Explorer*.

To view documents assigned an issue

1. In the *Case Review*, ensure the *Case Explorer* and *Item List* panel are showing.
2. In the *Case Explorer*, click on the **Explore** tab. Ensure all the folders are checked on this tab.
3. In the *Case Explorer*, click on the **Tags** tab.
   See The Tags Tab on page 42.
4. Uncheck everything on the *Tags* tab, then expand the **Issues** and check the issue(s) that you want to see.
5. Click the **Apply** check mark button in the *Case Explorer* panel.
   All documents with the selected issue appear in the *Item List* panel.

6.5.3 Viewing Documents with a Category Coded

You can view all the documents assigned to a specific category using the *Tags* tab in the *Case Explorer*.

To view documents assigned an issue

1. In the *Case Review*, ensure the *Case Explorer* and *Item List* panel are showing.
2. In the *Case Explorer*, click on the **Explore** tab. Ensure all the folders are checked on this tab.
3. In the *Case Explorer*, click on the **Tags** tab.
   See The Tags Tab on page 42.
4. Uncheck everything on the *Tags* tab, then expand the **Categories** and check the category that you want to see.
5. Click the **Apply** check mark button in the *Case Explorer* panel.
6. All documents with the selected category appear in the *Item List* panel.

7 Coding Documents

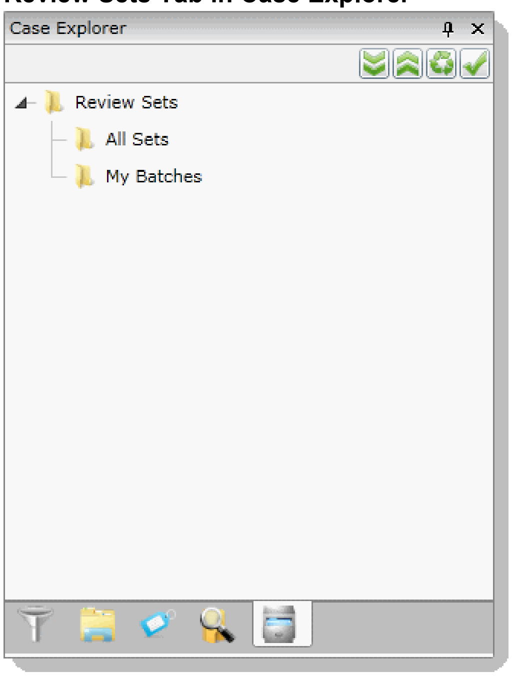
7.1 The Review Sets Tab

The Review Sets tab in the Case Explorer panel can be used to create review sets and view review sets in the Review Batches panel. Review sets are batches of documents that users can check out for coding and then check back in. When a document is checked out, it can only be edited by the user that has it checked out.

Before you code a set of documents, you can check out a review set so that you can track the documents you code and to structure your workflow. Case managers can create and associate review sets. When you are done coding a set of documents, you can check them back in if you have the Check In/Check Out Review Batches permission.

See Checking In/Out a Review Set on page 49.

Review Sets Tab in Case Explorer



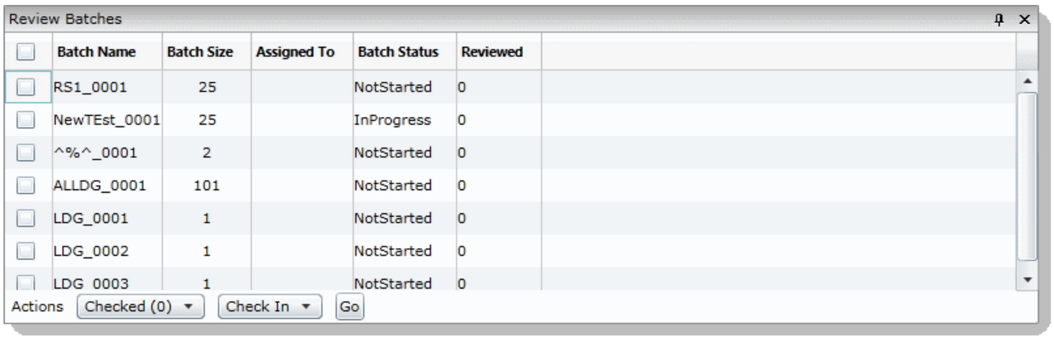
Elements of the Review Sets Tab

Elements	Description
Review Sets	Contains the All Sets and My Batches folders.
All Sets	Displays all the review sets available.
My Batches	Displays review sets that you have checked out.

7.1.1 The Review Batches Panel

The Review Batches panel in Case Review displays review batches. You can check in and check out batches from this panel.

Review Batch Panel



Elements of the Review Batches Panel

Element	Description
Batch Name Column	Displays the name of the review set.
Batch Size Column	Displays the number of documents in review set.
Assigned To Column	Displays the user that the review set is assigned to.
Batch Status	Displays the status of the review set.
Reviewed	Displays the number of documents reviewed in set.
Actions	Expand the first actions drop-down and select one of the following options: ● All: To include all review sets in the panel in the action ● Checked: To include checked review sets in the action ● Unchecked: To include all the unchecked review sets in the action
Actions Check In/ Out	The second Actions drop-down allows you to select to either Check In or Check Out the review set.
Go Button	Click to execute the selected actions.

7.1.2 Checking In/Out a Review Set

Reviewers with the Check In/Check Out Review Batches permission can check out sets of documents for coding. Case managers can create and associate review sets for reviewers. When you are done coding a set of documents, you can check them back in if you have the Check In/Check Out Review Batches permission.

To check out a review set

1. Log in as a user with Check In/Check Out Review Batches permission.

2. Click the *Case Review* button in the *Case List* panel next to the case.
3. In the *Case Review*, ensure that the *Review Batches* panel is showing.
   See The Review Batches Panel on page 49.
4. In the *Review Batches* panel, check the batch(es) that you want to check out. Skip this step if you are checking out all the review batches.
5. In the first *Actions* drop-down in the bottom of the panel, select one of the following:
   - **Checked**: Select this to check out the checked review batches.
   - **All**: Select this to check out all of the review batches, including those not visible on the current page.
6. In the second *Actions* drop-down, select one of the following:
   - **Check Out**: Select this to check out the review set. Only one person can have a review set checked out at a time.
   - **Check In**: Select this to check in a checked out review set.
7. Click **Go**.
8. Click **OK**.

7.2 Using the Coding Panel

7.2.1 The Coding Panel

Coding is putting values into the fields (columns) of documents. The Coding panel in Case Review allows you to use coding layouts to change the data of the selected document. Coding layouts can be created on the Tagging Layout tab of the Home page. Fields in grey on the Coding tab are read only. Fields in orange on the Coding tab are required.

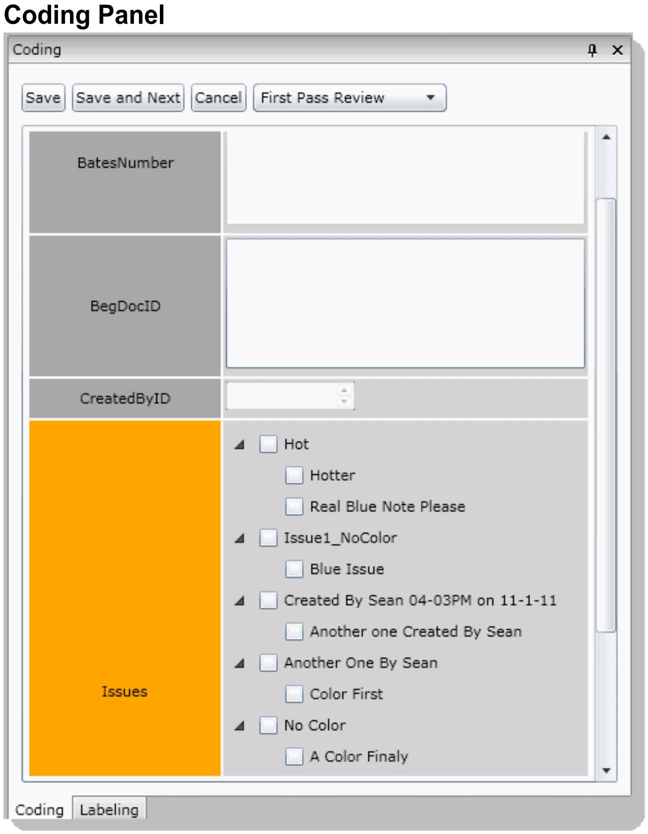
Reviewers with View Coding Layout permission can code the data of a document using the *Coding* panel and the mass actions in the *Item List* panel. Coding is putting values into the fields (columns) of documents. Coding allows you to identify descriptive pieces of information that never had metadata, like images that were loaded and need to have dates manually added into the field. The *Coding* panel in *Case Review* allows you to use coding layouts to code the selected document.

See Coding Single Documents on page 52.

See Coding Multiple Documents on page 53.

Coding layouts can be created by the case manager in the *Tagging Layout* tab of the *Home* page.

Coding Panel



Elements of the Coding Panel

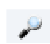
Element	Description
Edit Button	Click to edit the selected layout.
Layout Drop-down	All available layouts for the user are in this drop-down.

7.2.2 Coding Single Documents

Reviewers with the View Coding Layout permission can code the data of documents outlined in a coding layout. Layouts are defined by the case manager. Layouts include custom fields, categories, and issues. You can code the data for all of these things as long as they are included in the Layout defined by the case manager.

You can code single documents using the Coding panel. Fields in grey in the coding layout are read only. Fields in blue in the coding layout are required.

To code single documents

1. Log in as a user with *View Coding Layout* permission.
2. Click the *Case Review* button  in the *Case List* panel next to the case.
3. In the *Case Review*, ensure that the *Item List, Case Explorer* and *Coding* panel are showing.
4. If you are coding a checked out review batch, in the *Case Explorer*, click the **Review Batches** tab, expand the **My Batches** folder, and select the batch that you want to code. The documents for the selected batch appear in the *Item List* panel.
   See The Review Batches Panel on page 49.
5. In the *Item List* panel, select the document that you want to code.
   See Using the Item List Panel on page 19.
6. In the *Coding* panel, expand the layout drop-down and select the layout that you want to use. You must be associated with the layout in order to use it. Case managers can associate layouts to users and groups.
   See The Coding Panel on page 51.
7. In the *Coding* panel, click **Edit**.
8. Edit the data to reflect accurate data. The options available will differ depending on the layout that the case manager created.
9. Click one of the following:
   - **Save**: Click this to save your changes and stay on the same document.
   - **Save and Next**: Click this to save your changes and go to the next document in the *Item List* panel.

   Note: You will only be able to click Save if all the required fields (blue fields) are populated.

7.2.3 Coding Multiple Documents

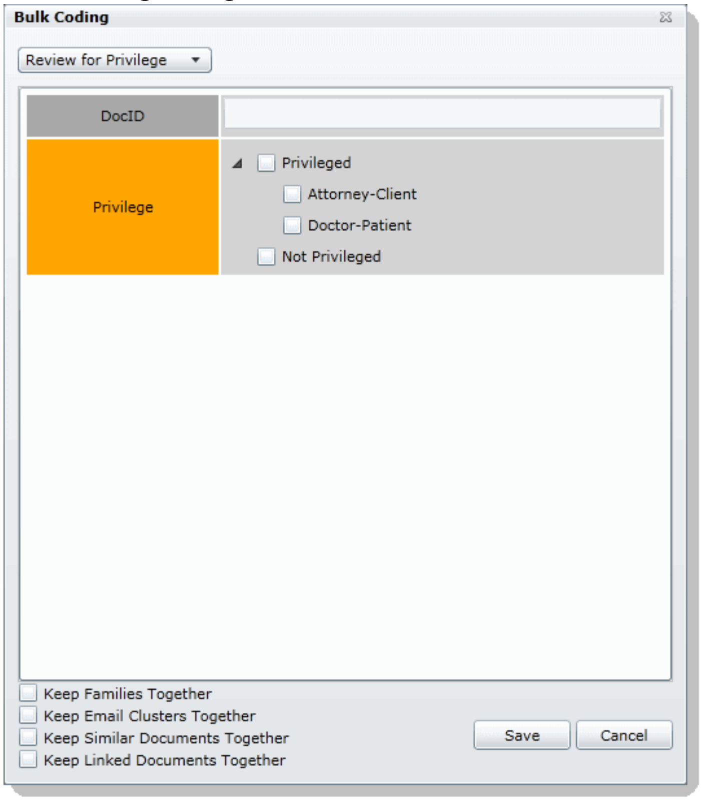
Reviewers with the View Coding Layout permission can code the data of documents outlined in a coding layout. Layouts are defined by the case manager. Layouts include custom fields, categories, and issues. You can code the data for all of these things as long as they are included in the Layout defined by the case manager.

You can code multiple documents using the mass actions in the *Item List* panel. Fields in grey in the coding layout are read only. Fields in blue in the coding layout are required.

To code multiple documents

1. Log in as a user with *View Coding Layout* permission.
2. Click the *Case Review* button  in the *Case List* panel next to the case.
3. In the *Case Review*, ensure that the *Item List* and *Case Explorer* panel are showing.
4. If you are coding a checked out review batch, in the *Case Explorer*, click the **Review Batches** tab, expand the **My Batches** folder, and select the batch that you want to code. The documents for the selected batch appear in the *Item List* panel.
   See The Review Batches Panel on page 49.
5. In the *Item List* panel, check the documents that you want to code. Skip this step if you are coding for all the documents.
   See Using the Item List Panel on page 19.
6. In the first *Actions* drop-down at the bottom of the panel, select one of the following:
   - **Checked**: Select this to code only the documents that you checked.
   - **All**: Select this to code all the documents in the Item List panel, including those on pages not currently visible.
7. In the second *Actions* drop-down, select **Bulk Coding**.

Bulk Coding Dialog



8. In the *Bulk Coding* dialog, select the layout in the layout drop-down.
9. Edit the data to reflect accurate data. The options available will differ depending on the layout that the case manager created. Check boxes with a dash (-) indicates that some of the documents have the box checked. Click the check box until it becomes a check mark to apply it to all the selected documents.
10. (Optional) Check the following Keep Together check boxes if desired:
    - **Keep Families Together**: Check to apply the same coding to documents within the same family as the selected documents.
    - **Keep Email Clusters Together**: Check to apply the same coding to email documents within the same cluster as the selected documents.
    - **Keep Related Documents Together**: Check to apply the same coding to all documents related to the selected documents.
    - **Keep Linked Documents Together**: Check to apply the same coding to all documents linked to the selected documents.
11. Click **Save**.

8 Annotating Evidence

Reviewers with the *Add Annotations* permission can annotate documents using the *Natural* and *Image* panels in the *Case Review*.

In the Natural panel, the following annotation options are available:

- Adding a Note (page 55)
- Adding a Highlight (page 57)
- Adding a Link (page 58)
- Adding a Transparent Rectangle (page 57)
- Adding a Transparent Rectangle (page 57)
- Selecting a Highlight Profile (page 61)
- Selecting a Markup Set (page 61)

Redactions, transparent rectangles, and markup sets are also available on the *Image* panel.

8.1 Adding a Note

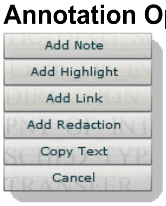
Reviewers with the Add Notes permission can add notes to documents in the Natural panel of the Case Reviewer. Notes can be viewed and deleted from the Notes panel for users with the View Notes and Delete Notes permission.

See The Notes Panel on page 31.

To add a note

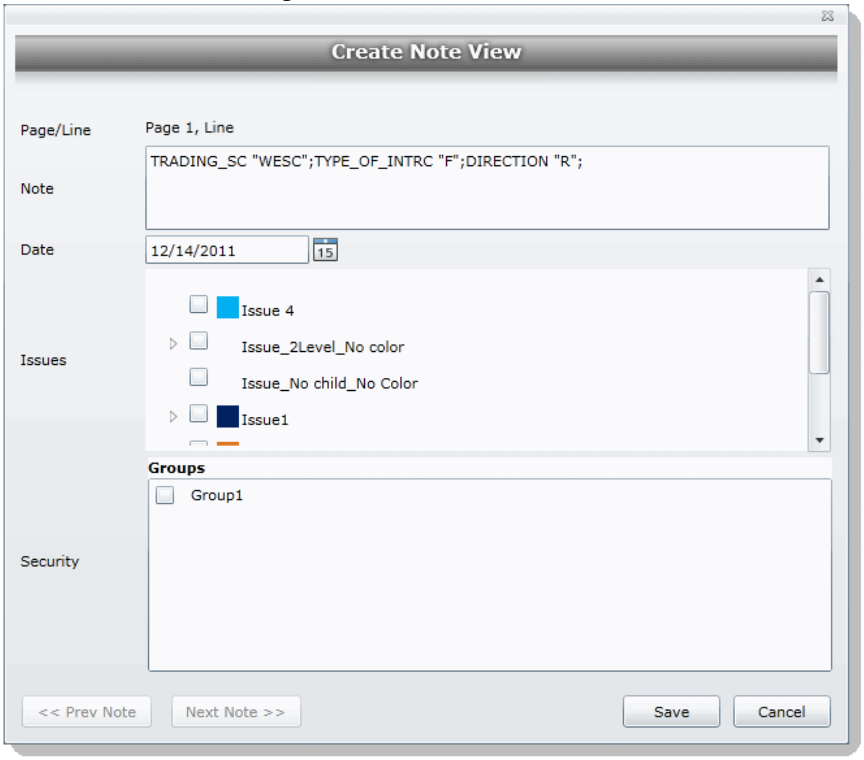
1. Log in as a user with Add Notes permission.
2. Click the *Case Review* button  in the *Case List* panel next to the case.
3. In the *Case Review*, ensure that the *Item List* and *Natural* panel are showing.
4. Select a document in the *Item List* panel that has a native application. The document shows up in the *Natural* panel without requiring the native application to view it.
5. In the *Natural* panel, click the **Redact** tab.
6. Click on the **Select Text** tool button.
7. Highlight the text in the body of the document to which you want to add a note.
   The annotation options are displayed in a drop-down below the highlighted portion.

Annotation Options



8. Select **Add Note**.

Create Note View Dialog



9. Enter a note in the *Note* field.
10. Select a *Date* for the note.
11. (Optional) Check issues related to the note.

Note: If you check an issue that has a color associated with it, the selected text will be highlighted that color.

12. Check the groups with which you want to share the note.
13. Click **Save**.

8.2 Adding a Highlight

Reviewers with the Add Annotations permission can add highlights to documents in the Natural panel of Case Review.

To add a highlight

1. Log in as a user with Add Annotations permission.
2. Click the *Case Review* button  in the *Case List* panel next to the case.
3. In the *Case Review*, ensure that the *Item List* and *Natural* panel are showing.
4. Select a document in the *Item List* panel that has a native application. The document shows up in the *Natural* panel without requiring the native application to view it.
5. In the *Natural* panel, click the **Redact** tab.
6. Click on the **Select Text** tool button.
7. Highlight the text in the body of the document to which you want to add a highlight.
8. In the annotation options drop-down that appears, select **Add Highlight**.

8.2.1 Adding a Transparent Rectangle

Reviewers with the Add Annotations permission can add transparent rectangles to documents in the *Natural* or *Image* panel of *Case Review*. The following steps describe how to add a transparent rectangle in the *Natural* panel, but the steps will also work in the *Image* panel.

To add a transparent rectangle

1. Log in as a user with *Add Annotations* permission.
2. Click the *Case Review* button  in the *Case List* panel next to the case.
3. In the *Case Review*, ensure that the *Item List* and *Natural* panel are showing.
4. Select a document in the *Item List* panel that has a native application. The document shows up in the *Natural* panel without requiring the native application to view it.
5. In the *Natural* panel, click the **Redact** tab.
6. Click the Transparent Rectangle tool button .
7. Click and drag the rectangle onto the body of the document.

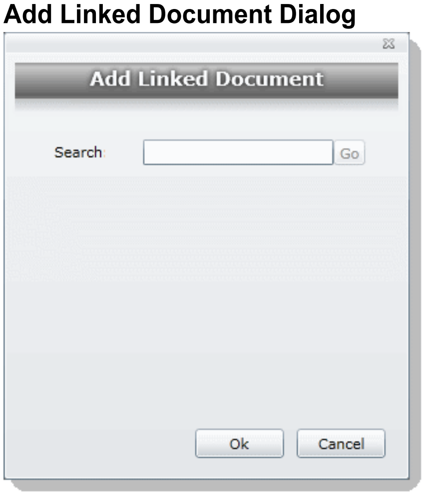
8.3 Adding a Link

Reviewers with the Add Annotations permission can add links to documents in the *Natural* panel of *Case Review*.

To add a link

1. Log in as a user with Add Annotations permission.
2. Click the *Case Review* button  in the *Case List* panel next to the case.
3. In the *Case Review*, ensure that the *Item List* and *Natural* panel are showing.
4. Select a document in the *Item List* panel that has a native application. The document shows up in the *Natural* panel without requiring the native application to view it.
5. In the *Natural* panel, click the **Redact** tab.
6. Click on the **Select Text** tool button.
7. Highlight the text in the body of the document that you want to link to another document.
8. In the annotation options drop-down that appears, select **Add Link**.

Add Linked Document Dialog



9. In the *Search* field, enter the DocID of the document you want to link to.
10. Press the tab button to activate the *Go* button and click **Go**.
11. Select the document you want to link to from the search results.
12. Click **OK**.

8.4 Adding a Redaction

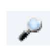
Reviewers with the *Add Annotations* permission can add reactions to documents in the *Natural* panel of *Case Review*. There are two ways to add redactions. You can add them using the Redaction button or the Add Redaction selection in the annotation options drop-down.

To add a redaction using the Redaction Button

Note: The following steps describe how to add a redaction in the *Natural* panel, but the steps will also work in the *Image* panel.

1. Log in as a user with *Add Annotations* permission.
2. Click the *Case Review* button  in the *Case List* panel next to the case.
3. In the *Case Review*, ensure that the *Item List* and *Natural* panel are showing.
4. Select a document in the *Item List* panel that has a native application. The document shows up in the *Natural* panel without requiring the native application to view it.
5. In the *Natural* panel, click the **Redact** tab.
6. Click the **Redact** tool button .
7. Click and drag the rectangle onto the body of the document.

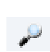
To add a redaction using the annotation options drop-down

1. Log in as a user with *Add Annotations* permission.
2. Click the *Case Review* button  in the *Case List* panel next to the case.
3. In the *Case Review*, ensure that the *Item List* and *Natural* panel are showing.
4. Select a document in the *Item List* panel that has a native application. The document shows up in the *Natural* panel without requiring the native application to view it.
5. In the *Natural* panel, click the **Redact** tab.
6. Click on the **Select Text** tool button.
7. Highlight the text in the body of the document to which you want to add a redaction.
8. In the annotation options drop-down that appears, select **Add Redaction**.

8.4.1 Deleting Annotations

Users with the *Delete Annotations* permission can delete their own and other user's annotations in the *Natural* panel in the *Case Review*.

To delete an annotation

1. Log in as a user with Delete Annotations permission.
2. Click the *Case Review* button  in the *Case List* panel next to the case.
3. In the *Case Review*, ensure that the *Item List* and *Natural* panel are showing.
4. Select a document in the *Item List* panel that has a native application. The document shows up in the *Natural* panel without requiring the native application to view it.

5. In the *Natural* panel, click the **Redact** tab.
6. Select the annotation that you want to delete and click the **Delete** button .

8.4.2 Toggling Redactions On and Off

You can toggle redactions on and off in the *Natural* and *Image* panels so that you can view or hide them without deleting redactions.

To toggle redactions on and off

1. In the *Case Review*, ensure that the *Item List* and *Natural* panel are showing.
2. Select a document in the *Item List* panel that has a native application. The document shows up in the *Natural* panel without requiring the native application to view it.
3. In the *Natural* panel, click the **Redact** tab.
4. Click the **Redactions Off** button .
5. Click the button again to turn them back on.

8.5 Profiles and Markup Sets

8.5.1 Selecting a Highlight Profile

Persistent highlighting profiles are defined by the case manager and can be toggled on and off using the *Highlight Profile* drop-down in *Natural* panel in the *Case Review*.

To select a highlight profile

1. In the *Case Review*, ensure that the *Item List* and *Natural* panel are showing.
2. Select a document in the *Item List* panel that has a native application. The document shows up in the *Natural* panel without requiring the native application to view it.
3. In the *Natural* panel, expand the **Highlight Profile** drop-down and select a profile.

8.5.2 Selecting a Markup Set

Markup sets are a set of markups performed by a specified group of users. For example, you can create a markup set for paralegals, then when paralegal reviewers perform annotations on documents in the Case Review, all of their markups will only appear when Paralegal is selected as the markup for the document in the *Natural* or *Image* panel.

Note: Only redactions and highlights are included in markup sets.

Markup sets are created by the case manager on the home page.

To select a markup set

1. In the *Case Review*, ensure that the *Item List* and *Natural* panel are showing.
2. Select a document in the *Item List* panel that has a native application. The document shows up in the *Natural* panel without requiring the native application to view it.
3. In the *Natural* panel, expand the **Markup Set** drop-down and select a markup set.

9 Deleting Documents

Users with the Edit Document permission can delete documents in the *Item List* panel of the *Case Review*. Users must be careful when deleting documents that the case is backed up first.

You cannot delete documents that are a part of a production set.

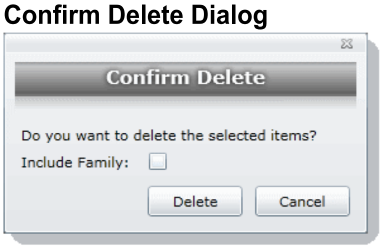
Note: Documents that have been brought into Summation using the Evidence Processing Wizard cannot be deleted.

9.1 Deleting a Document

To delete a document

1. Log in as a user with Edit Document permissions.
2. Click the *Case Review* button  in the *Case List* panel next to the case.
3. In the *Case Review*, ensure that the *Item List* panel is showing.
4. Check the documents that you want to delete. Skip this step if you are deleting all the documents.
5. In the first Actions drop-down, select one of the following:
    - Checked: Select this to delete just the checked documents.
    - All: Select this to delete all of the documents, including documents on pages currently not visible.
6. In the second Actions drop-down, select **Delete**.
7. Click **Go**.

Confirm Delete Dialog



8. Check **Include Family** to delete family documents as well.
9. Click **Delete**.
   The job is sent to the Work List for the case manager to complete.

Searching Summation Data

The part describes how to search Summantion data and includes the following sections:

1 Introduction

This document will help you filter and search through data in the Summation Case Review.

1.1 Searching Evidence

You can use searching to help you find evidence files that are relevant to your case. After you perform a search, you can save your search or share your search with Groups. Then, you can filter your result set to further cull down evidence. As you find relevant files, you can tag the files with Labels, Issues, or Categories for further review or for export.

You can search for text that is either in the file name or in the body of a file. You can also search by columns in the Item List panel.

When you perform a search, it only searches the checked files from the following items in the Case Explorer:

- Document Groups
- Labels
- Issues
- Categories

Any files that meet the search criteria will then be the only files shown in the Item List. When you start a search, be mindful of the items in the list that you are starting with. For example, if you have applied a filter to show only DOC files, and you search for a text string that you think is in a PDF file, it will not find it.

You can do the following:

- See Running Quick Searches on page 11.
- See Running an Advanced Search on page 13.
- See Running Recent Searches on page 22.
- See Saving a Search on page 23.
- See Searching in Natural View on page 12.

1.2 Understanding Search Operators

You can use a Boolean search to find the logical relationships among the search terms and phrases that you enter. A Boolean search consists of the following three full logical operators:

- OR
- AND

You can also use implied Boolean symbols directly in the search terms or phrases that you specify. The following are some examples of implied Boolean that you can use.

Full Boolean logic: AND
Implied Boolean logic search example: marijuana + cocaine

You add implied Boolean logic symbols manually. However, you can add full Boolean logic by either typing the element in the text field or you can click the element's button in the user interface.

If you use more than one logical operator, you should use parentheses to indicate precisely what you want to search for. For example, "apple and pear or orange" could mean either "(apple and pear) or orange", or it could mean "apple and (pear or orange)."

Noise words, such as "if," "and," or "the" are ignored in searches.

Also, characters such as #, @, $, and similar characters are ignored. Only alpha-numeric characters are recognized. Therefore, if you searched for "mckay accessdata," you would find mckay@accessdata. The search ignores the "@" sign as a non-word character and finds the works "mckay" and "accessdata" together.

The following search operators are available in the advanced search.

Advanced Search Operators

Operator	Description
Equal	Searches for the exact value entered.
Not Equal	Searches for everything in the selected field except the exact value entered.
Exists	Searches for the selected field.
Fails	Searches for all documents without the selected field.
GreaterThan	Searches for a number greater than the value entered.
GreaterThanEqualTo	Searches for a number greater than or equal to the value entered.
LessThan	Searches for a number less than the value entered.
LessThanEqualTo	Searches for a number less than or equal to the value entered.
Contains	Searches for the value entered.
NotContains	Searches for everything except the value entered.
Between	Searches between a range of dates.
NotBetween	Searches for all dates except the range selected.

1.3 Understanding Boolean Logic Options

The following table describes the boolean options that you can use in searches. Some boolean options are combined in the table to serve as examples of what is possible.

Only the AND and OR options are used in the Advanced search, but any of these items can be used to run a quick search.

See Understanding Regular Expressions on page 17.

Boolean Logic Options

Option	Description
AND	Returns as search results those evidence files that have all of the search words that you specified, or must contain the search words that you specified. For example: marijuana AND cocaine or marijuana + cocaine
OR	Returns as search results those evidence files that have any of the search words that you specified, at least one of the search words that you specified, or should contain the search words that you specified. For example: marijuana OR cocaine
NOT	Returns as search results those evidence files that do not contain the search words that you specified, or should not contain the search words that you specified. This expression is an efficient way to eliminate potential privileged data from production sets. Used the expression at the beginning of your search word or phrase. For example: NOT licensed or - licensed Matches all evidence files except those with the word “licensed” in them.
W/N	Returns as search results those evidence files that include the specified word or phrase that is found within so many number of words (for example, W/2) of another. The word range is W/1 - W/8. For example: (rock AND stump) W/2 (fence AND gate) or (pear w/10 peach) W/7 (apple OR plum) This option is an excellent way to look for embedded email with a To and From header set to W/ 8 from. You can also use this option to search for evidence files with known words in certain locations or instant messaging chats.
xfirstword, xlastword	These are fixed search words used by the search engine to represent the first word of the document and the last word of the document. For example: copyright W/5 xlastword Matches when “copyright” if found within ten words of the end of the document.
AND NOT	Returns as search results those evidence files that contain the expression on the left when the expression on the right is not found. For example: peach AND NOT pineapple

Boolean Logic Options (Continued)

Option	Description
OR NOT	Returns as search results those evidence files that contain either the left expression or specifically not containing the right expression. For example: peach OR NOT pineapple
NOT W/N	Returns as search results those evidence files where the expression on the left does not occur within so many number of words of the right expression. For example: peach NOT W/8 pineapple
ANDANY	Returns as search results those evidence files that match the left word or phrase with the optional combination of the word or phrase on the right. For example: (grape and pear) ANDANY (pineapple or melon)

2 Running Quick Searches

In most cases, relevant data and privileged information in a data set is found using quick searches. You can use the basic search field in the Item List panel to help you perform fast filtering on selected evidence.

To run a quick search

1. Log in as a user with Run Search privileges.
2. Click the *Case Review* button  in the *Case List* panel next to the case.
3. In *Case Review*, ensure that the *Case Explorer*, the *Item List*, and *Natural* panel are showing.
4. In the *Case Explorer*, default scope selection includes all evidence items in the case. Using the check boxes, uncheck items from both the *Explore* and *Tags* tabs to exclude items from the scope of the search. These scope items include:
   - Document Groups
   - Production Sets
   - Transcripts
   - Notes
   - Exhibits
   - Labels
   - Issues
   - Categories
5. In the *Facets* tab of the *Case Explorer*, you may select any combination of facets to apply to the current search scope.
6. Click the **Apply** check mark button in the top of the *Case Explorer*. This will apply the currently selected scope and any selected facets to the *Item List*, allowing you to search and review on the resulting subset. The facets will persist through searches until you clear them. Scopes may be changed and searches re-run by use of the *Apply* button as well. After updating a facet or scope item, you may click the *Apply* button, which will update the scope and re-run any search that has not been cleared out by use of the *Clear Search* button in the *Search Options* menu of the *Item List* panel.
7. In the search bar of the *Item List* panel, enter a word, or multiple words separated by commas. You may also enter a boolean search phrase in the search bar.

   See Understanding Regular Expressions on page 17.

   See Understanding Boolean Logic Options on page 9.
8. Click **Go** to execute the search.

The search is performed within the specified scope and only searches the body content of the documents within the scope. Search results appear in the *Item List* panel.

If you are searching by keyword, you can select a document from your search results, and see highlighted instances of the word in the *Natural* view.

Quick searches will also appear in the *Recent Searches* on the *Searches* tab of the *Case Explorer*.

2.1 Searching in Natural View

In the Natural panel, you can search by keyword in the Search tab for the selected document.

To search in the Natural panel

1. In *Case Review*, ensure the *Natural* and *Item List* panel are showing.
2. Select a document in the *Item List* that has a native application.
3. In the *Natural* panel, click the **Search** tab.
4. In the *Search* field, enter a keyword for which you want to search.
   Summation predicts the word you are looking for and it appears in the drop-down below the search field.
5. The first instance of the word is highlighted in the natural view.
6. Click the next and previous buttons to see the other instances of the keyword.

3 Running Advanced Searches

3.1 Running an Advanced Search

If using a simple search does not return the results you expected, you can use advanced searching techniques to pinpoint relevant data and privileged information.

AccessData software uses the utility dtSearch to index case data. In Advanced Searching, you can query the index using a specialized query language. In addition to extended searching capabilities, the index allows searches to be returned in seconds instead of the minutes or hours that are required for a standard linear search.

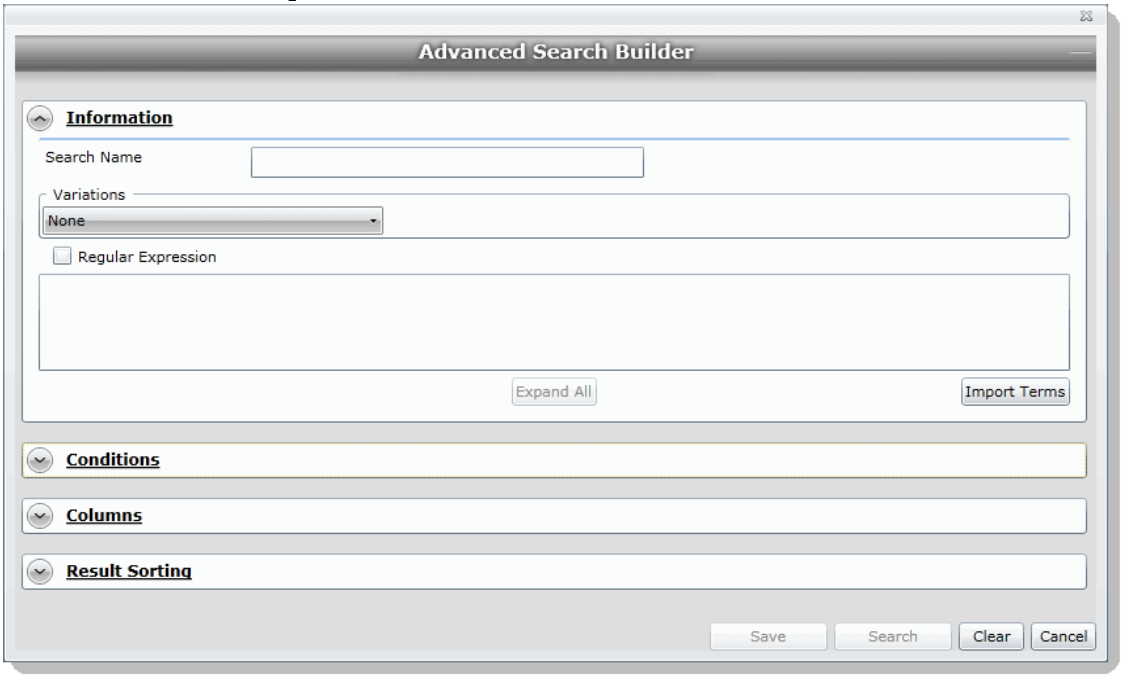
For more information on using dtSearch syntax, you can view the following document on the AccessData website:

http://accessdata.com/downloads/media/dtSearch%207-23-08.pdf

To run an advanced search

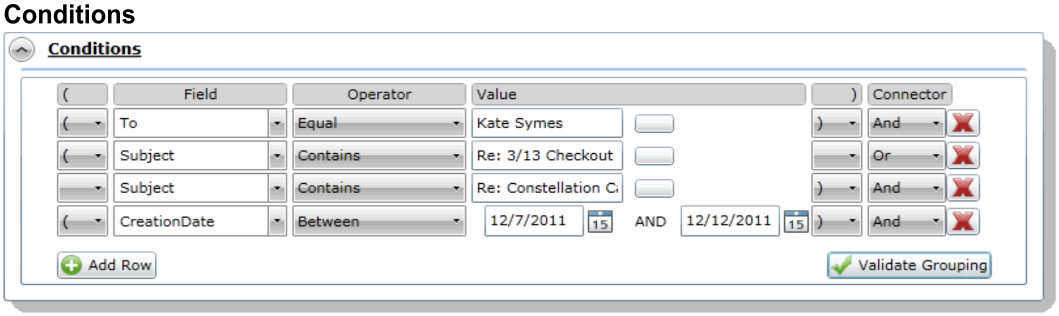
1. Log in as a user with Run Search privileges.
2. Click the *Case Review* button in the *Case List* panel next to the case.
3. In *Case Review*, ensure that the *Case Explorer*, the *Item List*, and *Natural* panel are showing.
4. In the *Case Explorer*, default scope selection includes all evidence items in the case. Using the check boxes, uncheck items from both the *Explore* and *Tags* tabs to exclude them from the scope of the search. These scope items include:
   - Document Groups
   - Production Sets
   - Transcripts
   - Notes
   - Exhibits
   - Labels
   - Issues
   - Categories
5. In the *Facets* tab of the *Case Explorer*, you can select any combination of Facets to apply to the current search scope.
6. Click the **Apply** check mark button in the top of the *Case Explorer*. This applies the currently selected scope and any selected Facets to the *Item List*, allowing search and review on the resulting subset. The scope of a search is saved along with the query. This Facet will persist through searches until you clear it. Scopes may be changed and searches re-run by use of the *Apply* button. After updating a Facet or scope item, you may click the **Apply** button to update the scope and re-run any search that has not been cleared out by use of the **Clear Search** button in the *Search Options* menu.
7. Click the **Search Options** button in the *Item List* panel and select **Advanced Search**.

Advanced Search Dialog



8. In the Information section, do the following:
   8a. Enter a Name for the search if you want to save the search. Otherwise, the search will appear in the Recent Searches list and will not be able to be saved.
   8b. (Optional) Select the type of Variation you want to include in your search.
   See Understanding Advanced Variations on page 16.
   8c. Check Regular Expression if you want your search criteria to be a regular expression.
   See Understanding Regular Expressions on page 17.
   8d. In the text field, enter the freeform text you want to include in the search. Freeform searching lets you combine keyword, boolean, and regular expression criteria to perform a search on evidence files.
   8e. To add related terms for the words you entered, click **Expand All**.
   See Using the Term Browser to Create Search Strings on page 19.
   8f. To import a list of terms from a TXT file, click **Import Terms**.
   See Importing Index Search Terms on page 20.
9. Expand the **Conditions** section to search within the fields/columns of the documents.

Conditions



10. In the *Conditions* section, do the following:

10a. Select a field that you want to search within.

See the Case Manager Guide for more information on creating custom fields.

10b. Select an Operator from the drop-down.

See Understanding Search Operators on page 8.
See Understanding Boolean Logic Options on page 9.

10c. Select or enter a value using the following:

- Field: Enter text or symbols.
- Date: Enter a date or click the calendar to select a date.
- Look up button: Click the blank button to look up available search criteria for the selected field.

10d. Select either “And” or “Or” as the connector.

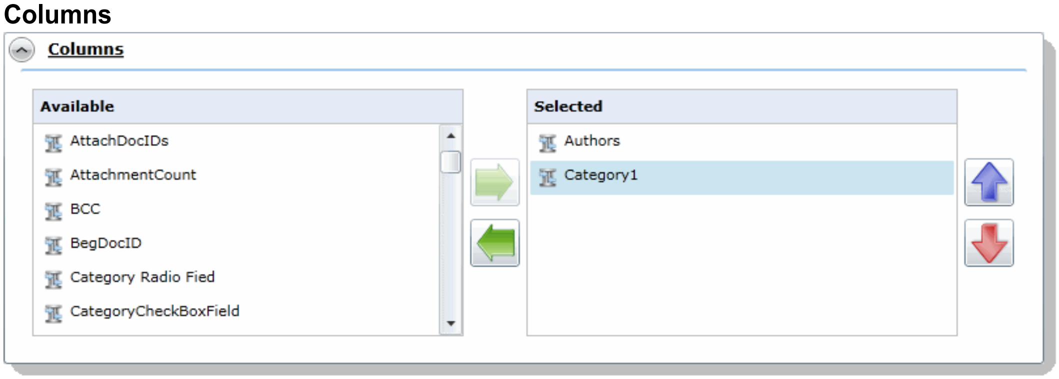
See Understanding Boolean Logic Options on page 9.

10e. Click **Add Row** to add additional conditions.

10f. Set parenthetical criteria. Then, click **Validate Grouping** to validate your parenthesis.

11. Expand the **Columns** section to add visible columns to your search results.

Columns

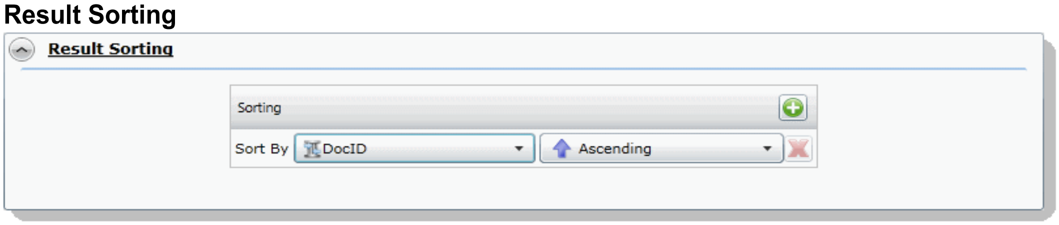


11a. Click the right arrow to add columns and the left arrow to remove columns.

11b. Click the up and down arrows to adjust the order of the columns.

12. Expand **Result Sorting** to select the column by which you want the search results to be sorted. The column does not need to be visible to sort by it.

Result Sorting



12a. In the *Sort By* drop-down, select the field you want to sort by.

12b. In the second drop-down, select whether you want to sort by Ascending or Descending.

13. Click **Search**.

3.2 Understanding Advanced Variations

The following table describes the Variation options in the Information section of the Advanced Search dialog.

Variation Options in the Advanced Search Dialog

Search Variations	Description
None	No search criteria are applied.
Stemming	Finds grammatical variations on word endings. For example, stemming reduces the words “fishing,” “fished,” “fishy,” and “fisher” to the root word “fish.”
Phonic	Finds words that sound like the word that you are searching and begins with the same first letter. For example, searching for “whale” using phonic, would also find wale and wail.
Synonyms	Finds word synonyms. For example, searching on “fast” would also find “quick” and “rapid.” You can enable this option for all words in a request. You can also add the “&” character after certain words in your request.
Related	Finds all words in the search criteria and any related words from the known related categories.
Fuzzy	Finds words that have similar spellings, such as “raise” and “raize.” You can enable this option for all words in a request. The level of fuzziness that you can set is 1-10. The higher the level of fuzziness, the more differences are allowed when matching words, and the closer these differences can be to the start of the word. Setting too many letter differences may make the search less useful. Dragging the slider bar to the right increases the number of letters in a word that can be different from the original search term. Dragging the slider bar to the left decreases the number of letters in a word that can be different from the original search term. You can also add fuzziness directly in the search term you enter using the “%” character. The number of % characters that you add determines the number of differences that are ignored when you search for a word. The position of the % characters determines how many letters at the start of the word have to match exactly. For example, “ca%nada” must begin with “ca” and have just one letter difference between it and “canada.” Whereas, “c%%anada” must begin with “c” and have only two letter differences between it and “canada.” In another example, marijuana can be spelled “marihuana” or “maryjuana.” In this case, your search expression could be “mar%%uana.” As with the fuzzy slider bar setting, you should exercise care when you use multiple % symbols because the number of junk hits rises quickly with each added error.

3.3 Understanding Regular Expressions

You can use the regular expressions to search through large quantities of text information for repeating forms of data, and advanced combinations of characters.

A regular expression (regex) that you enter must meet the following criteria:

- Use quotes and begin with ##.
- Match a single whole word. For example, "##app.*ie" would not find "apple pie."
- Only letters are searchable. Characters that are not indexed by dtSearch are not searchable.
- Searches that include beginning of line or end of line regex criteria, such as ^ and $, do not work.

You can find more information about regular expression searching by going to the following AccessData website:

http://www.accessdata.com/media/en_us/print/techdocs/Web_regexp.pdf

See Running an Advanced Search on page 13.

To search evidence files using regular expressions

1. In *Case Review*, in the Item List panel, click **Search Options** > **Advanced Search**.
2. Select **Regular Expression**.
3. In the text field, enter the words and special characters that you want to use in the search pattern. See Basic Regular Expression Characters on page 17.
4. Click **Search**. The hit results are displayed in the **Evidence** pane.

3.3.1 Basic Regular Expression Characters

The following table describes some of the characters that you can use in creating your own regular expression search.

See Understanding Regular Expressions on page 17.

Examples of Regular Expressions

Expression	Example
.	Matches any single character. For example: r.ad Would match "read" or "road."
^	Matches the start of a line.
$	Matches the end of a line.
\	Treats the next character as a literal. For example: \+45 Would not be interpreted as one or more, but as "45."
[ ]	A bracket expression. Matches a single character that is contained within the brackets. For example: bon[abcd] Would match "bona" and "bond", but not "bone."

Examples of Regular Expressions (Continued)

Expression	Example
[a-z]	The dash inside the brackets indicates a range of characters. For example: [a-z] Matches any single lower-case character.
[^]	Matches a single character that is not contained within the brackets. For example, [^abc] matches any character other than a, b, or c. And [^a-z] matches any single character that is not a lowercase letter from a to z. Or, [^b]at matches all strings matched by .at except bat.
*	Matches the preceding element zero or more times. For example: .* Matches any string of characters, or nothing.
+	Matches the preceding element one or more times. For example: [rs]+at Matches “rat,” “sat,” “rrat,” “rsat,” “srat,” “sssrat,” and so on, but not “at.” Matches any string of at least one character.
[a-z]+	Matches any sequence of one or more lower-case characters.

3.4 Using the Term Browser to Create Search Strings

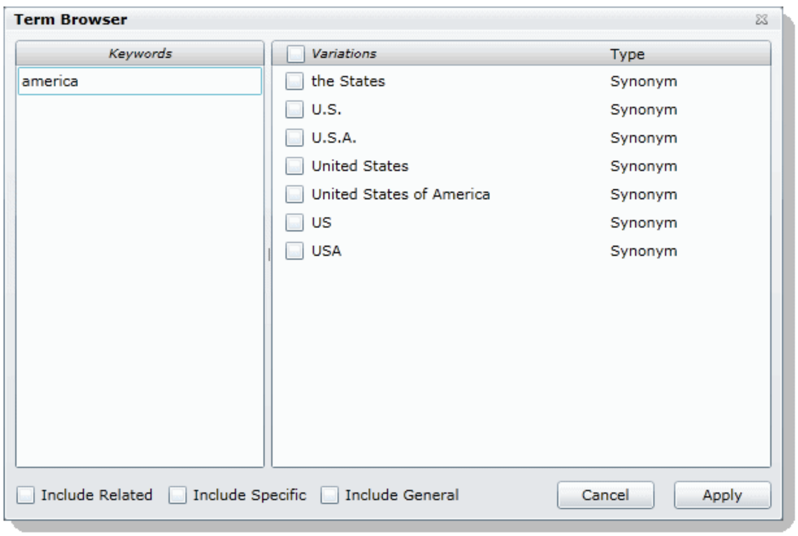
You can build a search using terms that are related to any keyword. You can use the Term Browser to generate a list of similar words. You then select which words you want to include in the search.

For example, you may start with a keyword of delete. By using the Term Browser, it will suggest synonyms, such as erase and cut. It will also suggest related terms, such as cut, deletions, excise, and expunge. It will also suggest general related terms, such as censor, remove, take, and withdraw. You can select which of those words to include in your search.

To search for terms using related words

1. In *Case Review*, in the Item List panel, click **Search Options** > **Advanced Search**.
2. Enter a keyword.
3. Click **Expand All**.

Term Browser



4. In the *Term Browser,* highlight the keyword.
   A list of synonyms is generated.
5. To add other related words, select the **Include Related**, **Include Specific**, and **Include General** check boxes.
6. Select the words that you want to include in the search or click **Variations** to select all words.
7. To build a search including the words that you selected, click **Apply**.
8. You can edit the search or run it by clicking **Search**.

3.5 Importing Index Search Terms

You can import a list of search terms. This lets you reuse a list of search terms that you saved from previous searches, or that you saved for documentation purposes.

To import a saved search terms file

1. In *Case Review*, in the Item List panel, click **Search Options** > **Advanced Search**.
2. Click **Import** to import a set of search terms.
3. Select the text file that you previously saved.
4. Click **Open**.

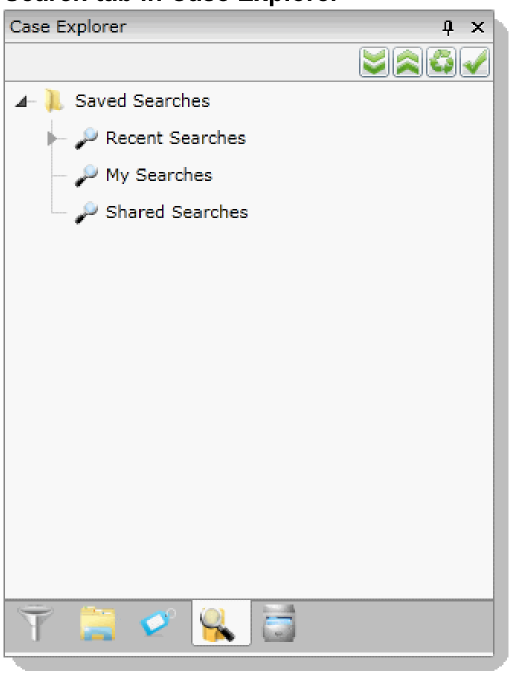
4 Re-running Searches

You can re-run searches by using the Search tab in the Case Explorer panel in the Case Review.

4.1 The Search Tab

The *Search* tab in the *Case Explorer* can be used to view recent searches, your searches, and shared searches.

Search tab in Case Explorer



Elements of the Search Tab

Element	Description
Saved Searches	Contains the Recent Searches, My Searches, and Shared Searches.
Recent Searches	Every time a search is performed, it is saved in the recent searches. The last 10 searches are saved here in chronological order. Users can execute and edit searches from Recent Searches.
My Searches	Displays all the searches that the user has saved. Users can execute, delete and edit searches from My Searches. Users can also share their searches.
Shared Searches	Displays all the shared searches that the user has permissions to access. Users can execute searches from Shared Searches.

4.2 Running Recent Searches

When you execute a search, the search conditions are saved. You can view and reuse recent searches. The last ten searches are saved in the Recent Searches. To run recent searches, you must have the Run Searches permission.

To run a recent search

1. Log in as a user with Run Searches permissions.
2. Click the *Case Review* button  in the *Case List* panel next to the case.
3. In *Case Review*, ensure the *Case Explorer* is showing.
4. Click on the **Searches** tab.
5. Expand the *Recent Searches*.
6. Right-click the search and select **Run Search**.
   The search is run using the original search scope and the original search criteria. The search results appear in the *Item List* panel.

4.2.1 Clearing Search Results

After you have performed a search, the items in the Item List are the result of the list. You can clear the search result to view the documents in the Grid before you performed the search. Clearing the list will also clear the Recent Searches.

To clear search results

1. In *Case Review*, ensure the Item List panel is showing.
2. Click **Search Options** > **Clear Recent Searches**.

4.3 Saving a Search

You can save any advanced search that you design in the Advanced Search Builder. All saved searches are stored in the *Searches* tab of the *Case Explorer*. You can use saved searches to run past searches again or to share your search with a group of users.

To save a search

1. Log in as a user with Run Search privileges.
2. Click the *Case Review* button  in the *Case List* panel next to the case.
3. In *Case Review*, ensure that the *Case Explorer*, and the *Item List* panel are showing.
4. In the *Case Explorer*, default scope selection includes all evidence items in the case. Using the check boxes, uncheck items from both the *Explore* and *Tags* tabs to exclude them from the scope of the search. These scope items include:
   - Document Groups
   - Production Sets
   - Transcripts
   - Notes
   - Exhibits
   - Labels
   - Issues
   - Categories
5. In the *Facets* tab of the *Case Explorer*, you can select any combination of Facets to apply to the current search scope.
6. Click the **Apply** check mark button in the top of the *Case Explorer*. This applies the currently selected scope and any selected Facets to the *Item List*, allowing search and review on the resulting subset. The scope of a search is saved along with the query. This Facet will persist through searches until you clear it. Scopes may be changed and searches re-run by use of the *Apply* button. After updating a Facet or scope item, you may click the **Apply** button to update the scope and re-run any search that has not been cleared out by use of the **Clear Search** button in the *Search Options* menu.
7. Click the **Search Options** button in the *Item List* panel and select **Advanced Search**.
8. Enter a *Name* for the search.
9. Enter criteria for the search.
   See Running Recent Searches on page 22.
10. Click **Save**.

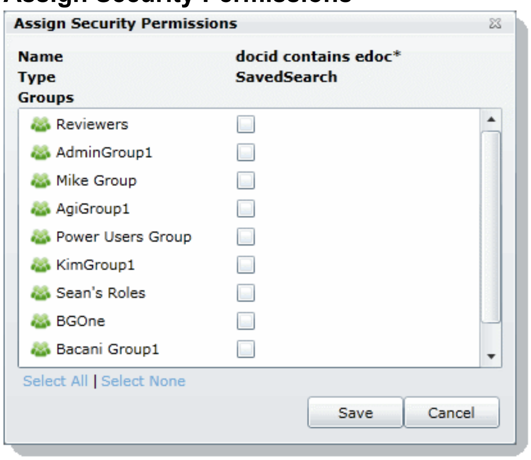
4.4 Sharing a Search

You can share your saved searches with other groups of users. To share a search, you need to have the Manage Searches permission.

To share a search

1. Log in as a user with Manage Searches permissions.
2. Click the *Case Review* button  in the *Case List* panel next to the case.
3. In *Case Review*, ensure the *Case Explorer* is showing.
4. Click on the **Searches** tab.
5. Expand *My Searches*.
6. Right-click the search and select **Manage Permissions**.

Assign Security Permissions



7. Check the groups with which you want to share the search.
8. Click **Save**.

5 Culling Data

In *Case Review*, you can filter evidence to help view only relevant evidence for the case. After you have applied filters, the results are then displayed in the *Item List*. You can also use searches and column sorting to help you further review and cull down evidence.

5.1 About Filter Facets

You can use filters to help you cull your evidence. There are many pre-defined filter facets that you can use. Some of the filter facets are dynamic based on the evidence files that you have. All of the filter facets are organized into facet categories.

By default, when you first open a case in *Case Review*, all filter facets are applied, and as a result, all evidence is listed in the *Item List*. You use the filter facets to exclude evidence from the *Item List*.

Facets are persistent across searches and have to be cleared by you manually.

See Available Filter Facet Categories on page 26.

You can use a single facet or multiple facets.

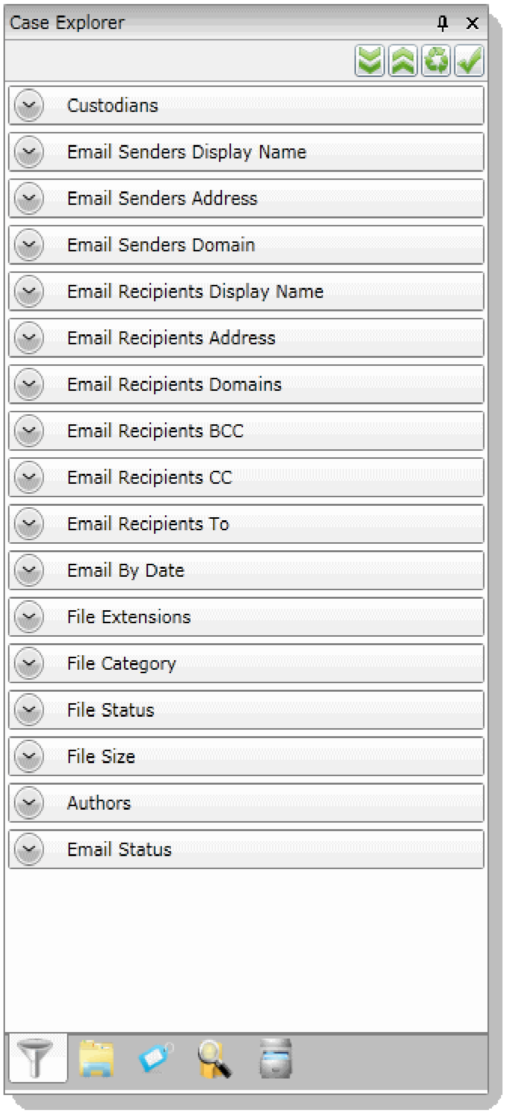
5.1.1 The Facets Tab

The Facets panel in Case Review lists the available filters to apply to documents. You can filter evidence to help view only relevant evidence for the case. After you have applied filters, the results are then displayed in the Item List. You can also use searches and column sorting to help you further review and cull down evidence.

The Facets Tab in the Case Explorer allows you to filter before (and maintain after) conducting any searches. This allows targeting specific areas of data for search and review with persistent filters. You may maintain the applied filter(s) as long as desired.

You can use one or more filter facets to cull down the evidence. By default, when you first open a case in Case Review, all filter facets are applied, and as a result, all evidence is listed in the Item List. You use the filter facets to exclude evidence from the Item List.

Facets Panel



You can use filters to help you cull your evidence. There are many pre-defined filter facets that you can use. Some of the filter facets are dynamic based on the evidence files that you have. All of the filter facets are organized into facet categories. You can use a single facet or multiple facets.

5.1.2 Available Filter Facet Categories

The following table lists the filter facet categories that are available in the *Filters* tab of the Case Explorer.

Filter Facet Categories in the Filters Panel

Filter Facet	Description
Custodians	Filters evidence based on custodians associated to the case.
Email Senders Display Name	Filters evidence based on the email senders display name. You can drill down to specific values.

Filter Facet Categories in the Filters Panel (Continued)

Filter Facet	Description
Email Senders Address	Filters evidence based on the email senders address.
Email Senders Domain	Filters evidence based on the email senders domain.
Email Recipients Display Name	Filters evidence based on the email recipients display name. You can drill down to specific values.
Email Recipients Address	Filters evidence based on the email recipients address. You can drill down to specific values.
Email Recipients Domains	Filters evidence based on the email recipients domain. You can drill down to specific values.
Email Recipients BCC	Filters evidence based on BCC recipient address, display name, and domain. You can drill down to specific values.
Email Recipients CC	Filters evidence based on CC recipient address, display name, and domain. You can drill down to specific values.
Email Recipients To	Filters evidence by To recipient address, display name, and domain. You can drill down to specific values.
Email by Date	Filters evidence by email date. You can select to filter by the Delivered date or the Submitted date. You can drill down to date ranges or specific dates.
File Extensions	Filters evidence by file extension, including: .doc, .docx, .log, .msg, .rtf, .txt, .wpd, .wps.
File Category	Filters evidence by file category, including: archives, databases, documents, email, executables, folders, graphics, internet/chat files, mobile phone data, multimedia, OS/file system files, other encryption files, other known types, presentations, slack/free space, spreadsheets, unknown types, and user types.
File Status	Filters evidence by file status, including: bad extension, email attachments, email related items, encrypted files, and OLE sub-items.
File Size	Filters evidence by file size.
Authors	Author of Microsoft Office documents.
Email Status	Filters evidence by email status, including: attachments, related items, replies, and forwarded.

5.1.3 Examples of How Filters Work

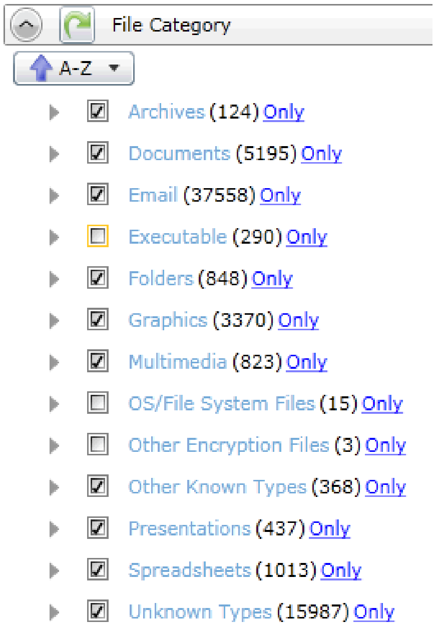
Including and Excluding Items

Next to each filter facet is a check box. By default, all filter facets are selected. Next to each filter facet is also a count of the number of files that match that facet’s criteria.

The following figure shows an example of the *File Category* with all of the individual facets in that category.

As an example of how you can use this category, to help reduce irrelevant files, you can exclude executable and system files.

File Category Filter



For each facet, there is also a link labeled *Only*. You can click *Only* for a facet and that one facet will be checked and all other facets in that category will be cleared.

You can also click on the facet name which will exclude all other facets and all other categories.

See Configuring Filters Facets on page 31.

Using a Single Filter Facet

You can filter your evidence based on one or more filter facets. There may be times when you want to use a single facet.

For example, there is a facet category called *Tags*. Inside that category is a facet for each of the labels that have been used in the case. You can clear all but one label facet and only the files with that label are displayed; all other files are excluded.

Another example is filtering for a single custodian or email sender.

Using Multiple Facets in a Single Filter Category

You can filter evidence using multiple filter facets within a single facet category. For example, there is a filter facet category called *File Category*. Inside that category are individual filter facets for each type of files that are in the case (archives, documents, emails, graphics, spreadsheets, and so on.) You can exclude the types of files that you do not need to review while leaving the file types that you do want to review.

Using the N/A Facet

In most of the facet categories, there is a special filter facet that is labeled *N/A*, which stands for “not applicable.” If you check this, the filter will display items to the results that are not applicable to that category.

For example, if you apply a single filter facet for one or more email addresses, and *N/A* is unchecked for that category, then the only results will be emails. If you also check *N/A,* then other file types will also be displayed, such as documents, spreadsheets, and PDFs, because they don't have an email address property.

As another example, suppose that you are configuring only the *Tags* category. Suppose you check the *Responsive* label only. When you apply that facet, you will see only the files that have the *Responsive* label applied. If you also check the *N/A* facet in the *Labels* category, files with any other label will still be excluded, but files without a label also display.

As another example, you can see a list of all files that do not have a custodian applied to them. In the *Custodians* category, you can select only the *N/A* facet, and that excludes all files that have a custodian applied.

If your case has no files that pertain to a facet category, it will show *N/A* as the only item in the facet.

Note: If you click **Only** for a name under the *Email Recipients To* facet category, the *N/A* box is not automatically cleared. It will clear all the other buttons in the respective section.

Refining Evidence Using Filters in Multiple Facet Categories

You can use multiple filter facets together in order to further refine your evidence. For example, suppose you have applied a filter facet for a single custodian and you want to refine it further to only include spreadsheets and documents that are related to that custodian. You can apply another set of facets for file extensions choosing to exclude all files but *Documents* and *Spreadsheet* files. By doing this, you can combine the two facet categories and display only spreadsheets and documents that have a certain custodian.

For example, suppose you are using the *Custodian* and *File Extensions* facet categories together. Suppose you select one custodian, *Sarah*, who has 20 files of multiple file types associated with her. Suppose that in the *File Extensions* category you select one file extension, *PDF*, and there are 40 PDF files associated with multiple custodians, 5 of which are associated with Sarah. If those two facets are the only items that you select, it will display only the PDF files that have Sarah as the custodian. In this example, the result would show only the 5 PDF files associated with Sarah.

As another example, you may need to create an export set of a specific custodian's data, but at the same time, remove anything that is obviously unimportant to reviewers. You can do the following:

- Using the *Custodians* category, select only the one custodian.
- Using the *File Extensions* category, exclude unimportant file types, such as *EXE* and *DLL* files.
- Using the *Email Senders Domain* category, exclude all emails that came from ESPN.com and Comast.com.

As another example, a development in a case may reveal that some very important evidence may exist as an email attachment sent either to or by a custodian within a specific date range. You can do the following:

- Using the *Custodians* category, select only the one custodian.
- Using the *File Status* category, select only *Email Attachments*.
- Using the *Email by Date* category, select only emails delivered in March and April of 2009.

Email Recipient Filter Facet Counts

When viewing filter facets, a count of the items related to each facet is displayed. For any given filter facet that is selected, the filter count will be part of the total number of items displayed in the Item List. For example, suppose you configure filter facets to show only PDF and XLS files and the filter counts show 6 PDF files and 4 XLS files. In the Item list, only the 10 PDF and XLS files will be displayed. The total of the two filter counts will match the number of files in the Item List.

There is a situation where the filter count may be higher than the count of items in the Item list. There are six different filter facet categories that are related to email recipients. To help reduce the length of the list of recipients, there is a first-level division that contains alphabetical ranges of the names that are used. For example, ABurr --> AHamilton, ALincoln --> ASteveson, and so on. From that first level, you can drill down to individual names.

The filter counts displayed for the first levels (a range of names) may by higher than the number of emails in the Item List. The reason is that a single email may have been sent to multiple recipients. In the Item List, that email is reflected as one single item, yet in the first-level list of the facet, the counts may reflect 5 recipients of that one email. Because there can be more recipients than emails, this can cause the first-level filter count to be higher than the Item List count.

5.2 Configuring Filters Facets

To configure filter facets, you specify the items that you want to exclude. As you configure filter facets, the results are displayed to the *Item List*. As you clear filter facets, files are removed from the *Item List*.

The *Filters* list denotes with an icon which facet categories you have configured.

Note: You must be careful when excluding evidence. Once evidence has been excluded using a filter in the *Filters* panel, the only way to display that evidence again is to recheck the specific filter or reset all of the filters. No other filter facet will return the evidence to the item list.

After you have configured filter facets, you can save your configuration. You can also load filters that you have previously saved. Saved filters are part of the case and cannot be used with other cases.

To apply a single filter facet to evidence

1. In the *Filters* panel on the *Case Review* page, expand the facet category that you want to use.
   For a list of facets categories, see Available Filter Facet Categories (page 26).

   To expand all categories, click **Expand**.
2. In the expanded facet category, click the *Facet name* link.
   Click this link to exclude all other facets and facet categories.
   For example, in the *File Category* category, if you click the facet named **Email**, you will only get email messages.
3. To undo the single facet, click .

To apply one or more filter facets to evidence

1. In the *Filters* panel on the *Case Review* page, expand the facet category that you want to use.
   For a list of facet categories, see Available Filter Facet Categories (page 26).

   To expand all categories, click **Expand**.
2. In the expanded category, perform one of the following tasks:
   - *Check*: Manually check the items that you want to include.
   - *Uncheck*: Manually uncheck the items that you want to exclude.
   - *Only*: Click **Only** to uncheck all other facets in the category.
   - *Expand*: Many facets can be expanded to show dynamic facets. For example, in the Email By Date category, there is a Delivered facet. You can expand it to show detailed facets for years, months, or days.
3. Click **Apply**.
   The *Item List* will change to display only the items that you filtered for.

   When you change the configuration of a category, a appears next to the category name. This shows you which categories have been configured.
4. (Optional) Repeat steps 2 and 3 as often as needed. After making any changes, you must click **Apply**.

5. (Optional) To reset facets, do any or all of the following:
   - To undo an individual facet, check the box for an item that you previously unchecked.
   - To reset all facets in a single category, click the next to the category name.
   - To undo all filters, click **Reset**.
6. Click **Apply**.

5.3 Filtering by Column in the Item List Panel

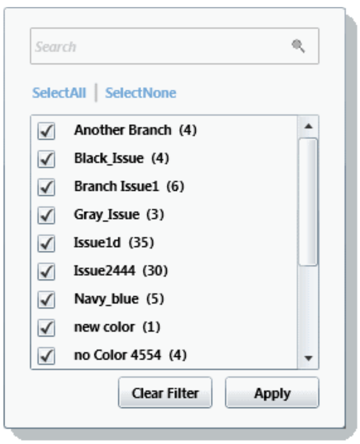
You can filter the evidence in the Item List panel by the data in the columns. You cannot filter the content of the first three columns. You can apply multiple column filters.

Column Filters do not persist and will be cleared out when you either execute a new search or use the **Clear Search** button.

To filter evidence by data in columns

1. In Case Review, ensure the Item List panel is showing.
2. Select the document groups, labels, or issues that you want to view from the Case Explorer.
3. In the Item List panel, click on the column filters button .

Column Filters



4. Uncheck the items that you want to filter out of your view.
5. You can use the *Search* bar to search by keyword among the items in the column.
6. Click **Apply**.
   All documents with the item that you unchecked are removed from the *Item List* panel.

5.3.1 Clearing Column Filters

You can clear column filters that you have applied to the Item List panel.

To clear column filters

1. In *Case Review*, ensure the *Item List* panel is showing.
2. Select the document groups, labels, or issues that you want to view from the *Case Explorer*.
3. In the *Item List* panel, click on the column filters button .
4. Click **Clear Filter**.

Exporting Summation Data

The part describes how to export Summantion data and includes the following sections:

1 Introduction

This document is about creating and exporting production sets for a case. Exporting, in most cases, is performed by the case manager. You need the correct permissions to create and export production sets.

1.1 About Production Sets and Exports

When you sort through data, organization remains key to preparing a streamlined set of data to include in a report that is delivered to the attorney for the criminal case, civil case, or corporate authorities for a corporate security case. To prepare data for the final report, you can create production sets of filtered data that you can export to various formats.

After applying labels to the evidence set, you can create a production set. A production set is the final output.

When you create production sets, you can only use one label per set.

Note: Production set records cannot be labeled. Creating a production set results in new items being created, these resulting items, cannot be labeled.

See Export Tab on page 10.

See Exporting Production Sets on page 26.

The following table describes the export formats that you can use for your production sets.

Export Formats

Format	Description
AD1	Creates an AD1 forensic image of the documents included in the Export Set. AD1 is a forensic file format that integrates with FTK. An AD1 contains the logical structure of the original files and the original files themselves. The AD1 file is hashed and verifiable to ensure that no changes have occurred to it.
Image Load File Export	Converts the native documents to a graphic format such as TIFF, JPG, or PDF. It creates a load file in the IPRO LFP or the Opticon OPT formats. This is similar to Load File Export except that it does not contain any metadata.
Native Export	Exports the native documents in their original format and optionally rendered images into a directory of your choosing. This export does not provide a load file.

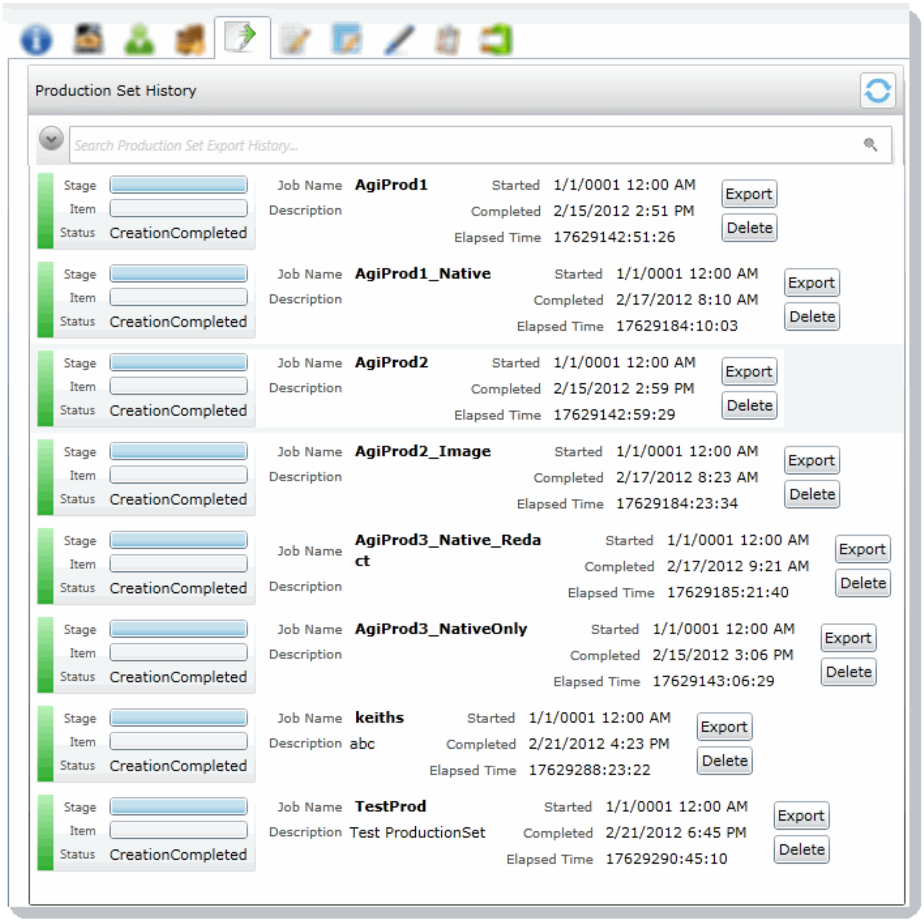
Export Formats (Continued)

Format	Description
Load File Export	Exports your choice of Native, Filtered text (includes the OCR text that was created during processing), rendered images of the native document, and optionally OCR text of the rendered images. If the recipient intends to use third-party software to review the export set, select Load File Export. You have the option of exporting rendered documents in the following formats: ● Concordance ● EDRM (Electronic Discovery Reference Model) XML ● Generic ● iCONECT ● Introspect ● Relativity ● Ringtail (flat file) ● Summation eDII ● CaseVantage Some programs have load file size limits. If needed, you can split load files into multiple files. If you use the Concordance, Generic or Relativity exports, and include rendered images, you will also get an LFP and OPT file.

1.2 Export Tab

The Export tab on the Home page can be used to export or delete production sets and view the history.

Export Tab



Export Tab Elements

Element	Description
Production Set History Search Field	Enter text to search by production set name.
Production Set List	Lists the production sets and the status of the production sets.
Export Button	Click to export the production set to a load file.
Delete Button	Click to delete the production set.

2 Creating Production Sets

When you create a production set, you include all of the evidence to which you have applied a given label. After you create the production set, you export the set to an AD1 image file, an image load file, a native export, or a load file.

Note: Once you've created a production set you cannot add documents to that set even if you use the same labels. You will need to label the additional documents and then create a new set using the same label.

Case managers with the Create Production Sets permission can create production sets.

To create a production set

1. Before you create a production set, be sure you have applied at least one label to evidence files that you want to filter into the export set.
2. Log in as a user with Create Production Set rights.
3. Click the **Case Review**  button next to the case in the *Case List*.
4. In the *Case Explorer*, select the **Explore** tab, right-click the *Production Sets* folder, and select **Create Production Set**.
5. See Production Set General Options (page 11) for information on how to fill out the options in the General Options screen.
6. Click **Next**.
7. See Production Set Files to Include Options (page 13) for information on the option in the Files to Include screen.
8. Click **Next**.
9. In the *Columns to Include*, click the right arrow to add a column to the production set and the left arrow to remove a column from the production set. You can rearrange the order of the columns by clicking the up and down arrows.
10. Click **Next**.
11. See U.S. Volume Document Options (page 15) for information on the options in the *Volume Document Options* screen.
12. See Production Set Image Branding Options (page 22) for information on the options in the Image Branding Options screen.
13. In the Summary screen, review the options that you have selected for the production set and click the Edit (pencil) button if you want to make any changes.
14. Click **Save**.

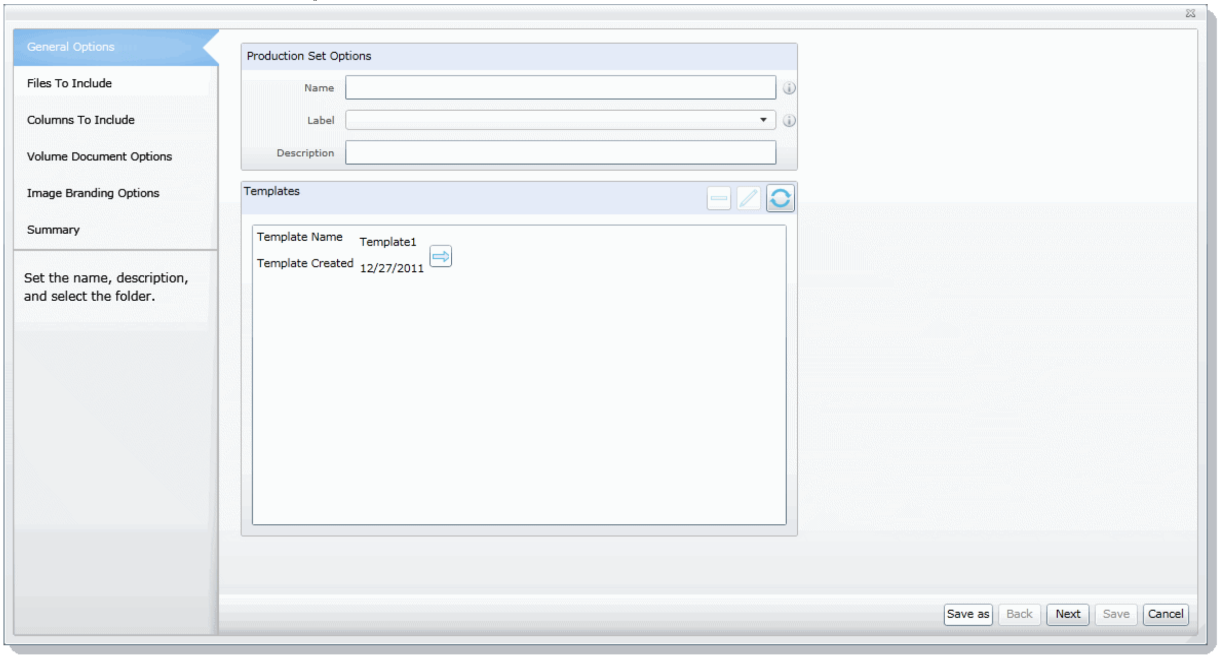
    After your production set is created, it will appear in the *Export* tab of the *Home* page and under the *Production Sets* folder in the *Case Explorer* of the *Case Review*.

2.1 Production Set General Options

The following table describes the options that are available on the **General Options** screen of the production set wizard.

See Export Tab on page 10.

Production Set General Options Screen



General Export Options

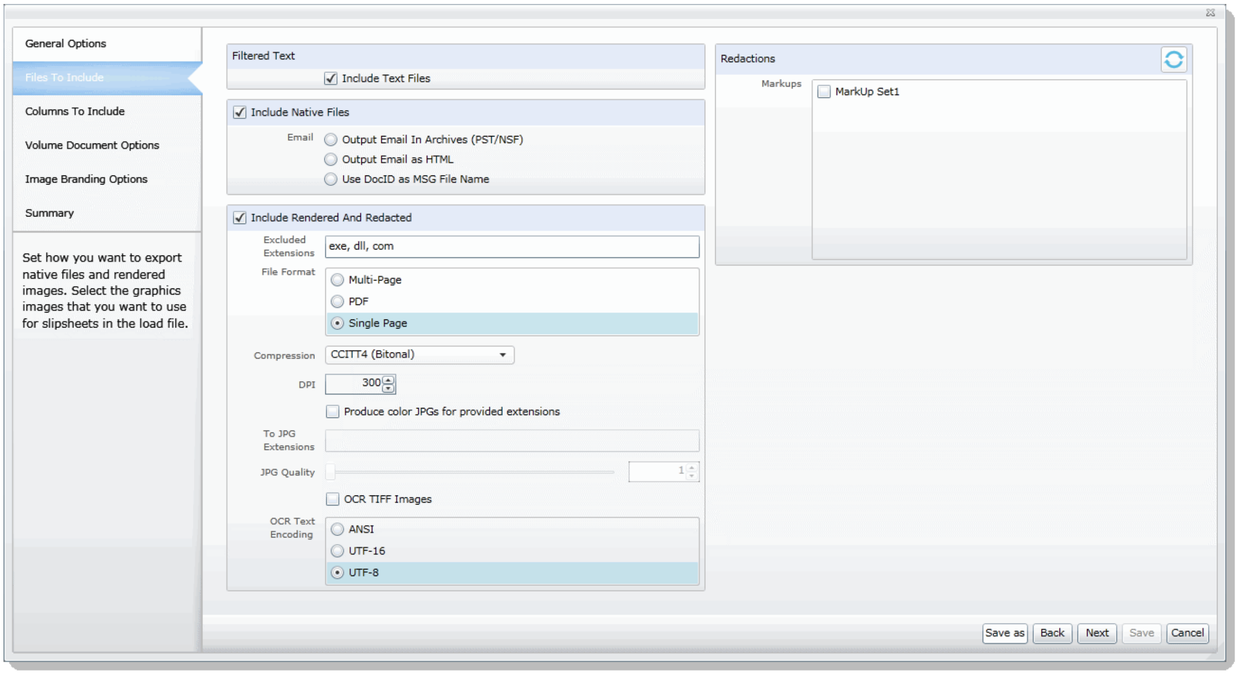
Option	Description
Name	Enter the name of the production set job you are creating. This does not need to be a unique name, but it is recommended that you make all names unique to avoid confusion.
Label	Select the label that has the documents you want to include in the production set.
Description	Enter a description for the production set if desired.
Templates	Select a template to populate all the fields of the production set wizard using the options selected in a previous production set.

2.2 Production Set Files to Include Options

The following table describes the options that are available on the *Files to Include* screen of the production set wizard.

See Export Tab on page 10.

Production Set Files to Include Screen



Files to Include Options

Option	Description
Include Text Files	Select this to include all filtered text files in the production set. This does not include redacted text. This will not re-extract text from native files.
Include Native Files	Select this option if you want to include the native documents with the production set. This will only include native files that have not been redacted. If the native file has been redacted, a pdf of the file will be included.
Output Email in Archives	Select this option if there are emails that were originally in a PST or an NSF format and you want to put them into a PST or NSF container.
Output Email as HTML	Select this option if there are emails that were originally in a PST or NSF and you want to make them HTML files.
Output email as MSG	Select this option if there are emails that you want to make into MSG files.
Include Rendered and Redacted Images	Select this option to include images that have been created in the Case Review. Additionally, if an image has not yet been created, this option will convert the native document to an image format.

Files to Include Options (Continued)

Option	Description
Excluded Extensions	Enter the file extensions of documents that you do not want to be converted. File extensions must be typed in exactly as they appear and separated by commas between multiple entries. This field does not allow the use of wild card characters. The default values are: EXE, DLL, and COM
File Format	Select which format you want the native file converted to: ● **Multi-page** - one TIFF image with multiple pages for each document. ● **PDF** - one PDF file with multiple pages for each document. ● **Single Page** - a single TIFF image for each page of each document. For example, a 25 page document would output 25 single-page TIFF images.
Compression	● **CCITT3 (Bitonal)** - Produces a lower quality black and white image. ● **CCITT4 (Bitonal)** - Produces a higher quality black and white image. ● **LZW (Color)** - Produces a color image with LZW compression. ● **None (Color)** - Produces a color image with no compression (This is a very large image). ● **RLE (Color)** - Produces a color image with RLE compression.
DPI	Set the resolution of the image. The range is from 96 - 1200 dots per inch (DPI).
Produce color JPGs for provided extensions	This and the following two options are available if you are rendering to CCITT3 or CCITT4 format and allows you to specify certain file extensions to render in color JPGs. For example, if you wanted everything in black and white format, but wanted all PowerPoint documents in color, you would choose this option and then type PPT or PPTX in the **To JPG Extensions** text box. Additionally, you can choose the quality of the resulting JPG from 1 - 100 percent (100 percent being the most clear, but the largest resulting image).
To JPG Extensions	Lets you specify file extensions that you want exported to JPG images.
JPG Quality	Sets the value of JPG quality (1-100). A high value (100) creates high quality images. However, it also reduces the compression ratio, resulting in large file sizes. A value of 50 is average quality.
OCR TIFF Images	Creates a page by page OCR text file from the rendered images. By default, the text file uses a TXT extension. As a best practice, you would not create both Filtered Text files and OCR text files. However, if you do both, the Filtered Text files use a TXT extension and the OCR text files use an OCR.TXT extension. If you create only OCR text files and not Filtered Text files, the OCR text files use a TXT extension.

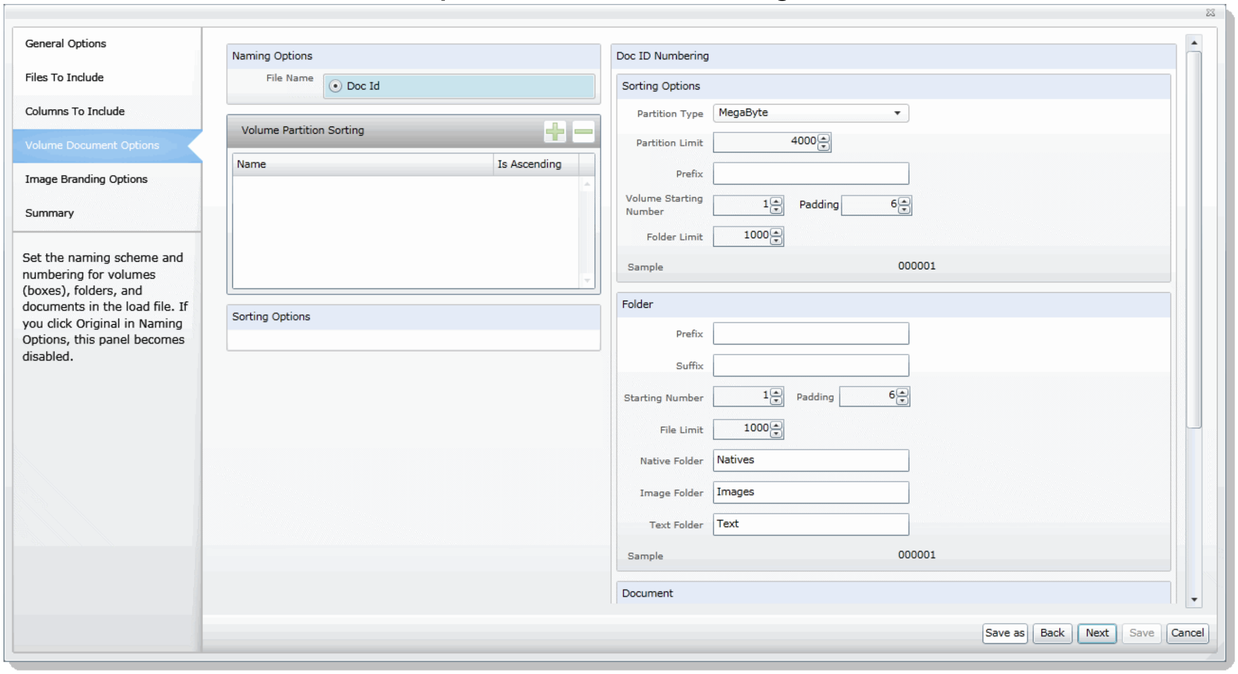
Files to Include Options (Continued)

Option	Description
OCR Text Encoding	● **ANSI** - Encodes text files using ANSI. ANSI encoding has the advantage of producing a smaller text file than a Unicode file (UTF). ANSI-encoded text files process faster and save space. The ANSI encoding includes characters for languages other than English, but it is still limited to the Latin script. If you are exporting documents that contain languages written in scripts other than Latin, you need to choose a Unicode encoding form. Unicode encoding forms contain the character sets for all known languages. ● **UTF- 16** Encodes load files using UTF-16. ● **UTF - 8** (Default) Encodes load files using UTF-8. For more information on the Unicode standard, see the following website http://www.unicode.org/standard/principles.html
Redactions Markups	Check the Markup Sets that you want included in the production set. Markups will be burned into the images that are created.

2.2.1 U.S. Volume Document Options

This section describes the options available in the Volume Document Options screen of the production set wizard if you have US numbering enabled. US numbering is default. The following table describes the options available in the following screen.

Production Set Volume Document Options Screen US Numbering



Volume Document Options Screen

Option Type	Option	Description
Naming Options		Choose a naming option:
	DOCID	(Default) This file naming allows you to determine what the name of the files will be, based on the document ID numbering scheme. This option is used with the *Document Numbering Options* on this tab. In Case Review, you can view the DocID that is created for exported files. This is useful in associating an exported file with the original file.
Volume Partition Sorting		You can sort the documents before they are converted and named. This allows you to choose one or more metadata field values to sort the documents in ascending or descending order. You can choose any combination of fields by which to sort, however, it is not recommended to choose more than 3 fields to sort by.
	 (Volume Partition Sorting)	Add volume partition sorting filters based on specified ascending or descending fields.
	 (Volume Partition Sorting)	Delete the selected sorting option.
	Sorting	Specify the order that the files are listed in each volume. Sorting occurs on the parent document. For example, you might sort by **Ascending** on the field **FILESIZE**. In such case, the first volume contains the largest file sizes, and the last volume contains the smallest file sizes.
	Field	Set the column heading by which you want to sort.

Volume Document Options Screen (Continued)

Option Type	Option	Description
	Add	Add the sorting options that you have selected. You can add one or more sorting filters.
Volume Sample		Provide a sample of the volumes.
Volume Options		Select a volume folder structure for the output files. The selections will determine how much data is put into each folder before a new folder is created and the folder structure in which the output is placed. See About the U.S. Volume Structure Options on page 19.
	Partition Limit	Set the size of the partition based on the partition type that you have selected.
	Prefix	Specify the prefix-naming convention you want to use for the root volume of the production set.
	Starting Number	Set the starting number of the first partition in the production set.
	Padding	Specify the number of document counter digits that you want. The range is 1 to 21. 0 padding is not available.
	Folder Limit	Create a new numbered volume when the specified folder limit is reached inside the volume.
Folder		Lets you name and limit the size or the number of items that are contained in a folder. An export can have one or more folders.
	Prefix	Specifies the prefix-naming convention that you want to use for the folders within the volume of the export.
	Suffix	Specifies the suffix-naming convention that you want to use for the folders within the volume of the export.
	Starting Number	Sets the starting number of the first folder within the volume of the export.
	Padding	Specify the number of document counter digits that you want. The limit is 21.
	File Limit	Creates a new numbered folder when the specified file limit is reached inside the folder.
	Native Folder	Lets you set the name of the **Natives** folder.
	Image Folder	Lets you set the name of the **Image** folder. See Files to Include Options on page 13.
	Text Folder	Lets you set the name of the **Text** folder where text files go that are generated by the OCR engine. See Files to Include Options on page 13.
Document		
	Numbering Options	See About U.S. Document Numbering Options on page 20.
	Prefix	Specifies the prefix-naming convention that you want to use for the document and page numbering within the folders of the export.

Volume Document Options Screen (Continued)

Option Type	Option	Description
	Suffix	Specifies the suffix-naming convention that you want to use for the document and page numbering within the folders of the export.
	Starting Number	Sets the starting number of the first folder within the volume of the export.
	Padding	Specify the number of document counter digits that you want. The limit is 21.
	Continue from last used number	Lets you have sequential numbering across all exports per legal matter. Sets **Starting Number** to the last document number plus 1 from the last export. In order to enable this, you must also enable the *Use Last Document Number* option in the export default settings.

2.2.1.1 About the U.S. Volume Structure Options

You can specify the volume folder structure for the output files. The selections will determine how much data is put into each folder before a new folder is created and the folder structure in which the output is placed.

See U.S. Volume Document Options on page 15.

The output files will be contained within the following hierarchy:

- *Volume folder* - Contains two levels of subfolders for organizing the files. A new volume will be created when a specified limit is reached.

  You can choose from the following limits.

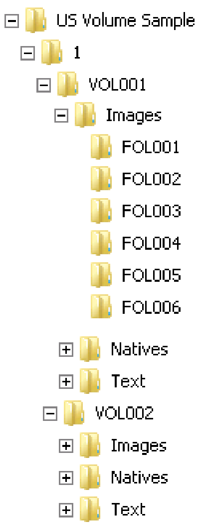
Limits

Limit	Description
Documents	Output will be placed into a volume until the specified number of documents has been reached, then a new volume will be created. For example, if you export 2000 files and you set the partition limit to 1000, you will have two document volumes.
Images	Output will be placed into a volume until the specified number of images has been reached, then a new volume will be created. This option is useful because a single, large document may create one image per page.
Megabyte	Output will be placed into a volume until the specified megabyte size of all of the files has been reached, then a new volume will be created. For example, you can set a partition limit of 4000 MB if you intend to burn the files to DVD media.
Single	All output will be placed into one volume.

  You can also specify a volume folder limit. In order to prevent issues with Microsoft Windows Explorer, you can specify an additional limit of the number of folders in a volume. This works in addition to the selected limit type. If the specified volume limit is not reached, but the folder limit is, a new volume will be created.

- *File type folder* - The first level subfolders within each volume are separated by the file types of the exported files. By default, the folders are named by file type, for example, native documents, images, or text files.
- *Level 2 folder* - The second level folders contain the actual files being exported. You can specify a limit of the total number of files per folder. This limit, once reached, will create a new folder within the same file type folder until the volume maximum or number of folders has been reached.

Using the *Partition Type*, *Partition Limit,* and *Folder limit* values together, you can create the volume structure that meets your needs. The following graphic is an example of a volume structure.



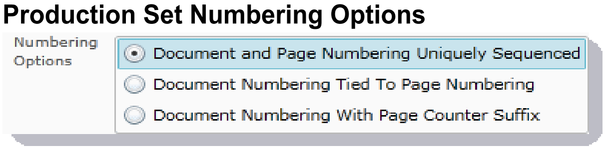
Note: No document that has been rendered will have its rendered pages divided into more than one folder.

2.2.1.2 About U.S. Document Numbering Options

If you have chosen to use a DocID naming scheme for the output files, you can specify the method for creating Doc IDs. This section describes the Numbering options found in the Volume Document Options screen of the Production Set wizard.

See U.S. Volume Document Options on page 15.

Production Set Numbering Options



You will choose from the document numbering options:

- **Document and Page Numbering Uniquely Sequenced**

  This option generates a sequential number that is applied to the document without regard to the rendered pages that may or may not be produced. The images will also be numbered sequentially without regard to the document number.

  For example, if you have two documents each that produce two images during conversion, the output would be:

Example Output

Native Documents	Image Output
ABC00001.doc	ABC00001.tif
	ABC00002.tif
ABC00002.doc	ABC00003.tif
	ABC00004.tif

You can optionally specify a prefix- and a suffix-naming convention.

- **Document Numbering Tied to Page Numbering**

  This option generates a sequential number for every page created. The corresponding document name will be the same as its first page generated for each document.

  For example, if you have two documents each that produce two images during conversion, the output would be::

Example Output

Native Documents	Image Output
ABC00001.doc	ABC00001.tif
	ABC00002.tif
ABC00003.doc	ABC00003.tif
	ABC00004.tif

You can optionally specify a prefix- and a suffix-naming convention.

- **Document Numbering with Page Counter Suffix**

  This option generates a sequential number for every document and the pages produced for that document will carry the document's name with a counter as a suffix that represents which page is represented by the image.

  For example, if you have two documents each that produce two images during conversion, the output would be:

Example Output

Native Document	Image Output
ABC00001.doc	ABC00001.001.tif
	ABC00001.002.tif
ABC00002.doc	ABC00002.001.tif
	ABC00002.002.tif

2.3 Production Set Image Branding Options

You can brand the rendered pages of TIFF and PDF images with a header, footer, watermark, or Bates numbering from the Production Set wizard.

See Export Tab on page 10.

Image Branding Screen

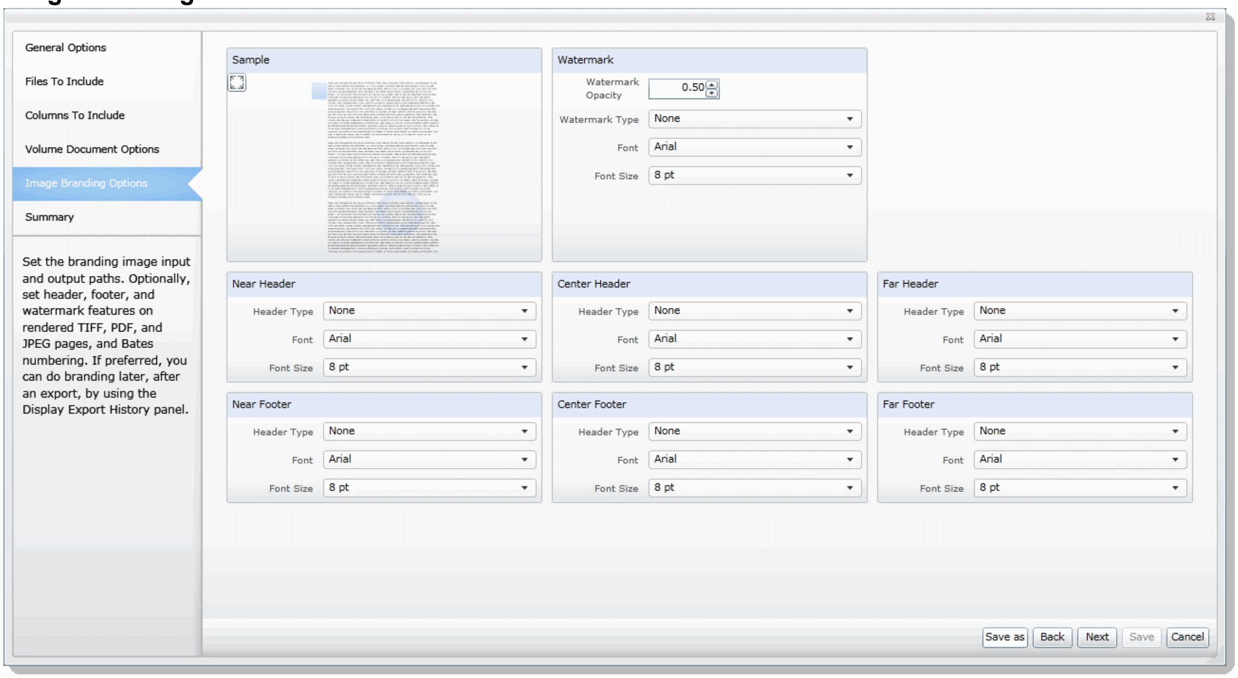


Image Branding Options

Option Group	Options	Options	Description
Sample			Displays a sample of the image branding options selected.
Watermark			Set options to brand a watermark to the middle of the document.
	Opacity		Sets the visibility of the watermark text.
Watermark/ Header/Footer Type			There are multiple types of image branding available. The options in the Watermark, Header and Footer groups will differ depending on the Type that you select.
	None		No branding on the image.

Image Branding Options (Continued)

Option Group	Options	Options	Description
	Bates		Turns Bates numbering of rendered image pages on or off. Bates numbering is a term used for placing an identifying number on every page of evidence files that are presented in court. If you create a production set of evidence files with the setting to produce multi-page TIFF images or PDF files, the TIFF or PDF file name is the Bates number of the first page of the document, which is known as the BegDoc (beginning document) number. Bates numbering is not driven by the document or page numbering that was assigned in the *Volume/Document Options* panel.
		Prefix	Specify up to any 25 alphanumeric characters except the forward slash or backward slash. You can use a separator to create a visual break between the different sections of the Bates number.
		Starting Number	Sets the starting number to a value from 1-100.
		Padding	Specify the number of document counter digits that you want. The limit is 42.
		Font	Sets the font style for the text.
		Font Size	Sets the font size for the text.
	Doc ID		Displays the Doc ID in the designated location.
		Font	Sets the font style for the text.
		Font Size	Sets the font size for the text.
	Field		Displays the selected field value in the designated location.
		Field	Select one of the available fields to display in the designated location.
		Font	Sets the font style for the text.
		Font Size	Sets the font size for the text.
	Global Endorsement		Displays the entered text in the designated location.
		Text	Enter the text that you want to appear in the designated location.
		Font	Sets the font style for the text.
		Font Size	Sets the font size for the text.
	Page ID		Displays the page ID number in the designated location.
		Font	Sets the font style for the text.

Image Branding Options (Continued)

Option Group	Options	Options	Description
		Font Size	Sets the font size for the text.

2.4 Additional Production Set Options

2.4.1 Saving Production Set Options as a Template

After configuring the production set options, you can save the settings as a template. The template can be reused for future production sets with the current case or other cases.

To save options as a template

1. Access the production set wizard and set the options for the production set.
   See Export Tab on page 10.
2. In the production set wizard, click **Save As**.
3. Enter a name for the template.
4. Click **Save**.

2.4.2 Deleting a Production Set

Users with production set rights can delete production sets from Case Review.

To delete a production set

1. Log in as a user with Production Set rights.
2. Click the **Case Review**  button next to the case in the *Case List*.
3. In the *Case Explorer*, select the **Explore** tab, expand the *Production Sets* folder, right-click the production set that you want to delete and select **Delete**.
4. Click **OK**.

2.4.3 Sharing a Production Set

Users with production set rights can share production sets that they have created with other groups of users.

To share a production set

1. Log in as a user with Production Set rights.
2. Click the **Case Review**  button next to the case in the *Case List*.
3. In the *Case Explorer*, select the **Explore** tab, expand the *Production Sets* folder, right-click the production set that you want to delete and select **Manage Permissions**.
4. Check the groups that you want to have access to the production set that you created and click **Save**.

3 Exporting Production Sets

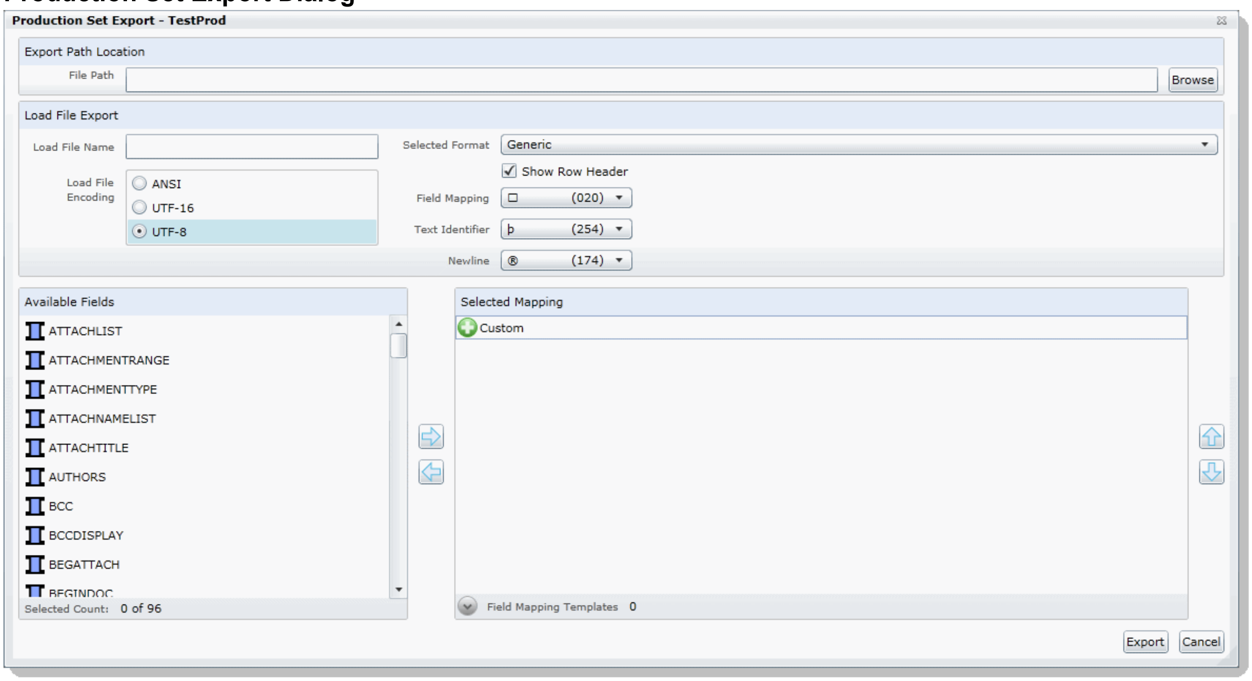
3.1 Exporting Production a Set

After you create a production set, you can export it containing only the files needed for presentation to a law firm or corporate security professional.

To export a production set

1. On the *Home Page*, select a case and click the  **Export** tab.
2. Next to the production set that you want to export, click **Export**.

Production Set Export Dialog



3. Enter or browse to the path where you want to save the export.
4. Enter a name for the Load File.

5. Select a format that you want to use for the export. The following formats are available:
   - **CaseVantage** - Generates a DII file specifically formatted for use with the AD Summation CaseVantage program.
   - **Concordance** - Generates a DAT file that can be used in Concordance.
   - **EDRM** - Generates an XML file that meets the EDRM v1.2 standard.
   - **Generic** - Generates a standard delimited text file.
   - **iCONECT** - Generates an XML file formatted for use with the iConect program.
   - **Introspect** (IDX file) - Generates an IDX file specifically formatted for use with the Introspect program.
   - **Relativity** - Generates a DAT file that can be used in Relativity.
   - **Ringtail (flat file)** - Generates a delimited text file that can be converted to be used in Ringtail.
   - **Summation eDII** - Generates a DII file specifically formatted for use with the AD Summation iBlaze or Enterprise programs.

   Note: If you are outputting a Concordance, Relativity, or Generic load file, and include rendered images, you will also get an OPT and LFP file in the export directory.

6. Depending on the load file format you choose, you may need to check whether or not to show the row header for the columns of data. The Show Row Header option is only available for the following load file formats:
   - Concordance
   - Generic
   - Introspect
   - Relativity
   - Ringtail (Flat File)
7. Select an option for Load File Encoding. The following options are available:
   - **ANSI** - Encodes load files using ANSI (for text written in the Latin script).

     ANSI encoding has the advantage of producing a smaller load file than a Unicode file (UTF). ANSI-encoded load files process faster and save space. The ANSI encoding includes characters for languages other than English, but it is still limited to the Latin script.

     If you are exporting documents that contain languages written in scripts other than Latin, you need to choose a Unicode encoding form. Unicode encoding forms contain the character sets for all known languages.
   - **UTF-8** - (Default) Encodes load files using UTF-8.

     For more information on the Unicode standard, see the following website:

     http://www.unicode.org/standard/principles.html

     Most commonly used for text written in Chinese, Japanese, and Korean.
   - **UTF-16** - Encodes load files using UTF-16.

     Similar to UTF-8 this option is used for text written in Chinese, Japanese, and Korean.
8. Select a **Field Mapping** character. This delimiter is the character that is placed between the columns of data. The default delimiters are recommended by the program to which the load file was intended. However, you can change these defaults by selecting the drop-down and choosing an alternative.

   Field Mapping is available for the following load file formats:
   - Concordance
   - Generic
   - Introspect
   - Relativity
   - Ringtail (Flat File)

9. Select a **Text Identifier** character. This delimiter is the character that is placed on either side of the value within each of the columns. All of the text that follows the character and precedes the next occurrence of the same character is imported as one value.

   The default delimiters are recommended by the program to which the load file was intended. However, you can change these defaults by selecting the drop-down and choosing an alternative. If you do not wish to use a delimiter, you can choose the (none) option.

   Text Identifier is available for the following load file formats:

   - Concordance
   - Generic
   - Introspect
   - Relativity
   - Ringtail (Flat File)

10. Select a **Newline** character. This is a replacement character for any newline (carriage return/line feed) character. The default delimiters are recommended by the program to which the load file was intended. However, you can change these defaults by selecting the drop-down and choosing an alternative. If you do not wish to use a delimiter, you can choose the (none) option.

    Newline is available for the following load file formats:

    - Concordance
    - Generic
    - Introspect
    - Relativity
    - Ringtail (Flat File)

11. Select the **Available Fields** of metadata to be included in the load file and click the right arrow to add the field.
12. Some load file applications require that certain fields be in the load file. In such cases, you can click the Custom plus button to add a custom field entry that is not already listed in the **Available Fields** list.
13. Click **Export**.

Using Summation Mobile

The part describes how to use Summantion Mobile and includes the following section:

1 Using Summation Mobile

Summation Mobile is an application that you can use to work on your Summation cases off of the network. Summation Mobile uses the Copy Case utility to make a copy of a Summation case from the network application to your laptop that you can review off of the network. You can do your work on the copied case in Summation Mobile and then you can merge your changes back into the network case. Summation Mobile is an add on product. Contact your sales representative for information on how to get Summation Mobile.

1.1 Prerequisites

To use Summation Mobile, you need the following things:

- Summation Mobile installed on your laptop (automatically installs the Copy Case utility)
- Rights to the case you are copying
- Connection to the network during copying

1.1.1 Summation Mobile Limitations

The following are limitations for Summation Mobile:

- Maximum of 2 million records
- Maximum of 3 users
- Processing CPUs cannot exceed 4

1.1.2 Tasks You Can't Perform

You cannot perform the following tasks in a copied case:

- Create/Delete Case
- Manage Users
- Manage Groups
- Manage Roles
- Manage Permissions
- Manage Custom Columns (including adding Categories)
- Manage Tagging Layouts
- Manage Persistent Highlighting Profiles
- Manage Markup Sets
- Manage Redaction Reasons
- Manage AutoText Options
- Manage Permissions for: Labels, Issue Values, Saved Searches, and Category Values

- Create/Rename/Delete Production Sets
- Rename Saved Searches
- Delete Evidences
- Create images for the records with electronic documents

1.1.3 Deletions in Summation Mobile

Deleting the following items in a copied case will NOT delete them from the network case after the merge:

- Labels
- Notes
- Transcript Groups / Transcripts
- Exhibits
- Saved Searches
- Document Records

1.2 Copying a Case

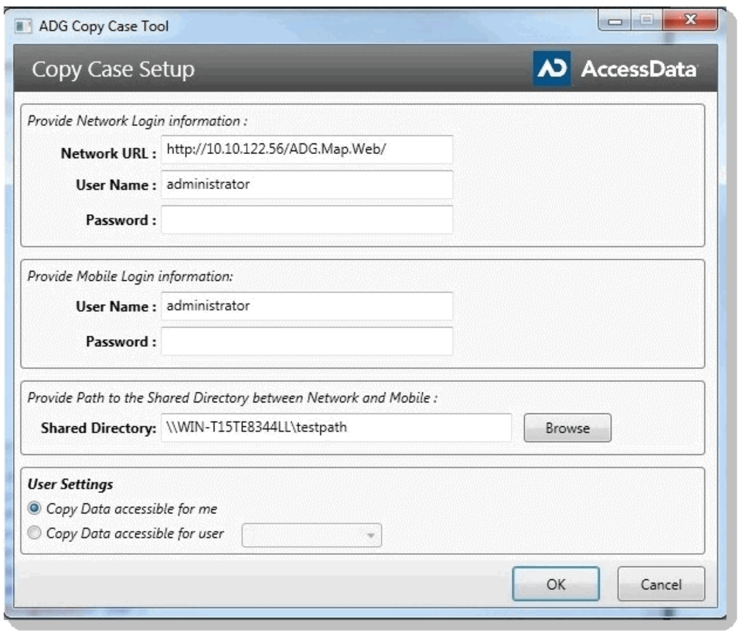
Using the Copy Case utility, you can copy a case from the network application to your laptop for off network use. The laptop where you copy your case may also be referred to as the “local machine.” You must fulfill the prerequisites in order to copy a case.

See Prerequisites on page 7.

To copy a case

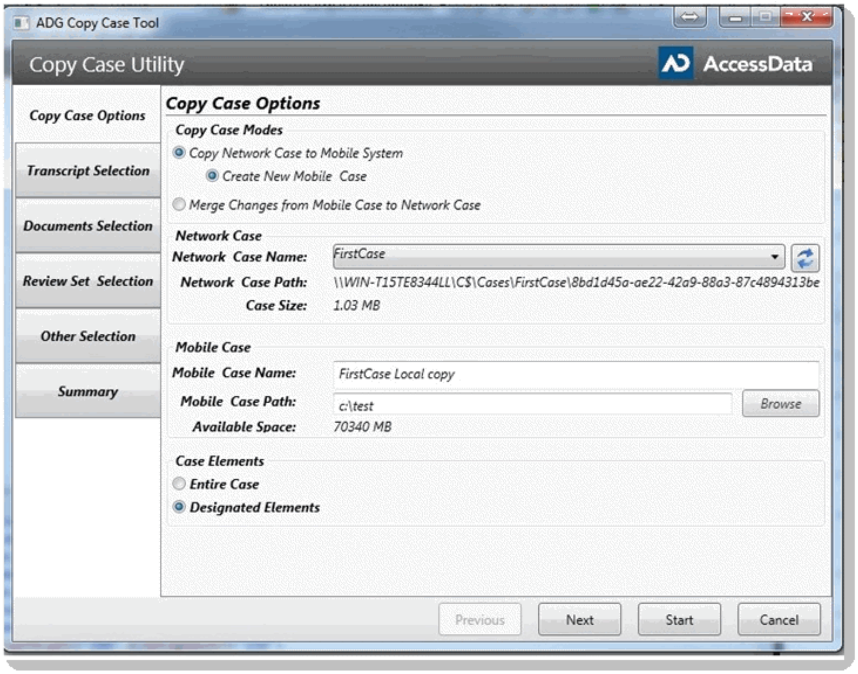
1. Open the Copy Case utility on your laptop.

Copy Case Utility



2. In the *Provided Network Login Information* group box, enter the following:
   - **Network URL**: Enter the URL for the network Summation application.
   - **User Name**: Enter a user with rights to the network.
   - **Password**: Enter the password for the user you entered.
3. In the *Provide Mobile Login Information* group box, enter the following:
   - **User Name**: Enter a user that has access to the case you want to copy.
   - **Password**: Enter the password for the user you entered.
4. Browse to a *Shared Directory*. This directory needs to be a location where both the network and local machine has Read/Write access (used to store data temporarily during the copy process).
5. Click **OK**.

Copy Case Options Screen



6. In the *Copy Case Modes* group box, select **Copy Network Case to Mobile System**.
7. In the *Network Case* group box, expand the case drop-down and select the case that you want to copy. Only cases that you have access to will appear.

   The *Network Case Path* and *Case Size* are automatically populated when you select a case.

   Note: With SQL Express on the local machine, you are limited in the size of the case that you can copy.

8. In the *Mobile Case* group box, do the following:

   8a. Enter a new name for the case by which it will be saved on the local machine.

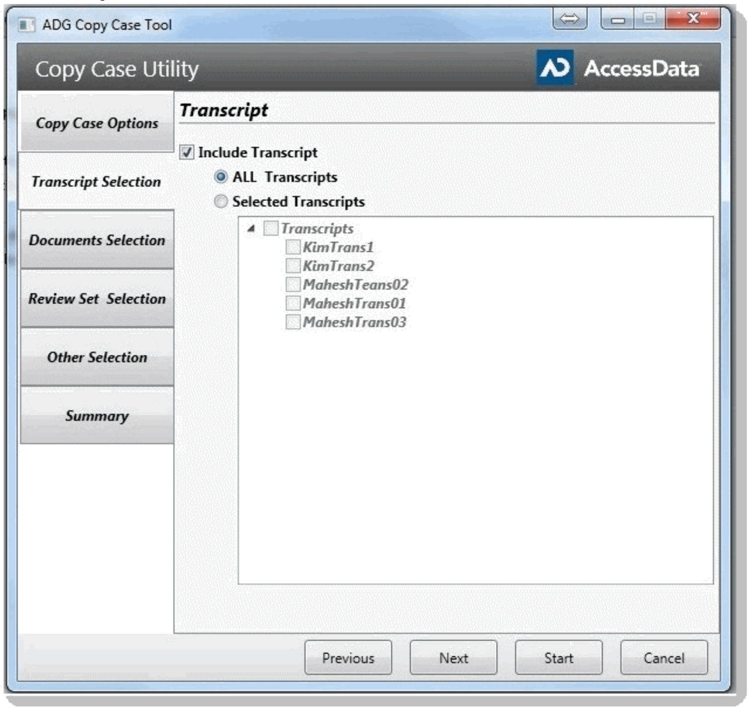
   8b. Browse to a location on the local machine where you want to save the case.

9. In the *Case Elements* group box, select one of the following:
   - **Entire Case**: Select this to copy the entire case to the local machine.
   - **Designated Elements**: Select this to choose what elements you want to copy. You can specify to copy the following: Transcript Groups, Review Sets, Production Sets, Saved Searches, and Labeled Documents.

   Note: What you select in the *Case Elements* group box will determine the next screen you see.

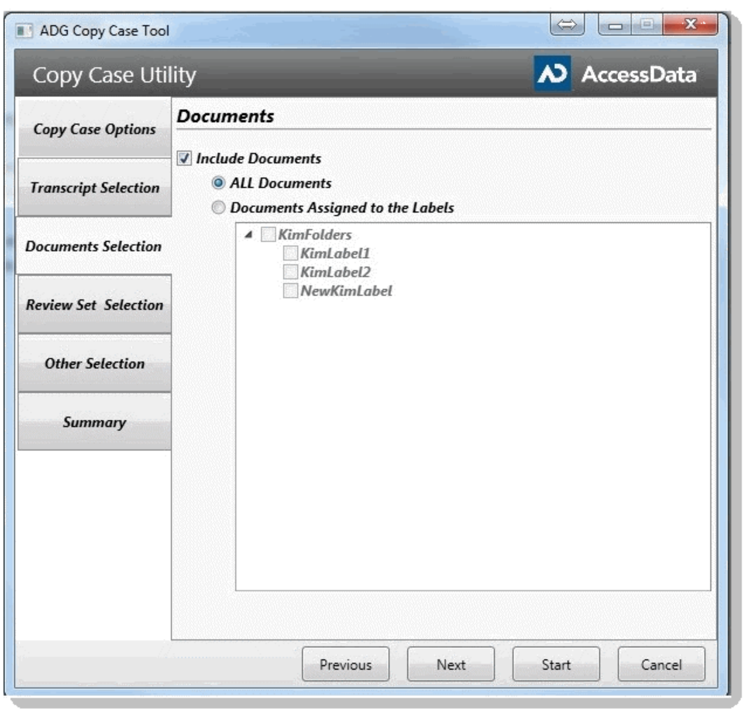
10. Click **Next**.
11. If you selected to copy the *Entire Case*, skip to the Summary step.
12. If you selected to copy *Designated Elements*, you will see the *Transcript Selection* screen.

Transcript Selection Screen



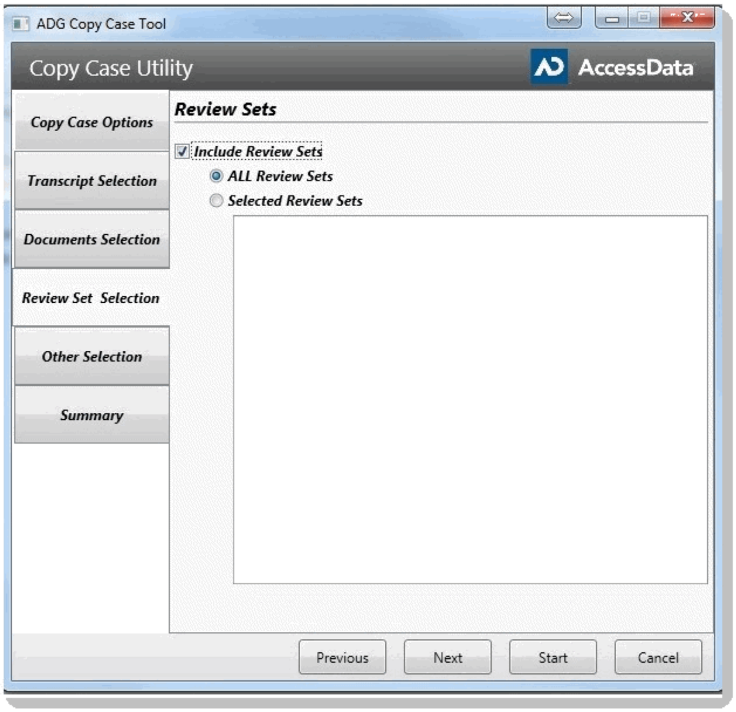
13. In the *Transcript Selection* screen, make selections among the following and click **Next**:
    - **Include Transcript**: Check this to include transcripts in the copy.
        - **All Transcripts**: Select this to include all the transcripts in the case, in the copy.
        - **Selected Transcripts**: Select this to include only the transcript groups that you check in the copy.

Documents Selection Screen



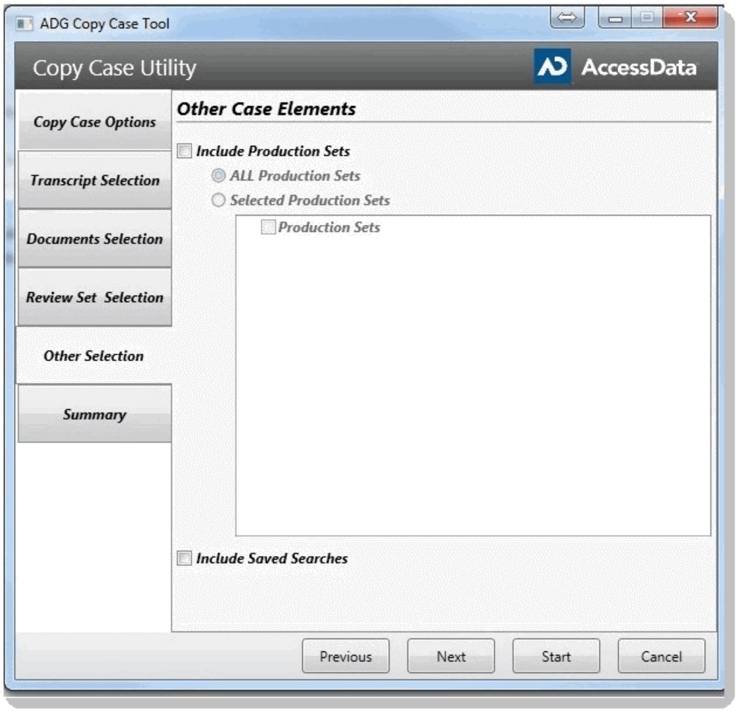
14. In the *Documents Selection* screen, make selections among the following and click **Next**:
    - **Include Documents**: Check this to include documents in the copy.
        - **All Documents**: Select this to include all the documents in the case, in the copy.
        - **Documents Assigned to the Labels**: Select this to include only the documents assigned to labels that you check in the copy.

Review Set Selection Screen



15. In the *Review Sets* screen, make selections among the following and click **Next**:
    - **Include Review Sets**: Check this to include review sets in the copy.
        - **All Review Sets**: Select this to include all the review sets in the case, in the copy.
        - **Selected Review Sets**: Select this to include only the review sets that you check in the copy.

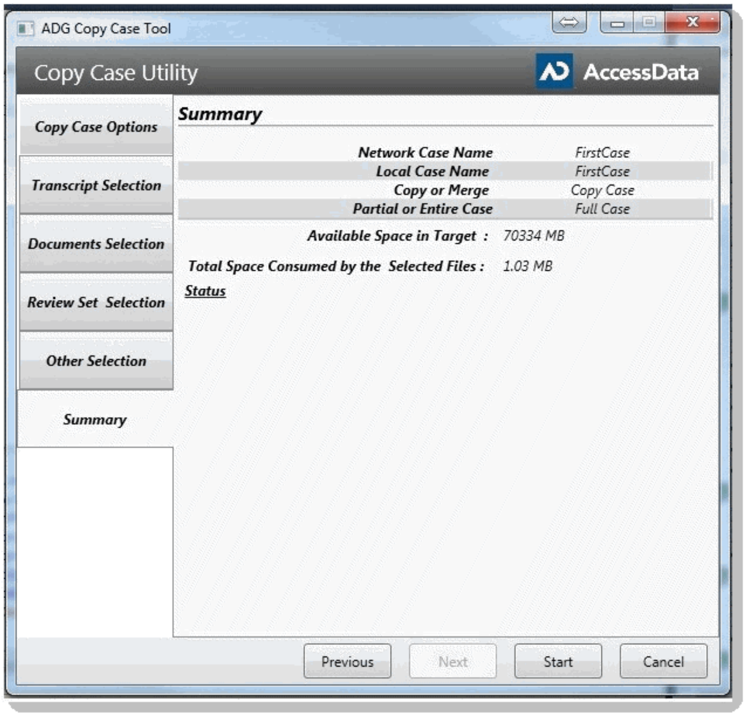
Other Selection



16. In the Other Selection screen, make selections among the following and click **Next**:
    - **Include Production Sets**: Check this to include production sets in the copy.
        - **All Production Sets**: Select this to include all the production sets in the case, in the copy.
        - **Selected Production Sets**: Select this to include only the production sets that you check in the copy.
    - **Include Saved Searches**: Check to include saved searches in the copy.

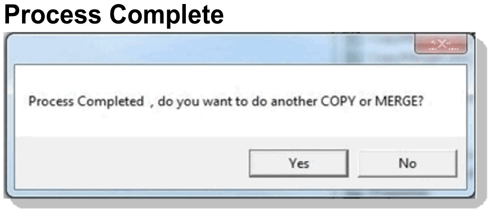
Note: Production sets cannot be changed. If you copy them to your local machine, you will not be able to make any changes to existing production sets and you will not be able to merge them back in to the network case. You can copy them for viewing purposes only.

Summary Screen



17. In the *Summary* screen, review the selections you have made and click **Start**.

Process Complete



18. Click **Yes** to perform another copy or **No** if you are done.
19. Click **Close**.

1.3 Opening the Copy of Your Case Using Summation Mobile

Once you have copied a case to your laptop, you can access the case copy using Summation Mobile that is installed on your laptop. The laptop where you copy your case may also be referred to as the "local machine."

See Copying a Case on page 9.

See Summation Mobile Limitations (page 7) for the limitations of Summation Mobile.

To open your copied case

1. Do one of the following:
   - Double-click the Summation Mobile icon on your desktop.
   - Open a browser and enter localhost or the IP address of your machine.
2. Log in to Summation.
3. Review your case as usual.

1.4 Merging a Copied Case

After you have made your changes to the copied case, you can merge the case back into the network application.

Note: You can merge a copied case only ONCE. Once you have merged a copied case, you cannot merge that copy again. You will need to make another copy of the network case to merge the case again.

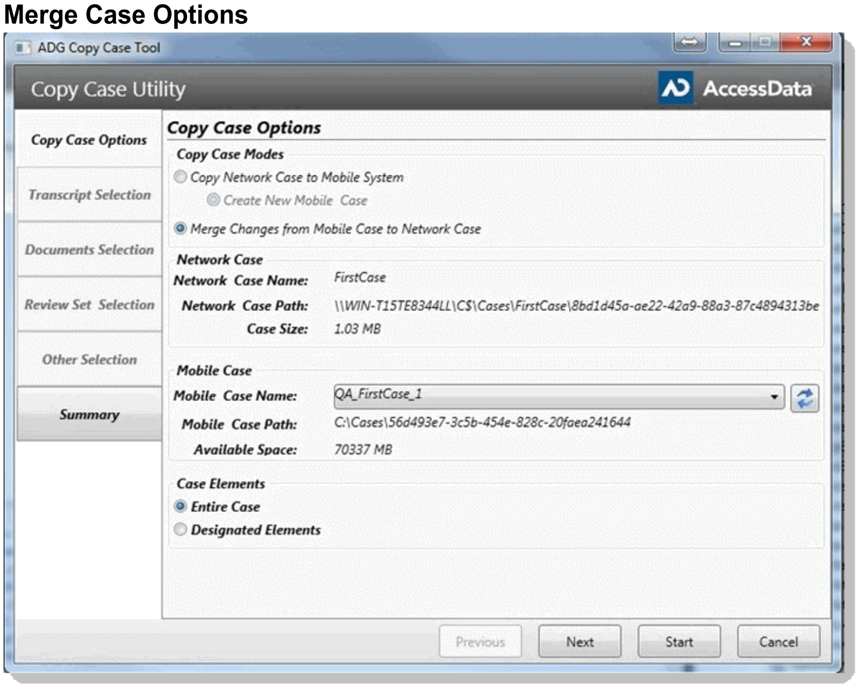
If conflicts appear in a merge, you will be presented with the choice to keep the network version or the copied case version of the conflict. Choosing the copied version will overwrite the network version.

The laptop where you copy your case may also be referred to as the “local machine.”

To merge a copied case back in to the network application

1. Ensure your laptop is connected to the network.
2. Open the Copy Case utility on your laptop.
3. In the *Provided Network Login Information* group box, enter the following:
   - **Network URL**: Enter the URL for the network Summation application.
   - **User Name**: Enter a user with rights to the network.
   - **Password**: Enter the password for the user you entered.
4. In the *Provide Mobile Login Information* group box, enter the following:
   - **User Name**: Enter a user that has access to the case you want to merge.
   - **Password**: Enter the password for the user you entered.
5. Browse to a *Shared Directory*. This directory needs to be a location where both the network and local machine has Read/Write access (used to store data temporarily during the merge process).
6. Click **OK**.

Merge Case Options



7. In the *Copy Case Modes* group box, select **Merge Changes from Mobile Case to Network Case**.
8. In the *Mobile Case* group box, select a copied case from the local machine.

   The respective *Network case Name* and *Network case Path* will be populated automatically.
9. In the *Case Elements* group box, select one of the following:
   - **Entire Case**: Select this to merge the entire case copy to the network application.
   - **Designated Elements**: Select this to choose what elements you want to merge. You can specify to merge the following: Transcripts, Documents, Review Sets, Saved Searches, and Labeled Documents.

Important: Ensure that you check all the items that you want to merge because you will not be able to merge anything again after the merge is complete. You can only merge a case once.

Note: What you select in the *Case Elements* group box will determine the next screen you see.

10. Click **Next.**
11. If you selected to copy the *Entire Case*, skip to the Summary step.
12. If you selected to copy *Designated Elements*, you will see the *Transcript Selection* screen.
13. In the *Transcript Selection* screen, make selections among the following and click **Next**:
    - **Include Transcript**: Check this to include transcripts in the merge.
      - **All Transcripts**: Select this to include all the transcripts in the case, in the merge.
      - **Selected Transcripts**: Select this to include only the transcript groups that you check in the merge.
14. In the *Documents Selection* screen, make selections among the following and click **Next**:
    - **Include Documents**: Check this to include documents in the merge.
      - **All Documents**: Select this to include all the documents in the case, in the merge.
      - **Documents Assigned to the Labels**: Select this to include only the documents assigned to labels that you check in the merge.
15. In the *Review Sets* screen, make selections among the following and click **Next**:
    - **Include Review Sets**: Check this to include review sets in the merge.
      - **All Review Sets**: Select this to include all the review sets in the case, in the merge.
      - **Selected Review Sets**: Select this to include only the review sets that you check in the merge.

Note: Production sets cannot be changed. You will not be able to merge production sets back in to the network case. You can copy them for viewing purposes only.

16. In the *Summary* screen, review the selections you have made and click **Start.**
17. Click **Yes** to perform another copy or **No** if you are done.
18. Click **Close**.