Intralinks Access Gatekeeper User Guide

Intralinks 24x7x365 support US: + (1) 212 543 7800 UK: +44 (0)20 7623 8500.
See Intralinks login page for other national numbers

Table of Contents

Chapter 1: Introduction

Intralinks' Access Monitoring Service (AMS) provides visibility into your staff's exposure to deals or deal information on Intralinks exchanges and workspaces. The service gives those of you who support compliance, legal, audit, or the control room function within your organization the ability to determine which staff members should be monitored in their access to deals or deal information.

Note: Both Intralinks Platform exchanges and IL5 workspaces can be monitored. Throughout this document, the term *exchange* is used for both exchanges and workspaces.

In the Intralinks system, the staff members to be monitored become members of a group. Their members of a group. Their membership is defined by their email addresses. The exchanges to be monitored are associated with the monitored group. Your Intralinks representative works with you to identify the users and the exchanges to be monitored.

Using AMS, you can generate a report that contain various details about of the users who are being monitored. You can see detailed information about users' access to deals and, on exchanges enabled with the public/private feature, the users' ability to view private- and/or public-side information.

If your organization chooses to use the Access Gatekeeper feature, you also can control users' access to deals and deal information. As the Access Gatekeeper, you can restrict users' access to specific exchanges and determine whether they should be allowed to view public side information only. This feature enables you to more effectively adhere to the compliance policies established for your organization.

Chapter 2: Managing users in monitored groups

Overview

Users are monitored in their exchange access on a group basis. Managing users involves adding users to and removing them from monitored groups. A user's eligibility to become a member of monitored group is based on the domains defined to the group. These domains, and the exchanges to be monitored, are defined when the Intralinks administrator creates the monitored group.

In general, the Access Gatekeeper and Intralinks administrator can add users to a monitored group. However, the Intralinks administrator has broader privileges in performing this function.

The following table shows how the ability to manage users differs by role.

CDC-Monitored Group?*	**Task**	**Access Gatekeeper**	**Intralinks administrator**
No	Add user?	Yes	Yes
	Add user from different domain?	No	Yes
	Remove user?	Yes	Yes
Yes	Add user from different domain?	No	Yes
	Remove user?	No	No

***** *A CDC-monitored group is a group that has been defined with complete domain coverage (CDC). All users whose email addresses match the defined domains are automatically added to the monitored group. As new users with the same domains are added to the Intralinks global user directory, their names are also automatically added to the monitored group.*

Notice that only the Intralinks administrator is permitted to add users from other domains to a monitored group for which complete domain coverage (CDC) is enabled. However, neither the Intralinks administrator nor the Access Gatekeeper can remove users from a CDC-monitored group.

This chapter shows you how to add users to a non-CDC monitored group and remove them from the group.

If you have used Intralinks exchanges before, skip to "Adding users to a monitored group" on page 5. Otherwise, follow the procedure in the next section to log into Intralinks.

Logging into Intralinks

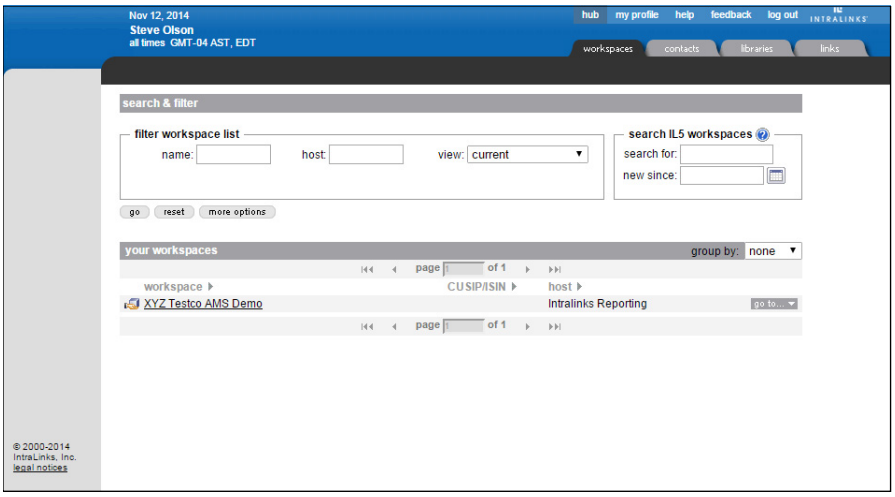
When the Intralinks administrator registers you as a user and establishes your role as Access Gatekeeper, you will receive an email containing a temporary password that you will use, along with your email address, to log into the system.

▶ To log in

1. Open your Internet browser and type **www.Intralinks.com** in the address window.
2. When the site is displayed, click the key icon in the upper left corner of the screen. A screen listing Intralinks services appears.
3. Click the **Intralinks (Dealspace, Fundspace, Debtspace, Studyspace, Connect)** option. The Intralinks login screen appears
4. Enter your email address and password, and then click **Log In**.

   If you use any Intralinks Platform exchanges, the Intralinks Platform **Hub** appears, displaying the exchanges to which you have access. Click the **Intralinks 5 Hub** option on the left side of the screen to display the IL5 **Hub**.

   If you do not use any Intralinks Platform exchanges, the IL5 **Hub** appears automatically.



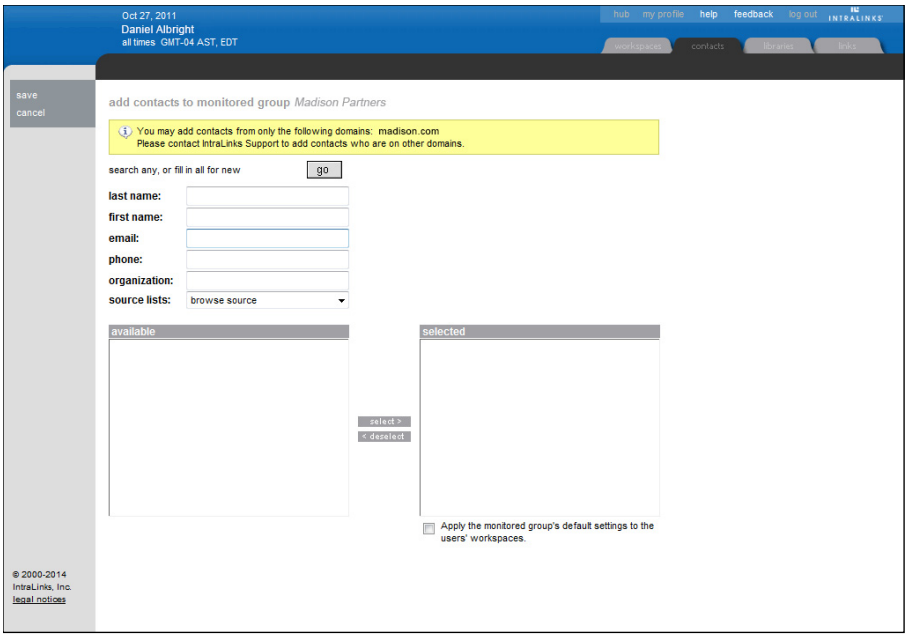
You will already have been informed of the name of the exchange containing the Access Monitoring Service reports. (These reports are described in Chapter 4, *Viewing AMS reports*, on page 20.) If you use other exchanges, those names will be displayed, as well.

Double-click the name of a exchange to enter the exchange.

Adding users to a monitored group

▶ To add users to a non-CDC monitored group

1. Display the **update default for users in monitored group** screen and click the **add users to this group** command. (For information about accessing this screen, see chapter Chapter 3, *Managing compliance settings*, on page 9.)



2. Enter the email address of the user you want to add to the monitored group and click **go**.

   If the user is not found, fill in all of the fields and click **go**.

   The user's name appears in the "available" pane.

3. Highlight the user's name in the "available" pane, and click the **select>** button to move the user's name to the "selected" pane.

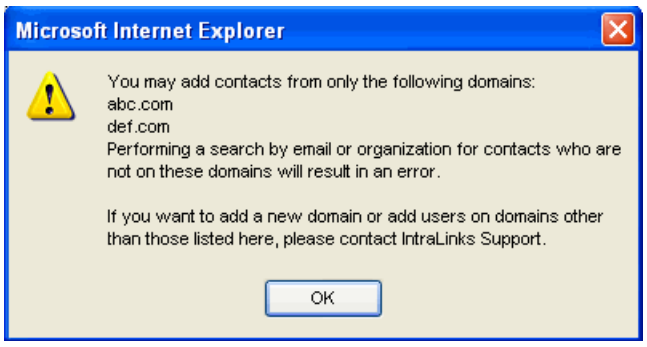
4. Repeat the previous two steps to continue to add users to the monitored group.

5. If you want to apply default exchange access settings to these users, click the check box at the bottom of the selected pane.

6. When you have finished adding the users, click the **save** command.

   The **monitored group report** screen is displayed. Clicking **cancel** also returns display to this screen. (For information about using this screen, see chapter 3.)

Note: If you attempt to add a user on a domain other than the domains defined for the monitored group, the following message will appear:



The message reminds you that you can add users only on the defined domains and recommends that you contact Intralinks to add users on other domains to this group. The Intralinks administrator adds you as Access Gatekeeper to this group.

Note: If you attempt to add a user who is a member of another Access Gatekeeping monitored group, the following message is displayed:

The message states the name and organization of the user. If you want to remove users from the monitored group of which they are already members, contact Intralinks.

Also, if you inadvertently attempt to add a user to a monitored group who is already a member of the same group, this action will not be completed and no message will be displayed.

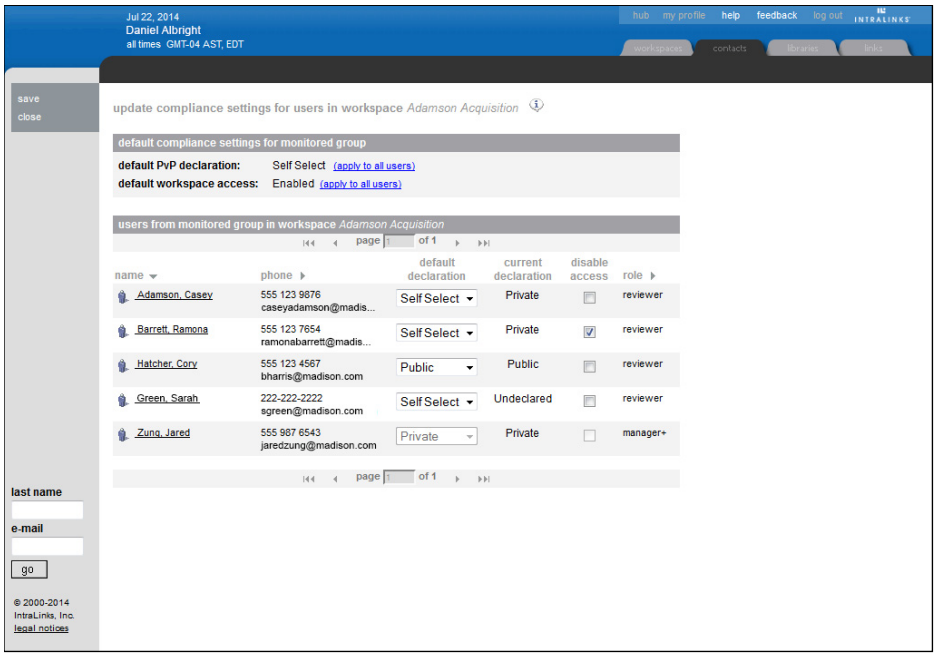
Removing users from a monitored group

You can remove users from a monitored group on the *update defaults for users in monitored group* screen, described in chapter 3. Select the user and click the **remove** command on this screen.

Viewing a list of monitored workspaces and exchanges

The **workspace list** screen allows you to view a list of all Intralinks Platform exchanges and IL5 workspaces that include members of the selected business group. The screen includes all active exchanges and workspaces in the active, hold and preparation phases. You can filter the list by exchange/workspace name, host and phase.

To display the **workspace list** screen, click the workspace list link on the **monitored group report** screen.



Only exchanges in which the users are monitored are included on the **Workspace List** screen.

Chapter 3: Managing compliance settings

Overview

The term “Access Gatekeeper” is the Intralinks term for someone in the position to monitor users’ access to information on Intralinks exchanges. In the role of Access Gatekeeper, you are not only able to do this but also to restrict a user’s access to exchanges or to private side information on a public/private-enabled exchange if you feel such access might present compliance issues within your organization. You can also determine whether a user should make this determination on his or her own. (For information about the public/private feature, see *Securing Private Side Information on the Intralinks Exchange: A Guide for Exchange Managers & Publishers*.)

Monitoring users is facilitated by grouping the users to be monitored. Users are grouped together according to their domains and the exchanges they can access. (The domains and exchanges are defined to the monitored group by the Intralinks administrator, an Intralinks staff member responsible for assisting you in your Access Gatekeeper role.) You can oversee multiple monitored groups, and more than one Access Gatekeeper can oversee the same monitored group. You yourself may be in a position to be monitored as well, but you will not be a member of the group you are monitoring. Also, you may serve exclusively in the role of Access Gatekeeper and have no reason to access exchanges.

Ample methods are built into the system for communicating to the user and to exchange managers why the user may not be permitted access to a exchange or exchange content, as well as how to contact the relevant party if questions arise about a user’s restricted access.

This chapter shows you how to control users’ access to exchanges and exchange content.

Compliance setting definitions

This section defines the different compliance settings that you apply to control a user’s access to exchanges and exchange content.

The values that you specify to control a user’s access to a exchange are defined in the following table.

Exchange access settings	
Value	Effect
Enabled	User can access all exchanges to which user has access. (Default)
Disabled – all	User cannot access any exchanges.
Disabled – non-PvP	User can access only public/ private-enabled* exchanges to which user has access.

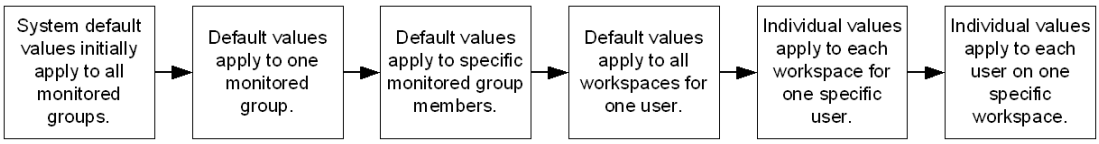
** Public/private-enabled exchanges are exchanges on which the exchange manager has differentiated public side information from private side information.*

The values that you specify to control a user's access to public/private side information on a exchange are defined in the following table.

Public/private content preference declaration settings	
Value	Effect
Public	User can view information appropriate only for the public side on public/private-enabled exchanges to which user has access.
Self-Select	User can choose to view only public, or both public and private information on public/ private-enabled exchanges to which user has access. (System default)

On public/private-enabled exchanges, the user makes a content preference declaration about viewing public or private side information. You have the ability to determine and override the user's declaration.

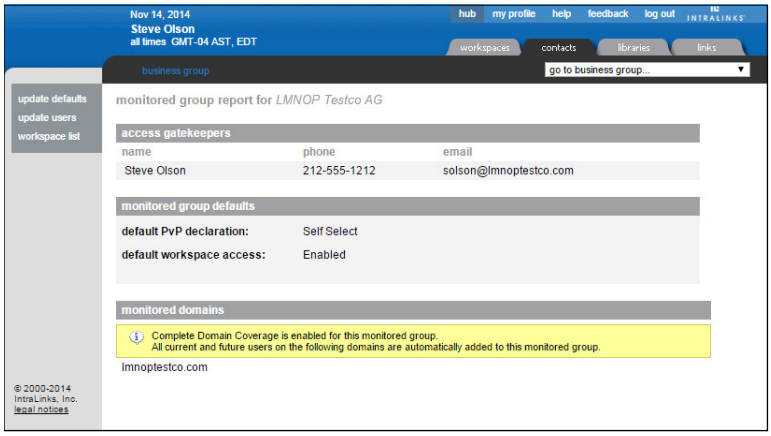
The following graphic represents the flow that you may follow when assigning access rights. Any of these values (except for the system default values) can be modified at any time. The information in this chapter is presented in the order shown in the graphic.



As users become members of a monitored group, the default values assigned to the group govern their ability to access both their existing and future exchanges (defined by product code). These values can be overridden at the group level, individual user level, and exchange level.

Assigning values for exchange access and exchange content

You begin the process of assigning access values from the monitored group report screen for the selected group. To access this screen, click the contacts tab dropdown list and select the group name. If you are assigned to only one monitored group, the monitored group report screen will be immediately displayed.



The contact information for the Access Gatekeepers assigned to this group appears in the top section of this screen. The current default values applied to all users in the group appear in the middle section of the screen. The domains defined for the monitored group are listed in the lower section. If complete domain coverage was defined for the group, this is stated as an informational message in the lower section of the screen. (For information about complete domain coverage, see Chapter 2, *Managing users in monitored groups*, on page 4.)

You use this screen to assign or update default access values for the users in the monitored group and to add users to the group. (Managing users in a monitored group is explained in chapter 2.)

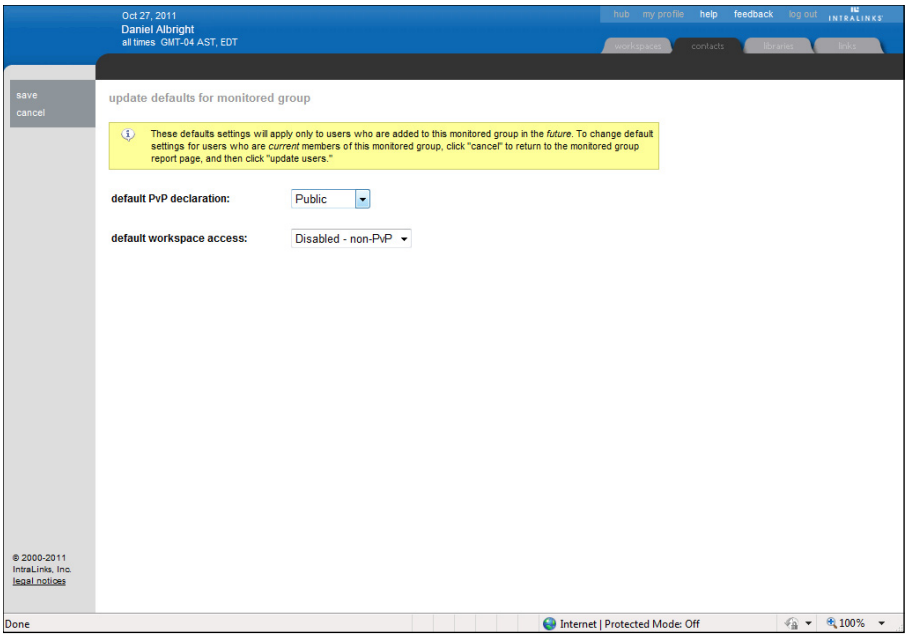
Assigning group default access values

You begin by assigning default access values to future members of the monitored group. When users are added to the group, they automatically inherit these values for their exchanges as they are added to them.

Note: These values do not apply to current group members' exchanges. Changing current members' default access values is performed on another screen. For more information, see "Assigning default values to current group members" on page 12.

▶ To assign group default access values

1. On the *monitored group report* screen, click the **update defaults** command. The **update defaults for monitored group** screen is displayed.



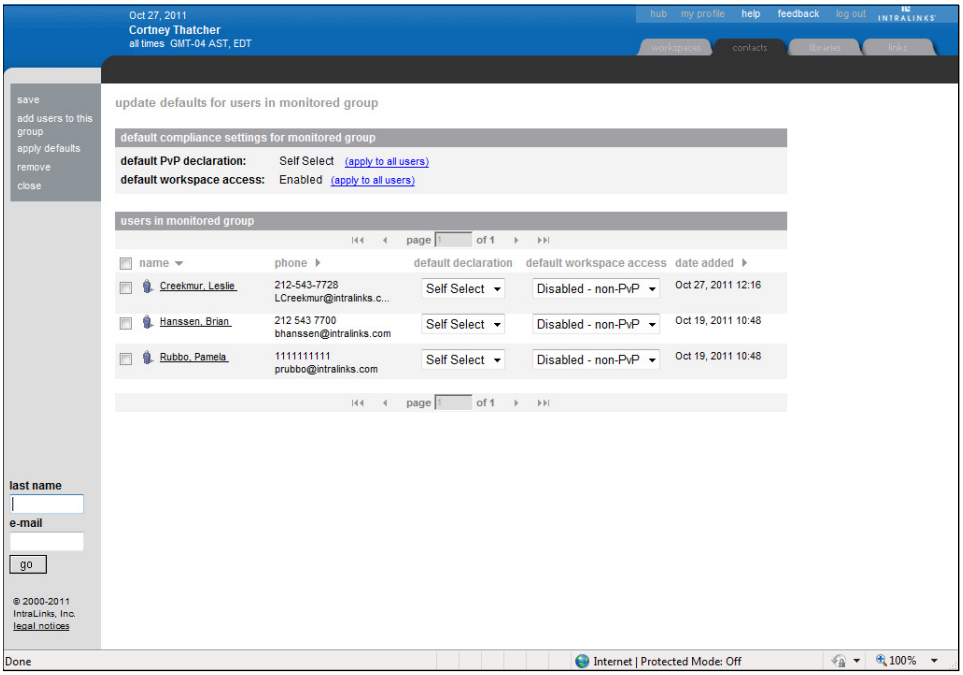
2. If the public/private feature is enabled for exchanges, select the desired value from the **default PvP declaration** dropdown list. The values are **Public** and **Self Select**.
3. Select the desired value from the default exchange access dropdown list. The values are **Enabled, Disabled - All**, and **Disabled - Non PvP**.
4. Click the **save** command to save the values you selected.

   Clicking **cancel** ignores any changes you made to this screen. Both actions return display to the **monitored group report** screen.

Assigning default values to current group members

You can assign default access values to all current group members' existing or future exchanges. This task assumes that you have already added members to the monitored group.

To assign values to current group members, click the **update users** command on the *monitored group report* screen. The **update defaults for users in monitored group** screen is displayed.

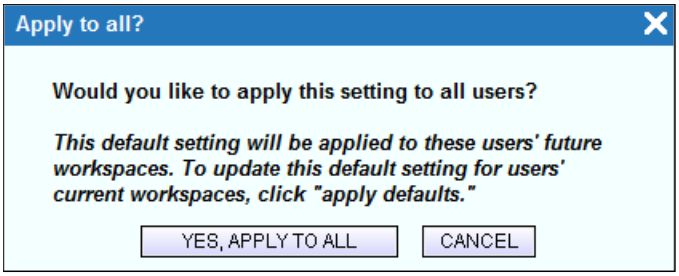


This screen displays all of the current members of the monitored group, along with their contact information and the date they were added to the group. The default compliance settings at the top of the screen that were applied to all future members of the monitored group (see "Assigning group default access values" on page 11) can be applied to all of the current members' future exchanges.

The current default declaration to be applied to all of each user's exchanges is displayed in the *default declaration* column corresponding to the user. The current default access setting to be applied to all of the user's exchanges is displayed in the *default exchange access* column. These values will be applied to all of the user's existing exchanges.

▶ To assign group default values to current members' future exchanges

1. Click **apply to all users** for either or both default settings at the top of the screen. The following message is displayed.



2. Click **Yes, Apply to All** to confirm your action, or **Cancel** to cancel the action.

▶ *To assign default values to current members' existing exchanges*

1. Click the check box corresponding to the user's name, and then select the value from the **default declaration** and **default access** dropdown lists as

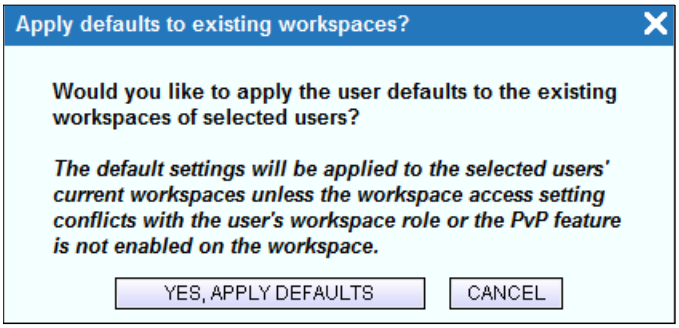
required. This means that all exchanges currently accessed by the selected user will have the same settings.

For example, assume that Sue currently has access to three exchanges. You assign Sue's default exchange access as **enabled** and her default declaration as **public**. This means that Sue will be able to access all three exchanges and see *only* public side information on each exchange (assuming that the public/private feature is enabled for each exchange).

To view a user's name that is not readily visible on the screen, enter the user's last name or email address in the corresponding search field and click **go**.

If you want to select all of the users in the monitored group, regardless of whether their name is readily visible on the screen, click the *name* check box.

2. When you have finished assigning values for selected users, click the **apply defaults** command. The following message is displayed.



Note: You may know that a user listed on this screen has a exchange role that cannot be restricted, such as a exchange manager. This message informs you that the assigned values will not be applied to such users. This will be explained in the next section.

3. Click **Yes, Apply Defaults** to save the new values. The *monitored group report* screen is displayed. Clicking **Cancel** displays the current screen.

Other tasks performed on this screen

Removing users

You also use this screen to remove users from the monitored group. However, before attempting to remove a user, you should be aware of the following conditions:

- Users cannot be members of a monitored group that was created with the complete domain coverage (CDC) feature. The only ways to remove a user from a CDC-monitored group are to remove the user's domain from the monitored group or to deregister the user.
- Users must be removed from all monitored exchanges on which they are active before they can be removed from the group.

Note: No message is displayed informing you that the user has been removed from the group.

To remove one or more users from the monitored group, click the check box corresponding to each user's name, and then click the **remove** command. A

message appears confirming whether you want to remove the user's name. (Note that the **remove** command does not appear if the monitored group was defined with complete domain coverage.)

Adding users

You also use this screen to access the screen you use to add users to the monitored group by clicking the **add users to this group** command. Note, however, that if this monitored group was defined with complete domain coverage, only the Intralinks administrator can add users to the group. (Adding users to a monitored group is explained in chapter 2.)

Save your changes!

When you have finished working with the **update default for users in monitored group** screen, remember to click **save** to save all the changes made to this series of screens.

If you attempt to navigate to another page of users without saving the selections made on the currently displayed page, a message will appear informing you that your selections will not be retained.

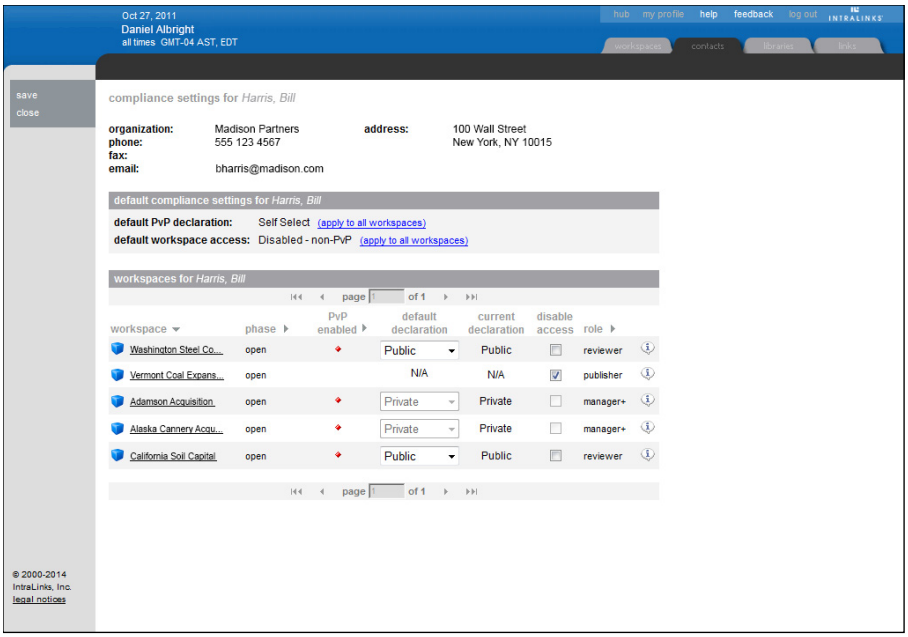
Assigning values to a specific user's exchanges

You can change the compliance settings on each existing exchange accessed by a specific user, with the following exceptions:

- Managers' and publishers' declaration values are always "private."
- Users cannot be restricted from exchanges on which they serve as any level of manager, as a publisher + or as a reviewer+. The system recognizes these users in their exchange roles and pre-defines the values.

▶ **To assign values for a specific user's exchanges**

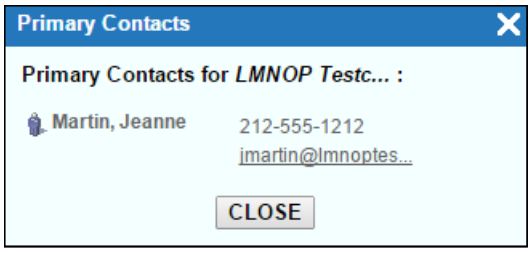
◇ On the **update default for users in monitored group** screen, click the user's name. The compliance settings for the selected user are displayed.



The user's name and contact information are displayed at the top of the screen. The **default compliance settings** section displays the values that can be assigned to all of the user's existing exchanges.

The **monitored exchanges** section displays:

- All of the monitored exchanges on which the user is active.
- An icon representing public/private-enabled exchanges.
- The current default declaration and current declaration values for the exchange.
- A check box used to disable the user's access to a exchange.
- The user's role on the exchange.
- A link to the name of the exchange's primary contact's information. When you click this icon, a message similar to the one shown here is displayed:

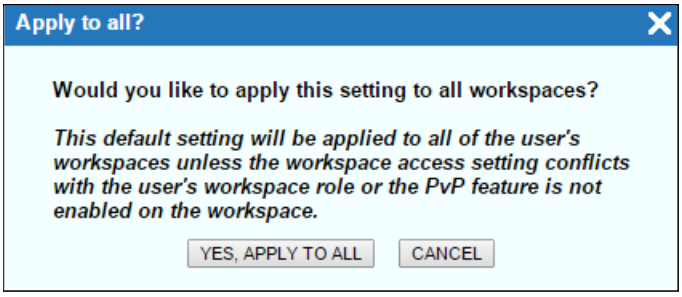


Multiple exchange contacts' names may also appear in this message.

You can review and modify the user's current default values for all exchanges, or modify settings on a exchange-by-exchange basis.

▶ To modify the user's current default value to be applied to all exchanges

1. Click **apply to all exchanges** for either or both default settings at the top of the screen. A message prompts you to confirm your action.



2. Click the appropriate response.
3. In the **monitored exchanges** section of the screen, you may note that some selections are not available to you. These selections correspond to users whose exchange roles do not allow you to restrict them from accessing exchanges or exchange content. The following table displays the values that can be assigned to users' exchanges according to their roles on the exchange.

Role	Public or Self Select	Disable Access?
Reviewer	Public or Self Select	Yes
Reviewer+	Public or Self Select	No
Previewer	Public or Self Select	Yes
Previewer+	Self Select	No
Publisher	Self Select	Yes
Publisher+	Self Select	No
All Managers	Self Select	No

Here are a few scenarios to explain the values that can be applied to a user:

- Rebecca is a manager on exchange ABC, which is public/private-enabled. Therefore, her **default declaration** value is **Private**, as is the **current declaration** value. The **default declaration** value cannot be changed. Rebecca's access to the ABC exchange cannot be disabled, so the **disable access** check box is inactive.
- Rebecca is a reviewer on exchange XYZ, which is public/private-enabled. While Rebecca's **current declaration** value is **Public**, you know that her access to private side information will not pose a compliance risk. Therefore, you can change the *default declaration* value to **Self Select**. Now Rebecca can determine for herself whether she wants to access public or private information on the XYZ exchange.
- Rebecca is a reviewer on exchange WKS, which is *not* enabled for the public/private feature. Since you believe that Rebecca's access to information on this exchange may cause a compliance risk, you check the

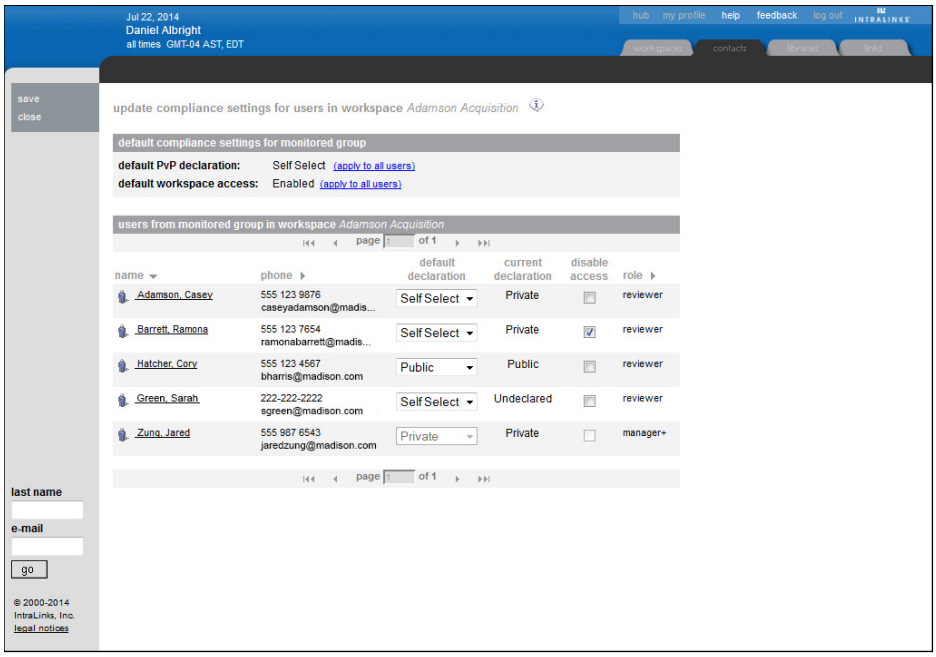
disable access check box, thus preventing Rebecca from accessing exchange WKS.

4. To modify the default declaration for a exchange, select the desired value from the corresponding **default declaration** dropdown list.
5. To disable the user's access from the exchange, click the corresponding check box in the **disable access** column.
6. When you have made the desired changes to this screen, click the **save** command to save your changes.

If you attempt to navigate to another page without saving the selections made on the currently displayed screen, you will be prompted to save changes.

Assigning values to monitored group members on the same exchange

You can view the monitored group members who are active on a specific exchange and modify their default declaration and default access values. To do this, click the exchange name on the **compliance settings for <username>** screen. This displays the **update compliance settings for users in <exchange name>** screen.



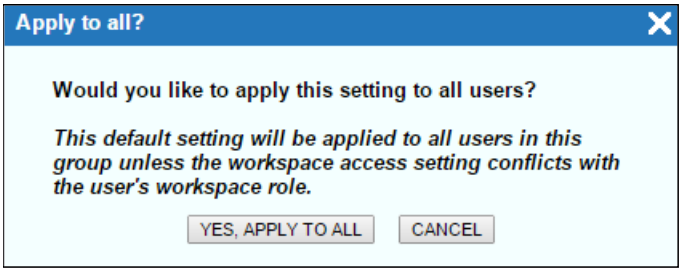
This screen lists the name of each user who is active on the exchange, the user's contact information, the user's current declaration value, and the user's role on this exchange. The  is a link to the name of the exchange's primary contact's information.

You can scroll through pages if the number of users on this exchange exceeds the screen size limits. You can also search for a user by last name or email address.

You can apply the monitored group's default values to all users on this exchange, or modify the values for individual users.

▶ To assign the monitored group's default values to all of the users on this exchange

1. Click **apply to all users** for either or both of the default settings at the top of this screen. The following message is displayed.



2. Click **Yes, Apply to All** to confirm your action, or **Cancel** to cancel the action. The message disappears from the screen.

▶ To modify an individual user's values

1. Display the desired value for a user's default declaration in the *default declaration* column. Remember that you cannot change a exchange manager's or publisher's default declaration because they are always **Private**.

   Note: If the public/private feature is not enabled for the exchange, the default declaration and current declaration columns are not displayed.

2. Click the check box in the *disable* column corresponding to the users whose access to this exchange should be restricted.

If you attempt to navigate to another page or close this window before you save your changes, a message reminds you to save your changes.

Chapter 4: Viewing AMS reports

Overview

User access to exchange and exchange content is monitored by Intralinks' Access Monitoring Services (AMS), which produces a report, on a daily or weekly basis, that is accessible from a predetermined secure exchange. The following information is included in the AMS report:

- Access detail – for each deal on which a monitored user is active, a list of items that have been viewed by any of the users, including the item's title and folder, the item's public/private content classification (where available), the name of the user who accessed the item, and the access date/time.
- Exposure detail – a list of all deals the monitored users have access to, including the name of the user who last accessed each deal and the date of this access.
- Exposure by user – for each monitored user, a list of the deals the user has access to and his/her public/private declaration for the deal (if the public/private feature is enabled).
- Public/private declarations – for each monitored user, an audit of each time the user has changed his/her declaration during the reporting period on all the deals accessible by the user.
- Monitored users – a control report that identifies every employee who has an Intralinks ID and is being monitored by AMS reporting.

  The report is available in either Microsoft Excel (.xls) or Extensible Markup Language (.xml) format.

  Note: XML report generation is recommended for its portability to other databases for ease of data manipulation and reporting purposes. XML is also ideal for clients with a large Intralinks user base and corresponding volume of exchange exposure, thus avoiding the row limitations of Excel. Two additional files (ams_default.dtd and AMS XML Report.doc) have been added to your exchange to help your IT team assist you in interpreting the contents of the XML file.

Viewing AMS reports

AMS reports are generated on the basis (daily or weekly) and in the format (Excel or XML) that you arranged with your Intralinks representative. Your representative also informed you about the name of the exchange to which the generated AMS report would be delivered. You serve in the role of manager on this exchange.

Reports are generated overnight and delivered to the exchange by 10 a.m. on the day you expect to receive the report. An email alert is your signal that the report is ready for viewing. You will be informed about delays in report generation in an email from Intralinks.

To view AMS reports

1. Log into Intralinks and go to the exchange containing the AMS report. If you have access to only one exchange on Intralinks, that exchange will appear automatically when you log in.
2. Click the **publication** tab to view the list of AMS reports.

   The reports are organized in folders, first by year and then by month. Within each month's folder is a publication that contains AMS reports for specific time periods.
3. Display the name of the desired report by clicking the publication name or expanding (clicking the **+**) the publication.
4. Click the report name, then select **Open** in the dialog box.
5. The report is displayed. You can also choose to save the report to a local drive.
6. Click **close** to return to the list of AMS reports.

Deleting AMS reports

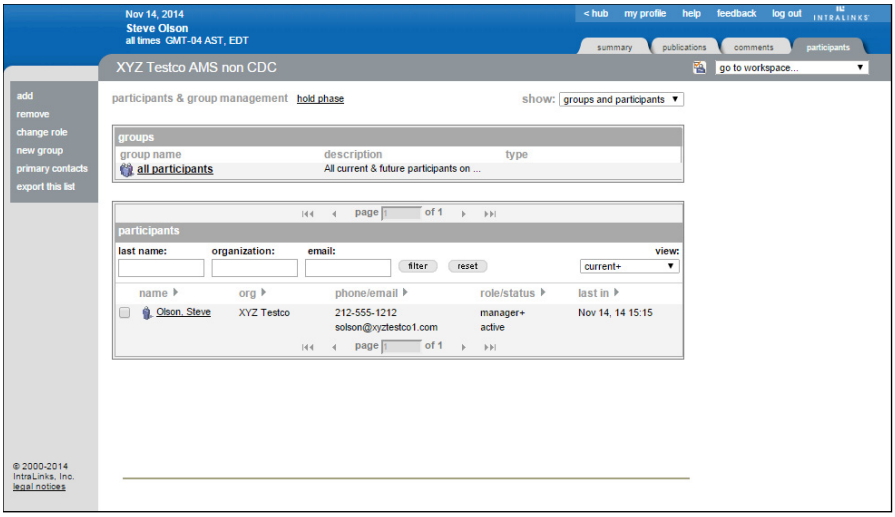
You can delete AMS reports from view but not delete them from the Intralinks system. On the screen that lists the publications on the exchange, click the **delete** command on the left side of the screen or from the *action* menu to the right of each publication.

To view a list of deleted reports, select **deleted** from the view field on the screen listing the publications, then click **go**.

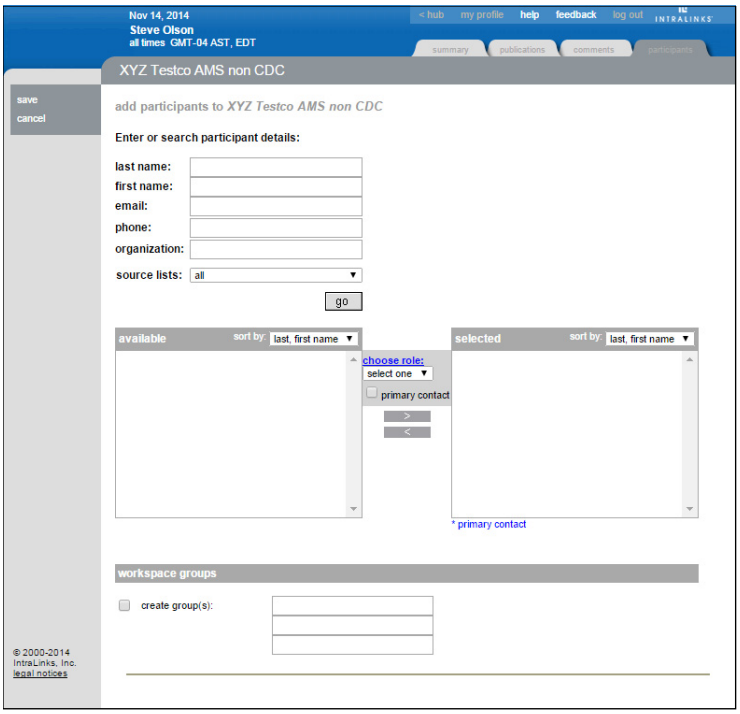
Enabling colleagues to view AMS reports

You can add colleagues to the AMS reports exchange so that they can receive alerts when reports are available for viewing. To do this:

1. With the AMS reporting exchange displayed on the screen, click the **participants** tab. This displays the **participants & group management** screen.



2. Click the **add** command. This action displays the screen on which you provide information about the colleague you want to add to the exchange.



3. Enter your colleague's name, email address, phone number, and organization in the appropriate fields.
4. Click **go**.
5. Your colleague's name is added to the "available" list.
6. Select the **reviewer** exchange role from the dropdown list to give your colleague read-only access rights. Select the manager role to give your colleague the ability to delete reports and to add other colleagues.
7. Click the right arrow button (**>**) to add the name to the "selected" list.
8. Click **save**.

   This action adds your colleague's name to the exchange and sends your colleague two email alerts: one is an invitation to the exchange, and the other is a temporary password.