AD Summation

Administration Guide

WebBlaze

Version 3.1
Published: September 2010

AD Summation
425 Market Street, 7th Floor
San Francisco, CA 94105 USA

Contents

Introduction

AD Summation WebBlaze provides users with secure, dynamic access to AD Summation iBlaze case data using a standard Microsoft Windows Internet Explorer web browser. This guide contains information about the following administrative topics:

- Licensing AD Summation WebBlaze
- Setting Password Rules
- Adding Users and Groups
- Setting Group Security and Case Access
- Working with Forms
- Sample Groups and Permissions

The AD Summation WebBlaze interface contains additional administrative functions. See the AD Summation *WebBlaze Online Help* for more information about these functions.

AUDIENCE

This document is intended for AD Summation WebBlaze administrators who have installed the WebBlaze server and who are ready to set up user groups. You must complete the procedures described in the *AD Summation WebBlaze Installation Guide* before proceeding with the information found in this guide.

Once you install the AD Summation WebBlaze server, the **Administrator Console** that you access within AD Summation iBlaze is modified to allow you to administer access for WebBlaze.

STYLES USED IN THIS DOCUMENT

This document provides a number of visual cues to help guide you. The following styles are used in this document:

Italicized Text – Italicized text indicates a new term or a term that is specific to AD Summation WebBlaze or AD Summation. The first time that a new term is used, it is italicized and accompanied by a definition.

Italicized text also indicates the title of another document or section within this document.

Bold Text – Bold text indicates an item that is found on the AD Summation WebBlaze interface, such as a menu option, a window, a field, or a dialog.

NOTE: Notes call attention to supplemental yet important information about the topics covered in this document. Notes also provide suggestions on how to deal more effectively with AD Summation WebBlaze administration, or warnings that you should heed.

Licensing AD Summation WebBlaze

There are two concepts that you should understand when setting user permissions. First, the user must have a seat license. Second, the user must have explicitly assigned permissions to access case data. This section discusses licensing. See the *Setting Group Security and Case Access* section in this document for more information about permissions.

UNDERSTANDING AD SUMMATION WEBBLAZE LICENSING

The AD Summation WebBlaze licensing structure is based on named seats. This means that each AD Summation WebBlaze user must be assigned a licensed seat in order to use the WebBlaze server. The named seat licensing structure allows you to pre-assign a seat license to a particular user or to allow AD Summation WebBlaze to auto-assign the seat license from a pool of available licenses. A user has exclusive use of a seat license until you, the administrator, manually reassign the license to another user or place the license back into the pool of available licenses for auto-assignment.

NOTE: AD Summation WebBlaze licenses and AD Summation iBlaze licenses are completely separate from one another and must be purchased separately.

Your AD Summation WebBlaze installation code includes information about the number of purchased and named seat licenses. You can use the **Administrator Console** in AD Summation iBlaze to activate the additional seats. For more information, see the *Updating Seat Count* section in this document.

NOTE: You must have Internet access on the computer that runs the **Administrator Console** in order to use the **Update Seat Count** option.

To access licensing functions:

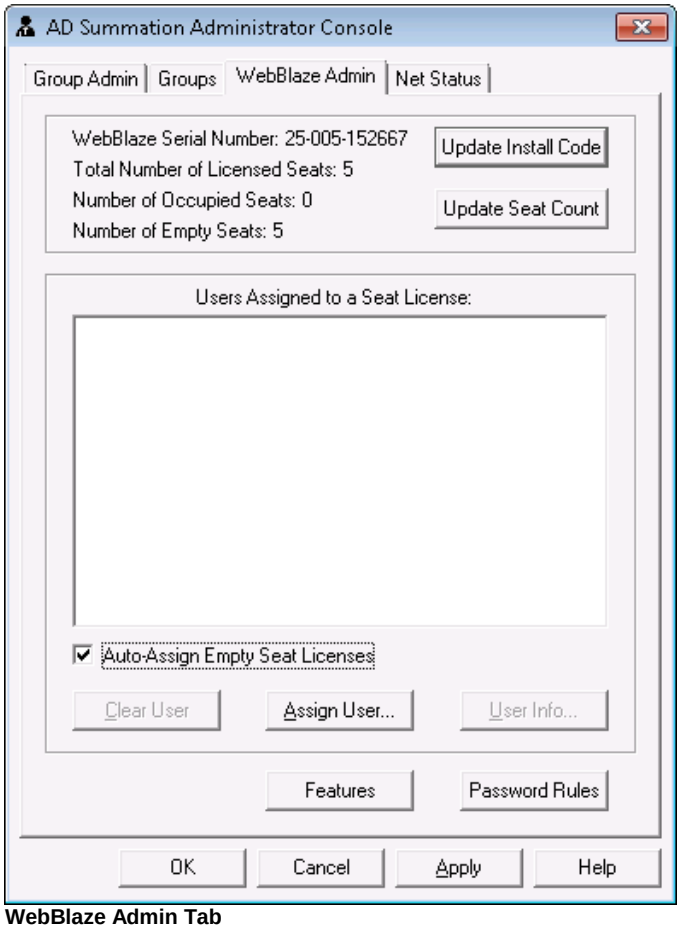
1. From the **File** menu in AD Summation iBlaze, select **Administrator Console**.
   The **Enter Administrator Console Password** dialog is displayed.

   NOTE: Make sure the **Case Explorer** is in focus in order to access **Administrator Console** from the **File** menu.

2. Provide your administrator password and click **OK**.
   The **Administrator Console** is displayed.

   NOTE: The first time that you log into the **Administrator Console**, the default password is **Admin**. Change this password as soon as possible by clicking **System Options** on the **Group Admin** tab and selecting **Set Admin Console Password**.

3. Click the **WebBlaze Admin** tab.



WebBlaze Admin Tab

AUTO-ASSIGNING EMPTY SEAT LICENSES

AD Summation WebBlaze can automatically assign available seat licenses to users when they log on to WebBlaze. A seat is auto-assigned if it is available and if the user has appropriate permissions.

To enable the auto-assignment of seats:

1. Click the **Auto-Assign Empty Seat Licenses** check box on the **WebBlaze Admin** tab of the **Administrator Console.**
2. Click **Apply**.
   Licenses are automatically assigned to users as they log on to AD Summation WebBlaze.
3. If you have no additional administrative tasks in the **Administrator Console**, click **OK**.
   The **Administrator Console** is closed.

UPDATING SEAT COUNT

If you purchase additional seat licenses, use the **Administrator Console** to activate the additional seats. To update the seat count, click **Update Seat Count** on the **WebBlaze Admin** tab. You can also click **Update Install Code** and enter the installation code provided to you by AD Summation to update your seat count.

The information box on the top of the tab reflects your available seats.

NOTE: You must have Internet access on the computer that runs the **Administrator Console** in order to use the **Update Seat Count** option.

ASSIGNING AND CLEARING A LICENSE FOR A USER

You can explicitly assign a seat license to a user. This gives this user exclusive use of a named seat license, removing a seat from the pool of available seats. The seat is associated with the user, and the user is only allowed to log in to AD Summation WebBlaze from one computer at a time.

Before assigning a license to a user, you must add the user to the system. For more information about adding users, see the *Adding Users and Groups* section in this document.

To assign a named seat license to a user:

1. On the **WebBlaze Admin** tab, click **Assign User**.
   The **Select Users to License** dialog is displayed.
2. Select the user or users to whom you want to assign a seat license and click **OK**.
   The user or users are listed in the **Users Assigned to a Seat License** box, and the information box on the top of the tab reflects the number of used seats.

   NOTE: The **Users Assigned to a Seat License** box lists both the users who were assigned seat licenses manually and the users who were automatically assigned seat licenses by AD Summation WebBlaze.
3. Click **Apply** and then **OK**.
   The **Administrator Console** is closed.

To clear a license for a user and return it to the pool of available seats:

1. In the **Users Assigned to a Seat License** box, select the user whose seat license you want to return to the pool of available licenses.
2. Click **Clear User**.

   The user's name is removed from the **Users Assigned to a Seat License** box, and the information box on the top of the tab reflects the number of available seats.
3. Click **Apply** and then **OK**.
   The **Administrator Console** is closed.

VIEWING USER INFORMATION

The **WebBlaze Admin** tab allows you to view the permissions assigned to users who are listed in the **Users Assigned to a Seat License** box.

To view information about a user:

1. In the **Users Assigned to a Seat License** box, select the user whose permissions you want to see.
2. Click **User Info**.
   The **User Info** dialog is displayed, allowing you to see the permissions that the user has been assigned in both WebBlaze and iBlaze. Note that this information is read-only. For more information about setting permissions, see the *Setting Group Security and Case Access* section in this document.
3. Click **OK** to close the **User Info** dialog.

Setting Password Rules

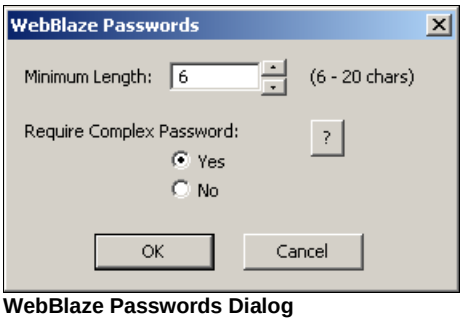
You have the option to enforce password rules for AD Summation WebBlaze users. There are two types of rules:

- **Minimum Length** – Passwords can be between six and twenty characters. You have the option to set a minimum length of six characters or higher. The default minimum password length is six characters.
- **Require Complex Password** – Passwords can contain additional rules. Passwords must not contain the user's account name. In addition, they must contain characters from each of the four following categories:
    - Capital letters (A - Z)
    - Lowercase letters (a - z)
    - Digits (0 - 9)
    - Non-alphanumeric characters (such as !, $, #, or %)

You can set password rules on the **WebBlaze Admin** tab in the **Administrator Console**.

To set password rules for AD Summation WebBlaze users:

1. On the **WebBlaze Admin** tab, click **Password Rules**.
   The **WebBlaze Passwords** dialog is displayed.



WebBlaze Passwords Dialog

2. In the **Minimum Length** box, specify the minimum number of characters that users must include in their passwords.
3. In the **Require Complex Password** area, specify whether you want to use complex password rules.
4. Click **OK**.
   The dialog is closed.
5. If you have no additional administrative tasks in the **Administrator Console**, click **OK**.
   The password complexity rules are set and the **Administrator Console** is closed.

Adding Users and Groups

Permission to access case data on the AD Summation WebBlaze server is assigned through the **Administrator Console** within AD Summation iBlaze. The **Administrator Console** is updated during the installation process of the AD Summation WebBlaze server to include administration settings and tabs that are specific to WebBlaze. This section covers the following topics:

- Adding users and assigning them AD Summation WebBlaze passwords (you can assign WebBlaze passwords to existing AD Summation users as well).
- Creating groups and adding users to the groups (you can also add users to existing groups).

You can also assign security and access case elements, such as specific transcripts or forms. For more information, see the *Setting Group Security and Case Access* section in this document.

NOTE: For security reasons, AD Summation recommends that you create a group and set security on it before adding users to the group. This prevents users from potentially logging on to AD Summation WebBlaze before you have limited their access.

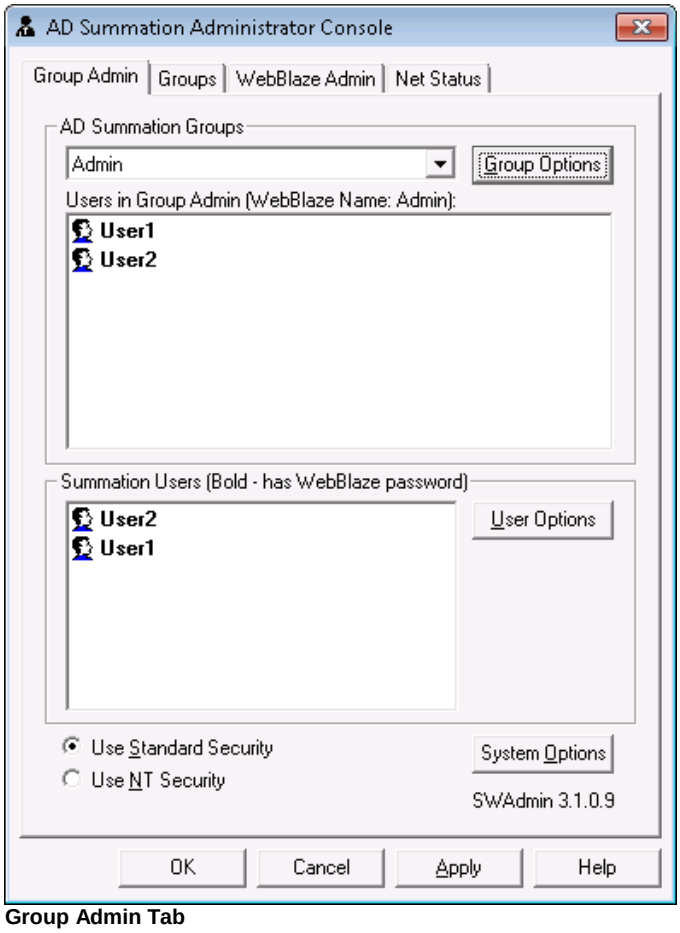
You can add users and groups on the **Group Admin** tab of the **Administrator Console**.

To access the **Group Admin** tab:

1. From the **File** menu in AD Summation iBlaze, select **Administrator Console**.
   The **Enter Administrator Console Password** dialog is displayed.

   NOTE: Make sure the **Case Explorer** is in focus in order to access the **Administrator Console** from the **File** menu.

2. Type your administrator password in the box and click **OK**.
   The **Administrator Console** is displayed, with the **Group Admin** tab topmost by default.



Group Admin Tab

ADDING USERS AND ASSIGNING AD SUMMATION WEBBLAZE PASSWORDS

Existing AD Summation users are listed in the **Summation Users** box in the lower portion of the **Group Admin** tab. You can add new users in this area, and you can assign AD Summation WebBlaze passwords to existing users. This section explains how to do both.

ASSIGNING AD SUMMATION WEBBLAZE PASSWORDS TO EXISTING USERS

Users who have AD Summation WebBlaze passwords are listed in bold in the **Summation Users** box. Users who do not have WebBlaze passwords are listed in regular text. You can assign a AD Summation WebBlaze password to an existing user in the **Summation Users** box.

To assign a AD Summation WebBlaze password to an existing user:

1. Select the user to whom you want to assign a WebBlaze password and click **User Options**.
   A menu is displayed.
2. Select **Set WebBlaze Password**.
   The **User Password Change Dialog** is displayed.

   NOTE: You can access this same menu by right-clicking a user name.
3. Type a password in the **WebBlaze Password** box.
4. Retype the password in the **Re-Enter Password** box.

5. Click **OK**.
6. Repeat Steps 1 through 5 for other users as needed.

7. When you are finished assigning passwords, click **Apply**.
   The passwords are saved.
8. If you have no additional administrative tasks in the **Administrator Console**, click **OK**.
   The **Administrator Console** is closed.

ADDING USERS

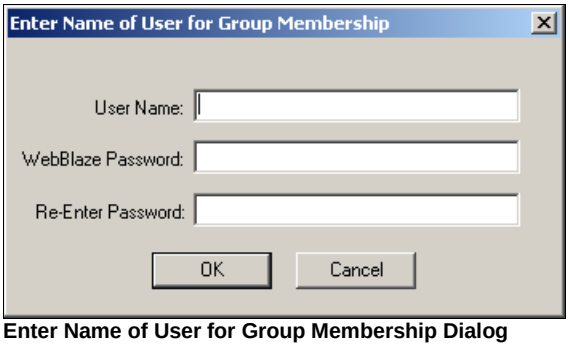
You can add new AD Summation WebBlaze users in the **Summation Users** box on the **Group Admin** tab.

NOTE: When you create users with **NT Security**, these users will only be able to log in to AD Summation WebBlaze. These users will not be able to access the network in which the AD Summation WebBlaze server and the AD Summation LAN server reside.

To add users:

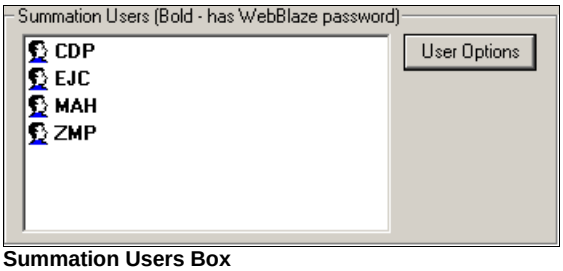
1. In the **Summation Users** box, click **User Options**.
   A menu is displayed.

   NOTE: You can also access this same menu by right-clicking a user name.
2. Click **Add User to System**.
   The **Enter Name of User for Group Membership** dialog is displayed.



Enter Name of User for Group Membership Dialog

3. Type the user name that you want to assign to the user in the **User Name** box.
4. Type a password for the user in the **WebBlaze Password** box.
5. Retype the password in the **Re-Enter Password** box.
6. Click **OK**.
   The user is added to the **Summation Users** box and the **Enter Name of User for Group Membership** dialog remains open.



Summation Users Box

7. Repeat Steps 3 through 6 for any additional users that you need to add.

8. Click the **Close** icon in the upper right of the dialog when you are finished adding users.
9. Click **Apply**.
   The user names and passwords are saved.
10. If you have no additional administrative tasks in the **Administrator Console**, click **OK**.
    The **Administrator Console** is closed.

You can now create groups and add the users to groups.

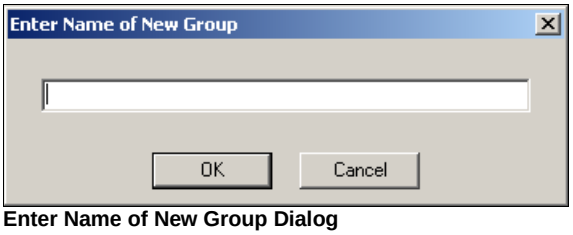
ADDING GROUPS

Permissions and case access are set for users on a per group basis. Therefore, you have to assign users to a group to give them access to AD Summation WebBlaze features and cases. You can add groups in the **AD Summation Groups** box on the **Group Admin** tab. If you already have existing groups set up that fit your needs, skip to Step 4 in the following procedure to learn how to add users to a group. Once you have set up your groups, you can set permissions for those groups. For information about setting permissions, see the *Setting Group Security and Case Access* section in this document.

Read the *Appendix A: Sample Groups and Permissions* section in this document for ideas about groups and the permissions that you might want to assign to them. This appendix is not an exhaustive list, but can be used as a starting point. Groups and permissions will vary according to your needs and the practices of your firm.

To add a group:

1. In the **AD Summation Groups** area, click **Group Options**.
   A menu is displayed.
2. Select **Add AD Summation Group**.
   The **Enter Name of New Group** dialog is displayed.

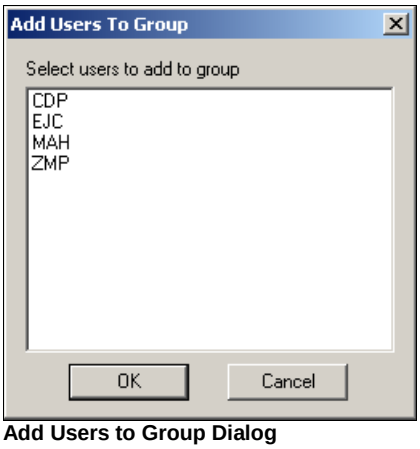


Enter Name of New Group Dialog

3. Type the name of the new group in the box and click **OK**.
   The group is listed in the **AD Summation Groups** drop down list, and you can add users to the **Users in Group** box.

   NOTE: If you want to add users to an existing group, select the group from the drop down list and follow the remaining steps in this procedure.

4. Click **Group Options**.
   A menu is displayed.
5. Click **Add Users to AD Summation Group**.
   The **Add User to Group** dialog is displayed, listing the AD Summation users.



Add Users to Group Dialog

6. Select the user or users that you want to add to the group and click **OK**.
   The users are added to the group and listed in the **Users in Group** box.
7. Click **Apply**.
   Your additions are saved.
8. If you have no additional administrative tasks in the **Administrator Console**, click **OK**.
   The **Administrator Console** is closed.

You can now set group security and case access.

Setting Group Security and Case Access

There are three levels of security that you can set:

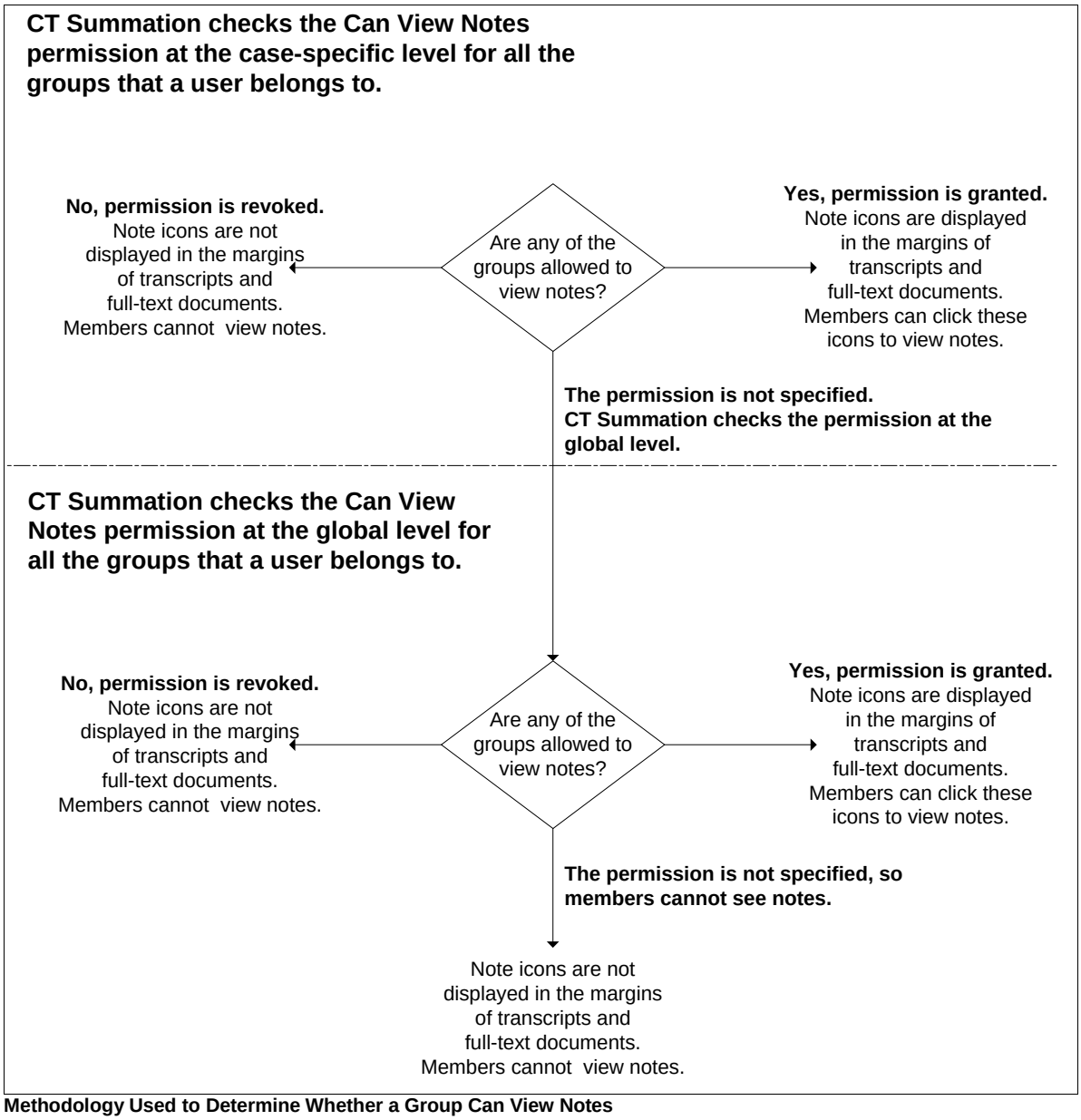
- **Global permissions** – These are permissions for a group that apply to any case in AD Summation WebBlaze. Group members can use or are blocked from using a function in any case that they are working on in AD Summation WebBlaze. For example, you can allow users to mark up images in all cases.
- **Case-specific permissions** – These are permissions for a group that apply to a specific case. Group members can use or are blocked from using a function in a specific case that they are working on in AD Summation WebBlaze. For example, in a particular case, you can disallow members from marking up images even though the members can mark up images in all other cases. Case-specific permissions take priority over global permissions.
- **Access permissions for specific case elements** – Group members can be allowed or disallowed to access specific case elements, such as the **Events** form or specific transcripts.

AD Summation recommends that you set a group's global permissions for all cases in AD Summation WebBlaze first, and then allow or disallow permissions for a specific case as needed.

It is helpful to understand the way that AD Summation applies permissions for users. The system first looks at the functions that a user has permission to use by checking the case-specific permissions for all the groups to which the user belongs. If a permission is granted or revoked for use within a specific case, AD Summation uses that setting. If a permission is left unspecified, AD Summation checks the permission at the global level. If a permission is granted or revoked at the global level, that setting is used. If the permission is not specified, the user does not have access to that function.

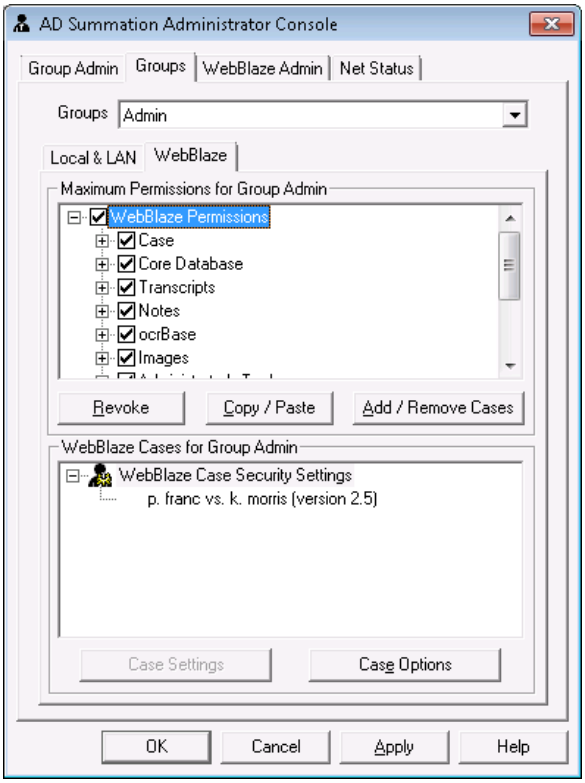
NOTE: If a user belongs to two groups and the same permission is granted in one group and revoked in the other, the revocation takes priority.

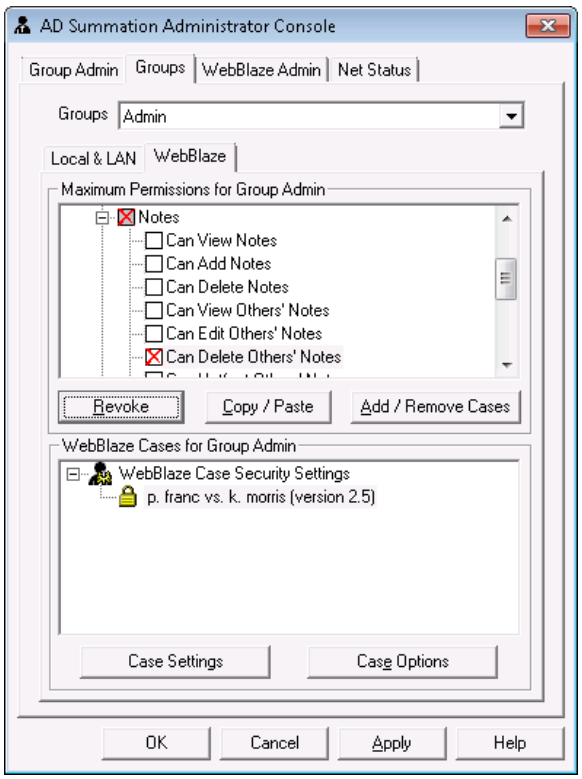
The following diagram illustrates the method that AD Summation uses to determine which WebBlaze functions are available to a group, using the **Can View Notes** permission as an example.



Methodology Used to Determine Whether a Group Can View Notes

In the following example, the **Testifying Experts** group is allowed to use all of the **Notes** functionality at the global level (the screen on the left). For the **P. Franc vs. K. Morris** case, most of the **Notes** permissions are not specified (the screen on the right). Therefore, AD Summation applies the global permissions to the **P. Franc vs. K. Morris** case, allowing the group to use these functions. However, the permission **Can Delete Others' Notes** is revoked for the **P. Franc vs. K. Morris** case. This means that the users in the **Testifying Experts** group are not allowed to delete others' notes, even though this function is allowed at the global level.





Notes Permissions for All Cases and a Specific Case

The basic steps for setting permissions at global and case-specific levels are as follows:

1. Set the maximum level of permissions for the group at the global level. For information about setting permissions for a group, see *Setting the Securable Permissions for a Group*.
2. Add the case or cases to which the group will have access using AD Summation WebBlaze. For more information about adding cases, see *Specifying Case Access Settings*. At this point, you can also set access permissions to case elements.
3. With a specific case selected, set the appropriate case-specific permissions for the group if it is necessary to further restrict or override the global permissions that were set in Step 1. For information about these permissions, see *Setting the Securable Permission for a Group*.
4. If you did not set access to case elements in Step 2, set access to various case items per the needs of the group and your firm. You can also set a password for the case. For more information about these items, see *Specifying Case Access Settings*.

SETTING THE SECURABLE PERMISSIONS FOR A GROUP

You can set group permissions globally and for specific cases in AD Summation WebBlaze. These functions are listed according to the categories shown on the **Administrator Console** in the **Maximum Permissions for Group** box. As an administrator, you can select a category heading to grant, revoke, or leave unspecified all the permissions within that category.

It is important to note that some permissions are dependent upon related permissions. For example, if the group is not granted the permission **Can Open Form View**, the group will not be able to use the related functions **Can Add to Database** and **Can Edit Database** even if those permissions are granted. This is because the group needs access to the Form View in order to use the **Can Add to Database** and **Can Edit Database** functions.

NOTE: You should understand how permissions work for a group at a case-specific level and at a global level. This information is provided at the beginning of the *Setting Group Security and Case Access* section in this document.

To set securable permissions for a group:

1. From the **File** menu in AD Summation iBlaze, select **Administrator Console**.
   The **Enter Administrator Console Password** dialog is displayed.

   NOTE: Make sure the **Case Explorer** is in focus in order to access the **Administrator Console** from the **File** menu.
2. Type your administrator password in the box and click **OK**.
   The **Administrator Console** is displayed.
3. Click the **Groups** tab.
4. From the **Groups** drop down list, select the group for which you want to set permissions.
5. Click the **WebBlaze** tab underneath the drop-down list.
6. In the **WebBlaze Cases for Group** box, click **WebBlaze Case Security Settings**.

   NOTE: Selecting **WebBlaze Case Security Settings** allows you to set global security for cases in AD Summation WebBlaze. You will set security for specific cases later in the procedure.
7. In the **Maximum Permissions for Group** box, set the permissions for the group. See the *Securable Permissions for a Group* table in this document for descriptions of the categories and functions for which you can set permissions. You can grant or revoke a permission, or leave the permission unspecified.
8. To grant a permission, click the check box next to the permission. A check mark is displayed in the check box.
9. To revoke a permission, highlight the permission and click **Revoke**.
   A warning message is displayed.
10. Click **OK**.
    A red **X** is displayed in the check box.
11. Click **Apply**.
    The permissions are set.
12. Click **Add/Remove Cases** to select the cases to which the group will have access. (For detailed information about setting case security and creating case paths to case data, see the *Using the Administrator Console* topics in the AD Summation iBlaze Online Help.)
    The **Case Info Files** dialog is displayed.
13. Select the cases to which the group will have access and click **OK**.
    The cases are listed in the **WebBlaze Cases for Group** box.

NOTE: At this point, you can opt to specify access to various case elements, such as specific forms, transcripts, or Document Collections. For more information, see the *Specifying Case Access Settings* section in this document.

14. In the **WebBlaze Cases for Group** box, select a case for which to set permissions.
15. In the **Maximum Permissions for Group** box, set the permissions for the group while working in the case you selected. Alternatively, if you do not set case-specific permissions in this step, the group will inherit the global permissions that you set in Step 7. See the *Securable Permissions for a Group* table in this document for descriptions of the categories and functions for which you can set permissions.
16. Click **Apply**.
    The permissions are set.
17. Repeat these steps for additional cases if necessary.
    Your additions are saved.
18. If you have no additional administrative tasks in the **Administrator Console**, click **OK**.
    The **Administrator Console** is closed.

At this point, you can further restrict or grant access to case-specific items. For more information, see *Specifying Case Access Settings*.

SECURABLE PERMISSIONS FOR A GROUP TABLE

CATEGORY	PERMISSION	DESCRIPTION
Case	Can View Case Organizer Tabs	The **Case Organizer** is available in the **Case Explorer**. You can further specify which **Case Organizer** outlines should be available to the group. For more information, see *Specifying Case Access Settings.*
	Can View Case Organizer Links	The ability to click and view links to images, transcripts, and OCR documents from a **Case Organizer** outline. This permission works in conjunction with the **Can View Transcripts**, **Can View Images**, and **Can View ocrBase Docs** permissions. For instance, if a group has been granted the **Can View Case Organizer Links** permission, but does not have the **Can View Transcripts** permission, the group members will not see any links to transcripts that exist in the outline. **NOTE:** This permission provides the ability to view and click these links. **Case Organizer** outlines may contain links to privileged information or other material that you do not want to expose. Such exposure may lead to the discovery of the linked item. For this reason, AD Summation recommends that you do not grant the **Can View Case Organizer Links** permission for groups with users who are external to your firm.
	Can View eDocs	The **eDocs & eMail** component is added to the **Case Explorer**. Group members can include these components in a search from the **Core Database**, and have the ability to view e-mail messages, attachments, and electronic documents from either a **Core Database** record or from the **Search Results** page.
	Can View Others' Search Results' HotFacts	The ability to see **HotFact** designations on records that are specified as **HotFacts** by other users in the **Search Results** report. If this permission is not granted, users will only be able to search for their own **HotFact** designations.

CATEGORY	PERMISSION	DESCRIPTION
	Can Open Search Results	The ability to check items in the **Case Explorer** to search, and display search hits on the **Search Results** page. **NOTE**: Users must have this permission in order to conduct searches of multiple case elements simultaneously. Users can only search those areas that they have permission to view. For example, if group members have access to **Transcripts** and **Document Collections**, they can search both of these case components at the same time. However, these users will not be able to search the **Core Database** unless they have permission to view this case component.
	Can Batch Add MultiEntry Items	The ability to add the same information to a multi-entry field in more than one record at the same time.
	Can Tally	The ability to use the **Tally** feature on applicable fields. This feature allows group members to see the number of times an entry (such as a date or an issue) occurs in a given field.
Core Database	Can View Core DB	The **Core Database** is listed in the **Case Explorer**, and group members can open it to display records. Group members can also include it in a search if the **Can Open Search Results** permission is also granted.
	Can Add to Database	The ability to add new summaries to the **Core Database** through the Form View. This permission requires that **Can Open Form View** and **Can Edit Database** be allowed. If **Can Edit Database** is not allowed, group members will receive an empty form with read-only fields.
	Can Edit Database	The ability to edit **Core Database** records through the Form View. This permission requires that **Can Open Form View** be allowed.
	Can Open Form View	The ability to switch to the Form View. This permission must be allowed if you want to allow group members to perform related functions such as adding records or editing records. You can further specify which forms should be available to the group. (For more information, see *Specifying Case Access Settings*.)
	Can Open Column View	The ability to open the **Core Database** in Column View, or switch to the Column View from the Form View. You can further specify which forms should be available to the group. (For more information, see *Specifying Case Access Settings*.) The forms' corresponding tables are displayed in the Column View.
	Can HotFact Core	The ability to mark records in the **Core Database** as **HotFacts**. This permission requires the ability to open either the Column View or the Form View, and also requires the ability to edit the database (**Can Open Form View** or **Can Open Column View**, **Can Edit Database**).
	Can View Stacked Core Form	The ability to view the stacked form for a record. The stacked form displays the fields that are listed in the Column View. You can further specify which forms should be available to the group. (For more information, see *Specifying Case Access Settings*.) This permission requires that **Can Open Form View** be allowed.
	Can Add & Edit Lookups	The ability to add items to lookup tables and edit items in lookup tables. This option requires that **Can Batch Add MultiEntry Items** and **Can Edit Database** be allowed, as well as either **Can Open Column View** or **Can Open Form View**.
	Can Delete Lookups	The ability to delete items in lookup tables.
Transcripts	Can View Transcripts	The ability to view transcripts in the **Case Explorer** and include them in searches, if the **Can Open Search Results** permission is also allowed. You can further specify which transcripts or transcript groups should be available to the group. (For more information, see *Specifying Case Access Settings*.)

CATEGORY	PERMISSION	DESCRIPTION
	Can View Evidence Links in Transcripts	The ability to click links within an open transcript to view related testimony in another transcript or images in the **Core Database**. If this permission is revoked (or is not granted), group members will not see the links within a transcript. **NOTE**: Your transcripts may contain links to privileged information or other material that you do not want to expose. Such exposure may lead to the discovery of the linked item. For this reason, AD Summation recommends that you use extreme care when granting this permission to groups with users who are external to your firm.
Notes	Can View Notes	The **Transcript Notes** and **ocrBase Notes** case components are listed in the **Case Explorer** and can be included in searches, if the **Can Open Search Results** permission is also allowed. If a group does not have the ability to view notes created by others (**Can View Others' Notes**), then the only notes that a group member can search are his or her own notes. This permission also displays note icons in the margins of transcripts and full-text documents in the **ocrBase**.
	Can Add Notes	The ability to add notes to a transcript or a document in the **ocrBase**. This function requires that the group has the ability to view notes (**Can View Notes**).
	Can Delete Notes	The ability to delete transcript or **ocrBase** notes. If the group does not have the ability to view notes created by others (**Can View Others' Notes**), then members can only delete their own notes.
	Can View Others' Notes	The ability to view notes created by other users. This permission is useful, for example, if you want to block users outside of your firm from viewing attorney or other employee notes.
	Can Edit Others' Notes	The ability to edit other users' transcript notes and **ocrBase** notes. This function requires that the group has the ability to view notes created by others (**Can View Others' Notes**).
	Can Delete Others' Notes	The ability to delete other users' transcript notes and **ocrBase** notes. This function requires that the group has the ability to view notes created by others (**Can View Others' Notes**).
	Can Hotfact Others' Notes	The ability to mark notes created by other users as **HotFacts**. This function requires that the group has the ability to view notes created by others (**Can View Others' Notes**).
ocrBase	Can View ocrBase Docs	The **ocrBase** case component is listed in the **Case Explorer**, and the group has the ability to view **ocrBase** documents from either a **Core Database** record or by including the **ocrBase** component in a search from the **Case Explorer**.
Images	Can View Images	The ability to view images from a **Core Database** record, from a **Document Collection**, from the **Search Results** page, or from an **ocrBase** document.
	Force Burn-in Redactions	Redactions are always burned-in for members of the group. Users cannot view an image without redactions displayed. Compare with **Can View Original Image**.
	Force Burn-in Markups	Image markups are always burned-in for members of the group. Users cannot view an image without markups displayed. Compare with **Can View Original Image**.
	Can View Original Image	The ability to see an original image without redactions or markups. This permission will be overridden if **Force Burn-In Redactions** or **Force Burn-in Markups** is granted. Conversely, these permissions are overridden if **Can View Original Image** is granted.
	Can Add Markups	The ability to add markups to images. If you want the group to be able to add markups, **Can View Images** must also be allowed.
	Can View Others' Markups	The ability to view image markups created by other users. If you want the group to be able to view markups, **Can View Images** must also be allowed.

CATEGORY	PERMISSION	DESCRIPTION
	Can Edit Others' Markups	The ability to edit the image markups created by other users. If you want the group to be able to edit markups created by others, **Can View Images** and **Can View Others' Markups** must also be allowed.
	Can Delete Others' Markups	The ability to delete image markups created by other users. If you want the group to be able to delete markups created by others, **Can View Images** and **Can View Others' Markups** must also be allowed.
	Can Set Image Label Information	The ability to add labels to images. Image labels can be set on a per-user basis.
Administrator's Tools	Can View Net Status	The ability to view the **Net Status** page. The **Net Status** page shows who is online, the IP address of each user, the last access date and time for each user, the login date and time for each user, and the case that each user is accessing.
	Can Administer Net Status	The ability to use the functions on the **Net Status** page to get an updated view of the net status, end another user's session, and block and allow AD Summation WebBlaze access.
	Can Set Timeout	The ability to view and administer the **Set Timeout** page. This page is used to set the amount of time users are idle before their logins time out.
	Can Administer Login Status	The ability to view and administer the **Login Status** page. This page is used to unlock user logins, set the **Lockout Timeout**, set the **Login Failure Timeout**, view and clear the **Login Log** and **Case Access Log**, and **Update Login Status**.
	Can Set Max Rows Returned	The ability to view and administer the **Search Results Limit** page. This page is used to set the maximum number of rows that can be returned in a search, which affects the amount of time needed to perform a search.
	Can Set Global Date & Time Format	The ability to view and administer the **Date & Time Format** page. This page is used to set the default date and time formats used globally in AD Summation WebBlaze. The date and time settings apply to new WebBlaze users and to existing WebBlaze users who have not changed the date and time settings in the **User's Tools**.
	Can Administer Review Sets	The ability to create, edit, and delete **Review Sets**.
	Can View All Review Sets	The ability to view all existing **Review Sets**. Users are able to view **Review Sets** that are assigned to them. If this permission is granted, group members can see all **Review Sets**, regardless of whom they are assigned to.
User's Tools	Can Message Users	The ability to use the **Messaging** function to send messages to other users on the system. The **Messaging** page displays the user names of other users who are currently using AD Summation WebBlaze.
	Can View Version About	The ability to see and click the AD Summation WebBlaze version number on the bottom right side of the **Home** Page. Clicking this number displays detailed WebBlaze information that is useful to AD Summation Product Support for troubleshooting. You should review the information displayed on the **WebBlaze Version About** window before deciding to expose this information to external users.
	Can Change Password	The ability for group members to change their own passwords. You can enforce complex password rules to ensure the security of your data. For more information, see *Setting Password Rules*.
	Can Set Date & Time Format	The ability for group members to set the date and time formats used throughout their personal instances of AD Summation WebBlaze.
Messages & Alerts	Can View Global Alerts	The ability for group members to see global alerts on the AD Summation WebBlaze **Home** page. These alerts are visible to all users regardless of the cases that they are working on.
	Can Add & Edit Global Alerts	The ability for group members to create or edit global alerts. These alerts are visible to all users regardless of the cases that they are working on. This ability requires that **Can View Global Alerts** also be allowed.

CATEGORY	PERMISSION	DESCRIPTION
	Can Delete Global Alerts	The ability to delete global alerts that are displayed on the AD Summation WebBlaze Home page. This ability requires that **Can View Global Alerts** also be allowed.
	View Case Alerts	The ability to view an alert that is applicable to a specific case on the AD Summation WebBlaze **Home** page.
	Can Add & Edit Case Alerts	The ability to create or edit alerts on the AD Summation WebBlaze Home page that pertain to a case. This ability requires that **View Case Alerts** also be allowed.
	Can Delete Case Alerts	The ability to delete an alert that pertains to a case that is displayed on the AD Summation WebBlaze **Home** page. This ability requires that **View Case Alerts** also be allowed.
Document Collections	Can View Document Repository	The **Document Collections** case component is listed in the **Case Explorer** and group members can select a **Document Collection** to open. You can further specify which collections should be available to the group. (For more information, see *Specifying Case Access Settings*.)
	Can Open Doc Collection Column View	The ability to open a **Document Collection** in Column View, or switch to the Column View from the Form View. You can further specify which forms should be available to the group. (For more information, see *Specifying Case Access Settings*.) The forms' corresponding tables are displayed in the Column View.
	Can Open Doc Collection Form	The ability to switch to Form View. This permission must be allowed if you would like for group members to perform related functions such as adding records or editing records. You can further specify which forms should be available to the group. (For more information, see *Specifying Case Access Settings*.)
	Can Add to Doc Collection	The ability to add a record to a **Document Collection** in the Form View. This ability requires that **Can Open Doc Collection Form** is also allowed.
	Can Edit Doc Collection	The ability to edit a **Document Collection** in the Form View. This ability requires that **Can Open Doc Collection Form** is also allowed.
	Can Hotfact Doc Collection	The ability to mark records in **Document Collections** as **HotFacts**.
	Can Search Doc Collections	The ability to select a **Document Collection** in the **Case Explorer** to include in a search.
	Can View Stacked Doc Coll Form	The ability to view the stacked form for a **Document Collection** record. The stacked form displays the fields that are listed in the Column View. You can further specify which forms should be available to the group. (For more information, see *Specifying Case Access Settings*.)
People & Events	Can View People	The ability to view the **People** table.
	Can View Chronology of Events	The ability to view the **Chronology of Events** table.
	Can View Event Links	The ability to click and view links to depositions (in the **DepoIDs** column) or to **Core Database** record information and associated images (in the **DocID** column). This permission works in conjunction with the **Can View Transcripts**, **Can View Core DB**, and **Can View Images** permissions. **NOTE**: Some **Chronology of Events** records may contain links to depositions or to **Core Database** record information and images. **Chronology of Events** records may contain links to privileged information or other material that you do not want to expose. Such exposure may lead to the discovery of the linked item. For this reason, AD Summation recommends that you use extreme care when granting this permission for groups with users who are external to your firm.
	Can Set Event Effects	The ability to assign event effects to **Chronology of Events** items. This allows group members to identify an item with a range of effects from **Very Negative** to **Very Helpful**.

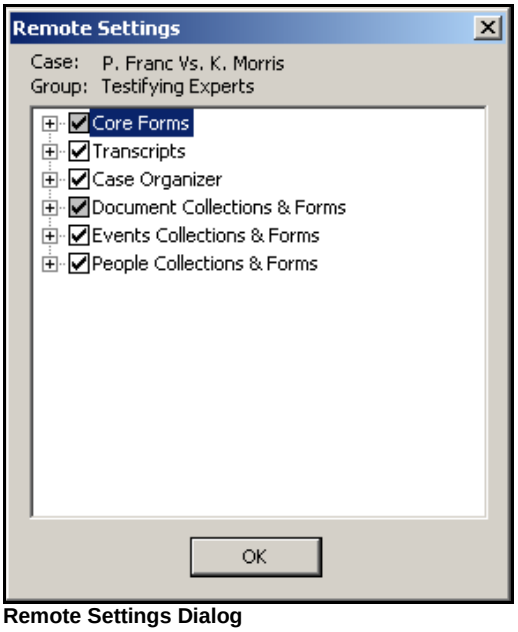
SPECIFYING CASE ACCESS SETTINGS

You can grant or revoke access to specific case elements for a group according to the needs of the group and your firm. In addition, you can also set a password for accessing the case. This section explains both of these tasks.

NOTE: The steps in this section assume that you are setting access for a case that you have already added to the **WebBlaze Cases for Group** box. You may also set access at the time that you add the case. See the *Setting the Securable Permissions for a Group* section in this document for more information.

To specify case access settings:

1. In the **WebBlaze Cases for Group** box, select the case for which you want to set access to case items.
2. Click **Case Settings**.
   The **Remote Settings** dialog is displayed. The settings available on this dialog are determined by the permissions that are set for the group and by the items that are available in the case. For example, if the group does not have permissions set in the **Case** and **Core Database** categories in the **Maximum Permissions for Group** box, then the **Core Forms** and **Case Organizer** settings will appear as **Revoked** in the **Remote Settings** dialog. As an additional example, the items listed under the **Document Collections & Forms** and **Transcripts** categories are dependent upon the availability of **Document Collections**, transcripts, and transcript collections in the case.



Remote Settings Dialog

3. Adjust access as needed, and click **OK** to save your changes. The *Case Access Settings* table displayed below describes the categories on the **Remote Setting**s dialog.

CASE ACCESS SETTINGS TABLE

CATEGORY	DESCRIPTION
Core Forms	Specifies the **Core Database** forms that the group members can access from within AD Summation WebBlaze. Clicking this category gives the group access to all the forms listed. You can also restrict access to specific forms.
Transcripts	Specifies whether the group has access to all transcripts associated with the case, or to one or more different transcript groups. The transcript groups listed correspond to those set up in the **Case Explorer** in AD Summation iBlaze.

CATEGORY	DESCRIPTION
Case Organizer	Specifies the **Case Organizer** areas pertaining to the case that the group can access, including specific tabs that were set up locally.
Document Collections & Forms	Specifies the **Document Collections** pertaining to the case that the group can access. You can expand each collection and specify individual forms pertaining to the collection that the group can access.
Events Collections & Forms	Specifies the **Chronology of Events** collections and forms that the group can access. You can expand each collection and specify individual forms pertaining to the collection that the group can access.
People Collections & Forms	Specifies the **People** collections and forms that the group can access. You can expand each collection and specify individual forms pertaining to the collection that the group can access.

SETTING A PASSWORD FOR A SPECIFIC CASE

You can set a password for specific cases. This requires users to enter a case password before opening a case in AD Summation WebBlaze.

To set a password for a case:

1. In the **WebBlaze Cases for Group** box, select the case for which you want to set a password.
2. Click **Case Options**.
   A menu is displayed.
3. Select **Set Password on this case**.
   The **Set Case Password** dialog is displayed.
4. Type a password for the case in the **New Password** box.
5. Retype the password in the **Confirm New Password** box.
6. Click **OK**.
   The password is set for the case.

Working with Forms

When you install AD Summation WebBlaze, the **Form Editor** that comes with AD Summation iBlaze is automatically upgraded. You do not have to take any additional steps to use the forms that were originally created in AD Summation iBlaze. Your forms are automatically upgraded when you add a case to WebBlaze. For information about creating or modifying forms, see the **Form Editor** topics in the AD Summation iBlaze Online Help.

NOTE: When you install AD Summation WebBlaze, the **Data Access** components (**DataAccess.exe**) are placed in your AD Summation iBlaze program directory. These components are required to work with certain parts of the **Administrator Console** and the new **Form Editor**. You may be prompted to install the **Data Access** components when using the **Administrator Console** or the **Form Editor**.

Appendix A: Sample Groups and Permissions

This appendix provides example setups for typical groups and the permissions that you might want to assign to them. The groups described in this section do not provide an exhaustive list and are for the purpose of example only. Groups and permissions will vary according to your needs and the practices of your firm.

FIRST CHAIR LAWYER

This group can access all case data, transcripts, and notes. This includes the **Core Database**, images, documents in the **ocrBase**, electronic documents, e-mail messages, the **Chronology of Events**, and so on.

This group has administrative rights and permissions to the entire case, and has view all, add all, and edit all rights.

These settings are an example of the general use of the features and functionality of AD Summation WebBlaze.

GENERAL COUNSEL

This group can access specific documents such as images, documents in the **ocrBase**, select data housed in a **Review Set**, and subsets of transcript information. This group should also have access to the **ocrBase** and to images.

This group can add information to the beginning of the **Summary** and **Attynote** fields, and has the ability to add issues and to tally. This group has read-only rights to other data, and can add notes to selected transcripts and **ocrBase** documents.

These settings provide focused access and “prepend” collaborative functionality. Counsel has access to just those documents that he or she seeks to review, with the corresponding ability to collaborate on those documents and transcripts. Edit rights are limited for this group.

CO-COUNSEL

This group can access the **Core Database**, images, **ocrBase** documents, and all transcripts.

This group can add information to the beginning of the **Attynote** field and the end of the **Issues** field, has read-only access to other fields and can tally and print. In addition, this group can annotate **ocrBase** documents and transcripts and can edit their own notes and make them **HotFacts**, but cannot otherwise edit notes.

These settings provide search, retrieval, and review access to the entire **Core Database**, with selected columns available for remote editing and the rest with read-only access.

TESTIFYING EXPERTS

This group has access to **Document Collections** limited to select records, images, and transcripts.

This group has read-only access to case elements, and does not have access to the **Core Database** or to transcript notes.

These settings provide limited access to specific information to prepare an expert to develop an opinion and testify appropriately. By placing specific, limited information in its own **Document Collection**, privileged and

work-product information is protected. This setup guards against inadvertent disclosure and unintended, court-ordered disclosure because the information that experts have access to is segregated from the rest of the database.

NON-TESTIFYING EXPERT CONSULTANTS

This group has access to **Document Collections** limited to select records, images, limited objective columns, and selected transcripts.

This group can add notes to a consultant's notes field, and has read-only rights to the rest of the data. This group can annotate transcripts and **ocrBase** documents, and can view images. Redactions and markups are burned-in on images for this group.

These settings provide a consulting expert with the ability to review and comment upon a selected group of documents as images and OCR text with limited access to database information.